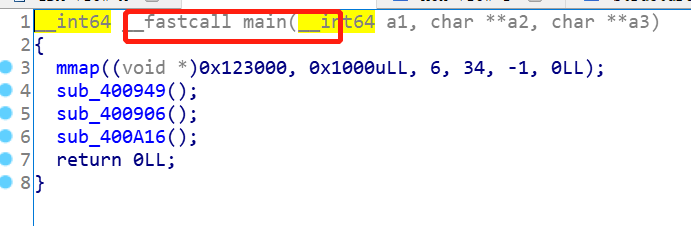
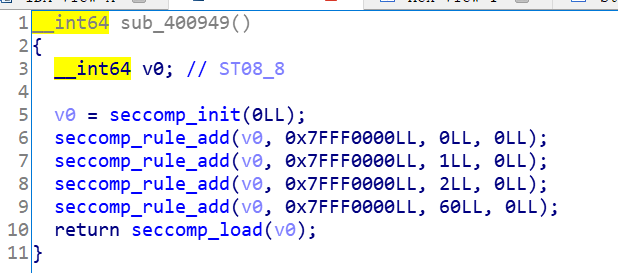
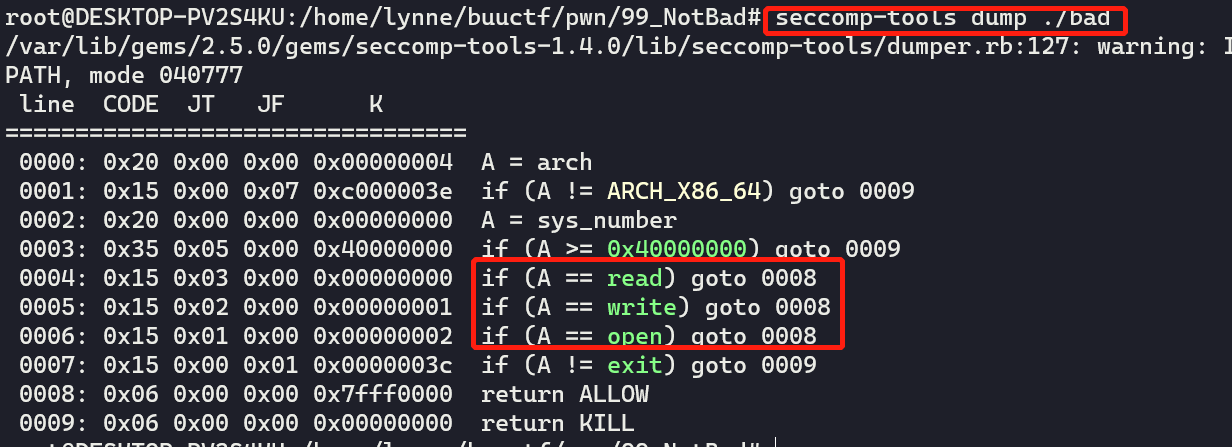


越是这种，越有点难搞啊





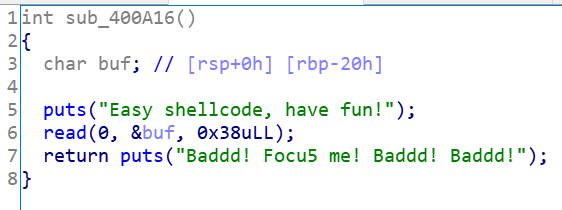
又有沙箱，看一眼



只能orw了

但是不知道该怎么办，搜了一下，可以ret2rsp，算是学习了一个新的知识。

一会会儿去整理一下。



可以手写汇编。

Shellcraft.read()

Asm(mov rax, 0x123000; call rax) 不需要栈迁移，可以直接执行程序流

