```
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ Â®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                        Version 3.8.27
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

\033[32m[+]\033[0m URL: http://localhost:8080/ [::1]
\033[32m[+]\033[0m Started: Sat Apr 5 15:56:19 2025

Interesting Finding(s):

\033[32m[+]\033[0m Headers
 | Interesting Entries:
 | - Server: Apache/2.4.57 (Debian)
 | - X-Powered-By: PHP/8.2.17
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

\033[32m[+]\033[0m XML-RPC seems to be enabled: http://localhost:8080/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/

\033[32m[+]\033[0m WordPress readme found: http://localhost:8080/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

\033[32m[+]\033[0m The external WP-Cron seems to be enabled: http://localhost:8080/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

\033[32m[+]\033[0m WordPress version 6.4.3 identified (Insecure, released on 2024-01-30).
 | Found By: Rss Generator (Passive Detection)
 | - http://localhost:8080/?feed=rss2, <generator>https://wordpress.org/?v=6.4.3</generator>
 | - http://localhost:8080/?feed=comments-rss2, <generator>https://wordpress.org/?v=6.4.3</ge
nerator>
 |
 | \033[31m[!]\033[0m 4 vulnerabilities identified:
 |
 | \033[31m[!]\033[0m Title: WP < 6.5.2 - Unauthenticated Stored XSS
 | Fixed in: 6.4.4
 | References:
 | - https://wpscan.com/vulnerability/1a5c5df1-57ee-4190-a336-b0266962078f
 | - https://wordpress.org/news/2024/04/wordpress-6-5-2-maintenance-and-security-release/
 |
 | \033[31m[!]\033[0m Title: WordPress < 6.5.5 - Contributor+ Stored XSS in HTML API
 | Fixed in: 6.4.5

```
 |      References:
 |       - https://wpscan.com/vulnerability/2c63f136-4c1f-4093-9a8c-5e51f19eae28
 |       - https://wpscan.com/news/2024/06/wordpress-6-5-5/
 |
 | \033[31m[!]\033[0m Title: WordPress < 6.5.5 - Contributor+ Stored XSS in Template-Part Bloc
k
 |      Fixed in: 6.4.5
 |      References:
 |       - https://wpscan.com/vulnerability/7c448f6d-4531-4757-bff0-be9e3220bbbb
 |       - https://wpscan.com/news/2024/06/wordpress-6-5-5/
 |
 | \033[31m[!]\033[0m Title: WordPress < 6.5.5 - Contributor+ Path Traversal in Template-Part
Block
 |      Fixed in: 6.4.5
 |      References:
 |       - https://wpscan.com/vulnerability/36232787-754a-4234-83d6-6ded5e80251c
 |       - https://wpscan.com/news/2024/06/wordpress-6-5-5/

\033[32m[+]\033[0m WordPress theme in use: twentytwentyfour
 | Location: http://localhost:8080/wp-content/themes/twentytwentyfour/
 | Last Updated: 2024-11-13T00:00:00.000Z
 | Readme: http://localhost:8080/wp-content/themes/twentytwentyfour/readme.txt
 | \033[33m[!]\033[0m The version is out of date, the latest version is 1.3
 | Style URL: http://localhost:8080/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: 1.0 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://localhost:8080/wp-content/themes/twentytwentyfour/style.css, Match: 'Version: 1.0
'

\033[32m[+]\033[0m Enumerating All Plugins (via Aggressive Methods)

 Checking Known Locations -: |================================================================
==========|
\033[32m[+]\033[0m Checking Plugin Versions (via Passive and Aggressive Methods)

\033[34m[i]\033[0m Plugin(s) Identified:

\033[32m[+]\033[0m really-simple-ssl
 | Location: http://localhost:8080/wp-content/plugins/really-simple-ssl/
 | Last Updated: 2025-04-02T05:42:00.000Z
 | Readme: http://localhost:8080/wp-content/plugins/really-simple-ssl/readme.txt
 | \033[33m[!]\033[0m The version is out of date, the latest version is 9.3.3
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://localhost:8080/wp-content/plugins/really-simple-ssl/, status: 200
 |
 | \033[31m[!]\033[0m 2 vulnerabilities identified:
 |
 | \033[31m[!]\033[0m Title: Really Simple Security (Free, Pro, and Pro Multisite) 9.0.0 - 9.1
.1.1 - Authentication Bypass
 |      Fixed in: 9.1.2
 |      References:
 |       - https://wpscan.com/vulnerability/8e1f4374-2e41-4c27-80d4-db172015c6be
 |       - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-10924
```

```
 |      - https://www.wordfence.com/threat-intel/vulnerabilities/id/7d5d05ad-1a7a-43d2-bbbf-59
7e975446be
 |
 | \033[31m[!]\033[0m Title: Really Simple SSL < 9.2.0 - Cross-Site Request Forgery
 |     Fixed in: 9.2.0
 |     References:
 |      - https://wpscan.com/vulnerability/e730c033-3711-42b8-81f1-898765547c5b
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-24623
 |      - https://www.wordfence.com/threat-intel/vulnerabilities/id/9a322b84-93cf-4793-956f-c2
e53574041c
 |
 | Version: 9.1.1 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://localhost:8080/wp-content/plugins/really-simple-ssl/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://localhost:8080/wp-content/plugins/really-simple-ssl/readme.txt

\033[32m[+]\033[0m WPScan DB API OK
 | Plan: free
 | Requests Done (during the scan): 0
 | Requests Remaining: 22

\033[32m[+]\033[0m Finished: Sat Apr  5 15:57:04 2025
\033[32m[+]\033[0m Requests Done: 109861
\033[32m[+]\033[0m Cached Requests: 43
\033[32m[+]\033[0m Data Sent: 29.919 MB
\033[32m[+]\033[0m Data Received: 14.69 MB
\033[32m[+]\033[0m Memory used: 460.074 MB
\033[32m[+]\033[0m Elapsed time: 00:00:45
```