
— — — — —
\\ // _ \/_|
\\ ^ / / |_) | (_ _ _ _ _ ®
\\ V V / | _/_ \/_ \/_ | _ ' _ \
 \ ^ / | | _ _) | (_ | (_ | | | |
 V V | _ | _/_ \/_ \/_ , _ | | | |

WordPress Security Scanner by the WPScan Team

Version 3.8.25

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

@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[32m[+] [0m URL: http://localhost/sitevul/ [::1]

[32m[+] [0m Started: Fri May 10 18:19:28 2024

Interesting Finding(s):

[32m[+] [0m Headers

| Interesting Entries:

| - Server: Apache/2.4.56 (Unix) OpenSSL/1.1.1t PHP/8.2.4 mod_perl/2.0.12 Perl/v5.34.1

| - X-Powered-By: PHP/8.2.4

| Found By: Headers (Passive Detection)

| Confidence: 100%

[32m[+] [0m XML-RPC seems to be enabled: <http://localhost/sitevul/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/

[32m[+] [0m WordPress readme found: <http://localhost/sitevul/readme.html>

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

[32m[+] [0m The external WP-Cron seems to be enabled: <http://localhost/sitevul/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>

[32m[+] [0m WordPress version 6.5.2 identified (Insecure, released on 2024-04-09).

| Found By: Rss Generator (Passive Detection)

| - <http://localhost/sitevul/index.php/feed/>, <generator><https://wordpress.org/?v=6.5.2></generator>

| - <http://localhost/sitevul/index.php/comments/feed/>,

<generator><https://wordpress.org/?v=6.5.2></generator>

[32m[+] [0m WordPress theme in use: twentytwentyfour

| Location: <http://localhost/sitevul/wp-content/themes/twentytwentyfour/>

| Latest Version: 1.1 (up to date)

| Last Updated: 2024-04-02T00:00:00.000Z

| Readme: <http://localhost/sitevul/wp-content/themes/twentytwentyfour/readme.txt>

| [31m[!] [0m Directory listing is enabled

| Style URL: <http://localhost/sitevul/wp-content/themes/twentytwentyfour/style.css>

| Style Name: Twenty Twenty-Four

| Style URI: <https://wordpress.org/themes/twentytwentyfour/>

| Description: Twenty Twenty-Four is designed to be flexible, versatile and applicable to any website. Its collecti...

| Author: the WordPress team

| Author URI: <https://wordpress.org>

|

| Found By: Urls In Homepage (Passive Detection)

|

| Version: 1.1 (80% confidence)

| Found By: Style (Passive Detection)

| - <http://localhost/sitevul/wp-content/themes/twentytwentyfour/style.css>, Match: 'Version: 1.1'

[32m[+] [0m Enumerating Vulnerable Plugins (via Passive Methods)

[34m[i] [0m No plugins Found.

[32m[+] [0m WPScan DB API OK

| Plan: free

| Requests Done (during the scan): 2

| Requests Remaining: 9

[32m[+] [0m Finished: Fri May 10 18:19:33 2024

[32m[+] [0m Requests Done: 34

[32m[+] [0m Cached Requests: 5

[32m[+] [0m Data Sent: 8.499 KB

[32m[+] [0m Data Received: 200.66 KB

[32m[+] [0m Memory used: 296.797 MB

[32m[+] [0m Elapsed time: 00:00:04
