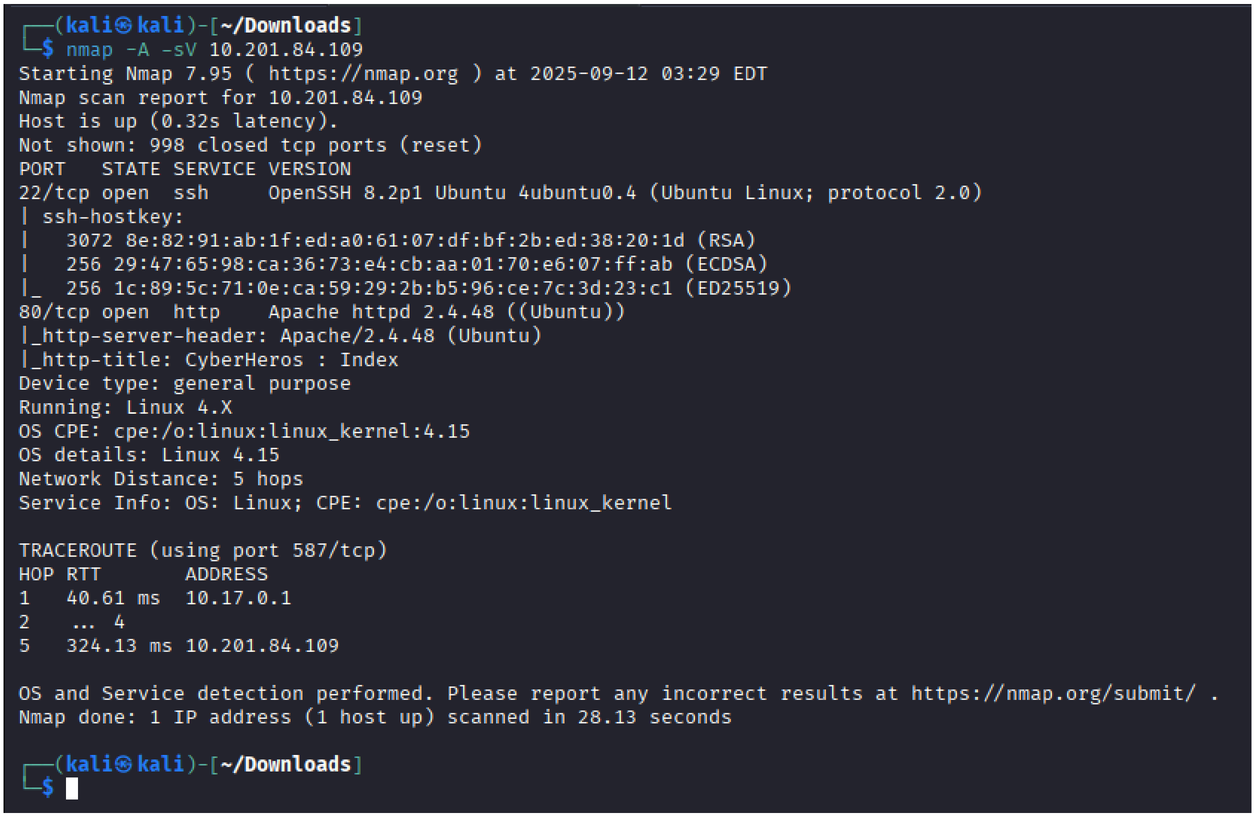
CyberHeroes

The given IP Address: 10.201.84.109
Connect to OpenVPN
<sudo openvpn>

Perform Nmap Scan on the IP address

Nmap -A -sV 10.201.84.109

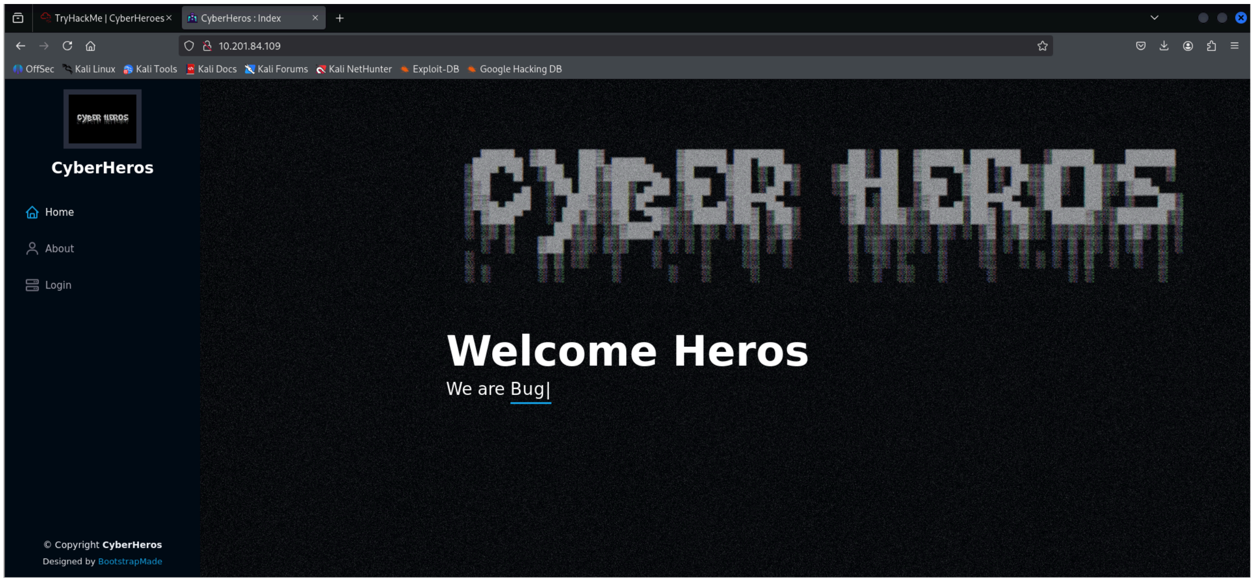


```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -A -sV 10.201.84.109
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-12 03:29 EDT
Nmap scan report for 10.201.84.109
Host is up (0.32s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   3072 8e:82:91:ab:1f:ed:a0:61:07:df:bf:2b:ed:38:20:1d (RSA)
|   256 29:47:65:98:ca:36:73:e4:cb:aa:01:70:e6:07:ff:ab (ECDSA)
|_  256 1c:89:5c:71:0e:ca:59:29:2b:b5:96:ce:7c:3d:23:c1 (ED25519)
80/tcp open  http    Apache httpd 2.4.48 ((Ubuntu))
|_http-server-header: Apache/2.4.48 (Ubuntu)
|_http-title: CyberHeros : Index
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
Network Distance: 5 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 587/tcp)
HOP RTT       ADDRESS
1   40.61 ms  10.17.0.1
2   ... 4
5   324.13 ms 10.201.84.109

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.13 seconds

┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

Identified open ports:

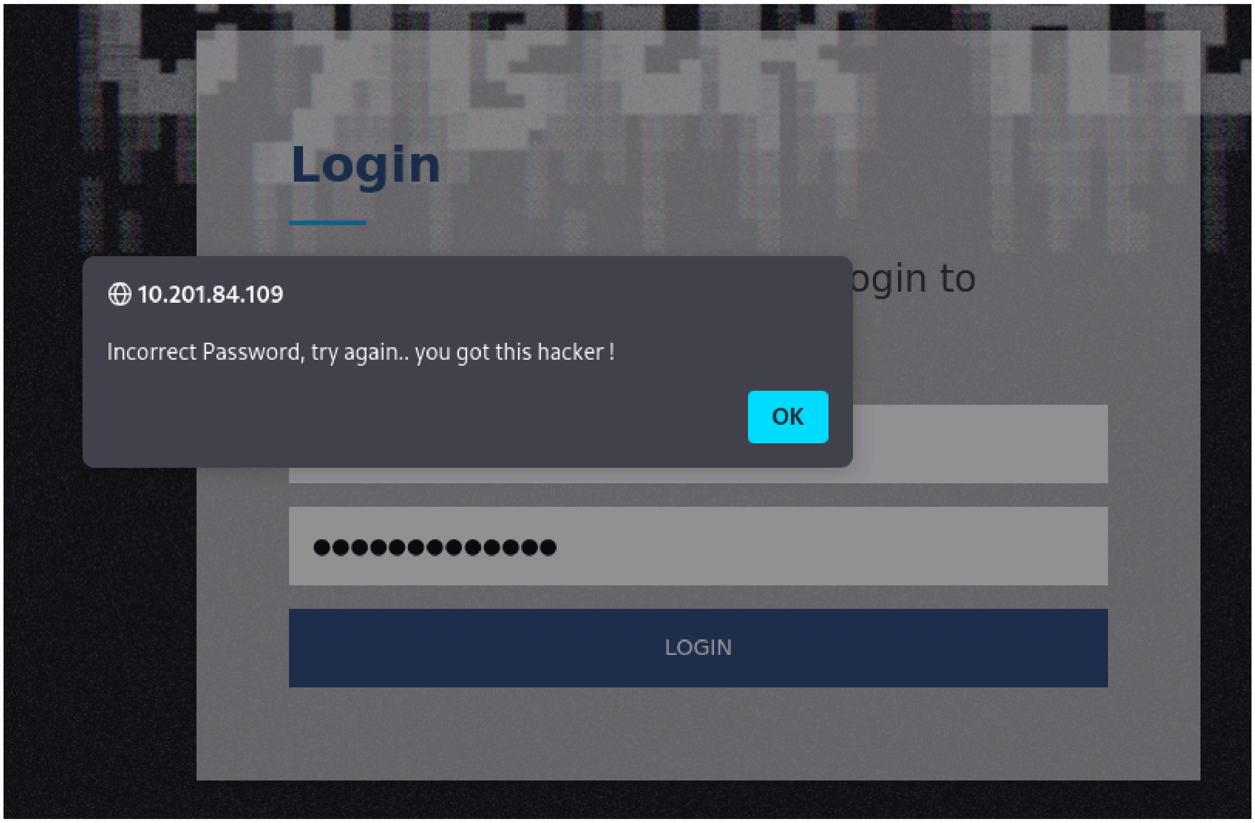
a. 80 - HTTP
b. 22 - SSH

Checking out the web browser



Attempting a simple sql injection attack:

‘ or ‘1’=’1



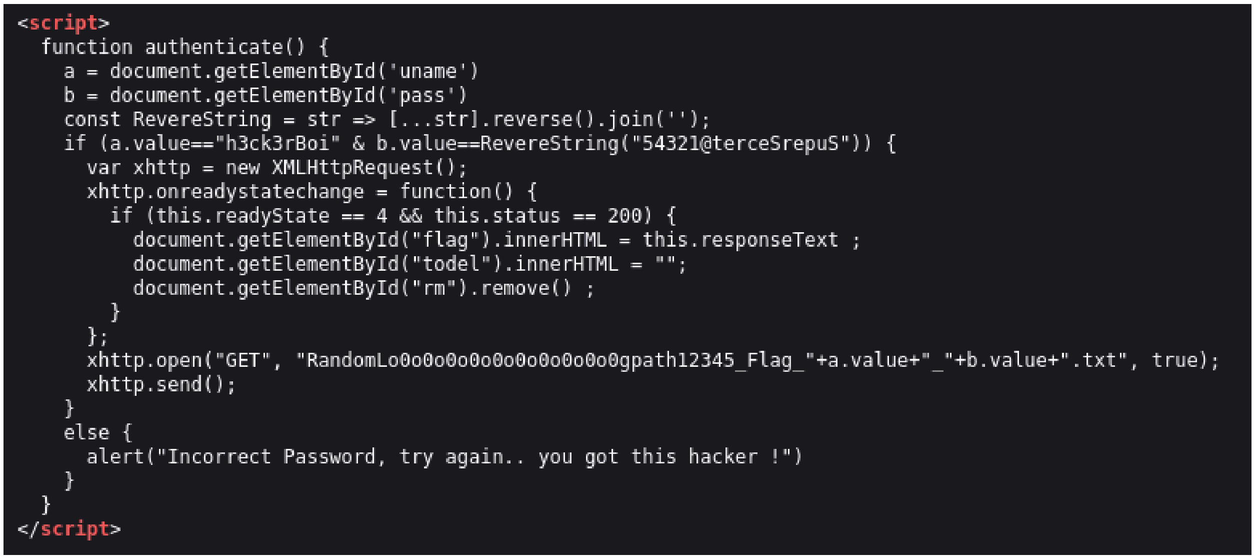
Incorrect Password, try again.. you got this hacker !

Checking /robots.txt

Nothing

Inspecting the code:
Ctrl + U

I see a function written on the HTML code:

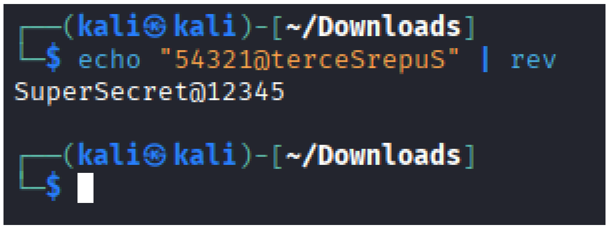


```
<script>
  function authenticate() {
    a = document.getElementById('uname')
    b = document.getElementById('pass')
    const RevereString = str => [...str].reverse().join('');
    if (a.value=="h3ck3rBoi" & b.value==RevereString("54321@terceSrepuS")) {
      var xhttp = new XMLHttpRequest();
      xhttp.onreadystatechange = function() {
        if (this.readyState == 4 && this.status == 200) {
          document.getElementById("flag").innerHTML = this.responseText ;
          document.getElementById("todel").innerHTML = "";
          document.getElementById("rm").remove() ;
        }
      };
      xhttp.open("GET", "RandomLo0o0o0o0o0o0o0o0o0o0gpath12345_Flag_"+a.value+"_"+b.value+".txt", true);
      xhttp.send();
    }
    else {
      alert("Incorrect Password, try again.. you got this hacker !")
    }
  }
</script>
```

a = document.getElementById(‘uname’)
b = documentgetElementById(‘pass’)

a.value == “h3ck3rBoi”
b.value == ReverseString (“54321@terceSrepuS”)

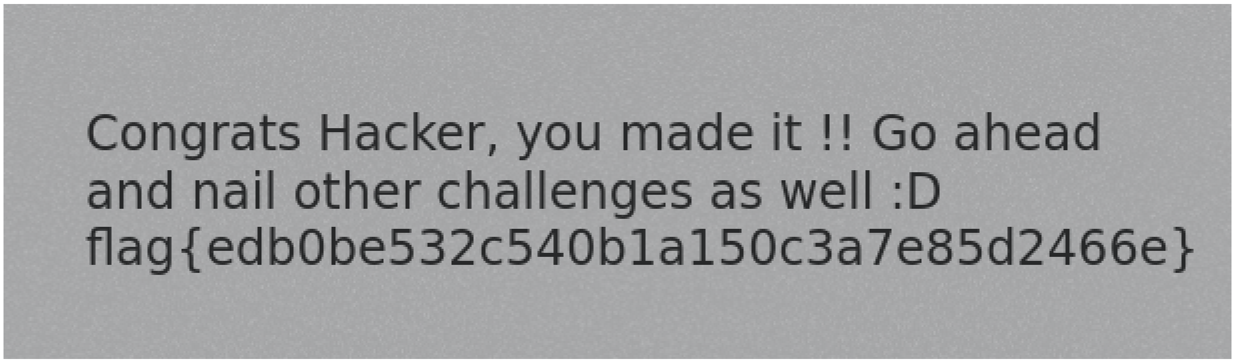
Reversing the string using Echo command
<echo “54321@terceSrepuS” | rev>



```
┌──(kali㉿kali)-[~/Downloads]
└─$ echo "54321@terceSrepuS" | rev
SuperSecret@12345

┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

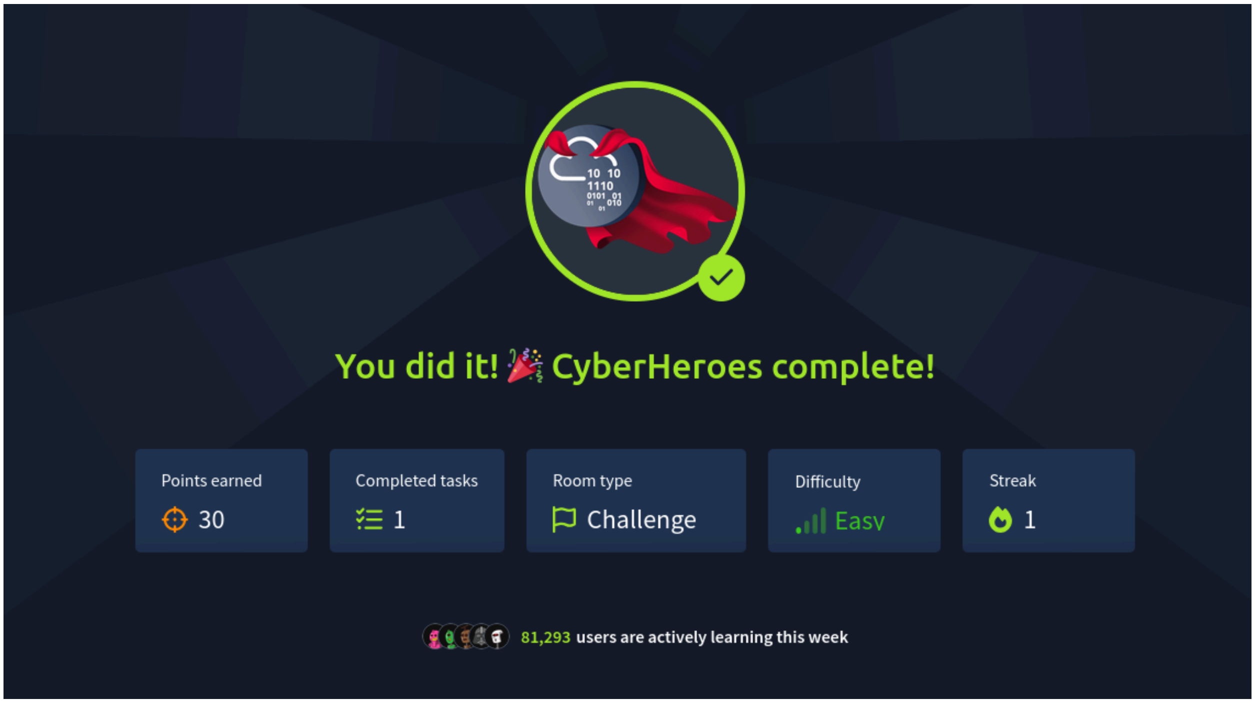
Using those credentials to login:

Username = h3ck3rBoi
Password = SuperSecret@12345



Congrats Hacker, you made it !! Go ahead and nail other challenges as well :D
flag{edb0be532c540b1a150c3a7e85d2466e}

Flag: flag{edb0be532c540b1a150c3a7e85d2466e}



You did it! 🎉 CyberHeroes complete!

Points earned: 30

Completed tasks: 1

Room type: Challenge

Difficulty: Easy

Streak: 1

81,293 users are actively learning this week