how to hack WordPress site with Kali Linux

first of all, start-up kali Linux and start up your terminal.

we need to install a tool to scan the site the tool we will use is WPSCAN. WPSCAN is great for scouting out a WordPress website.

to install this tool type in your terminal git clone https://github.com/wpscanteam/wpscan.git  you can just copy and paste this.

there are many good alternative websites if you don't have kali Linux and still want to check your vulnerability I recommend <https://hackertarget.com/wordpress-security-scan/>

to use the tool WPSCAN you need an account on their website. This account is needed to get the API token without this token you cannot scan so make an account on this site <https://wpscan.com/wordpress-security-scanner> click on get started and fill in your account details.

once you made an account your API token will look something like this. You cannot use mine because I have regenerated it so it is not usable anymore

Afbeelding met tekst

Automatisch gegenereerde beschrijving

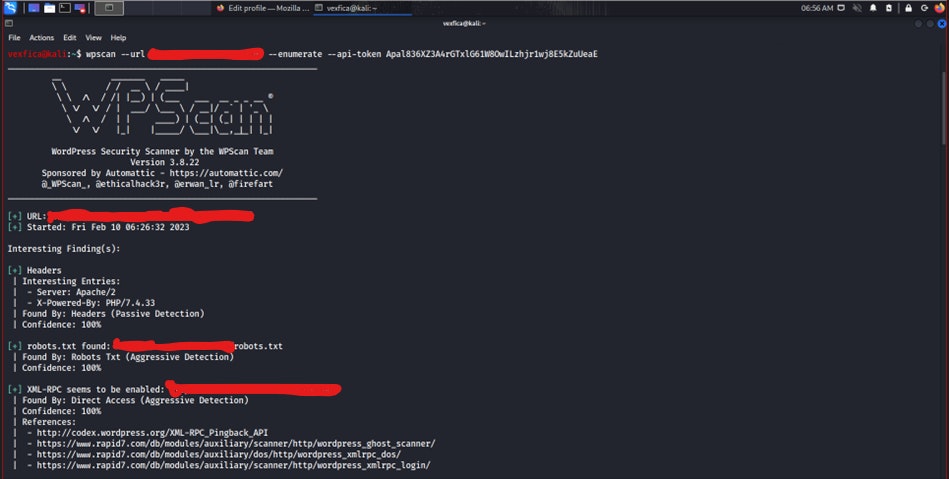
go back to kali Linux and your terminal and type the following command

wpscan --url <https://www.example.com> --enumera -api token 23jk45h4jkhLKJ%HKJ$%H$KJ%Hkj4589GDF0(\*DG&

instead of <https://www.example.com> you put your wordpress site and instead of

23jk45h4jkhLKJ%HKJ$%H$KJ%Hkj4589GDF0(\*DG&  you copy your own api token

if everything up to now went well you will see something like this



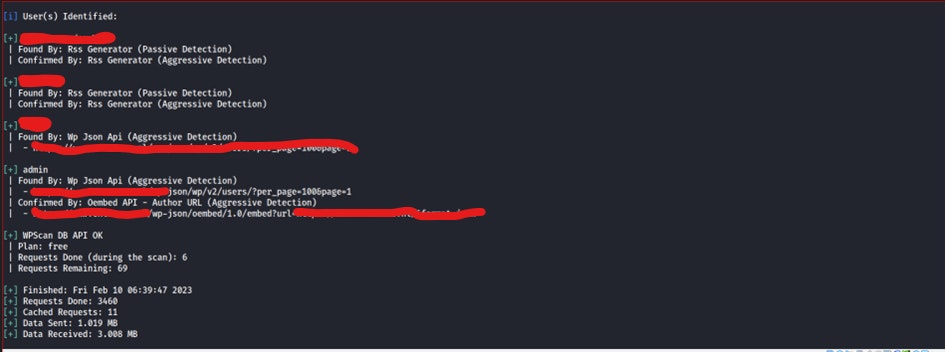
I crossed the URL out for privacy purposes

You want to search for vulnerabilities and exploits in this scan I will give you an example

Afbeelding met tekst

Automatisch gegenereerde beschrijving

in this screenshot above you can see a vulnerability. The scan has found 6 vulnerabilities. Now the question is how to use these vulnerabilities. if you copy the References: links in google you will see how to use this vulnerability however in this tutorial will not be using one of those 6 vulnerabilities.



will be using a wordlist attack. you can see in this screenshot above the admin users I have found I have crossed them out for privacy purposes. now that we know the admin usernames we can use a wordlist attack to crack the password.

To make this work you need to make or download your own wordlist or use the Rockyou wordlist that's already installed in the default Kali Linux

the command i used is sudo wpscan --password-attack xmlrpc -t 20 -U users1,user2 -P /Desktop/vexfica/wordlist/rockyou.txt --url [www.example.com](https://www.example.com)

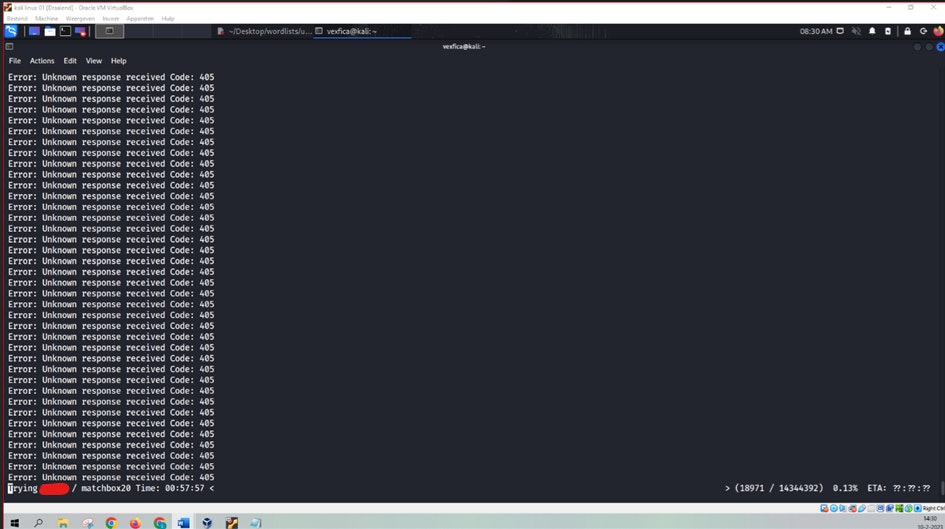
short exaplanation -t stand for how many threads i want i selected 20 what this mean is it will try 20 password in a second.

-U stand for the users you want to try these password on

-P stand for the path your wordlist is in

--url stand for the website you want to hack

This is how it will look like when it is trying all the passwords in the list as you can see I let it on for a full 1 hour since this wasn't an easy password it took a long while but I got the password in the end after 1 hour and 23 minutes.



However, I cannot share this screen with you since I like to keep the password private. The wordlist will stop when the password is found so, for example, if the password and username are admin it will be found in about 6 seconds because that's almost the first one on the list. if you make your own personalized wordlist the process will go faster.

there are about 810 million WordPress sites you can do this on however I only recommend you use this on sites you have permission to pentest or your own personalize pentesting site

I hope you have learned something and found my post interesting this guide is only made for educational purposes. With this, I will end my guide and wish you good luck on your hacking journey.