**ME and MY GIRLFRIEND 1 CTF**

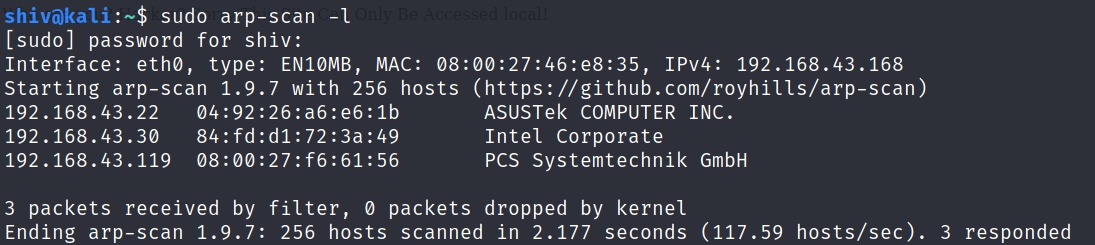
**Download link : - <https://www.vulnhub.com/entry/me-and-my-girlfriend-1,409/>**

**Step-1:-**

**After installing , turn it on and first thing we have to find to IP address of the machine.**

**So for that we have to scan the network . For that we will use this command**

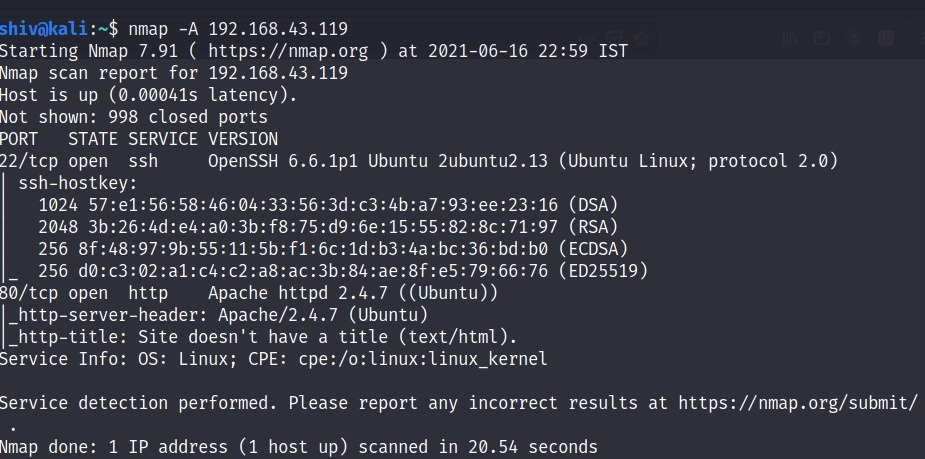
**Command: arp- scan -l**

****

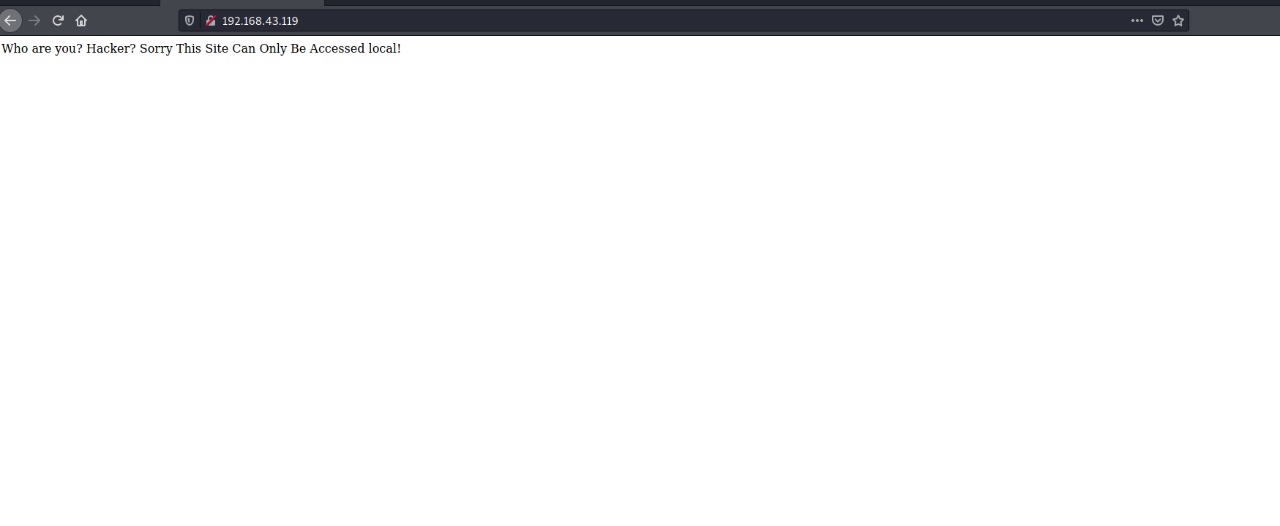
**Step -2:-**

**Now we are going to scan the IP address using nmap .**

**Command: nmap -A “Your IP Address”**

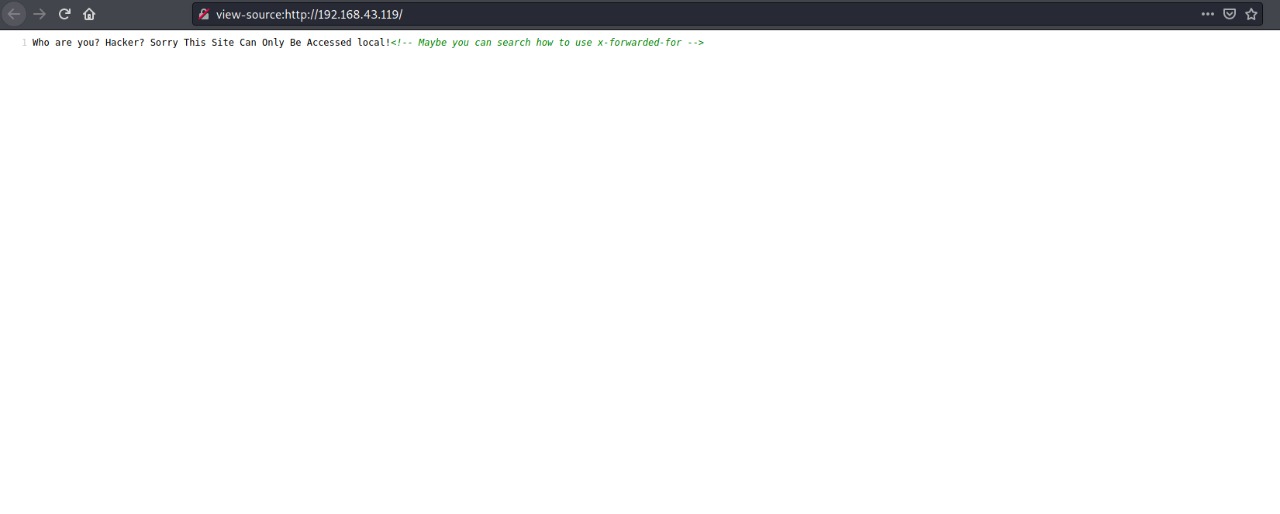
****

**Now you can see its has a http server running and its showing like this ->**

****

**Step -3:-**

**We have to get more information to get into this machine so first try to look into source-code of this page ,i found this -->**

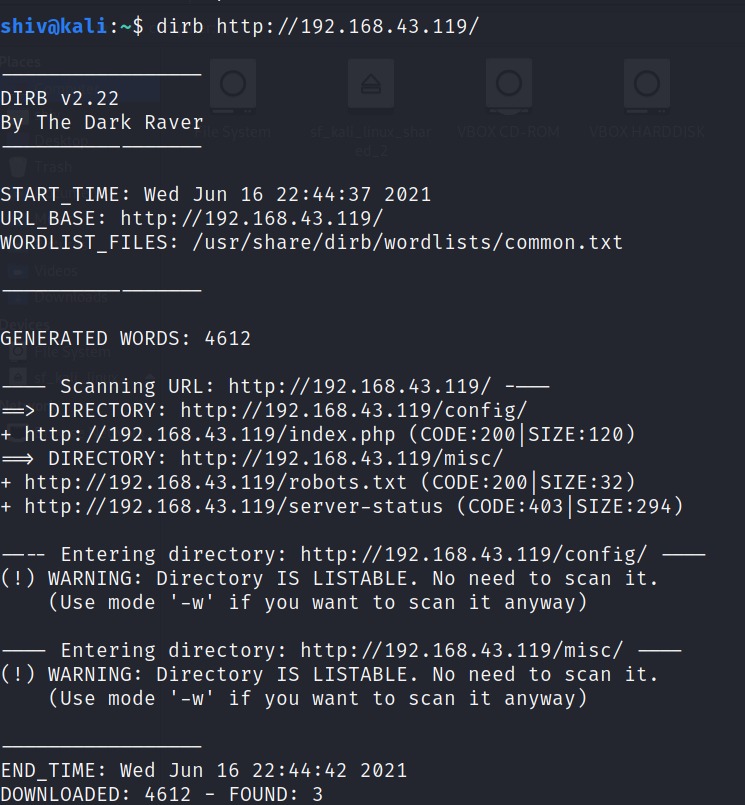
****

**It is saying we can use x-forward . Now keep it in the mind and lets go find some new clue.**

**We can use a command to find out sub pages of this main page. For that we will use this command**

**Command:- dirb http:// “your ip address”/**

**Result will be this**

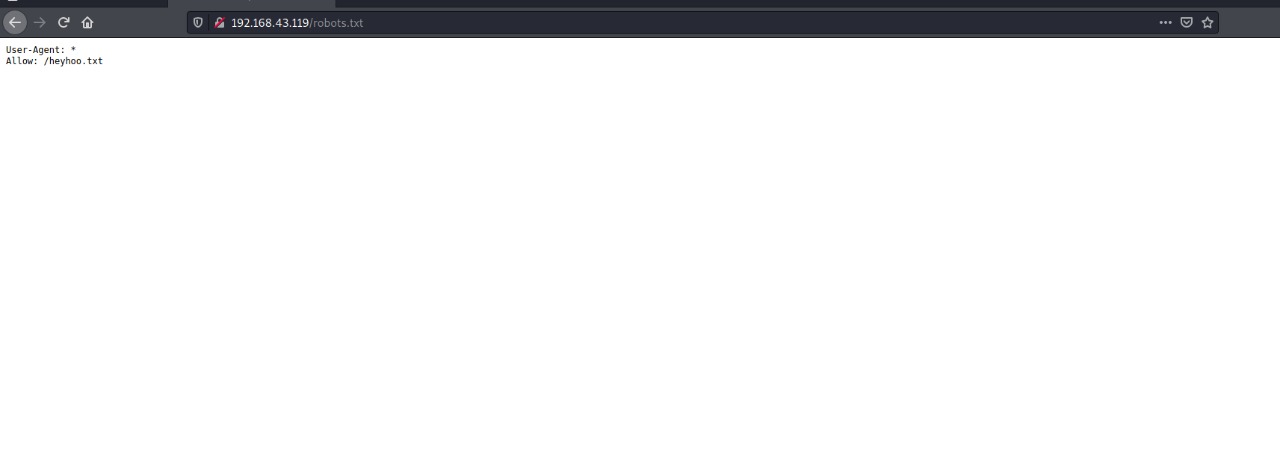
****

**We can see it has this pages now lets check this pages .**

**First check index.php page.**

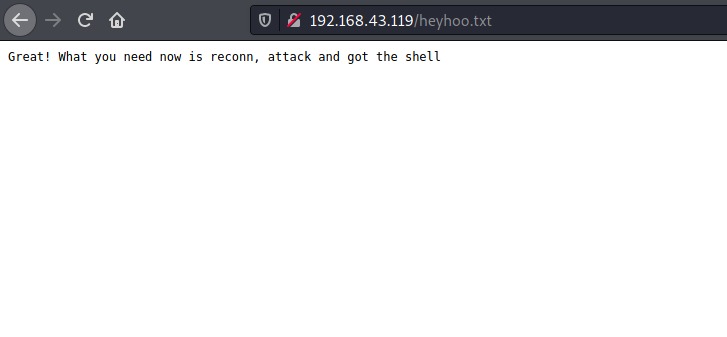
**But it was not opening.**

**Lets check the robots.txt page**

****

**Oh nice we have found another sub page.**

**Lets open /heyhoo.txt**

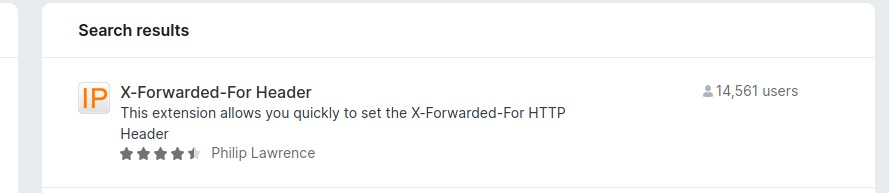
****

**Ok now we are getting this information.**

**Step -4 :-**

**Now as previous information we get to know about we have to use x -forward , so lets try that for that we will use a add-on in the browser.**

**Now go to the right-top corner and press 3 straight lines and then click add-on now search x-forward and you will get this ->**

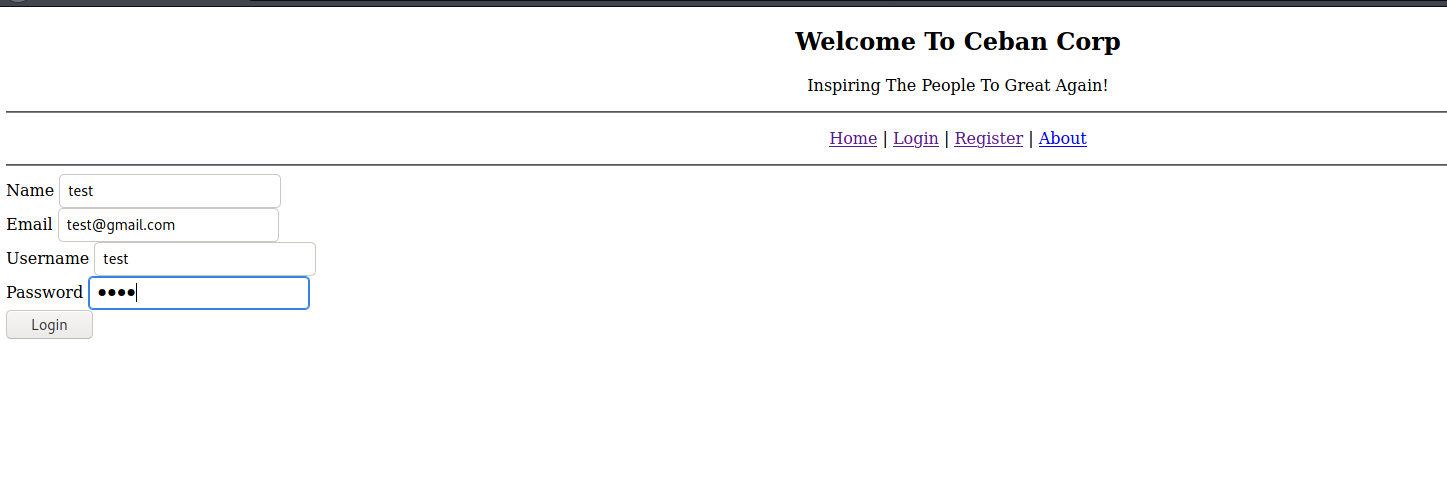
****

**Add that on your browser and then set the IP address at 127.0.0.1 and click the x-forward box.**

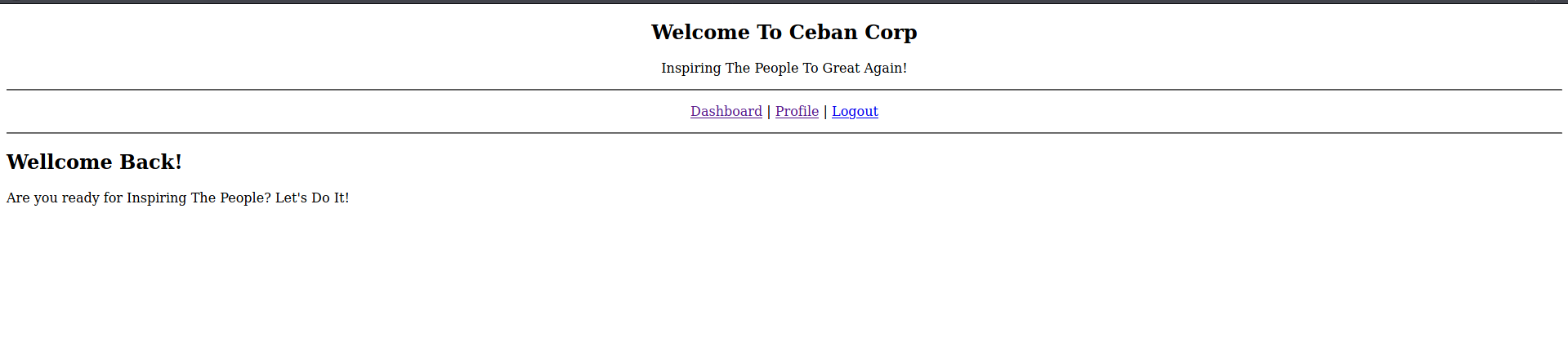
**Now refresh the main page and you will get this --->**

****

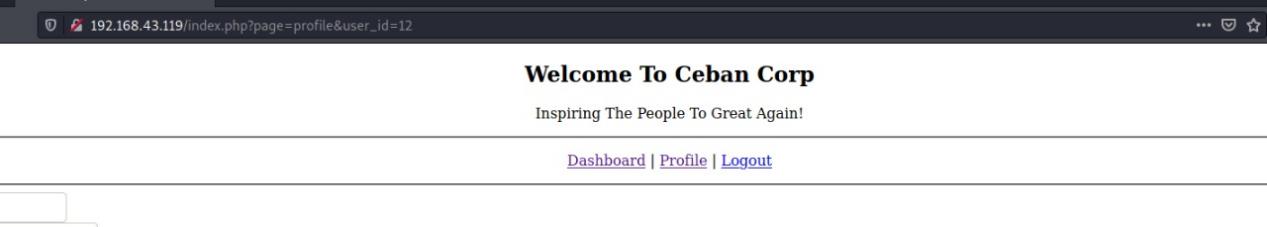
**So now we have found this page and by seeing it I can say we are almost done . Now cause I am new user so lets register on this company by a new account.**



**Now login and then again give your username and password and login into. This what I have found ->**



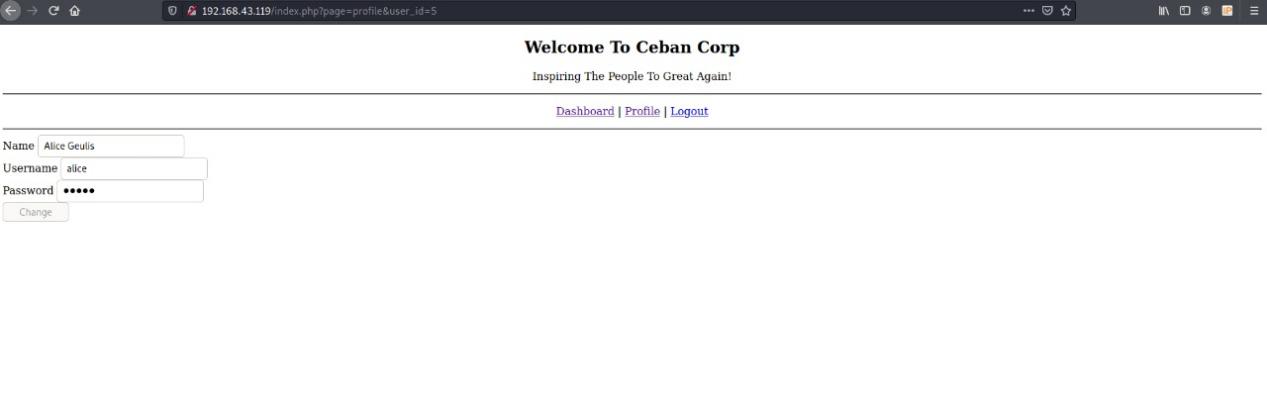
**I can see there are 3 options , I am in Dashboard and lets go to the profile section and search for something and then I saw this ->**

****

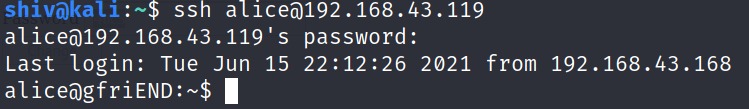
**My id number is 12 , so I tried to change it with 1 and boom we got into someones id**

****

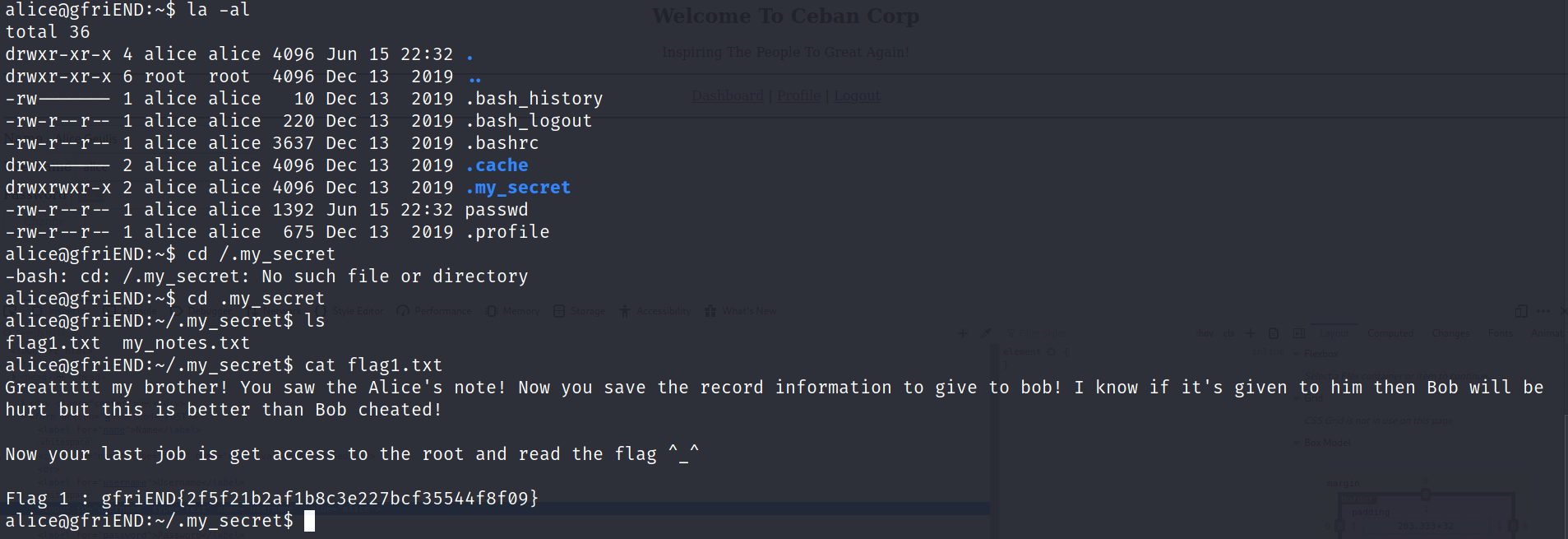
**After searching for other id’s I found this id and its look like this id we are searching for.**

****

**Now we have the id and password , lets login into the ssh server .**

****

**And we are in ,now lets find the flag**



**So here we have used “la -al” command and the we saw a “.my\_secret” file , so lets hop into that we can see 2 txt file including the flag1 file. Then we used “cat” command to read that file**

**Flag 1 : gfriEND{2f5f21b2af1b8c3e227bcf35544f8f09}**

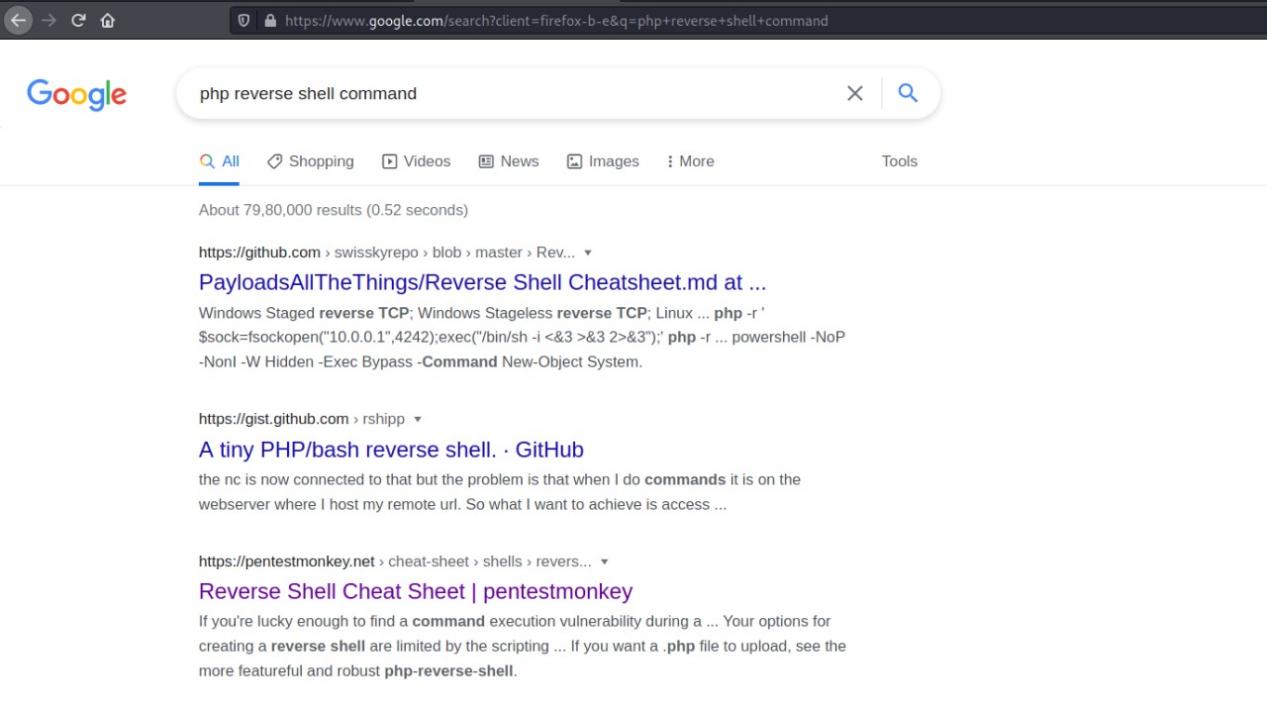
**Now for the next flag we have to access root on this machine.**

**For that ->**

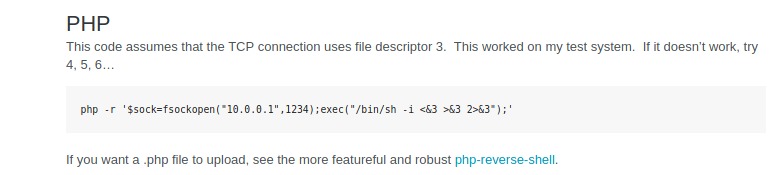
****

**We are going to see what we have permission to run in root , so I used “sudo -l “ command to find out and we found we can run php without password.**

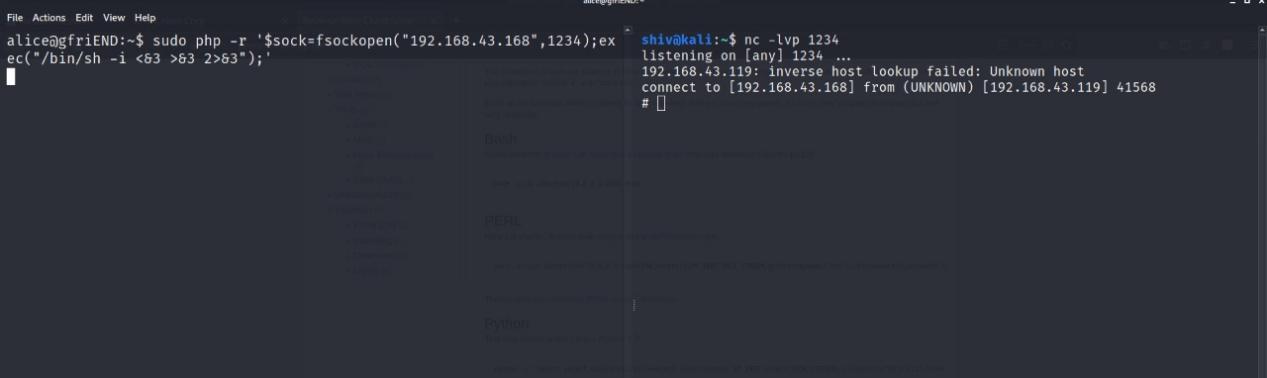
**So we are going to use php reverse shell script to access the root .**

****

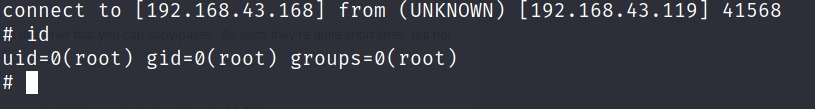
**I took the php command from the 3rd website from the search.**

****

**Now copy that command and change the ip with your ip and create a listener in an other terminal and run the command**

****

**And boom we got the root .**

****

**Now search for the flag2 file .**

****

**Here is the 2nd flag : Flag 2: gfriEND{56fbeef560930e77ff984b644fde66e7}.**