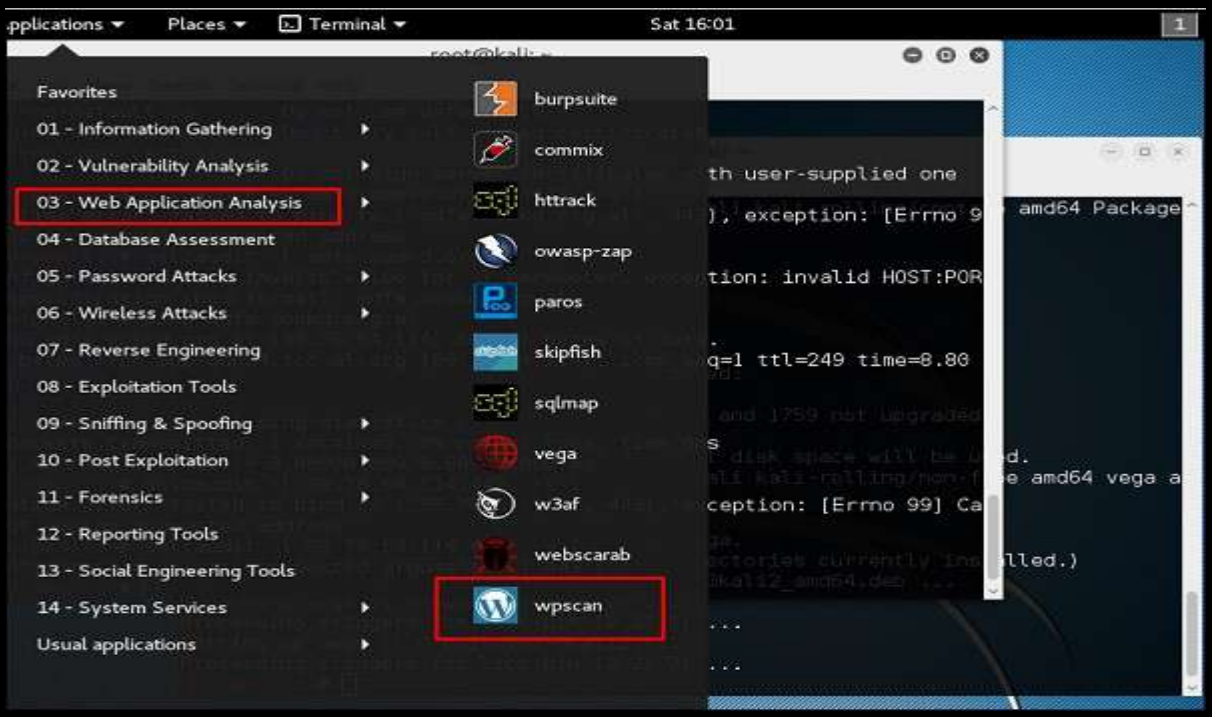
Website Penetration Testing-CMS Scanning Tools

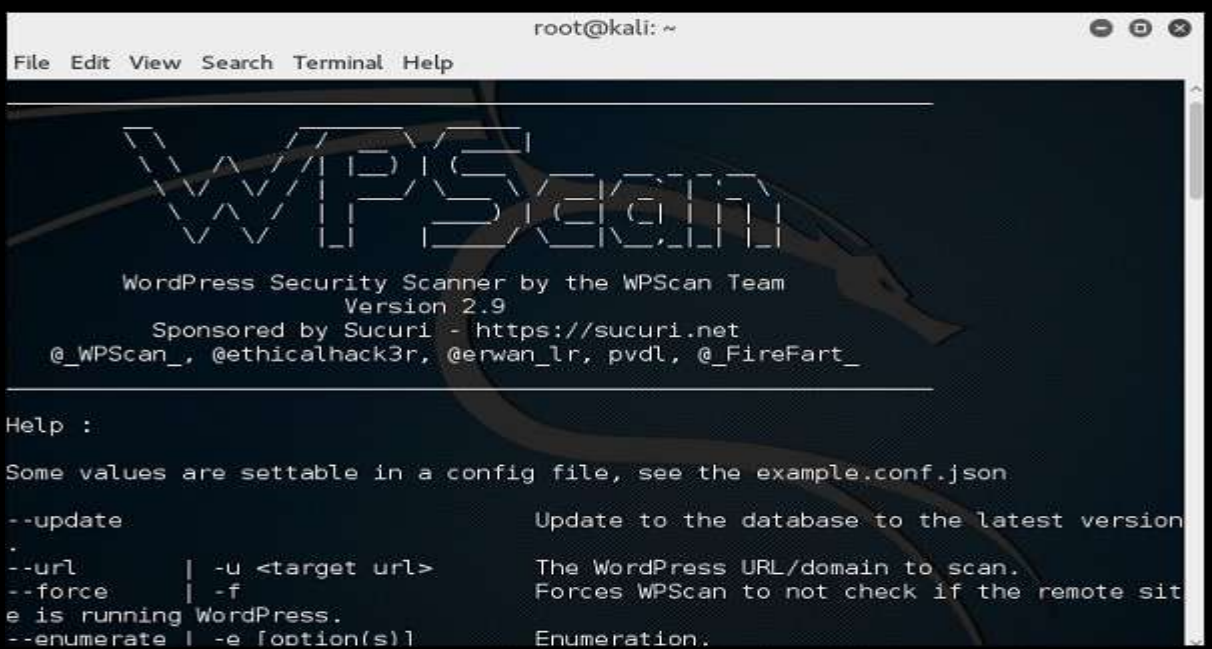
WPScan

WPScan is a black box WordPress vulnerability scanner that can be used to scan remote WordPress installations to find security issues.

Step 1 – To open WPscan go to Applications → 03-Web Application Analysis → "wpscan".



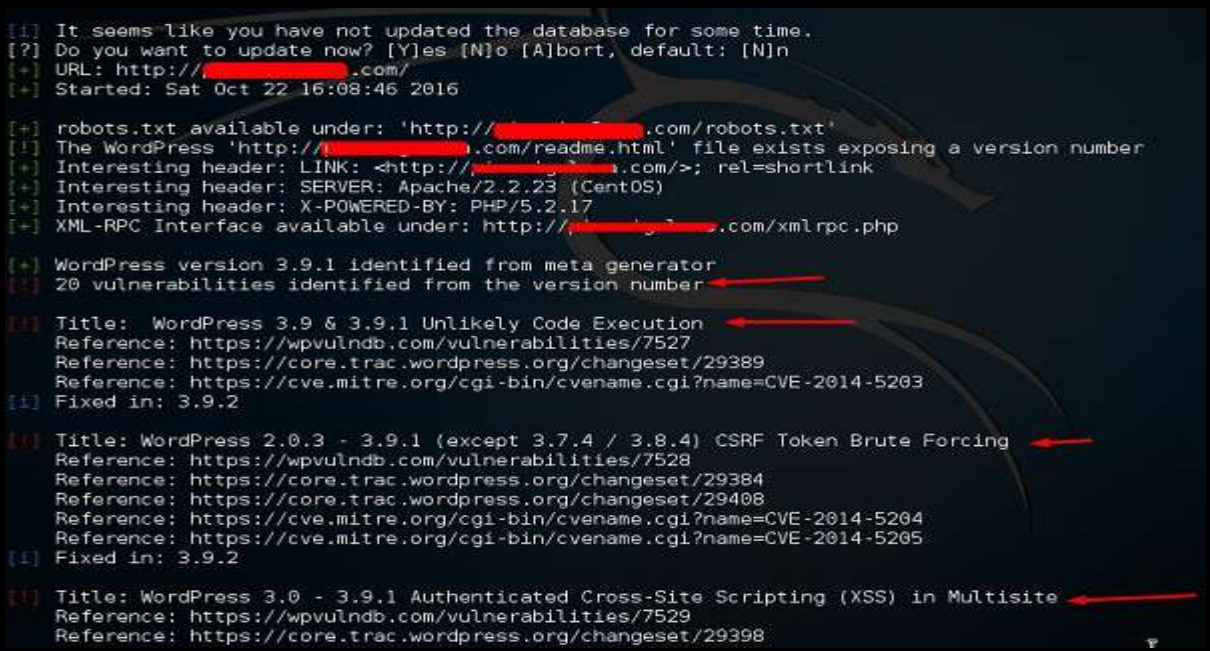
The following screenshot pops up.



Step 2 – To scan a website for vulnerabilities, type "**wpscan –u URL of webpage"**.

If the scanner is not updated, it will ask you to update. I will recommend to do it.

Once the scan starts, you will see the findings. In the following screenshot, vulnerabilities are indicated by a red arrow.



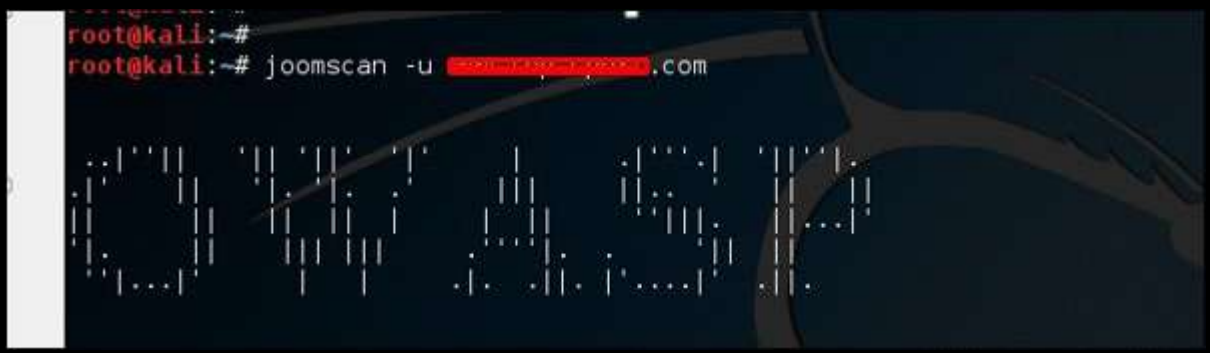
Joomscan

Joomla is probably the most widely-used CMS out there due to its flexibility. For this CMS, it is a Joomla scanner. It will help web developers and web masters to help identify possible security weaknesses on their deployed Joomla sites.

Step 1 – To open it, just click the left panel at the terminal, then "**joomscan – parameter**".

Step 2 – To get help for the usage type "**joomscan /?**"

Step 3 – To start the scan, type " joomscan –u URL of the victim".



Results will be displayed as shown in the following screenshot.

```
File  Edit  View  Search  Terminal  Help


Vulnerabilities Discovered
==========================

# 1
Info -> Generic: htaccess.txt has not been renamed.
Versions Affected: Any
Check: /htaccess.txt
Exploit: Generic defenses implemented in .htaccess are not available, so exploit
ing is more likely to succeed.
Vulnerable? Yes

# 2
Info -> Generic: Unprotected Administrator directory
Versions Affected: Any
Check: /administrator/
Exploit: The default /administrator directory is detected. Attackers can brutefo
rce administrator accounts. Read: http://yehg.net/lab/pr0js/view.php/MULTIPLE%20
TRICKY%20WAYS%20TO%20PROTECT.pdf
Vulnerable? Yes
```

```
15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30%20from%20jos_users--
Vulnerable? No

# 27
Info -> Component: Joomla Component com_searchlog SQL Injection
Versions Affected: 3.1.0 <=
Check: /administrator/index.php?option=com_searchlog&act=log
Exploit: /administrator/index.php?option=com_searchlog&act=log
Vulnerable? No

# 28
Info -> Component: Joomla Component com_djartgallery Multiple Vulnerabilities
Versions Affected: 0.9.1 <=
Check: /administrator/index.php?option=com_djartgallery&task=editItem&cid[]=1'+a
nd+1=1+--+
Exploit: /administrator/index.php?option=com_djartgallery&task=editItem&cid[]=1'
+and+1=1+--+
Vulnerable? N/A

There are 2 vulnerable points in 28 found entries!

~[*] Time Taken: 28 min and 20 sec
~[*] Send bugs, suggestions, contributions to joomscan@yehg.net
root@xfx:~#
```