WPScan Enumeration

Enumerating a Website with WPScan

The `--enumerate` flag is used to enumerate various components of the WordPress application such as plugins, themes, and users. By default, WPScan enumerates vulnerable plugins, themes, users, media, and backups. However, specific arguments can be supplied to restrict enumeration to specific components. For example, all plugins can be enumerated using the arguments `--enumerate ap`. Let's run a normal enumeration scan against a WordPress website.

Note: The default number of threads used is 5, however, this value can be changed using the "-t" flag.

WPScan Enumeration

WPScan Enumeration

```
Avenger666@htb[/htb]$ wpscan --url http://blog.inlanefreight.com --enumerate --api-token Kffr4fdJzy9qVcT

[+] URL: http://blog.inlanefreight.com/

[+] Headers
|  - Server: Apache/2.4.38 (Debian)
|  - X-Powered-By: PHP/7.3.15
| Found By: Headers (Passive Detection)

[+] XML-RPC seems to be enabled: http://blog.inlanefreight.com/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
|  - http://codex.wordpress.org/XML-RPC_Pingback_API

[+] The external WP-Cron seems to be enabled: http://blog.inlanefreight.com/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
|  - https://www.iplocation.net/defend-wordpress-from-ddos

[+] WordPress version 5.3.2 identified (Latest, released on 2019-12-18).
| Found By: Rss Generator (Passive Detection)
|  - http://blog.inlanefreight.com/?feed=rss2, <generator>https://wordpress.org/?v=5.3.2</generator>

[+] WordPress theme in use: twentytwenty
| Location: http://blog.inlanefreight.com/wp-content/themes/twentytwenty/
| Readme: http://blog.inlanefreight.com/wp-content/themes/twentytwenty/readme.txt
| [!] The version is out of date, the latest version is 1.2
| Style Name: Twenty Twenty

[+] Enumerating Vulnerable Plugins (via Passive Methods)
[i] Plugin(s) Identified:
[+] mail-masta
| Location: http://blog.inlanefreight.com/wp-content/plugins/mail-masta/
| Latest Version: 1.0 (up to date)
| Found By: Urls In Homepage (Passive Detection)
| [!] 2 vulnerabilities identified:
|
| [!] Title: Mail Masta 1.0 - Unauthenticated Local File Inclusion (LFI)
|      - https://www.exploit-db.com/exploits/40290/
| [!] Title: Mail Masta 1.0 - Multiple SQL Injection
|      - https://wpvulndb.com/vulnerabilities/8740
[+] wp-google-places-review-slider
| [!] 1 vulnerability identified:
| [!] Title: WP Google Review Slider <= 6.1 - Authenticated SQL Injection
|     Reference: https://wpvulndb.com/vulnerabilities/9933

[i] No themes Found.
<SNIP>
[i] No Config Backups Found.
<SNIP>
[i] No Medias Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
<SNIP>
[i] User(s) Identified:
[+] admin
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] david
<SNIP>
[+] roger
<SNIP>
```

WPScan uses various passive and active methods to determine versions and vulnerabilities, as shown in the scan output above.

Connect to Pwnbox
Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK 1136ms

Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...

Questions

Answer the question(s) below to complete this Section and earn cubes!

Cheat Sheet

Target: Click here to spawn the target system!

+ 1 Enumerate the provided WordPress instance for all installed plugins. Perform a scan with WPScan against the target and submit the version of the vulnerable plugin named "photo-gallery".

1.5.34

Submit Hint

Previous Next

Mark Complete & Next

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left