┌──(root㉿kali)-[~]

└─# wpscan --api-token ZwK8LE3a2UwN86wHQn5YawFCoUHeatBYPKlE7vuLKCU --url https://zero2infynite.com/ --plugins-detection aggressive --enumerate vp

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

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

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

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

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

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

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

WordPress Security Scanner by the WPScan Team

Version 3.8.22

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

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

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

[+] URL: https://zero2infynite.com/ [104.21.49.237]

[+] Started: Wed Feb 8 13:37:00 2023

Interesting Finding(s):

[+] Headers

| Interesting Entries:

| - cf-cache-status: DYNAMIC

| - report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=yTtFxSzkWE5F3YT0ViSGsE5hZ89muEsurR2htUj8XoxmhhR%2FAMbdxyFpSw9xw77SO78WPaFqBz%2BXG00GkzRTFmJwbCXEI9NE4YXpRC%2BtVeD0HiUNLZtYQGk0vVXtWoUbR0xwtg%3D%3D"}],"group":"cf-nel","max\_age":604800}

| - nel: {"success\_fraction":0,"report\_to":"cf-nel","max\_age":604800}

| - server: cloudflare

| - cf-ray: 796678d469cd9963-FRA

| - alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

| Found By: Headers (Passive Detection)

| Confidence: 100%

[+] robots.txt found: https://zero2infynite.com/robots.txt

| Interesting Entries:

| - /wp-admin/

| - /wp-admin/admin-ajax.php

| Found By: Robots Txt (Aggressive Detection)

| Confidence: 100%

[+] XML-RPC seems to be enabled: https://zero2infynite.com/xmlrpc.php

| Found By: Link Tag (Passive Detection)

| Confidence: 100%

| Confirmed By: Direct Access (Aggressive Detection), 100% confidence

| 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://zero2infynite.com/readme.html

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

[+] The external WP-Cron seems to be enabled: https://zero2infynite.com/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 6.1.1 identified (Latest, released on 2022-11-15).

| Found By: Rss Generator (Passive Detection)

| - https://zero2infynite.com/feed/, <generator>https://wordpress.org/?v=6.1.1</generator>

| - https://zero2infynite.com/comments/feed/, <generator>https://wordpress.org/?v=6.1.1</generator>

|

| [!] 1 vulnerability identified:

|

| [!] Title: WP <= 6.1.1 - Unauthenticated Blind SSRF via DNS Rebinding

| References:

| - https://wpscan.com/vulnerability/c8814e6e-78b3-4f63-a1d3-6906a84c1f11

| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3590

| - https://blog.sonarsource.com/wordpress-core-unauthenticated-blind-ssrf/

[+] WordPress theme in use: fastor

| Location: https://zero2infynite.com/wp-content/themes/fastor/

| Style URL: https://zero2infynite.com/wp-content/themes/fastor/style.css?ver=6.1.1

| Style Name: Fastor

| Style URI: http://cleventhemes.net/fastor/woocommerce

| Description: Fastor - MultiPurpose WooCommerce Wordpress Theme...

| Author: ClevenThemes

| Author URI: https://themeforest.net/user/cleventhemes

|

| Found By: Css Style In Homepage (Passive Detection)

| Confirmed By: Css Style In 404 Page (Passive Detection)

|

| Version: 2.0.0 (80% confidence)

| Found By: Style (Passive Detection)

| - https://zero2infynite.com/wp-content/themes/fastor/style.css?ver=6.1.1, Match: 'Version: 2.0.0'