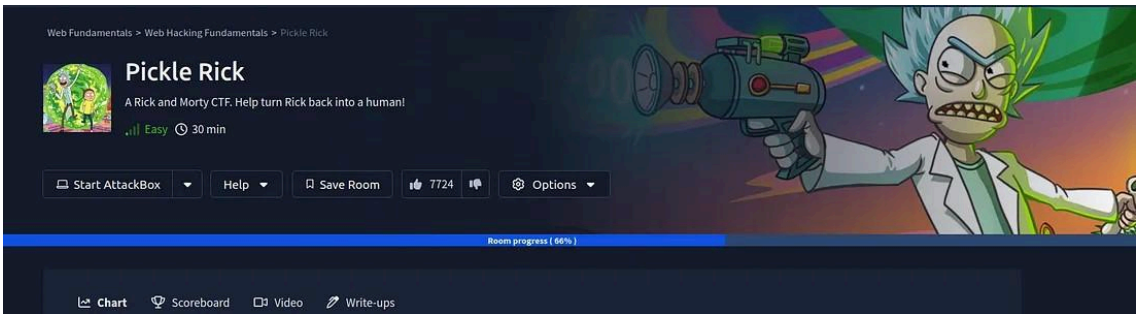
Pickle Rick

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

📚 Introduction



The Pickle Rick challenge is part of the Web Fundamentals path on TryHackMe. Although it’s marked as an Easy room, it can be a bit tricky if you're not sure what to look for.

When I first attempted this room, I spent a lot of time stuck in the enumeration phase. I used the default dirb wordlist, which didn’t reveal anything useful. As a result, I ended up wasting several hours searching for vulnerabilities in Apache and SSH — which were not actually relevant to solving the challenge.

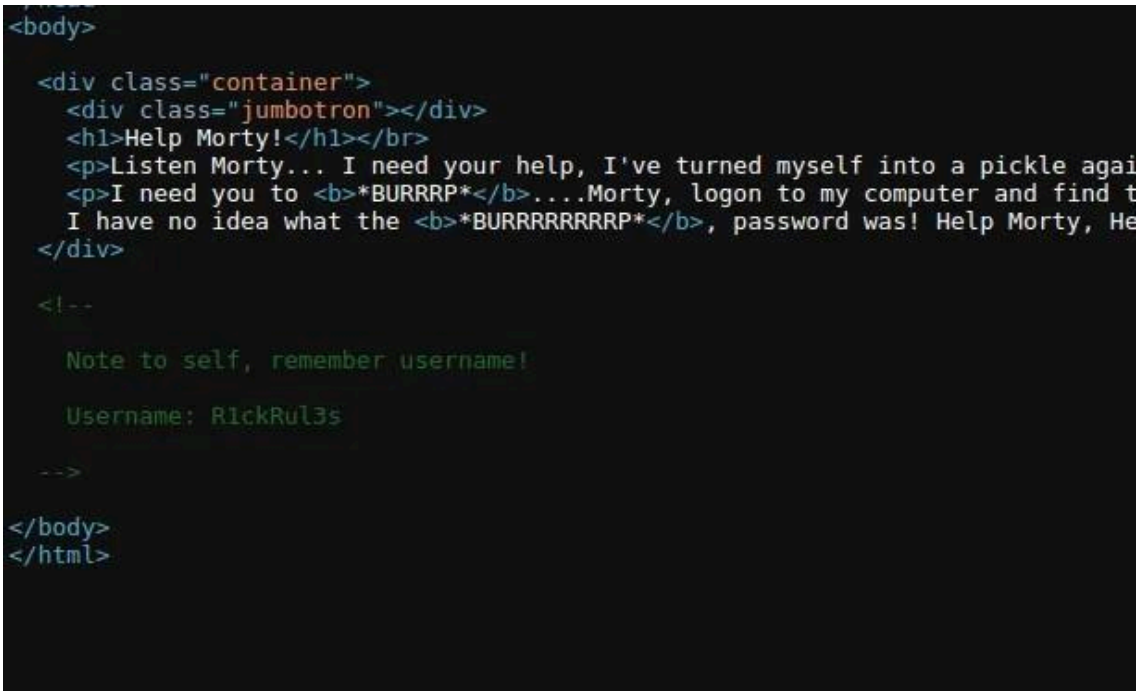
🔐 Looking for the Password

Even though the page says the password is:

> “Help Morty, Help!”

…it turns out that this isn’t the actual password. Since we’re in Rick’s world, it’s not that straightforward.

So, I decided to check the page source — and that’s where things started to get interesting.



👤 Found Username

From the clues in the page source, I discovered the username:

Username: R1ckRul3s

This was likely needed for logging into the web panel or accessing restricted files later in the challenge.

🔍 Nmap Scan

I used Nmap to check which ports are open:

nmap 10.10.112.195

Result:

Port 22 → SSH (open)

Port 80 → HTTP (open)

Port 2105 → Filtered

What I did next:

Since port 80 is open, I continued checking the website.

I also kept SSH (port 22) in mind in case I found a username and password.

🗂️ Ignoring Unnecessary Ports

Only port 2105 seemed unusual, but I decided to leave it for now since it wasn't needed to complete the challenge.

🔍 Directory Fuzzing

Next, I started fuzzing for directories to find hidden paths on the website.

I used the following command:

```
dirb http://10.10.112.195
```

This helped me discover important directories and files that were not linked on the main page.

🔍 Key Results:

```
/assets/          → 200 OK (directory exists)
/login.php        → 200 OK (login page)
/robots.txt       → 200 OK (accessible)
/server-status    → 403 Forbidden
Many .htaccess & .ht* files → 403 Forbidden
```

🤖 robots.txt

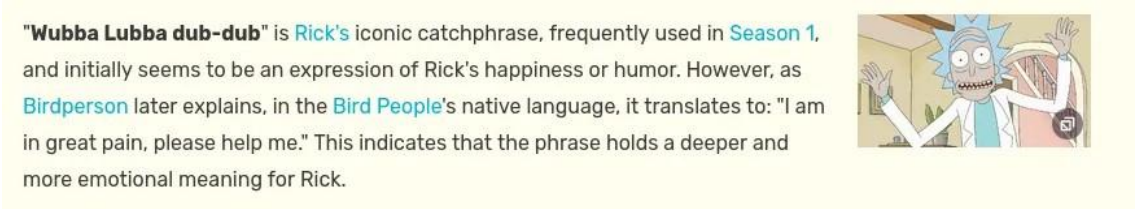
Found: /robots.txt

Opened it in the browser.

This file tells search engines what to avoid.

Sometimes it shows hidden paths.

It gave a helpful clue in this case.!



Found password "Help Morty, Help!" on the first page.

login.php returns 200 OK, confirming it's a valid login page.

Use the password there to access Ricky's computer.

Visiting the IP shows a message:

Password = "Help Morty, Help!"

Viewing page source reveals:

Username = R1ckRul3s

Ran nmap 10.10.112.195

Open ports: 22, 80, 2105 (filtered)

Directory fuzzing with dirsearch:

Notable finds:

/login.php → 200 OK

/robots.txt, /assets/, several 403s

Used login credentials:

Username: R1ckRul3s

Password: "Help Morty, Help!"

→ Login successful

Web shell is restricted — used base64 to read files.

Found files and decoded them:

1. base64 Sup3rS3cretPickl3Ingred.txt

→ echo "bXIuIG1lZXNlZWsgaGFpcgo=" | base64 -d

→ mr. meeseek hair

2. base64 clue.txt

→ echo "TG9vayBhcm91bmQgdGhlIGZpbGUgc3lzdGVtIGZvciB0aGUgb3RoZXIgaW5ncmVkaWVudC4K" | base64 -d

→ Hint: Check the file system

3. Navigated using ls .., ls ../..

Found in /home/rick/

→ base64 /home/rick/*

→ echo "MSBqZXJyeSB0ZWFyCg==" | base64 -d

→ 1 jerry tear

4. Used sudo to access root

→ sudo base64 /root/3rd.txt

→ fleeb juice

Final Ingredients:

mr. meeseek hair

1 jerry tear

fleeb juice
