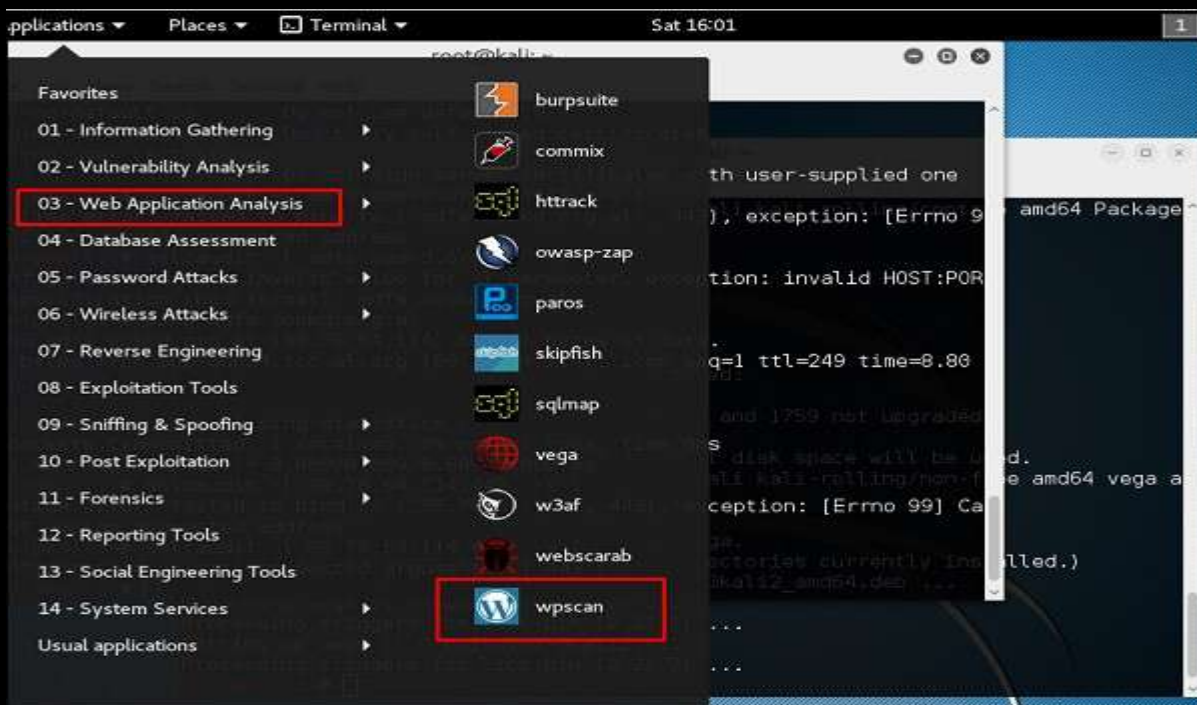


Website Penetration Testing-CMS Scanning Tools

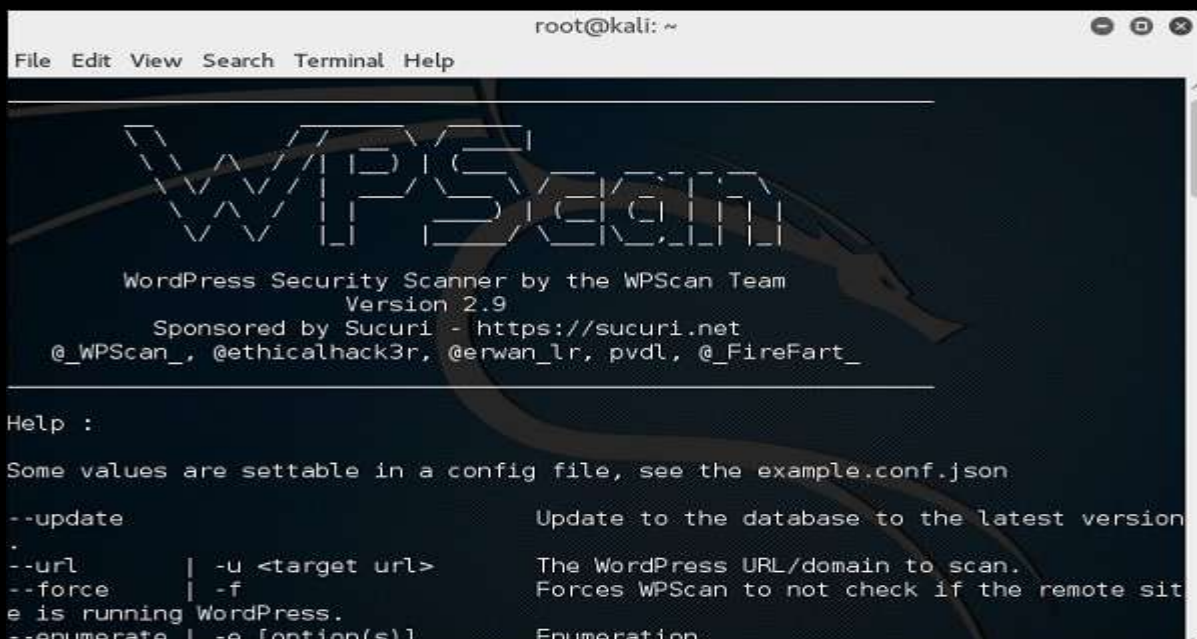
WPScan

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.

```
root@kali:~# wpscan -u itsolution.support  
  
WPSecan  
WordPress Security Scanner by the WPSecan Team  
Version 2.9  
Sponsored by Sucuri - https://sucuri.net  
@_WPSecan_, @ethicalhack3r, @erwan_lr, pvdL, @_FireFart_  
  
[!] It seems like you have not updated the database for some time.  
[?] Do you want to update now? [Y]es [N]o [A]bort, default: [N]y
```

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

```
[!] It seems like you have not updated the database for some time.  
[?] Do you want to update now? [Y]es [N]o [A]bort, default: [N]n  
[+] URL: http://[REDACTED].com/  
[+] Started: Sat Oct 22 16:08:46 2016  
  
[+] robots.txt available under: 'http://[REDACTED].com/robots.txt'  
[!] The WordPress 'http://[REDACTED].com/readme.html' file exists exposing a version number  
[+] Interesting header: LINK: <http://[REDACTED].com/>; rel=shortlink  
[+] Interesting header: SERVER: Apache/2.2.23 (CentOS)  
[+] Interesting header: X-POWERED-BY: PHP/5.2.17  
[+] XML-RPC Interface available under: http://[REDACTED].com/xmlrpc.php  
  
[+] WordPress version 3.9.1 identified from meta generator  
[+] 20 vulnerabilities identified from the version number  
  
[!] Title: WordPress 3.9 & 3.9.1 Unlikely Code Execution  
Reference: https://wpvulndb.com/vulnerabilities/7527  
Reference: https://core.trac.wordpress.org/changeset/29389  
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-5203  
[!] Fixed in: 3.9.2  
  
[!] Title: WordPress 2.0.3 - 3.9.1 (except 3.7.4 / 3.8.4) CSRF Token Brute Forcing  
Reference: https://wpvulndb.com/vulnerabilities/7528  
Reference: https://core.trac.wordpress.org/changeset/29384  
Reference: https://core.trac.wordpress.org/changeset/29408  
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-5204  
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-5205  
[!] Fixed in: 3.9.2  
  
[!] Title: WordPress 3.0 - 3.9.1 Authenticated Cross-Site Scripting (XSS) in Multisite  
Reference: https://wpvulndb.com/vulnerabilities/7529  
Reference: https://core.trac.wordpress.org/changeset/29398
```

```

[1] Title: WordPress 3.6 - 3.9.1 Xxe in GetID3 Library
Reference: https://wpvulndb.com/vulnerabilities/7530
Reference: https://github.com/JamesHeinrich/getID3/commit/dc8549079a24bb0619b6124ef2df767704f8d0bc
Reference: http://getid3.sourceforge.net/
Reference: http://wordpress.org/news/2014/08/wordpress-3-9-2/
Reference: http://lab.onsec.ru/2014/09/wordpress-392-xxe-through-media-upload.html
Reference: https://github.com/ONsec-Lab/scripts/blob/master/getid3-xxe.wav
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2053
[1] Fixed in: 3.9.2

[1] Title: WordPress 3.4.2 - 3.9.2 Does Not Invalidate Sessions Upon Logout
Reference: https://wpvulndb.com/vulnerabilities/7531
Reference: http://whiteoaksecurity.com/blog/2012/12/17/cve-2012-5868-wordpress-342-sessions-not-terminated-
pon-explicit-user-logout
Reference: http://blog.spiderlabs.com/2014/09/leveraging-lfi-to-get-full-compromise-on-wordpress-sites.html
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5868
[1] Fixed in: 4.0

[1] Title: WordPress 3.0-3.9.2 - Unauthenticated Stored Cross-Site Scripting (XSS)
Reference: https://wpvulndb.com/vulnerabilities/7680
Reference: http://klikki.fi/adv/wordpress.html
Reference: https://wordpress.org/news/2014/11/wordpress-4-0-1/
Reference: http://klikki.fi/adv/wordpress_update.html
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9031
[1] Fixed in: 4.0

[1] Title: WordPress <= 4.0 - Long Password Denial of Service (DoS)
Reference: https://wpvulndb.com/vulnerabilities/7681
Reference: http://www.behindthefirewalls.com/2014/11/wordpress-denial-of-service-responsible-disclosure.html
Reference: https://wordpress.org/news/2014/11/wordpress-4-0-1/
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9034

```

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 /?**”

```

root@kali:~# joomscan /?

```

Step 3 – To start the scan, type “**joomscan -u URL of the victim**”.

```

root@kali:~#
root@kali:~# joomscan -u http://192.168.1.100/

```



Results will be displayed as shown in the following screenshot.

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 exploiting 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 brute force administrator accounts. Read: <http://yehg.net/lab/pr0js/view.php/MULTIPLE%20TRICKY%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'+and+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:~#