

Done By: Prasanth P

Platform: Tryhackme

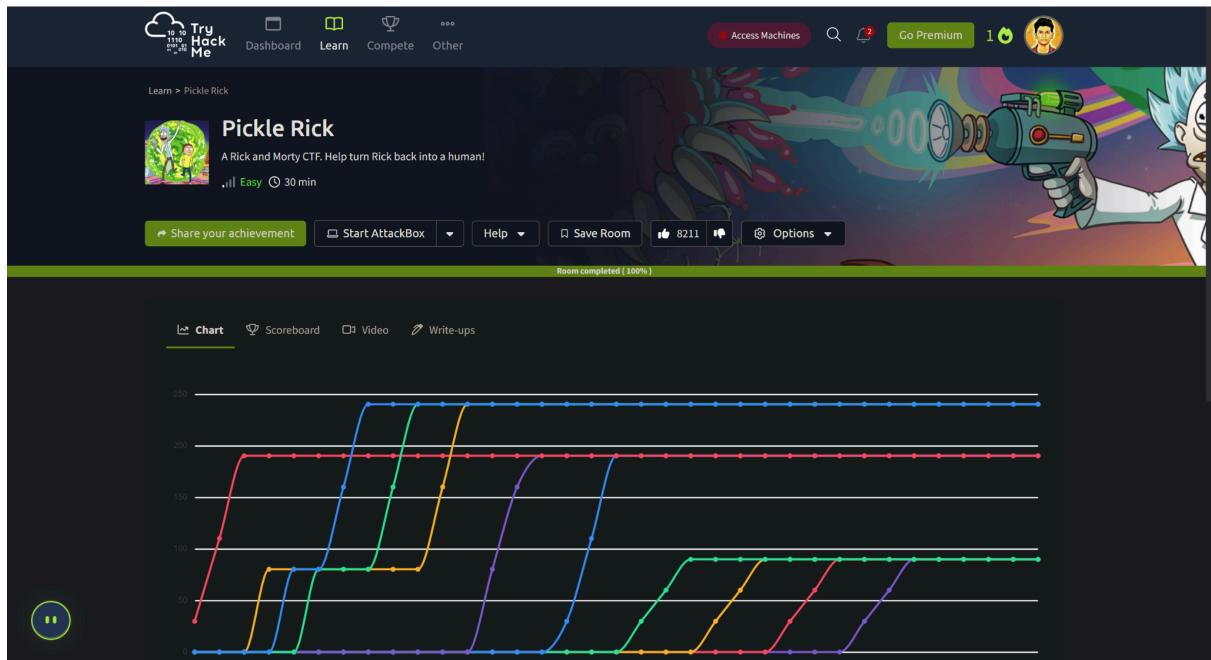
Category: CTF / Web Exploitation

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.

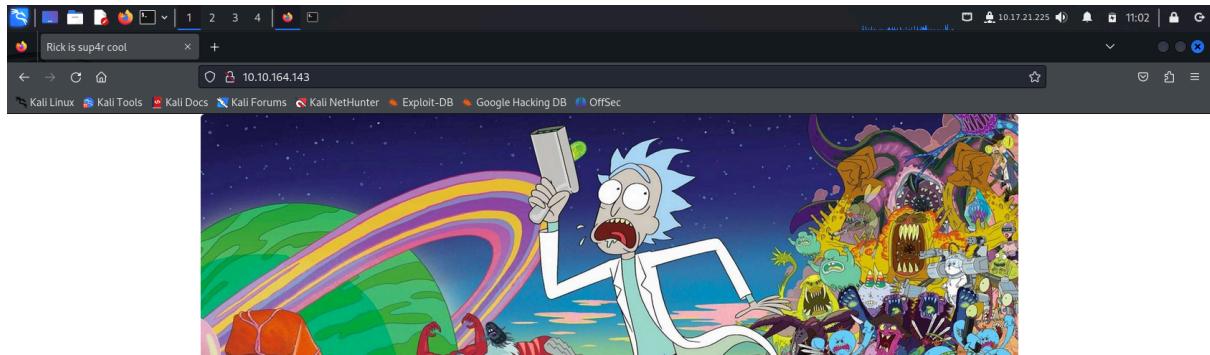
Connected to the machine from Kali Linux by OpenVPN.

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



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 "BURRRRRRRRP", password was! Help Morty, Help!

A screenshot of a terminal window titled 'view-source:http://10.10.169.185/'. The code shown is the source code of the website. It includes an HTML header with a title 'Rick is sugar cool', meta tags for viewport and bootstrap, and a CSS rule for a jumbotron background image. The body contains a jumbotron with a heading 'Help Morty!', a paragraph asking for help, and a note: 'Note to self, remember username! Username: RickRul3s'. The code ends with closing body and html tags.

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.

Rick is sup4r cool

10.10.164.143

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

```
[kali㉿kali:~/Downloads] kali㉿kali:~/Downloads $ nmap -sC -sV -oN nmap.txt 10.10.164.143
Starting Nmap 7.94 ( https://nmap.org ) at 2025-07-11 11:13 EDT
Nmap scan report for 10.10.164.143
Host is up (0.21s latency).
Not shown: 997 services closed by port
PORT      STATE SERVICE VERSION
22/tcp    open  ssh        OpenSSH 8.2p1 Ubuntu aubuntu#0.11 (Ubuntu; protocol 2.0)
| ssh-hostkey:
|   0x72:c4:dc:05:67:cc:7e:68:eb:fdb:e8:5:eb:62:0:f52:55 (RSA)
|   259:bc:e4:dc:12:b5:38:9:f2:23:11:68:ch:e0:56:42:41:6b (EDSA)
|_  256:ea:95:d2:dd:bf:bf:48:6c:ab:c6:52:9e:61:90:ac:b4 (D25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Rick is sup4r cool
Service Info: OS: Linux; CPE: cpe:/o:linlinux: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 68.19 seconds
```

(kali㉿kali:~/Downloads) ↵ [!] I need your help! BURRRRRP...Merry, 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 "BURRRRRRRRP..." password was! Help Merry, Help!

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.

The screenshot shows a Kali Linux desktop environment. In the top right, there's a terminal window titled 'kali@kali: ~/Downloads' with the command:

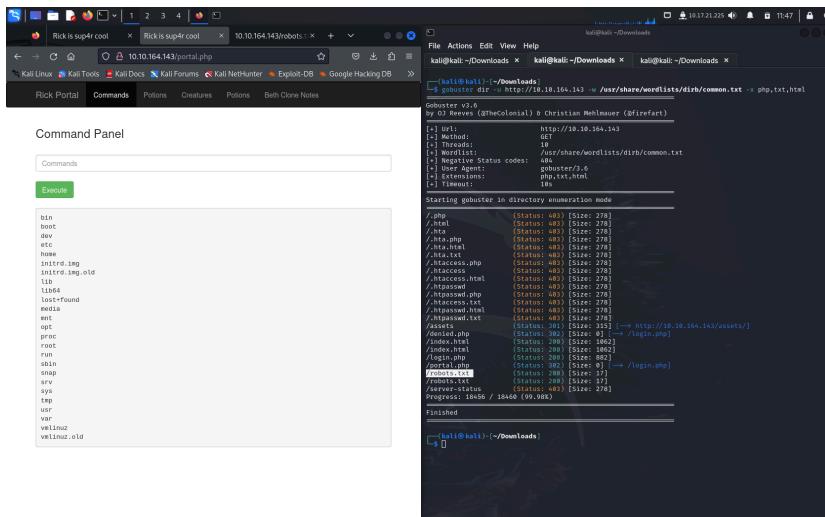
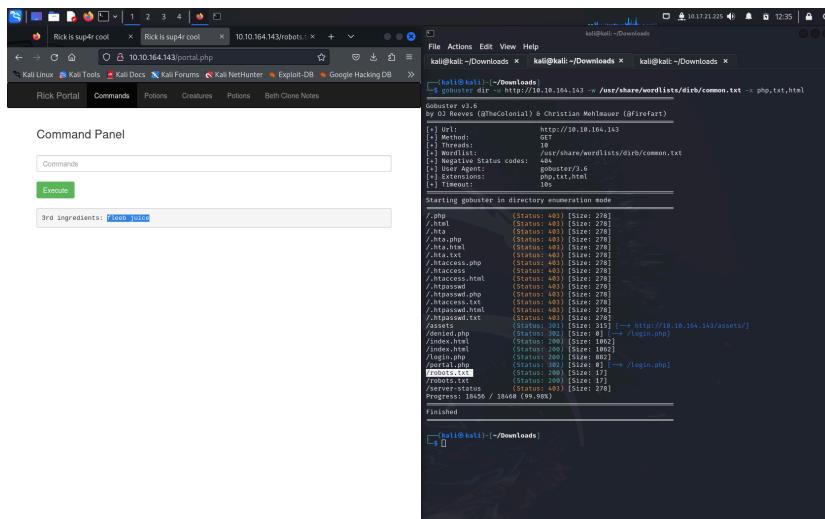
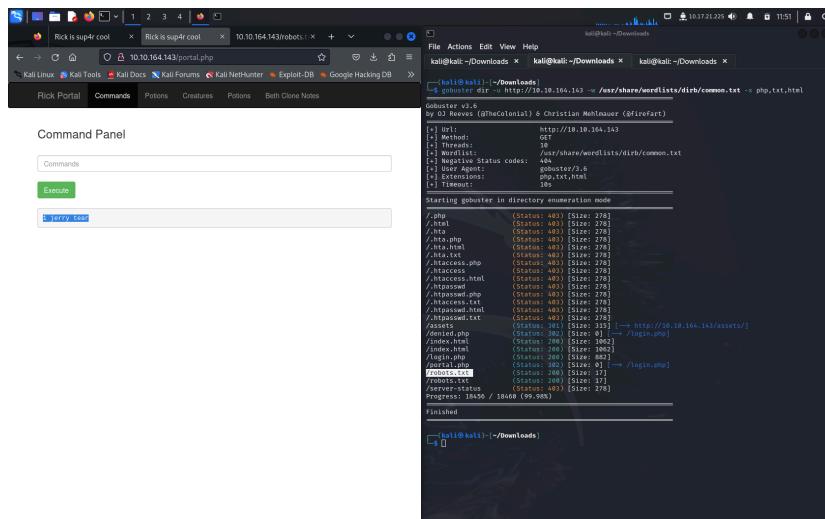
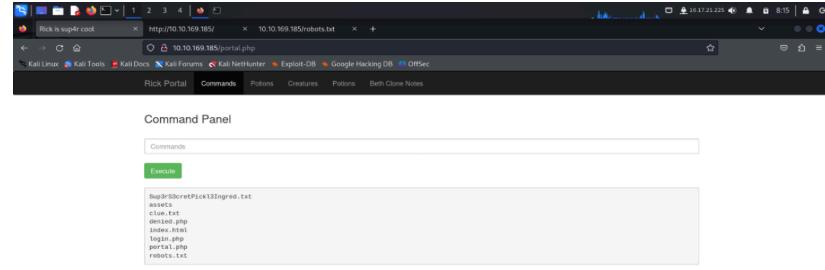
```
gobuster v3.6  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
[+] Url:          http://10.10.164.143  
[+] Threads:      10  
[+] Threads:      /usr/share/wordlists/dirb/common.txt  
[+] Threads:      404  
[+] Timeout:      gobuster/3.6  
[+] Extensions:  php,txt,html  
[+] Threads:      10s
```

Below this, the terminal shows the output of the gobuster command, which has found several files including 'assets', 'denied.php', 'index.html', 'index.php', 'login.php', 'portal.php', and 'robots.txt'. The progress bar at the bottom indicates 95.66% completion.

In the bottom left, there's a browser window titled 'Rick is sup4r cool' showing a 'Command Panel' with a text input field and a green 'Execute' button.

This screenshot is similar to the one above, showing the same terminal session and browser window. The terminal window now shows the result of the 'cd ls /home/rick' command, listing files 'rick' and 'ubuntu'.

The terminal output for the gobuster command is identical to the previous screenshot, showing the same findings and progress.



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

Room completed (100%)

ergbat05 c048 Muslier cooud ytaifnn cyc10 Epita3nde Vaibhav0x0.bin ramsey HackedD

Task 1 Pickle Rick



▶ Start Machine

This Rick and Morty-themed challenge requires you 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.

Deploy the virtual machine on this task and explore the web application: MACHINE_IP

Answer the questions below

What is the first ingredient that Rick needs?

mr. meeseek hair

✓ Correct Answer

What is the second ingredient in Rick's potion?

1 jerry tear

✓ Correct Answer

What is the last and final ingredient?

fleeb juice

✓ Correct Answer

5. Conclusion

Finally I was able 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.