Done By: Prasanth P

Platform: Tryhackme

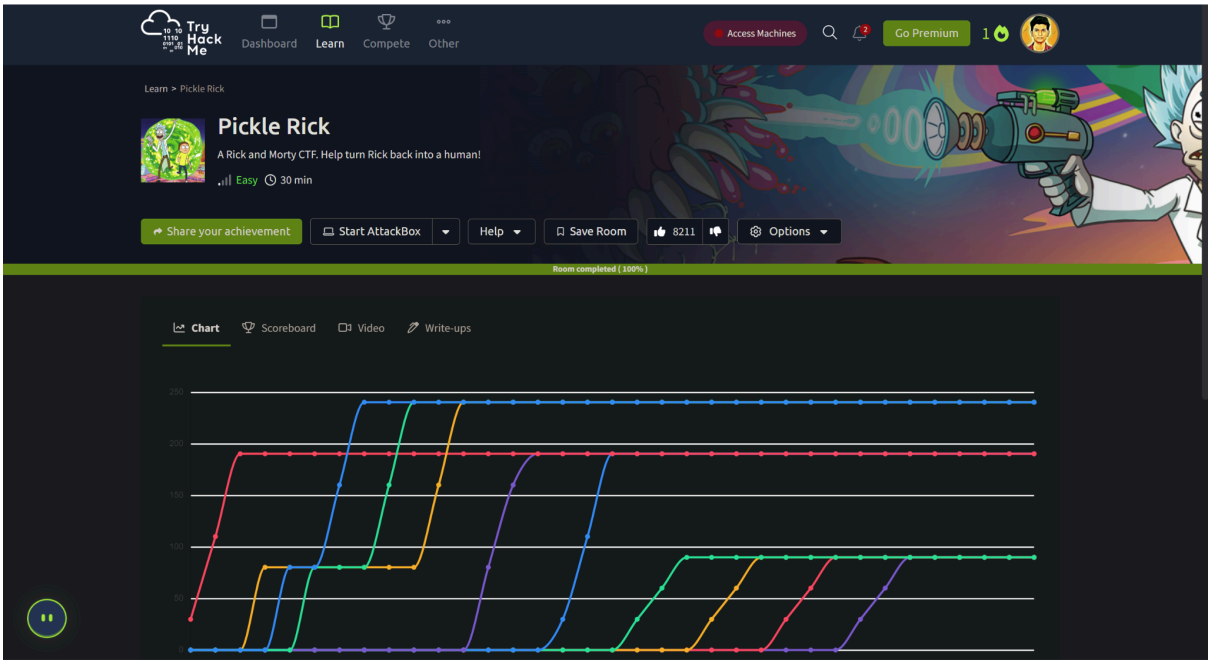
Category: CTF / Web Exploitation

Room: Pickle Rick

Difficulty: Easy

Aim:

To exploit a web server and find three ingredients to help Rick make his potion and transform himself back into a human from a pickle.

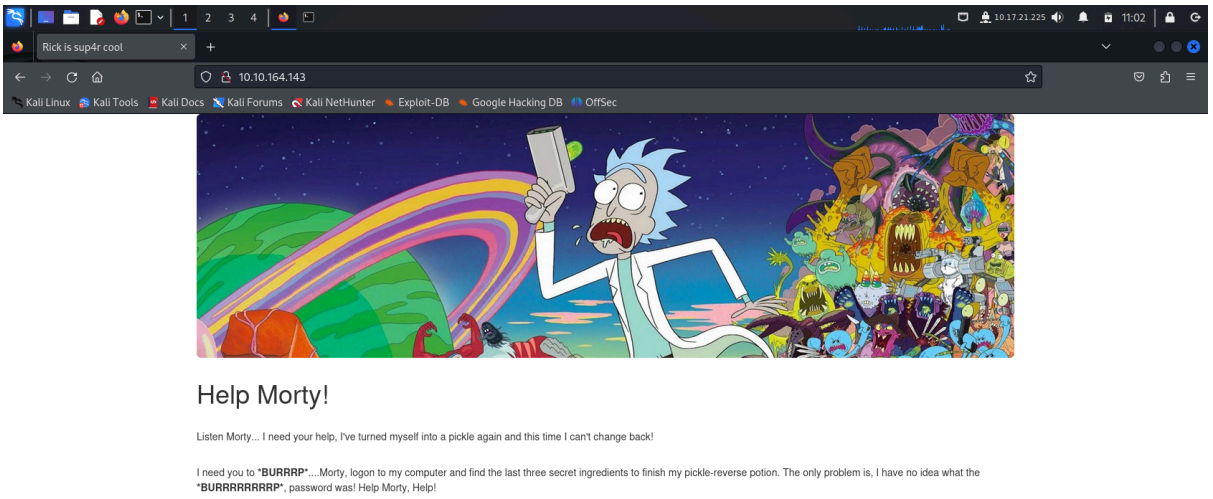


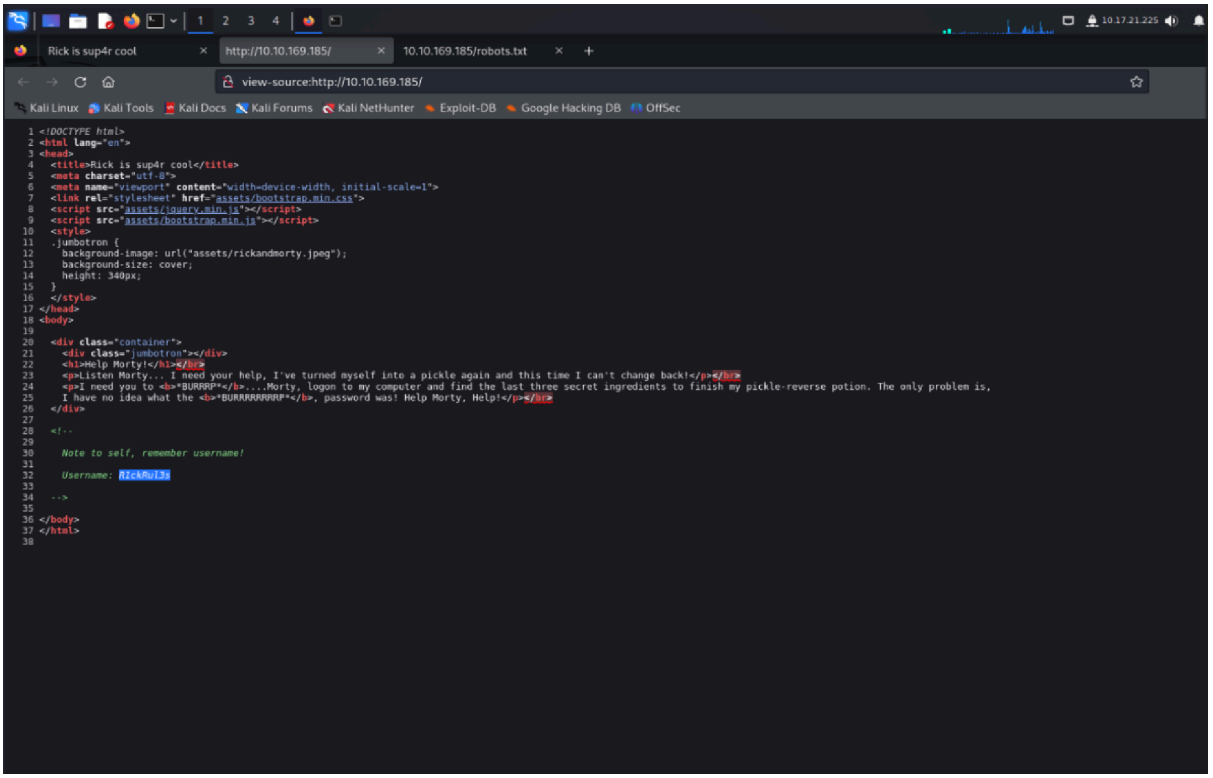
Tools Used:

- Virtual Box with Kali Linux
- Firefox Browser
- Nmap
- Gobuster

1.Access the website

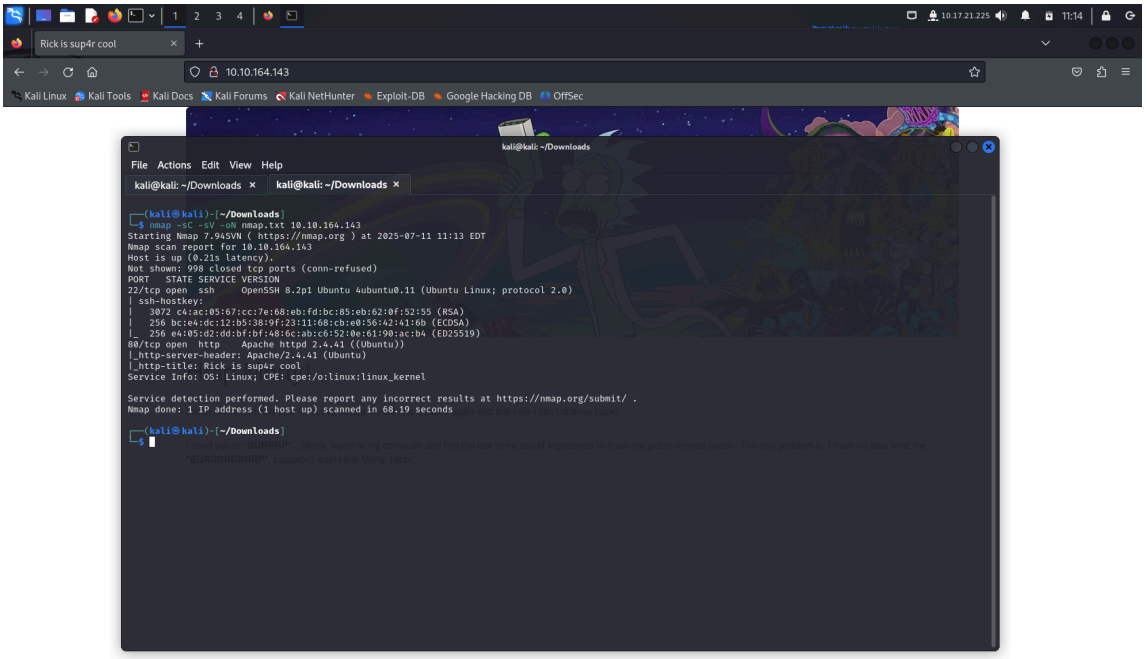
Navigated to the website by starting the machine in tryhackme.
Connected to the machine from Kali Linux by OpenVPN.
The IP was 10.10.164.143
Found a simple landing page with an image
I was unable to find further things, So then Inspected into the page source code.
Then I was able to find a comment stating a Username, RickRul3s





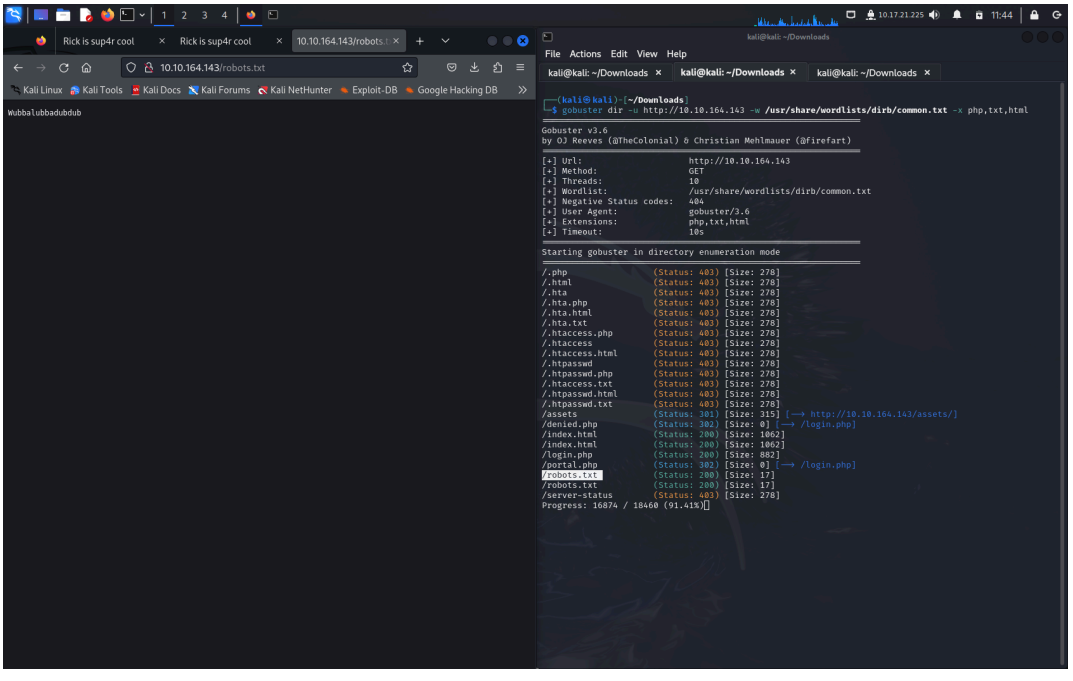
2. Nmap Scan

After landing on the page, I do a Nmap Scan and save the output in a file for future access.
After the scan I was able to find the open ports.



3. Gobuster Scan

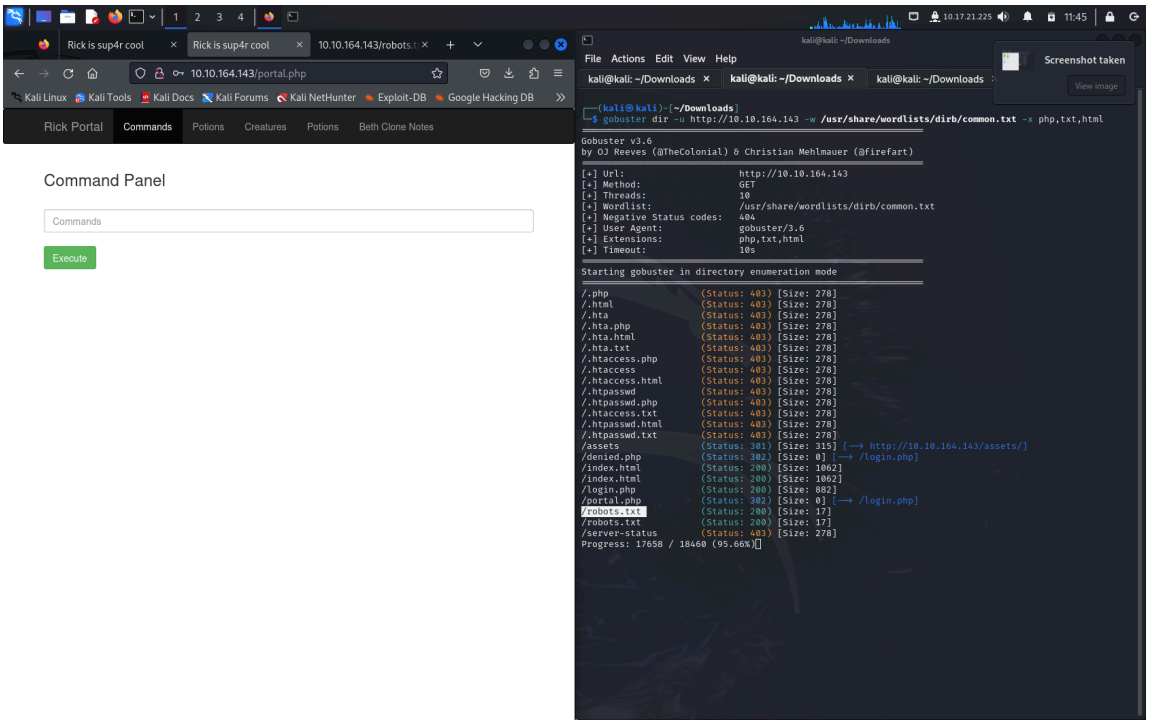
After identifying a web server (typically on ports 80 or 443, or other non-standard ports revealed by Nmap), the next step is to find hidden web resources..
So I used gobuster and was able to find all the web contents, directories and files that are not directly linked on the website, potentially revealing administrative panels, configuration files, or other information.
I was able to find the password from the robot.txt.
Then I located a login.php and was able to login successfully..

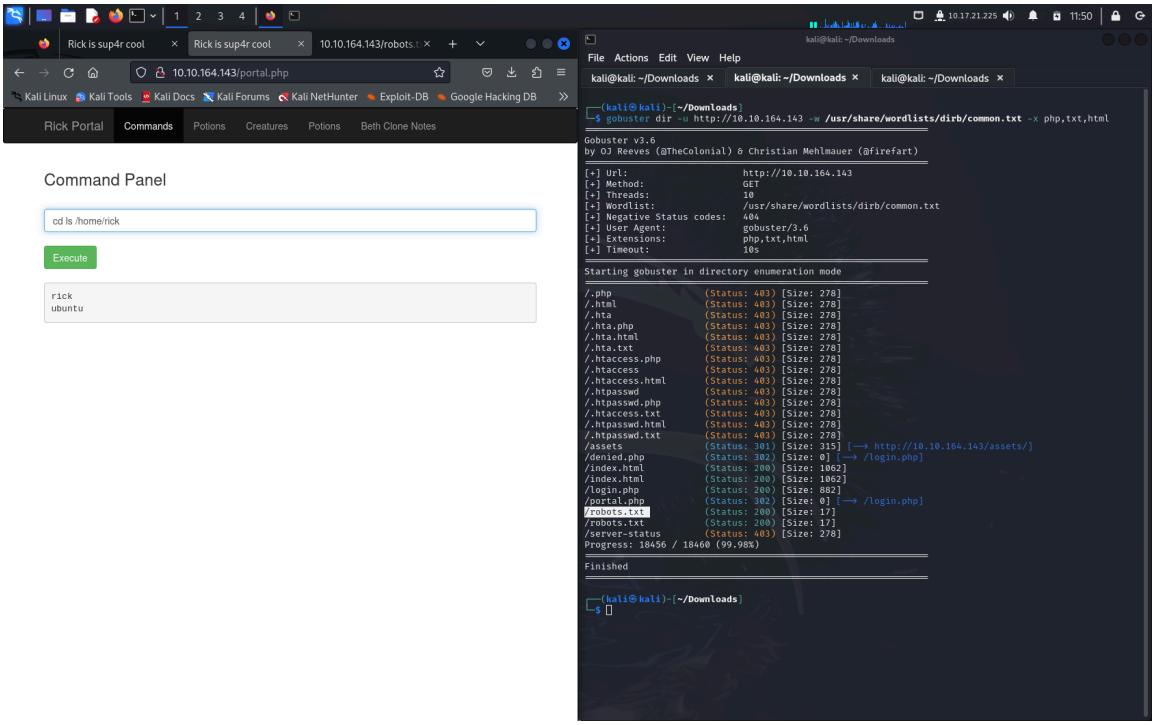


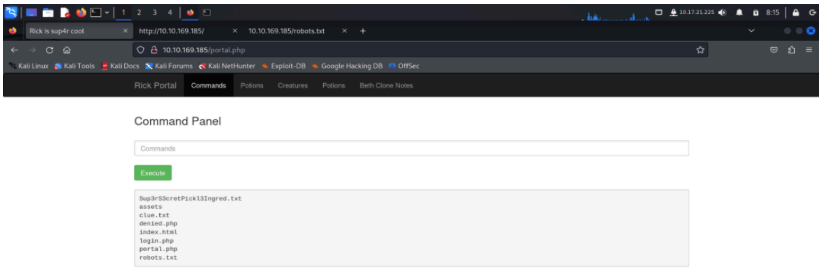
4. After login

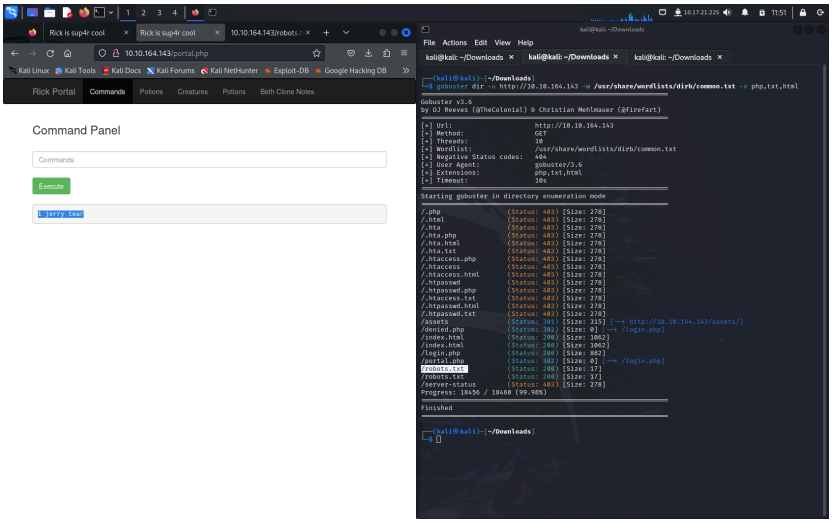
After login, I found a simple command panel.
So I used several linux commands to find the files I need.

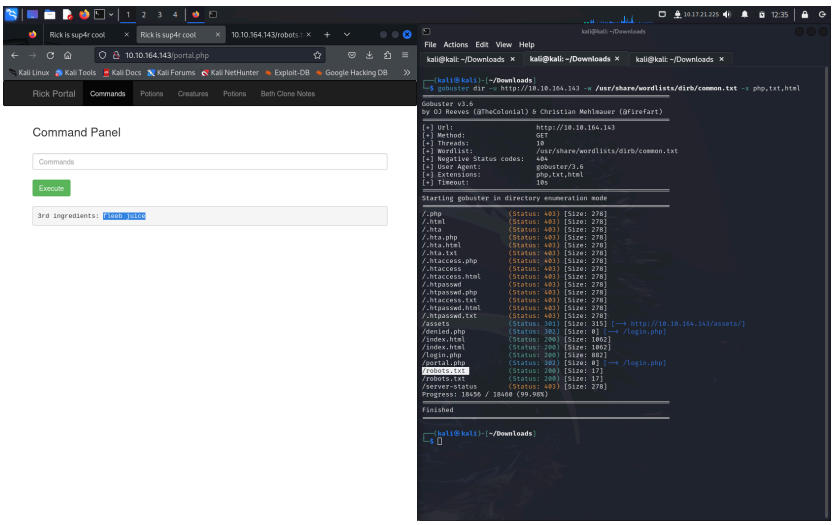
- pwd - to find the current directory
- cd - to navigate to folders
- ls - to list the file in the directory
- sudo - for root access
- less - the cat command for seeing the file content was disabled, so I guessed the less command and was successful.

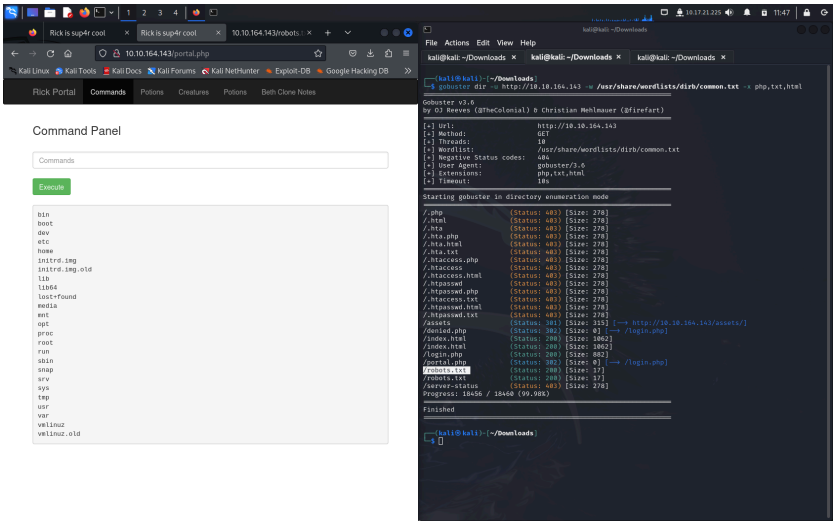


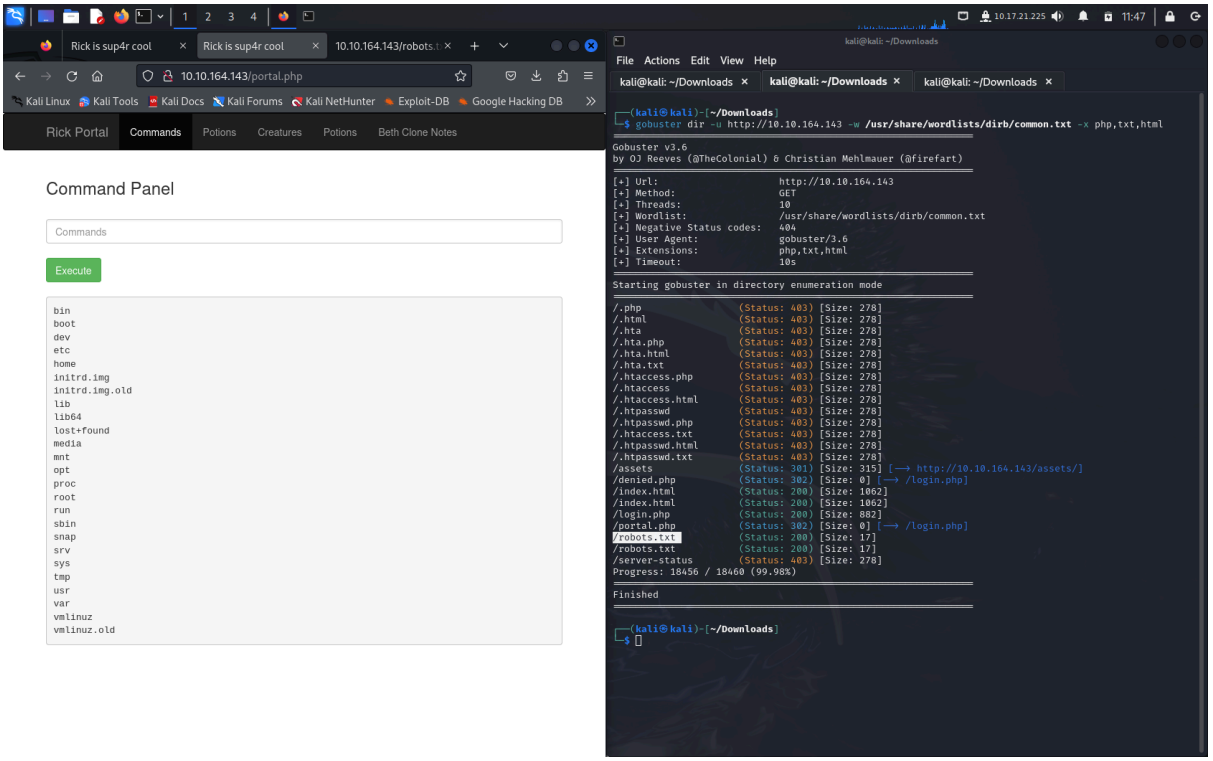



Rick is sup4r cool
http://10.10.169.185/
10.10.169.185/robots.txt
10.10.169.185/portal.php
Rick Portal
Commands
Potions
Creatures
Potions
Beth Clone Notes
Command Panel
Commands
Execute
Sup3rS3cretPick13Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt

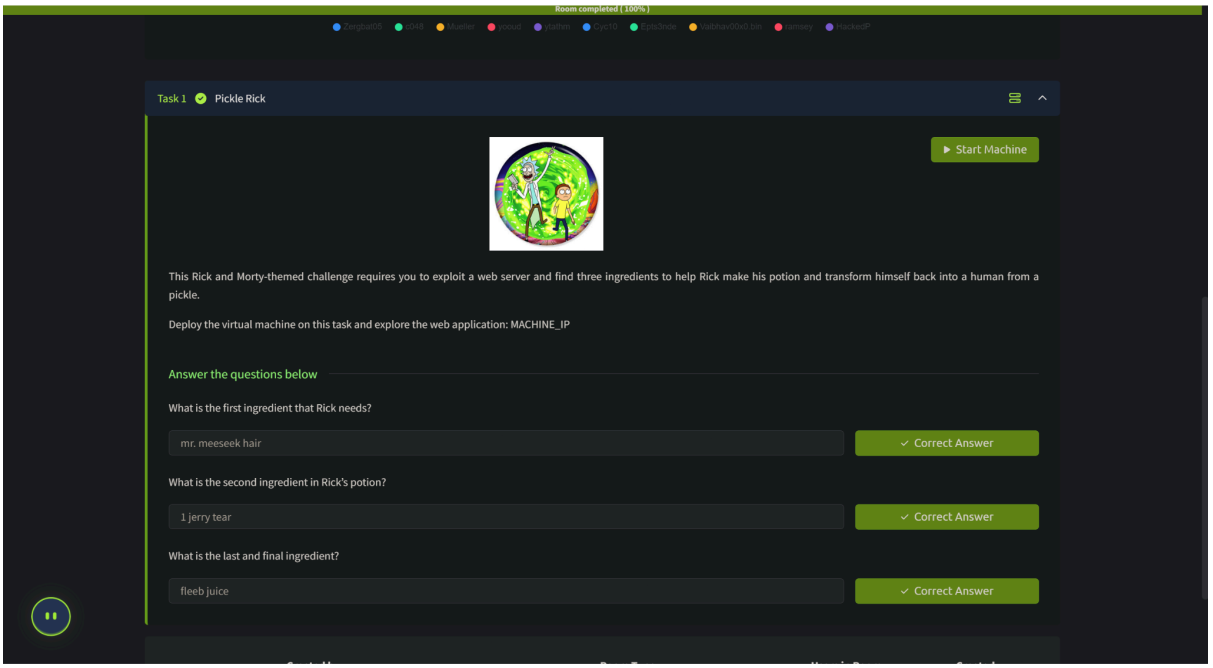

10.10.164.143/portal.php
Rick Portal
Commands
Potions
Creatures
Potions
Beth Clone Notes
Command Panel
Commands
Execute
1 jerry tear
kali@kali: ~/Downloads
$ gobuster dir -u http://10.10.164.143 -w /usr/share/wordlists/dirb/common.txt -x php,txt,html
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://10.10.164.143
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,txt,html
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
/.php (Status: 403) [Size: 278]
/.html (Status: 403) [Size: 278]
/.hta (Status: 403) [Size: 278]
/.hta.php (Status: 403) [Size: 278]
/.hta.html (Status: 403) [Size: 278]
/.hta.txt (Status: 403) [Size: 278]
/.htaccess.php (Status: 403) [Size: 278]
/.htaccess (Status: 403) [Size: 278]
/.htaccess.html (Status: 403) [Size: 278]
/.htpasswd (Status: 403) [Size: 278]
/.htpasswd.php (Status: 403) [Size: 278]
/.htaccess.txt (Status: 403) [Size: 278]
/.htpasswd.html (Status: 403) [Size: 278]
/.htpasswd.txt (Status: 403) [Size: 278]
/assets (Status: 301) [Size: 315] [--> http://10.10.164.143/assets/]
/denied.php (Status: 302) [Size: 0] [--> /login.php]
/index.html (Status: 200) [Size: 1062]
/index.html (Status: 200) [Size: 1062]
/login.php (Status: 200) [Size: 882]
/portal.php (Status: 302) [Size: 0] [--> /login.php]
/robots.txt (Status: 200) [Size: 17]
/robots.txt (Status: 200) [Size: 17]
/server-status (Status: 403) [Size: 278]
Progress: 18456 / 18460 (99.98%)
Finished


10.10.164.143/portal.php
Rick Portal
Commands
Potions
Creatures
Potions
Beth Clone Notes
Command Panel
Commands
Execute
3rd ingredients: fleeb juice
kali@kali: ~/Downloads
$ gobuster dir -u http://10.10.164.143 -w /usr/share/wordlists/dirb/common.txt -x php,txt,html
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://10.10.164.143
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,txt,html
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
/.php (Status: 403) [Size: 278]
/.html (Status: 403) [Size: 278]
/.hta (Status: 403) [Size: 278]
/.hta.php (Status: 403) [Size: 278]
/.hta.html (Status: 403) [Size: 278]
/.hta.txt (Status: 403) [Size: 278]
/.htaccess.php (Status: 403) [Size: 278]
/.htaccess (Status: 403) [Size: 278]
/.htaccess.html (Status: 403) [Size: 278]
/.htpasswd (Status: 403) [Size: 278]
/.htpasswd.php (Status: 403) [Size: 278]
/.htaccess.txt (Status: 403) [Size: 278]
/.htpasswd.html (Status: 403) [Size: 278]
/.htpasswd.txt (Status: 403) [Size: 278]
/assets (Status: 301) [Size: 315] [--> http://10.10.164.143/assets/]
/denied.php (Status: 302) [Size: 0] [--> /login.php]
/index.html (Status: 200) [Size: 1062]
/index.html (Status: 200) [Size: 1062]
/login.php (Status: 200) [Size: 882]
/portal.php (Status: 302) [Size: 0] [--> /login.php]
/robots.txt (Status: 200) [Size: 17]
/robots.txt (Status: 200) [Size: 17]
/server-status (Status: 403) [Size: 278]
Progress: 18456 / 18460 (99.98%)
Finished


10.10.164.143/portal.php
Rick Portal
Commands
Potions
Creatures
Potions
Beth Clone Notes
Command Panel
Commands
Execute
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
kali@kali: ~/Downloads
$ gobuster dir -u http://10.10.164.143 -w /usr/share/wordlists/dirb/common.txt -x php,txt,html
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://10.10.164.143
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,txt,html
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
/.php (Status: 403) [Size: 278]
/.html (Status: 403) [Size: 278]
/.hta (Status: 403) [Size: 278]
/.hta.php (Status: 403) [Size: 278]
/.hta.html (Status: 403) [Size: 278]
/.hta.txt (Status: 403) [Size: 278]
/.htaccess.php (Status: 403) [Size: 278]
/.htaccess (Status: 403) [Size: 278]
/.htaccess.html (Status: 403) [Size: 278]
/.htpasswd (Status: 403) [Size: 278]
/.htpasswd.php (Status: 403) [Size: 278]
/.htaccess.txt (Status: 403) [Size: 278]
/.htpasswd.html (Status: 403) [Size: 278]
/.htpasswd.txt (Status: 403) [Size: 278]
/assets (Status: 301) [Size: 315] [--> http://10.10.164.143/assets/]
/denied.php (Status: 302) [Size: 0] [--> /login.php]
/index.html (Status: 200) [Size: 1062]
/index.html (Status: 200) [Size: 1062]
/login.php (Status: 200) [Size: 882]
/portal.php (Status: 302) [Size: 0] [--> /login.php]
/robots.txt (Status: 200) [Size: 17]
/robots.txt (Status: 200) [Size: 17]
/server-status (Status: 403) [Size: 278]
Progress: 18456 / 18460 (99.98%)
Finished



After all these steps, I was able to complete this task successfully.



5. Conclusion

Finally I was abv to find all the ingredients and bring Rick back to his normal life.
This task helped me gain new knowledge and was a very good experience.