

# Forum:[Hack Forums](#)

Thread: [WPScan: A Guide to Ethical WordPress Security Testing](#)

JoseMar - January 23, 2025, 5:37 am

## WPScan: A Guide to Ethical WordPress Security Testing

### What is WPScan?

WPScan is a powerful, open-source vulnerability scanner that is designed for WordPress websites. It's a tool used by security professionals, ethical hackers, and website administrators to identify security issues in WordPress installations. WPScan can detect vulnerabilities in WordPress core, themes, plugins, and even weak user credentials.

Think of it as a kind of "health check" for WordPress sites: it helps you find weaknesses before malicious hackers do. It is widely used in ethical hacking with the purpose of ensuring that websites are secure, and also for practicing penetration testing in a controlled environment.

### Why is WPScan Important?

WordPress powers more than 40% of all sites on the internet, which makes it a favorite target for hackers. Most WordPress sites become vulnerable because of outdated software, poorly coded plugins, or weak passwords. WPScan helps you:

- Identify vulnerabilities before any attacker does.

- Test security of your own-or your clients'-WordPress sites.

- Learn about most common WordPress security issues in practice.

### How Does WPScan Work?

It scans a WordPress website and checks the components, core, themes, and plugins, against a database of known vulnerabilities. It also carries out brute-force attacks to test weak passwords. Here is a breakdown of its main features:

- Core Vulnerability Scanning:** Checks whether the installed version of WordPress is out of date or has known security weaknesses.

- Plugin and Theme Scanning:** Lists plugins and themes that are installed and then attempts to check them for vulnerabilities.

- User Enumeration:** This identifies usernames, which may be used in brute-force attacks.

- Password Brute-Forcing:** It tries weak passwords for identified users.

- Vulnerability Database:** WPScan utilizes the WPScan Vulnerability Database, and this is usually updated regularly on new vulnerabilities.

### Setting Up WPScan in Your Virtual Lab

First, before you begin with WPScan, you need to set up a safe environment where you can practice. How to do this on your PC or use different website like TryHackMe, HackTheBox etc... On your PC:

- Install Virtual Machine:** You have to download a virtual machine using tools such as VirtualBox or

VMware.

Set Up WordPress Site: On your virtual machine, you will be able to install WordPress. You can use XAMPP or Local by Flywheel for easy installation.

Install WPScan: WPScan is a Ruby-based tool. You can install it on Linux - Kali Linux is ideal - or on Windows using Docker.

## Installation Steps:

```
Code sudo apt update  
sudo apt install wpscan
```

## Running WPScan: Examples and Commands

Now that you're set up, let's run some scans! Here are a few examples:

### 1. Basic Scan

This command scans the target WordPress site for core, plugin, and theme vulnerabilities:

```
Code wpscan --url http://your-wordpress-site.com
```

### 2. Enumerate Users

To discover usernames on the site:

```
Code wpscan --url http://your-wordpress-site.com --enumerate u
```

### 3. Brute-Force Attack

To scan for weak passwords of a specific user:

```
Code wpscan --url http://your-wordpress-site.com --passwords /path/to/wordlist.txt --usernames  
admin
```

Note: This should only be performed on systems you either own or have permission to test.

### 4. Scan Specific Plugins

To scan for installed plugins for vulnerabilities:

```
Code wpscan --url http://your-wordpress-site.com --enumerate p
```

### 5. Update the Vulnerability Database

Make sure that your WPScan database is updated:

```
Code wpscan --update
```

## Interpreting WPScan Results

When you run a scan, WPScan will provide a detailed report. Here's what you might want to look out for:

WordPress Version: If it's out of date, it has known vulnerabilities.

Plugins/Themes: Check any installed plugins or themes for known vulnerabilities.

Users: Enumerated usernames are targets for brute-force attacks.

Vulnerabilities: WPScan will list known vulnerabilities and give links to more information.

For instance, if WPScan was to identify a plugin vulnerability, it may state :

```
Code [!] Plugin: vulnerable-plugin (v1.2.3)
```

Vulnerability: Arbitrary File Upload

Fixed in: v1.2.4

Reference: <https://wpvulndb.com/vulnerabilities/12345>

## Practical Example: Testing in Your Virtual Lab

Let's say you've set up a WordPress site in your virtual lab with the following details:

URL: `http://localhost/wordpress`

Installed Plugin: "Vulnerable Plugin v1.0"

User: admin

Run the following commands:

Scan the site:

Code `wpscan --url http://localhost/wordpress`

Enumerate users:

Code `wpscan --url http://localhost/wordpress --enumerate u`

Test for weak passwords with Wrodlist (BruteForce):

Code `wpscan --url http://localhost/wordpress --passwords /usr/share/wordlists/rockyou.txt --usernames admin`

Testing Wordpress without know the Username and password, Here we add Wordlist for Username -U and also for Password -P

Code `wpscan --url http://<machine-IP>/ -U <usernames.txt> -P <password-list.txt>`

Ethics what we need to follow:

Permission: Never scan a target without permission to do so.

Legal Use: Use WPScan only for ethical hacking, penetration testing, or securing your own systems.

Responsible Disclosure: If you find somebody else's site is vulnerable, practice responsible disclosure.

### Conclusion

WPScan is the basic box of tools for anyone dealing with WordPress security: you can find weaknesses, test your defenses, and learn ethical hacking in the most practical way. Practice in your virtual lab to earn hands-on experience and enhance your skills further while continuing to keep it ethical and responsible.

Remember, with great power comes great responsibility, and the use of such tools as WPScan is to make the web a safer place, not to take advantage of it. Happy scanning!