WordPress Enumeration with WPScan

WPScan is a vulnerability scanner that comes preinstalled with Kali Linux, but can be installed on most Linux distros.

The tool can be used to scan WordPress installations for vulnerability and security issues.

You can download the Turnkey image from here.

In this tutorial i am using WPScan to enumerate a WordPress website that is running on a Linux lab server, i am using Turnkey Linux with a WordPress preinstalled images for a server, the server is running on VMware Workstation.

DISCLAIMER: This software/tutorial is for educational purposes only. Please don’t use it for illegal activity. The author is not responsible for the use of the application or the users action.

Requirements

- Kali Linux
- WordPress Website

Step 1: WPScan Syntax

1.1 Update WPScan vulnerabilities database.

```
wpscan --update
```

1.2 Scan a website for vulnerabilities, you can either use a host name or a IP address.

```
wpscan --url 172.168.200.140
```

```
wpscan --url www.wordpress.local
```

NOTE: If you run WPScan on a website that is not running WordPress you will be notified in the output that the remote site is up, but not running WordPress.

```
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|
```

```
        WordPress Security Scanner by the WPScan Team
                       Version 3.6.0
          Sponsored by Sucuri - https://sucuri.net
      @_WPScan_, @ethicalhack3r, @erwan_lr, @_FireFart_
_______________________________________________________________


Scan Aborted: The remote website is up, but does not seem to be running WordPress.
root@iPhone:~#
```

1.3 Enumerate plugins

```
wpscan --url www.wordpress.local --enumerate p
```

1.4 Scan custom directory

```
wpscan --url www.wordpress.local --wp-content-dir custom-content
```

1.5 Enumerate themes

```
wpscan --url www.wordpress.local --enumerate t
```

1.6 Stealth Scan

```
wpscan --url www.wordpress.local --stealthy
```

1.7 Enumerate users, scan the target site for WordPress authors and usernames.

```
wpscan --url www.wordpress.local --enumerate u
```

```
[i] User(s) Identified:

[+] admin
 | Detected By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] testuser
 | Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)


[+] Finished: Thu Jul 18 15:09:44 2019
[+] Requests Done: 16
[+] Cached Requests: 42
[+] Data Sent: 3.339 KB
[+] Data Received: 26.85 KB
[+] Memory used: 102.207 MB
[+] Elapsed time: 00:00:01
root@iPhone:~#
```

NOTE: limit how many usernames WPScan will enumerate

```

```

Step 2: Brute Force WordPress Account Password

2.1 We can use WPScan to brute force a WordPress account.

To run the attack we need a password wordlist, there is one called “rockyou.txt” in Kali Linux.

You can find it in “/usr/share/wordlists/ “

Type the command into terminal to brute force the password for a user

```
wpscan –url [wordpress url] –wordlist [path to wordlist] –username [username] –threads [number of threads]
```

```
wpscan --url www.wordpress.local –wordlist /usr/share/wordlists/rockyou.txt –username testuser –threads 2
```

NOTE: Eventually, you should see the password listed in the terminal next to the login ID of the user.

Step 3: Optional

3.1 Use WPScan with Tor and proxychains, for more information on how to setup Tor and proxychains please check out our notes.

NOTE: You need to start the Tor service before running the command.

```
proxychains wpscan --url www.wordpress.local
```

Conclusion

As we can see it is very easy for a attacker to scan a WordPress site and brute force a account.

To avoid WordPress enumeration and brute force attacks use WordPress plugins that limits the number of login attempts for a specific username and IP address.

Furthermore administrators should avoid using usernames as nicknames and display names, display names ares shown in WordPress and easy to scan.

WPScan scans the URL’s for usernames, if the administrator username is not used for publishing, then the account wont be scanned by WPScan”

DISCLAIMER: This software/tutorial is for educational purposes only. Please don’t use it for illegal activity. The author is not responsible for the use of the application or the users action.