Rick and Morty CTF (TryHackme)

Target IP: **10.10.62.216**

Scan the target using **Nmap** to gather information on what ports and services are running on the target

```
root@ip-10-10-139-92:~# sudo nmap -sS 10.10.62.216

Starting Nmap 7.60 ( https://nmap.org ) at 2022-03-23 13:59 GMT
Nmap scan report for ip-10-10-62-216.eu-west-1.compute.internal (10.10.62.216)
Host is up (0.0014s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 02:72:E7:75:D9:F5 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds
```

This shows us that **Port 22 (SSH)** is open, and **Port 80 (HTTP)** is open.

Now that we know a website is living on the target, we scan the website using **dirb** to enumerate the directories and files inside the web server.

```
root@ip-10-10-139-92:~# sudo dirb http://10.10.62.216
```

```
---- Scanning URL: http://10.10.62.216/ ----
==> DIRECTORY: http://10.10.62.216/assets/
+ http://10.10.62.216/index.html (CODE:200|SIZE:1062)
+ http://10.10.62.216/robots.txt (CODE:200|SIZE:17)
+ http://10.10.62.216/server-status (CODE:403|SIZE:300)

---- Entering directory: http://10.10.62.216/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Wed Mar 23 14:02:52 2022
DOWNLOADED: 4612 - FOUND: 3
```

Dirb found the files, **index.html**, **robots.txt**, and **server-status**. Dirb also found a directory named **assets**.

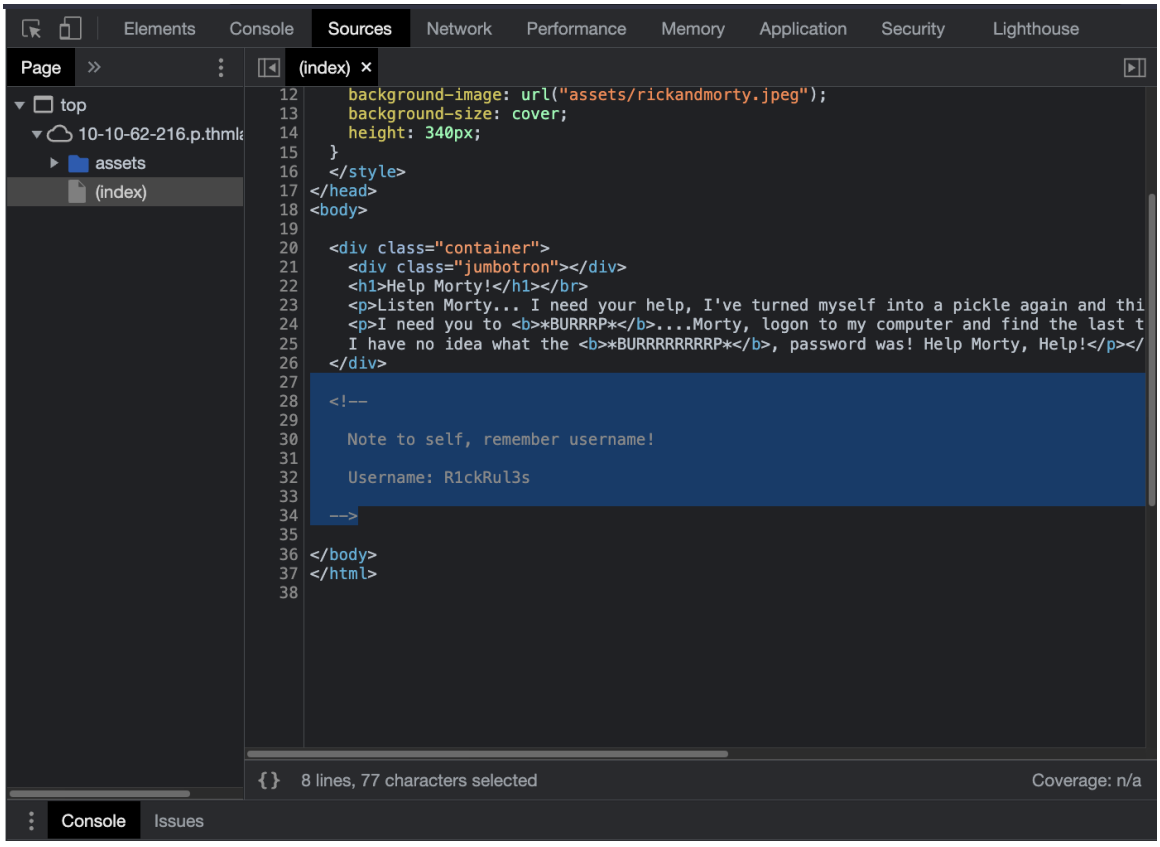
Navigating to the website displays the index page

Help Morty!

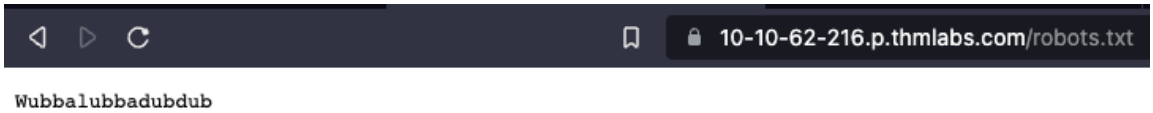
Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!

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!

Inspecting this with the developer tools leads you to find a username



Viewing the **robots.txt**



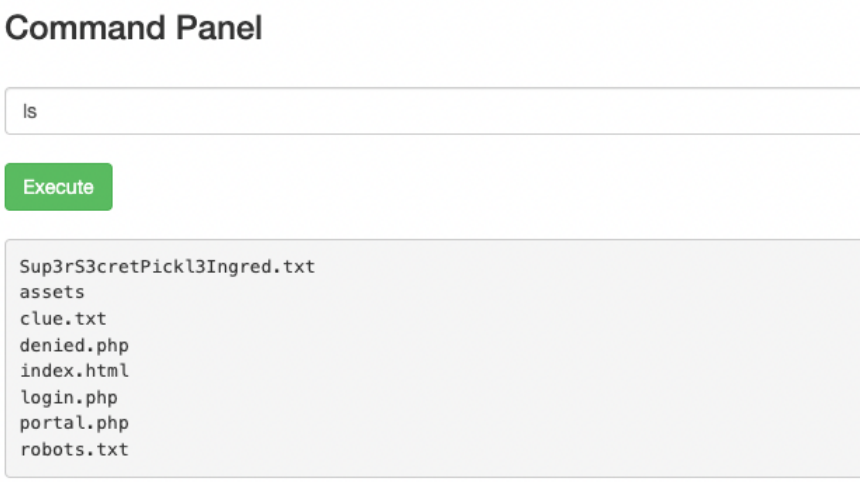

```
Wubbalubbadubdub
```

This looks like it could be a password

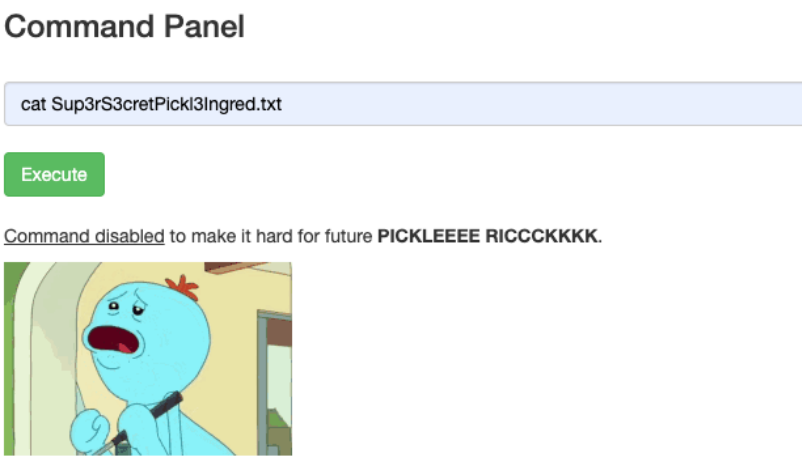
Using **Nikto** to scan the web application

```
root@ip-10-10-139-92:~# sudo nikto -host 10.10.62.216
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          10.10.62.216
+ Target Hostname:    ip-10-10-62-216.eu-west-1.compute.internal
+ Target Port:        80
+ Start Time:         2022-03-23 14:08:21 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0x426 0x5818c
cf125686
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ "robots.txt" retrieved but it does not contain any 'disallow' entries (which i
s odd).
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD
+ Cookie PHPSESSID created without the httponly flag
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 6544 items checked: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2022-03-23 14:08:30 (GMT0) (9 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

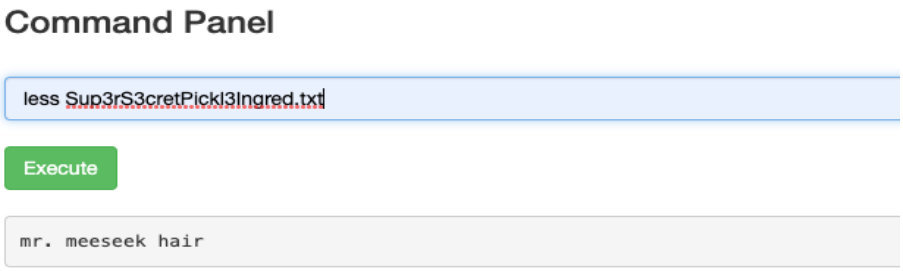
Navigating to the **login.php** page that Nikto found and entering in the username and password we got from robots.txt



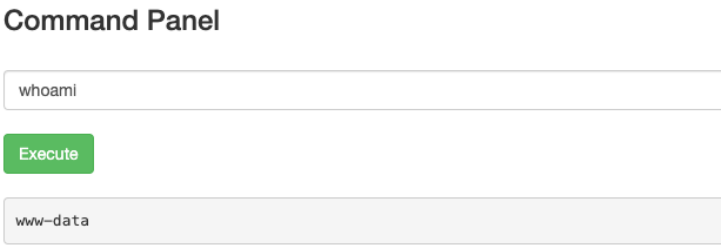
Trying to **cat Sup3rS3cretPickl3Ingred.txt**



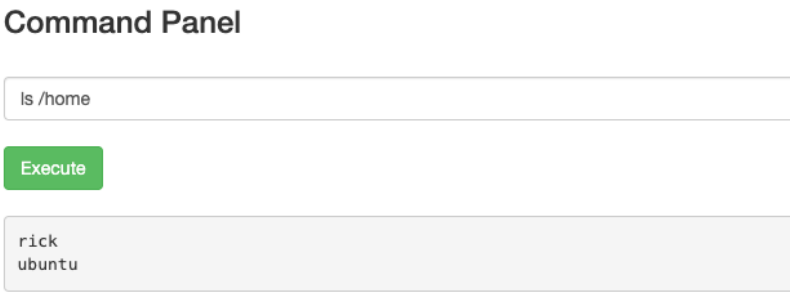
Since the cat command seems to be disabled, we need an alternative, **less** can be used for this.



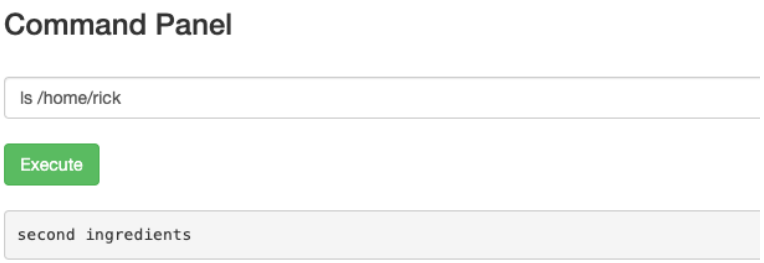
We now have the first flag, now to see what user account you're running commands on, run **whoami**



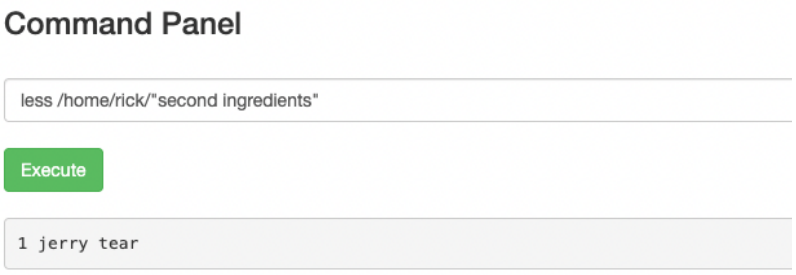
To get the users on the home directory, **ls /home**



We have two users, **rick** and **ubuntu**. LS-ing the rick users directory



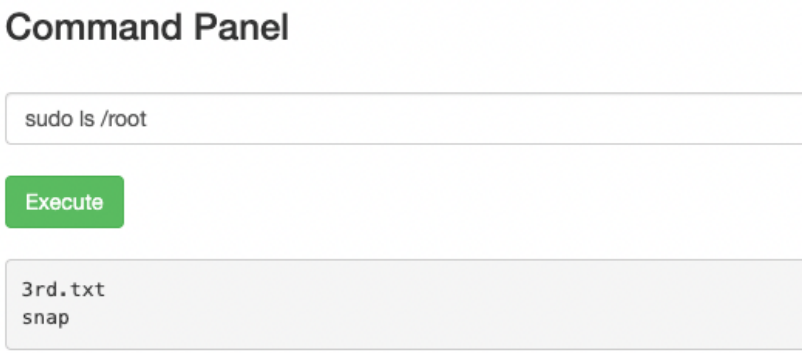
Less the second ingredients directory



We now have the second ingredient.

To view what commands the user is able to access, run **sudo -l**

From this output we're able to see that sudo commands do not require a password. Therefore we can directly access the root directory by doing **sudo ls /root**



Less the 3rd flag to complete the CTF and get all 3 flags