wpscan 3.8.7 Cheatsheet (ingenieriainformatica.uniovi.es)

A vulnerability scanner for WordPress websites

https://github.com/wpscanteam/wpscan

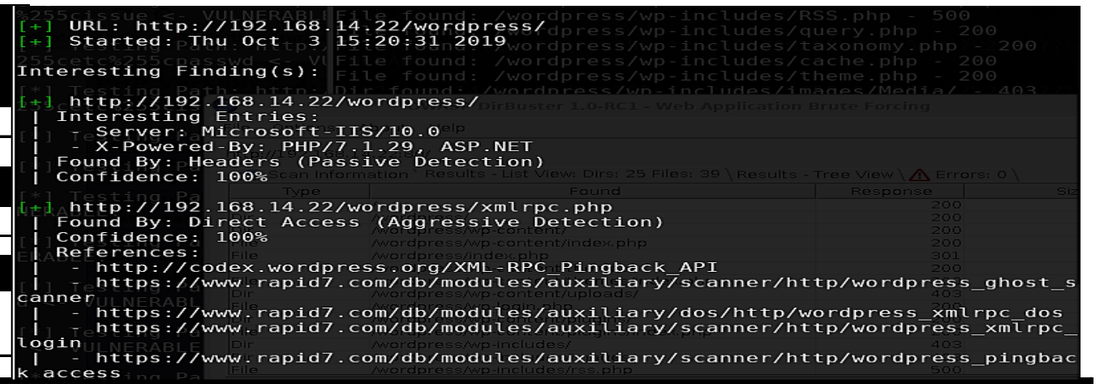
GENERAL USAGE

```
wpscan --url URL [options]
```

NOTES

Allowed Protocols: http, https

Default Protocol if none provided: http



OPTIONS

--[no-]banner: Whether or not to display the banner (Default: true)

--[no-]update: Whether or not to update the Database

--api-token TOKEN: The WPVulnDB API Token to display vulnerability data

--connect-timeout SECONDS: The connection timeout in seconds (Default: 30)

--cookie-jar FILE-PATH: File to read and write cookies (Default: /tmp/wpscan/cookie_jar.txt)

--cookie-string COOKIE: Cookie string to use in requests, format: cookie1=value1[; cookie2=value2]

--detection-mode MODE: Default: mixed (Available choices: mixed, passive, aggressive)

--disable-tls-checks: Disables SSL/TLS certificate verification, and downgrade to TLS1.0+ (requires cURL 7.66 for the latter)

--exclude-content-based REGEXP_OR_STRING: Exclude all responses matching the Regexp (case insensitive) during parts of the enumeration. (Both the headers and body are checked. Regexp delimiters are not required.)

-f, --format FORMAT: Output results in the format supplied (Available choices: cli-no-colour, cli-no-color, json, cli)

--force: Do not check if the target is running WordPress

-h, --help: Display the simple help and exit

--hh: Display the full help and exit

--http-auth login:password: Credentials to send if HTTP auth is used in the server

--multicall-max-passwords MAX_PWD: Maximum number of passwords to send by request with XMLRPC multicall (Default: 500)

-o, --output FILE: Output to FILE

-P, --passwords FILE-PATH: List of passwords to use during the password attack. (If no --username/s option supplied, user enumeration will be run.)

--password-attack ATTACK: Force the supplied attack to be used rather than automatically determining one. (Available choices: wp-login, xmlrpc, xmlrpc-multicall)

--plugins-detection MODE: Use the supplied mode to enumerate Plugins. (Default: passive) (Available choices: mixed, passive, aggressive)

--plugins-version-detection MODE: Use the supplied mode to check plugins' versions. (Default: mixed) (Available choices: mixed, passive, aggressive)

--proxy protocol://IP:port: Supported protocols depend on the cURL installed

--proxy-auth login:password: Credentials to send to a potential proxy in the network, so scan can take place in these scenarios

--random-user-agent, --rua: Use a random user-agent for each scan

-e, --enumerate [OPTS]: *Enumeration Process.*
Separator to use between the values: ','
Default: All Plugins, Config Backups (Value if no argument supplied: vp,vt,tt,cb,dbe,u,m)
Incompatible choices (only one of each group/s can be used):
- vp, ap, p
- vt, at, t
Available Choices:
vp Vulnerable plugins
ap All plugins
p Popular plugins
vt Vulnerable themes
at All themes
t Popular themes
tt Timthumbs
cb Config backups
dbe Db exports
u User IDs range. e.g: u1-5. Range separator to use: '-'
(Value if no argument supplied: 1-10)
m Media IDs range. e.g m1-15. Range separator to use: '-'
(Value if no argument supplied: 1-100)
(Permalink setting must be set to "Plain" for those to be detected)

--throttle MilliSeconds: Milliseconds to wait before doing another web request. If used, the max threads will be set to 1.

-U, --usernames LIST: List of usernames to use during the password attack. (Examples: 'a1', 'a1,a2,a3', '/tmp/a.txt')

--user-agent, --ua VALUE: Change the identification data that the tool sends to the server

-v, --verbose: Verbose mode

--version: Display the version and exit

--wp-content-dir DIR: The wp-content directory if custom or not detected, such as "wp-content"

--wp-plugins-dir DIR: The plugins directory if custom or not detected, such as "wp-content/plugins"

--request-timeout SECONDS: The request timeout in seconds (Default: 60)	**EXAMPLES**
--stealthy: Alias for --random-user-agent --detection-mode passive --plugins-version-detection passive	*wpscan --url http://<url>/blog --enumerate vp --plugins-detection aggressive* *wpscan --url http://<url> --wp-content-dir /wp-content/ --enumerate vp --plugins-detection aggressive*
-t, --max-threads VALUE: The max threads to use (Default: 5)	

by José Manuel Redondo López