WPScan Overview

Cheat Sheet

Using WPScan

WPScan is an automated WordPress scanner and enumeration tool. It determines if the various themes and plugins used by a WordPress site are outdated or vulnerable. It is installed by default on Parrot OS but can also be installed manually with `gem`.

```
Avenger666@htb[/htb]$ gem install wpscan
```

Once the installation completes, we can issue a command such as `wpscan --hh` to verify the installation. This command will show us the usage menu with all of the available command-line switches.

```
Avenger666@htb[/htb]$ wpscan --hh
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                        Version 3.8.1

       @_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 he
    -h, --help                                  Display the simple help and exit
        --hh                                    Display the full help and exit
        --version                               Display the version and exit
        --ignore-main-redirect                  Ignore the main redirect (if any) and scan t
    -v, --verbose                               Verbose mode
        --[no-]banner                           Whether or not to display the banner
                                                Default: true
        --max-scan-duration SECONDS             Abort the scan if it exceeds the time provid
    -o, --output FILE                           Output to FILE
    -f, --format FORMAT                         Output results in the format supplied
                                                Available choices: cli-no-colour, cli-no-col

        <SNIP>
```

There are various enumeration options that can be specified, such as vulnerable plugins, all plugins, user enumeration, and more. It is important to understand all of the options available to us and fine-tune the scanner depending on the goal (i.e., are we just interested to see if the WordPress site is using any vulnerable plugins, do we need to perform a full audit of all aspects of the site or are we just interested in creating a user list to use in a brute force password guessing attack?).

WPScan can pull in vulnerability information from external sources to enhance our scans. We can obtain an API token from WPVulnDB, which is used by WPScan to scan for vulnerability and exploit proof of concepts (POC) and reports. The free plan allows up to 50 requests per day. To use the WPVulnDB database, just create an account and copy the API token from the users page. This token can then be supplied to WPScan using the `--api-token` parameter.

Review the various WPScan options using the below Parrot instance by opening a shell and issuing the command `wpscan --hh`.

Connect to Pwnbox
Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location
UK 203ms

Terminate Pwnbox to switch location

Start Instance
∞ / 1 spawns left

Waiting to start...

Previous Next
Mark Complete & Next

My Workstation

OFFLINE

Start Instance
∞ / 1 spawns left