\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_ \_\_\_\_\_\_\_ \_\_\_\_\_

\ \ / / \_\_ \ / \_\_\_\_|

\ \ /\ / /| |\_\_) | (\_\_\_ \_\_\_ \_\_ \_ \_ \_\_ ®

\ \/ \/ / | \_\_\_/ \\_\_\_ \ / \_\_|/ \_` | '\_ \

\ /\ / | | \_\_\_\_) | (\_\_| (\_| | | | |

\/ \/ |\_| |\_\_\_\_\_/ \\_\_\_|\\_\_,\_|\_| |\_|

WordPress Security Scanner by the WPScan Team

Version 3.8.25

Sponsored by Automattic - https://automattic.com/

@\_WPScan\_, @ethicalhack3r, @erwan\_lr, @firefart

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[+] URL: https://challenge.mp-sec.org/ [3.228.165.80]

[+] Started: Wed Apr 24 11:48:51 2024

Interesting Finding(s):

[+] robots.txt found: https://challenge.mp-sec.org/robots.txt

| Found By: Robots Txt (Aggressive Detection)

| Confidence: 100%

[+] **XML-RPC seems to be enabled**: https://challenge.mp-sec.org/xmlrpc.php

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

| References:

| - http://codex.wordpress.org/XML-RPC\_Pingback\_API

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\_ghost\_scanner/

| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress\_xmlrpc\_dos/

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\_xmlrpc\_login/

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\_pingback\_access/

[+] **WordPress readme found**: https://challenge.mp-sec.org/readme.html

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

[+] **The external WP-Cron seems to be enabled**: https://challenge.mp-sec.org/wp-cron.php

| Found By: Direct Access (Aggressive Detection)

| Confidence: 60%

| References:

| - https://www.iplocation.net/defend-wordpress-from-ddos

| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.5.2 identified (Latest, released on 2024-04-09).

| Found By: Rss Generator (Aggressive Detection)

| - https://challenge.mp-sec.org/feed/, <generator>https://wordpress.org/?v=6.5.2</generator>

| - https://challenge.mp-sec.org/comments/feed/, <generator>https://wordpress.org/?v=6.5.2</generator>

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] elementor

| Location: https://challenge.mp-sec.org/wp-content/plugins/elementor/

| Last Updated: 2024-04-18T10:10:00.000Z

| [!] The version is out of date, the latest version is 3.21.1

|

| Found By: Urls In Homepage (Passive Detection)

|

| Version: 3.20.0 (100% confidence)

| Found By: Javascript Comment (Aggressive Detection)

| - https://challenge.mp-sec.org/wp-content/plugins/elementor/assets/js/admin-feedback.js, Match: 'elementor - v3.20.0'

| Confirmed By: Style Comment (Aggressive Detection)

| - https://challenge.mp-sec.org/wp-content/plugins/elementor/assets/css/admin.min.css, Match: 'elementor - v3.20.0'

[+] **envo-elementor-for-woocommerce**

| Location: https://challenge.mp-sec.org/wp-content/plugins/envo-elementor-for-woocommerce/

| Last Updated: 2024-04-23T11:25:00.000Z

| [!] The version is out of date, the latest version is 1.4.10

|

| Found By: Urls In Homepage (Passive Detection)

|

| Version: 1.4.7 (80% confidence)

| Found By: Readme - Stable Tag (Aggressive Detection)

| - https://challenge.mp-sec.org/wp-content/plugins/envo-elementor-for-woocommerce/readme.txt

[+] envo-extra

| Location: https://challenge.mp-sec.org/wp-content/plugins/envo-extra/

| Last Updated: 2024-04-10T11:07:00.000Z

| [!] The version is out of date, the latest version is 1.8.13

|

| Found By: Urls In Homepage (Passive Detection)

|

| Version: 1.8.12 (100% confidence)

| Found By: Query Parameter (Passive Detection)

| - https://challenge.mp-sec.org/wp-content/plugins/envo-extra/css/style.css?ver=1.8.12

| - https://challenge.mp-sec.org/wp-content/plugins/envo-extra/js/envo.js?ver=1.8.12

| Confirmed By: Readme - Stable Tag (Aggressive Detection)

| - https://challenge.mp-sec.org/wp-content/plugins/envo-extra/readme.txt

[+] woocommerce

| Location: https://challenge.mp-sec.org/wp-content/plugins/woocommerce/

| Last Updated: 2024-04-17T11:54:00.000Z

| [!] The version is out of date, the latest version is 8.8.2

|

| Found By: Urls In Homepage (Passive Detection)

| Confirmed By: Meta Generator (Passive Detection)

|

| Version: 8.7.0 (100% confidence)

| Found By: Query Parameter (Passive Detection)

| - https://challenge.mp-sec.org/wp-content/plugins/woocommerce/assets/css/woocommerce-layout.css?ver=8.7.0

| - https://challenge.mp-sec.org/wp-content/plugins/woocommerce/assets/css/woocommerce-smallscreen.css?ver=8.7.0

| - https://challenge.mp-sec.org/wp-content/plugins/woocommerce/assets/css/woocommerce.css?ver=8.7.0

| - https://challenge.mp-sec.org/wp-content/plugins/woocommerce/assets/js/frontend/add-to-cart.min.js?ver=8.7.0

| - https://challenge.mp-sec.org/wp-content/plugins/woocommerce/assets/js/frontend/woocommerce.min.js?ver=8.7.0

| - https://challenge.mp-sec.org/wp-content/plugins/woocommerce/assets/js/frontend/cart-fragments.min.js?ver=8.7.0

| Confirmed By: Meta Generator (Passive Detection)

| - https://challenge.mp-sec.org/, Match: 'WooCommerce 8.7.0'

[+] woocommerce-mercadopago

| Location: https://challenge.mp-sec.org/wp-content/plugins/woocommerce-mercadopago/

| Last Updated: 2024-04-17T16:12:00.000Z

| [!] The version is out of date, the latest version is 7.3.5

|

| Found By: Urls In Homepage (Passive Detection)

|

| Version: 7.3.1 (100% confidence)

| Found By: Readme - Stable Tag (Aggressive Detection)

| - https://challenge.mp-sec.org/wp-content/plugins/woocommerce-mercadopago/readme.txt

| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)

| - https://challenge.mp-sec.org/wp-content/plugins/woocommerce-mercadopago/readme.txt

[+] yith-woocommerce-compare

| Location: https://challenge.mp-sec.org/wp-content/plugins/yith-woocommerce-compare/

| Latest Version: 2.38.0

| Last Updated: 2024-04-15T11:54:00.000Z

|

| Found By: Urls In Homepage (Passive Detection)

|

| The version could not be determined.

[+] yith-woocommerce-wishlist

| Location: https://challenge.mp-sec.org/wp-content/plugins/yith-woocommerce-wishlist/

| Latest Version: 3.32.0

| Last Updated: 2024-04-09T09:30:00.000Z

|

| Found By: Urls In Homepage (Passive Detection)

|

| The version could not be determined.

[+] Enumerating Config Backups (via Aggressive Methods)

Checking Config Backups - Time: 00:12:11 <=> (137 / 137) 100.00% Time: 00:12:11

[i] No Config Backups Found.

[!] 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: Wed Apr 24 12:06:45 2024

[+] Requests Done: 177

[+] Cached Requests: 5

[+] Data Sent: 0 B

[+] Data Received: 376.831 KB

[+] Memory used: 28.711 MB

[+] Elapsed time: 00:17:54