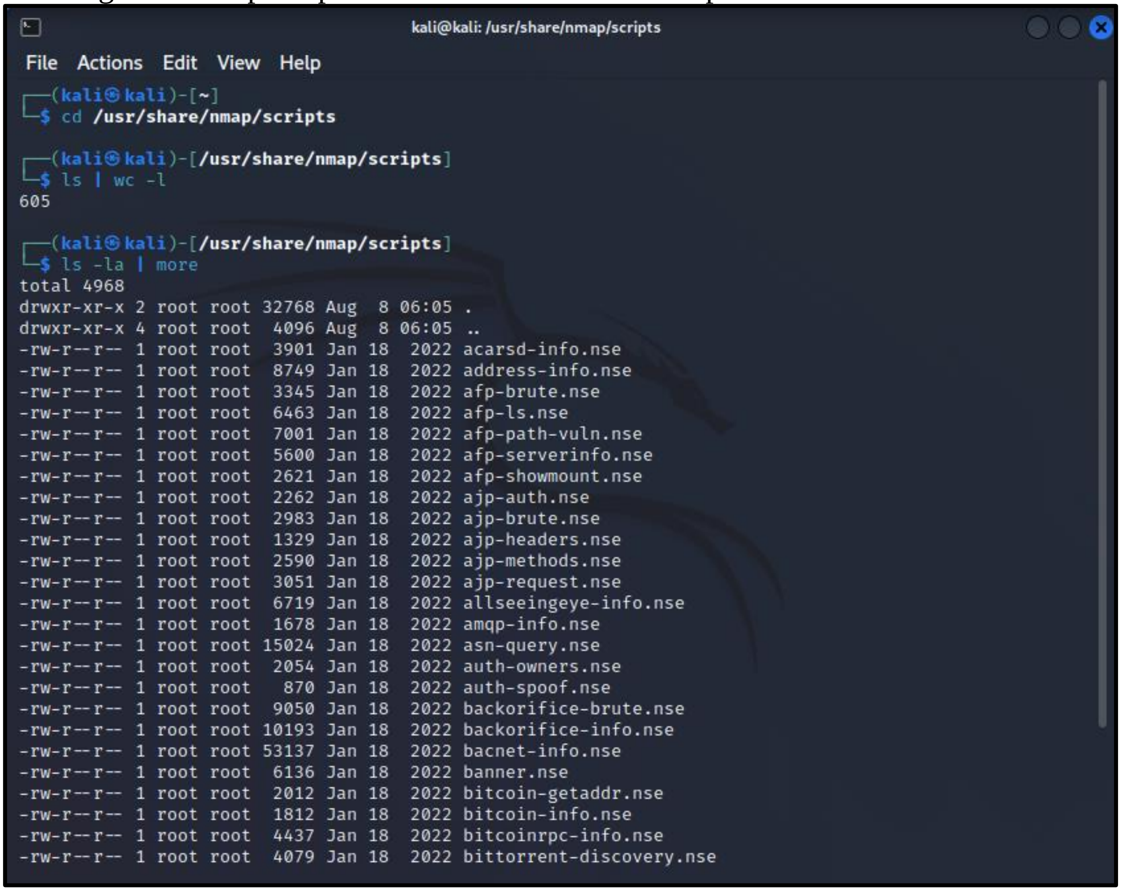
Practical 4

Aim: Practical on vulnerability scanning and assessment

Vulnerability Scanning using Nmap:

1. Navigate to nmap scripts folder and view all the scripts in that folder

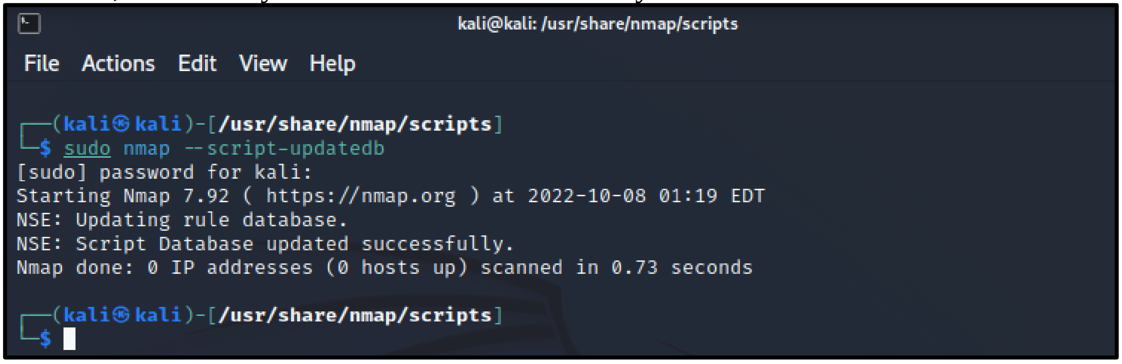


kali@kali: /usr/share/nmap/scripts
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ cd /usr/share/nmap/scripts

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ ls | wc -l
605

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ ls -la | more
total 4968
drwxr-xr-x 2 root root 32768 Aug  8 06:05 .
drwxr-xr-x 4 root root  4096 Aug  8 06:05 ..
-rw-r--r-- 1 root root  3901 Jan 18  2022 acarsd-info.nse
-rw-r--r-- 1 root root  8749 Jan 18  2022 address-info.nse
-rw-r--r-- 1 root root  3345 Jan 18  2022 afp-brute.nse
-rw-r--r-- 1 root root  6463 Jan 18  2022 afp-ls.nse
-rw-r--r-- 1 root root  7001 Jan 18  2022 afp-path-vuln.nse
-rw-r--r-- 1 root root  5600 Jan 18  2022 afp-serverinfo.nse
-rw-r--r-- 1 root root  2621 Jan 18  2022 afp-showmount.nse
-rw-r--r-- 1 root root  2262 Jan 18  2022 ajp-auth.nse
-rw-r--r-- 1 root root  2983 Jan 18  2022 ajp-brute.nse
-rw-r--r-- 1 root root  1329 Jan 18  2022 ajp-headers.nse
-rw-r--r-- 1 root root  2590 Jan 18  2022 ajp-methods.nse
-rw-r--r-- 1 root root  3051 Jan 18  2022 ajp-request.nse
-rw-r--r-- 1 root root  6719 Jan 18  2022 allseeingeye-info.nse
-rw-r--r-- 1 root root  1678 Jan 18  2022 amqp-info.nse
-rw-r--r-- 1 root root 15024 Jan 18  2022 asn-query.nse
-rw-r--r-- 1 root root  2054 Jan 18  2022 auth-owners.nse
-rw-r--r-- 1 root root   870 Jan 18  2022 auth-spoof.nse
-rw-r--r-- 1 root root  9050 Jan 18  2022 backorifice-brute.nse
-rw-r--r-- 1 root root 10193 Jan 18  2022 backorifice-info.nse
-rw-r--r-- 1 root root 53137 Jan 18  2022 bacnet-info.nse
-rw-r--r-- 1 root root  6136 Jan 18  2022 banner.nse
-rw-r--r-- 1 root root  2012 Jan 18  2022 bitcoin-getaddr.nse
-rw-r--r-- 1 root root  1812 Jan 18  2022 bitcoin-info.nse
-rw-r--r-- 1 root root  4437 Jan 18  2022 bitcoinrpc-info.nse
-rw-r--r-- 1 root root  4079 Jan 18  2022 bittorrent-discovery.nse
```

2. Update scripts

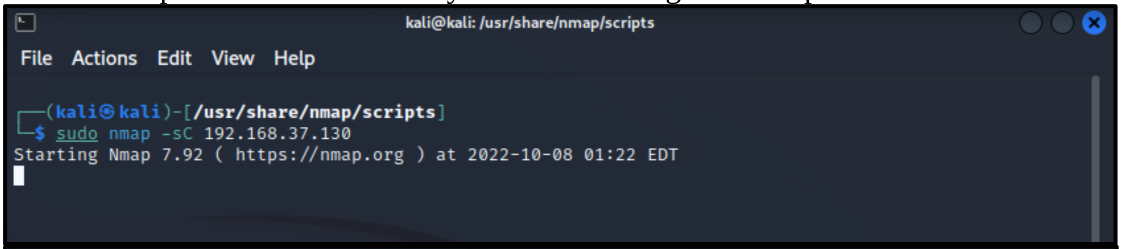
Before Nmap can be used to perform a vulnerability scan, penetration testers must update the Nmap script database to see whether there are any new scripts added to the database, so that they do not miss the vulnerability identification.



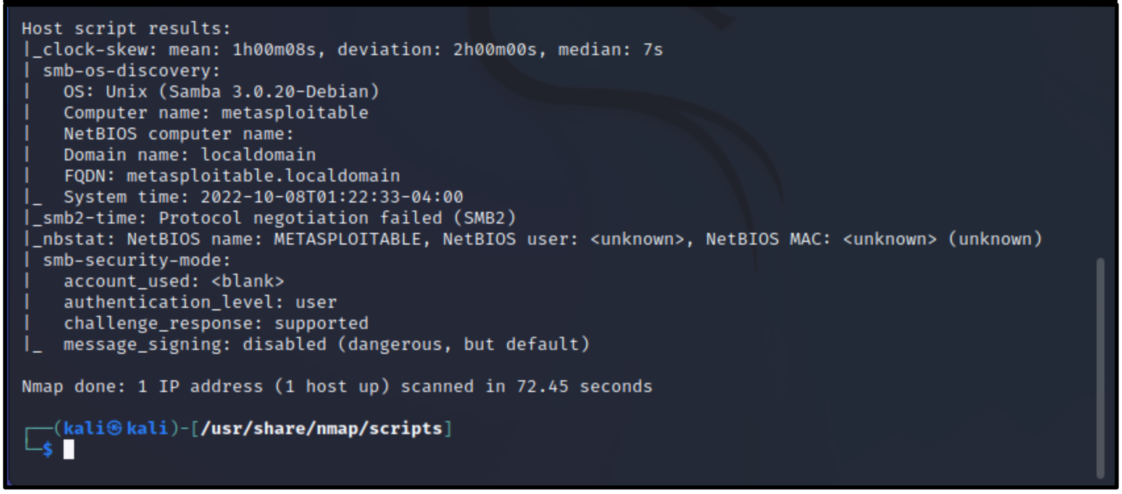
kali@kali: /usr/share/nmap/scripts
File Actions Edit View Help

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap --script-updatedb
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-08 01:19 EDT
NSE: Updating rule database.
NSE: Script Database updated successfully.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.73 seconds

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ 
```

3. Run Nmap to check vulnerability services running on metasploitable2.

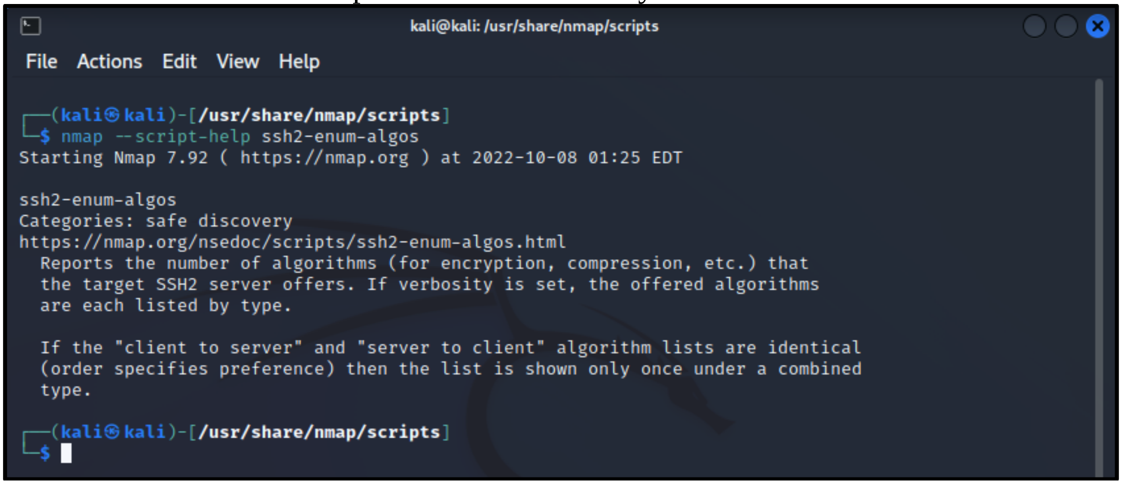

kali@kali: /usr/share/nmap/scripts
File Actions Edit View Help

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -sC 192.168.37.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-08 01:22 EDT
```



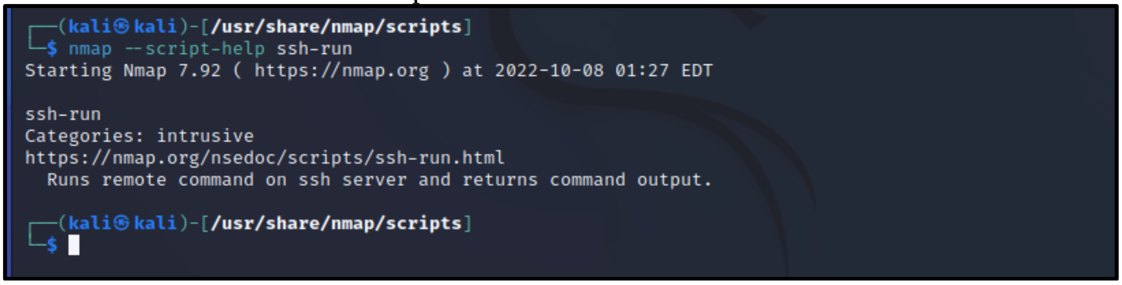
```
Host script results:
|_clock-skew: mean: 1h00m08s, deviation: 2h00m00s, median: 7s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2022-10-08T01:22:33-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Nmap done: 1 IP address (1 host up) scanned in 72.45 seconds

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$
```

4. Let us find available scripts to find vulnerability for ssh.


kali@kali: /usr/share/nmap/scripts
File Actions Edit View Help

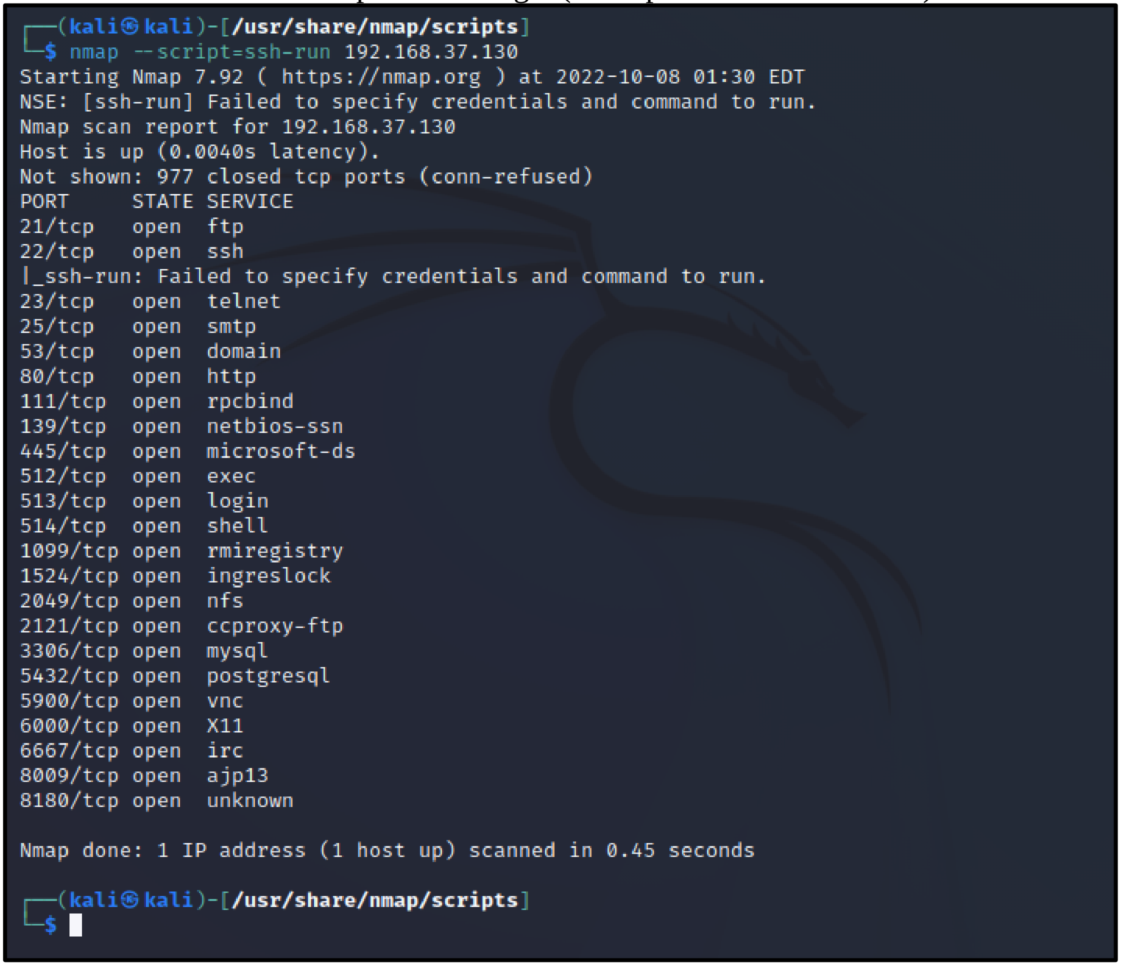
```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script-help ssh2-enum-algos
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-08 01:25 EDT

ssh2-enum-algos
Categories: safe discovery
https://nmap.org/nsedoc/scripts/ssh2-enum-algos.html
  Reports the number of algorithms (for encryption, compression, etc.) that
  the target SSH2 server offers. If verbosity is set, the offered algorithms
  are each listed by type.

  If the "client to server" and "server to client" algorithm lists are identical
  (order specifies preference) then the list is shown only once under a combined
  type.

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$
```

5. Get more info on ssh-run script



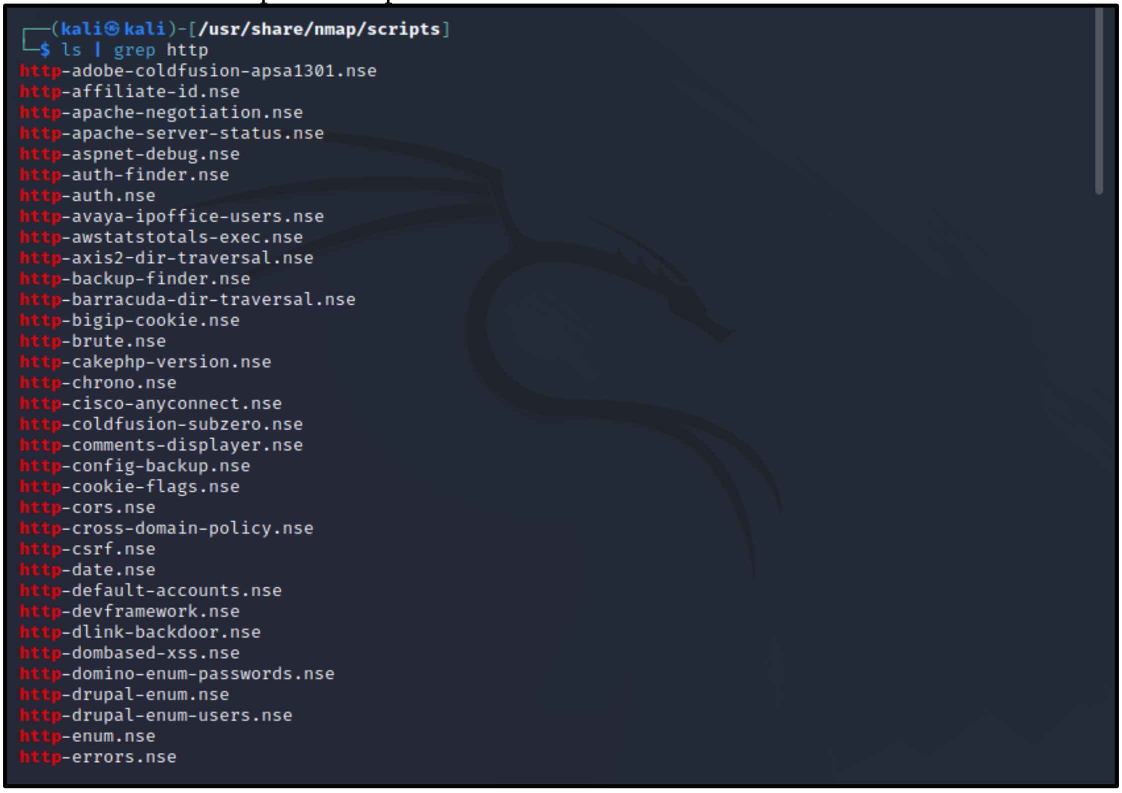
```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script-help ssh-run
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-08 01:27 EDT

ssh-run
Categories: intrusive
https://nmap.org/nsedoc/scripts/ssh-run.html
  Runs remote command on ssh server and returns command output.

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$
```

6. Let’s run the ssh-run script on our target (metasploitable2 IP Address)



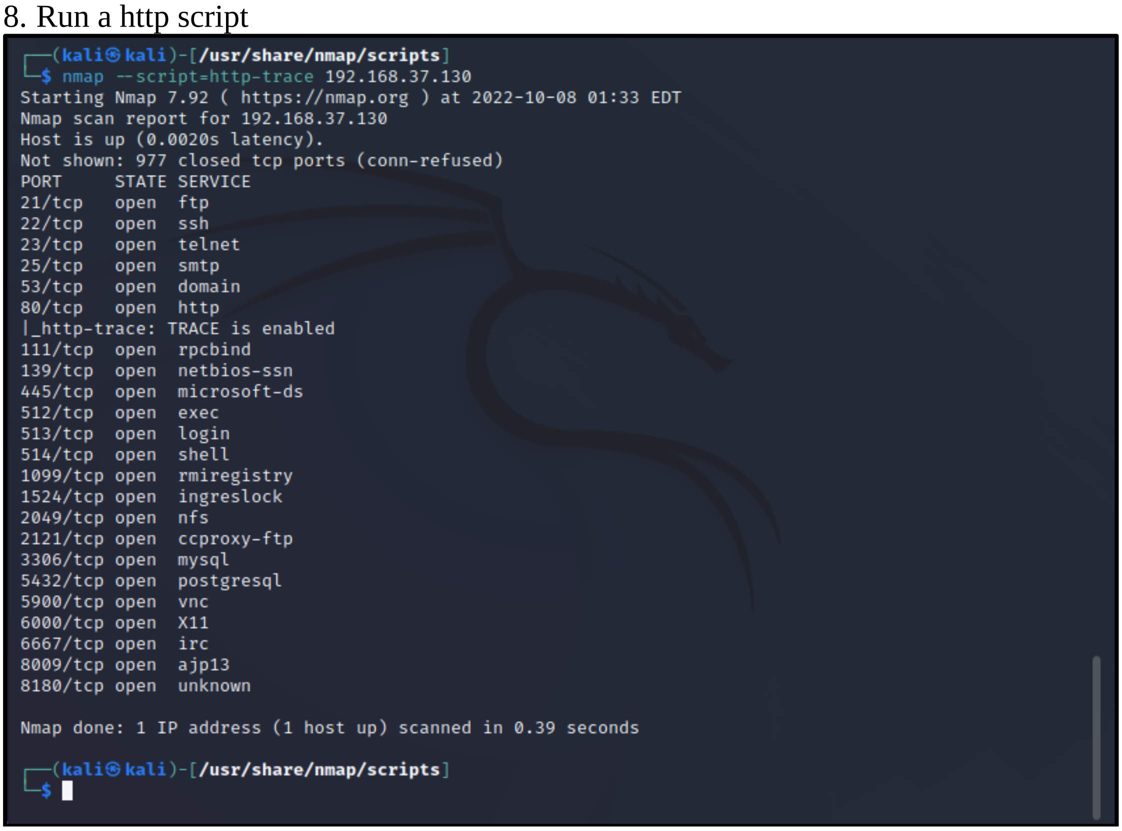
```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script=ssh-run 192.168.37.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-08 01:30 EDT
NSE: [ssh-run] Failed to specify credentials and command to run.
Nmap scan report for 192.168.37.130
Host is up (0.0040s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
|_ssh-run: Failed to specify credentials and command to run.
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

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

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ 
```

7. Get available scripts for http



```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ ls | grep http
http-adobe-coldfusion-apsa1301.nse
http-affiliate-id.nse
http-apache-negotiation.nse
http-apache-server-status.nse
http-aspnet-debug.nse
http-auth-finder.nse
http-auth.nse
http-avaya-ipoffice-users.nse
http-awstatstotals-exec.nse
http-axis2-dir-traversal.nse
http-backup-finder.nse
http-barracuda-dir-traversal.nse
http-bigip-cookie.nse
http-brute.nse
http-cakephp-version.nse
http-chrono.nse
http-cisco-anyconnect.nse
http-coldfusion-subzero.nse
http-comments-displayer.nse
http-config-backup.nse
http-cookie-flags.nse
http-cors.nse
http-cross-domain-policy.nse
http-csrf.nse
http-date.nse
http-default-accounts.nse
http-devframework.nse
http-dlink-backdoor.nse
http-dombased-xss.nse
http-domino-enum-passwords.nse
http-drupal-enum.nse
http-drupal-enum-users.nse
http-enum.nse
http-errors.nse
```

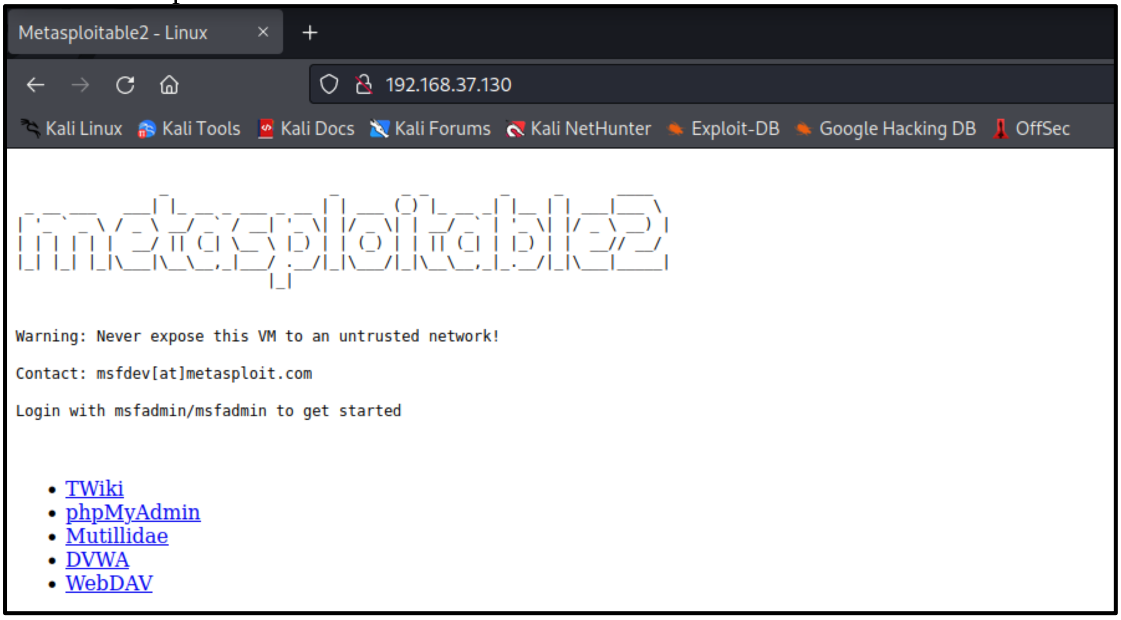
8. Run a http script



```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script=http-trace 192.168.37.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-08 01:33 EDT
Nmap scan report for 192.168.37.130
Host is up (0.0020s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
|_http-trace: TRACE is enabled
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ 
```

Web Server Vulnerability Scanning:

1. Run metasploitable2 website on Firefox in kali linux



```
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          
```

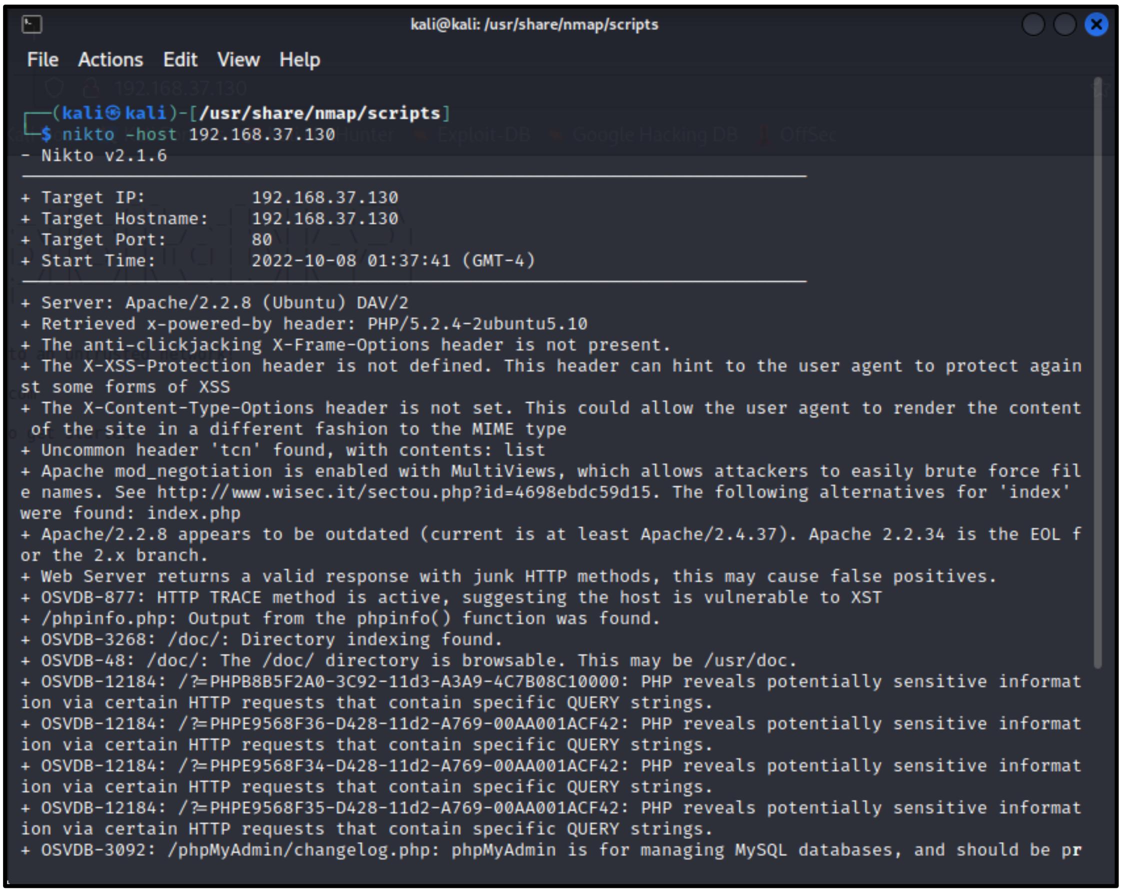
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

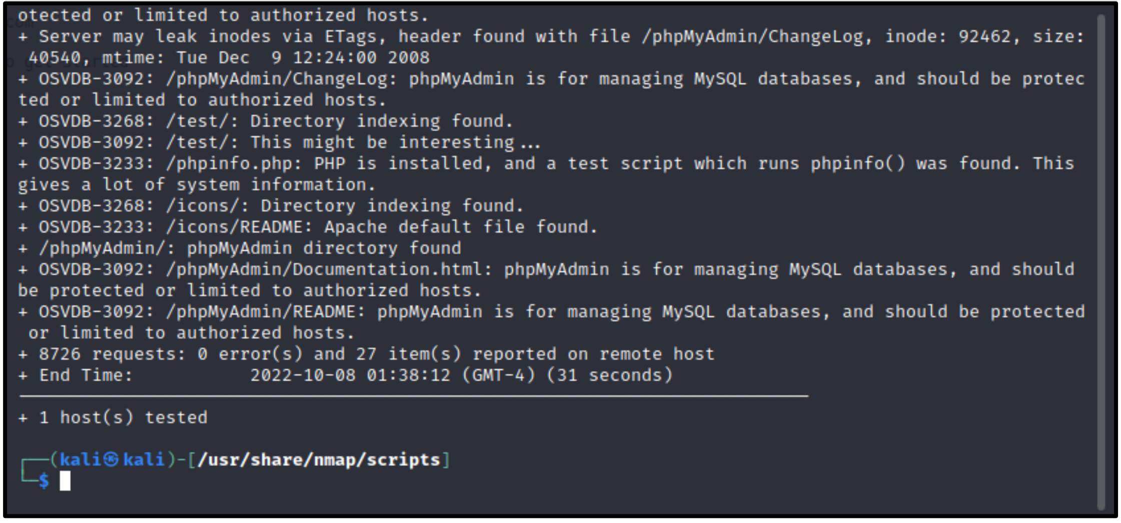
Login with msfadmin/msfadmin to get started

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

2. Using Nikto tool scan the target for vulnerabilities
“ nikto -host 192.168.37.130 ”



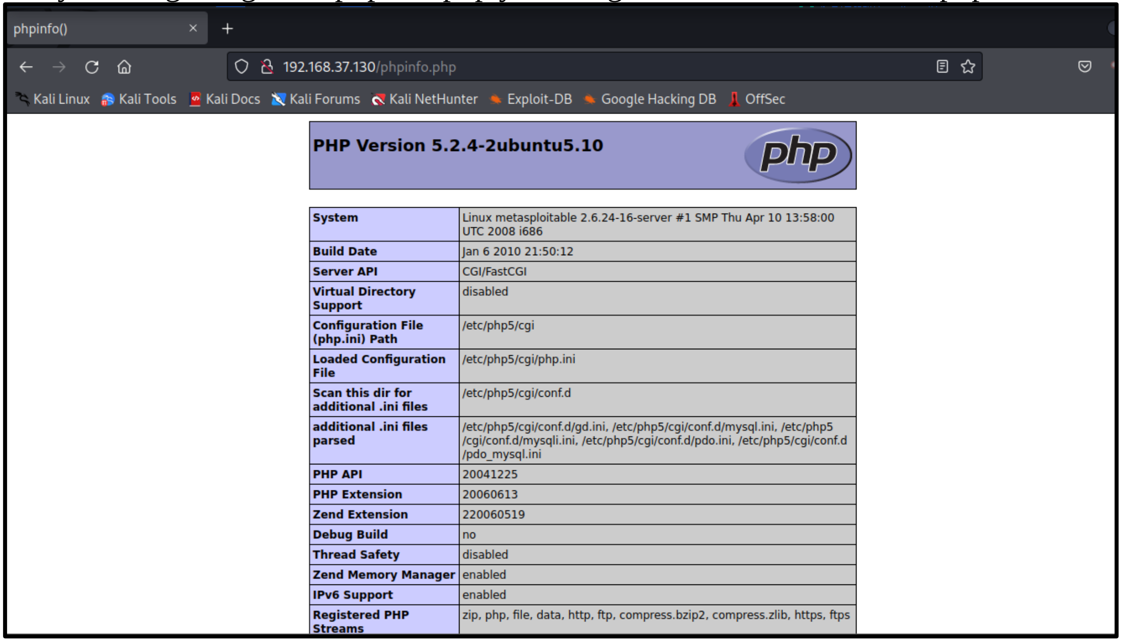
```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nikto -host 192.168.37.130
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.37.130
+ Target Hostname:    192.168.37.130
+ Target Port:        80
+ Start Time:         2022-10-08 01:37:41 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect again
st some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content
 of the site in a different fashion to the MIME type
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force fil
e names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index'
were found: index.php
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL f
or the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive informat
ion via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive informat
ion via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive informat
ion via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive informat
ion via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be pr
```



```
otected or limited to authorized hosts.
+ Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size:
 40540, mtime: Tue Dec  9 12:24:00 2008
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protec
ted or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This
gives a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpMyAdmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should
be protected or limited to authorized hosts.
+ OSVDB-3092: /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected
 or limited to authorized hosts.
+ 8726 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2022-10-08 01:38:12 (GMT-4) (31 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ 
```

As you can see, PHP5 has many vulnerabilities when installed on a server.

3. By running <targetIP>/phpinfo.php you can get information about the php version

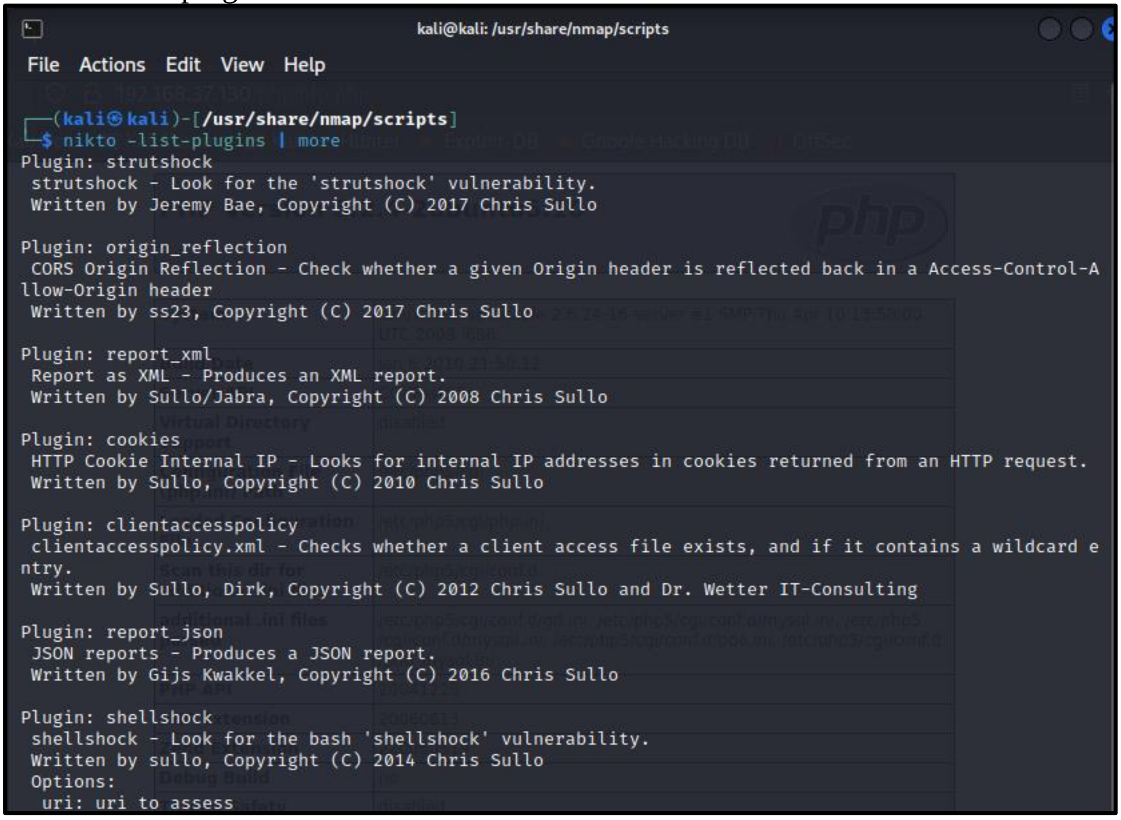


PHP Version 5.2.4-2ubuntu5.10

System	Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Build Date	Jan 6 2010 21:50:12
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/cgi
Loaded Configuration File	/etc/php5/cgi/php.ini
Scan this dir for additional .ini files	/etc/php5/cgi/conf.d
additional .ini files parsed	/etc/php5/cgi/conf.d/gd.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5/cgi/conf.d/mysqli.ini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5/cgi/conf.d/pdo_mysql.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	zip, php, file, data, http, ftp, compress.bzip2, compress.zlib, https, ftps

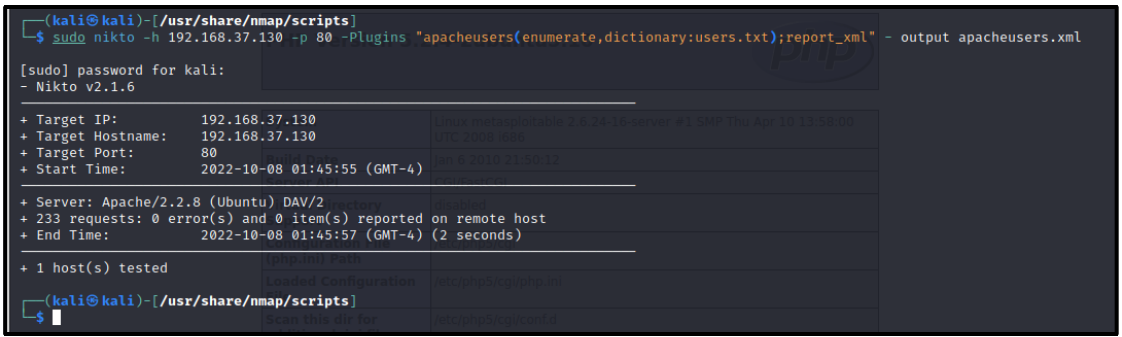
Customizing Nikto:

1. List all the plugins in the Nikto tool.

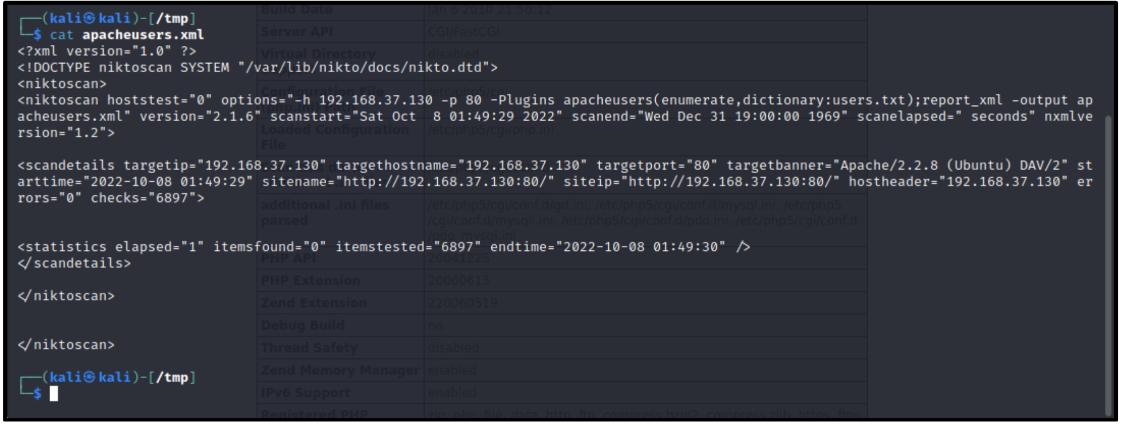


```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nikto -list-plugins | more
Plugin: strutshock
 strutshock - Look for the 'strutshock' vulnerability.
 Written by Jeremy Bae, Copyright (C) 2017 Chris Sullo

Plugin: origin_reflection
 CORS Origin Reflection - Check whether a given Origin header is reflected back in a Access-Control-A
llow-Origin header
 Written by ss23, Copyright (C) 2017 Chris Sullo

Plugin: report_xml
 Report as XML - Produces an XML report.
 Written by Sullo/Jabra, Copyright (C) 2008 Chris Sullo

Plugin: cookies
 HTTP Cookie Internal IP - Looks for internal IP addresses in cookies returned from an HTTP request.
 Written by Sullo, Copyright (C) 2010 Chris Sullo

Plugin: clientaccesspolicy
 clientaccesspolicy.xml - Checks whether a client access file exists, and if it contains a wildcard e
ntry.
 Written by Sullo, Dirk, Copyright (C) 2012 Chris Sullo and Dr. Wetter IT-Consulting

Plugin: report_json
 JSON reports - Produces a JSON report.
 Written by Gijs Kwakkel, Copyright (C) 2016 Chris Sullo

Plugin: shellshock
 shellshock - Look for the bash 'shellshock' vulnerability.
 Written by sullo, Copyright (C) 2014 Chris Sullo
 Options:
  uri: uri to assess
```

2. Running Nikto with specific plugin to find active users on the target server
“ sudo nikto -h 192.168.37.130 -p 80 -Plugins "apacheusers(enumerate,dictionary:users.txt);report_xml" - output apacheusers.xml ”



```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nikto -h 192.168.37.130 -p 80 -Plugins "apacheusers(enumerate,dictionary:users.txt);report_xml" - output apacheusers.xml

[sudo] password for kali:
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.37.130
+ Target Hostname:    192.168.37.130
+ Target Port:        80
+ Start Time:         2022-10-08 01:45:55 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ 233 requests: 0 error(s) and 0 item(s) reported on remote host
+ End Time:           2022-10-08 01:45:57 (GMT-4) (2 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ 
```

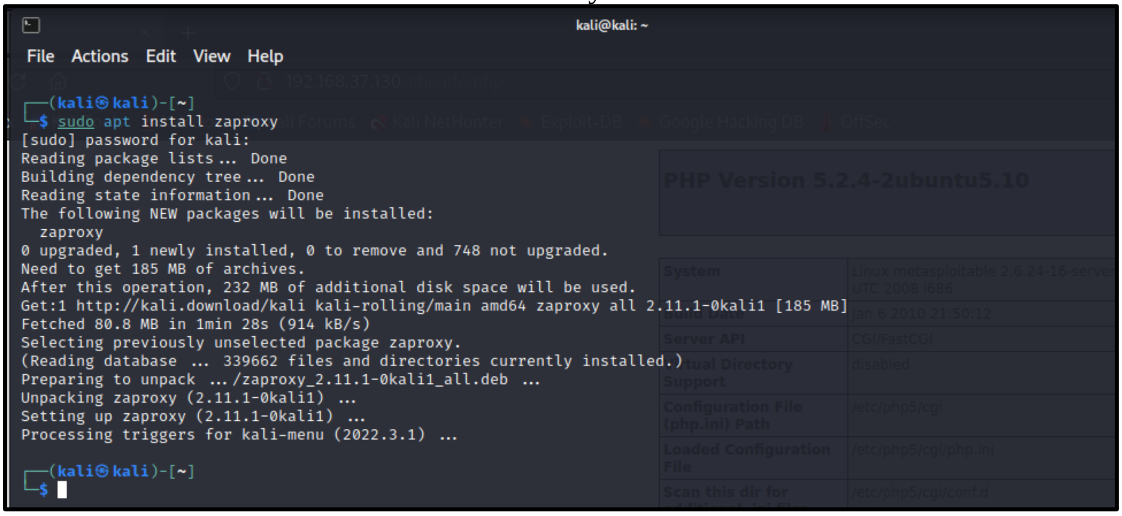


```
┌──(kali㉿kali)-[/tmp]
└─$ cat apacheusers.xml
<?xml version="1.0" ?>
<!DOCTYPE niktoscan SYSTEM "/var/lib/nikto/docs/nikto.dtd">
<niktoscan>
<niktoscan hoststest="0" options="-h 192.168.37.130 -p 80 -Plugins apacheusers(enumerate,dictionary:users.txt);report_xml -output ap
acheusers.xml" version="2.1.6" scanstart="Sat Oct  8 01:49:29 2022" scanend="Wed Dec 31 19:00:00 1969" scanelapsed=" seconds" nxmlve
rsion="1.2">

<scandetails targetip="192.168.37.130" targethostname="192.168.37.130" targetport="80" targetbanner="Apache/2.2.8 (Ubuntu) DAV/2" st
arttime="2022-10-08 01:49:29" sitename="http://192.168.37.130:80/" siteip="http://192.168.37.130:80/" hostheader="192.168.37.130" er
rors="0" checks="6897">


<statistics elapsed="1" itemsfound="0" itemstested="6897" endtime="2022-10-08 01:49:30" />
</scandetails>

</niktoscan>


</niktoscan>

┌──(kali㉿kali)-[/tmp]
└─$ 
```

OWASP ZAP:

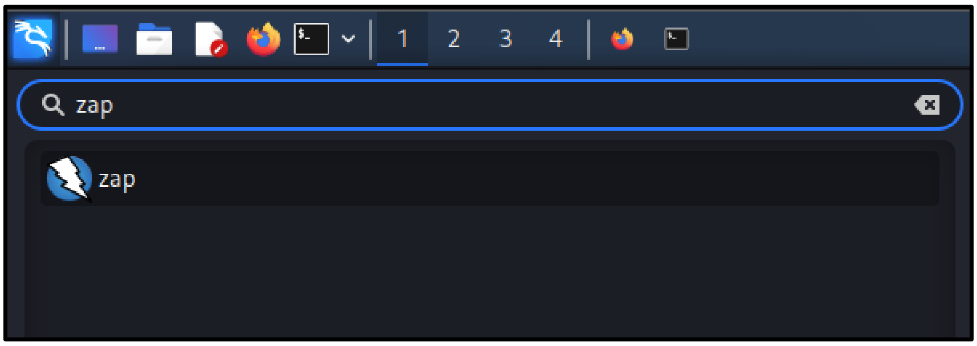
It is one of the most effective scanners based on the number of verified vulnerabilities that it has discovered.

1. Install the latest version of OWASP ZAP by

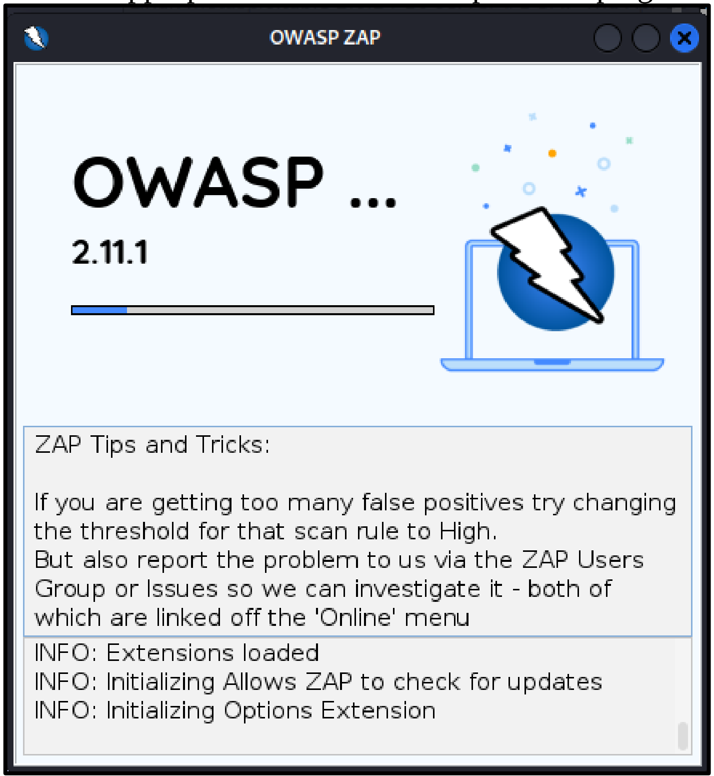


```
┌──(kali㉿kali)-[~]
└─$ sudo apt install zaproxy
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  zaproxy
0 upgraded, 1 newly installed, 0 to remove and 748 not upgraded.
Need to get 185 MB of archives.
After this operation, 232 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 zaproxy all 2.11.1-0kali1 [185 MB]
Fetched 80.8 MB in 1min 28s (914 kB/s)
Selecting previously unselected package zaproxy.
(Reading database ... 339662 files and directories currently installed.)
Preparing to unpack .../zaproxy_2.11.1-0kali1_all.deb ...
Unpacking zaproxy (2.11.1-0kali1) ...
Setting up zaproxy (2.11.1-0kali1) ...
Processing triggers for kali-menu (2022.3.1) ...

┌──(kali㉿kali)-[~]
└─$ 
```

2. Run the tool



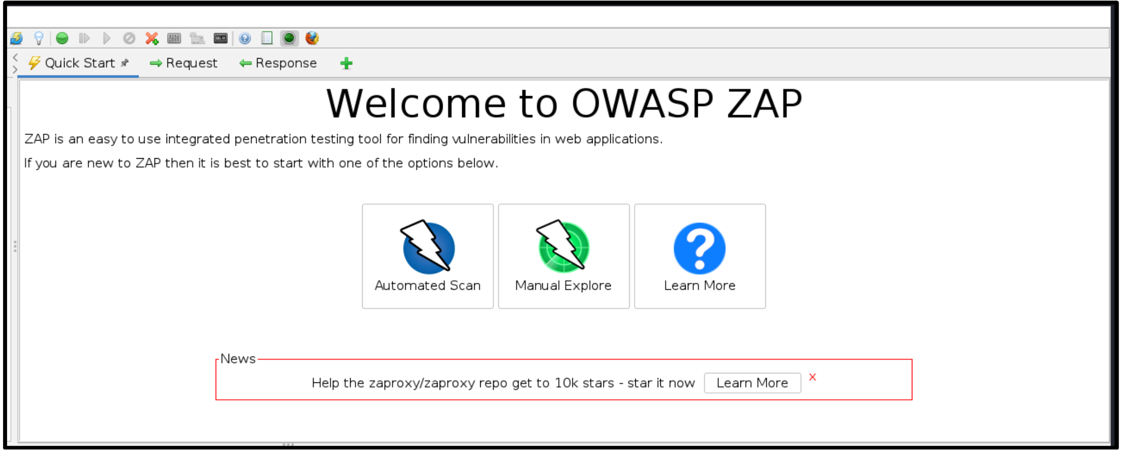
3. On start-up make the appropriate selections and update the plugins



ZAP Tips and Tricks:

If you are getting too many false positives try changing the threshold for that scan rule to High.
But also report the problem to us via the ZAP Users Group or Issues so we can investigate it - both of which are linked off the 'Online' menu

```
INFO: Extensions loaded
INFO: Initializing Allows ZAP to check for updates
INFO: Initializing Options Extension
```

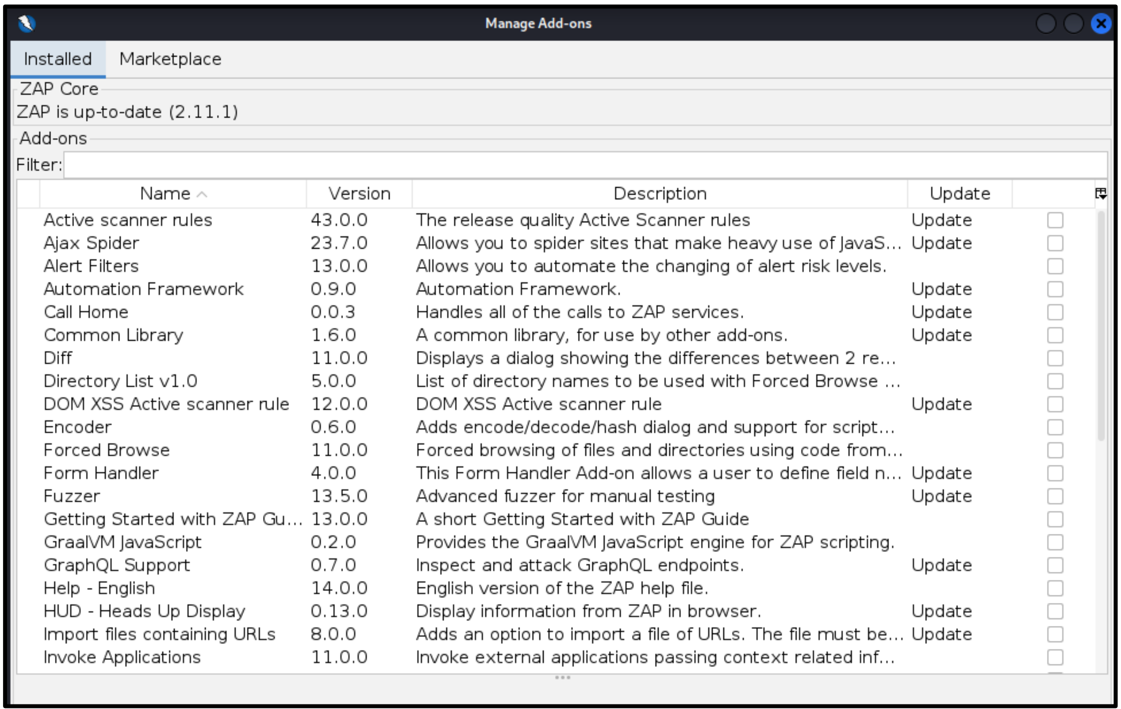


Welcome to OWASP ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

Help the zaproxy/zaproxy repo get to 10k stars - star it now



Manage Add-ons

Installed | Marketplace

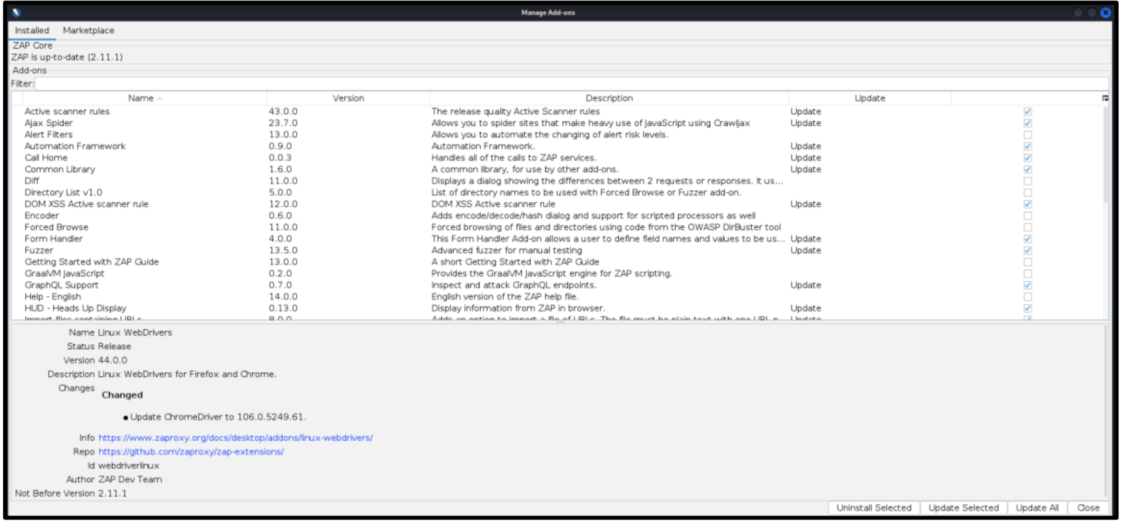
ZAP Core

ZAP is up-to-date (2.11.1)

Add-ons

Filter:

Name	Version	Description	Update	
Active scanner rules	43.0.0	The release quality Active Scanner rules	Update	□
Ajax Spider	23.7.0	Allows you to spider sites that make heavy use of JavaS…	Update	□
Alert Filters	13.0.0	Allows you to automate the changing of alert risk levels.		□
Automation Framework	0.9.0	Automation Framework.	Update	□
Call Home	0.0.3	Handles all of the calls to ZAP services.	Update	□
Common Library	1.6.0	A common library, for use by other add-ons.	Update	□
Diff	11.0.0	Displays a dialog showing the differences between 2 re…		□
Directory List v1.0	5.0.0	List of directory names to be used with Forced Browse …		□
DOM XSS Active scanner rule	12.0.0	DOM XSS Active scanner rule	Update	□
Encoder	0.6.0	Adds encode/decode/hash dialog and support for script…		□
Forced Browse	11.0.0	Forced browsing of files and directories using code from…		□
Form Handler	4.0.0	This Form Handler Add-on allows a user to define field n…	Update	□
Fuzzer	13.5.0	Advanced fuzzer for manual testing	Update	□
Getting Started with ZAP Gu…	13.0.0	A short Getting Started with ZAP Guide		□
GraalVM JavaScript	0.2.0	Provides the GraalVM JavaScript engine for ZAP scripting.		□
GraphQL Support	0.7.0	Inspect and attack GraphQL endpoints.	Update	□
Help - English	14.0.0	English version of the ZAP help file.		□
HUD - Heads Up Display	0.13.0	Display information from ZAP in browser.	Update	□
Import files containing URLs	8.0.0	Adds an option to import a file of URLs. The file must be…	Update	□
Invoke Applications	11.0.0	Invoke external applications passing context related inf…		□



Manage Add-ons

Installed | Marketplace

ZAP Core

ZAP is up-to-date (2.11.1)

Add-ons

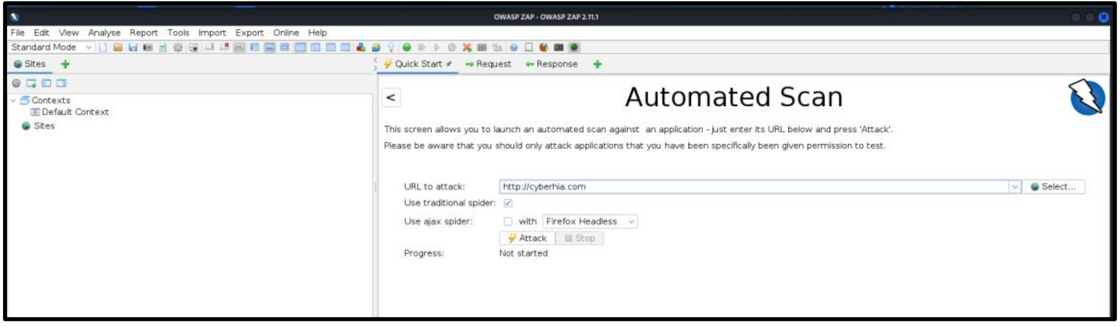
Filter:

Name	Version	Description	Update	
Active scanner rules	43.0.0	The release quality Active Scanner rules	Update	☑
Ajax Spider	23.7.0	Allows you to spider sites that make heavy use of JavaScript using Crawljax	Update	☑
Alert Filters	13.0.0	Allows you to automate the changing of alert risk levels.		□
Automation Framework	0.9.0	Automation Framework.	Update	☑
Call Home	0.0.3	Handles all of the calls to ZAP services.	Update	☑
Common Library	1.6.0	A common library, for use by other add-ons.	Update	☑
Diff	11.0.0	Displays a dialog showing the differences between 2 requests or responses. It us…		□
Directory List v1.0	5.0.0	List of directory names to be used with Forced Browse or Fuzzer add-on.		□
DOM XSS Active scanner rule	12.0.0	DOM XSS Active scanner rule	Update	☑
Encoder	0.6.0	Adds encode/decode/hash dialog and support for scripted processors as well		□
Forced Browse	11.0.0	Forced browsing of files and directories using code from the OWASP DirBuster tool		□
Form Handler	4.0.0	This Form Handler Add-on allows a user to define field names and values to be us…	Update	☑
Fuzzer	13.5.0	Advanced fuzzer for manual testing	Update	☑
Getting Started with ZAP Guide	13.0.0	A short Getting Started with ZAP Guide		□
GraalVM JavaScript	0.2.0	Provides the GraalVM JavaScript engine for ZAP scripting.		□
GraphQL Support	0.7.0	Inspect and attack GraphQL endpoints.	Update	☑
Help - English	14.0.0	English version of the ZAP help file.		□
HUD - Heads Up Display	0.13.0	Display information from ZAP in browser.	Update	☑
Import files containing URLs	8.0.0	Adds an option to import a file of URLs. The file must be plain text with one URL p…	Update	☑

Name Linux WebDrivers
Status Release
Version 44.0.0
Description Linux WebDrivers for Firefox and Chrome.
Changes **Changed**

- Update ChromeDriver to 106.0.5249.61.

Info https://www.zaproxy.org/docs/desktop/addons/linux-webdrivers/
Repo https://github.com/zaproxy/zap-extensions/
Id webdriverlinux
Author ZAP Dev Team
Not Before Version 2.11.1



OWASP ZAP - OWASP ZAP 2.11.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Contexts
Default Context
Sites
Quick Start
Request
Response
<

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

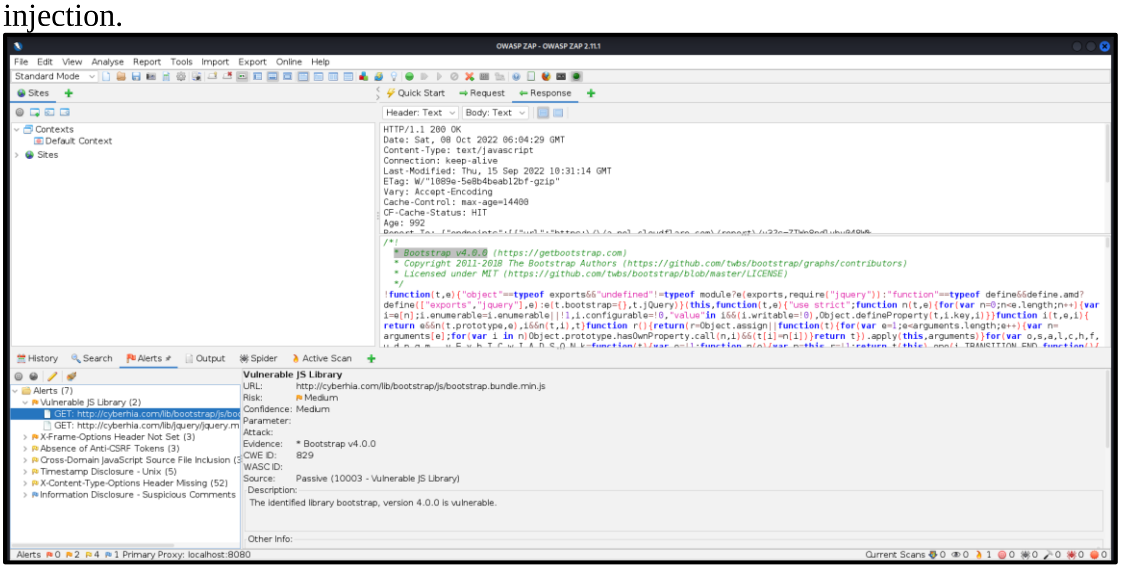
URL to attack: http://cyberhia.com

Use traditional spider: ☑

Use ajax spider: □ with Firefox Headless

Progress: Not started

4. After the scan you can click on the identified results to drill down to specific findings. OWASP ZAP can help you find vulnerabilities such as reflected cross-site scripting, stored cross-site scripting, SQL injection, and remote OS command injection.



```
HTTP/1.1 200 OK
Date: Sat, 08 Oct 2022 06:04:29 GMT
Content-Type: text/javascript
Connection: keep-alive
Last-Modified: Thu, 15 Sep 2022 10:31:14 GMT
ETag: W/"1089e-5e8b4beab12bf-gzip"
Vary: Accept-Encoding
Cache-Control: max-age=14400
CF-Cache-Status: HIT
Age: 992
```

```
/*!
  * Bootstrap v4.0.0 (https://getbootstrap.com)
  * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors)
  * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE)
  */
!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery")):"function"==typeof define&&define.amd?
define(["exports","jquery"],e):e(t.bootstrap={},t.jQuery)}(this,function(t,e){"use strict";function n(t,e){for(var n=0;n<e.length;n++){var
i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function i(t,e,i){
return e&&n(t.prototype,e),i&&n(t,i),t}function r(){return(r=Object.assign||function(t){for(var e=1;e<arguments.length;e++){var n=
arguments[e];for(var i in n)Object.prototype.hasOwnProperty.call(n,i)&&(t[i]=n[i])}return t}).apply(this,arguments)}for(var o,s,a,l,c,h,f,
```

Alerts (7)
- Vulnerable JS Library (2)
  - GET: http://cyberhia.com/lib/bootstrap/js/boo
  - GET: http://cyberhia.com/lib/jquery/jquery.m
- X-Frame-Options Header Not Set (3)
- Absence of Anti-CSRF Tokens (3)
- Cross-Domain JavaScript Source File Inclusion (3
- Timestamp Disclosure - Unix (5)
- X-Content-Type-Options Header Missing (52)
- Information Disclosure - Suspicious Comments

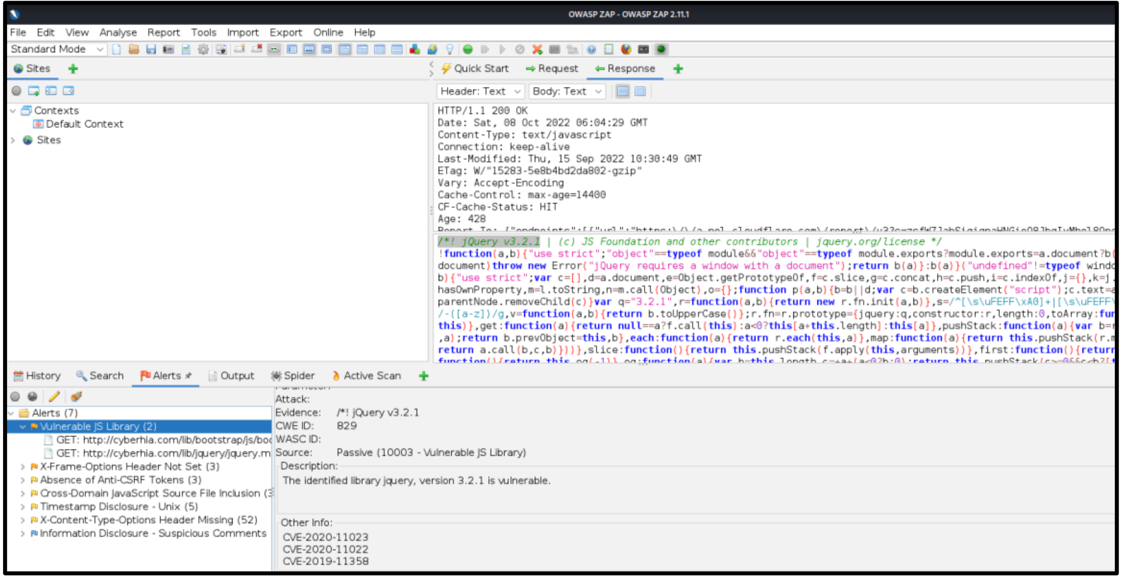
Vulnerable JS Library

URL: http://cyberhia.com/lib/bootstrap/js/bootstrap.bundle.min.js
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: * Bootstrap v4.0.0
CWE ID: 829
WASC ID:
Source: Passive (10003 - Vulnerable JS Library)

Description:
The identified library bootstrap, version 4.0.0 is vulnerable.

Other Info:

Alerts 0 2 4 1 Primary Proxy: localhost:8080 Current Scans 0 0 1 0 0 0 0 0



```
HTTP/1.1 200 OK
Date: Sat, 08 Oct 2022 06:04:29 GMT
Content-Type: text/javascript
Connection: keep-alive
Last-Modified: Thu, 15 Sep 2022 10:30:49 GMT
ETag: W/"15283-5e8b4bd2da802-gzip"
Vary: Accept-Encoding
Cache-Control: max-age=14400
CF-Cache-Status: HIT
Age: 428
```

```
/*! jQuery v3.2.1 | (c) JS Foundation and other contributors | jquery.org/license */
!function(a,b){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(
document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof windo
b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.
hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a
parentNode.removeChild(c)}var q="3.2.1",r=function(a,b){return new r.fn.init(a,b)},s=/^[\s\uFEFF\xA0]+|[\s\uFEFF\
/-([a-z])/g,v=function(a,b){return b.toUpperCase()};r.fn=r.prototype={jquery:q,constructor:r,length:0,toArray:fun
this)},get:function(a){return null==a?f.call(this):a<0?this[a+this.length]:this[a]},pushStack:function(a){var b=r
,a);return b.prevObject=this,b},each:function(a){return r.each(this,a)},map:function(a){return this.pushStack(r.m
return a.call(b,c,b)}))},slice:function(){return this.pushStack(f.apply(this,arguments))},first:function(){return
```

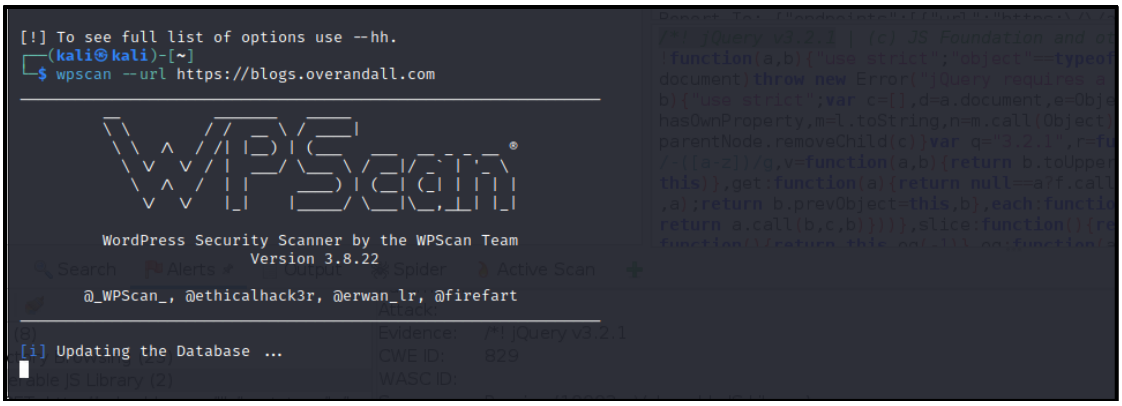
Alerts (7)
- Vulnerable JS Library (2)
  - GET: http://cyberhia.com/lib/bootstrap/js/boo
  - GET: http://cyberhia.com/lib/jquery/jquery.m
- X-Frame-Options Header Not Set (3)
- Absence of Anti-CSRF Tokens (3)
- Cross-Domain JavaScript Source File Inclusion (3
- Timestamp Disclosure - Unix (5)
- X-Content-Type-Options Header Missing (52)
- Information Disclosure - Suspicious Comments

Attack:
Evidence: /*! jQuery v3.2.1
CWE ID: 829
WASC ID:
Source: Passive (10003 - Vulnerable JS Library)

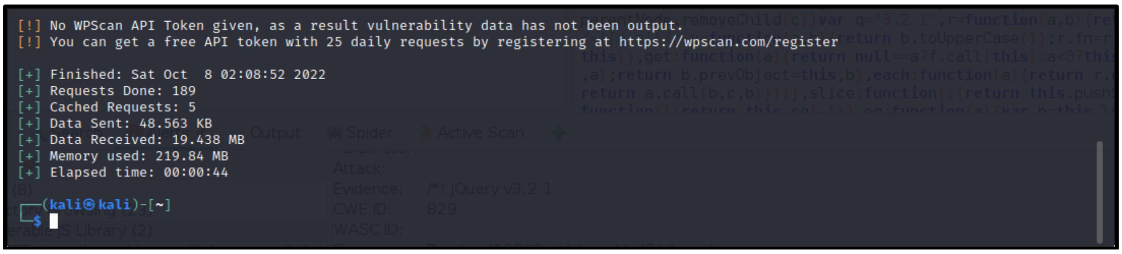
Description:
The identified library jquery, version 3.2.1 is vulnerable.

Other Info:
CVE-2020-11023
CVE-2020-11022
CVE-2019-11358

5. WPScan



```
[!] To see full list of options use --hh.
┌──(kali㉿kali)-[~]
└─$ wpscan --url https://blogs.overandall.com
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.22

       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] Updating the Database ...
```



```
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Sat Oct  8 02:08:52 2022
[+] Requests Done: 189
[+] Cached Requests: 5
[+] Data Sent: 48.563 KB
[+] Data Received: 19.438 MB
[+] Memory used: 219.84 MB
[+] Elapsed time: 00:00:44

┌──(kali㉿kali)-[~]
└─$ 
```