Pickle Rick CTF TryHackMe

Type: Easy

This document is my approach to solving the **pickle rick capture the flag**

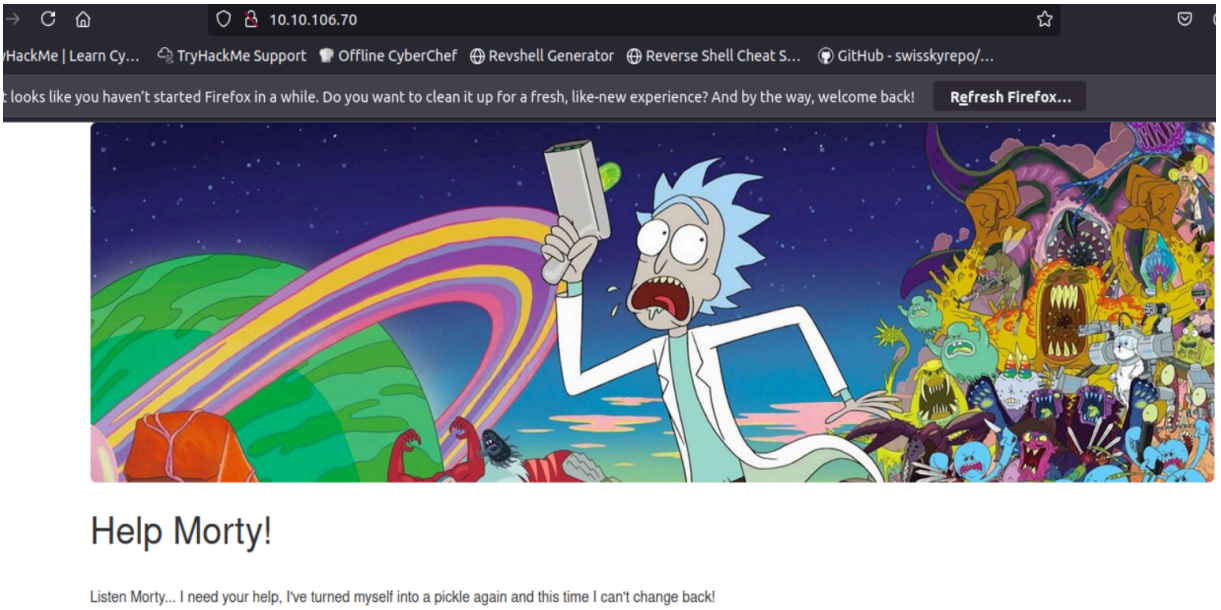
About Pickle Rickle CTF

This CTF theme is based on the **Rick and Morty TV show.**
The requirements of this CTF is to exploit a web server and find these 3 ingredients (flags).

Step 1: Start the machine

Step 2: Copy the ip address to web browser

This ip address contains a website which is running on http port 80



When we look up the source code of this website , we get username as commented.

```
<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>
```

So username is **RickRul3s**

Step 3: We need to find the login page of the website

Inorder to find the login page of the website , we need to directory bruteforce the website. In this CTF i use **dirb** tool to do it.
This is the initial dirb command i used to check.

```
root@ip-10-10-190-205:~# dirb  http://10.10.106.70/ -w /usr/share/wordlists/dirb/big.txt
```

```
root@ip-10-10-190-205:~# dirb  http://10.10.106.70/ -w /usr/share/wordlists/dirb/big.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Jul 11 09:57:36 2025
URL_BASE: http://10.10.106.70/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Stopping on warning messages

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.106.70/ ----
==> DIRECTORY: http://10.10.106.70/assets/
+ http://10.10.106.70/index.html (CODE:200|SIZE:1062)
+ http://10.10.106.70/robots.txt (CODE:200|SIZE:17)
+ http://10.10.106.70/server-status (CODE:403|SIZE:277)
```

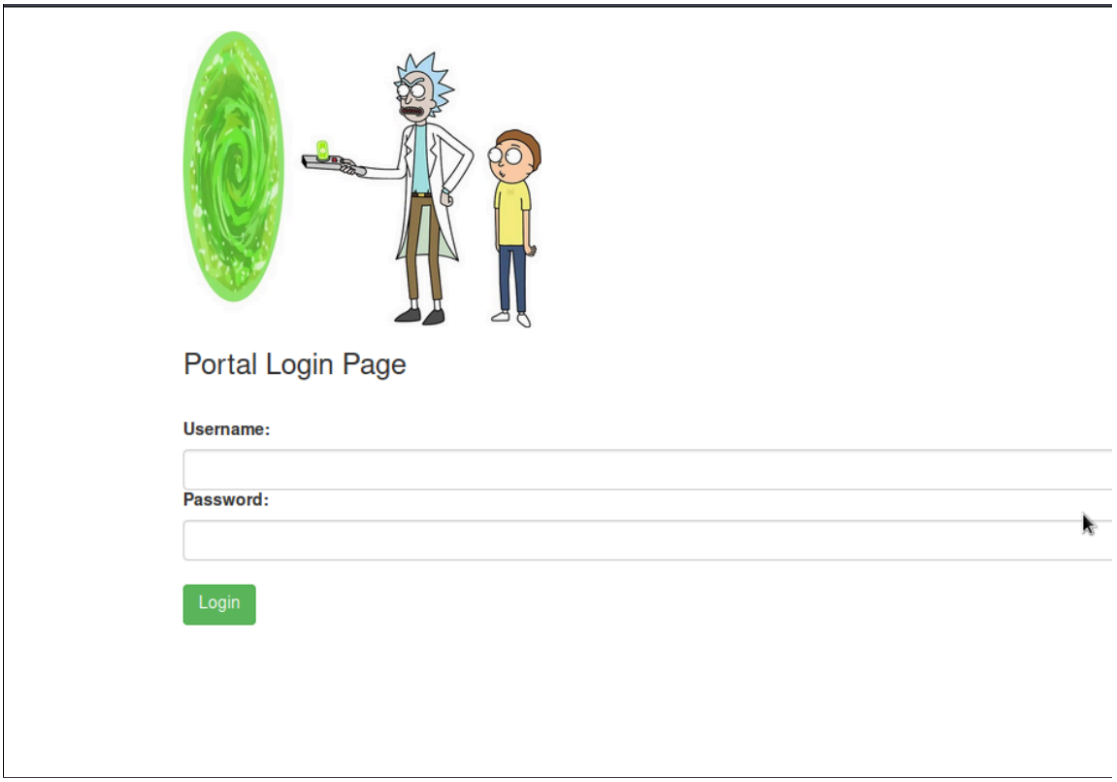
So we got the directories **assets, server-status and robots.txt**
But we didn't get the **website login directories.**

Inorder to get the login directories we need to use -X flag of dirb tool to add different file extensions such as **php,js,**...

```
DOWNLOADED: 9224 - FOUND: 3
root@ip-10-10-190-205:~# dirb  http://10.10.106.70/ -w /usr/share/wordlists/dirb/big.txt -X .js,.php

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Jul 11 09:58:03 2025
URL_BASE: http://10.10.106.70/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Stopping on warning messages
EXTENSIONS_LIST: (.js,.php) | (.js)(.php) [NUM = 2]

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.106.70/ ----
+ http://10.10.106.70/denied.php (CODE:302|SIZE:0)
+ http://10.10.106.70/login.php (CODE:200|SIZE:882)
+ http://10.10.106.70/portal.php (CODE:302|SIZE:0)

-----------------
```

So we got other directories **/denied.php, /login.php, /portal.php**

When we go through **login.php** we got our website

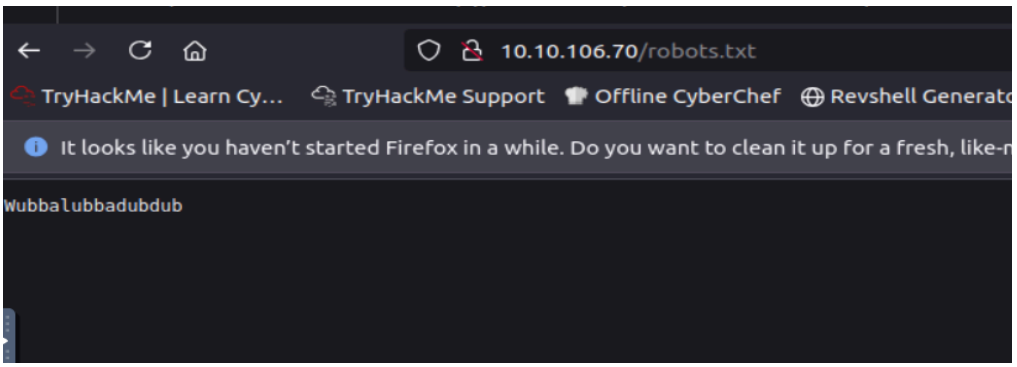


As of now we only got the username, not password. Inorder to find password we need to look other directories for clues.

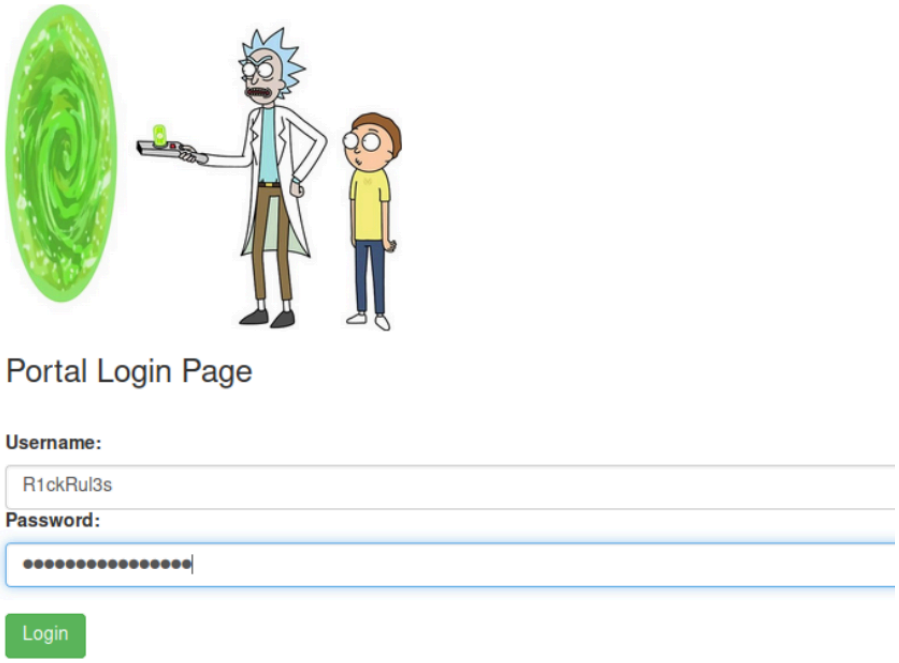
Step 4: Find the password

Currently we have **portal.php**, **denied.php** , **assets**, **server-status** and **robots.txt** to look.

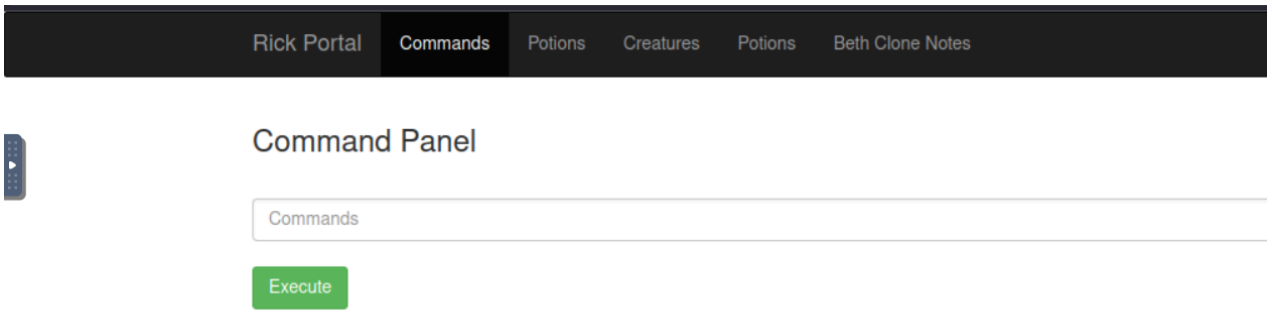
First Im going to look into robots.txt



We got random string , we need to check whether this is password or not

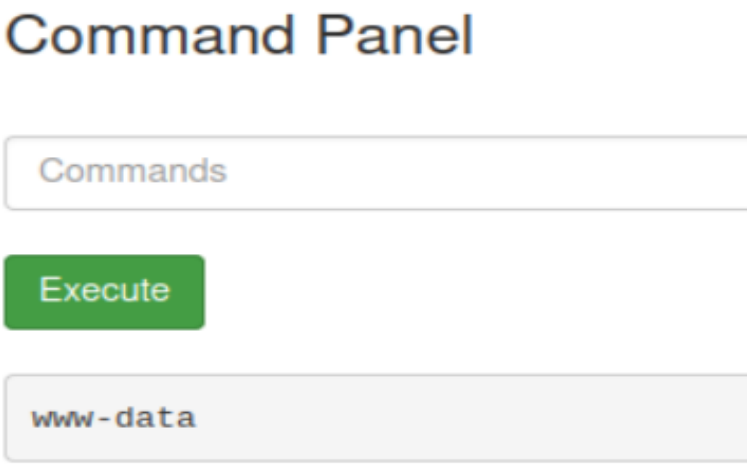


So we successfully login with that random string, so it is the password.



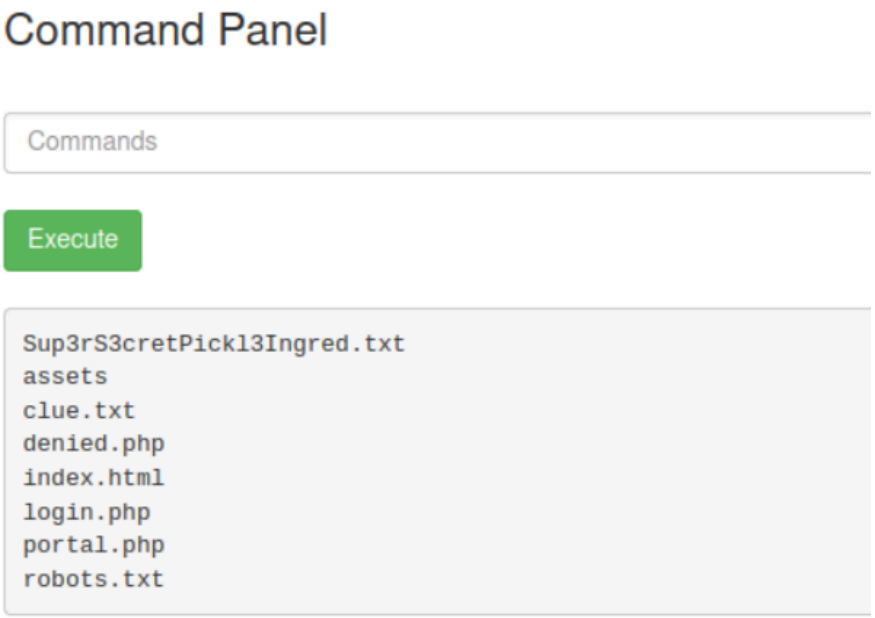
In this web interface, there is a command panel, we can execute commands here.
We need to try some **linux commands** to test it.

$ whoami



So the linux commands , so its basically a webshell. We are the user **www-data**, so we have access to all the permissions of this user.

$ ls



So we have some files and directories listed in the machine.

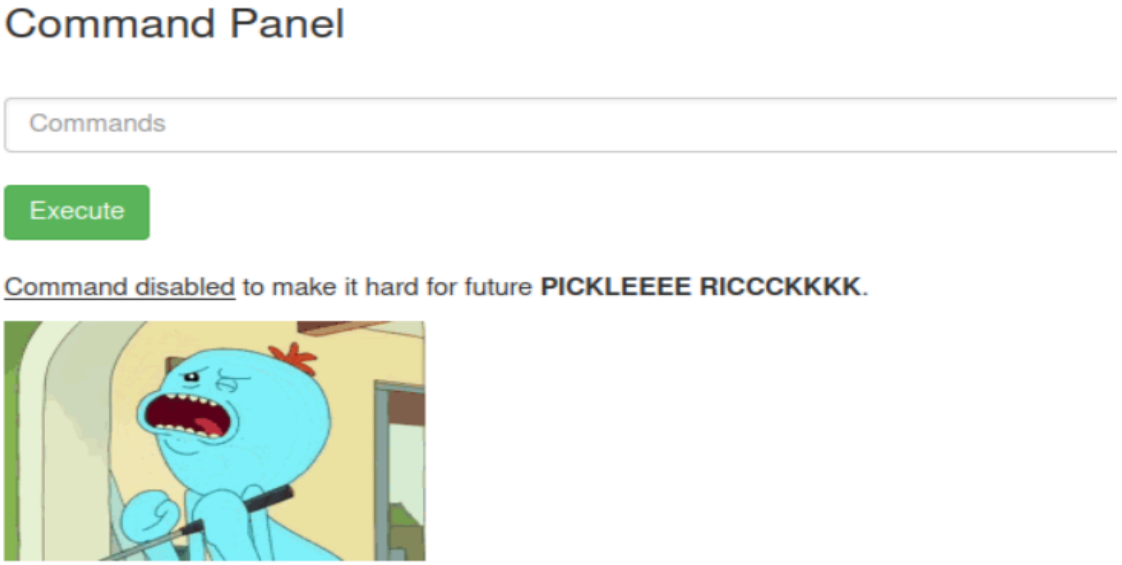
Our first question, what is the first ingredient that Rick needs?

Inorder to find the ingredient, we need to read the files from the lists.

First we need to read **Sup3rS3cretPickl3Ingred.txt**

In linux we use **cat** command to read files in terminal.

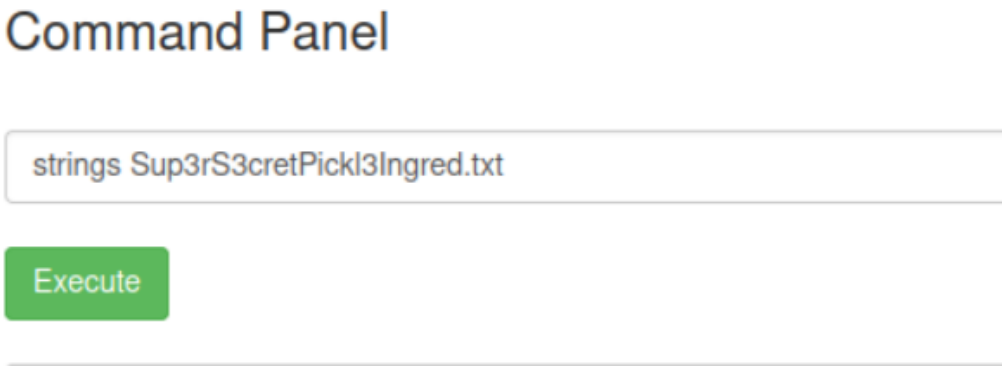
$ cat Sup3rS3cretPickl3Ingred.txt



We can see that we can't use **cat command** to read the files. So we need to try alternative methods .There are different ways to read the files other than the **cat** command.

In this **CTF** im using **strings** command to read the files.
Strings command is used in linux to print the readable strings in a file.

$ strings Sup3rS3cretPickl3Ingred.txt



We got the first flag after executing with **strings** command.

```
mr. meeseek hair
```

Answer 1: **mr. meeseek hair**

Our second question , what is the second ingredient in Rick's potion?

Inorder to find the second answer, we need to look for other files or clues in this system.

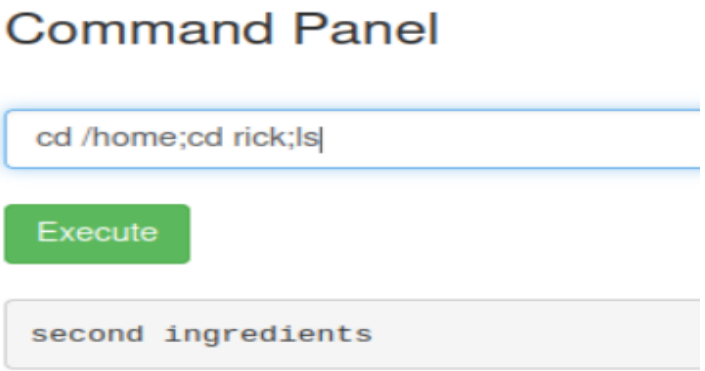
Since we are by default is in the **/var/www/html** directory, Im going to list for the /**home** directory to know which users are present and check if any other files or clues present or not.

$ cd /home;ls

So we have two users in this system **,rick & ubuntu**.

We need to look for the rick folder to check whether if some files exists or not.

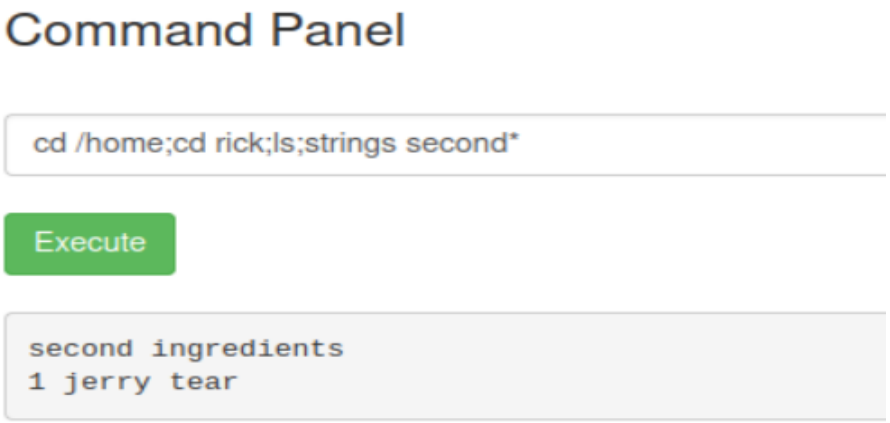
$ cd /home;cd rick;ls



So there is a file named **'second ingredients'** in the home directory of **rick**.

Read this file to get the **second ingredient.**

$cd /home;cd rick;ls;strings second*



So we got the second ingredient **1 jerry tear.**

Answer 2: **1 jerry tear**

Our third and last question, what is the last and final ingredient?

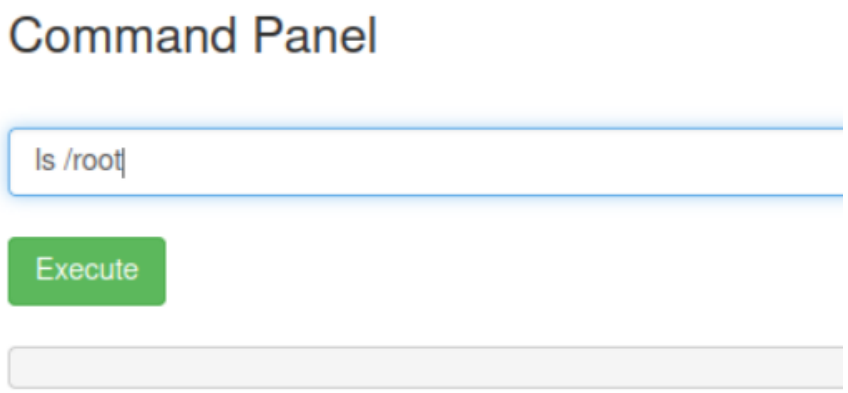
Inorder to find the last answer, we need to also look and check other files and folders.

One more user present in this system named **ubuntu**, but when we check upon that folder, its empty. Also when we check other folders like **assets** in **/var/www/html (default by user www-data)**, its contains the **source code** of the site, there is no information we need.

So we can assume that like the other answer we are possibly looking for is in the root users directory. But since we dont know the password of the root user, we can't access the home directory of the root user which is located in the **/root/.**

When we try to list the root directory , you can see that it is shown empty, because we dont have any permission to list or move to the root users directory.

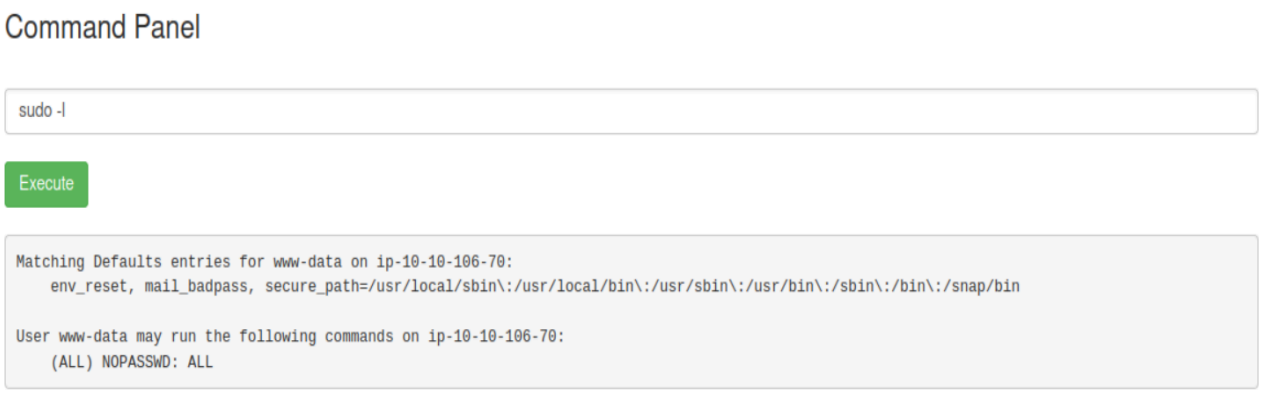
$ ls /root



So here we have two options like first we need to check our user (www-data) can execute sudo permission or not in this system, if not we need to escalate our privileges to root through any vulnerability exploitation or other.

‘**sudo -l**’ command is used to check whether the current user has permission to execute any specific commands using **sudo privileges**. It displays the **list of commands** that the user is allowed to run with **elevated (root) privileges**.

$ sudo -l

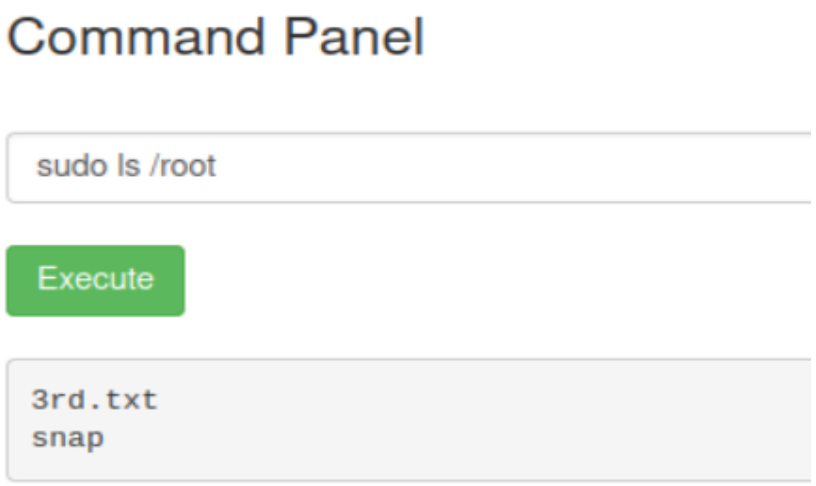


From above output of the command , you can see that the user **www-data** has full root privileges on the system and can execute any command as any user using **sudo** without needing any password. This represents a **critical security misconfiguration** in the system that allows for **instant privilege escalation** to **root.**

So from this , we can access the **root directory** and its files by adding **sudo** command as **prefix** to add our command.

We can check it by listing the home directory of the root.

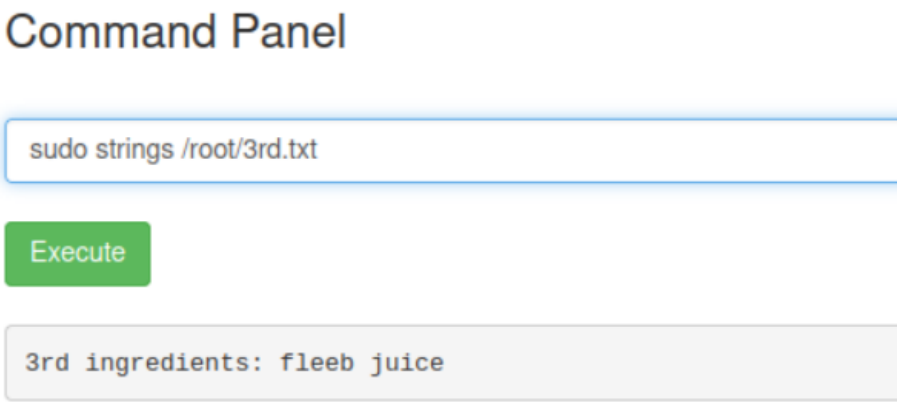
$ sudo ls /root



So you can see that we successfully listed the root directory and there is a file named **3rd.txt** is located in it.

We need to read this file to finally get the **final ingredient** using **strings** command.

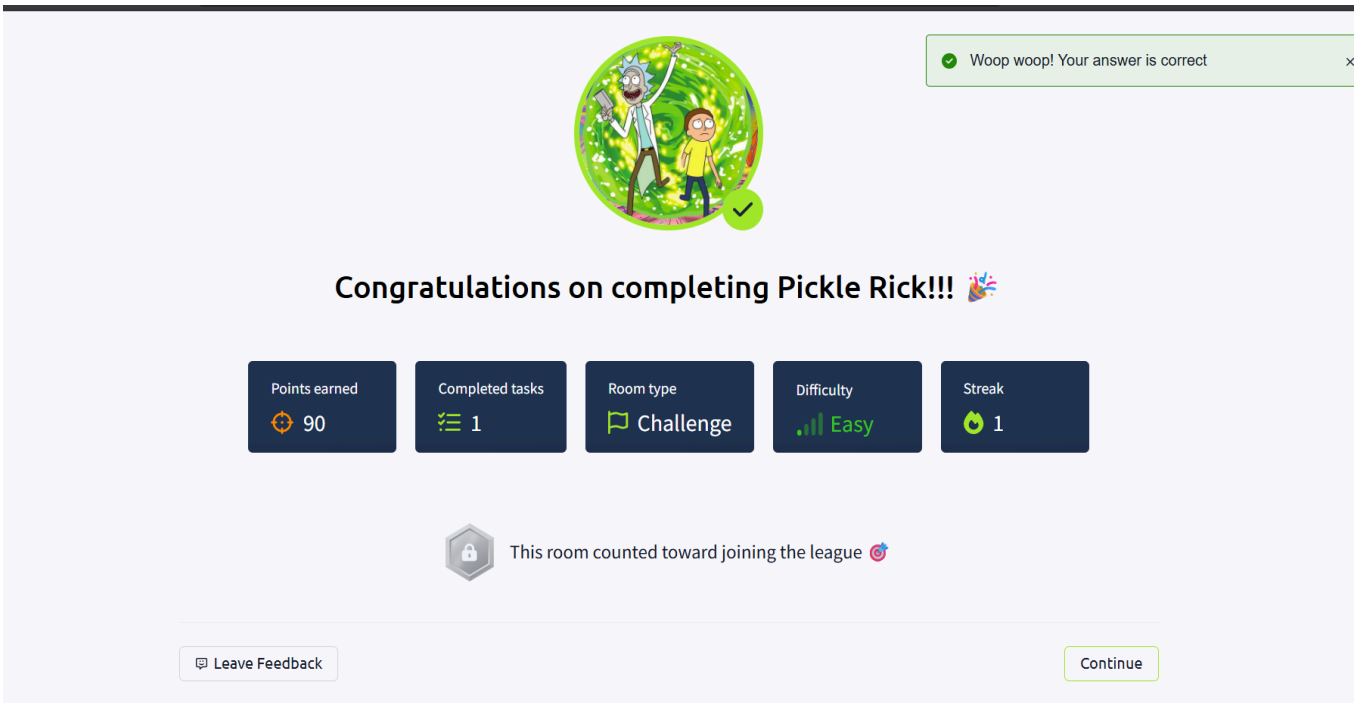
$ sudo strings /root/3rd.txt



From above you can see that we got our final ingredient, **fleeb juice.**

Answer 3: **fleeb juice**

So after submitting this three answers in our **PickleRick** room in TryHackMe.



Thankyou for taking time to read this document all way through