
Práctica

IAW - Implantación de Aplicaciones Web

Curso 2025/2026

Índice general

1 Auditoría de seguridad en WordPress con WPScan	1
1.1 Contenedor Docker con WPScan	1
1.2 Ejemplos básicos de uso	9
1.3 Seguridad en WordPress	9
2 Referencias	11
3 Licencia	12

19		This option is mandatory unless update or help or hh or version is/are supplied
20	-h, --help exit	Display the simple help and
21	--hh exit	Display the full help and
22	--version	Display the version and exit
23	-v, --verbose	Verbose mode
24	--[no-]banner banner	Whether or not to display the
25		Default: true
26	-o, --output FILE	Output to FILE
27	-f, --format FORMAT supplied	Output results in the format
28		Available choices: cli-no-colour, cli-no-color, json, cli
29	--detection-mode MODE	Default: mixed
30		Available choices: mixed, passive, aggressive
31	--user-agent, --ua VALUE	
32	--random-user-agent, --rua each scan	Use a random user-agent for
33	--http-auth login:password	
34	-t, --max-threads VALUE	The max threads to use
35		Default: 5
36	--throttle MilliSeconds doing another web request. If used, the max threads will be set to 1.	Milliseconds to wait before
37	--request-timeout SECONDS seconds	The request timeout in
38		Default: 60
39	--connect-timeout SECONDS seconds	The connection timeout in
40		Default: 30
41	--disable-tls-checks verification, and downgrade to TLS1.0+ (requires cURL 7.66 for the latter)	Disables SSL/TLS certificate
42	--proxy protocol://IP:port the cURL installed	Supported protocols depend on
43	--proxy-auth login:password	
44	--cookie-string COOKIE requests, format: cookie1=value1[; cookie2=value2]	Cookie string to use in
45	--cookie-jar FILE-PATH cookies	File to read and write
46		Default: /tmp/wpscan/ cookie_jar.txt
47	--force running WordPress or returns a 403	Do not check if the target is
48	--[no-]update Database	Whether or not to update the
49	--api-token TOKEN display vulnerability data, available at https://wpscan.com/profile	The WPScan API Token to
50	--wp-content-dir DIR custom or not detected, such as "wp-content"	The wp-content directory if

51	<code>--wp-plugins-dir DIR</code>	The plugins directory if custom or not detected, such as "wp-content/plugins"
52	<code>-e, --enumerate [OPTS]</code>	Enumeration Process
53		Available Choices:
54		vp Vulnerable plugins
55		ap All plugins
56		p Popular plugins
57		vt Vulnerable themes
58		at All themes
59		t Popular themes
60		tt Timthumbs
61		cb Config backups
62		dbe Db exports
63		u User IDs range. e.g: u1-5
64		Range separator to use: '-'
65		Value if no argument supplied: 1-10
66		m Media IDs range. e.g m1-15
67		Note: Permalink setting must be set to "Plain" for those to be detected
68		Range separator to use: '-'
69		Value if no argument supplied: 1-100
70		Separator to use between the values: ','
71		Default: All Plugins, Config Backups
72		Value if no argument supplied: vp,vt,tt,cb,dbe,u,m
73		Incompatible choices (only one of each group/s can be used):
74		- vp, ap, p
75		- vt, at, t
76	<code>--exclude-content-based REGEXP_OR_STRING</code>	Exclude all responses matching the Regexp (case insensitive) during parts of the enumeration.
77		Both the headers and body are checked. Regexp delimiters are not required.
78	<code>--plugins-detection MODE</code>	Use the supplied mode to enumerate Plugins.
79		Default: passive
80		Available choices: mixed, passive, aggressive
81	<code>--plugins-version-detection MODE</code>	Use the supplied mode to check plugins' versions.
82		Default: mixed
83		Available choices: mixed, passive, aggressive

	any) and scan the target url	
24	-v, --verbose	Verbose mode
25	--[no-]banner banner	Whether or not to display the Default: true
26		
27	--max-scan-duration SECONDS the time provided in seconds	Abort the scan if it exceeds
28	-o, --output FILE	Output to FILE
29	-f, --format FORMAT supplied	Output results in the format Available choices: cli-no- colour, cli-no-color, json , cli
30		
31	--detection-mode MODE	Default: mixed
32		Available choices: mixed, passive, aggressive
33	--scope DOMAINS to consider in scope.	Comma separated (sub-)domains
34		Wildcard(s) allowed in the trd of valid domains, e.g: *.target.tld
35		Separator to use between the values: ','
36	--user-agent, --ua VALUE	
37	--headers HEADERS in requests	Additional headers to append
38		Separator to use between the headers: ';' '
39		Examples: 'X-Forwarded-For: 127.0.0.1', 'X-Forwarded- For: 127.0.0.1; Another: aaa'
40	--vhost VALUE) to use in requests	The virtual host (Host header
41	--random-user-agent, --rua each scan	Use a random user-agent for
42	--user-agents-list FILE-PATH random-user-agent	List of agents to use with --
43		Default: /usr/local/bundle/ gems/cms_scanner-0.13.0/ app/user_agents.txt
44	--http-auth login:password	
45	-t, --max-threads VALUE	The max threads to use
46		Default: 5
47	--throttle MilliSeconds doing another web request. If used, the max threads will be set to 1.	Milliseconds to wait before
48	--request-timeout SECONDS seconds	The request timeout in
49		Default: 60
50	--connect-timeout SECONDS seconds	The connection timeout in
51		Default: 30
52	--disable-tls-checks verification, and downgrade to TLS1.0+ (requires cURL 7.66 for the latter)	Disables SSL/TLS certificate
53	--proxy protocol://IP:port	Supported protocols depend on

```

    the cURL installed
54     --proxy-auth login:password
55     --cookie-string COOKIE           Cookie string to use in
    requests, format: cookie1=value1[; cookie2=value2]
56     --cookie-jar FILE-PATH           File to read and write
    cookies
57                                     Default: /tmp/wpscan/
    cookie_jar.txt
58     --cache-ttl TIME_TO_LIVE         The cache time to live in
    seconds
59                                     Default: 600
60     --clear-cache                     Clear the cache before the
    scan
61     --cache-dir PATH                 Default: /tmp/wpscan/cache
62     --server SERVER                   Force the supplied server
    module to be loaded
63                                     Available choices: apache,
    iis, nginx
64     --force                           Do not check if the target is
    running WordPress or returns a 403
65     --[no-]update                     Whether or not to update the
    Database
66     --api-token TOKEN                 The WPScan API Token to
    display vulnerability data, available at https://wpscan.com/profile
67     --wp-content-dir DIR              The wp-content directory if
    custom or not detected, such as "wp-content"
68     --wp-plugins-dir DIR              The plugins directory if
    custom or not detected, such as "wp-content/plugins"
69     --interesting-findings-detection MODE Use the supplied mode for the
    interesting findings detection.
70                                     Available choices: mixed,
    passive, aggressive
71     --wp-version-all                 Check all the version
    locations
72     --wp-version-detection MODE       Use the supplied mode for the
    WordPress version detection, instead of the global (--detection-
    mode) mode.
73                                     Available choices: mixed,
    passive, aggressive
74     --main-theme-detection MODE       Use the supplied mode for the
    Main theme detection, instead of the global (--detection-mode) mode
75     .
76     -e, --enumerate [OPTS]           Enumeration Process
77                                     Available Choices:
78     vp  Vulnerable plugins
79     ap  All plugins
80     p   Popular plugins
81     vt  Vulnerable themes
82     at  All themes
83     t   Popular themes
84     tt  Timthumbs
85     cb  Config backups
86     db  Db exports
87     u   User IDs range. e.g: u1
    -5

```

88		Range separator to use: '_'
89		Value if no argument supplied: 1-10
90	m	Media IDs range. e.g m1 -15
91		Note: Permalink setting must be set to " Plain" for those to be detected
92		Range separator to use: '_'
93		Value if no argument supplied: 1-100
94		Separator to use between the values: ','
95		Default: All Plugins, Config Backups
96		Value if no argument supplied : vp,vt,tt,cb,dbe,u,m
97		Incompatible choices (only one of each group/s can be used):
98		- vp, ap, p
99		- vt, at, t
100	--exclude-content-based REGEXP_OR_STRING	Exclude all responses matching the Regexp (case insensitive) during parts of the enumeration.
101		Both the headers and body are checked. Regexp delimiters are not required.
102	--plugins-list LIST	List of plugins to enumerate
103		Examples: 'a1', 'a1,a2,a3', ' /tmp/a.txt'
104	--plugins-detection MODE	Use the supplied mode to enumerate Plugins.
105		Default: passive
106		Available choices: mixed, passive, aggressive
107	--plugins-version-all	Check all the plugins version locations according to the chosen mode (--detection-mode, -- plugins-detection and --plugins-version-detection)
108	--plugins-version-detection MODE	Use the supplied mode to check plugins' versions.
109		Default: mixed
110		Available choices: mixed, passive, aggressive
111	--plugins-threshold THRESHOLD	Raise an error when the number of detected plugins via known locations reaches the threshold . Set to 0 to ignore the threshold.
112		Default: 100
113	--themes-list LIST	List of themes to enumerate
114		Examples: 'a1', 'a1,a2,a3', ' /tmp/a.txt'
115	--themes-detection MODE	Use the supplied mode to enumerate Themes, instead of the global (--detection-mode) mode.

```
116                                     Available choices: mixed,  
117                                     passive, aggressive  
117 --themes-version-all                Check all the themes version  
    locations according to the chosen mode (--detection-mode, --themes-  
118 --themes-version-detection MODE      Use the supplied mode to  
    check themes versions instead of the --detection-mode or --themes-  
    detection modes.  
119                                     Available choices: mixed,  
120                                     passive, aggressive  
120 --themes-threshold THRESHOLD        Raise an error when the  
    number of detected themes via known locations reaches the threshold.  
    Set to 0 to ignore the threshold.  
121                                     Default: 20  
122 --timthumbs-list FILE-PATH           List of timthumbs' location  
    to use  
123                                     Default: /wpscan/.wpscan/db/  
124 --timthumbs-detection MODE           Use the supplied mode to  
    enumerate Timthumbs, instead of the global (--detection-mode) mode.  
125                                     Available choices: mixed,  
126                                     passive, aggressive  
126 --config-backups-list FILE-PATH      List of config backups'  
    filenames to use  
127                                     Default: /wpscan/.wpscan/db/  
128 --config-backups-detection MODE      Use the supplied mode to  
    enumerate Config Backups, instead of the global (--detection-mode)  
    mode.  
129                                     Available choices: mixed,  
130 --db-exports-list FILE-PATH          List of DB exports' paths to  
    use  
131                                     Default: /wpscan/.wpscan/db/  
132 --db-exports-detection MODE          Use the supplied mode to  
    enumerate DB Exports, instead of the global (--detection-mode) mode.  
133                                     Available choices: mixed,  
134                                     passive, aggressive  
134 --medias-detection MODE             Use the supplied mode to  
    enumerate Medias, instead of the global (--detection-mode) mode.  
135                                     Available choices: mixed,  
136                                     passive, aggressive  
136 --users-list LIST                   List of users to check during  
    the users enumeration from the Login Error Messages  
137                                     Examples: 'a1', 'a1,a2,a3', '  
    /tmp/a.txt'  
138 --users-detection MODE              Use the supplied mode to  
    enumerate Users, instead of the global (--detection-mode) mode.  
139                                     Available choices: mixed,  
140 -P, --passwords FILE-PATH           List of passwords to use  
    during the password attack.  
141                                     If no --username/s option  
142 -U, --usernames LIST                List of usernames to use
```

	during the password attack.	
143		Examples: 'a1', 'a1,a2,a3', '/tmp/a.txt'
144	--multicall-max-passwords MAX_PWD to send by request with XMLRPC multicall	Maximum number of passwords Default: 500
145		Force the supplied attack to be used rather than automatically determining one.
146	--password-attack ATTACK	Available choices: wp-login, xmlrpc, xmlrpc-multicall
147		The URI of the login page if different from /wp-login.php
148	--login-uri URI	
149	--stealthy --detection-mode passive --plugins-version-detection passive	Alias for --random-user-agent

1.2. Ejemplos básicos de uso

A continuación vamos a ver algunos ejemplos básicos de uso.

Ejemplo 1

Para obtener la lista de *plugins* instalados en nuestro sitio WordPress podemos ejecutar:

```
1 docker run -it --rm wpscanteam/wpscan --url http://192.168.22.20 --enumerate p
```

Donde **192.168.22.20** será la dirección IP de la máquina donde hemos realizado la instalación de WordPress.

Ejemplo 2

Para realizar un escaneo completo de un sitio WordPress podemos ejecutar:

```
1 docker run -it --rm wpscanteam/wpscan --url http://192.168.22.20
```

Donde **192.168.22.20** será la dirección IP de la máquina donde hemos realizado la instalación de WordPress.

Ejemplo 3

En este ejemplo haremos uso de la [API de WPScan](#) que nos permite detectar vulnerabilidades haciendo uso de su base de datos de vulnerabilidades.

Para poder hacer uso del servicio de la API de WPScan, es [necesario registrarse en su web](#) y obtener un TOKEN.

```
1 docker run -it --rm wpscanteam/wpscan --url http://192.168.22.20 --api-token 8pIlWnF2dxbgfvyQfDAUaV3T3iafo0u01K80Pr2KKRM
```

Donde **192.168.22.20** será la dirección IP de nuestro balanceador web.

1.3. Seguridad en WordPress

A continuación se muestran varias referencias relacionadas con la seguridad de WordPress.

- [Seguridad para WordPress](#). Colección de artículos de [Javier Casares](#).
- [WPdanger: Guía de seguridad para WordPress](#). Una guía en PDF de [Javier Casares](#)
- [Blog sobre administración de sistemas WordPress](#).

2 Referencias

- [WordPress](#)
- [WPScan](#)
- [Imagen WPScan en Docker Hub](#)
- [Ebook: 21 Trucos para tener tu WordPress seguro. SiteGround.](#)

3 Licencia

Esta página forma parte del curso Implantación de Aplicaciones Web de José Juan Sánchez y su contenido se distribuye bajo una licencia Creative Commons Reconocimiento-NoComercial-CompartirIgual 4.0 Internacional.