Pickle Rick – THM Report

By Shwetan Zagade

Hello fellow hackers, In this Rick and Morty themed challenge, we will exploit a web server to find 3 ingredients *(eventually answering the three questions for the challenges)* that will help Rick make his potion to transform himself back into a human from a pickle.

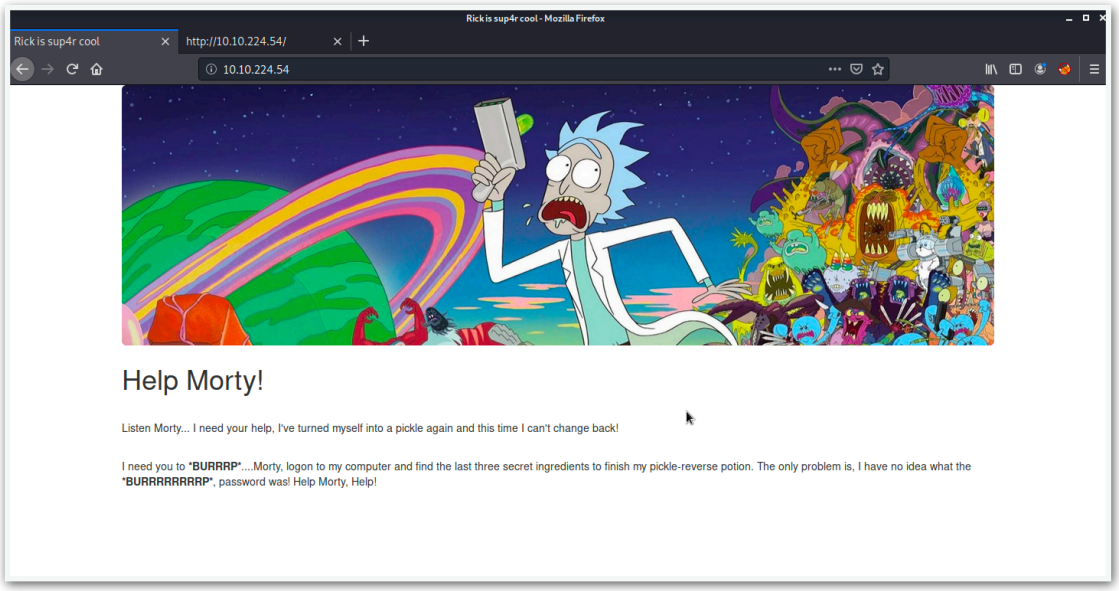
Resources/Tools I have used:

- Gobuster
- http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
- Netcat

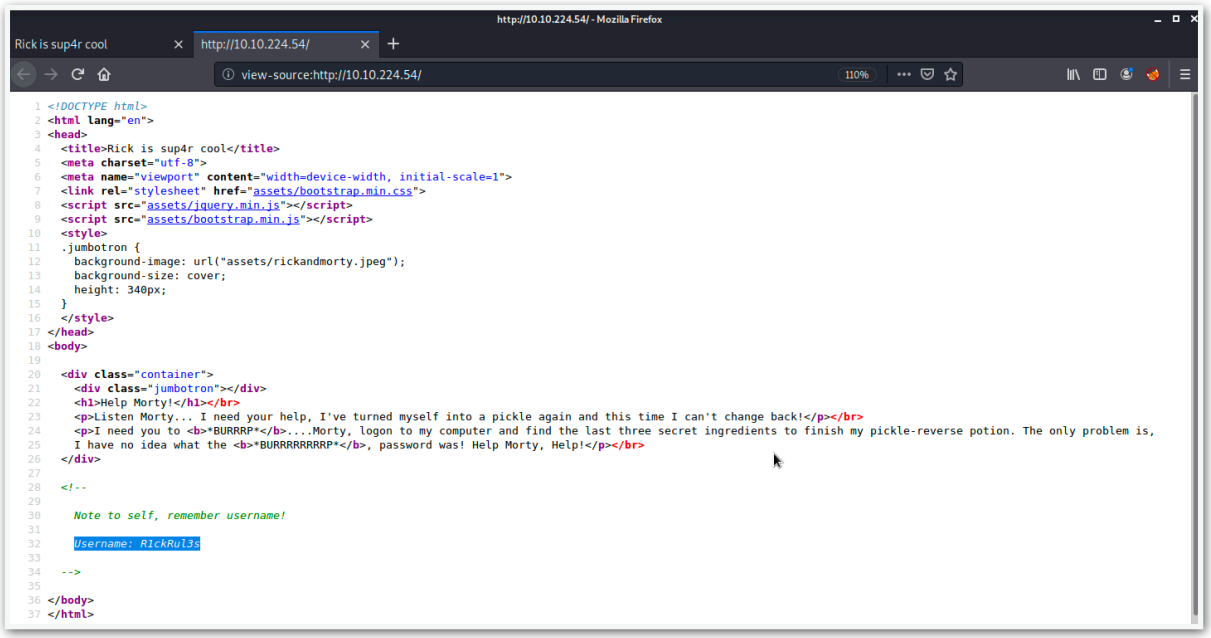
#Task 1 - This subtask requires you to find the first ingredient.

The first ingredient was found by following these steps:

- Browsed to the webpage

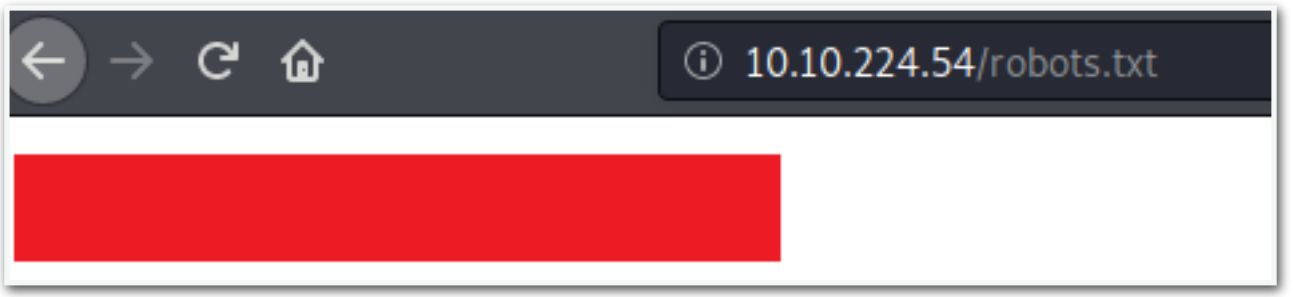


- Reviewed the source code of this page and came across the username “R1ckRul3s”.



source code

- Browsed to “robots.txt” file and found one interesting piece of information there.



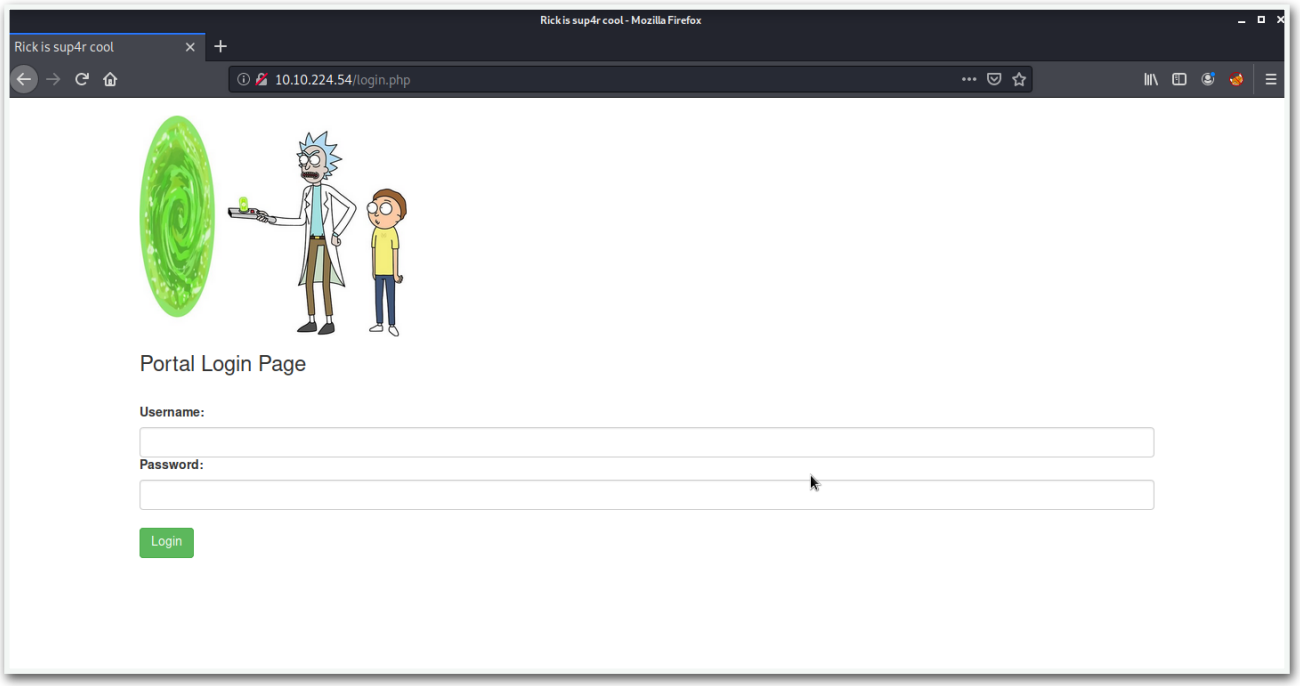
Robots file

- Used gobuster to brute force directories to discover directories and pages on this website. Gobuster discovered few interesting pages.

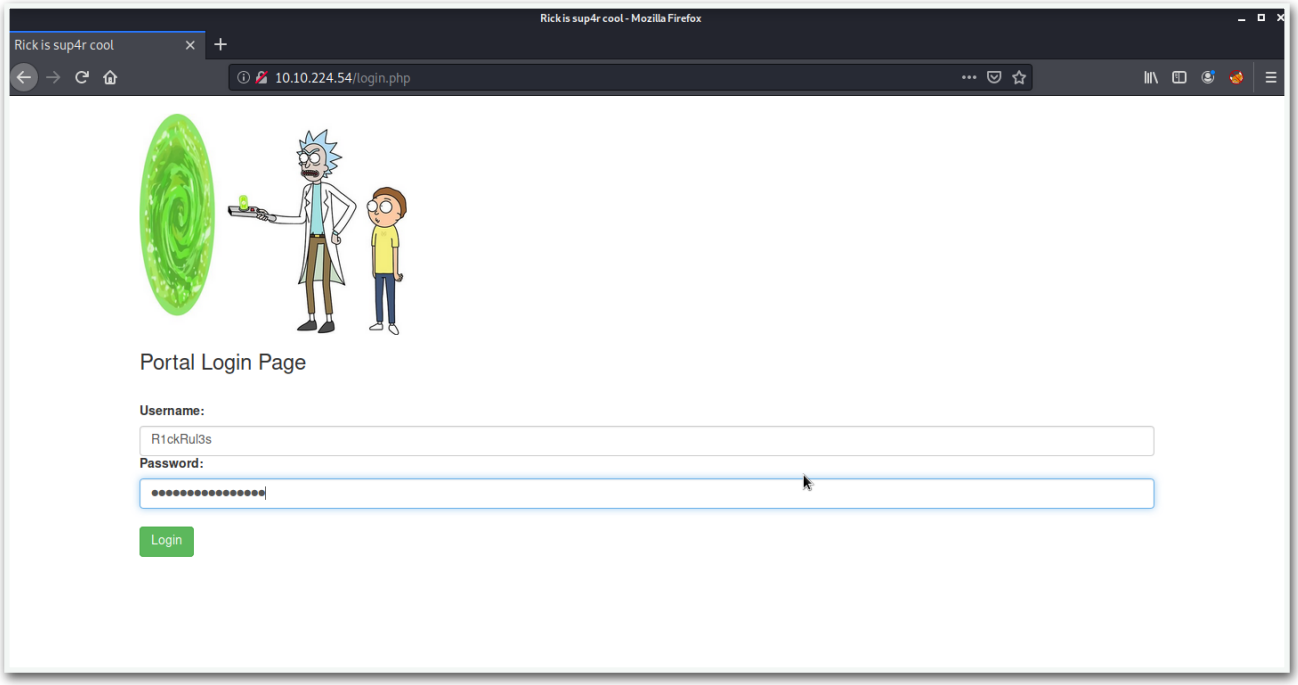
```
kali@kali:~/THM/PickleRick$ gobuster dir -u http://10.10.224.54 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,txt,zip -o pickle.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.224.54
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php,html,txt,zip
[+] Timeout:        10s
===============================================================
2020/05/16 21:42:08 Starting gobuster
===============================================================
/index.html (Status: 200)
/login.php (Status: 200)
/assets (Status: 301)
/portal.php (Status: 302)
/robots.txt (Status: 200)
```

gobuster output

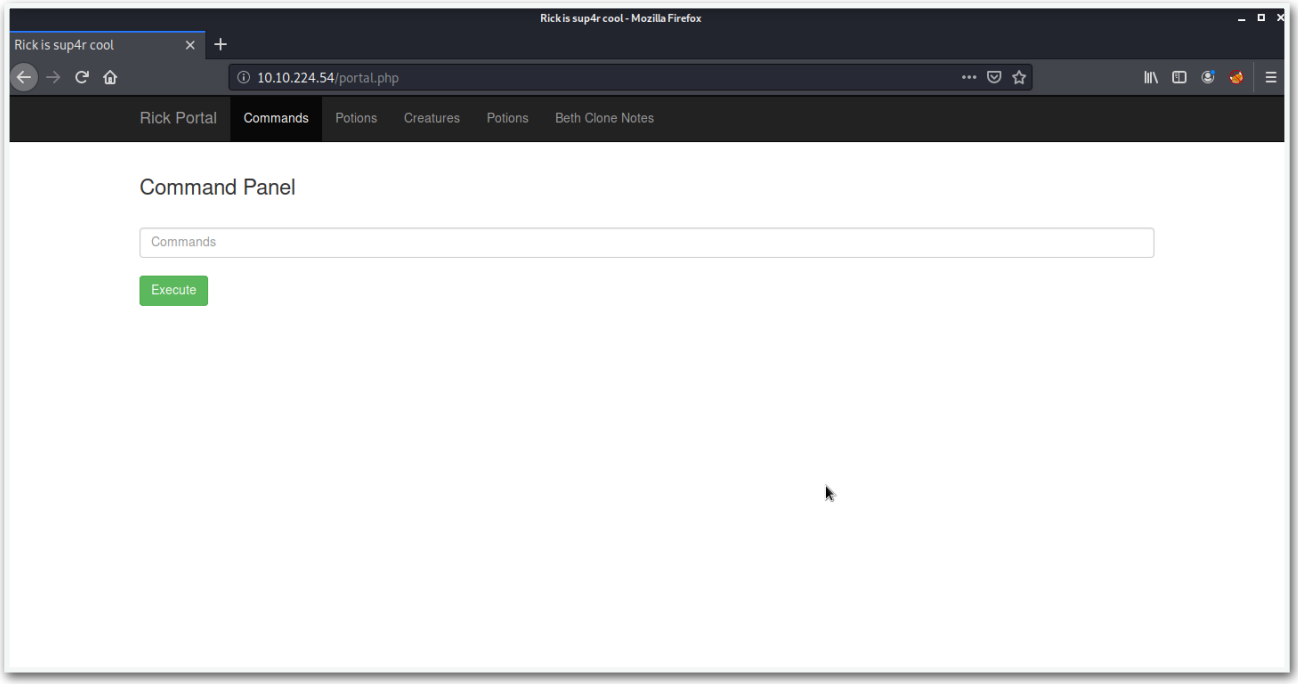
- Browsed to “login.php” and found a login page asking for a username and password. Tried information gathered in previous steps to login to this portal.



login.php

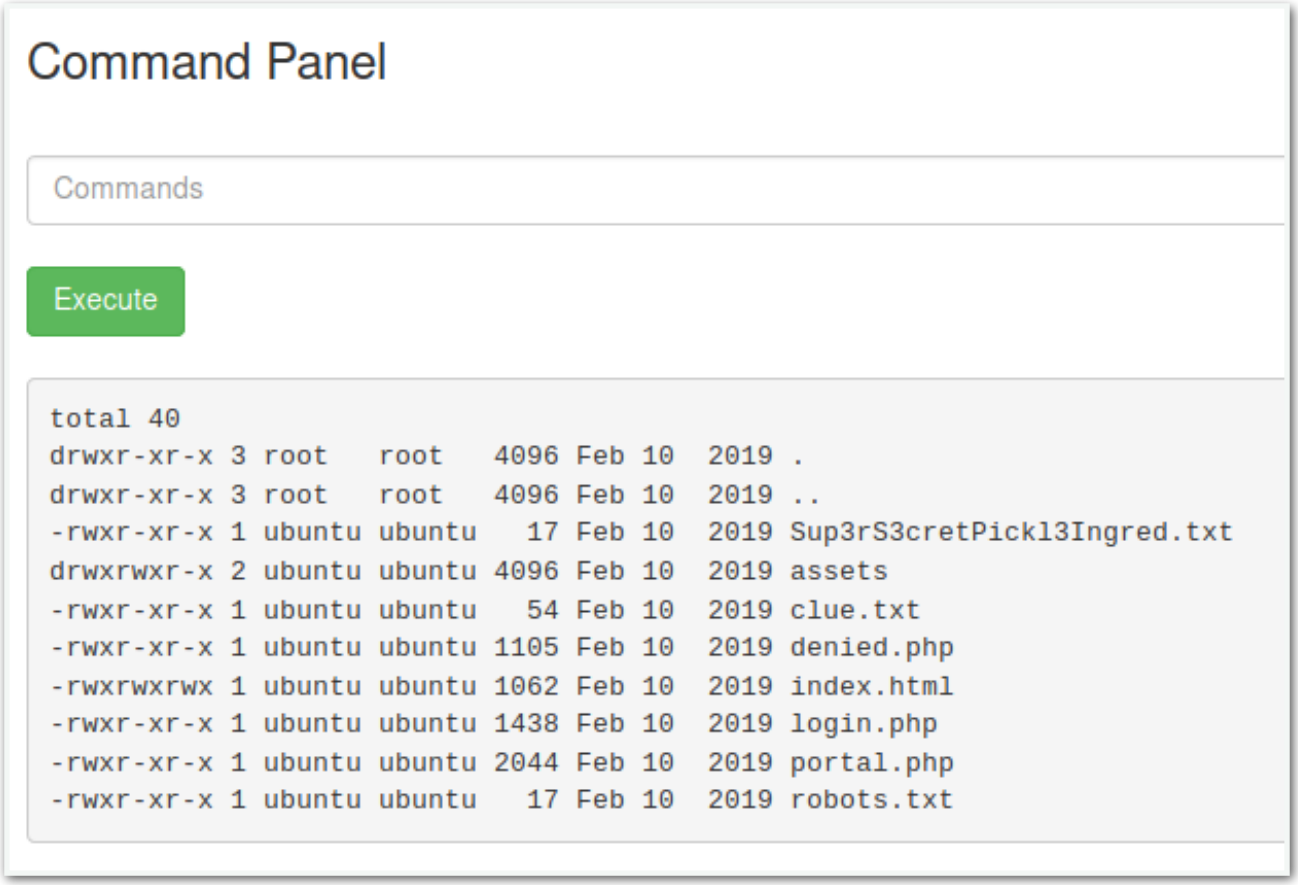


Credentials



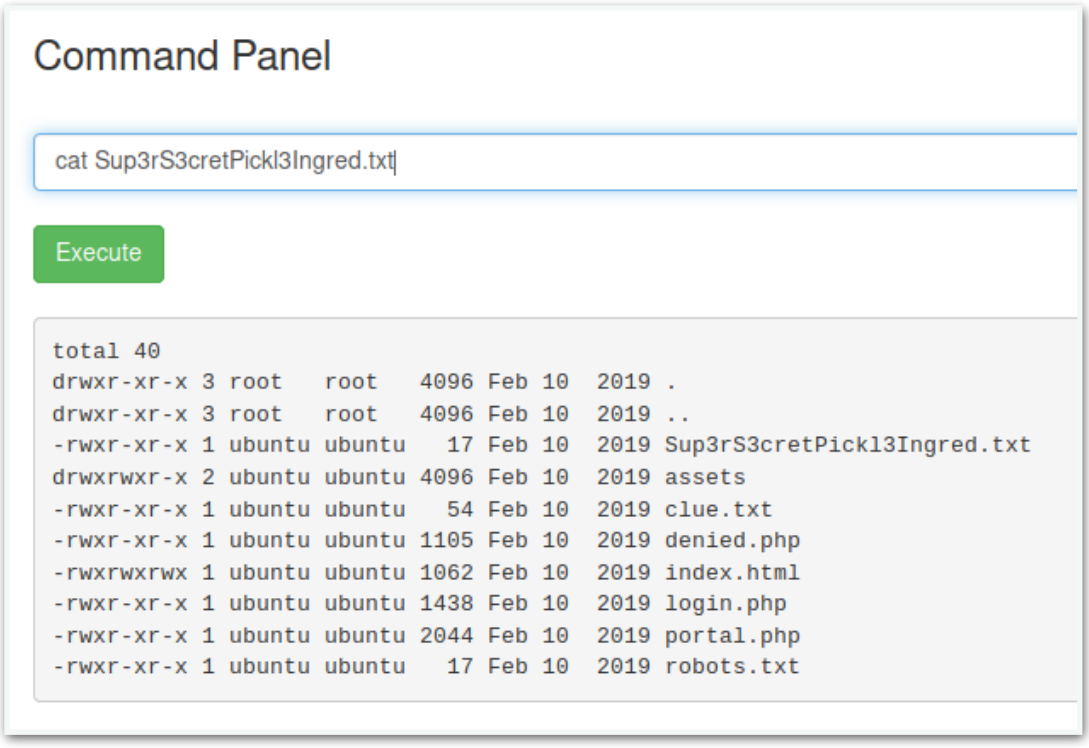
Login successful

- Tried listing the contents of directory.

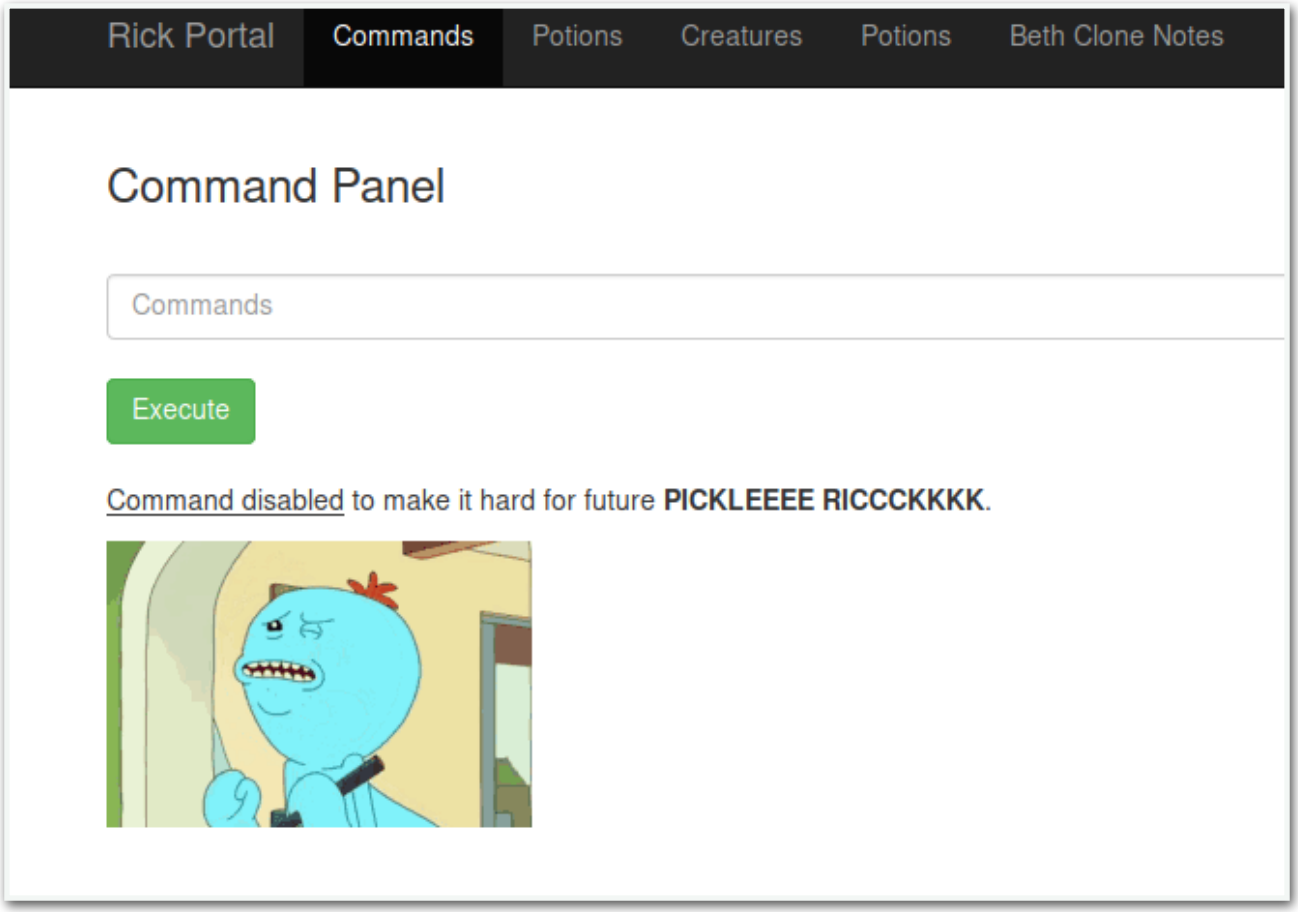


Directory listing

- Saw an interesting le “Sup3rS3cretPickl3Ingred.txt” but could not read contents of the le (using cat) as this functionality was disabled on the server.

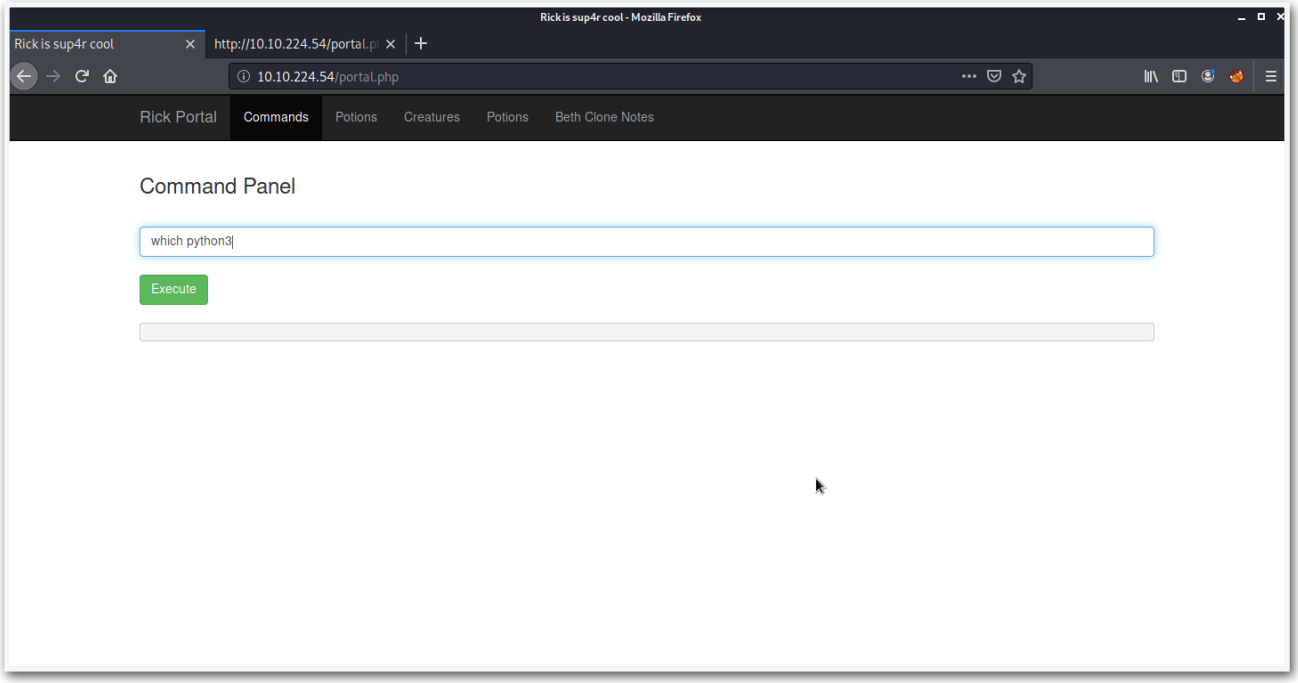


Tried ‘cat’ to read file

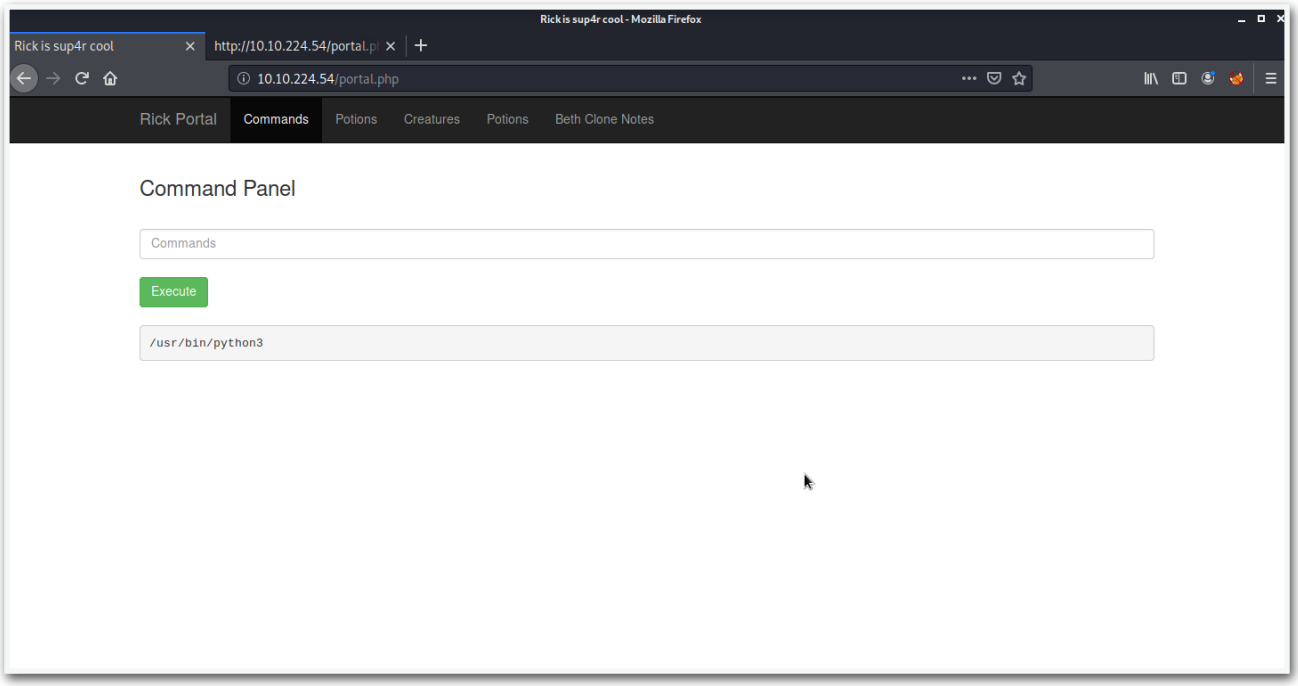


cat disabled

- As this was a very restrictive environment, tried getting a reverse shell from the server. First tried to identify if python (python2 was not available) is available on the server.

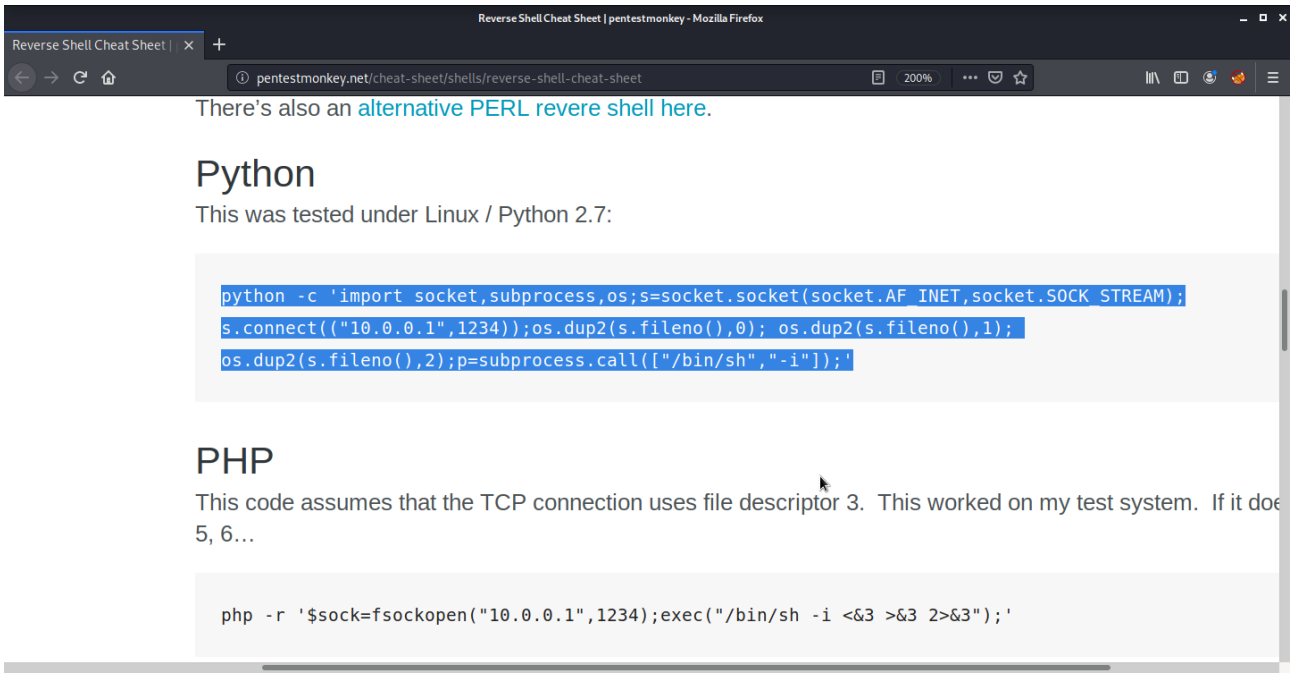


python3 check

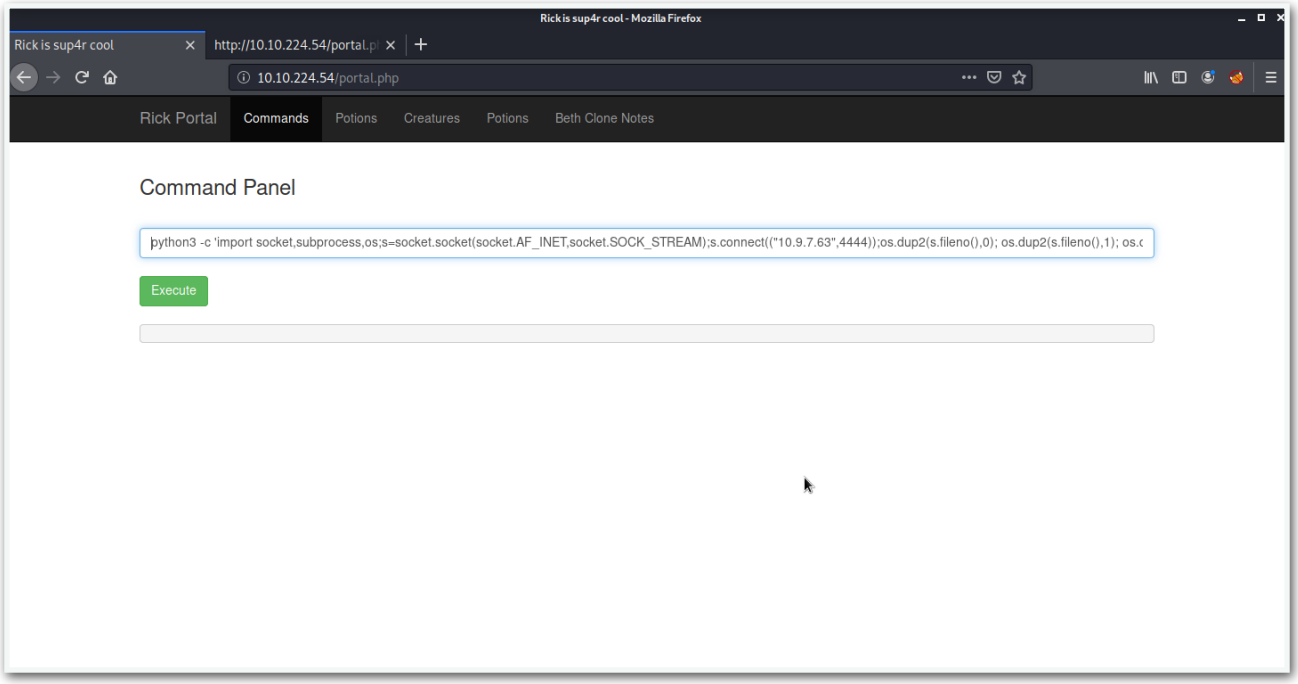


python3 available

- We had python3 available on the server. Used pentestmonkey cheat sheet for python reverse shell. Started a netcat listener on port 4444, copied the command, and changed IP and port to reflect our attack machine IP and local port (running netcat).



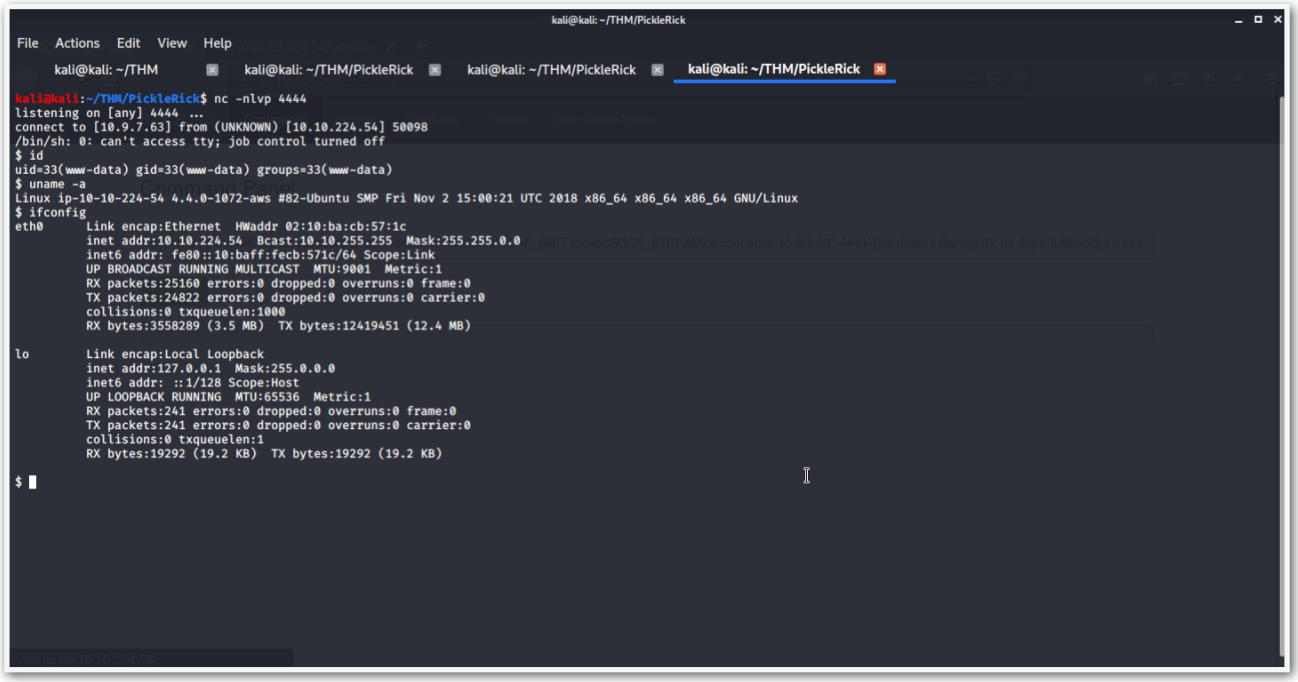
Python reverse shell from penestmonkey website



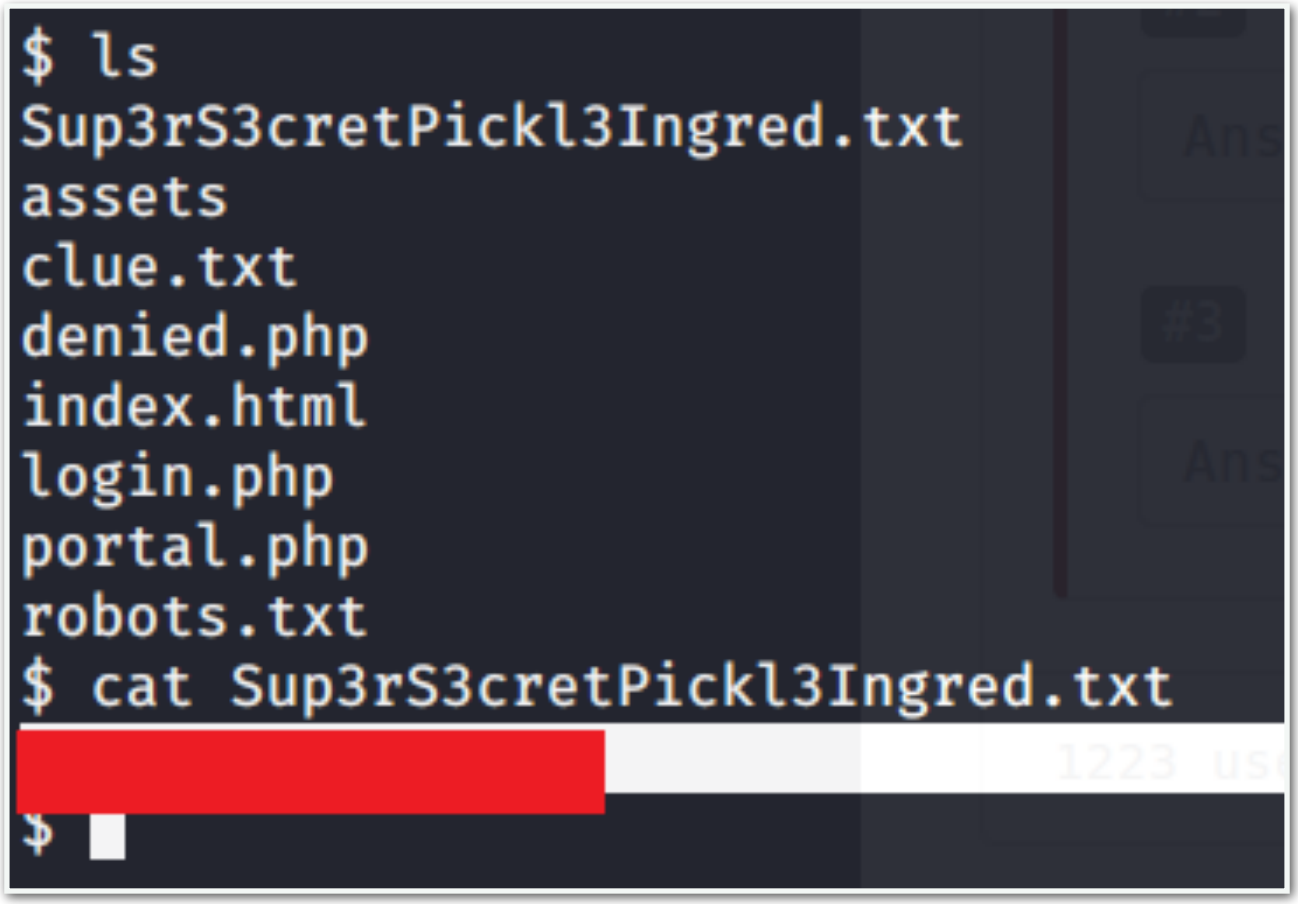
Python reverse shell command

Netcat listener

- Upon executing the python reverse shell command immediately got the shell with user “www-data” authority from system.

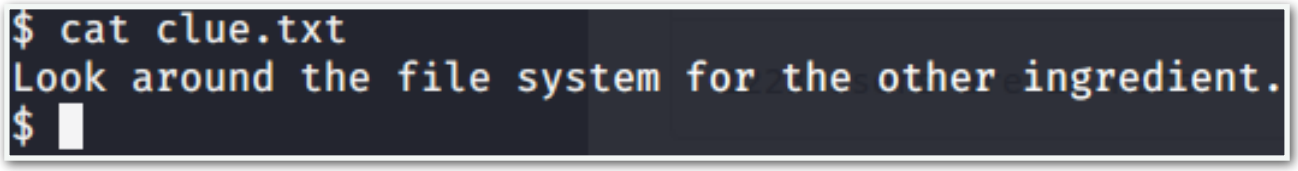


- From this folder, we got our first ingredient.



First ingredient

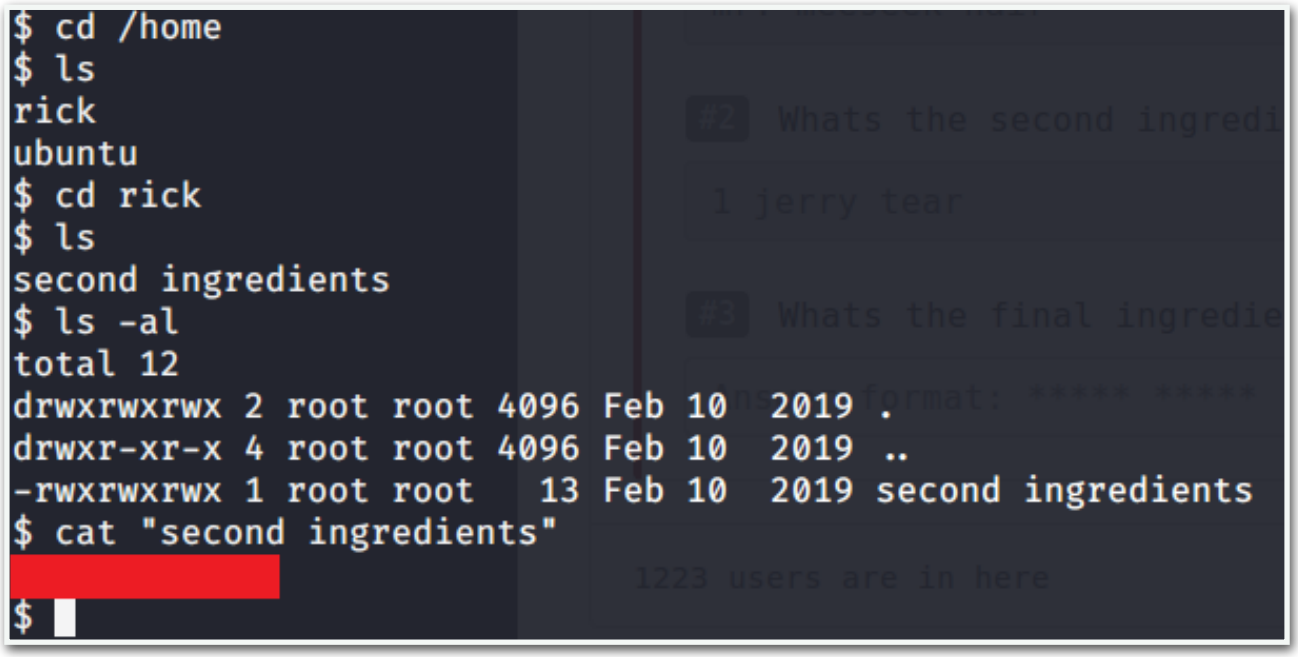
- From this folder read the le “clue.txt” to see contents of the le for remaining ingredients.



Clue.txt

#2 This subtask requires you to find the second ingredient.

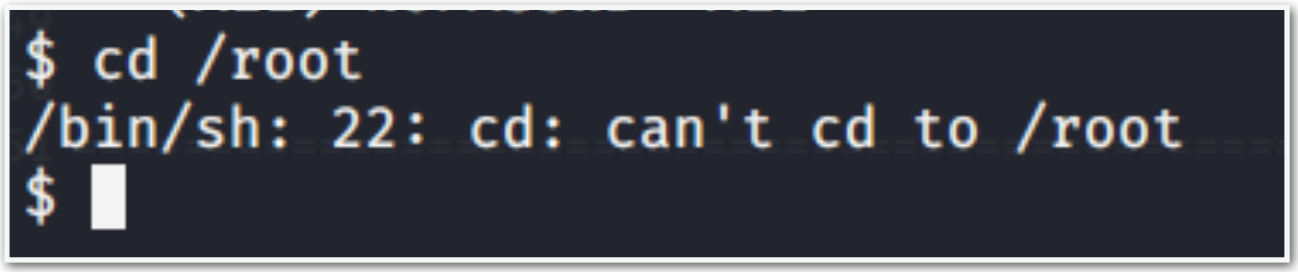
Browsed to “/home/rick” folder to get the second ingredient.



Second ingredient

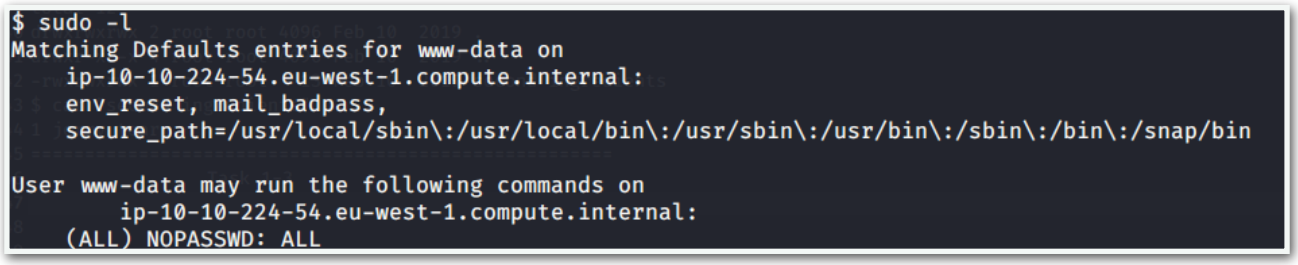
#3 This subtask requires you to find third ingredient.

- Tried accessing "/root" folder but access was denied to our current user (www- data).



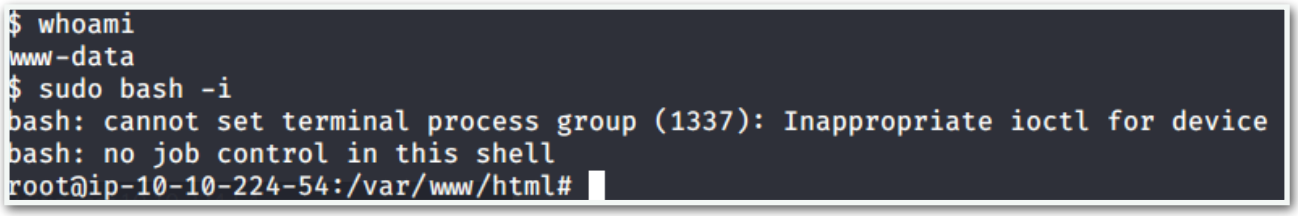
root folder inaccessible

- For privilege escalation tried to identify what commands are allowed to current user with root privileges and to our surprise all commands were allowed without any password.



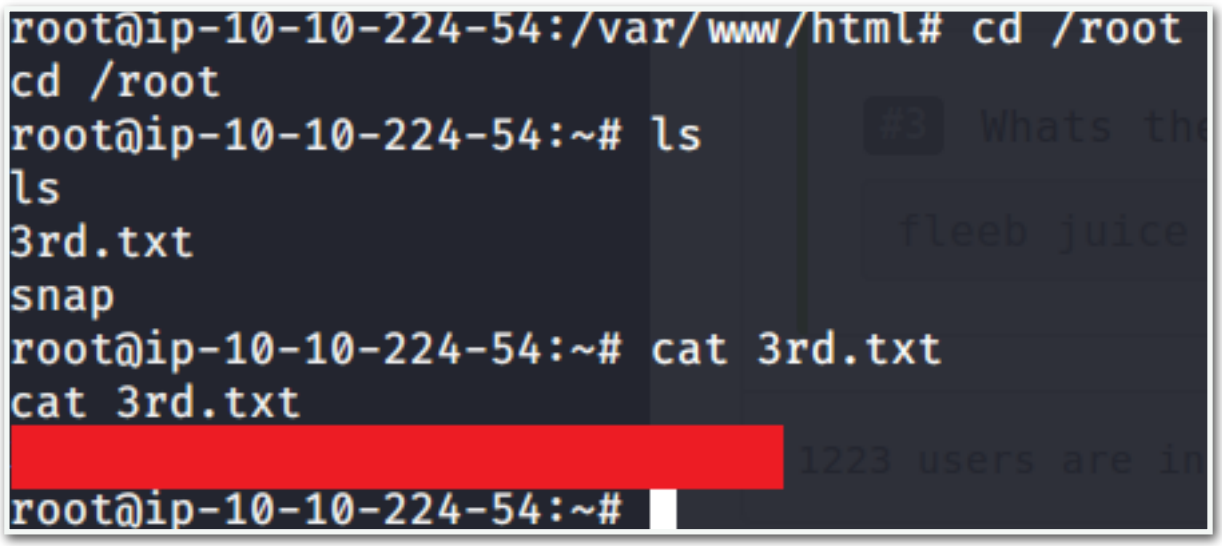
sudo -l

- Ran "sudo bash -i" to get root access to system.



root access

- Browsed to "/root" folder to get the third and last ingredient.



Third and last ingredient