Cyber_Heroes_WalkThrough

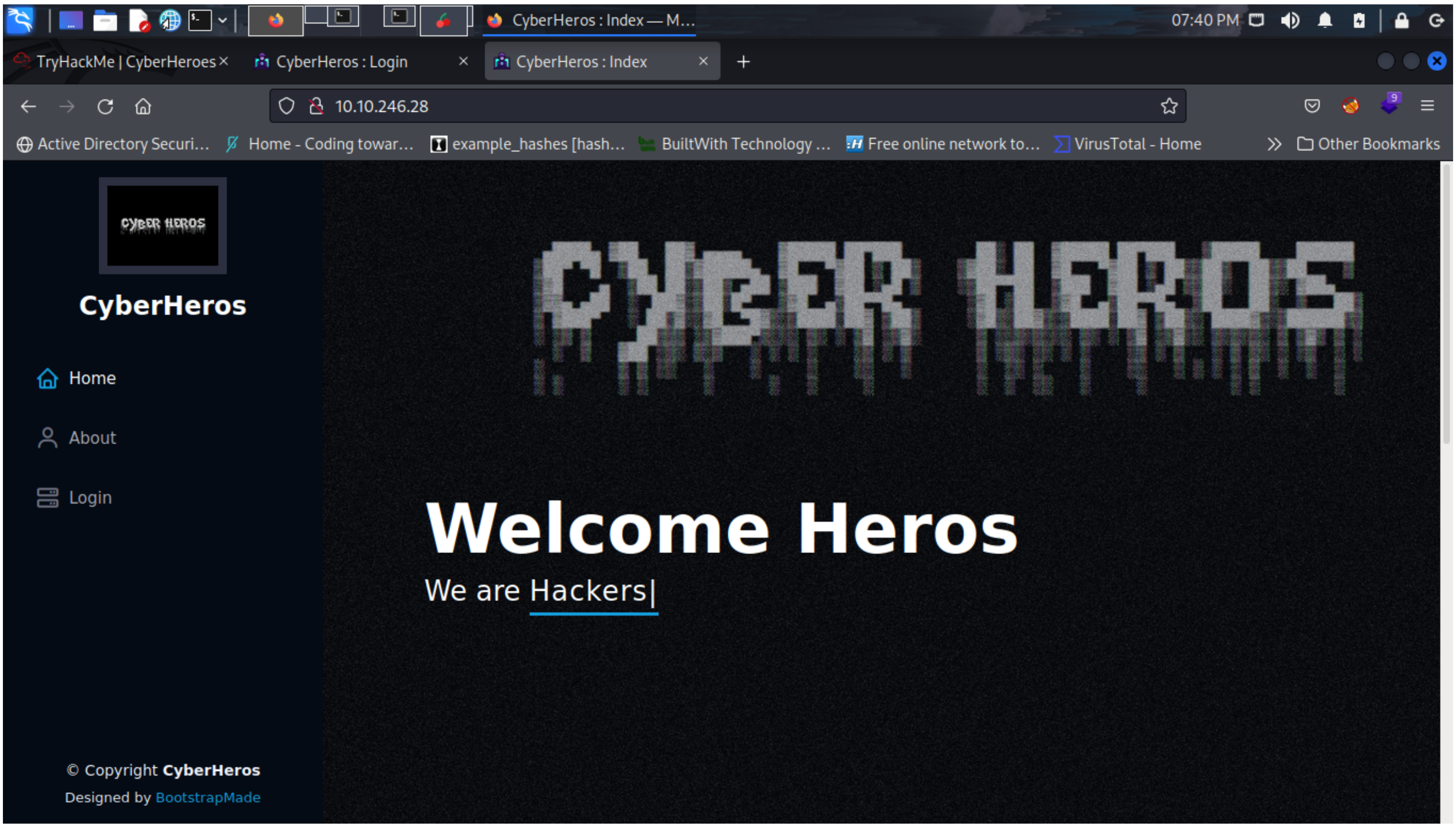
Nmap_Scan

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-21 20:04 EDT
Stats: 0:01:52 elapsed; 0 hosts completed (1 up), 1 undergoing NULL Scan
NULL Scan Timing: About 12.20% done; ETC: 20:19 (0:13:19 remaining)
Stats: 0:01:52 elapsed; 0 hosts completed (1 up), 1 undergoing NULL Scan
NULL Scan Timing: About 12.22% done; ETC: 20:19 (0:13:18 remaining)
Stats: 0:14:47 elapsed; 0 hosts completed (1 up), 1 undergoing NULL Scan
NULL Scan Timing: About 83.36% done; ETC: 20:22 (0:02:57 remaining)
Nmap scan report for 10.10.246.28
Host is up (0.22s latency).
Not shown: 65533 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 97:2a:33:1f:48:c8:30:f8:f5:ec:33:a2:6e:d9:ac:0f (RSA)
|   256 93:c6:ed:a8:67:16:60:b4:74:89:fd:94:c6:37:b5:14 (ECDSA)
|_  256 46:b1:65:50:66:4d:3d:73:42:28:3e:a9:60:2a:f1:d1 (ED25519)
80/tcp open  http    Apache httpd 2.4.48 ((Ubuntu))
|_http-title: CyberHeros : Index
|_http-server-header: Apache/2.4.48 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=8/21%OT=22%CT=1%CU=35929%PV=Y%DS=4%DC=T%G=Y%TM=6302CD0
OS:E%P=x86_64-pc-linux-gnu)SEQ(SP=FC%GCD=1%ISR=105%TI=Z%CI=Z%II=I%TS=A)OPS(
OS:O1=M506ST11NW7%O2=M506ST11NW7%O3=M506NNT11NW7%O4=M506ST11NW7%O5=M506ST11
OS:NW7%O6=M506ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)ECN(
OS:R=Y%DF=Y%T=40%W=F507%O=M506NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+
%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+
%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=
OS:S)

Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 1720/tcp)
HOP RTT       ADDRESS
1   171.70 ms 10.6.0.1
2   ... 3
4   313.30 ms 10.10.246.28

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 1278.99 seconds
```

Notes

We start wih an nmap scan. nmap -T4 -A -p- -sN 10.10.246.28 > nmap_scan
Ports 22 ssh, and 80 http are open lets explore.

Port_80



Welcome Heros

We are Hackers|

© Copyright **CyberHeros**
Designed by BootstrapMade

Notes

I went to the login page and tried some basic usernames and passwords, nothing worked.Next i ran gobuster.

Gobuster_Scan

```
sudo nmap -T4 -A -p- -sN 10.10.246.28 > Nmap_Scan                    1 ×
[sudo] password for kali:

┌──(kali㉿kali)-[~/Desktop/TRY HACK ME/Cyber_Heros]
└─$ gobuster dir -u http://10.10.246.28 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x
php,html,sh,txt -t 150
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.246.28
[+] Method:                  GET
[+] Threads:                 150
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              sh,txt,php,html
[+] Timeout:                 10s
===============================================================
2022/08/21 20:38:27 Starting gobuster in directory enumeration mode
```

```
===============================================================
/login.html          (Status: 200) [Size: 5753]
/index.html          (Status: 200) [Size: 6568]
/assets              (Status: 301) [Size: 313] [--> http://10.10.246.28/assets/]
/changelog.txt       (Status: 200) [Size: 2756]
```

Notes

I looked at the directories, but didn't find anything of importance.
Next i decided to look at the source code.

Source_Code_Review

```
function authenticate() {
      a = document.getElementById('uname')
      b = document.getElementById('pass')
      const RevereString = str => [...str].reverse().join('');
      if (a.value=="h3ck3rBoi" & b.value==RevereString("54321@t[redacted]")) {
        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() ;
          }
```

Notes

Looking at the source code i found a username and password, but the credentials didn't work.
i read the code closer and seen Reversestring, so just turn the password around and that gave me access.

Flag

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

Thanks i hope you enjoyed.