PICKLE RICK(EASY)

This was an easy level machine based on web and linux exploitation.

THINGS I LEARNED IN THIS-

1. Connected to THM network using openvpn
2. Web exploitation tool gobuster(I already knew about this a little bit)
3. Bypassing basic filters for remote command execution.

SETUP-

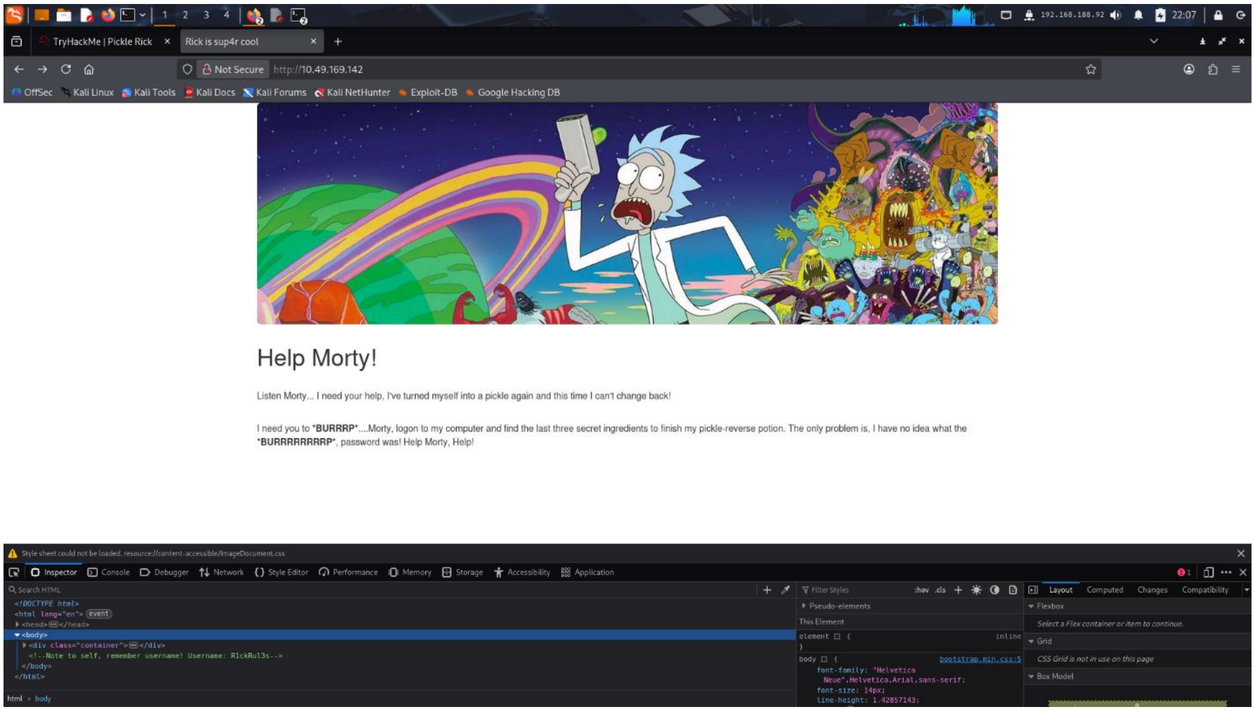
An website ip was provided, with description that we need secret ingredients to turn Pickle rick back to normal.

The page took me to a static website with similar description and a picture of cartoon/animation show rick and morty.

PROCESS-

My first instinct was to inspect the website and look at the code, cache, network, cookie, etc.

I found a username in the source code, so figured out I have to login somewhere and need password for it.



Help Morty!

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

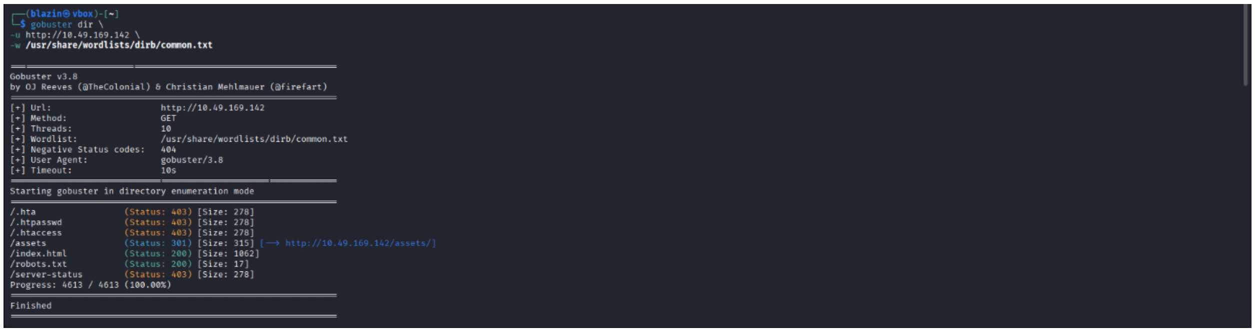
I need you to ***BURRRP***....Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is, I have no idea what the ***BURRRRRRRRP***, password was! Help Morty, Help!

Style sheet could not be loaded. resource://content-accessible/ImageDocument.css

```
<!DOCTYPE html>
<html lang="en"> event
<head>…</head>
<body>
  <div class="container">…</div>
  <!--Note to self, remember username! Username: R1ckRul3s-->
</body>
</html>
```

Then I proceeded to look for password in cookie,cache,etc. but didn’t find anything useful.

I did gobuster to find the login portal atleast. But I got 2 interesting things instead, an opening to /assets and a file named robots.txt.



```
┌──(blazin㉿vbox)-[~]
└─$ gobuster dir \
-u http://10.49.169.142 \
-w /usr/share/wordlists/dirb/common.txt

===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.49.169.142
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/assets               (Status: 301) [Size: 315] [--> http://10.49.169.142/assets/]
/index.html           (Status: 200) [Size: 1062]
/robots.txt           (Status: 200) [Size: 17]
/server-status        (Status: 403) [Size: 278]
Progress: 4613 / 4613 (100.00%)
===============================================================
Finished
===============================================================
```

I went to /assets first and found some gifs and js files, opened js files, did inspect the site and didn’t find anything useful.

Then proceeded to robots.txt, this contained random string, I thought this might be password and it didn’t look encoded.

After sometime being confused and trying to find the login page I used GPT and asked what I was doing wrong and then tried manually putting /login.php and got the login portal.

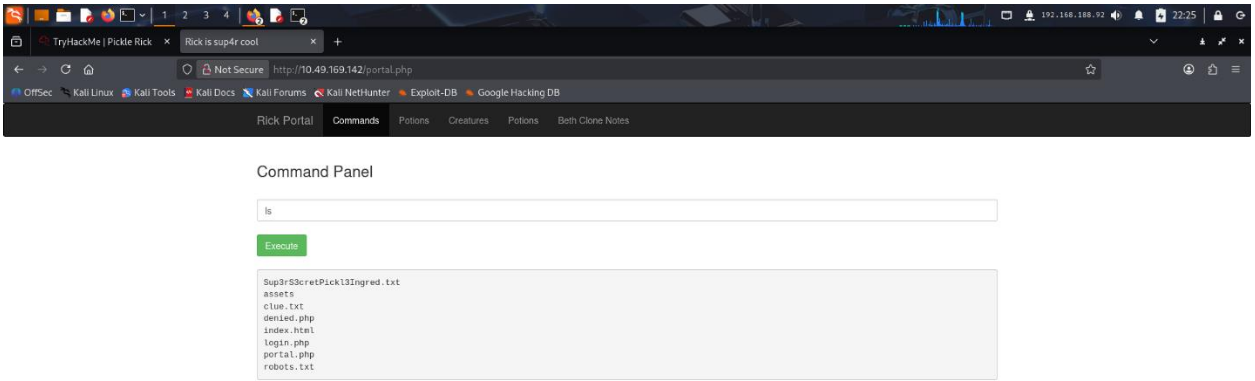
I used the username and password and and got into command execution portal site.

Only the command execution tab can be opened and all the other options were disabled.

I tried some basic commands like id, ls, whoami, interesting thing was it blocked certain keywords/commands like cat, so I had to use other commands other than that to open file and bypass the filter.

Doing ls gave the files in directory and one was named secret ingredient , one we would need.

I used head, it was block too, I did less and got the flag/ingredient.

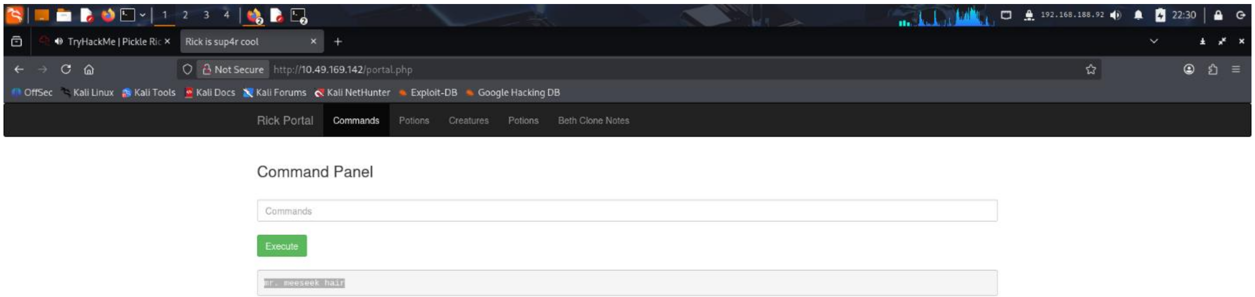


Command Panel

```
ls
```

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

The ingredient-



Command Panel

```
mr. meeseek hair
```

We needed to find 3 ingredients like that , but the challenge got completed after just putting the first ingredient and other 2 ingredients/flags were filled by themselves.

I then saw some write-ups about it , the other 2 flags required privilege escalation + forensics.

But the machine is quite old so I think that might be related to why we needed only one flag.

I will do my next machine that includes privilege escalation.