

Pickle Rick CTF - TryHackMe Quick Run-Through!

What I Did

Alright, so I jumped into the Pickle Rick CTF on TryHackMe. The goal was to help Rick get back to normal by finding three secret ingredients.

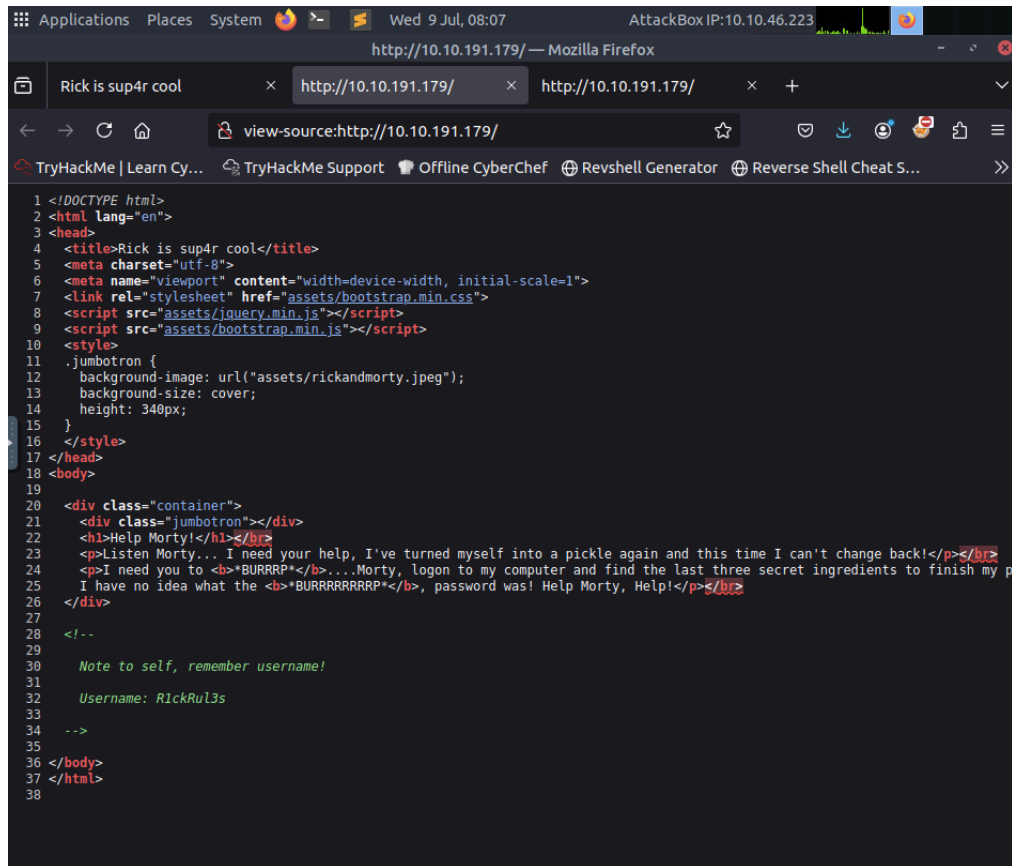
Getting Started (Recon)

1. **Found the IP:** First thing was finding the machine's IP, which was 10.10.191.179.
2. **Nmap Scan:** Ran an Nmap scan (`nmap -sC -sV 10.10.191.179`) to see what was open.

```
Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-10 22:35 +0530
Nmap scan report for 10.10.201.188
Host is up (0.19s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
|   3072 f6:8e:5c:a5:e3:50:ea:03:00:f1:75:de:ea:9e:cf:ba (RSA)
|   256  b7:68:01:6c:3a:d2:2a:4d:e7:ad:0a:43:bb:a0:27:16 (ECDSA)
|_  256  f3:47:5b:e0:a5:ec:c7:6d:ca:76:44:73:ee:00:cc:f6 (ED25519)
80/tcp    open  http
|_ http-title: Rick is sup4r cool

Nmap done: 1 IP address (1 host up) scanned in 18.72 seconds
```

3. **Website Check:** Hit up the website at `http://10.10.191.179/`. It had a cool Rick and Morty theme and a message from Rick about needing help and a "BURRRRRRAP" password.
4. **Source Code Dive:** Peeped at the website's source code and snagged a username hidden in a comment: R1ckRul3s.

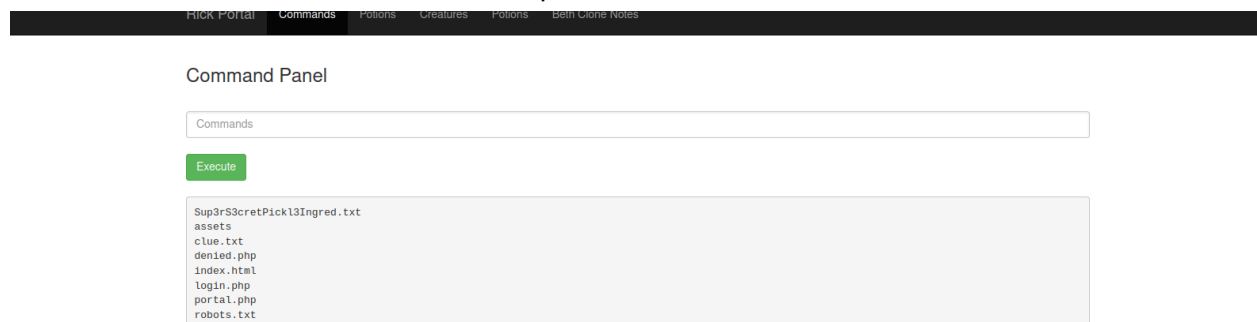


```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4 <title>Rick is sup4r cool</title>
5 <meta charset="utf-8">
6 <meta name="viewport" content="width=device-width, initial-scale=1">
7 <link rel="stylesheet" href="assets/bootstrap.min.css">
8 <script src="assets/jquery.min.js"></script>
9 <script src="assets/bootstrap.min.js"></script>
10 <style>
11 .jumbotron {
12   background-image: url("assets/rickandmarty.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>BURRRRP*</b>...Morty, logon to my computer and find the last three secret ingredients to finish my p
25 I have no idea what the <b>BURRRRRRRRRP*</b>, password was! Help Morty, Help!</p></div>
26 </div>
27
28 <!--
29 Note to self, remember username!
30
31 Username: RickRu13s
32
33 -->
34
35
36 </body>
37 </html>
38
```

5. **Gobuster Fun:** Fired up gobuster (gobuster dir -u http://10.10.191.179 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt) and found robots.txt and login.php.
6. **Robots.txt Clue:** Checked robots.txt (http://10.10.191.179/robots.txt) and BOOM! Found the password: Wubbalubbadubdub.

Getting In (Exploitation)

1. **Logged In:** Used RICKROLu3s and Wubbalubbadubdub to log into login.php. Got into some kind of command execution panel. Sweet!



2. **First Ingredient:** In the panel, I found Sup3rS3cretPickl3Ingred.txt. cat didn't work, but tac did the trick! First ingredient: mr. meeseek hair.
3. **Second Ingredient:** Explored / and /home, and found Rick's home directory. Inside, the second ingredient was waiting: 1 jerry tear.
4. **Third Ingredient & Root Access:** The last one was tricky. After some digging, I realized the current user could sudo without a password. So, I just sudo'd my way into the /root folder and grabbed the final ingredient: fleeb juice.

P.S : used AI to generate the report btw :)