

Forum:[Hack Forums](#)

Thread: [The best and smartest ways to find vulnerabilities of websites especially Wordpress.](#)

SIM-5652947 - May 18, 2025, 12:41 pm

What are some of the best tools you use for finding vulnerabilities?

Do you have any tips or strategies for identifying vulnerabilities that are actually useful and impactful?

How do you prioritize your findings to focus on the most critical issues?

Are there any specific techniques you use to maximize efficiency during scanning and testing?

Personally, I use tools like Nmap, Burp Suite, and Nikto for initial scans, but I'd love to hear about other tools or manual methods that you find effective. Any recommendations for tools or tips on how to discover high-value vulnerabilities would be greatly appreciated!

Dotexe - May 18, 2025, 12:47 pm

I'd say Metasploit, after enumeration phase you will most likely already have an idea what's running like services/softwares. The next logical phase would be to go for deep enumeration using Metasploit.

SIM-5652947 - May 18, 2025, 1:02 pm

Hey Dotexc, thanks for the Metasploit tip—clean and useful! Your posts always hit the mark. Keep it up! ?

Dotexe - May 18, 2025, 1:09 pm

No worries bro, if you need some more tips you can always slide a DM

Dolla\$ - May 18, 2025, 3:15 pm

wp-json

usually disclose all endpoints & custom ones if ur lucky

good ressource there : <https://hacktricks.boititech.com.br/pentesting/pentesting-web/wordpress>

DramaKing - May 19, 2025, 4:48 am

GVM is a good scanner.

Envy - May 19, 2025, 6:31 pm

Depending on whether you're the attacker or the site owner, from the site owner perspective there's a lot of tools and even free plugins you can install that will simply scan your site for vulnerabilities and/or malware depending on what you're looking for. For a lot of my client sites, I use "Hide My WP Ghost" which essentially allows you to rewrite every single WordPress path, your content folders, even API endpoints. That plugin has a "vulnerability scanner" that will sweep the site(s) real quick and notify you of any vulnerabilities in either the site, plugins, and what you can do to increase security (like disabling WP plugin and theme editor, for example).

WPHive (<https://wphive.com/>) is another good asset to use for making plugin decisions, it's almost like a "CarFax" for plugins - I believe they also have a browser plugin that when you're browsing WordPress directory for plugins or themes will notify you if the plugin has had any exploits or vulnerabilities recently, when it was, and whether or not it's being fixed or addressed. WPHive also gives detailed history on plugins, so for example WPHive would show multiple instances in which Jetpack has been exploited or risky to use because of severe vulnerabilities.

Then from the attacker perspective, pretty basic but:

Using a plugin detector and from the list of discovered plugins finding which still have exploitable vulnerabilities, is also another route. In some cases they're even documented or have an exact identifier of what type of exploit or vulnerability it is, narrowing it down. Of course something like this only works until a plugin is patched or updated, but even massive plugins like Jetpack are known to be common focus for attackers as it's basically shovel-ware in the sense Jetpack plugins are pushed with almost every mainstream WordPress hosting platform resulting in majority of WordPress sites opting in and using Jetpack.

Another wonderful, tried and true method of getting into WordPress sites is simply just bruteforcing the /wp-login.php page. It's crazy even nowadays how little security some WordPress sites considering there are even FREE security alternatives and then assets like ChatGPT which can help you rewrite common paths, secure and harden a website in step-by-step form if you had no clue how. In fact, you can even get ChatGPT to write you a small script you can paste into your browser's console (in Dev Tools, CTRL + F12) with a list of words (or even STRINGS) which you can execute a basic bruteforcing attack directly from your browser within only minutes (obviously, you'd want to perform this in a much more organized matter and with an established password list) but because a lot of these sites don't have bruteforce protection, this makes it still a susceptible method of obtaining backend access.

Then obviously the other worthy mentions from the other members, hope that helps.

jabba - May 19, 2025, 9:28 pm

Are people able to do perspective plug-ins

This gentleman is a god! He taught me step by step, but I have no basic knowledge, but I still thank him!

ShellPower - May 20, 2025, 2:47 am

People look for newly found vulnerabilities and try to exploit them before they are patched... somewhat like taking a ride on 0-days that are now publicly known, but will take time to patch (if they ever will, some things are never patched, or patched after months)

SIM-5652947 - May 20, 2025, 2:59 am

Hi Envy

I just wanted to take a moment to thank you for your detailed and insightful response to my question. Your explanation was incredibly helpful, especially the tools and methods you shared from both the site owner and attacker perspectives. The recommendations like Hide My WP Ghost and WPHive are gems, and your breakdown of common vulnerabilities was eye-opening. I really appreciate the time and effort you put into your answer—it's clear you know your stuff, Thanks again

for sharing your knowledge.

tope - May 21, 2025, 7:22 am

Is there anyone who know how I can find vulnerabilties or buy 0 day vulnerabilities.