CTF Report

By: Saniya Mary Jacob
CTF Room: Pickle Rick – TryHackMe

Scenario

Rick has turned himself into a pickle… again! My mission in this TryHackMe room was to **exploit a vulnerable web server**, uncover **three secret ingredients**, and help Rick brew a potion to become human once more. With tools like **nmap** and **gobuster**, I took on the role of a digital detective, diving into the world of Rick and Morty.

Tools Used

- `nmap` – for initial port scanning
- `gobuster` – for directory fuzzing
- **Web browser and terminal** – for exploitation and flag retrieval

---

Steps I got Involved

1. Reconnaissance with Nmap

I started by scanning the machine using `nmap -F <Machine IP>`. This revealed two open ports: **Port 22** – SSH & **Port 80** – HTTP.

2. Directory Discovery with Gobuster

Next, I explored hidden directories on the web server: gobuster dir -u http://<Machine IP> -w /usr/share/wordlists/dirb/common.txt
This helped me find several interesting paths like:

- `/index.html`
- `/login.php`
- `/robots.txt`

3. Exploring Robots.txt

Inside `robots.txt`, I found a suspicious string: **Wubbalubbadubdub...**Which felt like a *Rick-style clue*. I noted it down—it might be useful later.

4. Analyzing login.php

On inspecting `login.php`, I realized it was vulnerable. I attempted **simple authentication bypasses** and managed to access the admin panel without valid credentials—classic!

5. Exploiting the Admin Panel

Inside the admin panel, there was a command execution form where I could input arbitrary system commands. I used it to:

- List directories (`ls`)
- Read files (`cat <filename>`)
- And eventually extract the **three ingredients** Rick needed.

6. Capturing the Flags

Using the above steps, I successfully retrieved:

- Ingredient #1
- Ingredient #2
- Ingredient #3

Each was hidden in a file somewhere on the server…

Conclusion

The **Pickle Rick CTF** was both fun and educational. I practiced **web exploitation**, **directory fuzzing**, and **command injection** all within a creative Rick and Morty theme. It was a great exercise to reinforce core pentesting concepts in a light-hearted, hands-on way!