

Practical 4

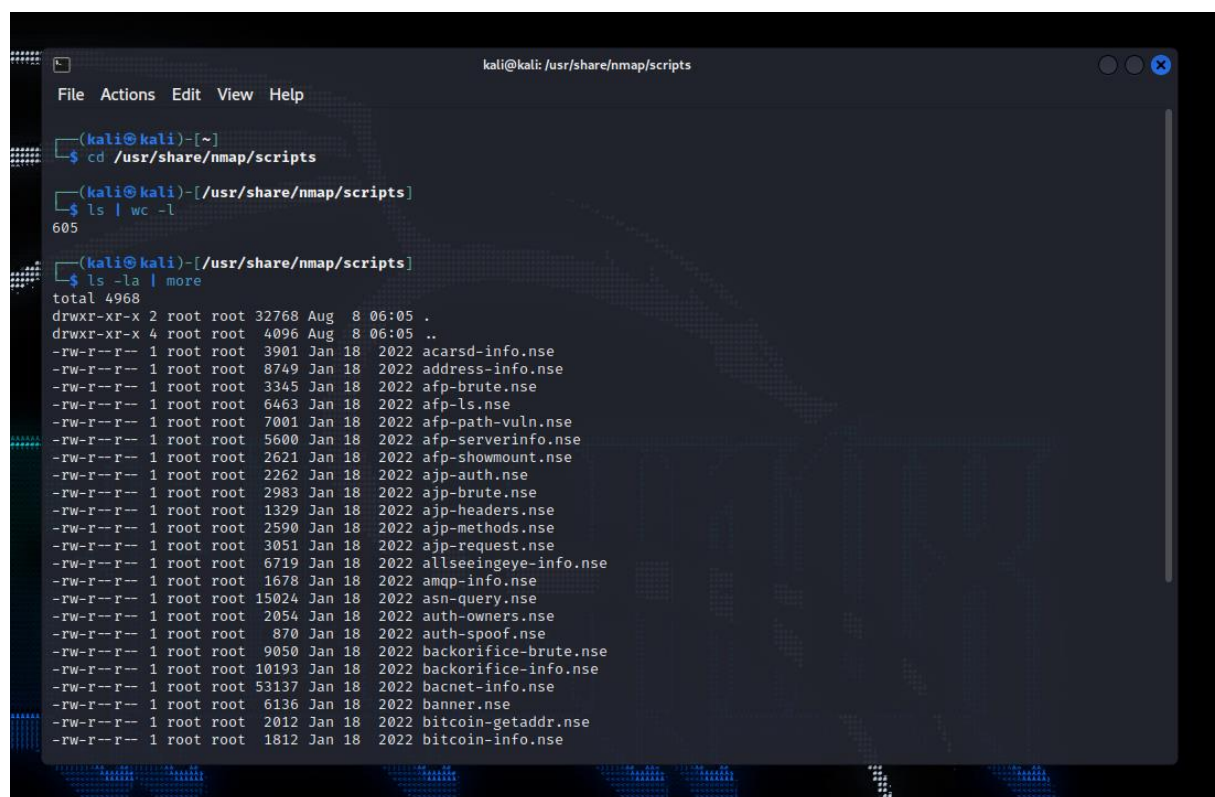
Aim: Practical on vulnerability scanning and assessment

NOTE: We will be using Nmap and other vulnerability tools for vulnerability analysis.

Our Target Machine will be metasploitable2 and target live hosts will be packtpub.com and cyberhia.com

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
```

2. Update scripts

Before firing up Nmap 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 don't miss the vulnerability identification:

```
sudo nmap --script-updatedb
```

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 192.168.101.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-07 15:53 EDT
```

```
kali@kali: /usr/share/nmap/scripts
File Actions Edit View Help
| server: irc.Metasploitable.LAN
| version: Unreal3.2.8.1. irc.Metasploitable.LAN
| uptime: 0 days, 0:03:53
| source ident: nmap
| source host: 8988EC2E.60779B34.FFFA6D49.IP
|_ error: Closing Link: edfwagcew[192.168.101.132] (Quit: edfwagcew)
8009/tcp open  ajp13
|_ ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  unknown
|_ http-title: Apache Tomcat/5.5
|_ http-favicon: Apache Tomcat
MAC Address: 00:0C:29:70:18:72 (VMware)

Host script results:
|_ clock-skew: mean: 1h00m05s, deviation: 2h00m00s, median: 4s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_ System time: 2022-10-07T15:53:14-04:00
|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)

Nmap done: 1 IP address (1 host up) scanned in 84.60 seconds
(kali@kali)-[/usr/share/nmap/scripts]
$
```

3. 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]
$ ls | grep ssh
ssh2-enum-algos.nse
ssh-auth-methods.nse
ssh-brute.nse
ssh-hostkey.nse
ssh-publickey-acceptance.nse
ssh-run.nse
ssshv1.nse

(kali@kali)-[/usr/share/nmap/scripts]
$ nmap --script-help ssh2-enum-algos
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-07 15:59 EDT

ssh2-enum-algos
Categories: safe discovery
https://nmap.org/nse/doc/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]
$
```

4. 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 2022-10-07 16:00 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]
$
```

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

```
(kali㉿kali)-[/usr/share/nmap/scripts]
$ nmap --script=ssh-run 192.168.101.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-07 16:02 EDT
NSE: [ssh-run] Failed to specify credentials and command to run.
Nmap scan report for 192.168.101.130
Host is up (0.0018s 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 0.68 seconds

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

6. Get available scripts for http

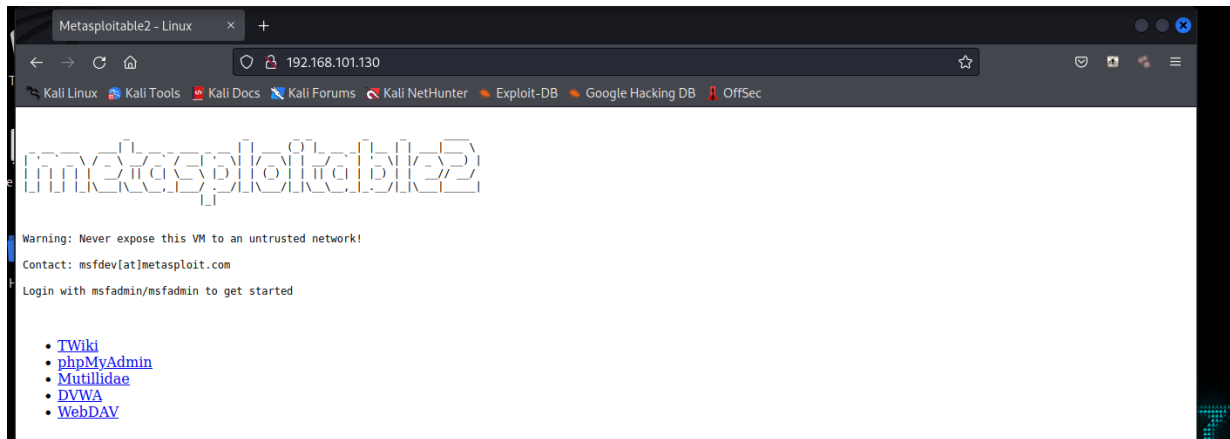
```
kali@kali: /usr/share/nmap/scripts

File Actions Edit View Help

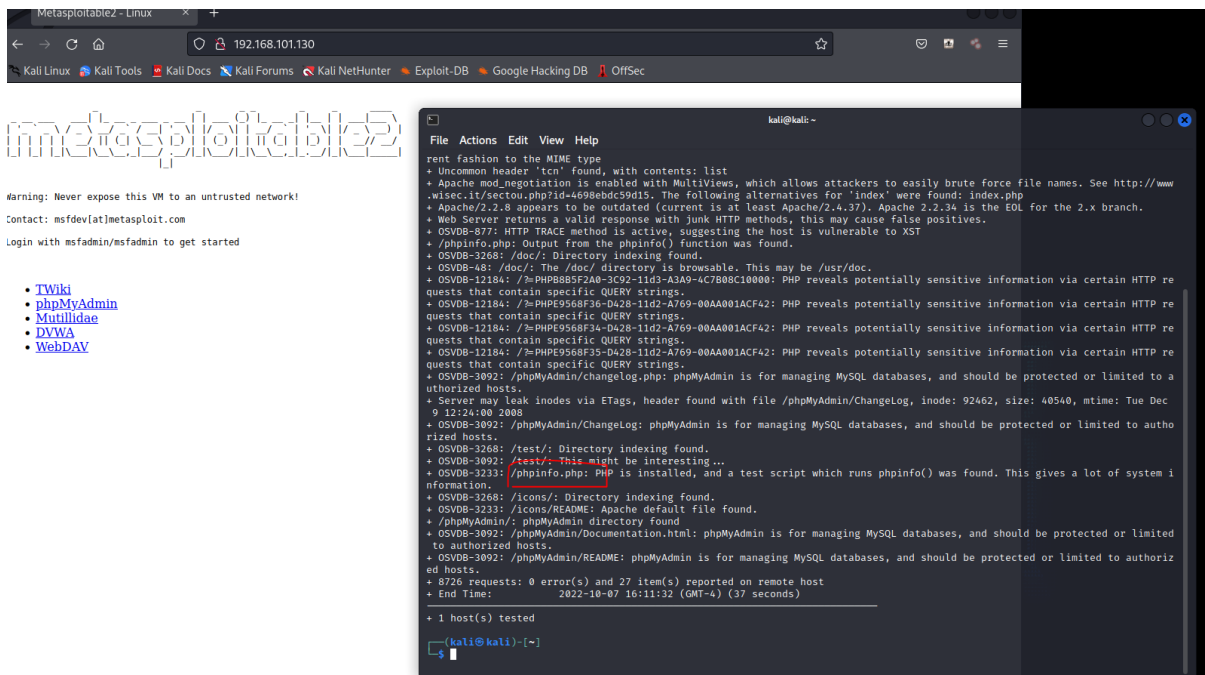
(kali㉿kali)-[/usr/share/nmap/scripts]
$ ls | grep http
http-adobe-coldfusion-apsa1301.nse
http-affiliate-id.nse
http-apache-negotiation.nse
http-apache-server-status.nse
http-aspnet-debug.nse
http-auth-finder.nse
http-auth.nse
http-avaya-ipoffice-users.nse
http-awstatstotals-exec.nse
http-axis2-dir-traversal.nse
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
```

Web Server Vulnerability Scanning

1. Run metasploitable2 website on firefox in kali linux

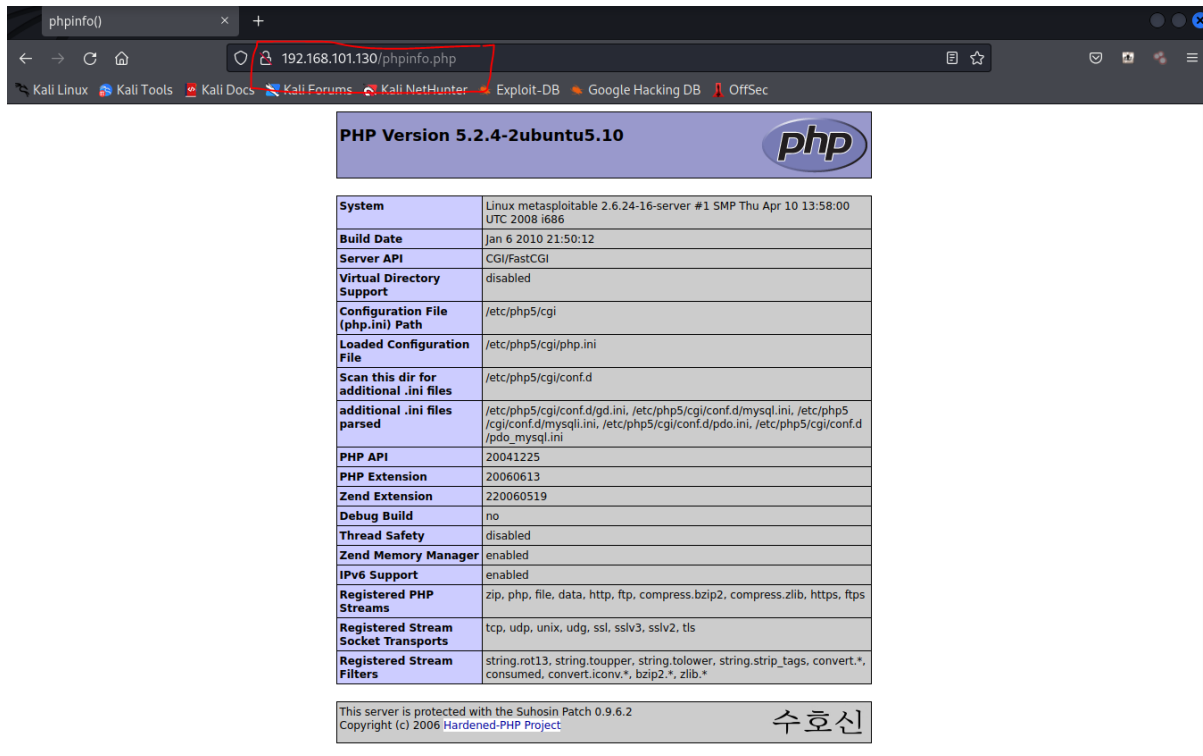


2. Using Nikto tool scan the target for vulnerabilities



As you can see php5 has many vulnerabilities when installed on server.

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



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
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
Registered Stream Filters	string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, convert.iconv.*, bzip2.*, zlib.*

This server is protected with the Suhosin Patch 0.9.6.2
Copyright (c) 2006 Hardened-PHP Project

수호신

Customizing Nikto

1. List all the plugins in the Nikto tool

```
(kali㉿kali)-[~]
└─$ nikto -list-plugins | more
Plugin: docker_registry
docker_registry - Look for the docker registry
Written by Jeremy Bae, Copyright (C) 2018 Chris Sullo

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

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

Plugin: outdated
Outdated - Checks to see whether the web server is the latest version.
Written by Sullo, Copyright (C) 2008 Chris Sullo

Plugin: report_text
Text reports - Produces a text report.
```

Figure 4.9: Listing all the plugins in Nikto

2. Running Nikto with specific plugin to find active users on the target server

```
kali@kali: /tmp
File Actions Edit View Help

(kali@kali)-[/tmp]
$ sudo nikto -h 192.168.101.130 -p 80 -Plugins "apacheusers(enumerate,dictionary:users.txt);report_xml" -output apacheuser
s.xml
- Nikto v2.1.6

+ Target IP: 192.168.101.130
+ Target Hostname: 192.168.101.130
+ Target Port: 80
+ Start Time: 2022-10-07 16:24:32 (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: 2022-10-07 16:24:33 (GMT-4) (1 seconds)

+ 1 host(s) tested

(kali@kali)-[/tmp]
$ cat apacheusers.xml
<?xml version="1.0" ?>
<!DOCTYPE niktoscan SYSTEM "/var/lib/nikto/docs/nikto.dtd">
<niktoscan>
<niktoscan hosttest="0" options="-h 192.168.101.130 -p 80 -Plugins apacheusers(enumerate,dictionary:users.txt);report_xml -
output apacheusers.xml" version="2.1.6" scanstart="Fri Oct 7 16:24:32 2022" scanend="Wed Dec 31 19:00:00 1969" scanelapsed="
seconds" nxmlversion="1.2">

<scandetails targetip="192.168.101.130" targethostname="192.168.101.130" targetport="80" targetbanner="Apache/2.2.8 (Ubuntu)
DAV/2" starttime="2022-10-07 16:24:32" sitename="http://192.168.101.130:80/" siteip="http://192.168.101.130:80/" hostheader
="192.168.101.130" errors="0" checks="6897">

<statistics elapsed="1" itemsfound="0" itemstested="6897" endtime="2022-10-07 16:24:33" />
</scandetails>

</niktoscan>
```

OWASP ZAP

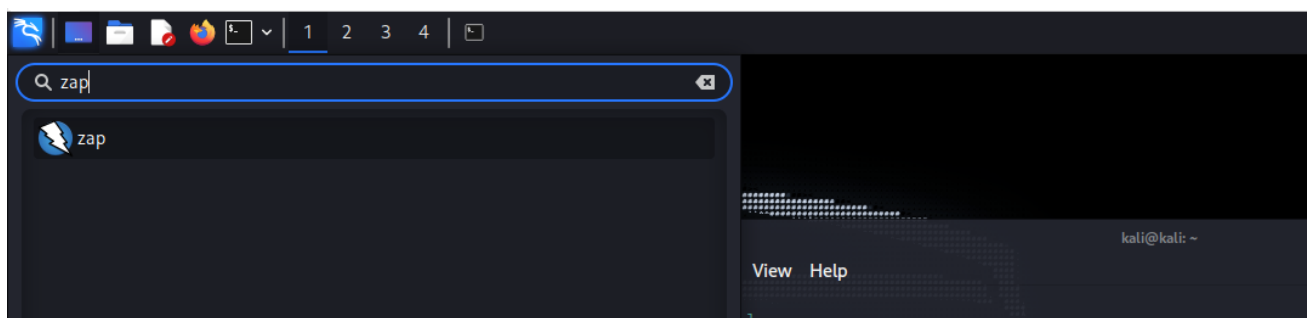
One of the most effective scanners based on the number of verified vulnerabilities discovered is OWASP ZAP. This tool is not preinstalled in Kali Linux 2021.

1. Install the latest version of OWASP ZAP by

```
kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ sudo apt install zaproxy
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
zaproxy is already the newest version (2.11.1-0kali1).
You might want to run 'apt --fix-broken install' to correct these.
The following packages have unmet dependencies:
 libgnutls-dane0 : Depends: libunbound8 (≥ 1.8.0) but it is not going to be installed
E: Unmet dependencies. Try 'apt --fix-broken install' with no packages (or specify a solution).
```

2. Run the tool



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

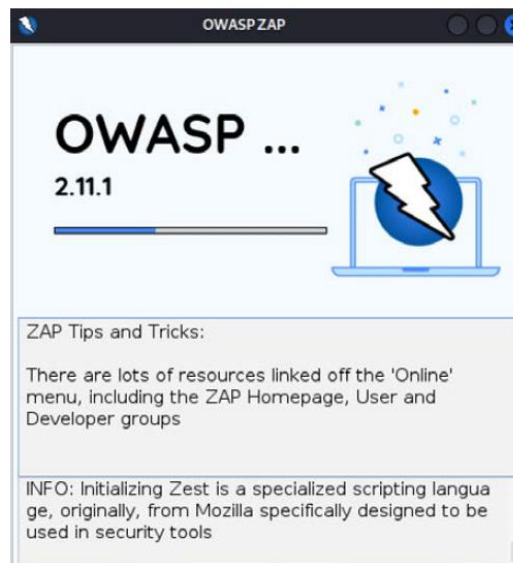
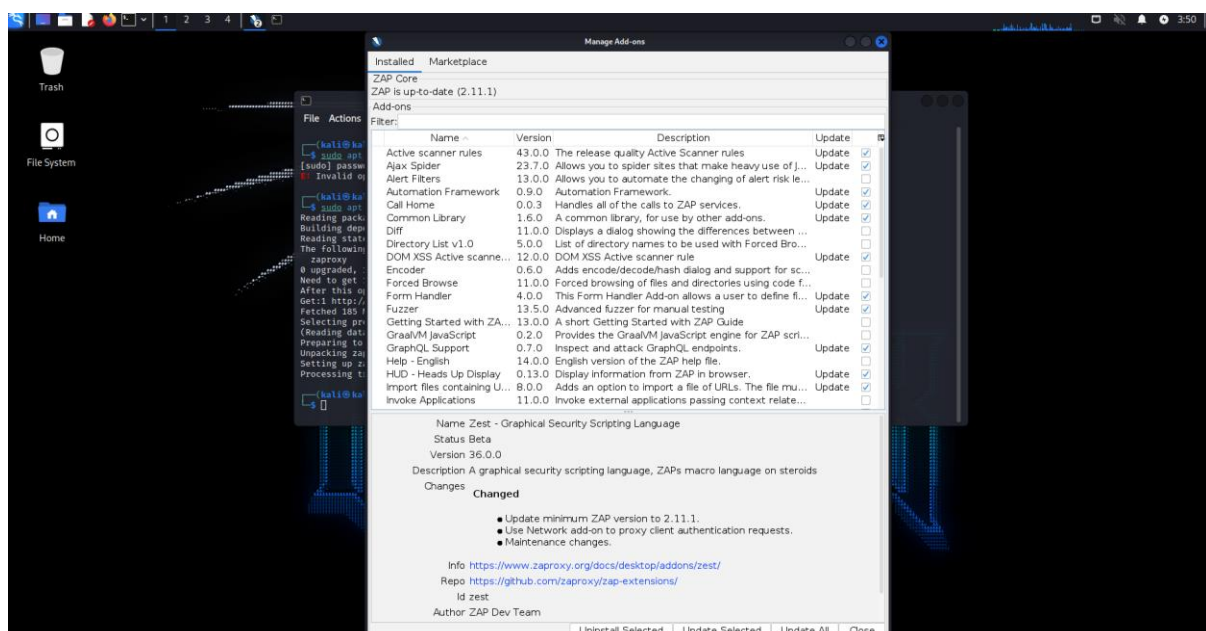
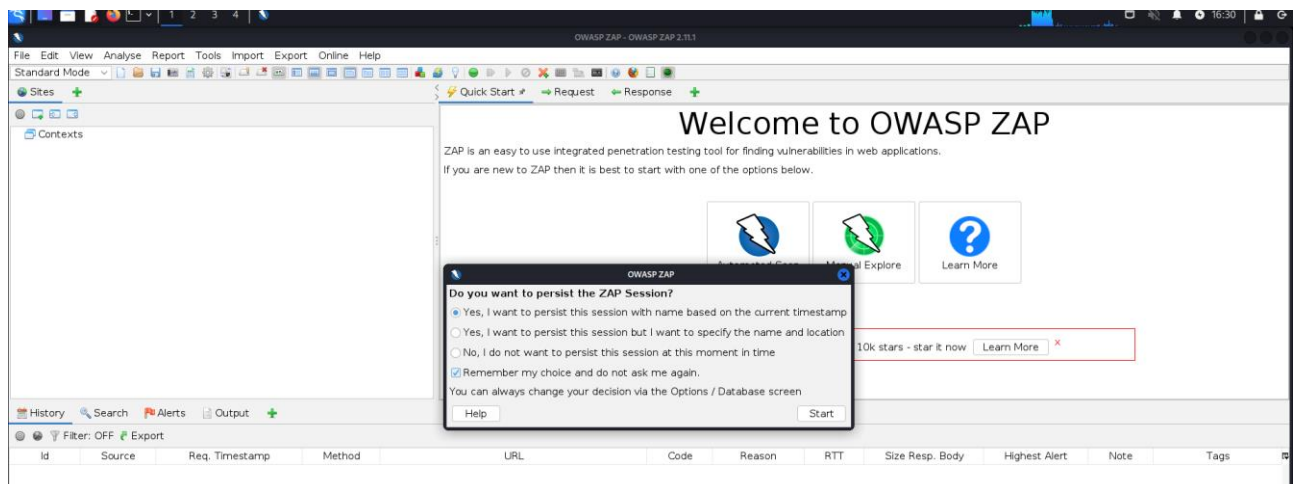
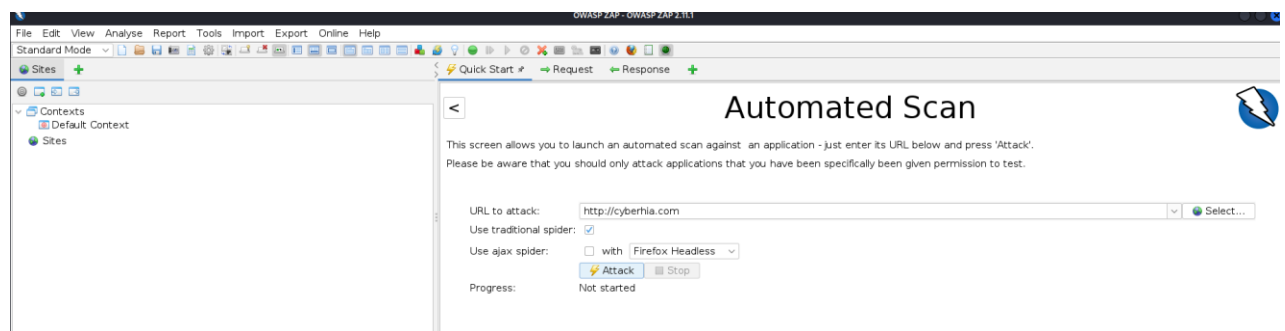


Figure 4.11: Loading the OWASP ZAP 2.11.1





3. 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.

