

Forum:[Hack Forums](#)

Thread: [how to find vulnerabilities in websites on windows?](#)

majmune1997453 - April 28, 2024, 3:31 am

I want to learn to find vulnerabilities in websites. So if you have some knowledge please reply to this post, it really helps out a ton.

witrecx - April 28, 2024, 2:47 pm

You could use wpscan for wordpress pages.

famedgod6 - April 28, 2024, 5:22 pm

Use something like Nmap or OWASP zap

nmap you can find vulnerability's by using

nmap --script vuln www.example.com

or you can use nmap www.example.com and get all the open ports but the best thing to do is

nmap -sV www.example.com to see what versions of the ports the website or server is running on, the google or search up on exploit-db if any of the ports are vulnerable, then you can use metasploit to exploit one of the vulnerable ports

but the best tool out there in my opinion is OWASP zap, basically this tool is like magic, it scans for web based vulnerability's and if there is one, it explain how its exploited, the solution to the problem, and the code thats leaving it vulnerable

its the best tool for bug bountys in my opinion

Vax_11 - April 29, 2024, 10:16 pm

Hi, i was wondering if theres any particular exploit with metasploitable to stress test passwords on wordpress? or is there any other tool you guys recommend to exploit the login page?

SilentNuke - April 30, 2024, 8:40 am

Can you run wpscan and nmap on windows?

I would suggest getting a kali VM or VPS - much better and more of a variety of tools at your disposal.