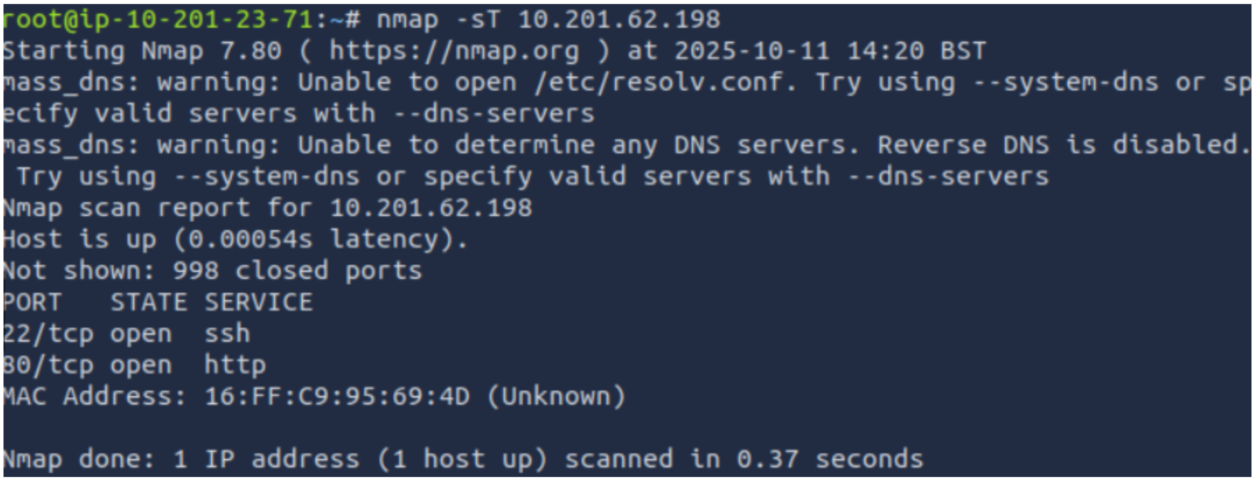
Pickle Rick CTF – TryHackMe

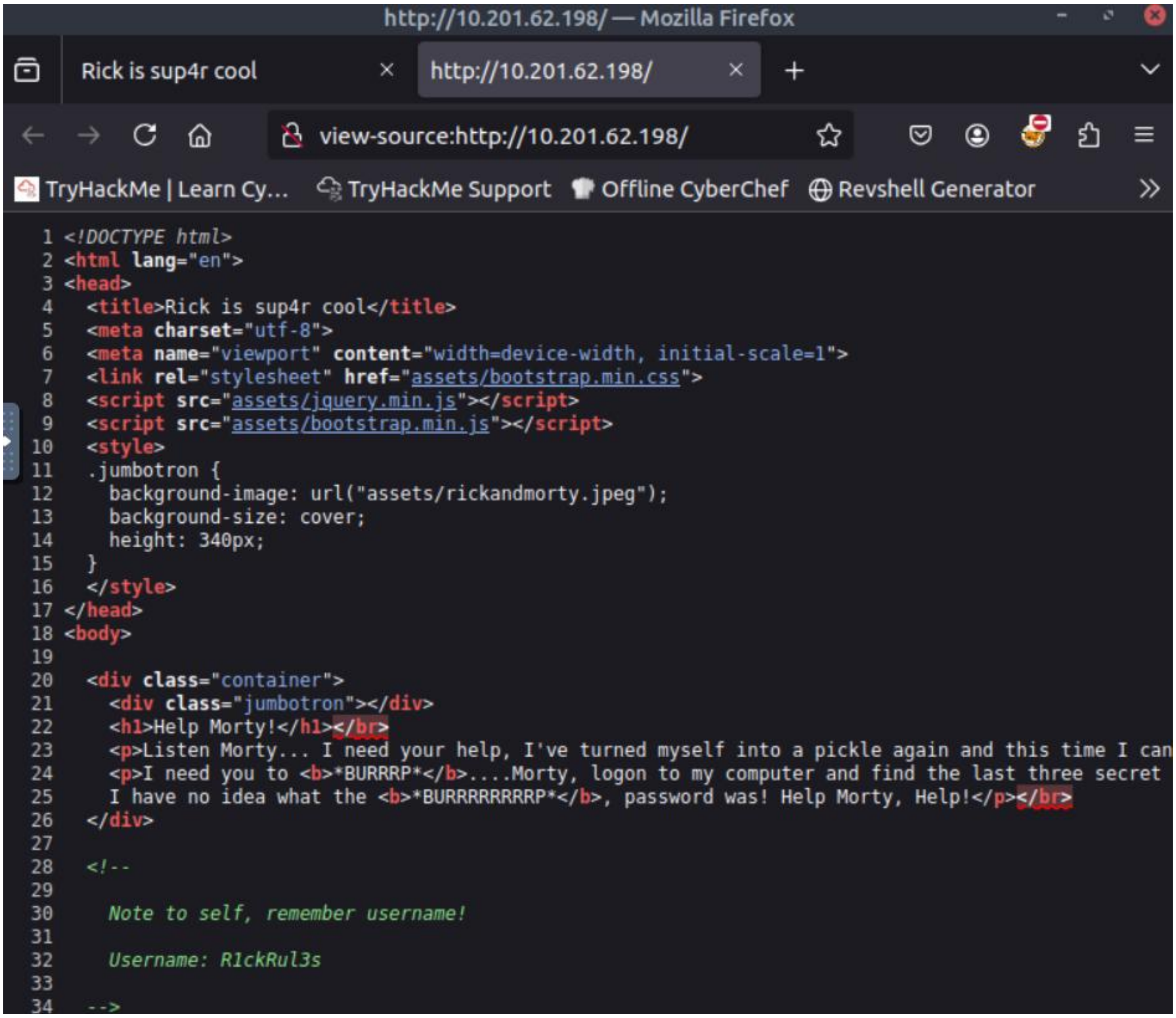
Completed: 10/11/2025

The Pickle Rick CTF is a Rick and Morty themed CTF hosted by TryHackMe where you are challenged to exploit a web server in order to find 3 flags. These flags are ingredients that are supposed to help Rick make a potion that will transform him back into a human. This is the first CTF I have ever completed, and it was incredibly valuable learning experience that taught me a lot!



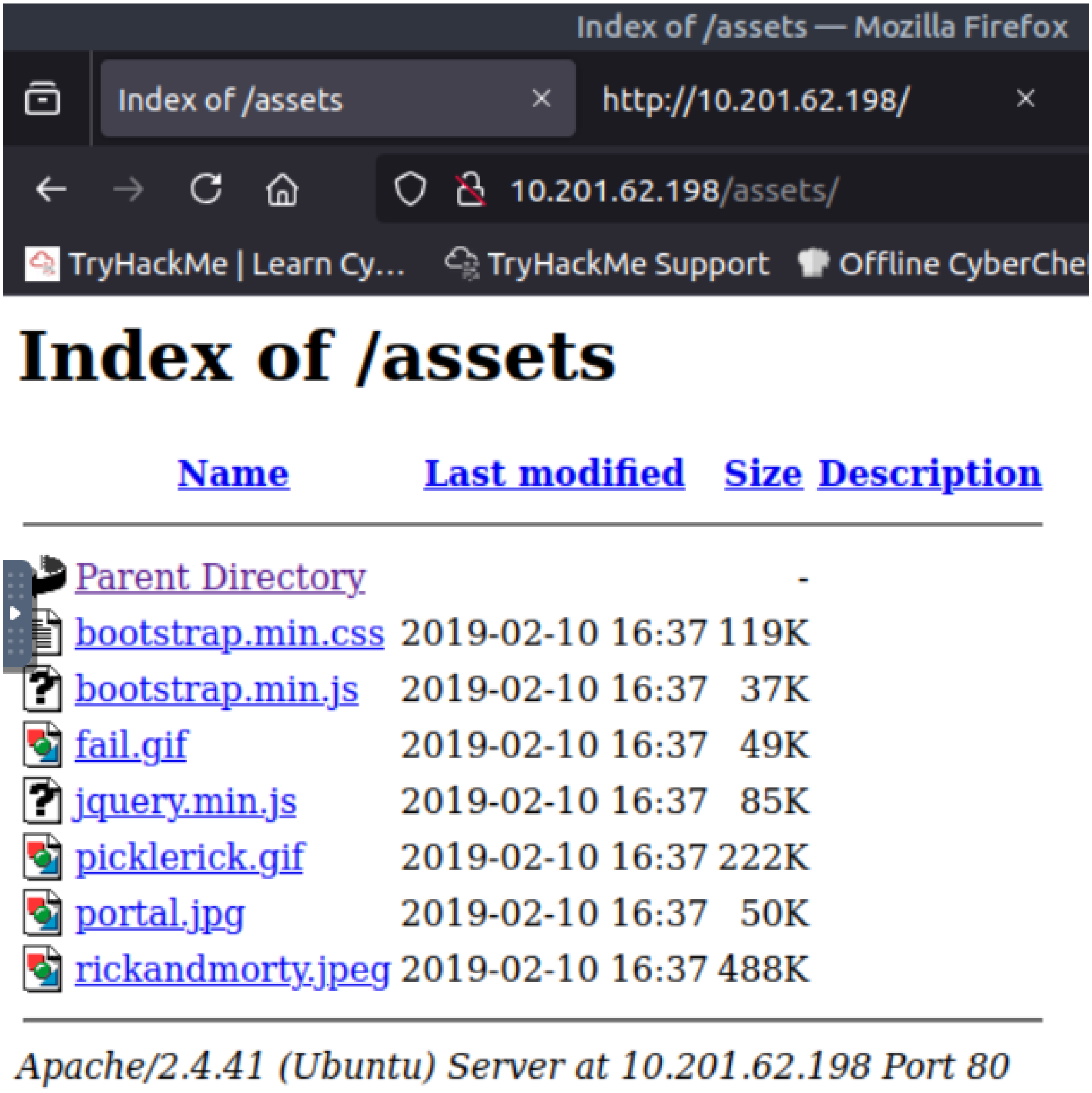
```
root@ip-10-201-23-71:~# nmap -sT 10.201.62.198
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-11 14:20 BST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or sp
ecify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.201.62.198
Host is up (0.00054s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 16:FF:C9:95:69:4D (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

I began with enumeration. I was provided with the target IP address (10.201.59.168), which I used to complete a port scan with Nmap. The port scan gave me plenty of useful information about the target machine. The machine was running on Ubuntu and had two ports open: port 22 (OpenSSH) and port 80 (HTTP).



```html
<!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
    <p>I need you to <b>*BURRRP*</b>....Morty, logon to my computer and find the last three secret
    I have no idea what the <b>*BURRRRRRRRP*</b>, password was! Help Morty, Help!</p></br>
  </div>

  <!--

    Note to self, remember username!

    Username: R1ckRul3s

  -->
```

Next up, I looked for information on the website that was being hosted by the machine. The webpage itself didn't say anything useful, but after a quick look at the source code, I found Rick's username: R1ckRul3s. I also found that the jquery and Bootstrap files are stored in a folder called "assets," so I decided to check if the folder was protected. The assets folder was not protected.

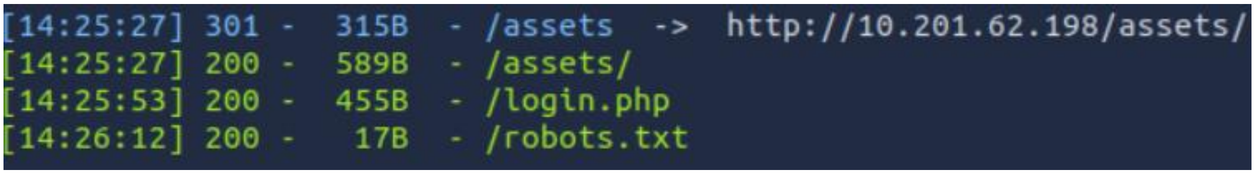


Index of /assets

Name	Last modified	Size	Description
Parent Directory		-	
bootstrap.min.css	2019-02-10 16:37	119K	
bootstrap.min.js	2019-02-10 16:37	37K	
fail.gif	2019-02-10 16:37	49K	
jquery.min.js	2019-02-10 16:37	85K	
picklerick.gif	2019-02-10 16:37	222K	
portal.jpg	2019-02-10 16:37	50K	
rickandmorty.jpeg	2019-02-10 16:37	488K	

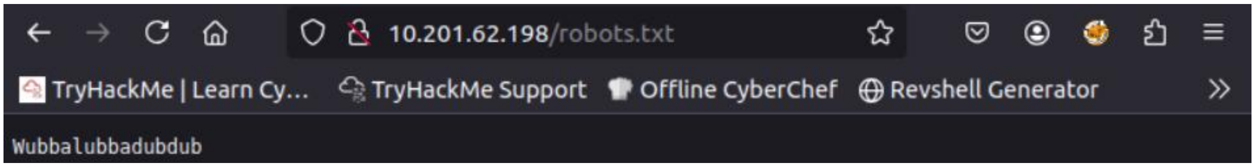
Apache/2.4.41 (Ubuntu) Server at 10.201.62.198 Port 80

A look at the assets folder showed me plenty of files that were being used for the website. The files were primarily images, CSS, or JavaScript files, which did not prove useful. As a result, I decided to try another method to find any hidden files.



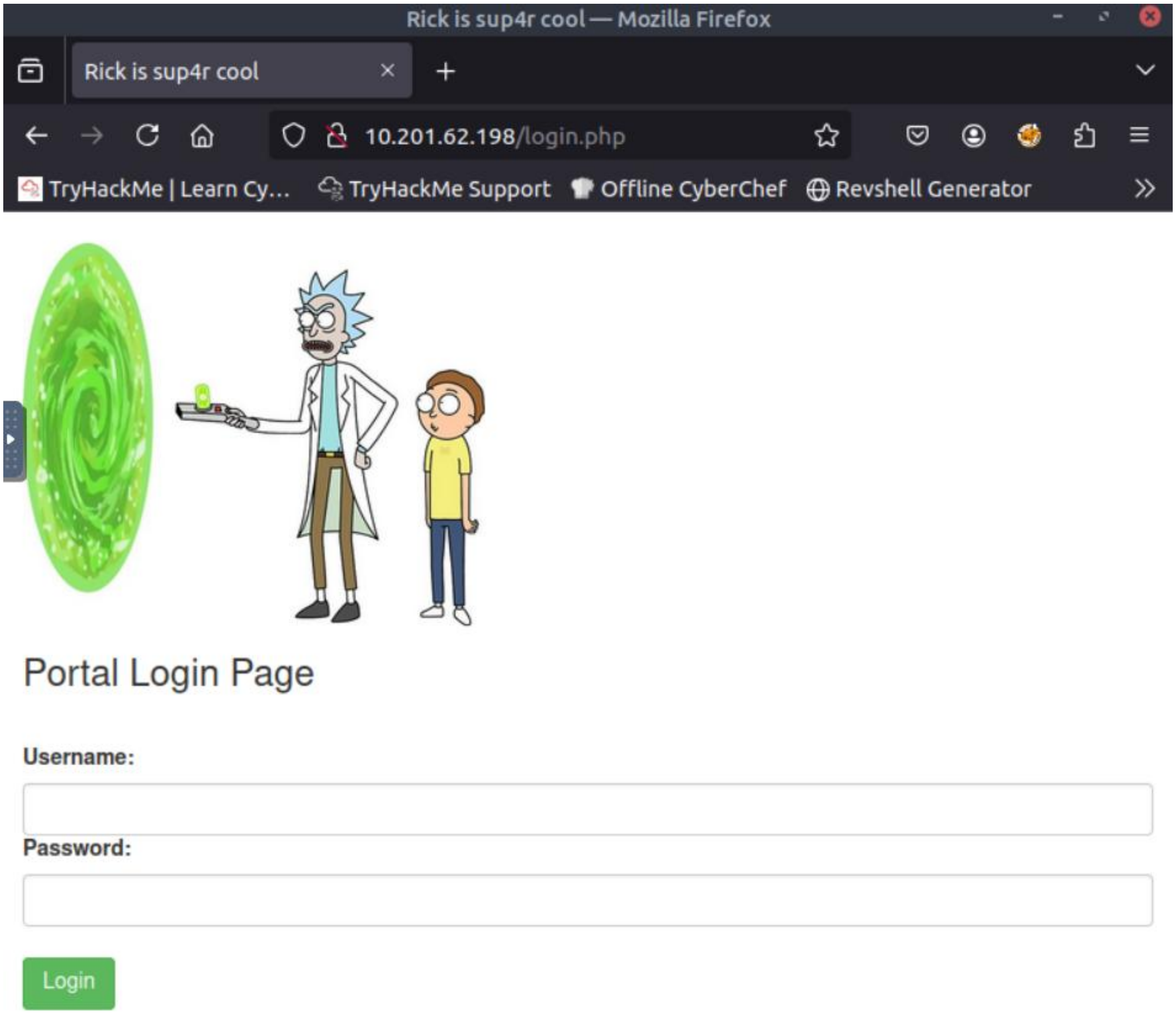
```
[14:25:27] 301 -   315B  - /assets  ->  http://10.201.62.198/assets/
[14:25:27] 200 -   589B  - /assets/
[14:25:53] 200 -   455B  - /login.php
[14:26:12] 200 -    17B  - /robots.txt
```

I used dirsearch, which told me that there was also a login page (login.php) and a text file (robots.txt).



```
Wubbalubbadubdub
```

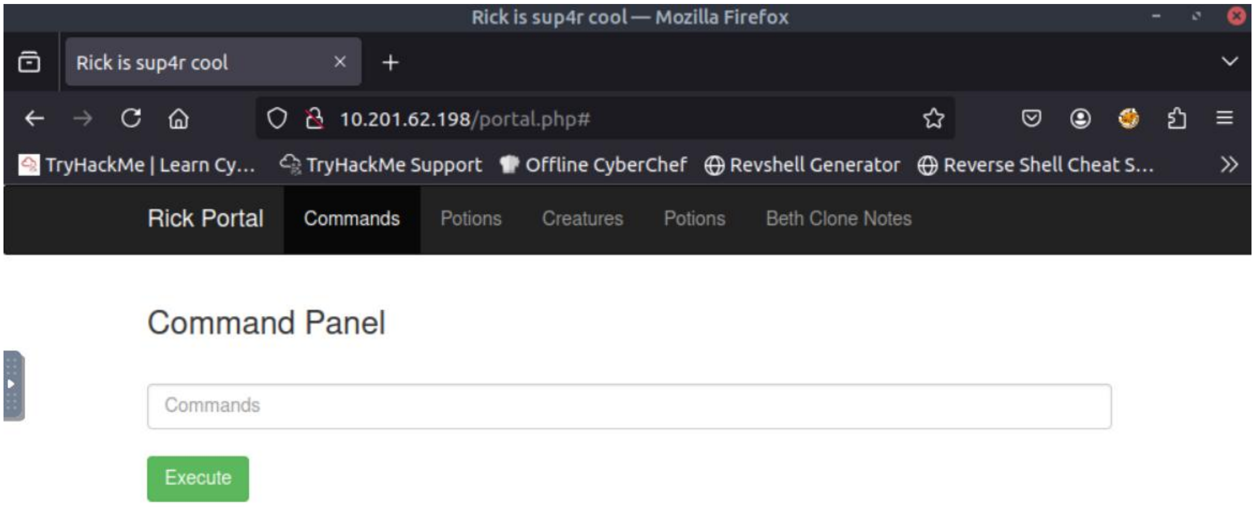
I began with a look at robots.txt, which simply contained the word "Wubbalubbadubdub." I took note of it since it might prove useful later.



Portal Login Page

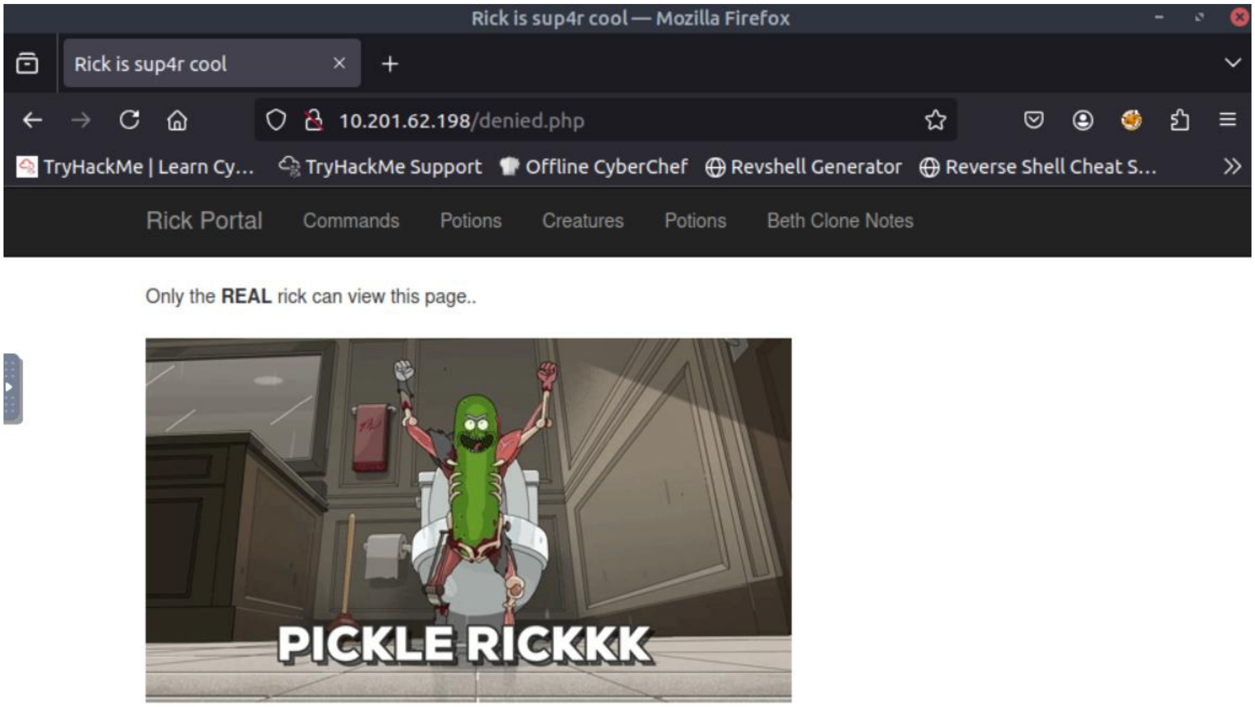
Username:

Password:



Command Panel

Next up, I checked login.php, which was a portal login page. I tried using “R1ckRul3s” as the username since I had found it hidden in the source code of index.html. I then tried using “Wubbalubbadubdub” as the password, and those credentials worked! I had successfully logged in to the portal.

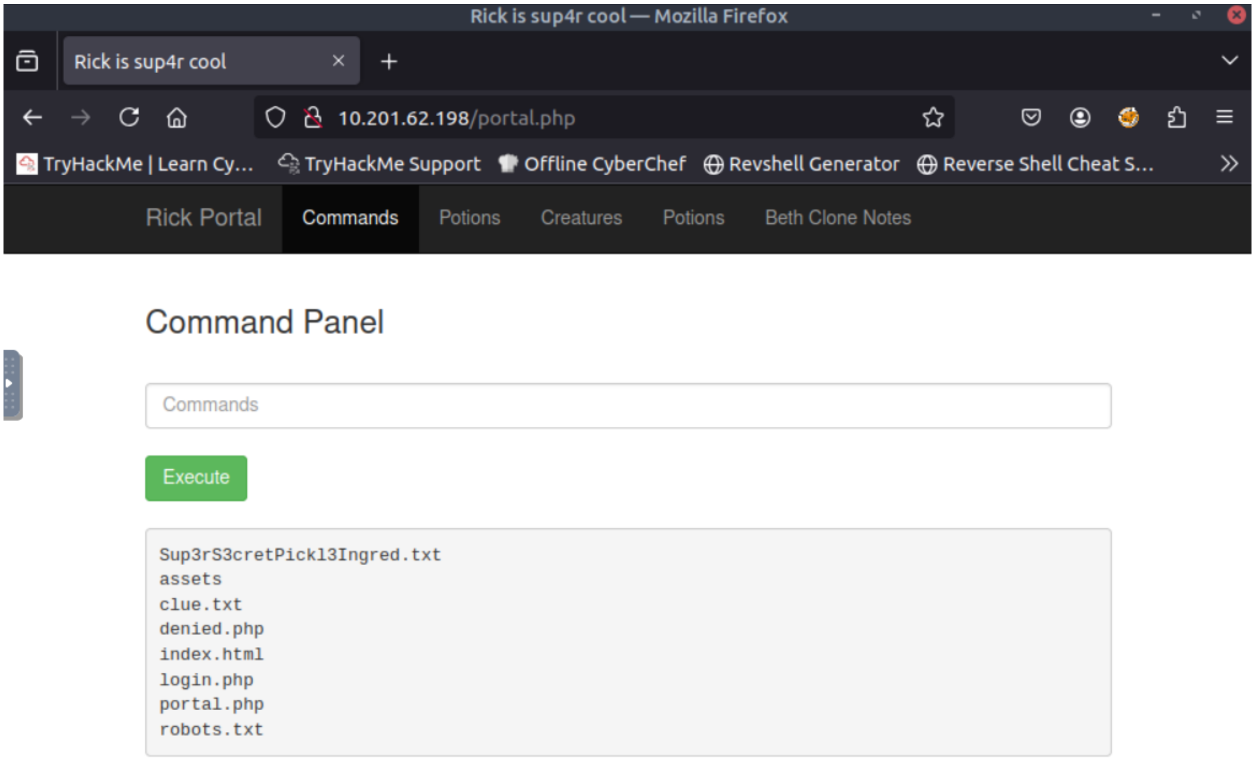


Rick is sup4r cool — Mozilla Firefox

10.201.62.198/denied.php

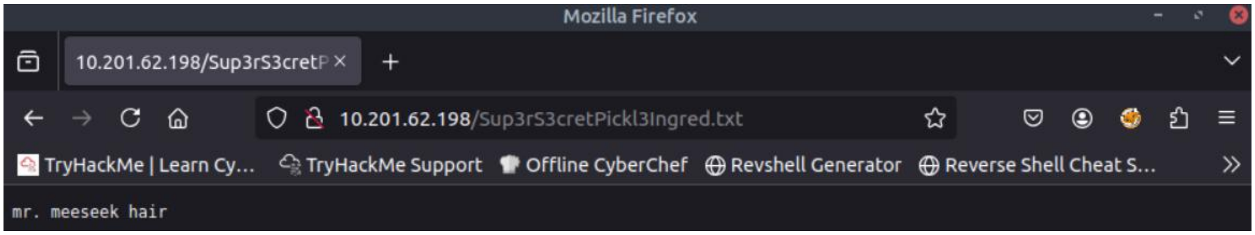
Only the **REAL** rick can view this page..

I was greeted with a command panel when I first logged in, but there were multiple other pages that I could access in the Rick portal. I could access Potions, Creatures, Potions (is this a duplicate?), and Beth Clone Notes. When I clicked on the pages, however, I was met with the message “Only the REAL rick can view this page..” I needed to try another method of accessing the pages to find the potion ingredients!



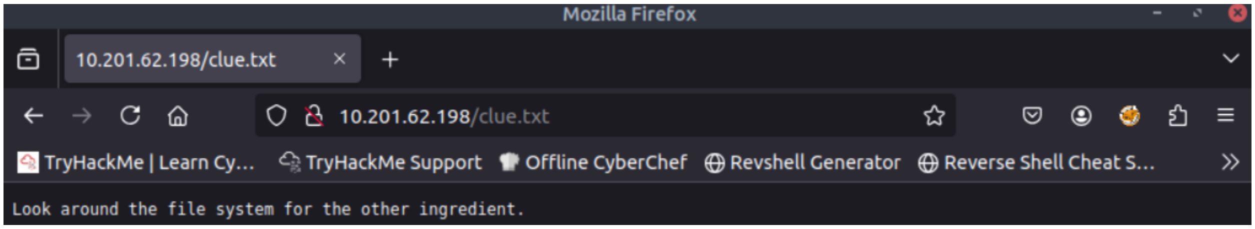
```
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```

My first idea was to use the command panel that I first saw after logging in. Using the "ls" command provided me with the same results I got using dirsearch, but there were two new files: Sup3rS3cretPickl3Ingred.txt and clue.txt.



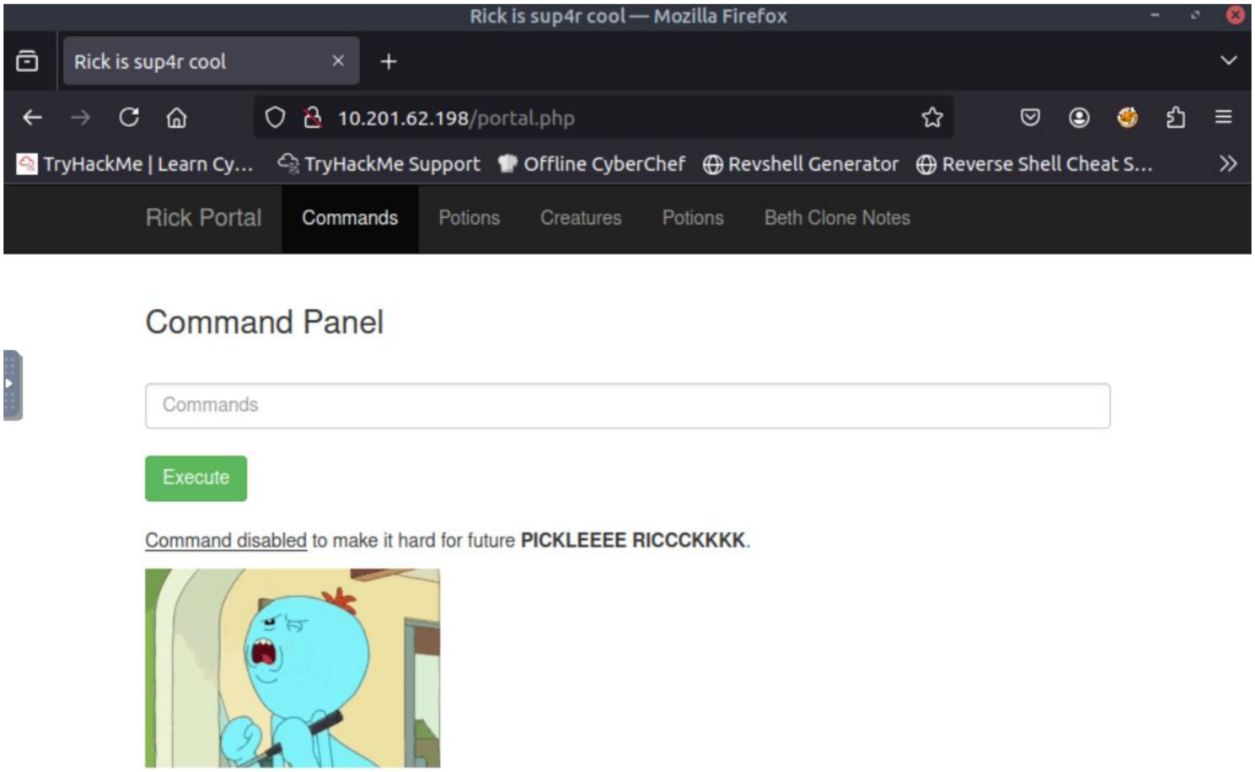
```
mr. meeseek hair
```

I started out by viewing Sup3rS3cretPickl3Ingred.txt. The page simply said "mr. meeseek hair."



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

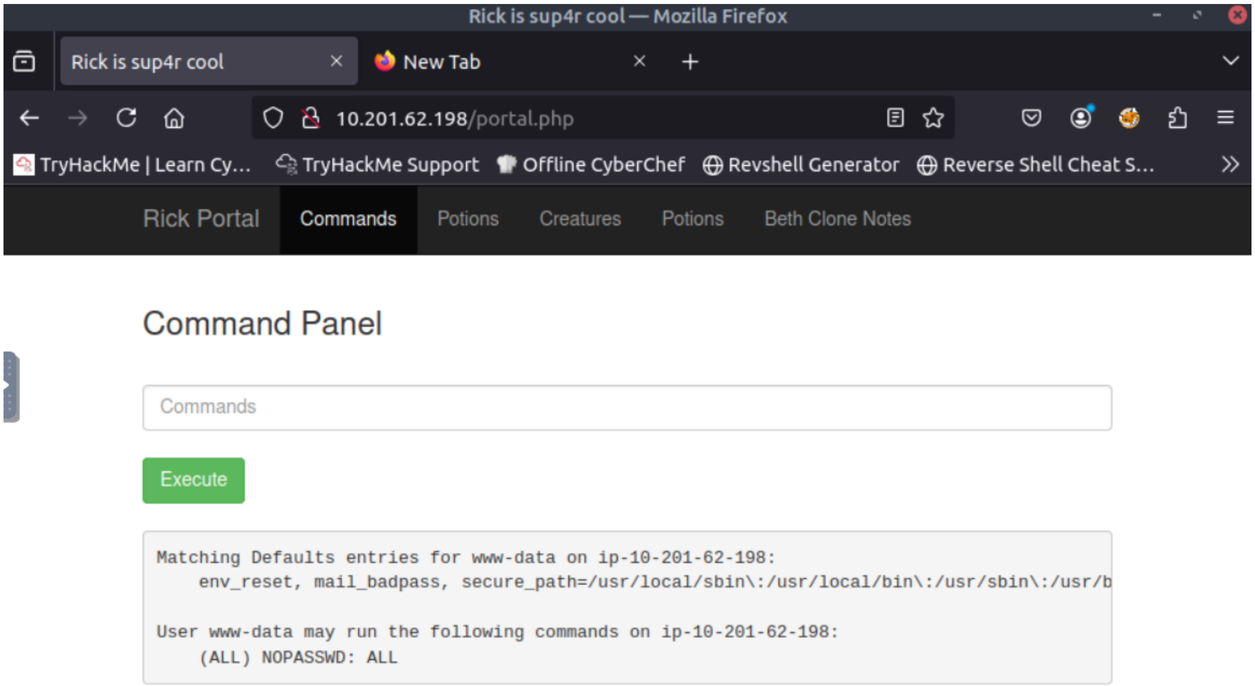
Next up, I visited clue.txt, which told me to "Look around the file system for the other ingredient."



Command Panel

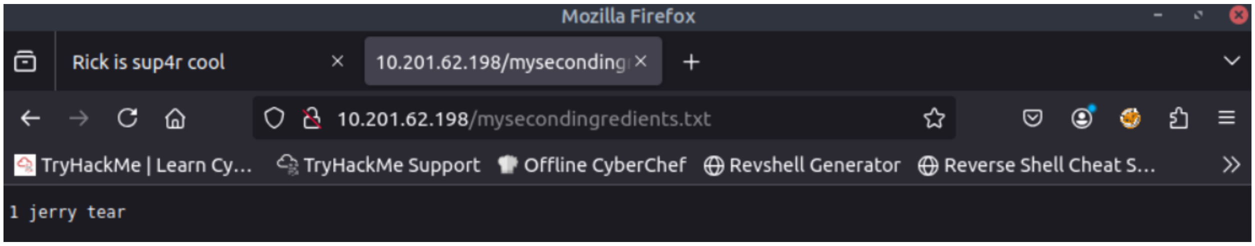
Command disabled to make it hard for future **PICKLEEEE RICCCKKKK**.

Since my Nmap scan had told me that the target machine was running Ubuntu, I decided to run the “ls /home” command to see what users are on the machine. I found two users: ubuntu and rick. The user rick will likely have the files I need, so I started by investigating that. I executed “ls /home/rick” and found the file “second ingredients.” I executed “cd /home/rick” and “cat ‘second ingredients’,” but was met with an error. It told me that the command was disabled, which meant that I couldn’t access the file through the command panel. I couldn’t access it through the web server, either, so I had to find another way.



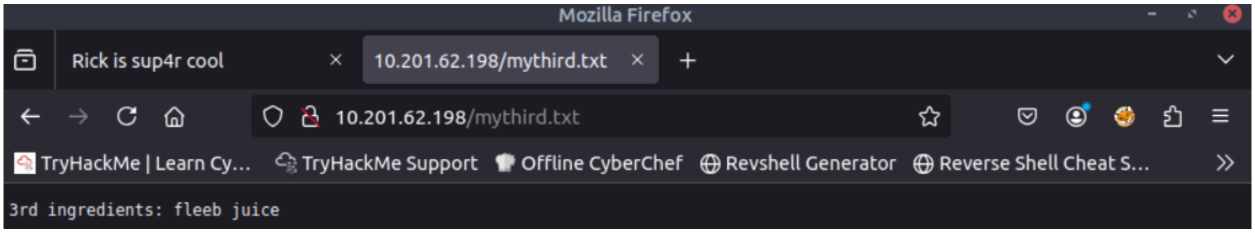
```
Matching Defaults entries for www-data on ip-10-201-62-198:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/b

User www-data may run the following commands on ip-10-201-62-198:
    (ALL) NOPASSWD: ALL
```

I checked to see if there was any way I could obtain root privileges. I ran “sudo -l” to find out, and as it turned out, I was able to do anything as long as I used the sudo command!



```
1 jerry tear
```

Any attempts to use the cat command didn't work, so I decided that I would try to view the file through the web browser like I had viewed Sup3rS3cretPickl3Ingred.txt. I copied 'second ingredients' from the /home/rick folder to another file, mysecondingredients.txt, and then I viewed mysecondingredients.txt in the web browser. This worked, and it told me that the second ingredient was "1 jerry tear." Only one ingredient left!



```
3rd ingredients: fleeb juice
```

I did some more digging through the file system, and when I viewed the /root folder, I found the file 3rd.txt, which wasn't viewable from the cat command. I applied the same strategy that I did for 'second ingredients' and found that the third ingredient was "fleeb juice."

And just like that, the CTF was completed! To turn Rick back into a human, he needed a mr.meeseek hair, 1 jerry tear, and fleeb juice. This was a really fun introduction to CTFs, and I had a lot of fun doing it!