

HackerDivulgation.com

DOCS

WPScan

WPScan es una herramienta gratuita que permite escanear sitios web creados con el CMS WordPress. Posee una base de datos de al menos 28 mil vulnerabilidades de WordPress. Esta herramienta puede ser útil para webmasters que trabajen con WordPress para comprobar que plugins, themes u otros complementos no presenten vulnerabilidades. En sistemas como Kali Linux o Parrot esta herramienta viene instalada por defecto.

Proyecto: [WPScan-Github](#)

¿Cómo montar un laboratorio con WordPress en servidor LAMP?

Disponible el siguiente artículo. <http://hackerdivulgation.com/articles/lab-wordpress>

Contenido

- [Requisitos](#)
- [Instalación](#)
- [Opciones](#)
- [Uso](#)
 - [Actualizar](#)
 - [Enumerar usuarios](#)
 - [Enumerar temas](#)
 - [Ataque de fuerza bruta](#)
- [Referencias](#)

Requisitos

Sin estos programas y librerías no se podrá instalar WPScan. Más información de los requisitos en [Github](#).

1. Ruby >= 2.5
2. Curl >= 7.72
3. RubyGems latest

Instalación de requisitos

Instalar las utilidades de Ruby.

```
sudo apt update  
sudo apt install ruby ruby-dev
```

Comprobar las versiones instaladas.

```
ruby -v  
gem -v
```

Nota: Curl en la mayoría de sistemas viene instalado por defecto.

Instalación

Con las dependencias instaladas solo resta ejecutar el siguiente comando.

```
sudo gem install wpscan
```

Opciones

Para desplegar la ayuda se usa el parámetro `--help` .

```
wpscan --help
```

```
(alex@hackerdivulgation)-[~]
$ wpscan --help

  _____
 /         \
|  WPSCAN  |
 \         /
  _____

WordPress Security Scanner by the WPScan Team
Version 3.8.20

@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

Usage: wpscan [options]
--url URL                                The URL of the blog to scan
                                         Allowed Protocols: http, https
                                         Default Protocol if none provided: http
                                         This option is mandatory unless update or help or hh or vers
ion is/are supplied
-h, --help                               Display the simple help and exit
--hh                                     Display the full help and exit
--version                               Display the version and exit
-v, --verbose                             Verbose mode
--[no-]banner                           Whether or not to display the banner
                                         Default: true
```

Visualizar todas las opciones --hh .

```
wpscan --hh
```

Parámetros básicos y más utilizados.

Parámetros	Descripción
--url URL	La URL del blog en WordPress.
-v, --verbose	Modo verbose, mostrar los pasos realizados en el escaneo.
--random-user-agent	Usar random user-agent por cada escaneo.
-e, --enumerate [OPTS]	Enumeración de procesos. Ejm: vp (Plugins vulnerables).
--plugins-detection MODE	Proceso de detección de plugins. Modo: mixed, passive, agresive.
-o, --output FILE	Exportar el escaneo a un archivo.

USO

Esta herramienta es muy flexible y presenta muchas formas de uso desde las básicas a las


avanzadas. A continuación, se mostrarán algunas.

Actualizar

Es importante siempre mantener actualizada la base de datos de vulnerabilidades de WordPress.

```
wpscan --update
```

```
(alex@hackerdivulgate)-[~]
$ wpscan --update
```



WordPress Security Scanner by the WPScan Team
Version 3.8.20

@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

```
[i] Updating the Database ...
[i] Update completed.
```

Enumerar usuarios

Conocer los usuarios WordPress, teniendo esta información se puede realizar un ataque de fuerza bruta para conocer la contraseña.

```
wpscan --url http://IP_OR_DOMAIN_TARGET -e u --no-banner
```

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

[+] admin
| Found By: Rss Generator (Passive Detection)
| Confirmed By:
|   Wp Json Api (Aggressive Detection)
|   - http://192.168.1.15/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)

[!] 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: Thu Mar 17 23:24:25 2022
[+] Requests Done: 23
[+] Cached Requests: 36
[+] Data Sent: 6.652 KB
[+] Data Received: 73.581 KB
[+] Memory used: 178.793 MB
[+] Elapsed time: 00:00:04
```

Enumerar temas

Algunos temas pueden tener vulnerabilidades que pueden ser explotadas.

```
wpscan --url http://IP_OR_DOMAIN_TARGET -e at --no-banner
```

```
[+] WordPress theme in use: twentytwentytwo
| Location: http://192.168.1.15/wordpress/wp-content/themes/twentytwentytwo/
| Last Updated: 2022-02-25T00:00:00.000Z
| Readme: http://192.168.1.15/wordpress/wp-content/themes/twentytwentytwo/readme.txt
| [!] The version is out of date, the latest version is 1.1
| Style URL: http://192.168.1.15/wordpress/wp-content/themes/twentytwentytwo/style.css?ver=1.0
| Style Name: Twenty Twenty-Two
| Style URI: https://github.com/wordpress/twentytwentytwo/
| Description: Built on a solidly designed foundation, Twenty Twenty-Two embraces the idea that everyone deserves a...
| Author: the WordPress team
| Author URI: https://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.0 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.1.15/wordpress/wp-content/themes/twentytwentytwo/style.css?ver=1.0, Match: 'Version: 1.0'
```

Ataque de fuerza bruta

Para este tipo de ataques se necesita un diccionario, por medio de ingeniería social se puede generar posibles contraseñas con [CUPP \(artículo disponible\)](#). También se puede hacer con diccionarios disponibles en internet o los diccionarios por defecto de Kali, estos se encuentran en la ruta `/usr/share/wordlist/`.

```
cp /usr/share/wordlists/fasttrack.txt /home/USER/Documents/wordlist.txt
```

```
(alex@hackerdivulgation)-[/usr/share/wordlists]
$ ls
dirb  dirbuster  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt.gz  wfuzz
```

```
wpscan --url http://IP_OR_DOMAIN_TARGET -U LIST_FILE_PATH -P FILE_PATH --randc
```

<https://www.youtube.com/watch?v=YjShYFUnaqk>

Referencias

1. Proyecto en Github. <https://github.com/wpscanteam/wpscan>
2. Página Oficial de WPScan. <https://wpscan.com/>
3. Video de ataque de fuerza bruta con WPScan. <https://www.youtube.com/watch?v=YjShYFUnaqk>



Esta obra está bajo una [licencia de Creative Commons Reconocimiento-NoComercial-SinObraDerivada 4.0 Internacional](https://creativecommons.org/licenses/by-nc-nd/4.0/).