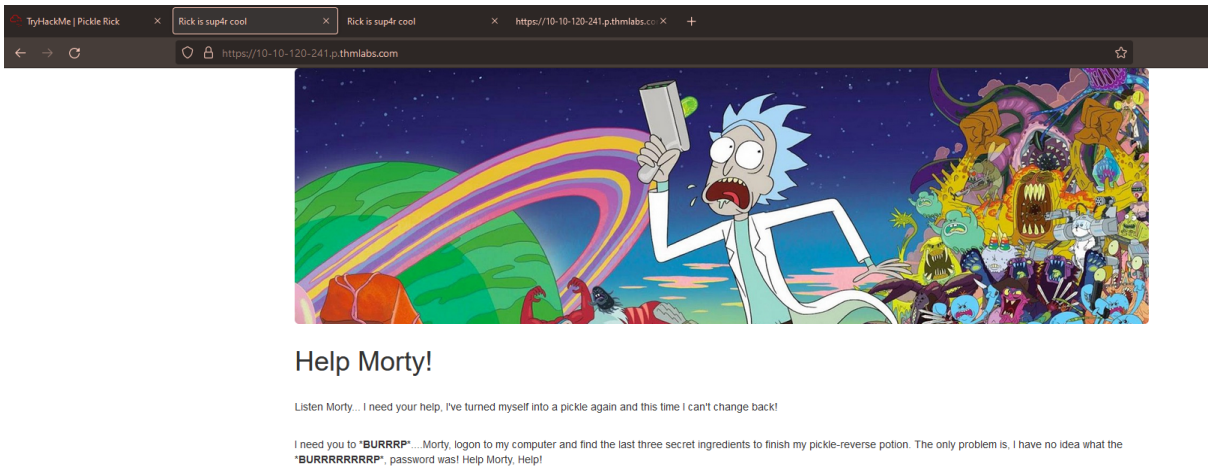
Pickle Rick

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 - R1ckRul3s

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 R1ckRul3s@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.
R1ckRul3s@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`

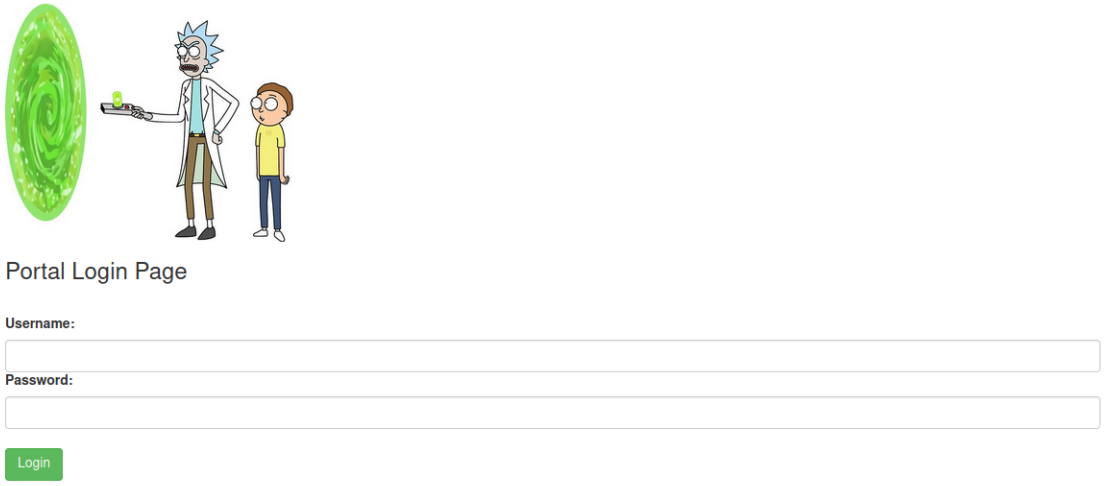
Boom ! Even though its not running completed, we found some relevant directory for the website.

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

Lets start with /login.php.

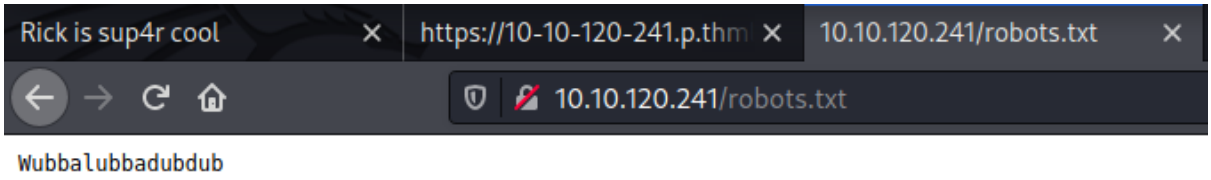
```
└─$ gobuster dir -u http://10.10.120.241 -w /usr/share/wordlists/dirbuster/directory-list-2.3-med
ium.txt -x php,txt,html
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] 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.



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

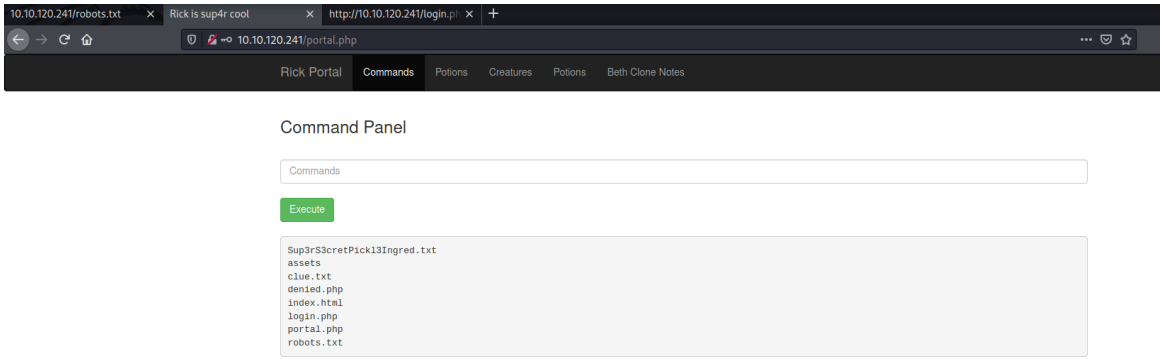


There you go !

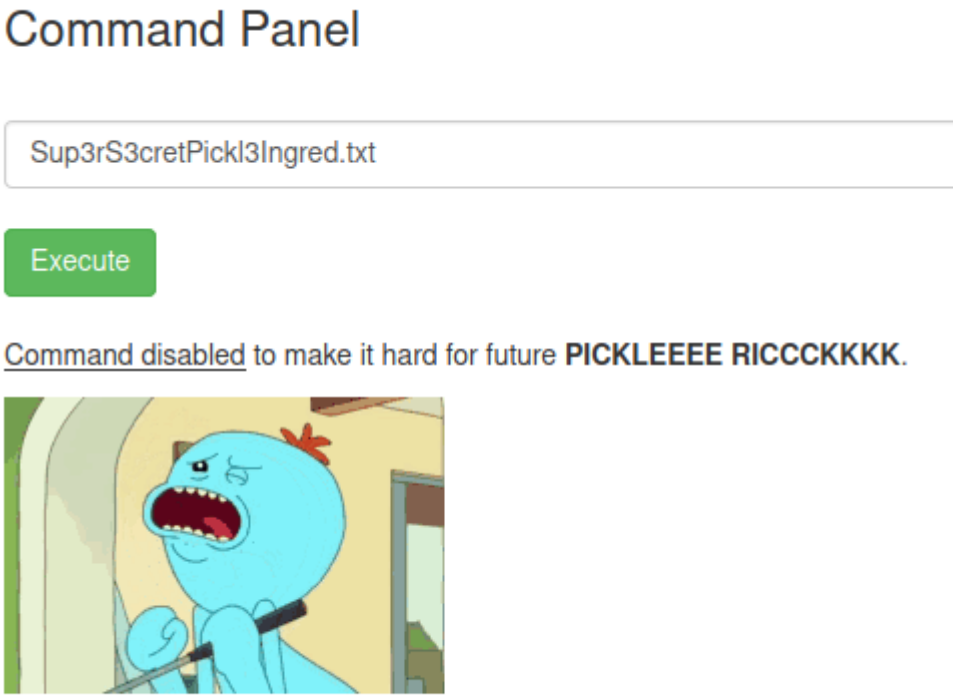
We are successfully login into the website.

▼ 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` .



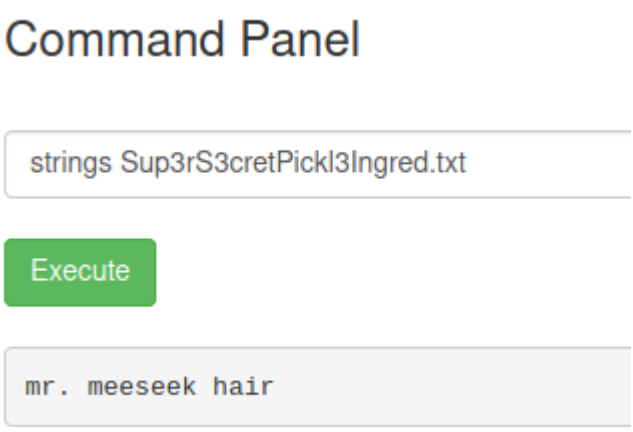
While trying to `cat` the content of this suspicious file, the webserver is disabled for the command we used.



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`

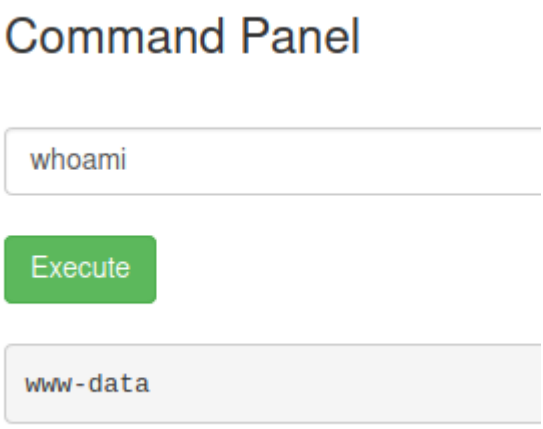
Flag 1 - mr. meeseek hair



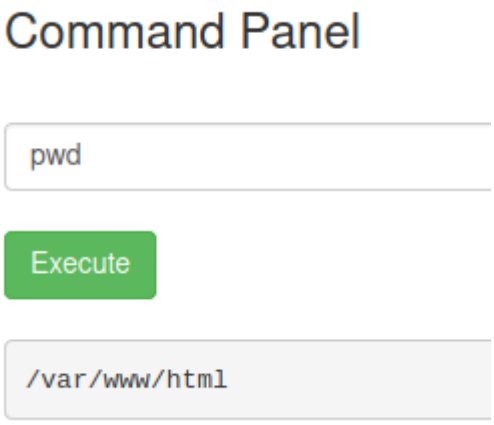
▼ Flag 2

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

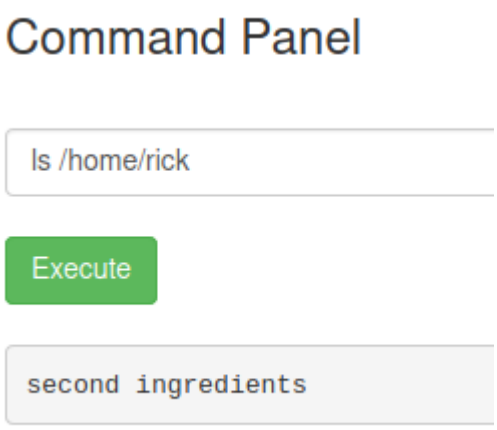
Used whoami to know that the username of the current user we are being.



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



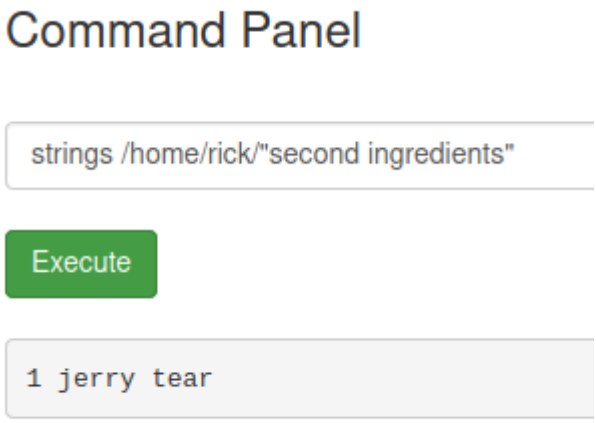
Used command `ls /home` we can see that there is two user, rick and ubuntu. Lets list out the content of rick directory and we found the second ingredients.



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



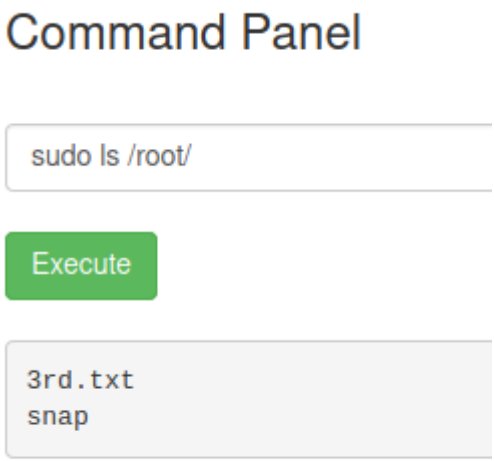
▼ Flag 3

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.

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

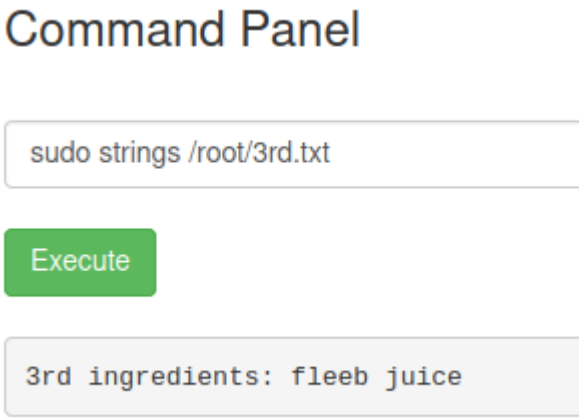
We found the 3rd.txt file in the directory. Lets output it with the same method as well.



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