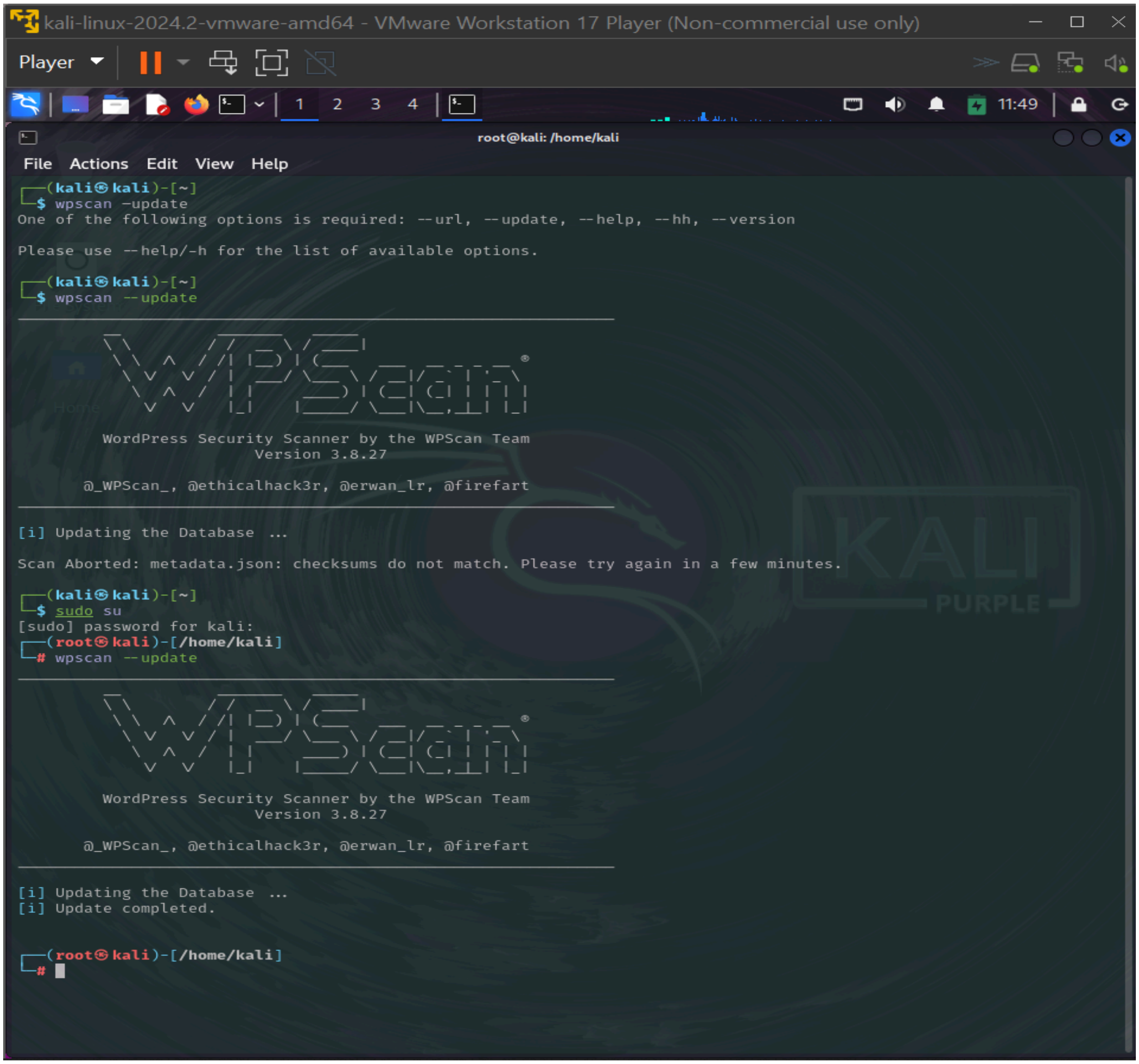
AUTOMATE WORDPRESS SCANNING WITH WPSCAN

Tools : KALI LINUX
Site ; WORD PRESS

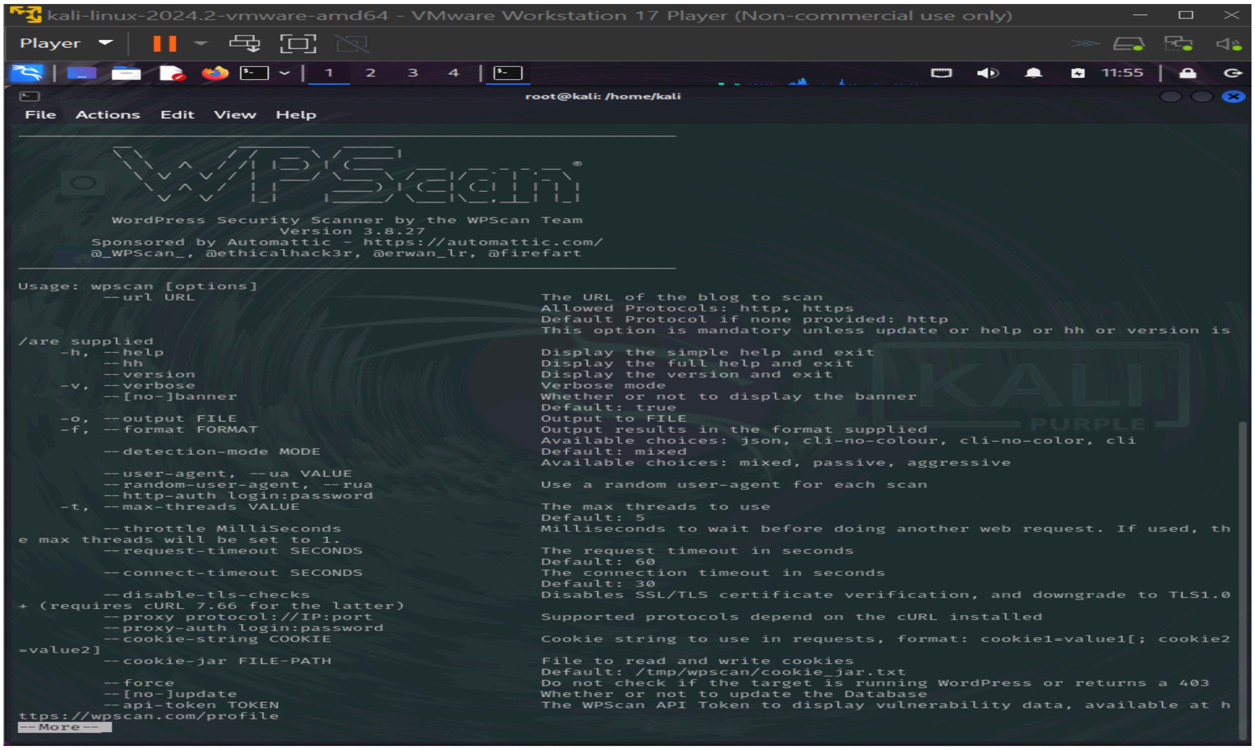
WPScan is a popular WordPress security scanner used for identifying vulnerabilities in WordPress websites. It's commonly used by security professionals and developers to secure their WordPress installations.

Input fro kali :

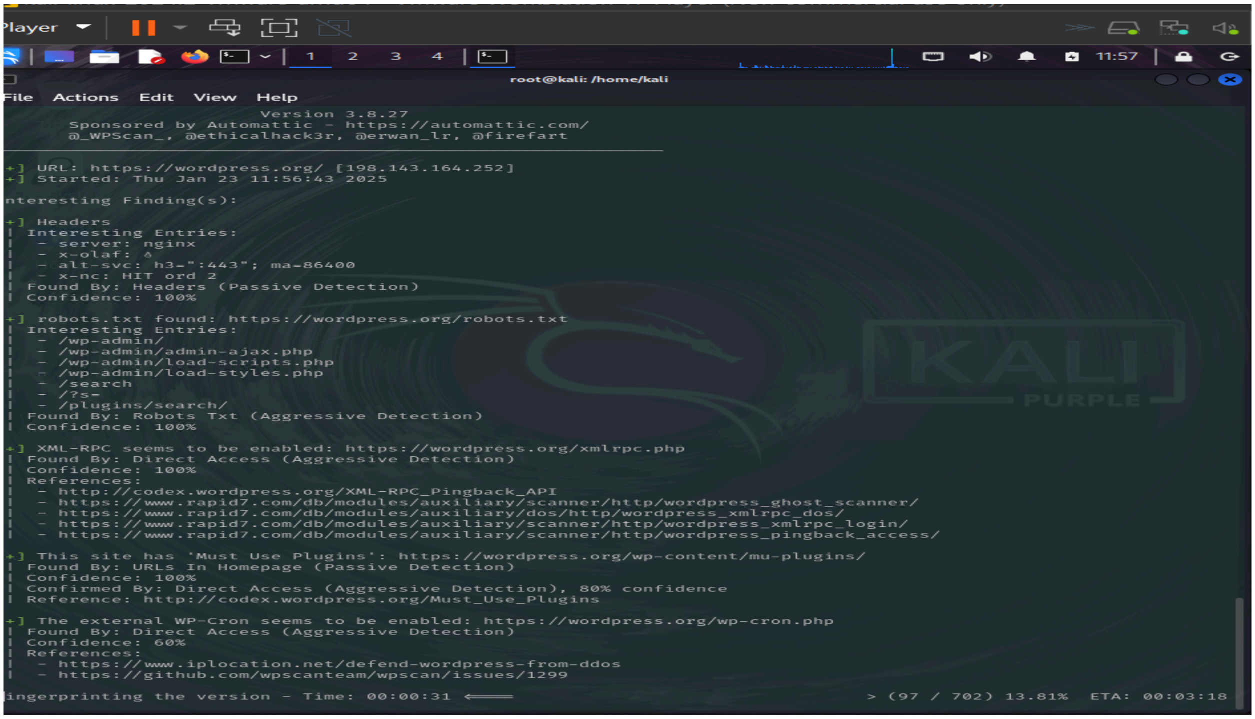


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1
2
3
4
11:49
root@kali: /home/kali
File
Actions
Edit
View
Help

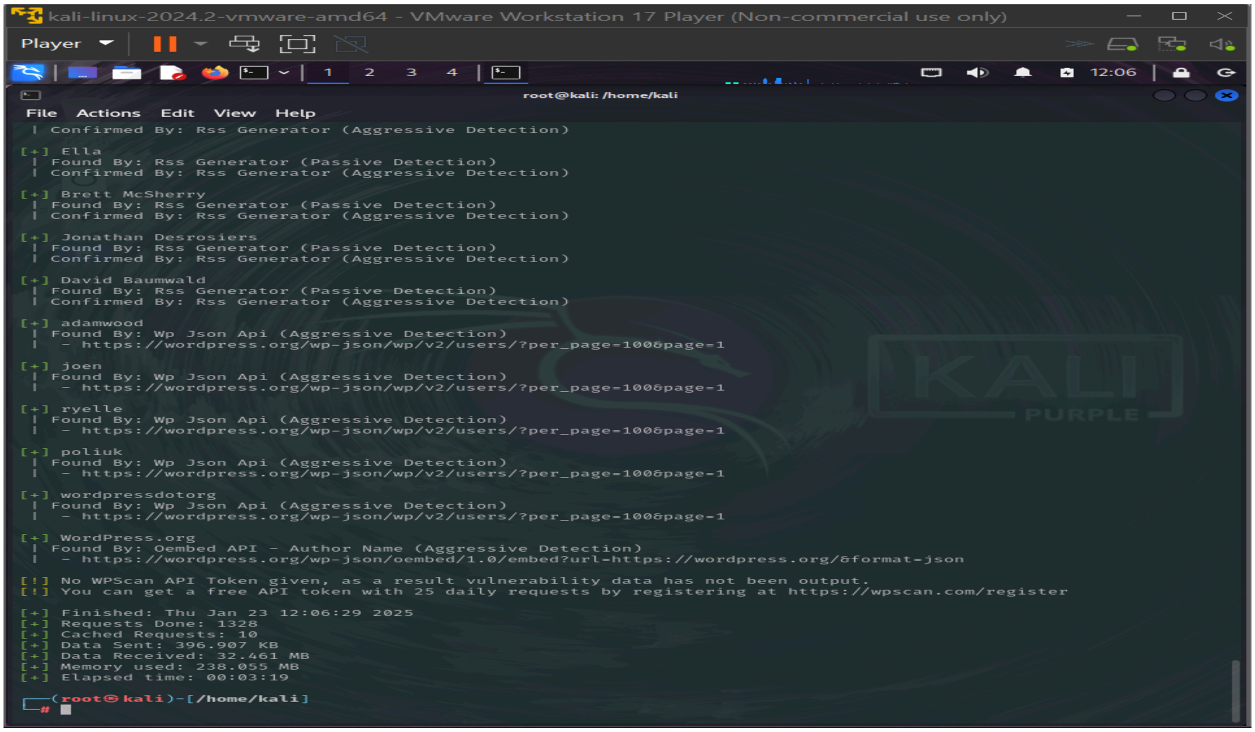
```
┌──(kali㉿kali)-[~]
└─$ wpscan –update
One of the following options is required: --url, --update, --help, --hh, --version

Please use --help/-h for the list of available options.

┌──(kali㉿kali)-[~]
└─$ wpscan --update
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.27

       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] Updating the Database ...

Scan Aborted: metadata.json: checksums do not match. Please try again in a few minutes.

┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# wpscan --update
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.27

       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] Updating the Database ...
[i] Update completed.


┌──(root㉿kali)-[/home/kali]
└─#
```


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1
2
3
4
11:55
root@kali: /home/kali
File
Actions
Edit
View
Help

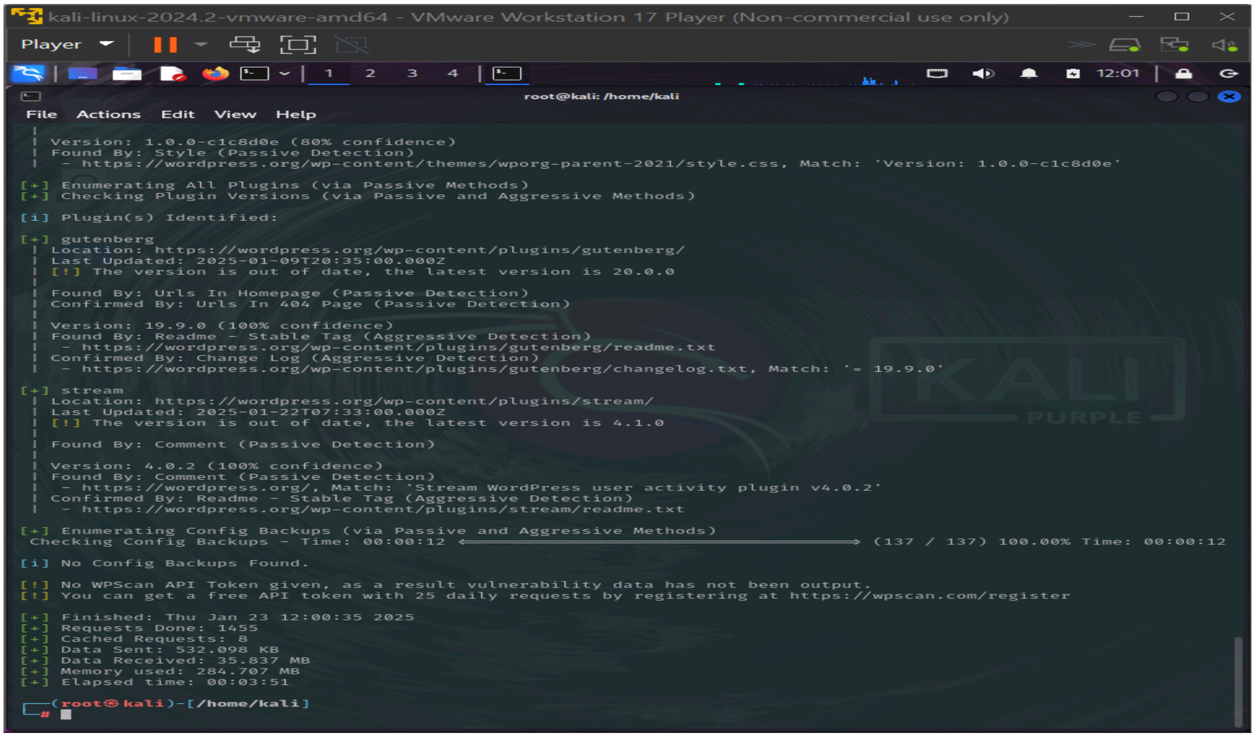
```
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| |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

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

Usage: wpscan [options]
        --url URL                                   The URL of the blog to scan
                                                    Allowed Protocols: http, https
                                                    Default Protocol if none provided: http
                                                    This option is mandatory unless update or help or hh or version is
/are supplied
    -h, --help                                      Display the simple help and exit
        --hh                                        Display the full help and exit
        --version                                   Display the version and exit
    -v, --verbose                                   Verbose mode
        --[no-]banner                               Whether or not to display the banner
                                                    Default: true
    -o, --output FILE                               Output to FILE
    -f, --format FORMAT                             Output results in the format supplied
                                                    Available choices: json, cli-no-colour, cli-no-color, cli
        --detection-mode MODE                       Default: mixed
                                                    Available choices: mixed, passive, aggressive
        --user-agent, --ua VALUE
        --random-user-agent, --rua                  Use a random user-agent for each scan
        --http-auth login:password
    -t, --max-threads VALUE                         The max threads to use
                                                    Default: 5
        --throttle MilliSeconds                     Milliseconds to wait before doing another web request. If used, th
e max threads will be set to 1.
        --request-timeout SECONDS                   The request timeout in seconds
                                                    Default: 60
        --connect-timeout SECONDS                   The connection timeout in seconds
                                                    Default: 30
        --disable-tls-checks                        Disables SSL/TLS certificate verification, and downgrade to TLS1.0
+ (requires cURL 7.66 for the latter)
        --proxy protocol://IP:port                  Supported protocols depend on the cURL installed
        --proxy-auth login:password
        --cookie-string COOKIE                      Cookie string to use in requests, format: cookie1=value1[; cookie2
=value2]
        --cookie-jar FILE-PATH                      File to read and write cookies
                                                    Default: /tmp/wpscan/cookie_jar.txt
        --force                                     Do not check if the target is running WordPress or returns a 403
        --[no-]update                               Whether or not to update the Database
        --api-token TOKEN                           The WPScan API Token to display vulnerability data, available at h
ttps://wpscan.com/profile
--More--
```



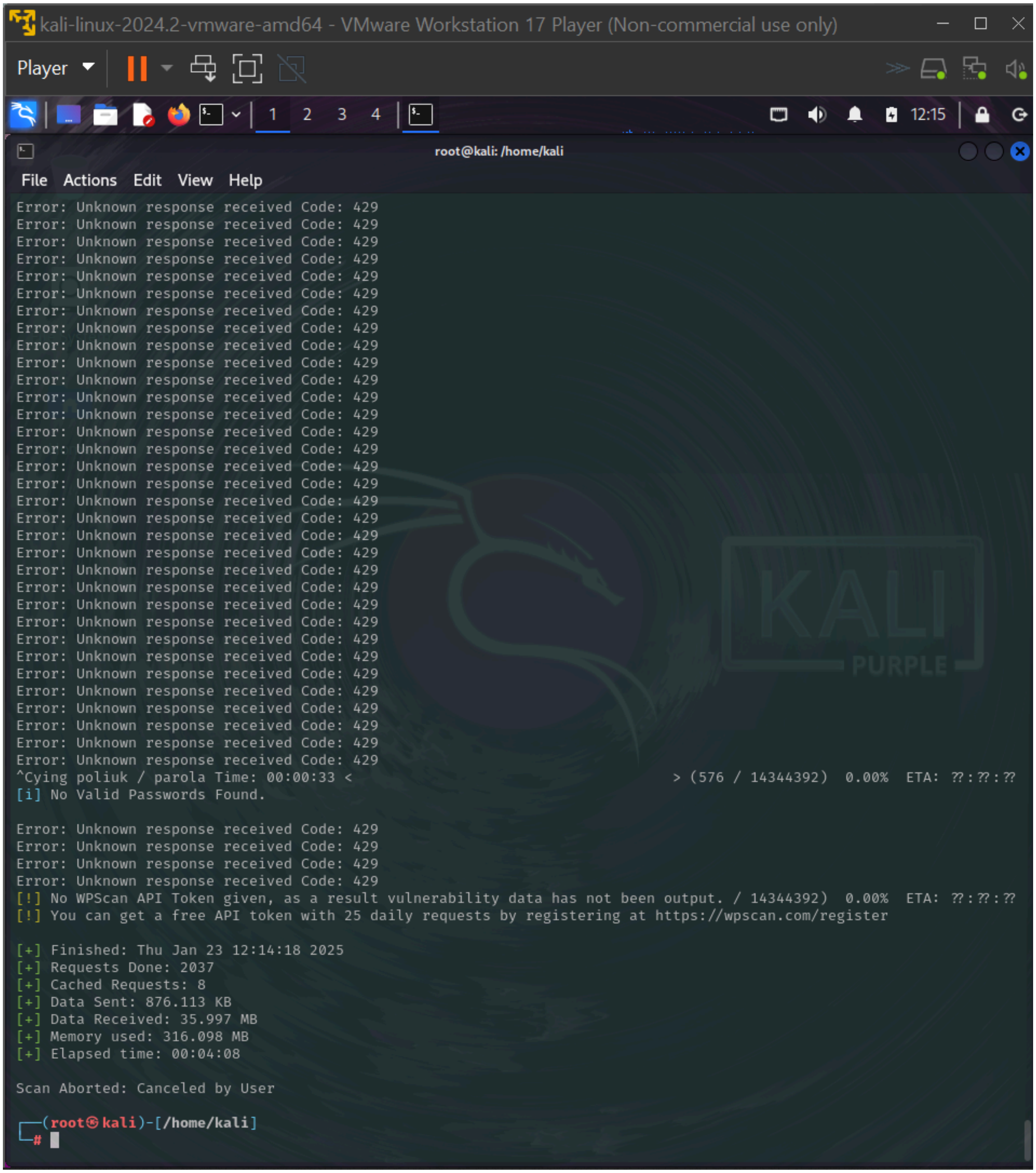
```
                         Version 3.8.27
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

+] URL: https://wordpress.org/ [198.143.164.252]
+] Started: Thu Jan 23 11:56:43 2025

nteresting Finding(s):

+] Headers
| Interesting Entries:
|  - server: nginx
|  - x-olaf: ⛄
|  - alt-svc: h3=":443"; ma=86400
|  - x-nc: HIT ord 2
| Found By: Headers (Passive Detection)
| Confidence: 100%

+] robots.txt found: https://wordpress.org/robots.txt
| Interesting Entries:
|  - /wp-admin/
|  - /wp-admin/admin-ajax.php
|  - /wp-admin/load-scripts.php
|  - /wp-admin/load-styles.php
|  - /search
|  - /?s=
|  - /plugins/search/
| Found By: Robots Txt (Aggressive Detection)
| Confidence: 100%

+] XML-RPC seems to be enabled: https://wordpress.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/

+] This site has 'Must Use Plugins': https://wordpress.org/wp-content/mu-plugins/
| Found By: URLs In Homepage (Passive Detection)
| Confidence: 100%
| Confirmed By: Direct Access (Aggressive Detection), 80% confidence
| Reference: http://codex.wordpress.org/Must_Use_Plugins

+] The external WP-Cron seems to be enabled: https://wordpress.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

ingerprinting the version - Time: 00:00:31 <====                        > (97 / 702) 13.81%  ETA: 00:03:18
```


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1
2
3
4
12:06
root@kali: /home/kali
File
Actions
Edit
View
Help

```
 | Confirmed By: Rss Generator (Aggressive Detection)

[+] Ella
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By: Rss Generator (Aggressive Detection)

[+] Brett McSherry
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By: Rss Generator (Aggressive Detection)

[+] Jonathan Desrosiers
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By: Rss Generator (Aggressive Detection)

[+] David Baumwald
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By: Rss Generator (Aggressive Detection)

[+] adamwood
 | Found By: Wp Json Api (Aggressive Detection)
 |  - https://wordpress.org/wp-json/wp/v2/users/?per_page=100&page=1

[+] joen
 | Found By: Wp Json Api (Aggressive Detection)
 |  - https://wordpress.org/wp-json/wp/v2/users/?per_page=100&page=1

[+] ryelle
 | Found By: Wp Json Api (Aggressive Detection)
 |  - https://wordpress.org/wp-json/wp/v2/users/?per_page=100&page=1

[+] poliuk
 | Found By: Wp Json Api (Aggressive Detection)
 |  - https://wordpress.org/wp-json/wp/v2/users/?per_page=100&page=1

[+] wordpressdotorg
 | Found By: Wp Json Api (Aggressive Detection)
 |  - https://wordpress.org/wp-json/wp/v2/users/?per_page=100&page=1

[+] WordPress.org
 | Found By: Oembed API - Author Name (Aggressive Detection)
 |  - https://wordpress.org/wp-json/oembed/1.0/embed?url=https://wordpress.org/&format=json

[!] 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: Thu Jan 23 12:06:29 2025
[+] Requests Done: 1328
[+] Cached Requests: 10
[+] Data Sent: 396.907 KB
[+] Data Received: 32.461 MB
[+] Memory used: 238.055 MB
[+] Elapsed time: 00:03:19

┌──(root㉿kali)-[/home/kali]
└─#
```


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1
2
3
4
12:01
root@kali: /home/kali
File
Actions
Edit
View
Help

```
 |
 | Version: 1.0.0-c1c8d0e (80% confidence)
 | Found By: Style (Passive Detection)
 |  - https://wordpress.org/wp-content/themes/wporg-parent-2021/style.css, Match: 'Version: 1.0.0-c1c8d0e'

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

[i] Plugin(s) Identified:

[+] gutenberg
 | Location: https://wordpress.org/wp-content/plugins/gutenberg/
 | Last Updated: 2025-01-09T20:35:00.000Z
 | [!] The version is out of date, the latest version is 20.0.0
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | Version: 19.9.0 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - https://wordpress.org/wp-content/plugins/gutenberg/readme.txt
 | Confirmed By: Change Log (Aggressive Detection)
 |  - https://wordpress.org/wp-content/plugins/gutenberg/changelog.txt, Match: '= 19.9.0'

[+] stream
 | Location: https://wordpress.org/wp-content/plugins/stream/
 | Last Updated: 2025-01-22T07:33:00.000Z
 | [!] The version is out of date, the latest version is 4.1.0
 |
 | Found By: Comment (Passive Detection)
 |
 | Version: 4.0.2 (100% confidence)
 | Found By: Comment (Passive Detection)
 |  - https://wordpress.org/, Match: 'Stream WordPress user activity plugin v4.0.2'
 | Confirmed By: Readme - Stable Tag (Aggressive Detection)
 |  - https://wordpress.org/wp-content/plugins/stream/readme.txt

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:12 <=======================================> (137 / 137) 100.00% Time: 00:00:12

[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: Thu Jan 23 12:00:35 2025
[+] Requests Done: 1455
[+] Cached Requests: 8
[+] Data Sent: 532.098 KB
[+] Data Received: 35.837 MB
[+] Memory used: 284.707 MB
[+] Elapsed time: 00:03:51

┌──(root㉿kali)-[/home/kali]
└─#
```


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1
2
3
4
12:15
root@kali: /home/kali
File
Actions
Edit
View
Help

```
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
^Cying poliuk / parola Time: 00:00:33 <                                    > (576 / 14344392)  0.00%  ETA: ??:??:??
[i] No Valid Passwords Found.

Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
Error: Unknown response received Code: 429
[!] No WPScan API Token given, as a result vulnerability data has not been output. / 14344392)  0.00%  ETA: ??:??:??
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Thu Jan 23 12:14:18 2025
[+] Requests Done: 2037
[+] Cached Requests: 8
[+] Data Sent: 876.113 KB
[+] Data Received: 35.997 MB
[+] Memory used: 316.098 MB
[+] Elapsed time: 00:04:08

Scan Aborted: Canceled by User

┌──(root㉿kali)-[/home/kali]
└─# 
```

Here we would be using WPSCAN to automatically scan WORDPRESS sites for vulnerabilities.

Here's a more compact version of the instructions:

WPScan Quick Guide

Prerequisites

- Use responsibly: Only scan websites with permission from the owner.
- WPScan comes pre-installed in Kali Linux.

1. Update WPScan Database

```
wpscan --update
```

2. View Help

```
wpscan -h | more
```

- Navigate pages with the **Space** key.
- Exit with **Ctrl + C**.

3. Quick Scan

```
wpscan --url https://wordpress.org/ --rua
--ignore-main-redirect
```

- **--url**: Target URL.
- **--rua**: Use random user-agent for each scan.
- **--ignore-main-redirect**: Ignore URL redirects.

Output: Provides basic information about plugins, WordPress version, and warnings.

4. Scan for Vulnerable Themes

```
wpscan --url https://wordpress.org/ --rua
--ignore-main-redirect --enumerate vt
```

Save Results to File:

```
wpscan --url https://wordpress.org/ --rua
--ignore-main-redirect --enumerate vt -o report.txt
```

5. Enumerate Users

```
wpscan --url https://wordpress.org/ --rua
--ignore-main-redirect --enumerate u
```

6. Password Brute Forcing

```
wpscan --url https://wordpress.org/ --rua
--ignore-main-redirect -P
/usr/share/wordlists/rockyou.txt -U otto42
```

-P: Path to the wordlist (e.g., `rockyou.txt`).

- **-U**: Target username(s).

Stop Process: Press **Ctrl + C**.