

Forum:[Hack Forums](#)

Thread: [How to find vulnerabilities in websites without any tools?](#)

majmune1997453 - May 4, 2024, 7:29 am

Hello,i just want to learn how to find vulnerabilities in websites wtihout any programs.Im just curious and want to learn something new so if you know please reply to this post.

Bastille - May 4, 2024, 7:32 am

Crystal ball, divination, tarot card maybe

Otherwise I don't know

Absence - May 4, 2024, 7:34 am

Doing it without tools would require a pretty good knowledge of how websites work, coding languages, exploitation, and more. Why is it you do not want to use tools?

Every website is different, you aren't going to find the same vulnerabilities everywhere, so if you are trying to learn, you should definitely have the tools. Maybe for beginners you can start at <https://www.hackthebox.com/>

But yeah, generally speaking, tools would be your friend in assessing vulnerabilities, especially if you are new.

Pr0m3th3us - May 4, 2024, 7:35 am

Correct me if I'm wrong but I would assume this require knowledge of reading code, and HTML ????. I mean if you not using a tool then that means your comprehension of these things is what's allowing to to find a vulnerability.

(May 4, 2024 07:32 AM)Yseurk Wrote: [\[CITE\]](#) Crystal ball, divination, tarot card maybe

Otherwise I don't know

Don't forget about Ouija board bro...

quelch - May 14, 2024, 5:08 pm

Before I say this, I just want to say that this is all for educational purposes, and I'm not responsible for whatever you do with this info. :D.

It's not easy, but if you know where to look, you can find websites to hack without tools. Assuming you mean programs like "downloadable" tools the web actually has a lot to offer in hacking, even without downloading anything.

First, you're going to need to be able to find the websites you're going to target. You can do this by using a method called Google Dorking, which is used a lot in OPSEC, but that's a rabbit hole for another time. What you need to know is that you can use the google hacking database (<https://www.exploit-db.com/google-hacking-database>) to basically make ultra-specific google searches.

For this method, find a google dork that will search for an admin panel of a website or the database of a website.

If you've found a website's admin page that looks like the security might not be top notch, you can

then get to the best part: Inputting variations of default admin passwords in the search boxes! Start with something like user: admin and password: admin, then move on to user: admin password: admin until something hits. It won't work for every website, but it's worth checking. There's a great list of default login info on <https://github.com/danielmiessler/SecLists/blob/master/Passwords/Default-Credentials/default-passwords.txt> - it's definitely worth a look.

Most websites this won't work. It's tough, but if you can't use tools, there might not be a point in going through every admin password (it'd just be mostly a waste of time). If it does work, congrats!

The only thing to look out for here is the difference between "wrong credentials" and "wrong password". If a website says "wrong password" when you use one username and "wrong credentials/login" when you use another, you know you've got the right username, and you've got the wrong password. This is when it might be worth it to start guessing the passwords like a madman.

If you go the google dorking for database route, you might be able to find a website's user logins, which could have an admin password. If you can find one, congrats, if you can't, then so be it.

If you have any questions, let me know. I'm happy to help! ?