WPScan Package Description

WPScan is a black box WordPress vulnerability scanner that can be used to scan remote WordPress installations to find security issues.

Source: http://wpscan.org/
WPScan Homepage | Kali wpscan Repo

- Author: The WPScan Team
- License: Other

Tools included in the wpscan package

wpscan – WordPress vulnerability scanner

root@kali:~# wpscan --help

```
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.6
          Sponsored by Sucuri - https://sucuri.net
      @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________
```

Help :

Some values are settable in a config file, see the example.conf.json

```
--update                    Update to the database to the latest version.
--url      | -u <target url>      The WordPress URL/domain to scan.
--force    | -f                   Forces WPScan to not check if the remote site is running WordPress.
--enumerate | -e [option(s)]      Enumeration.
  option :
```

```
    u       usernames from id 1 to 10
    u[10-20] usernames from id 10 to 20 (you must write [] chars)
    p       plugins
    vp      only vulnerable plugins
    ap      all plugins (can take a long time)
    tt      timthumbs
    t       themes
    vt      only vulnerable themes
    at      all themes (can take a long time)
  Multiple values are allowed : "-e tt,p" will enumerate timthumbs and plugins
  If no option is supplied, the default is "vt,tt,u,vp"

--exclude-content-based "<regexp or string>"
                        Used with the enumeration option, will exclude all occurrences based on the regexp or string supplied.
                        You do not need to provide the regexp delimiters, but you must write the quotes (simple or double).
--config-file  | -c <config file>   Use the specified config file, see the example.conf.json.
--user-agent   | -a <User-Agent>    Use the specified User-Agent.
--cookie <String>                   String to read cookies from.
--random-agent | -r                 Use a random User-Agent.
--follow-redirection                If the target url has a redirection, it will be followed without asking if you wanted to do so or no
--batch                             Never ask for user input, use the default behaviour.
--no-color                          Do not use colors in the output.
--wp-content-dir <wp content dir>   WPScan try to find the content directory (ie wp-content) by scanning the index page, ho
                        Subdirectories are allowed.
--wp-plugins-dir <wp plugins dir>   Same thing than --wp-content-dir but for the plugins directory.
                        If not supplied, WPScan will use wp-content-dir/plugins. Subdirectories are allowed
--proxy <[protocol://]host:port>    Supply a proxy. HTTP, SOCKS4 SOCKS4A and SOCKS5 are supported.
                        If no protocol is given (format host:port), HTTP will be used.
--proxy-auth <username:password>    Supply the proxy login credentials.
--basic-auth <username:password>    Set the HTTP Basic authentication.
--wordlist | -w <wordlist>          Supply a wordlist for the password brute forcer.
--username | -U <username>          Only brute force the supplied username.
--usernames     <path-to-file>      Only brute force the usernames from the file.
--threads  | -t <number of threads> The number of threads to use when multi-threading requests.
--cache-ttl       <cache-ttl>       Typhoeus cache TTL.
--request-timeout <request-timeout> Request Timeout.
--connect-timeout <connect-timeout> Connect Timeout.
--max-threads     <max-threads>     Maximum Threads.
--help     | -h                    This help screen.
--verbose  | -v                    Verbose output.
--version                           Output the current version and exit.
```

Examples :

-Further help ...
ruby ./wpscan.rb --help

-Do 'non-intrusive' checks ...
ruby ./wpscan.rb --url www.example.com

-Do wordlist password brute force on enumerated users using 50 threads ...
ruby ./wpscan.rb --url www.example.com --wordlist darkc0de.lst --threads 50

-Do wordlist password brute force on the 'admin' username only ...
ruby ./wpscan.rb --url www.example.com --wordlist darkc0de.lst --username admin

-Enumerate installed plugins ...
ruby ./wpscan.rb --url www.example.com --enumerate p

-Enumerate installed themes ...
ruby ./wpscan.rb --url www.example.com --enumerate t

-Enumerate users ...
ruby ./wpscan.rb --url www.example.com --enumerate u

-Enumerate installed timthumbs ...
ruby ./wpscan.rb --url www.example.com --enumerate tt

-Use a HTTP proxy ...
ruby ./wpscan.rb --url www.example.com --proxy 127.0.0.1:8118

-Use a SOCKS5 proxy ... (cURL >= v7.21.7 needed)
ruby ./wpscan.rb --url www.example.com --proxy socks5://127.0.0.1:9000

-Use custom content directory ...
ruby ./wpscan.rb -u www.example.com --wp-content-dir custom-content

-Use custom plugins directory ...
ruby ./wpscan.rb -u www.example.com --wp-plugins-dir wp-content/custom-plugins

-Update the DB ...
ruby ./wpscan.rb --update

-Debug output ...

ruby ./wpscan.rb --url www.example.com --debug-output 2>debug.log

See README for further information.

WPScan Usage Example

Scan a target WordPress URL and enumerate any plugins that are installed:

```
root@kali:~# wpscan --url http://wordpress.local --enumerate p
_______________________________________________________________

        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.6
          Sponsored by Sucuri - https://sucuri.net
      @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________

[+] URL: http://wordpress.local/
[+] Started: Mon Jan 12 14:07:40 2015

[+] robots.txt available under: 'http://wordpress.local/robots.txt'
[+] Interesting entry from robots.txt: http://wordpress.local/search
[+] Interesting entry from robots.txt: http://wordpress.local/support/search.php
[+] Interesting entry from robots.txt: http://wordpress.local/extend/plugins/search.php
[+] Interesting entry from robots.txt: http://wordpress.local/plugins/search.php
[+] Interesting entry from robots.txt: http://wordpress.local/extend/themes/search.php
[+] Interesting entry from robots.txt: http://wordpress.local/themes/search.php
[+] Interesting entry from robots.txt: http://wordpress.local/support/rss
[+] Interesting entry from robots.txt: http://wordpress.local/archive/
[+] Interesting header: SERVER: nginx
[+] Interesting header: X-FRAME-OPTIONS: SAMEORIGIN
[+] Interesting header: X-NC: HIT lax 249
[+] XML-RPC Interface available under: http://wordpress.local/xmlrpc.php

[+] WordPress version 4.2-alpha-31168 identified from rss generator
```

[+] Enumerating installed plugins ...

Time: 00:00:35 <==========> (2166 / 2166) 100.00% Time: 00:00:3

[+] We found 2166 plugins:

...