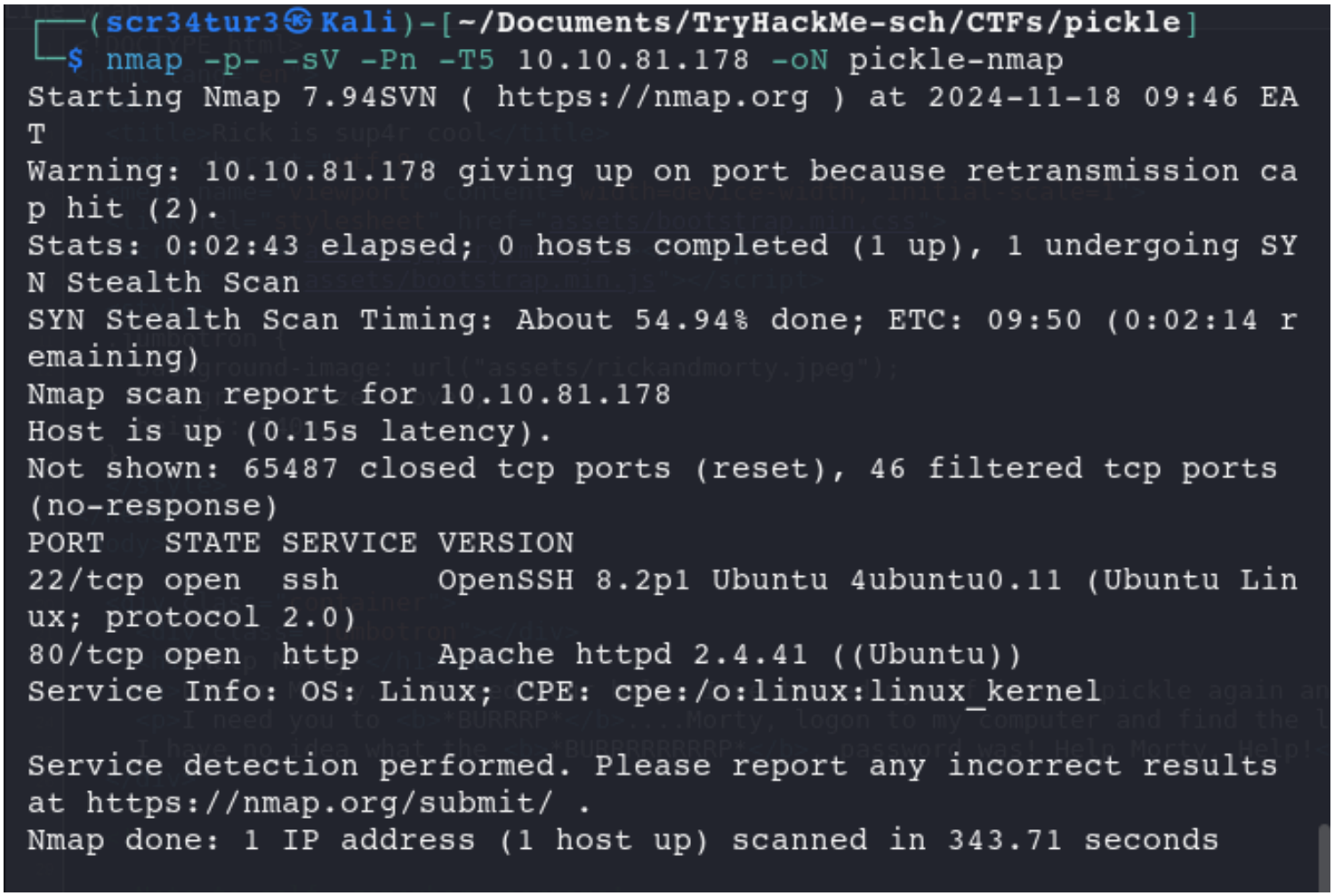
PICKLE WEB CHALLENGE

THIS IS A WEB CHALLENGE. SUPER BEGINNER FRIENDLY:)

Began by doing nmap scan against the target. pORT 22 and 80 were open.



When dealing with web challenges, its my habit checking for comments on the code using dev tools.
Here I got a valid username that I know it would be of use in the future.

Line Wrap

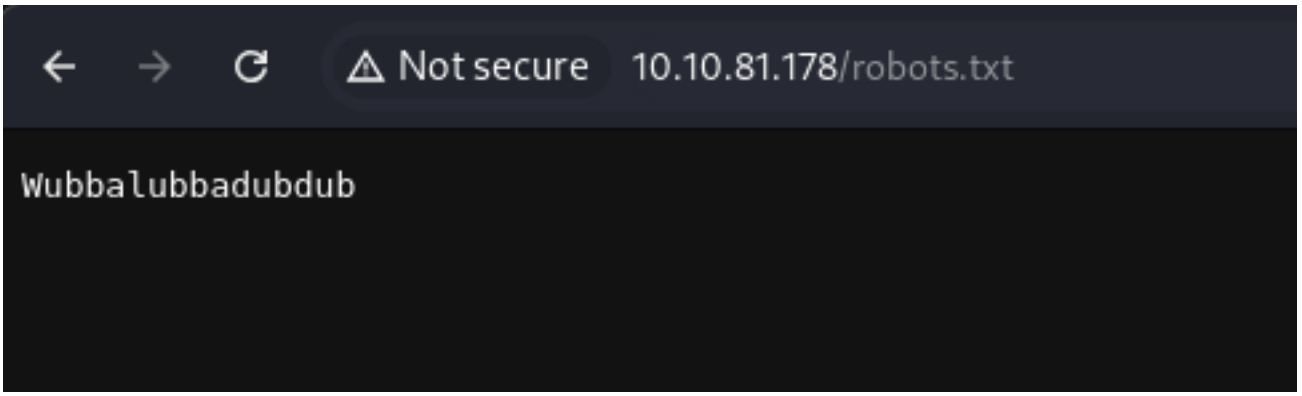
```
<!DOCTYPE html>
<html lang="en">
<head>
  <title>Rick is sup4r cool</title>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="stylesheet" href="assets/bootstrap.min.css">
  <script src="assets/jquery.min.js"></script>
  <script src="assets/bootstrap.min.js"></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>I need you to <b>*BURRRP*</b>....Morty, logon to my computer and find the last three secret ingredients to fi
    I have no idea what the <b>*BURRRRRRRR*</b>, password was! Help Morty, Help!</p></br>
  </div>

  <!--

    Note to self, remember username!

    Username: R1ckRul3s

  -->

</body>
</html>

```

Using dirsearch, I bruteforced for directories.
It appears there is a login page.

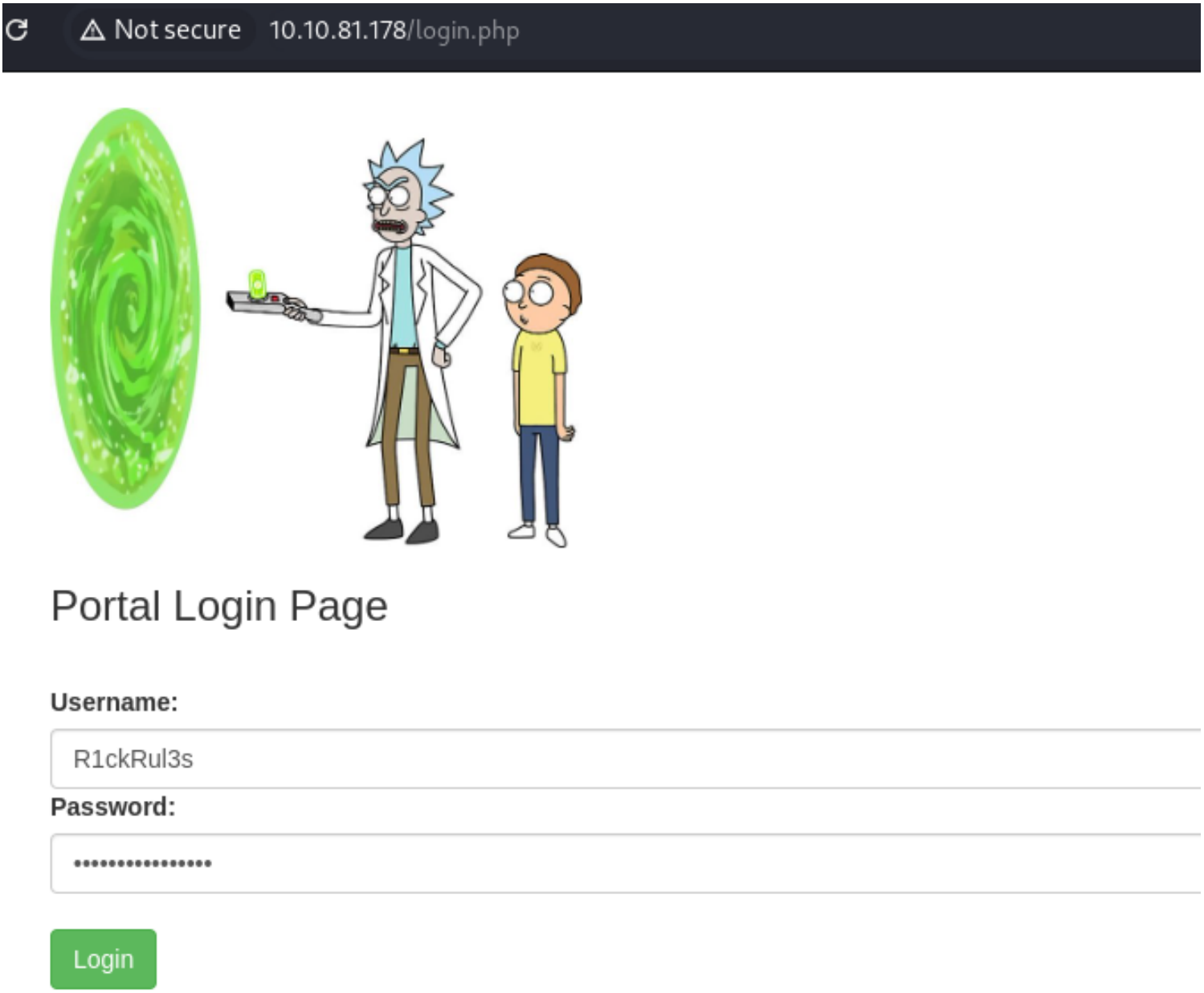
```
┌──(scr34tur3㉿Kali)-[~/Documents/TryHackMe-sch/CTFs/pickle]
└─$ dirsearch -u http://10.10.81.178/ -w /usr/share/seclists/Discovery/Web-Content/dirsearch.txt -t 50
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET
Threads: 50 | Wordlist size: 29378

Output File: /home/scr34tur3/Documents/TryHackMe-sch/CTFs/pickle/reports/http_10.10.81.178/__24-11-18_09-58-08.txt

Target: http://10.10.81.178/

[09:58:08] Starting:
[09:58:11] 403 -  277B  - /.html
[09:58:11] 403 -  277B  - /.php
[09:58:15] 403 -  277B  - /.htaccess.bak1
[09:58:15] 403 -  277B  - /.htaccess.orig
[09:58:15] 403 -  277B  - /.htaccess.sample
[09:58:15] 403 -  277B  - /.htaccessBAK
[09:58:15] 403 -  277B  - /.htaccessOLD
[09:58:15] 403 -  277B  - /.htaccessOLD2
[09:58:15] 403 -  277B  - /.httr-oauth
[09:58:15] 403 -  277B  - /.htaccess.save
[09:58:15] 403 -  277B  - /.htm
[09:58:51] 200 -  588B  - /assets/
[09:59:29] 403 -  277B  - /icons/
```

```
[09:59:29] 403 -  277B  - /icons/
[09:59:39] 200 -  455B  - /login.php
[10:00:02] 302 -    0B  - /portal.php  ->  /login.php
[10:00:17] 200 -   17B  - /robots.txt

Task Completed
```

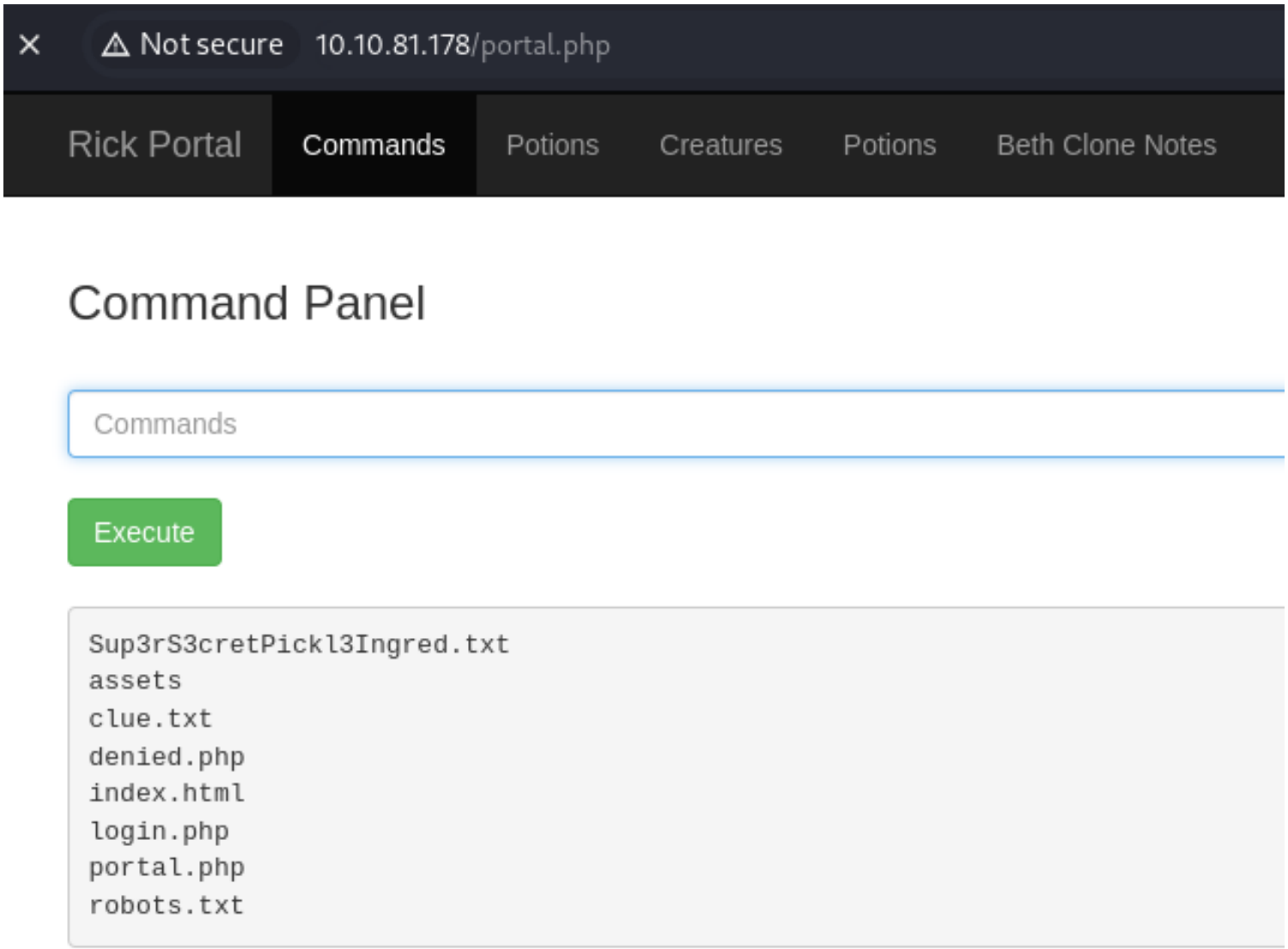
checking the robots.txt, found a random text.



Using the username found on the comment section, with the random text found under the robots.txt dir, It appeared this were valid creds for this page.

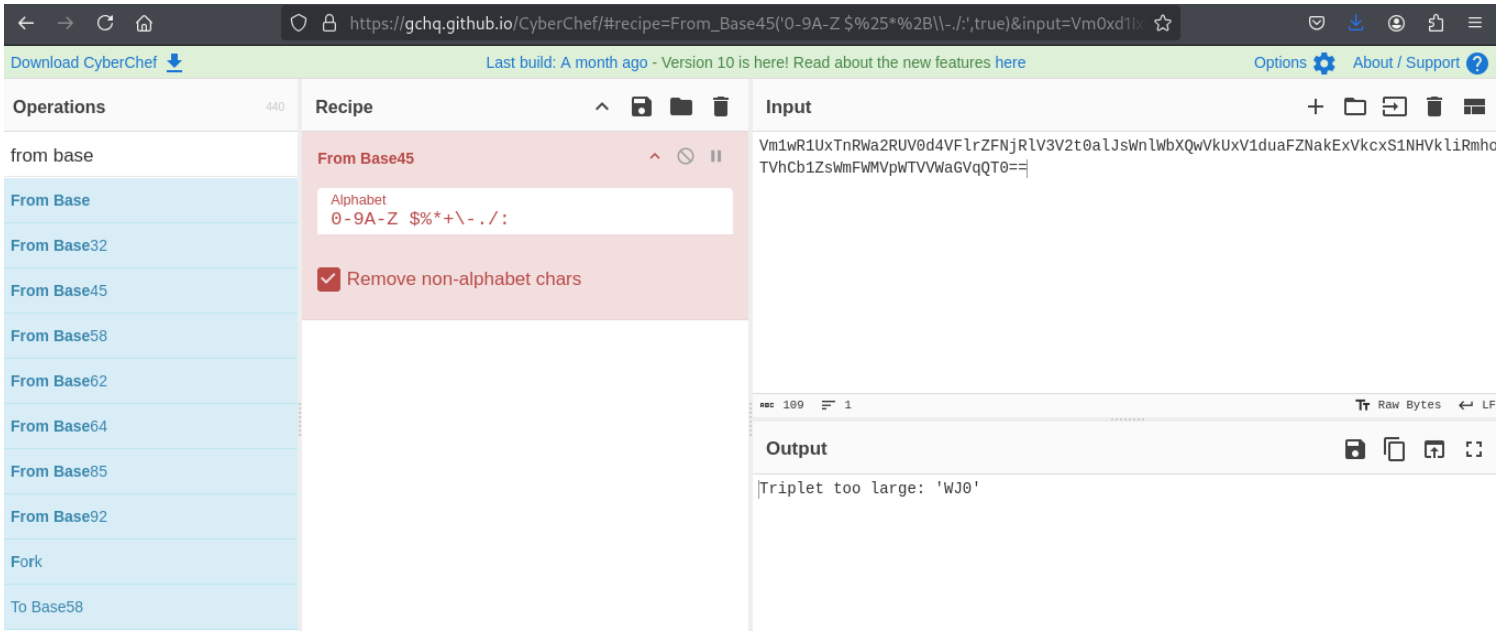


Once in, one was able to execute system commands, only that not all system commands were executable.
For Instance, trying to view the content of .txt file using the cat cmd, its not possible.

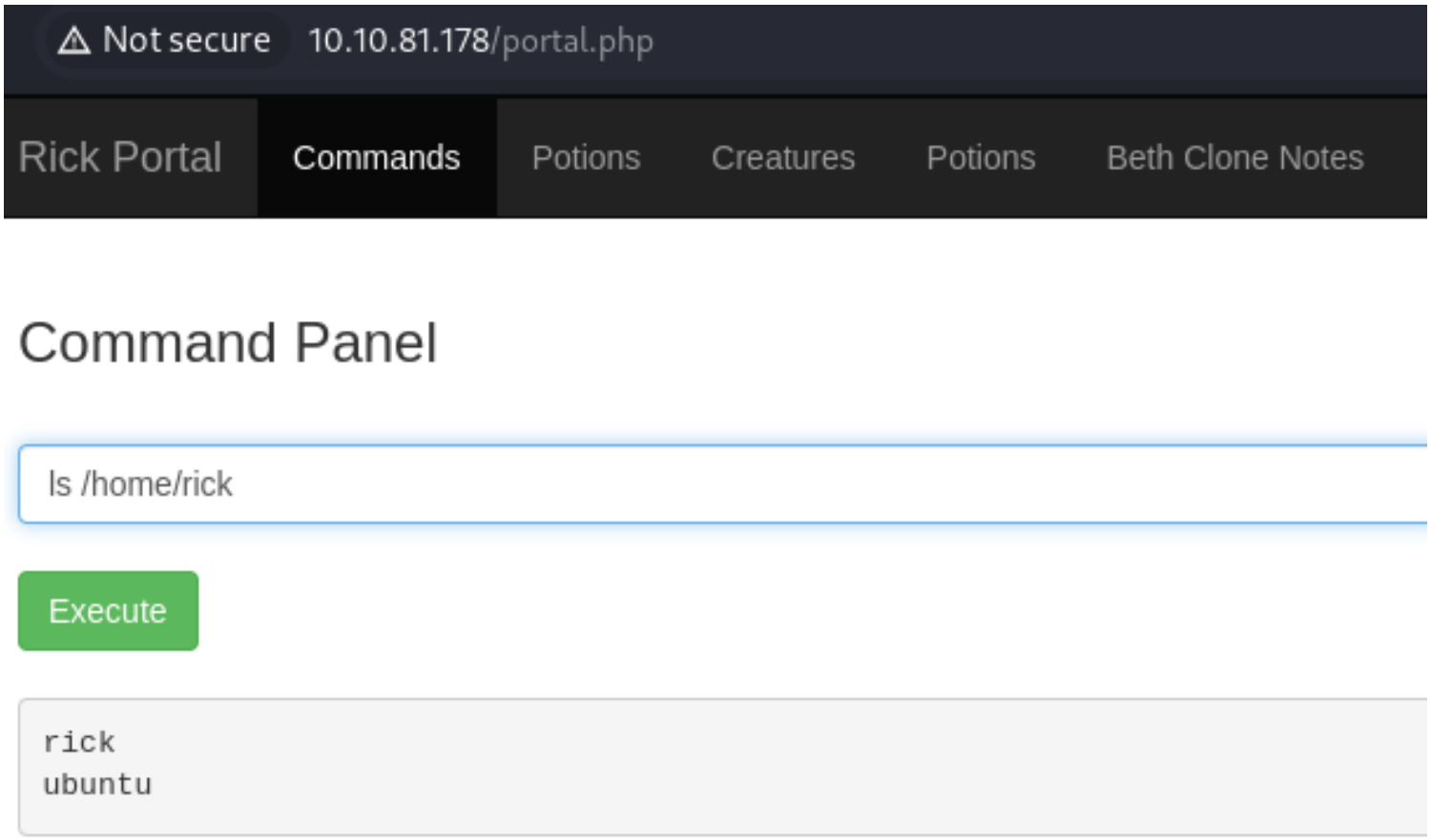


For this very reason, I downloaded this files and viewed its content from my local machine.

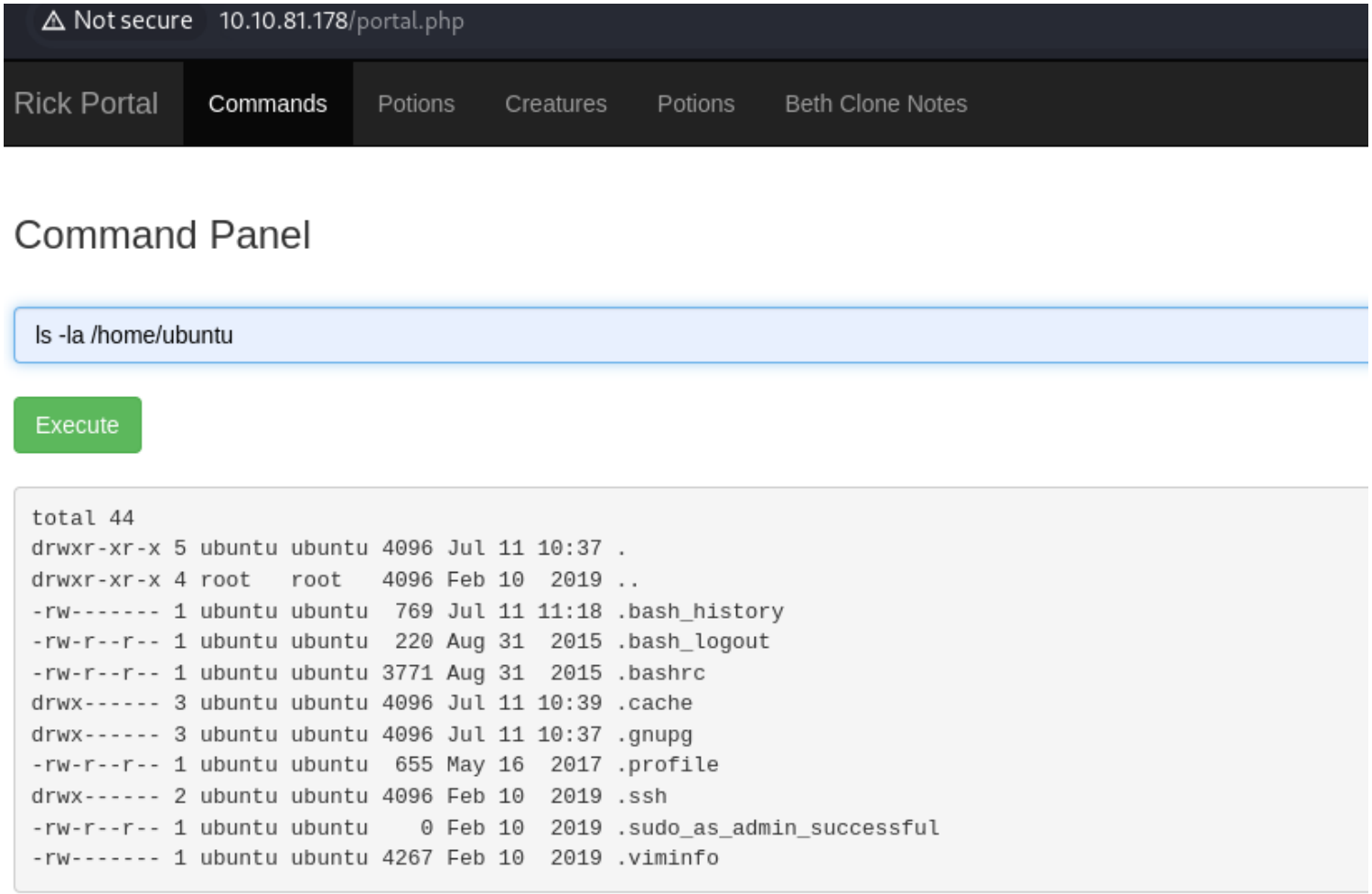
```
┌──(scr34tur3㉿Kali)-[~/Documents/TryHackMe-sch/CTFs/pickle]
└─$ wget http://10.10.81.178/Sup3rS3cretPickl3Ingred.txt
--2024-11-18 10:14:14--  http://10.10.81.178/Sup3rS3cretPickl3Ingred.txt
Connecting to 10.10.81.178:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17 [text/plain]
Saving to: 'Sup3rS3cretPickl3Ingred.txt'

Sup3rS3cretPickl 100%[=======>]      17  --.-KB/s    in 0s

2024-11-18 10:14:14 (498 KB/s) - 'Sup3rS3cretPickl3Ingred.txt' saved [17/17]

.: not enough arguments

┌──(scr34tur3㉿Kali)-[~/Documents/TryHackMe-sch/CTFs/pickle]
└─$ ls
Sup3rS3cretPickl3Ingred.txt  pickle.ctb      reports
pickle-nmap                  picklerick.gif
```



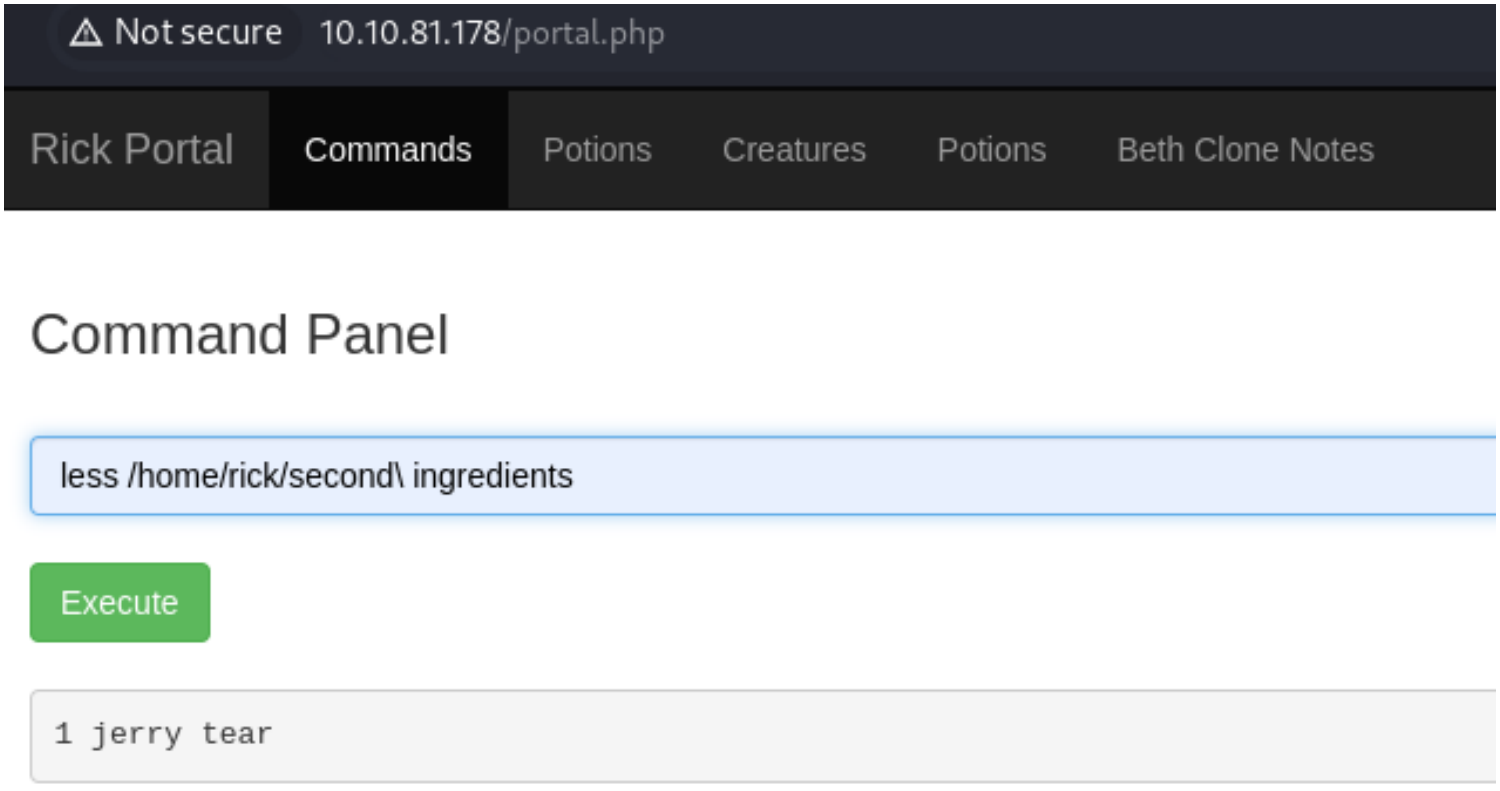
Here we can see there is a home directory of an interesting user called rick with whom I can ssh with to the server, however... this was not a success. Seemed the user did not exist anymore in the system.



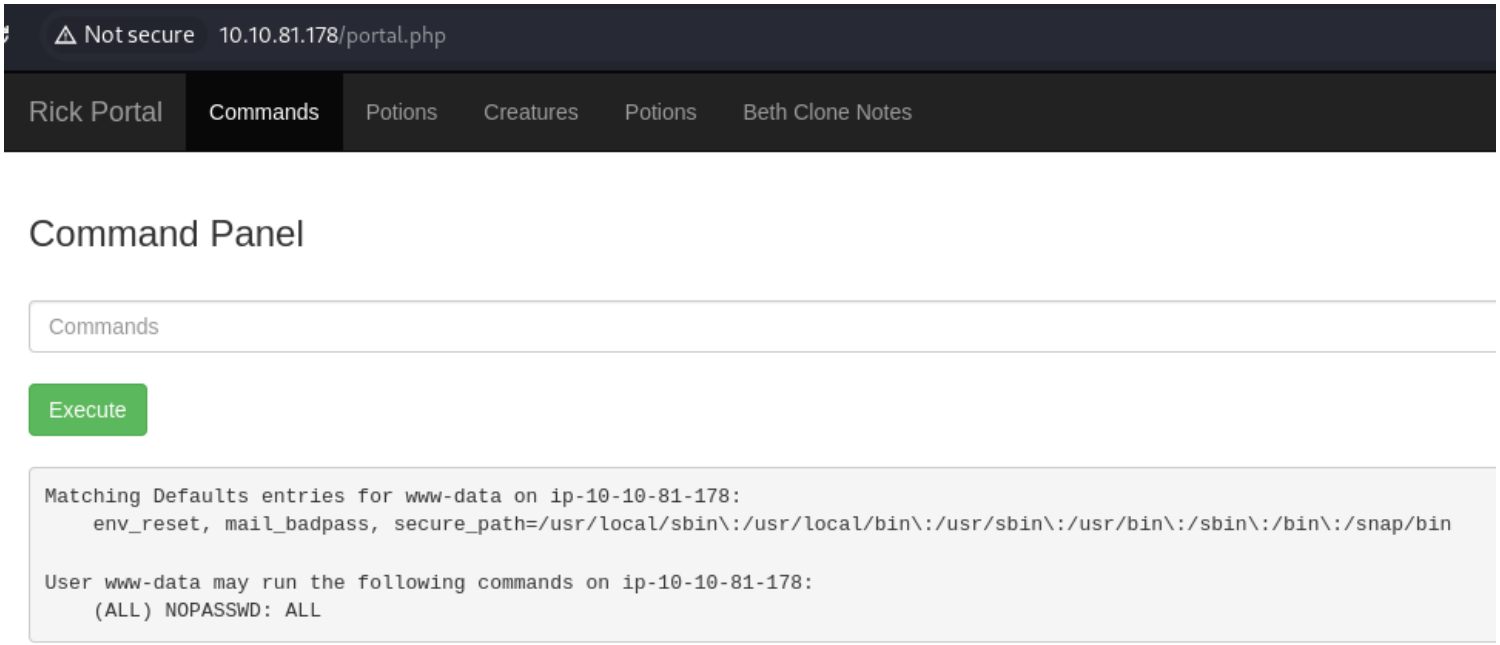
can see interesting .ssh file, however they were not downloadable from the server.



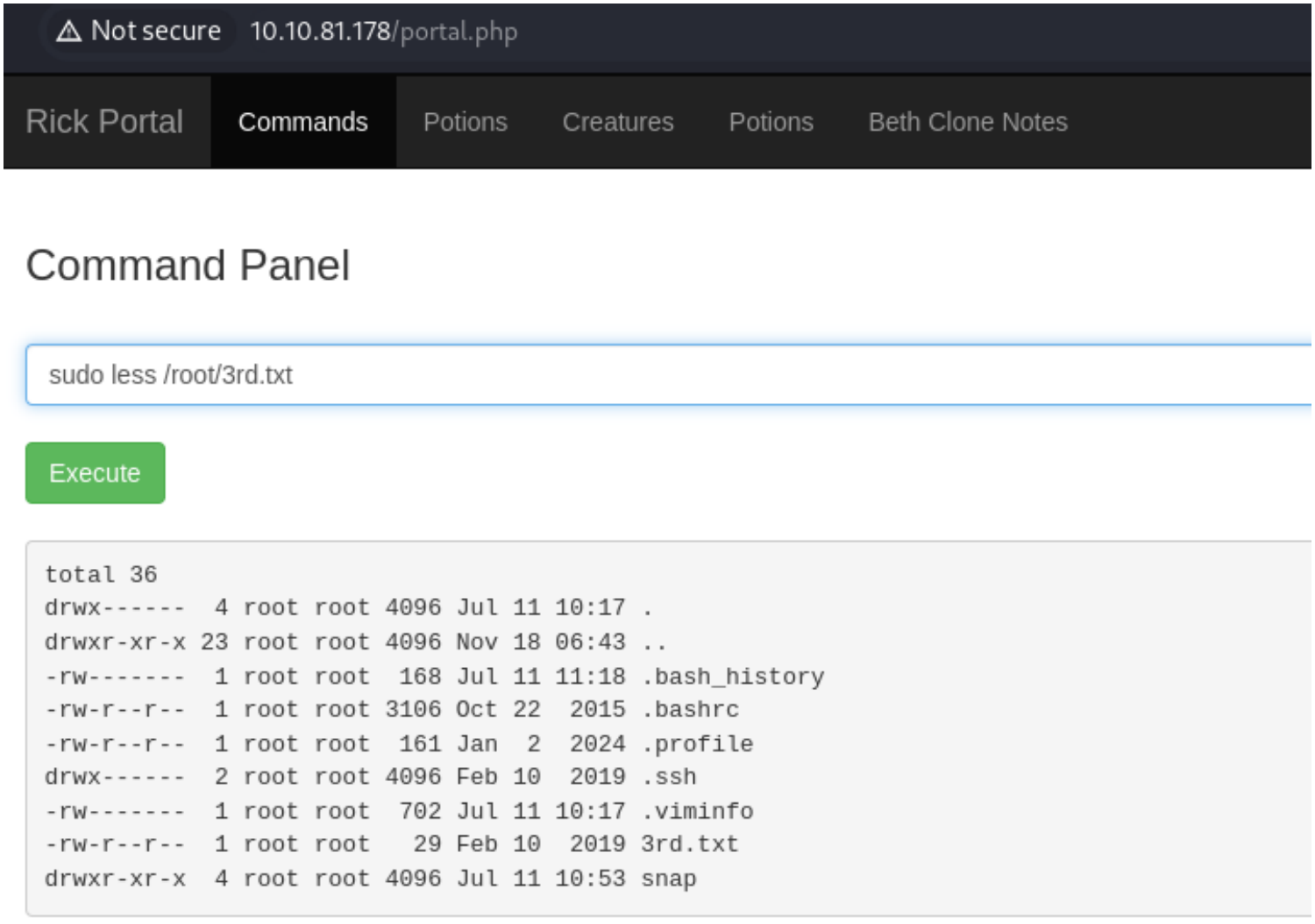
Under the home dir of rick, found the second ingredient that served as the second flag.



PrivEsc phase. Checking for commads the current user can execute, he had perm on files with sudo privileges.



I went ahead and read the 3rd text that was needed to complete this room.



THE END!!!