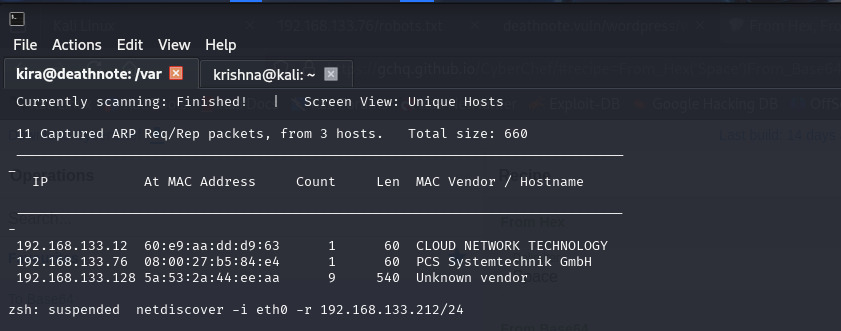
Deathnote:1 Walkthrough

This is one of the best series in Japanese anime where the character kira is plays vital role I have watched this series two time and I recommend you to watch deathnote.

1. **Enumeration**

First we need to know our ip address and check the both machine are in same network = bridge adapter.

To enumerate the machine ip address we use netdiscover

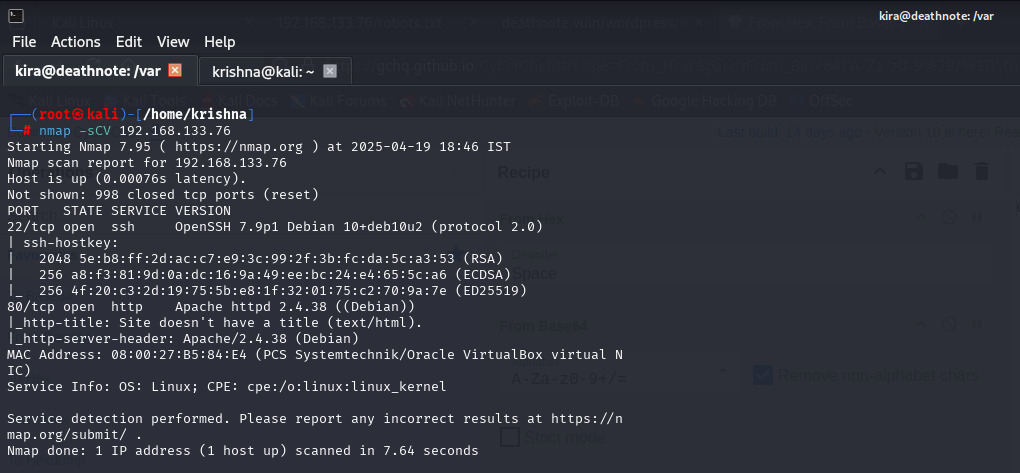
****netdiscover -i eth0 <ip>

Here we can see the IP address of deathnote machine.

## Reconnaissance

Now I have scanned the IP address to check any open ports, default script and version detection.

Here, the command Nmap –sC –sV –pn <ip>

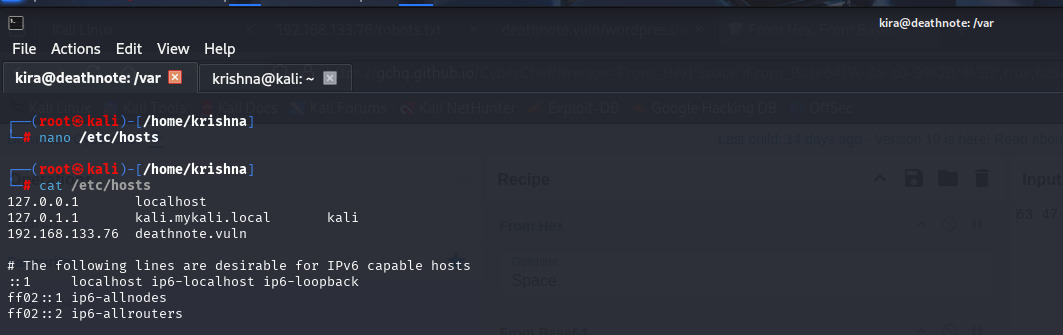


I got two open ports 22 SSH and 80 HTTP.

Heading over to the port 80 webpage. A deathnote.vuln page that’s running on WordPress. The page either doesn't work or hasn’t rendered properly, yet the machine is up.

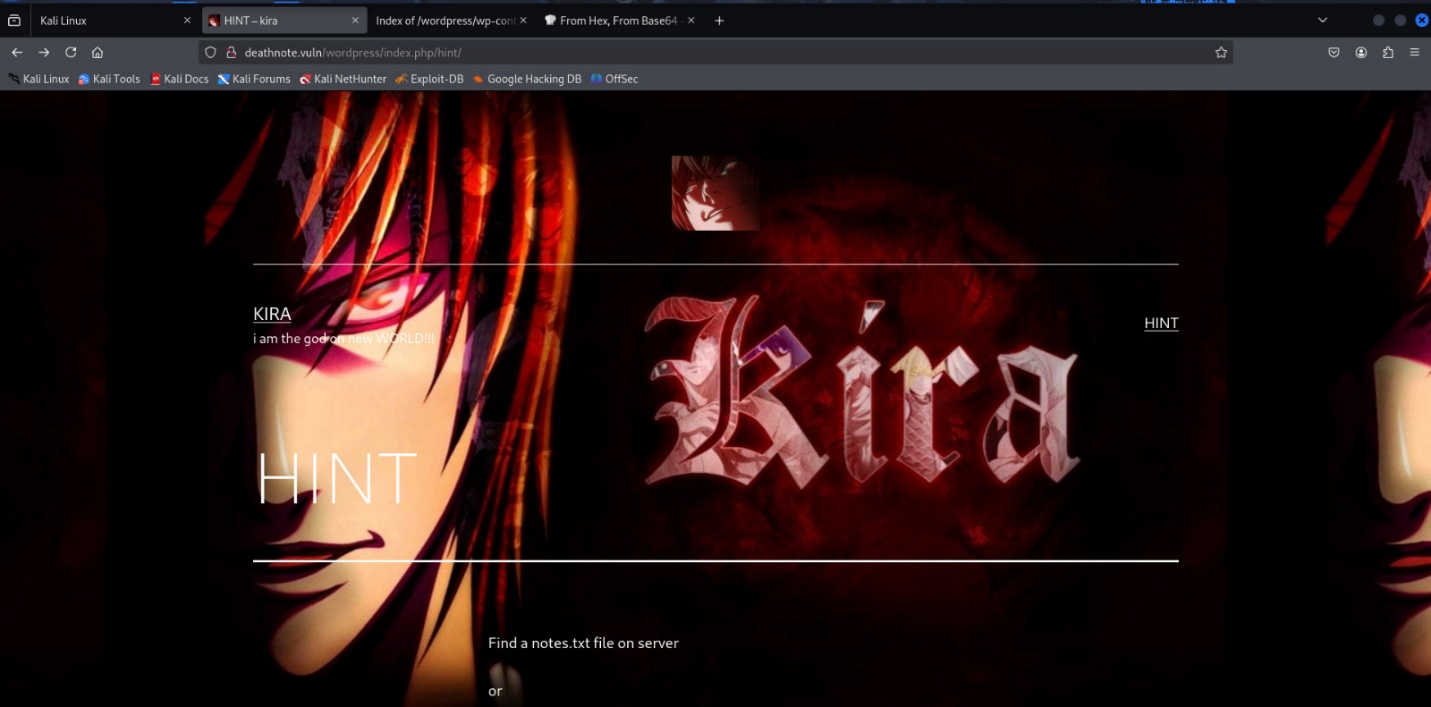
So, I had decided to add the deathnote.vuln to a list of my hosts to resolve this.

Now, I edited the /etc/hosts file using nano

nano /etc/hosts

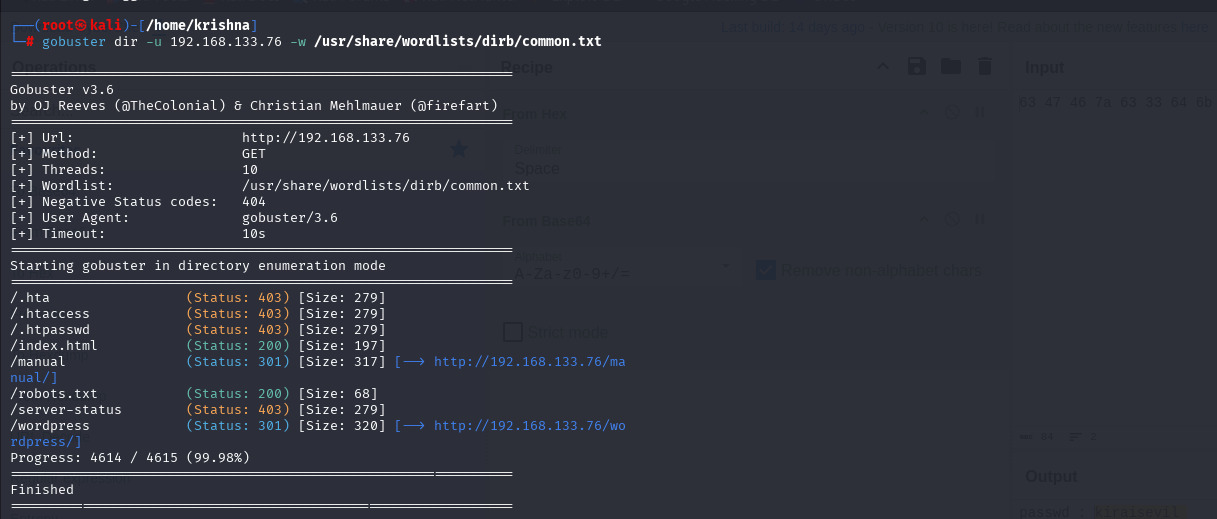
Viewing the lists of hosts updated and the deathnote.vuln appears.

Back to the webpage and after reloading it now works. The page looks like Kira’s page. There’s a hint at the top right of the page.

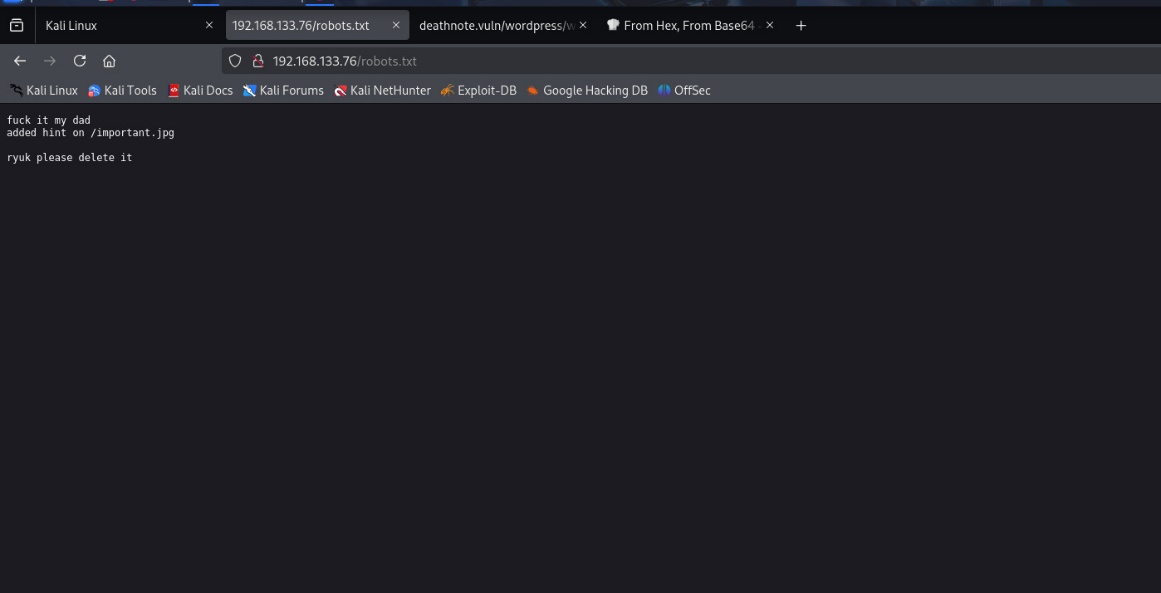


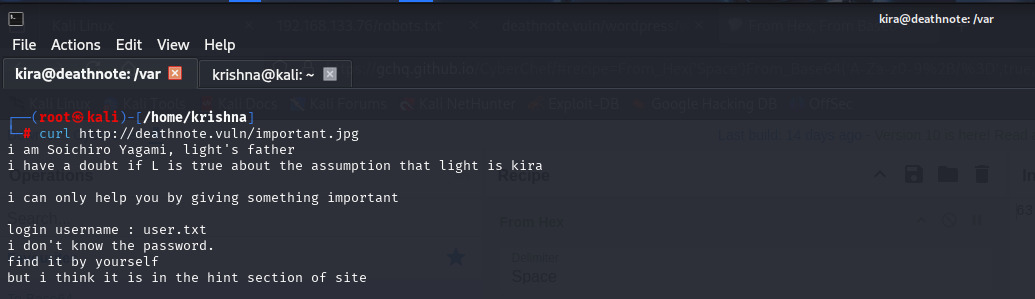
Navigating to the hint there, I got something interesting. There’s a notes.txt file somewhere on the server. The files that run the webpage are stored on the same server

GOBUSTER



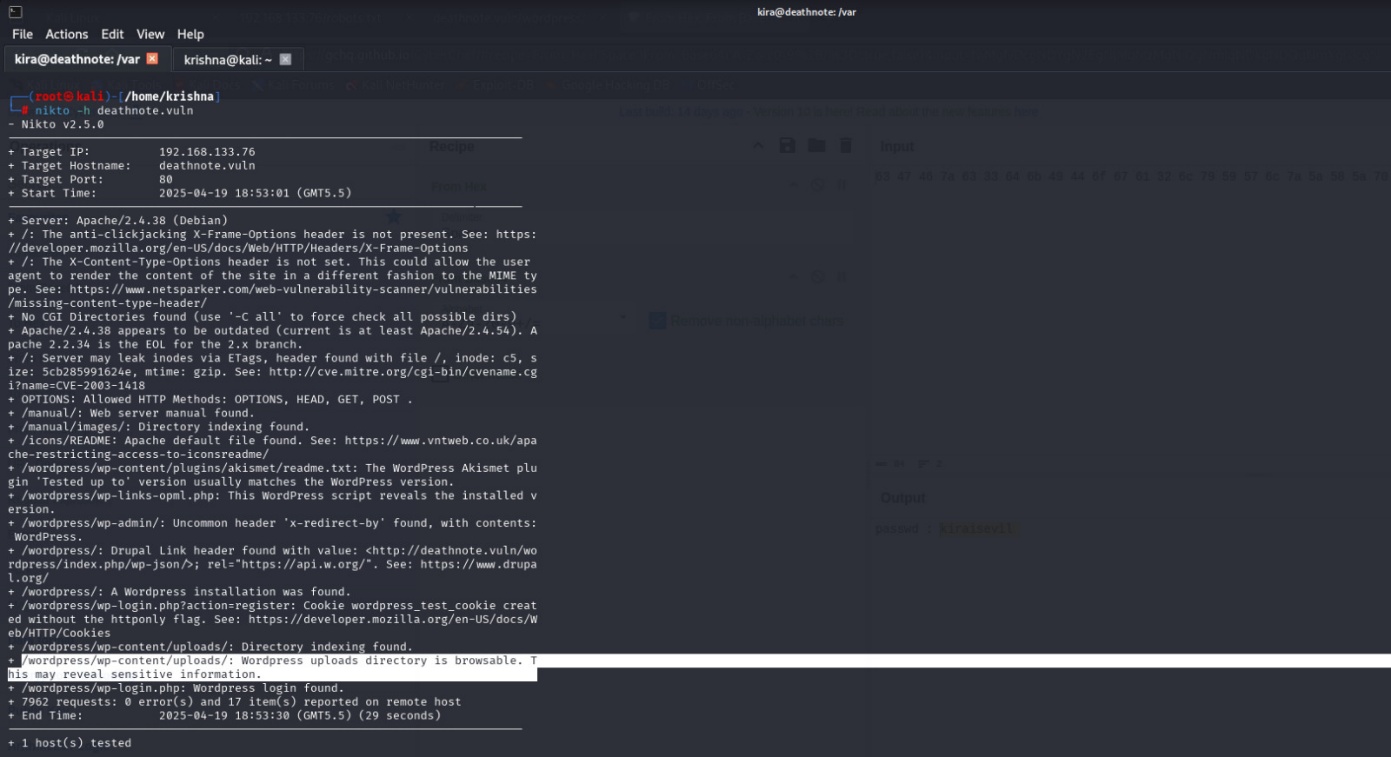
my enumeration using gobuster I found a robots.txt file. robots.txt is a text file that instructs automated web bots on how to crawl and/or index a website.



 Another hint is the /important .jpg. this is added by kira

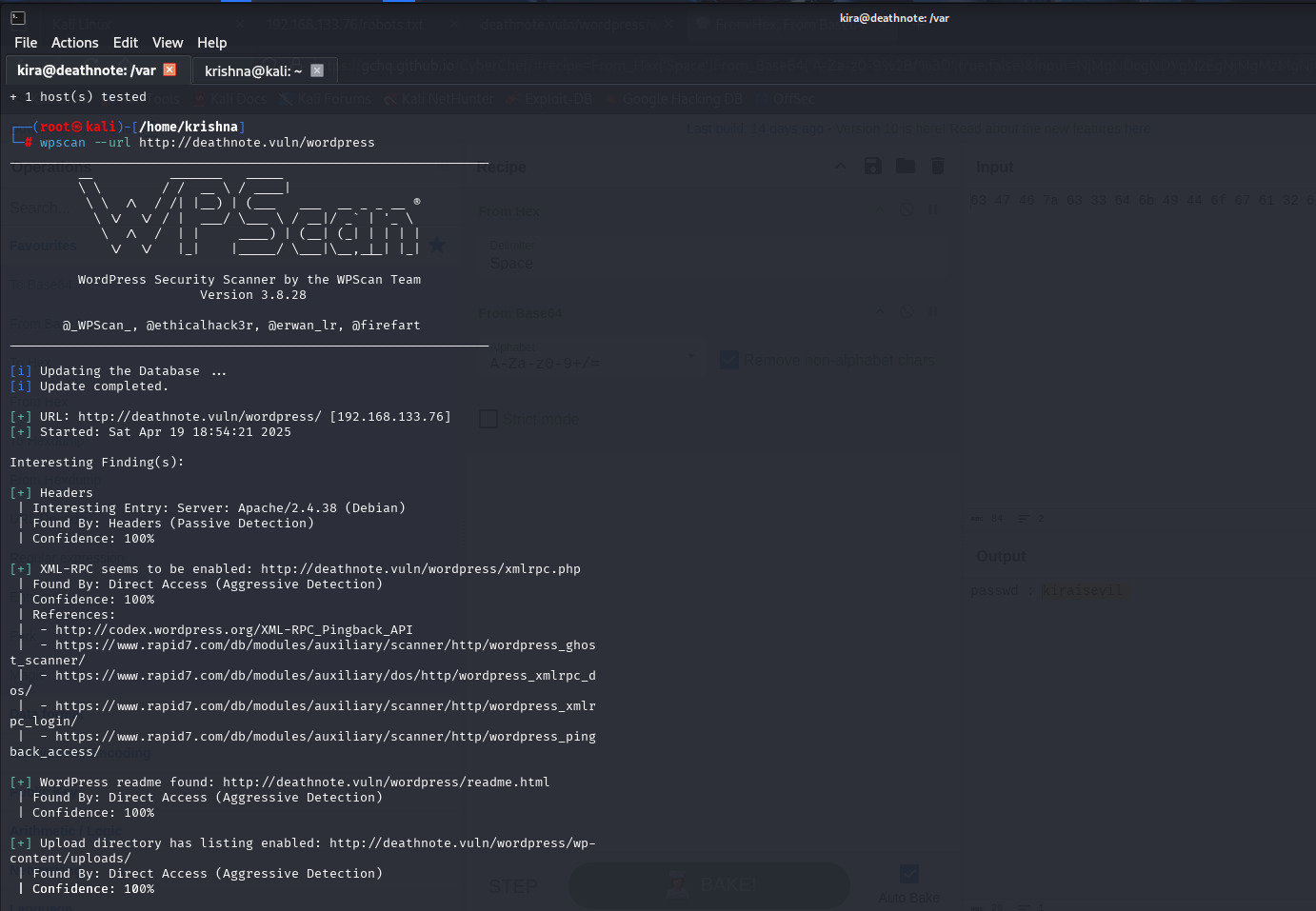
Light’s father hints that the login username will be found in the user.txt file.

Now we know that notes.txt and user.txt are somewhere in the server.

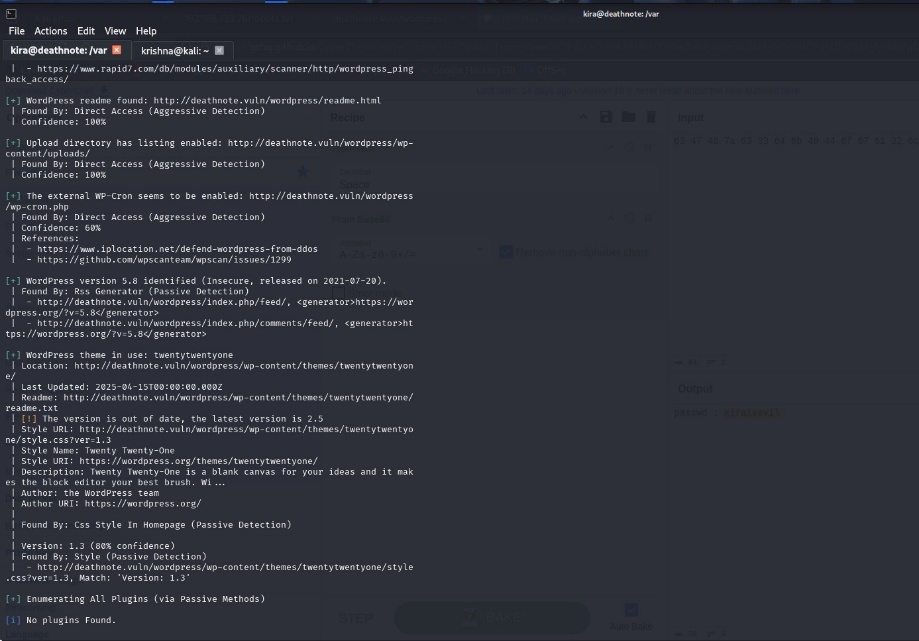
I enumerated the website for vulnerabilities using nikto. There’s a brow-sable directory that may reveal sensitive information.

The webpage is run on WordPress, there’s a specific tool to scan WordPress webpages, called wpscan.

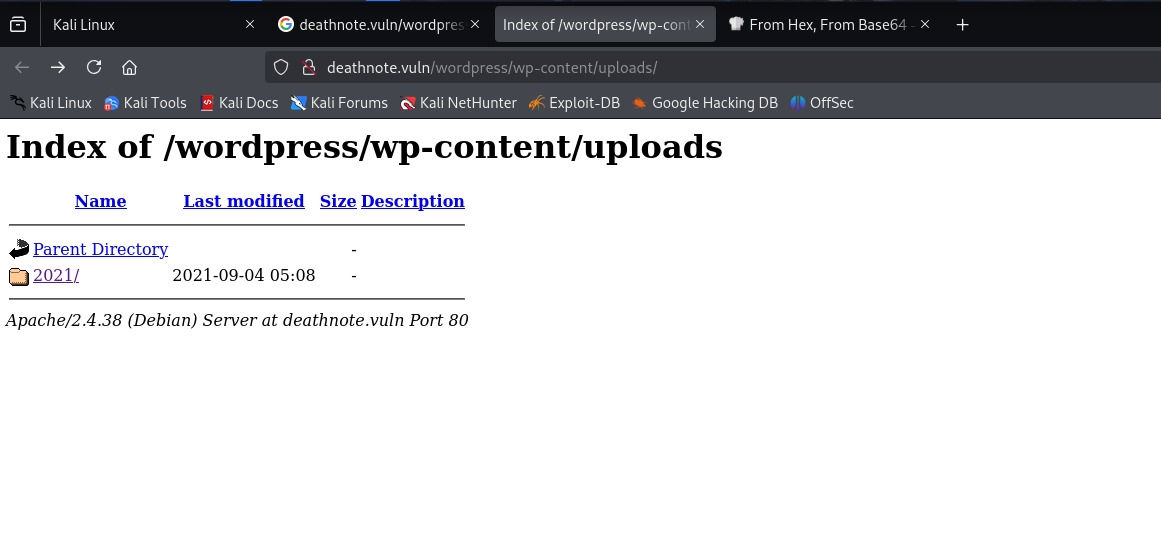
3.WPScan



Similar to Nikto here also I have found the uploads directory. This uploads directorys have the information that will be useful to us.

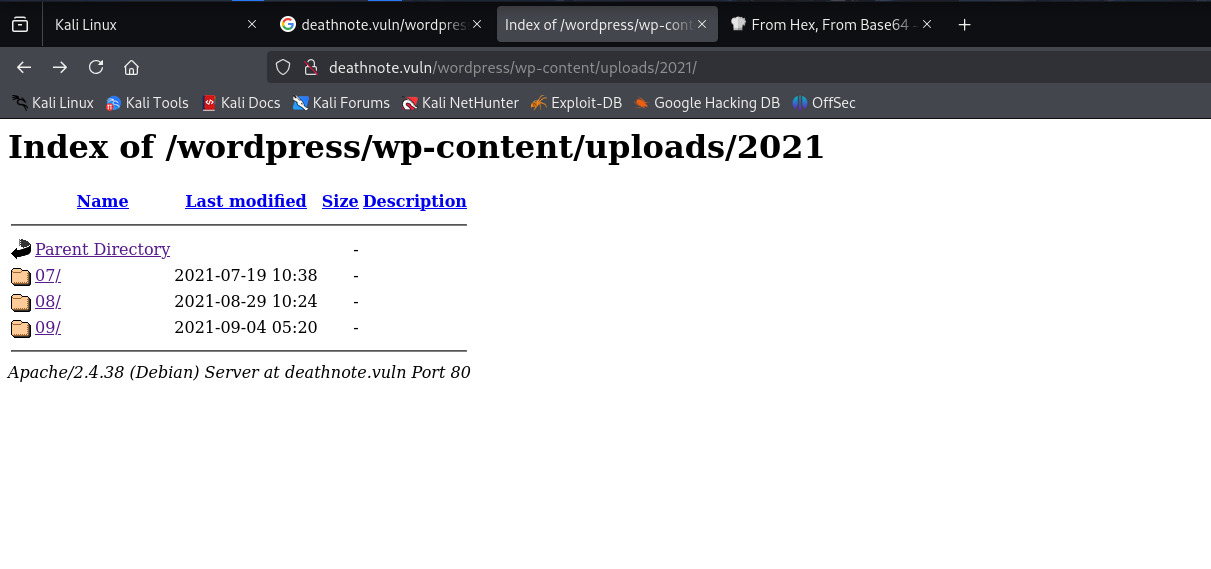


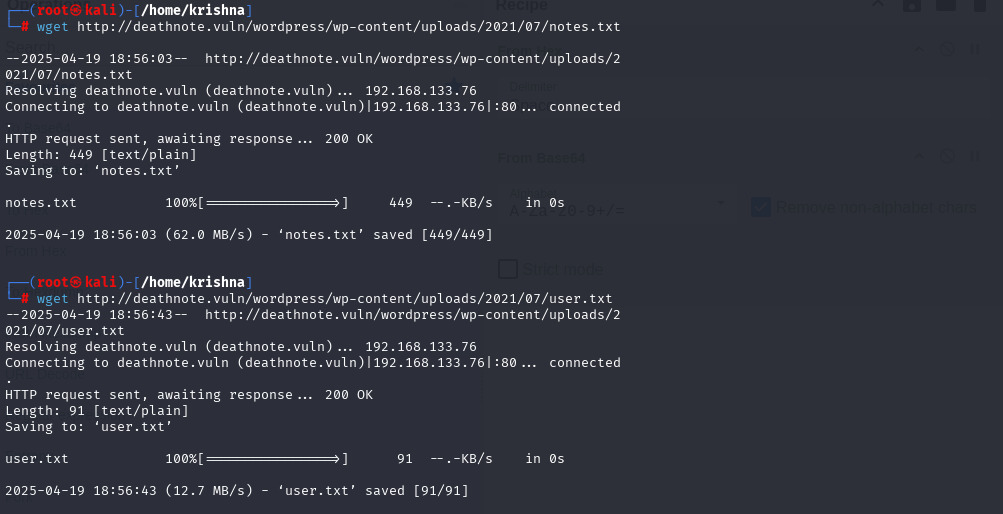
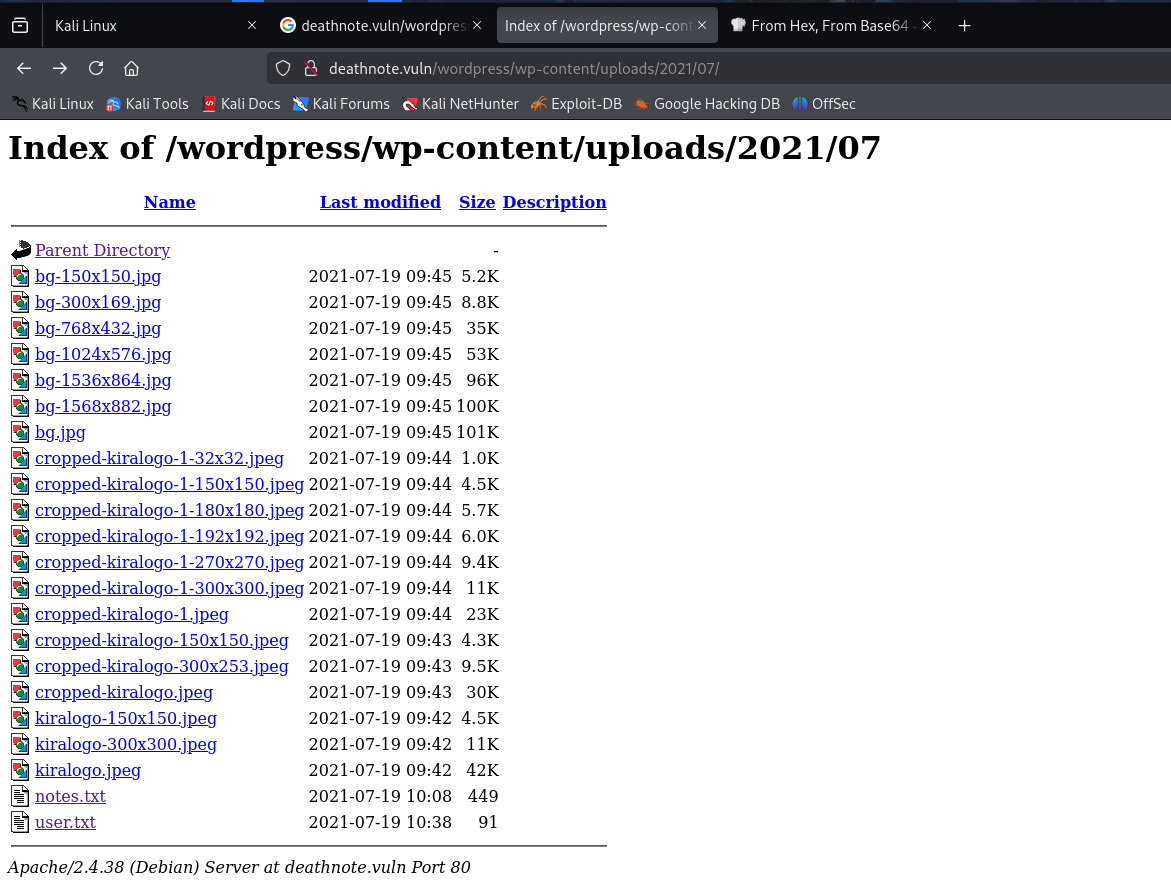
The directory are having the sub-derectorys to we can see in the WPScan and similar in nikto.



At the base directory, there’s a folder named 2021. Dive in.

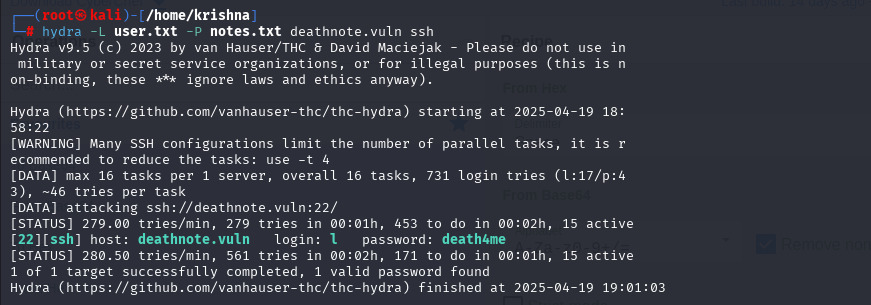
Out of the three folders, 07 had some resources, the webpage images, and two unusual files.



I grabbed them to my machine using the wget command and their respective URLs.

3. Exploitation

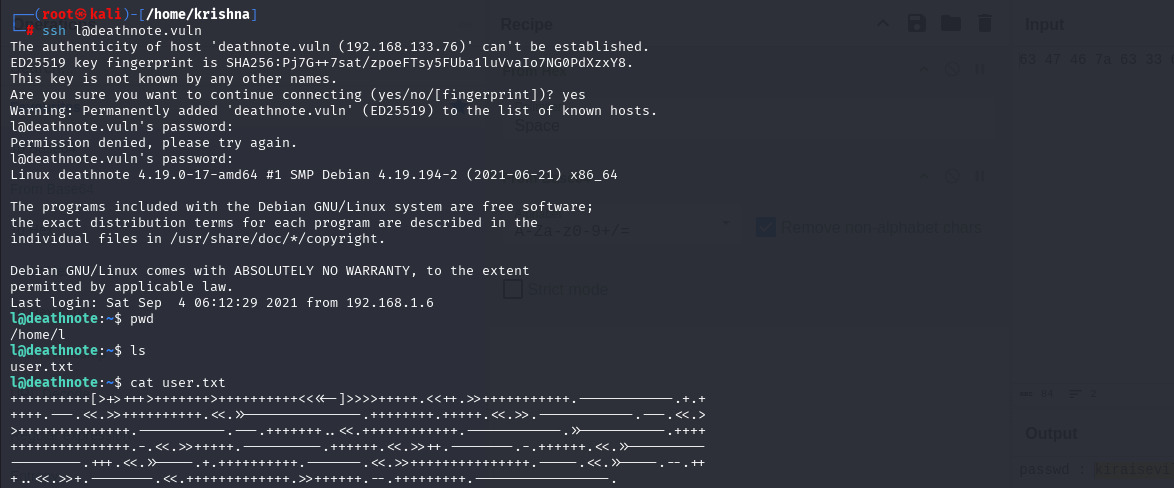
Now, we have got the note.txt and user.txt file from this we are going to findout the username and password worlists. To this I was using brute force hydra tool.

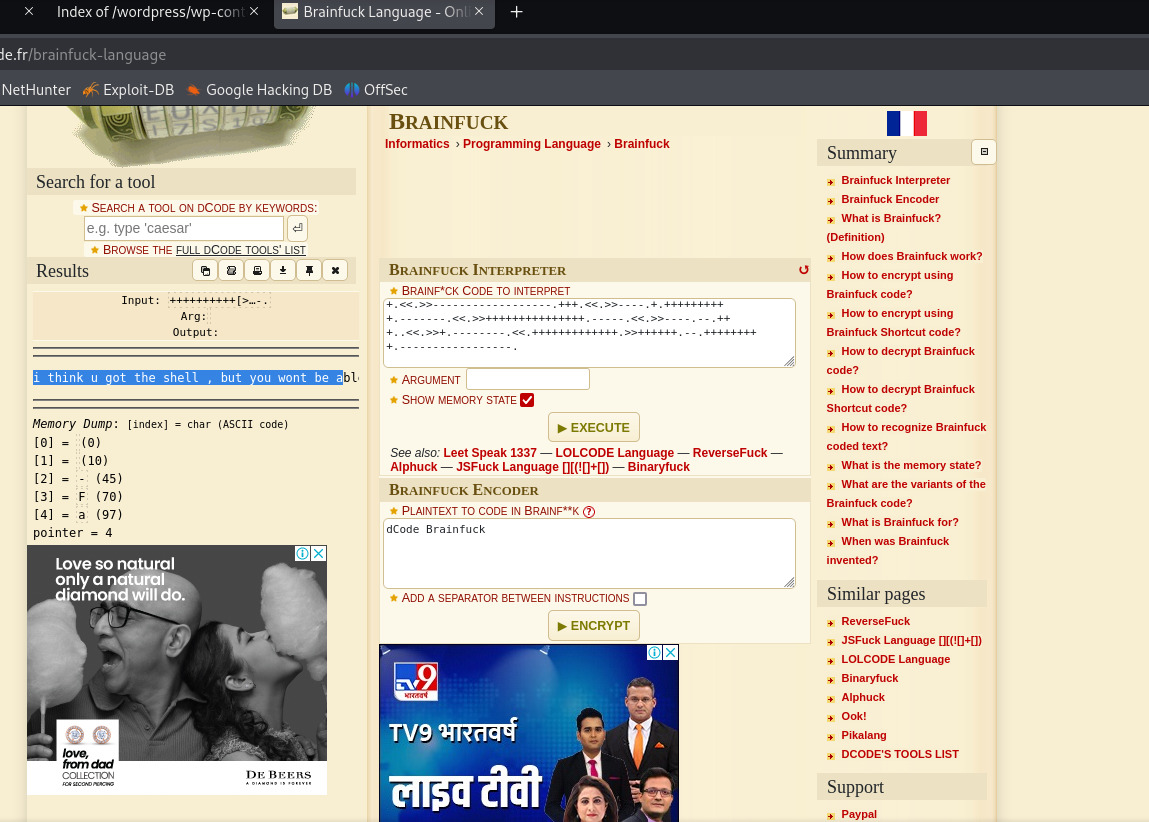
hydra — L /wordlist/ — P /wordlist/ /IP/ ssh

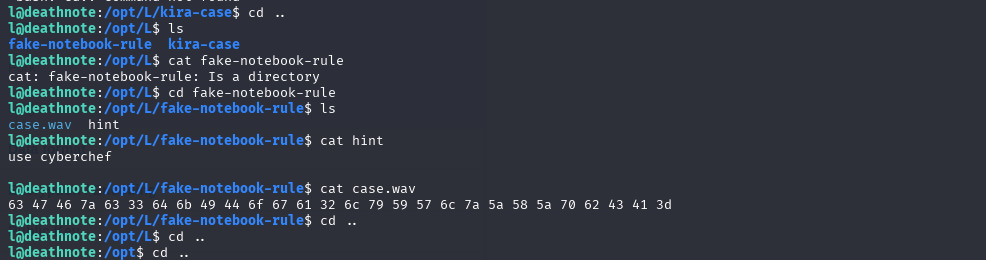
Here, we got the login and password credentials to login into deathnote remote system.

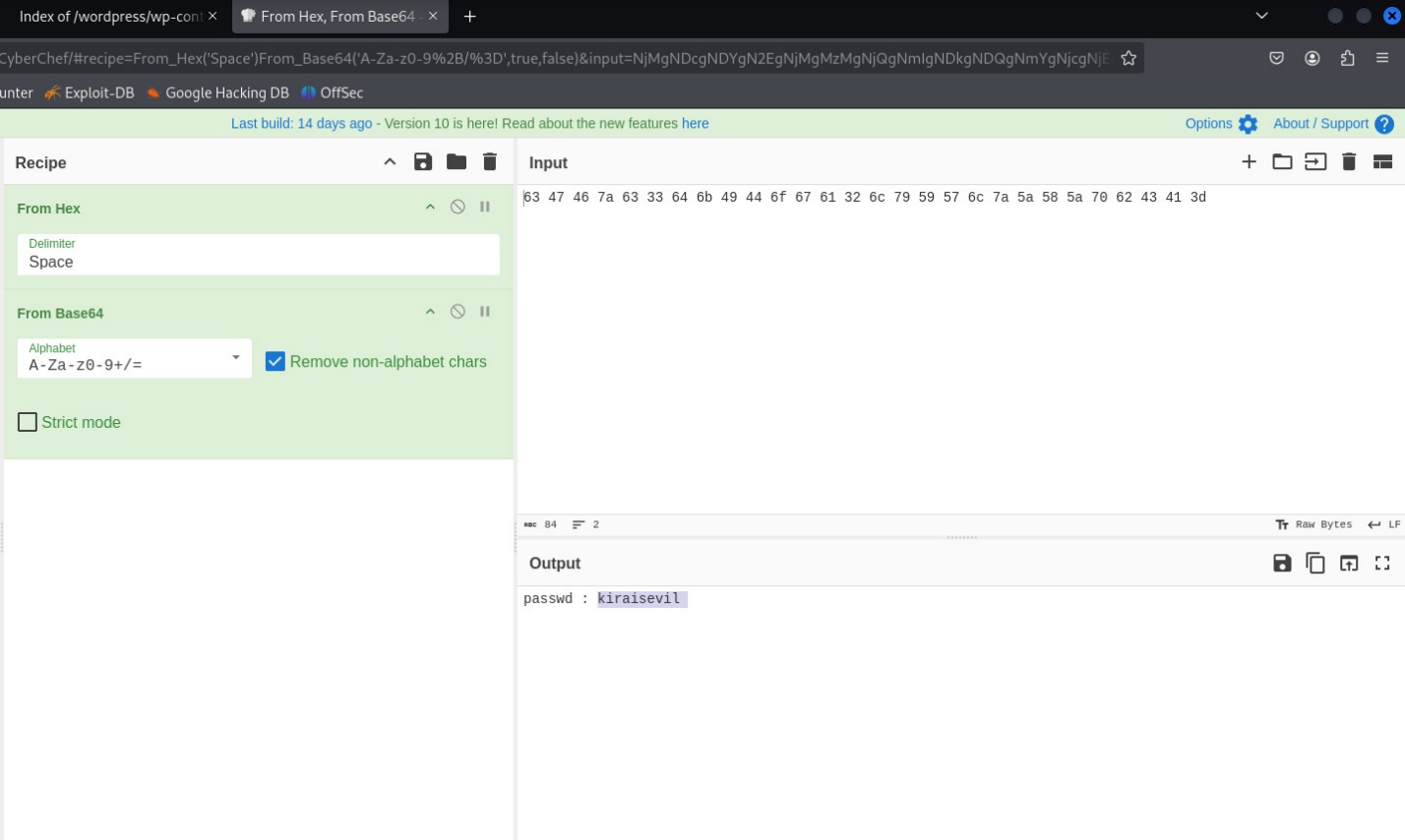
4. Getting a shell

Login with the credentials we got from brute force earlier.

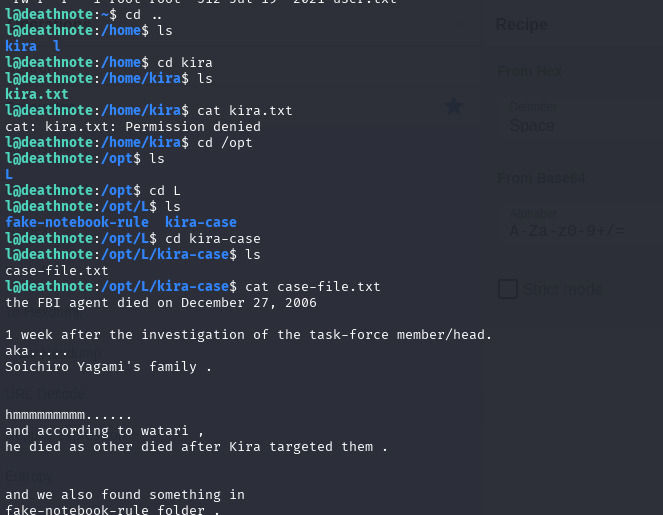
 Now **ssh** [**l@deathnote.vuln**](mailto:l@deathnote.vuln)

We are in, logged in as the user L. Right out of the gate there’s a user.txt file in L’s directory. It’s a coded message, the language used is brainfuck an esoteric programming language.

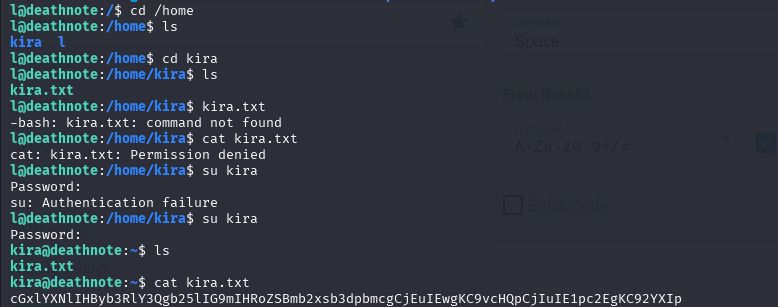
I enumerated the base directories and in the /opt folder there’s a folder named L. Two interesting files fake-notebook-rule and kira-case

Now go to  [cyberchef](https://gchq.github.io/CyberChef/" \t "_blank) to decode the message and we get another credential, a password.

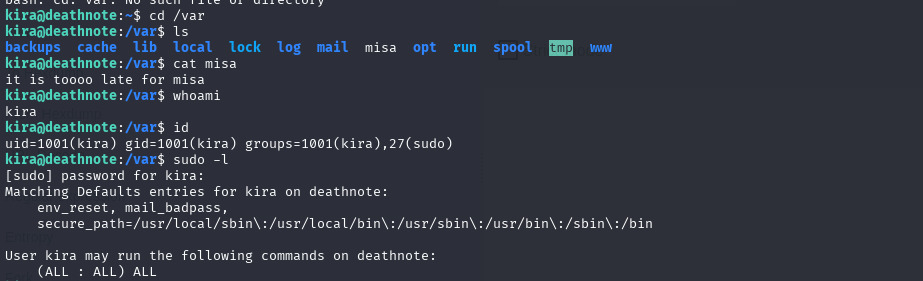
In the directory kira-case there’s a hint pointing to fake-notebook-rule



Back to the home directory, there are two users l and kira. In the kira directory, a kira.txt file looks like it’s only visible to kira.



The message was encoded with base64 and I quickly decoded it with the following command:

Looking at Kira’s permissions, I noticed Kira can run sudo with root privileges.

5. Privilege Escalation

I have tried to escalate to super user by same password i got and it is working and tried to access the root folder look what i have found.

