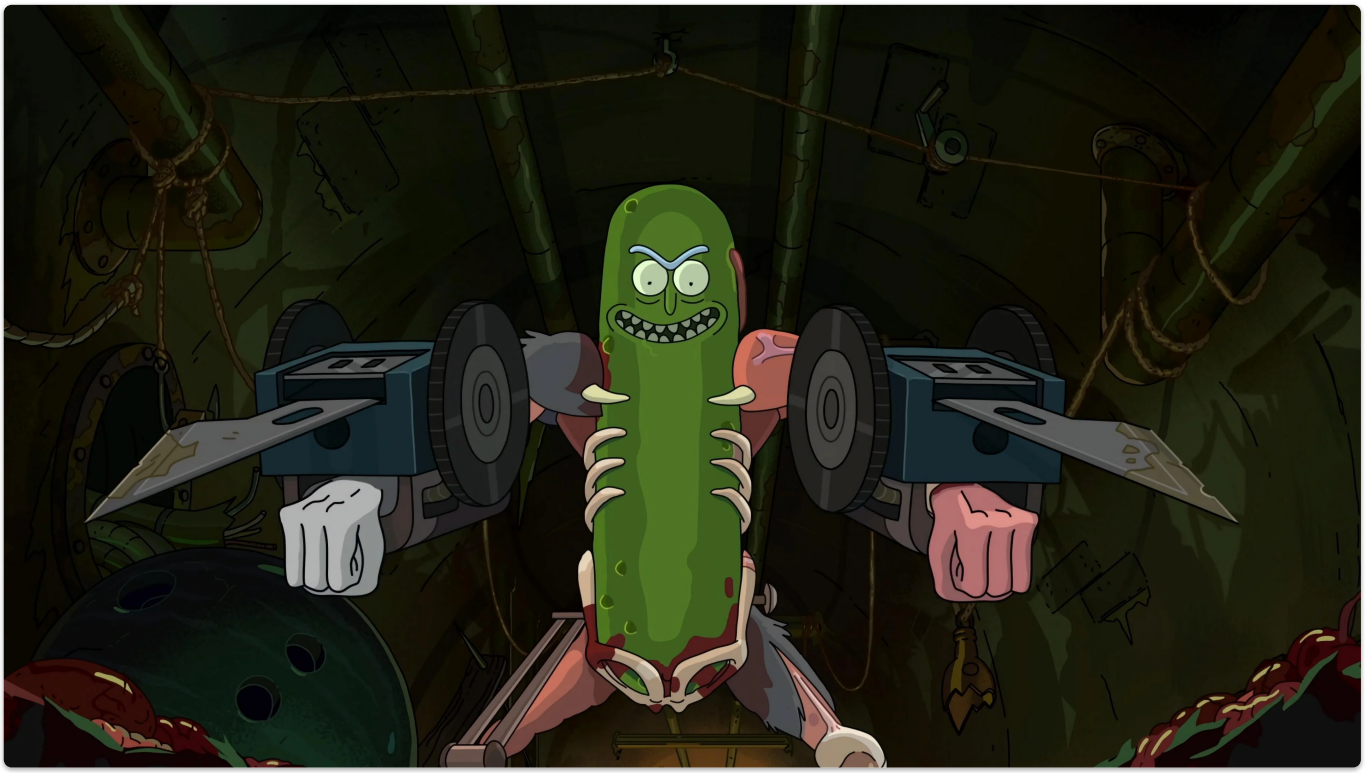
PICKLE RICK



GETTING STARTED

> Note
>
> To access the room, click on the link given below
> https://tryhackme.com/r/room/picklerick

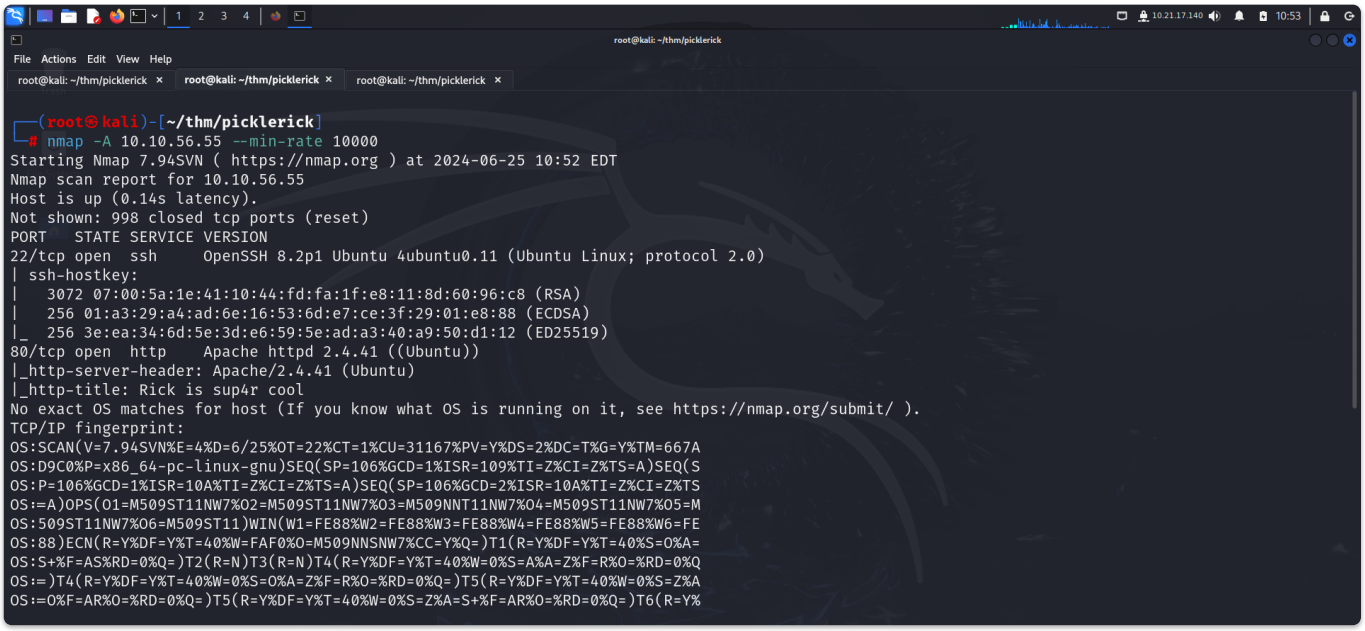
To work on the machine through our locally installed Linux, I downloaded the openvpn configuration file from here.

Finally, I ran the *openvpn* configuration file.

```
openvpn file.ovpn
```

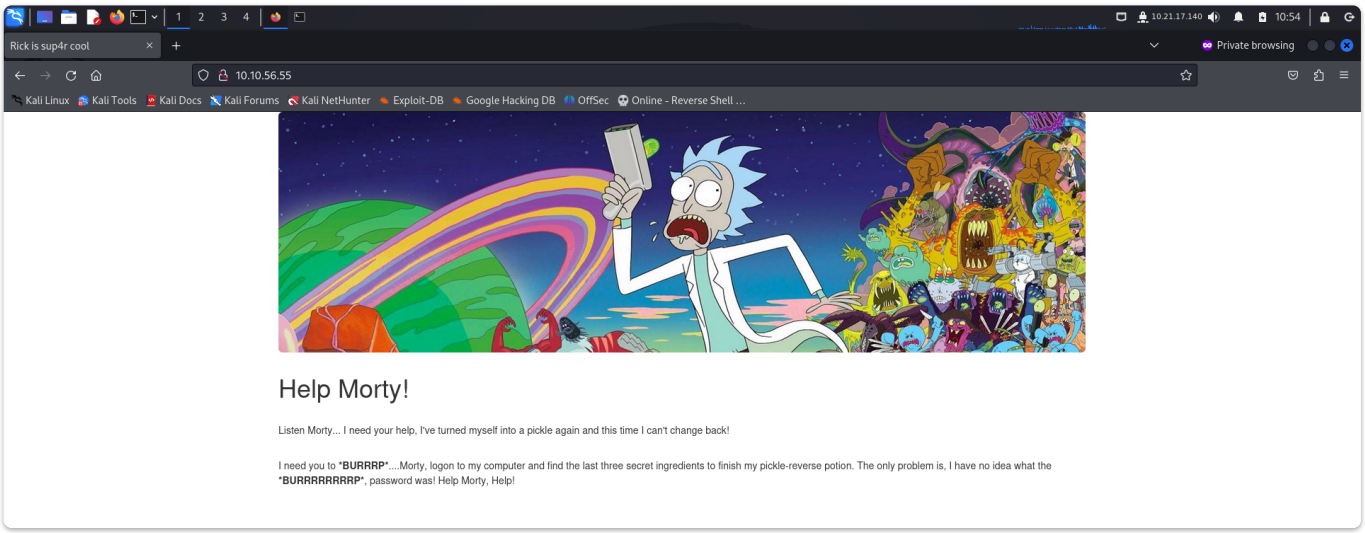
RECON

I performed an nmap aggressive scan to identify open ports and services running on the target.

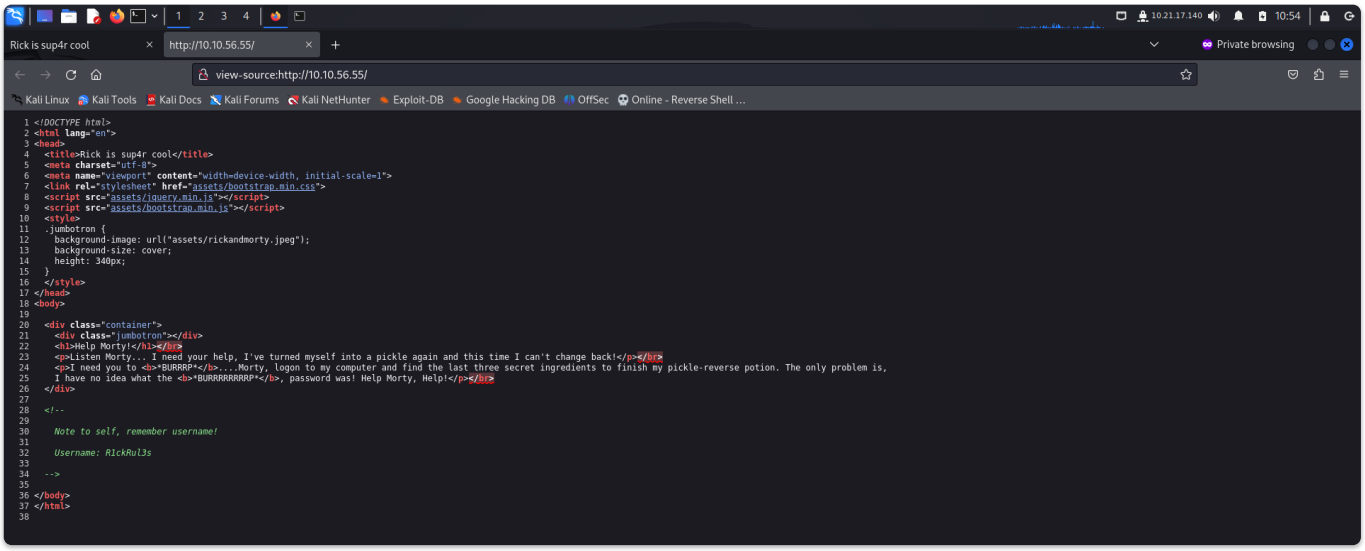


INGREDIENT 1

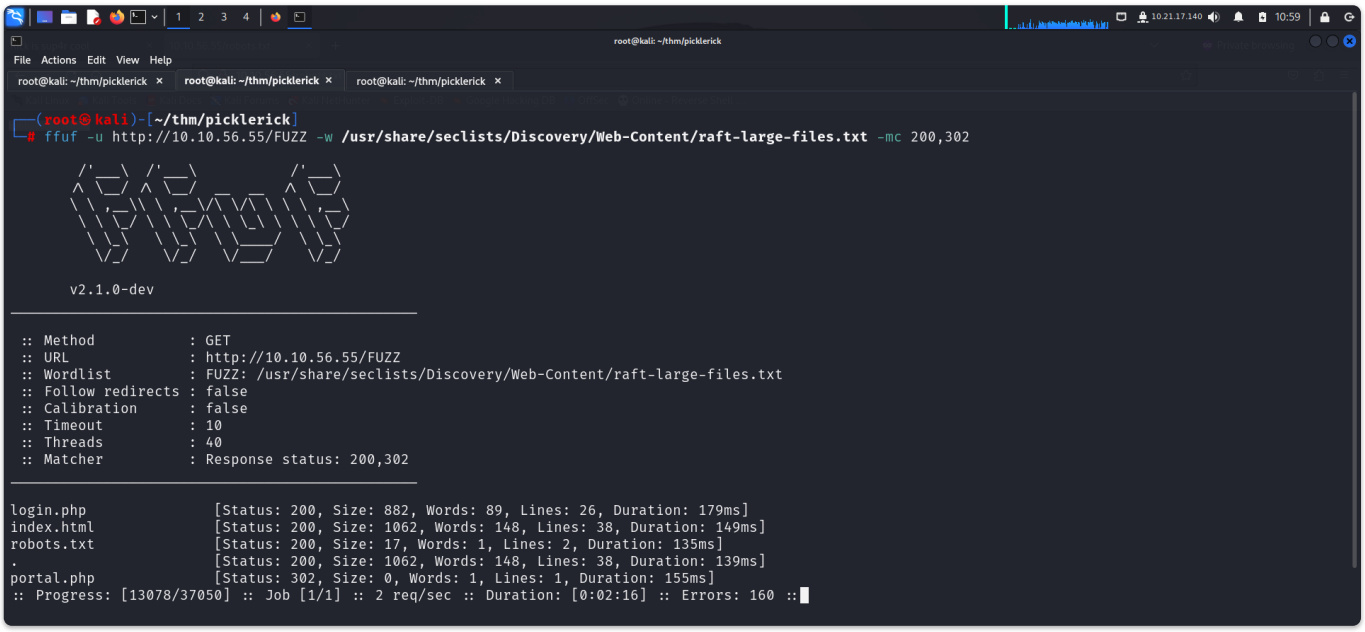
I visited the web server using a browser.



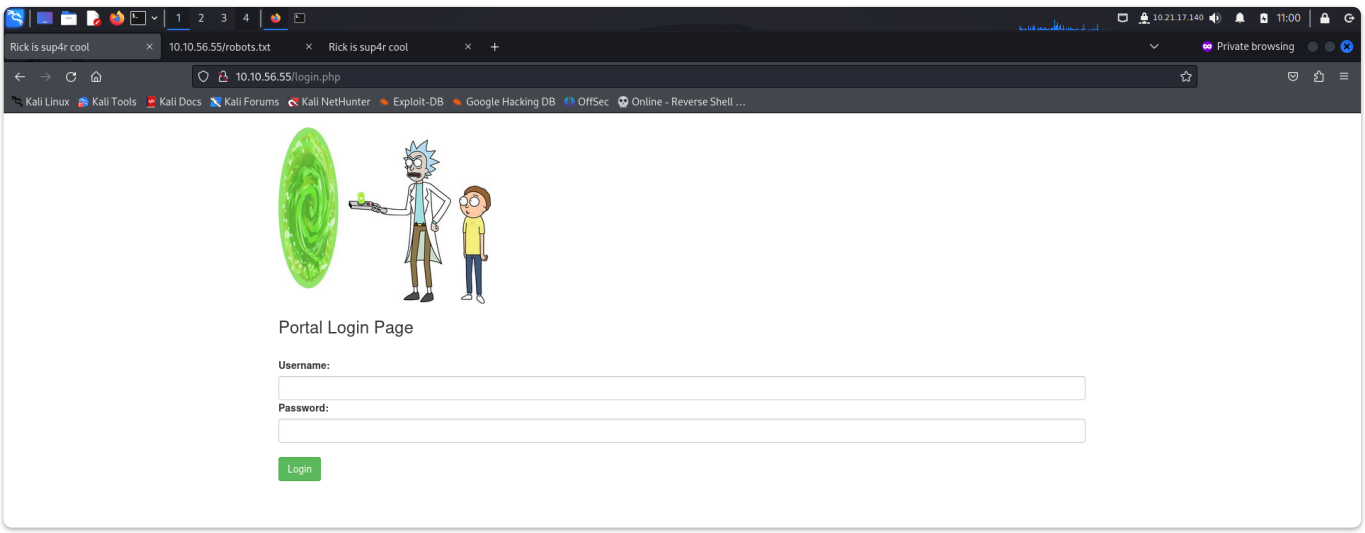
Upon inspecting the source code, I found a username.



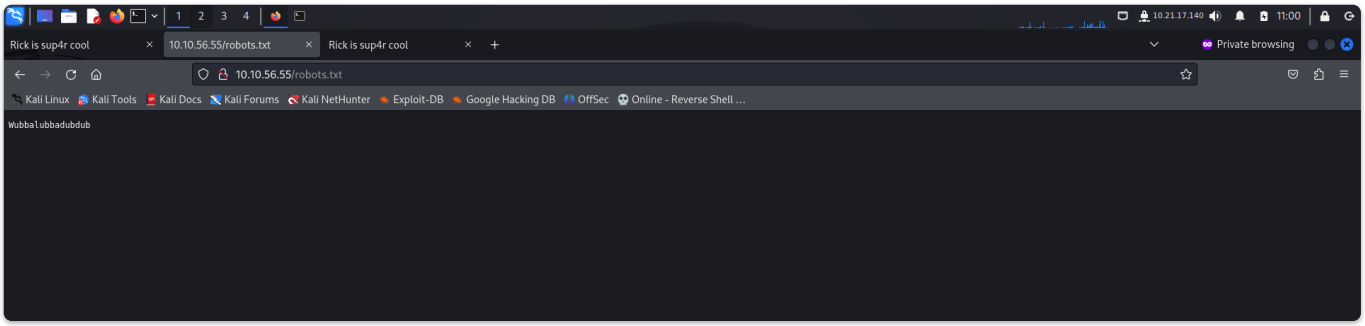
I performed a ffuf scan to find other files on the web server.



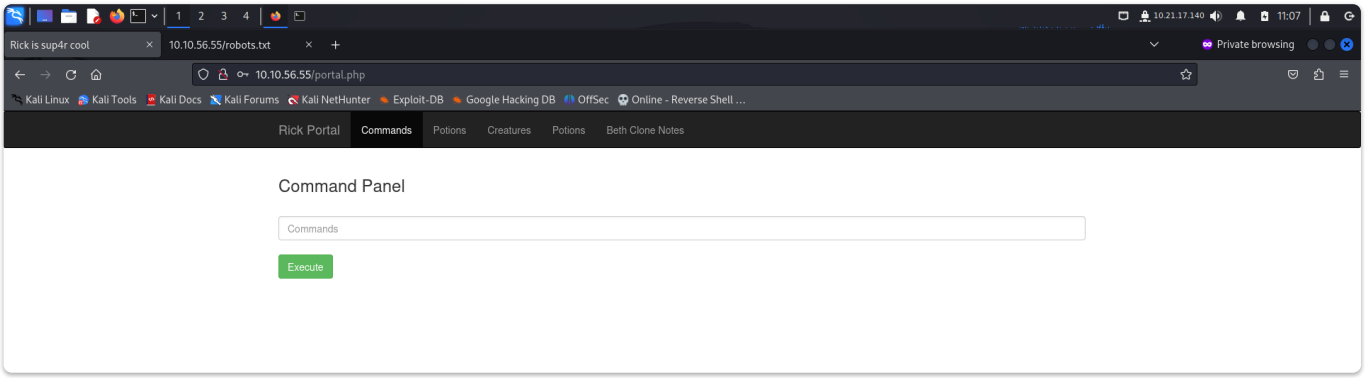
I accessed the *login.php* and got a login panel.



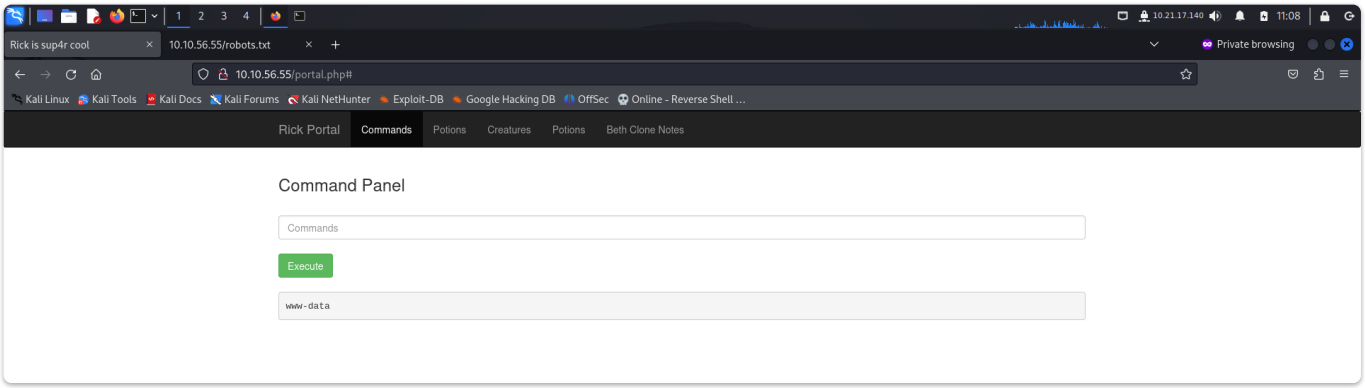
The *robots.txt* file also contained some text.



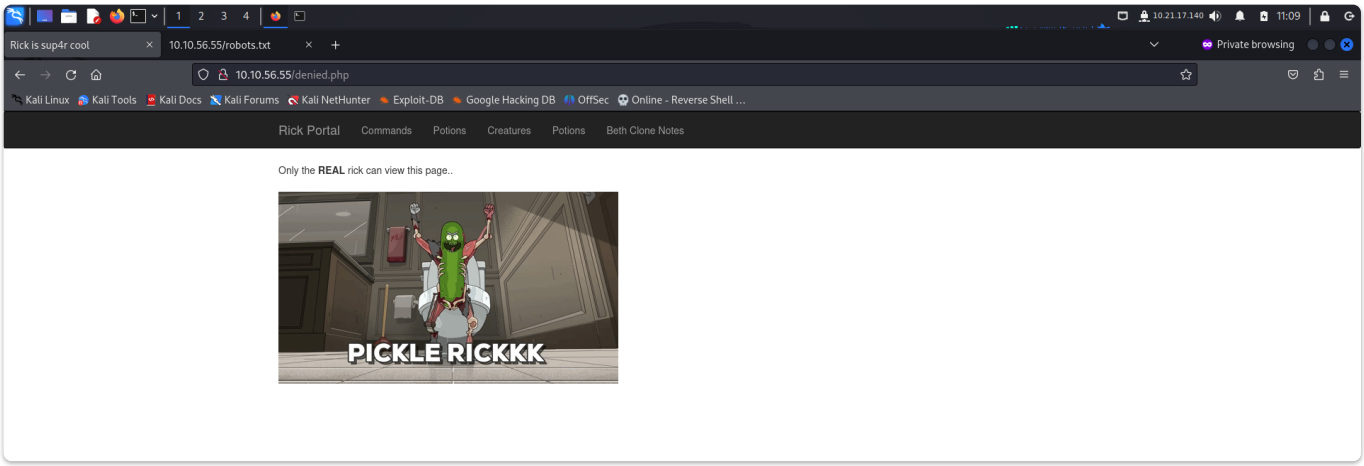
I tried logging in using the username I had found on the home page along with this text and gained access to a command panel.



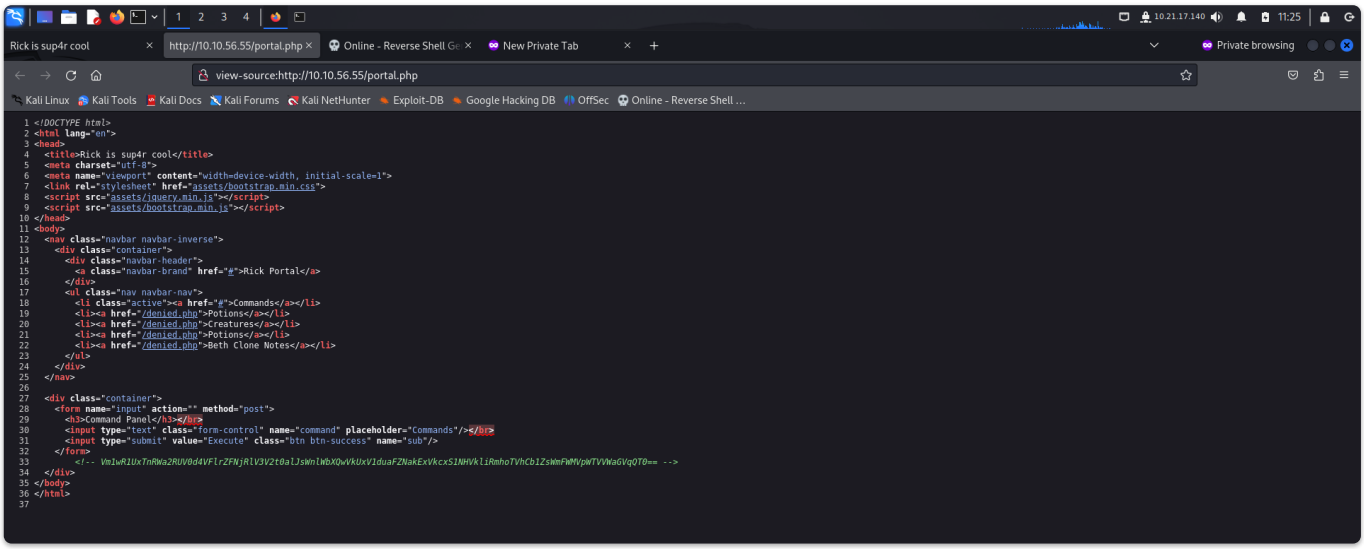
Using this panel, I executed whoami and received a response from the server.



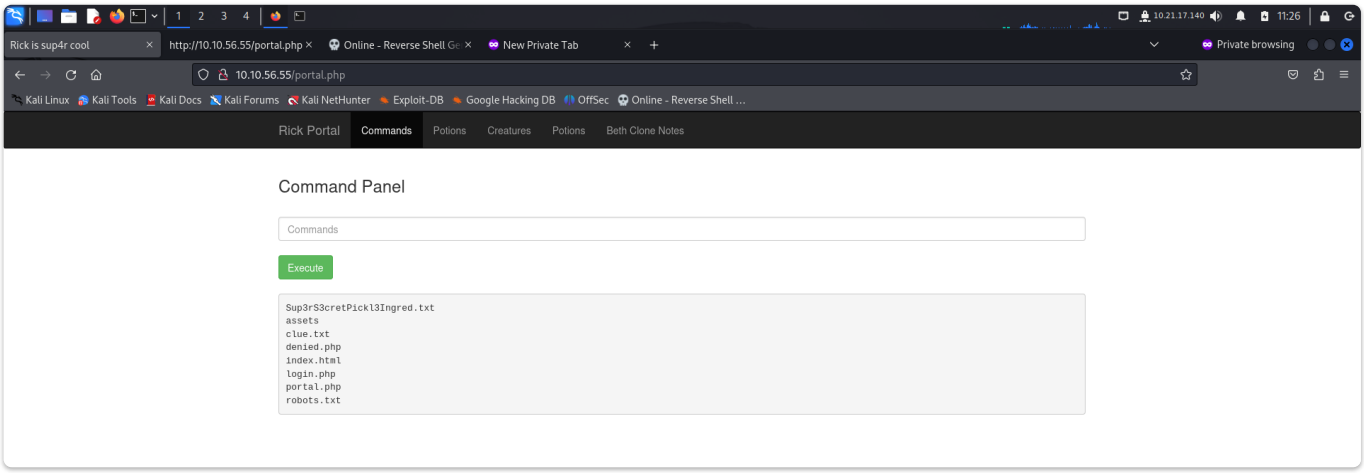
However, the other pages were inaccessible.



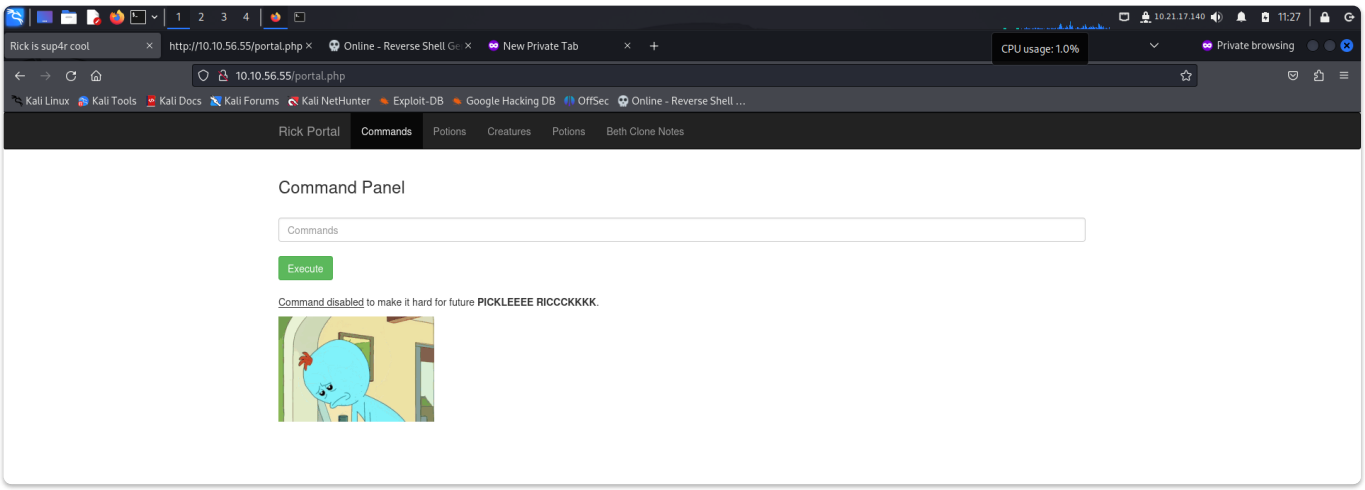
I viewed the source code of the command panel but found nothing interesting.



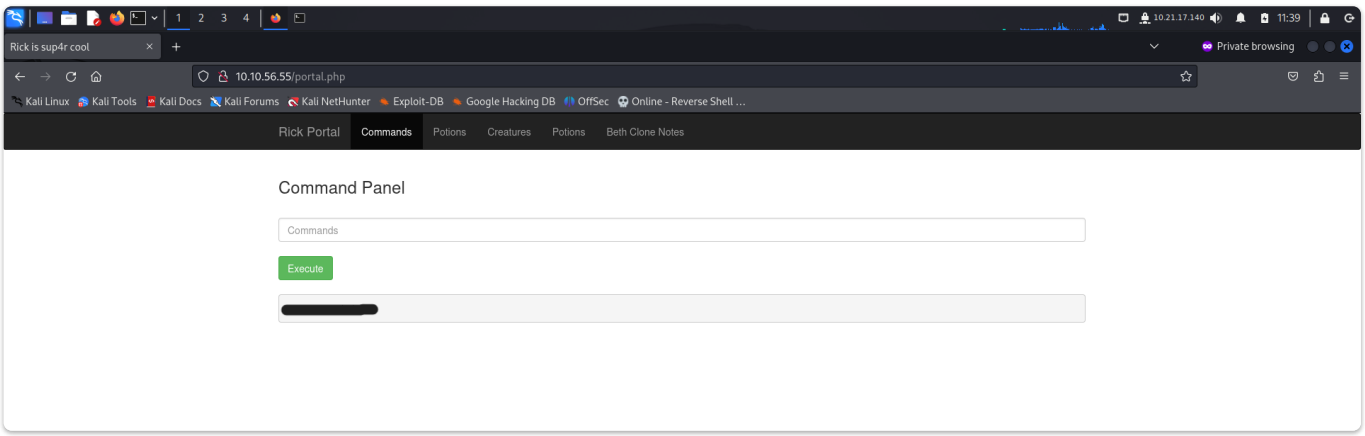
I then viewed the contents inside my folder by executing ls.



When I tried to read the ingredient, I encountered an error.



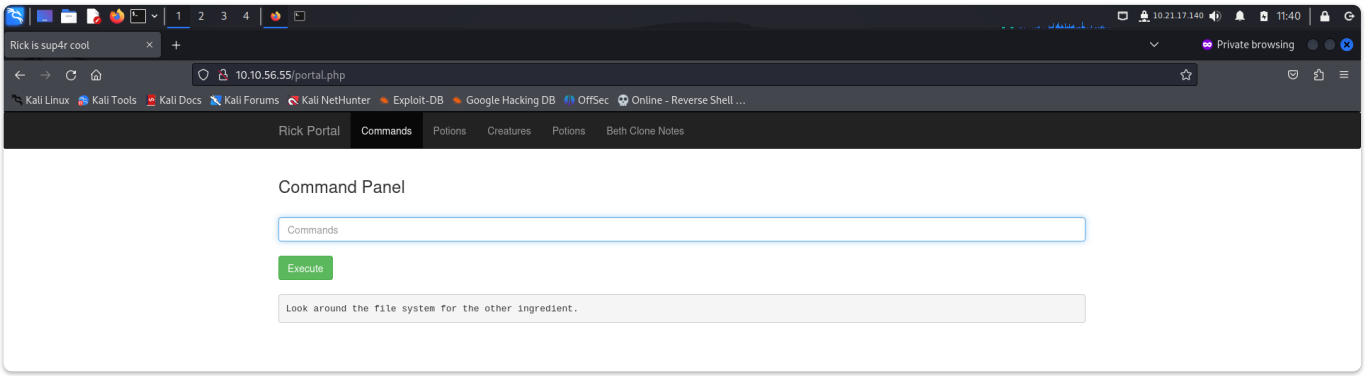
So I tried other ways to read it. Since it was present in the directory my page was located, I accessed it through the URL. Alternatively, even the command `less Sup3rS3cretPickl3Ingred.txt` worked.



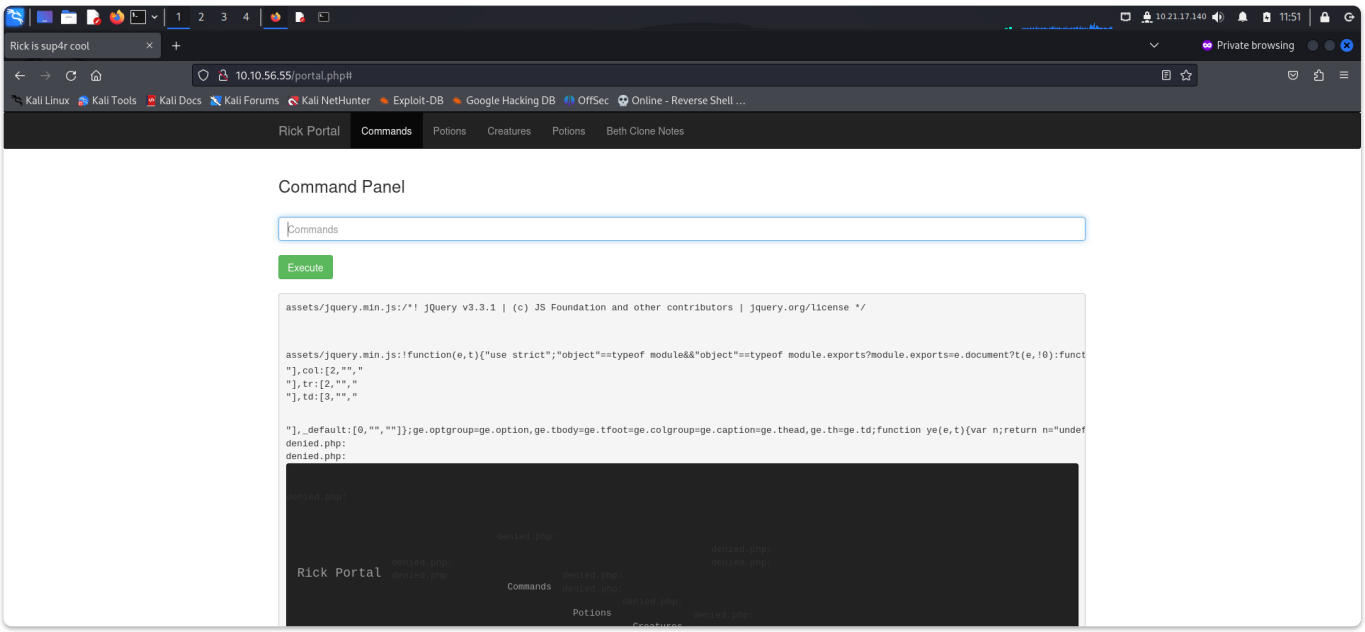
Hence, I obtained the first ingredient.

INGREDIENT 2

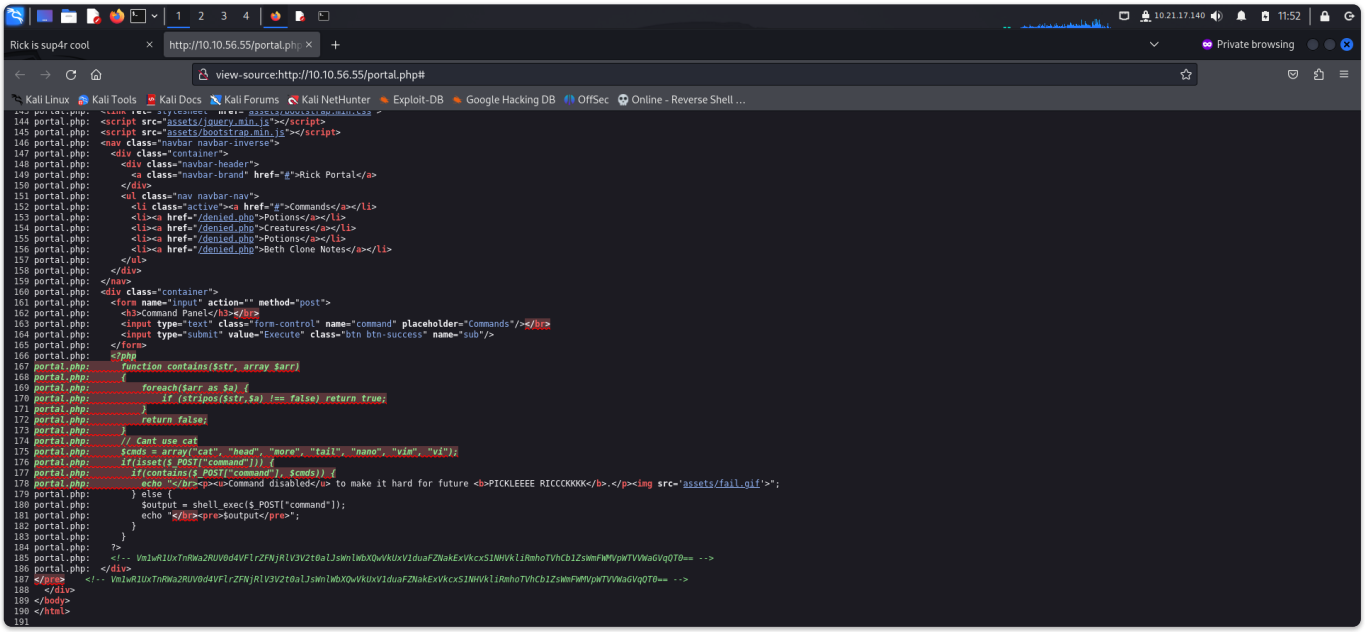
I looked at the *clue.txt* file for hints.



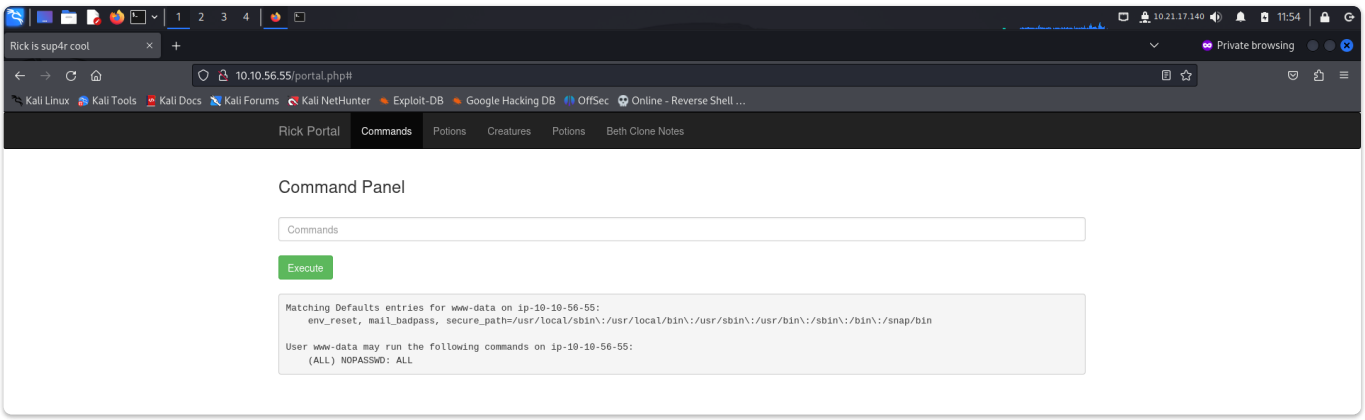
I executed `grep -R " "` to view all the codes in the current directory.



Upon viewing the source, I discovered the commands that weren't allowed to be used.

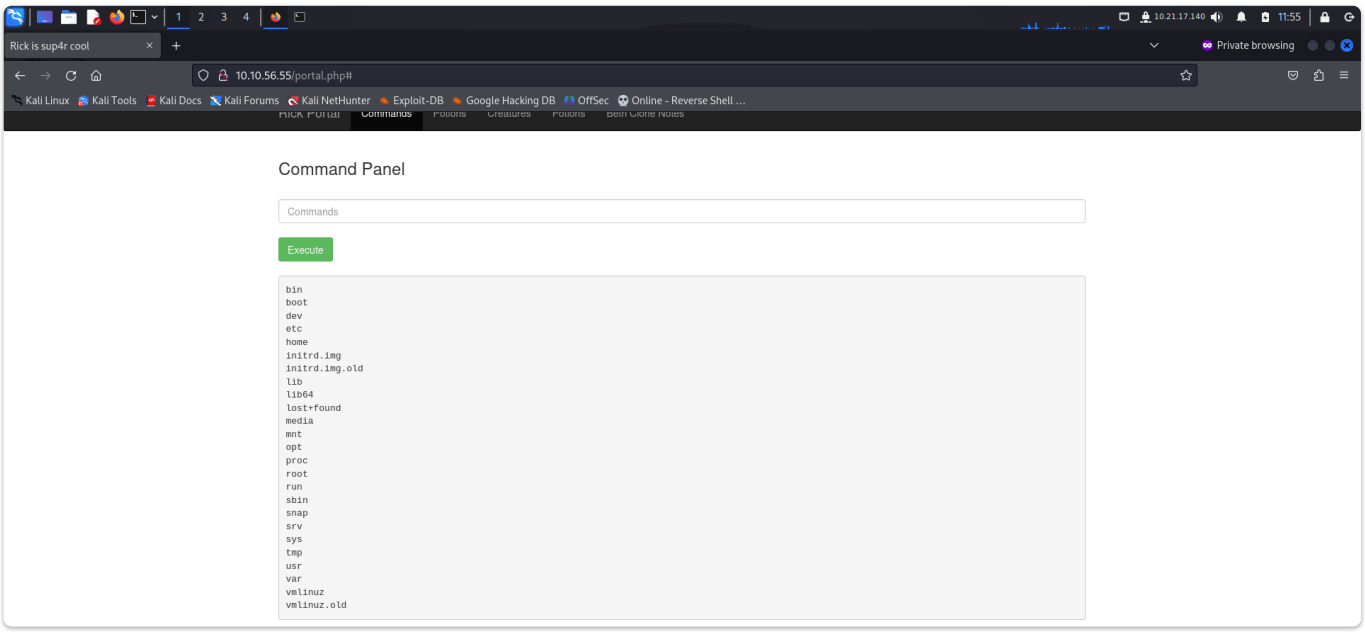


Since sudo wasn't restricted, I viewed my *sudo privileges* using sudo -l.

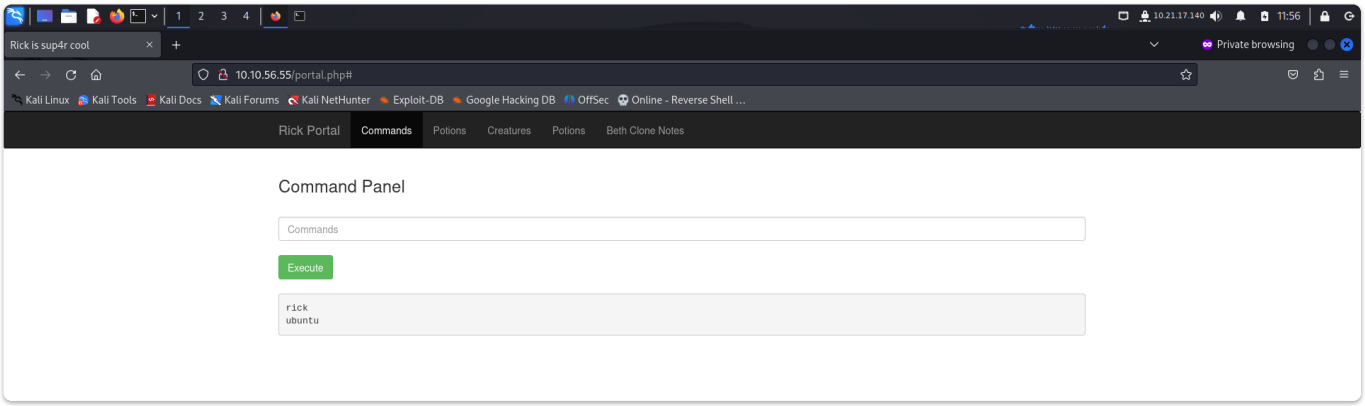


Hence, I was allowed to execute sudo without a password.

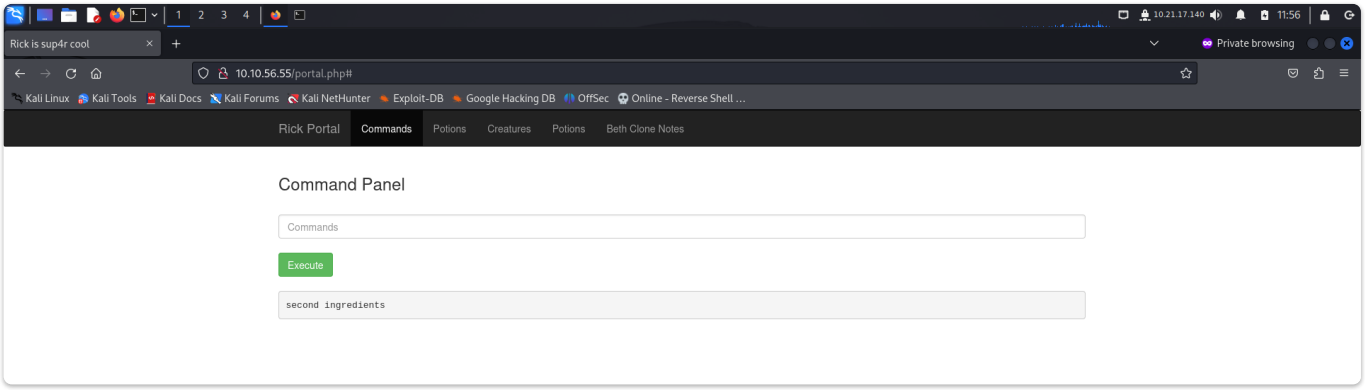
I executed ls ../../../.



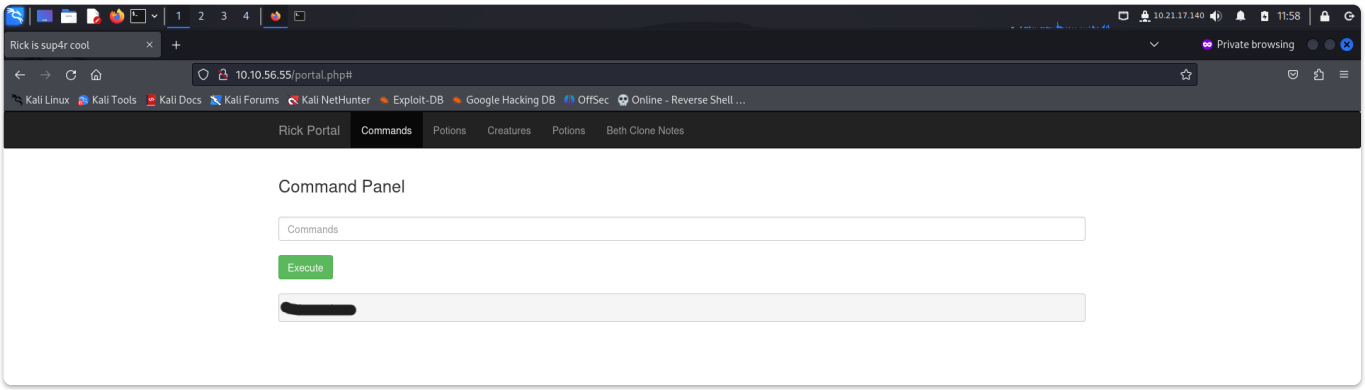
I then looked inside the home directory using ls ../../../home.



Then I looked inside *rick*.

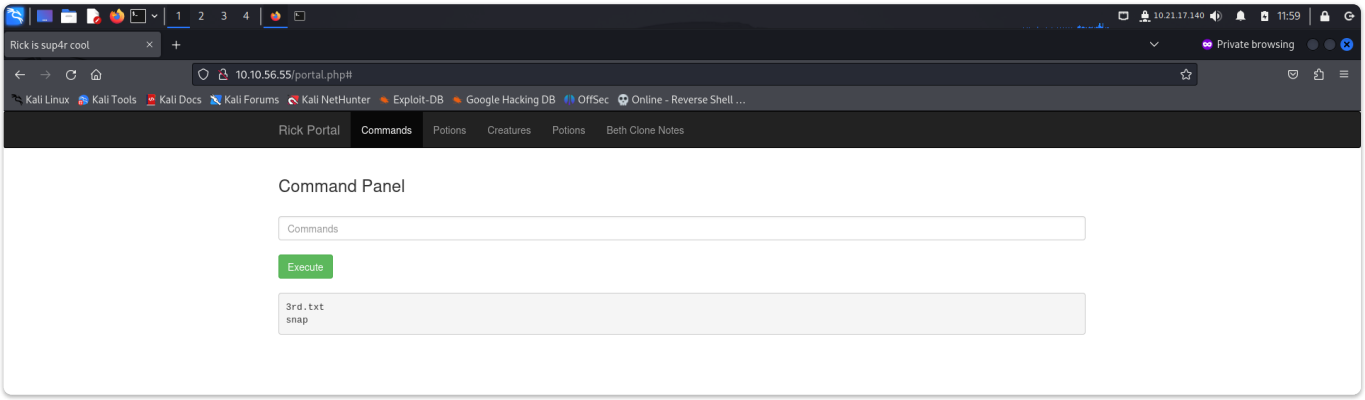


Finally, I read the second ingredient using less '../../../home/rick/second ingredient'.

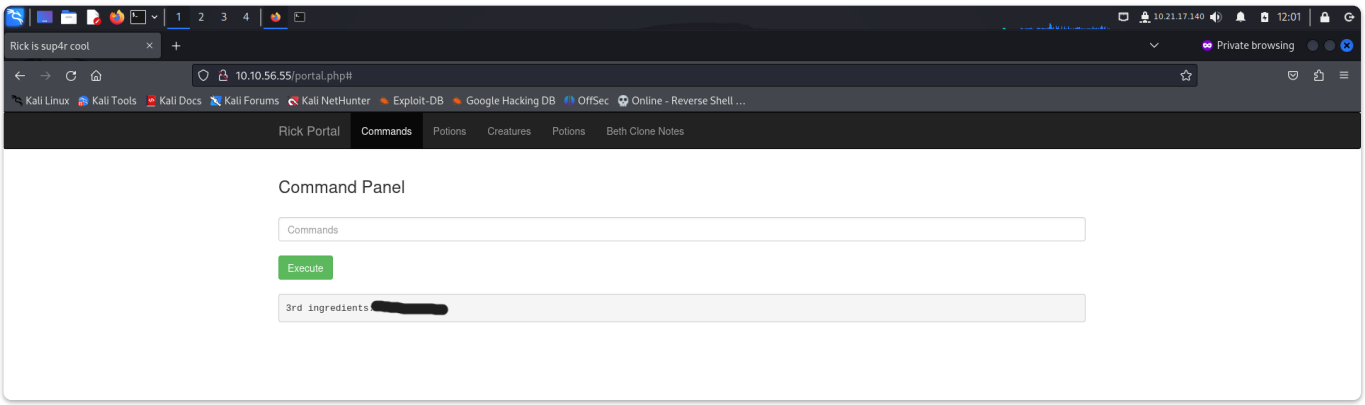


INGREDIENT 3

For the final ingredient, I looked inside the *root* directory using sudo ls ../../../root.



I then read this ingredient using sudo less '../../../root/3rd.txt'.



CLOSURE

Here's a summary of how I compromised the machine:

1. I collected login credentials through reconnaissance and used them to access the application.
2. Using the command panel, I retrieved the first ingredient from my current directory.
3. Similarly, I retrieved the second ingredient from the */home/rick* directory.
4. Finally, I obtained the final ingredient from the */root* directory using the sudo command.

That's it from my side, until next time :)