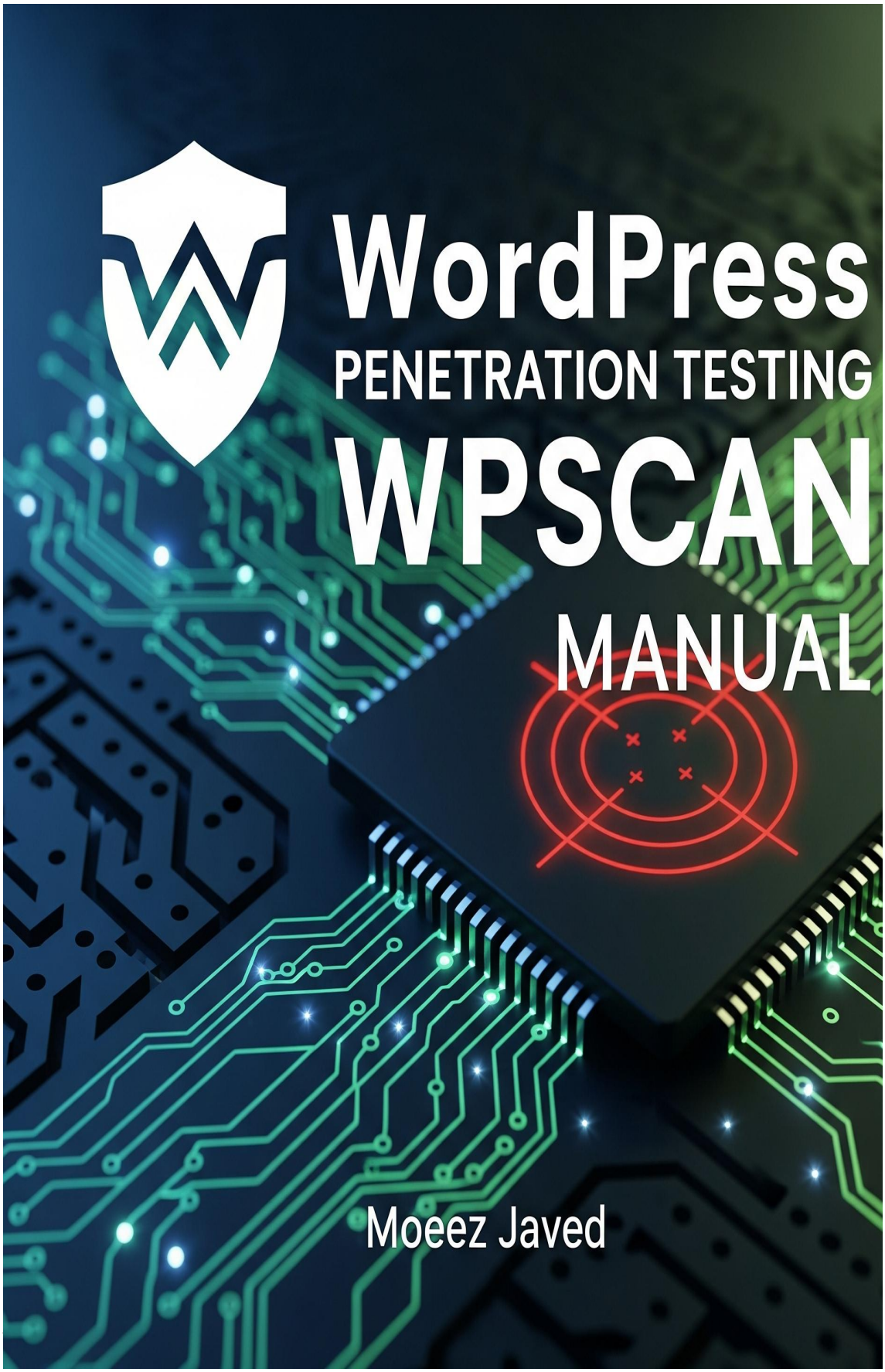
Made by Moeez Javed



Wordpress Penetration Testing WPScan Manual

Audience: Students learning WordPress security, vulnerability discovery, and defensive remediation.

Purpose: Teach what WPScan is, why it matters for defenders, how to install and run it safely in a lab, how to interpret results, and which remediation steps to take. This manual focuses on *responsible*, *authorized* use only — do **not** scan third-party or production sites without explicit written permission.

1. Introduction — What WPScan is and why it matters

WPScan is a command-line WordPress vulnerability scanner that discovers configuration issues, exposed files, plugin/theme versions, and known vulnerabilities by matching discovered versions and components against a vulnerability database. For defenders, WPScan helps you find the same signals attackers look for so you can patch, remove, or harden affected components before they are abused.

Why teach WPScan to students? - Teaches how to perform authorized vulnerability discovery and responsible disclosure. - Shows how attackers enumerate WordPress sites so defenders can close detection gaps. - Produces concrete findings (outdated plugins/themes, leaked backups) that map directly to remediation actions. cite turn0search0 turn0search5

2. Legal & ethical rules (READ FIRST)

- **Authorization only.** Only scan websites you own or have explicit written permission to test. Scanning third-party or production sites without permission can be illegal.

- **Use isolated lab targets** for student labs. Provide instructor-controlled WordPress images for exercises.

- **Be gentle by default.** Use passive/mixed detection modes and throttling to avoid harming a target.

- **Document activity.** Keep scan logs, dates, and authorization documentation.

3. Installation (Kali Linux and alternatives)

On Kali Linux (recommended for students):

sudo apt update **&&** sudo apt install wpscan -y

(Kali packages WPScan and its dependencies). cite turn0search0

Alternative installs (if you prefer): - Ruby gem (official distribution):

sudo gem install wpscan

- Docker image (isolated runtime):

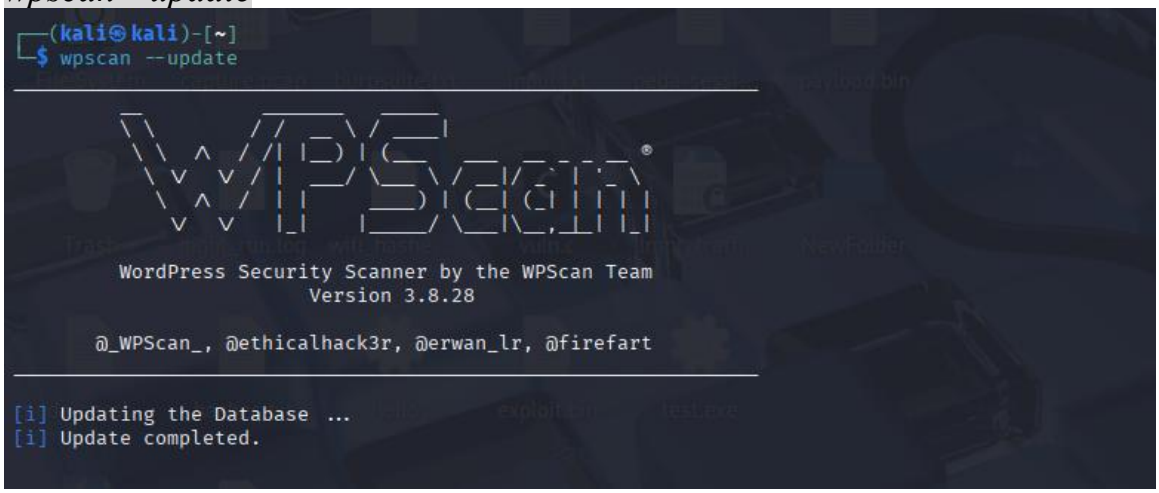
docker pull wpscanteam/wpscan

If you use a package manager, prefer the distro package for student labs; for development or the latest features you may use the gem or Docker. cite turn0search15 turn0search3

4. WPScan basics — update & API token

Update WPScan metadata (local database)

wpscan --update



Always run --update before scanning to use the latest vulnerability metadata. cite turn0search17

WPVulnDB API token - WPScan can use the WPVulnDB (wpscan.com) API to provide richer vulnerability details. Register at https://wpscan.com/api/ to obtain a free API token for educational use and place it in your commands as --api-token <TOKEN> or set the environment variable WPVULNDB_API_TOKEN for automation. Using the token enables verified vulnerability lookups; without it WPScan will still detect versions but cannot confirm vulnerability records. cite turn0search1 turn0search4

Example (temporary env var):

export WPVULNDB_API_TOKEN="your_token_here"

Or pass per-scan:

wpscan --url https://lab.example --api-token your_token_here

5. Safe, step-by-step scanning workflow (lab only)

Below are safe commands students will use in the lab. Replace http://lab.example with your instructor-provided lab WordPress URL or local IP.

5.1 Quick info / help

wpscan --help
wpscan --version

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

        WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

Current Version: 3.8.28
Last DB Update: 2025-08-28
```

5.2 Basic scan (non-aggressive)

wpscan --url http://lab.example --detection-mode passive --throttle 500 --random-user-agent --output lab-scan.txt --format cli

- --detection-mode passive minimizes requests and relies on public metadata.
- --throttle 500 adds 500 ms delay between requests to be polite.
- --random-user-agent helps avoid simple blocking rules.
- --output and --format store results for review.

5.3 Enumerate plugins, themes, users (read-only enumeration)

 # enumerate user accounts, active plugins, all plugins and themes
wpscan --url http://lab.example --enumerate u,ap,at --api-token YOUR_TOKEN --format json --output lab-enum.json

Common --enumerate options include: u (users), ap (all plugins), vp (vulnerable plugins only), p (popular plugins), at (all themes), vt (vulnerable themes), cb (config backups), dbe (database exports). Use them responsibly. cite turn0search2 turn1search5

5.4 Plugin detection mode (when you need extra coverage)

 # default is mixed; override with plugins-detection
wpscan --url http://lab.example --plugins-detection mixed --enumerate ap --api-token YOUR_TOKEN

Modes: passive, mixed (default), aggressive. Aggressive yields more results but is louder and may stress the server — use only on lab targets. cite turn1search2

5.5 Export JSON for programmatic analysis

wpscan --url http://lab.example --enumerate ap,at,u --api-token YOUR_TOKEN --format json --output results.json

This JSON can feed into scripts or a SIEM for triage.

6. Interpreting results & remediation guidance

When WPScan reports a vulnerable plugin or theme:

1. **Validate**: confirm the site actually uses the reported component and version (false positives happen).
2. **Patch**: update the plugin/theme/core to the latest secure version.
3. **Remove or disable**: if not needed, remove the plugin/theme.
4. **Harden**: limit administrative access, enforce strong passwords and 2FA, deploy a Web Application Firewall (WAF), and disable unnecessary endpoints (XML-RPC, REST endpoints) if not used.
5. **Test & monitor**: re-scan and add the site to regular vulnerability scans.

Common actionable items (prioritize by exposure): - Outdated core ⇒ **patch immediately**.
- Vulnerable plugin used on public site ⇒ remove or update; if no patch exists, block the vulnerable endpoints via WAF.
- Exposed backups/config files found (e.g., wp-config.php backups) ⇒ remove them from webroot and rotate secrets.

Step-by-Step Usage

Step 1: Verify Installation (Kali Linux)

wpscan --version

Check if WPScan is installed.

If not installed:

sudo apt update
sudo apt install wpscan -y

```
┌──(kali㉿kali)-[~]
└─$ sudo apt update
sudo apt install wpscan -y
[sudo] password for kali:
Hit:1 https://download.docker.com/linux/debian bookworm InRelease
Hit:2 http://http.kali.org/kali kali-rolling InRelease
Ign:3 https://apt.cutter.re/repo jammy InRelease
Ign:3 https://apt.cutter.re/repo jammy InRelease
Ign:3 https://apt.cutter.re/repo jammy InRelease
Err:3 https://apt.cutter.re/repo jammy InRelease
  Could not resolve 'apt.cutter.re'
25 packages can be upgraded. Run 'apt list --upgradable' to see them.
Warning: Failed to fetch https://apt.cutter.re/repo/dists/jammy/InRelease  Could not resolve 'apt.cutter.re'
Warning: Some index files failed to download. They have been ignored, or old ones used instead.
wpscan is already the newest version (3.8.28-0kali1).
The following packages were automatically installed and are no longer required:
  libdbi1t64       libivykis0t64       libsframe1         libvpx9                    python3-kubernetes                 python3-requests-oauthlib
  libgdata-common  libqt5ct-common1.8  libsigsegv2        linux-image-6.12.25-amd64  python3-packaging-whl              python3-responses
  libgdata22       librdkafka1         libsoup-2.4-1      python3-cachetools         python3-pyinstaller-hooks-contrib  python3-rsa
  libhdf4-0-alt    libriemann-client0  libsoup2.4-common  python3-google-auth        python3-pyu2f                      python3-wheel-whl
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 25
```

Step 2: Basic Scan (Red Team)

wpscan --url http://targetwordpress.local/

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

        WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

Scan Aborted: The target is responding with a 403, this might be due to a WAF. Please re-try with --random-user-agent
```

Firewall block it than we are using random user agent

wpscan --url https://rivalwears.com/ --random-user-agent

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

        WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: https:[redacted][106.0.62.94]
[+] Started: Thu Aug 28 03:31:27 2025

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache
 |  - X-Powered-By: PHP/7.4.33
 | Found By: Headers (Passive Detection)
```

```
[+] wp-smushit
 | Location: [redacted]wp-content/plugins/wp-smushit/
 | Last Updated: 2025-06-25T13:07:00.000Z
 | [!] The version is out of date, the latest version is 3.20.0
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | Version: 3.16.6 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - [redacted]wp-content/plugins/wp-smushit/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - https://rivalwears.com/wp-content/plugins/wp-smushit/readme.txt

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:02:35 <==========================================================> (137 / 137) 100.00% Time: 00:02:35

[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 Aug 28 03:35:21 2025
[+] Requests Done: 191
[+] Cached Requests: 7
[+] Data Sent: 67.502 KB
[+] Data Received: 888.909 KB
[+] Memory used: 272.008 MB
[+] Elapsed time: 00:03:53
```

This scans the target WordPress site to gather basic information.

Blue Team Tip: Monitor web server logs for unusual repeated requests.

Step 3: Enumerate Users (Red Team)

wpscan --url http://targetwordpress.local/ -e u

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

        WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: [redacted]
[+] Started: Thu Aug 28 03:53:37 2025
```

This attempts to enumerate WordPress usernames.

Blue Team Tip: Watch for author queries in access logs (/index.php?author=1).

Step 4: Enumerate Plugins (Red Team)

wpscan --url http://targetwordpress.local/ -e p

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

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: [redacted]
[+] Started: Thu Aug 28 03:52:21 2025

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
```

This checks installed plugins against the vulnerability database.

Blue Team Tip: Ensure all plugins are up to date and disable unused ones.

Step 5: Enumerate Themes (Red Team)

wpscan --url http://targetwordpress.local/ -e t

```
┌──(kali㉿kali)-[~]
└─$ wpscan --url [redacted] -e t
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: [redacted] [185.205.246.148]
[+] Started: Thu Aug 28 03:48:00 2025

Interesting Finding(s):
```

This attempts to enumerate installed themes.

Blue Team Tip: Remove unused themes and patch vulnerabilities quickly.

Step 6: Brute Force Login (Red Team - Lab Only)

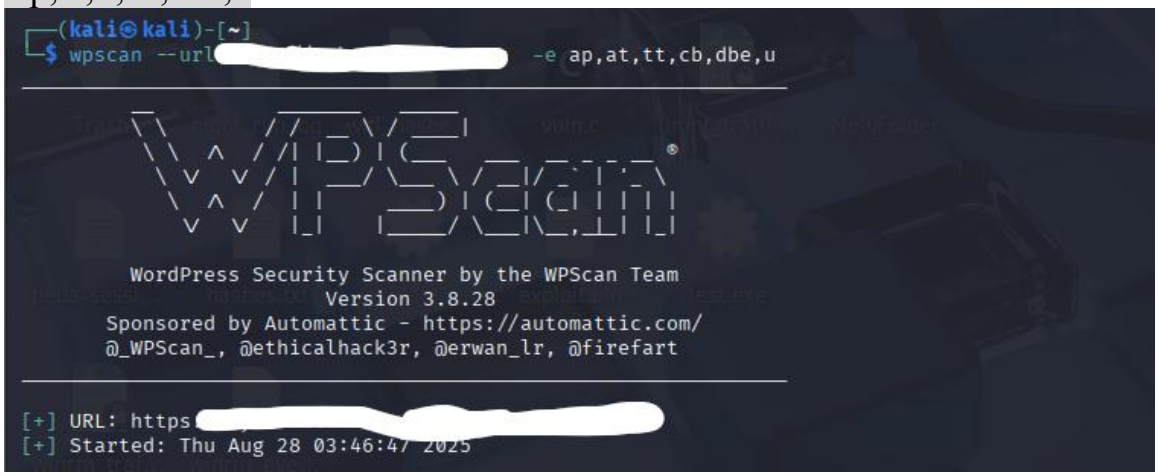
wpscan --url http://targetwordpress.local/ -U users.txt -P passwords.txt

This attempts a brute force login using a user and password list.

Blue Team Tip: - Enable account lockout for failed login attempts. - Use multi-factor authentication. - Monitor WordPress login attempts.

Step 7: Full Vulnerability Scan (Red Team)

wpscan --url http://targetwordpress.local/ --api-token <Your_API_Token> -e ap,at,tt,cb,dbe,u



Where: - ap = all plugins - at = all themes - tt = timthumbs - cb = config backups - dbe = database exports - u = users

Blue Team Tip: Harden WordPress with security plugins like Wordfence, Sucuri, or fail2ban.

Step 8: Defensive Monitoring (Blue Team)

tail -f /var/log/apache2/access.log | grep wpscan
tail -f /var/log/nginx/access.log | grep wpscan

This helps detect WPScan probing attempts in real-time

8. Practical tips & safety knobs

- Start with --detection-mode passive and --throttle to avoid service impact.

- Use --random-user-agent and --stealthy if you want to simulate low-noise reconnaissance — still, only on lab targets.

- Use --output (CLI/json) for record keeping and evidence.

- If a WAF blocks scans, coordinate with the instructor — do not try to bypass protections.

9. What WPScan does not do for you

- WPScan identifies likely vulnerable components by matching versions and known weakness records — it does **not** by itself exploit vulnerabilities or prove a site is compromiseable. Manual verification and patching are required.

- Password-guessing/brute-force features exist in WPScan, but those are **offensive** actions that must only be performed in a controlled red-team exercise with explicit authorization. This manual does **not** cover brute-force commands. cite turn0search2

10. Resources & references

- WPScan (official): installation, docs & API.
  cite turn0search3 turn0search4

- Kali tools page (package install). cite turn0search0

- WPScan CLI cheat sheet (enumeration flags & examples).
  cite turn0search2

11. Appendix — Quick command cheatsheet (lab-friendly)

```
# install on Kali
sudo apt update && sudo apt install wpscan -y
```

```
┌──(kali㉿kali)-[~]
└─$ sudo apt update
sudo apt install wpscan -y
[sudo] password for kali:
Hit:1 https://download.docker.com/linux/debian bookworm InRelease
Hit:2 http://http.kali.org/kali kali-rolling InRelease
Ign:3 https://apt.cutter.re/repo jammy InRelease
Ign:3 https://apt.cutter.re/repo jammy InRelease
Ign:3 https://apt.cutter.re/repo jammy InRelease
Err:3 https://apt.cutter.re/repo jammy InRelease
  Could not resolve 'apt.cutter.re'
25 packages can be upgraded. Run 'apt list --upgradable' to see them.
Warning: Failed to fetch https://apt.cutter.re/repo/dists/jammy/InRelease  Could not resolve 'apt.cutter.re'
Warning: Some index files failed to download. They have been ignored, or old ones used instead.
wpscan is already the newest version (3.8.28-0kali1).
The following packages were automatically installed and are no longer required:
  libdbi1t64       libivykis0t64       libsframe1         libvpx9                    python3-kubernetes                 python3-requests-oauthlib
  libgdata-common  libqt5ct-common1.8  libsigsegv2        linux-image-6.12.25-amd64  python3-packaging-whl              python3-responses
  libgdata22       librdkafka1         libsoup-2.4-1      python3-cachetools         python3-pyinstaller-hooks-contrib  python3-rsa
  libhdf4-0-alt    libriemann-client0  libsoup2.4-common  python3-google-auth        python3-pyu2f                      python3-wheel-whl
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 25
```

 # update local WPScan metadata

wpscan --update

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

        WordPress Security Scanner by the WPScan Team
                         Version 3.8.28

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

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

 # set your API token (temporary)
export WPVULNDB_API_TOKEN="YOUR_TOKEN"

 # simple passive scan and save human-readable output
wpscan --url http://lab.example --detection-mode passive --throttle 500 --random-user-agent --output lab-scan.txt --format cli

```
┌──(kali㉿kali)-[~/Desktop]
└─$ wpscan --url https://www.wpbeginner.com/ --detection-mode passive --throttle 500 --random-user-agent --output lab-scan.txt --format cli
```

```
1  ___________________________________________________________________
2          __          _______   _____
3          \ \        / /  __ \ / ____|
4           \ \  /\  / /| |__) | (___   ___  __ _ _ __   ®
5            \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
6             \  /\  /  | |     ____) | (__| (_| | | | |
7              \/  \/   |_|    |_____/ \___|\__,_|_| |_|
8
9          WordPress Security Scanner by the WPScan Team
10                          Version 3.8.28
11        Sponsored by Automattic - https://automattic.com/
12        @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
13 ___________________________________________________________________
14
15 [32m[+][0m URL: |
16 [32m[+][0m Started: Thu Aug 28 03:59:45 2025
17
18 Interesting Finding(s):
19
20 [32m[+][0m Headers
21  | Interesting Entries:
22  |  - cf-ray: 976245383c40fcf3-SIN
23  |  - cf-cache-status: HIT
24  |  - via: 1.1 google
25  |  - alt-svc: h3=":443"; ma=86400
```

 # enumerate users, all plugins, and all themes; save JSON

wpscan --url http://lab.example --enumerate u,ap,at --api-token YOUR_TOKEN --format json --output lab-enum.json

```
1 {
2   "banner": {
3     "description": "WordPress Security Scanner by the WPScan Team",
4     "version": "3.8.28",
5     "authors": [
6       "@_WPScan_",
7       "@ethicalhack3r",
8       "@erwan_lr",
9       "@firefart"
10    ],
11    "sponsor": "Sponsored by Automattic - https://automattic.com/"
12  },
13  "scan_aborted": "HTTP Error: https://wpscan.com/api/v3/status?version=3.8.28 (status: 401)",
14  "target_url": "https://www.wpbeginner.com/"
15 }
```

 # force plugin detection mode to mixed

wpscan --url http://lab.example --plugins-detection mixed --enumerate ap

```
┌──(kali㉿kali)-[~/Desktop]
└─$ wpscan --ur[redacted] --plugins-detection mixed --enumerate ap
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __   ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: https[redacted]
[+] Started: Thu Aug 28 04:06:23 2025

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 | [redacted]
 | [redacted]
 | [redacted]
 | [redacted]00
 | - cf-apo-via: tcache
 | - cf-edge-cache: cache,platform=wordpress
 | - x-powered-by: PHP/8.0.30
```

Conclusion

By practicing with WPScan in a controlled environment, interns gain: - **Red Team Skills:** Understanding attacker reconnaissance and exploitation techniques. - **Blue Team Skills:** Building defenses by monitoring logs, patching vulnerabilities, and hardening WordPress.

This dual perspective makes students stronger defenders by thinking like attackers.

End of WPScan manual