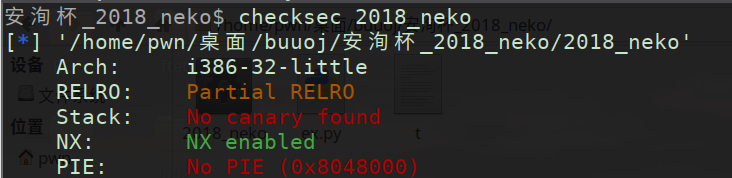
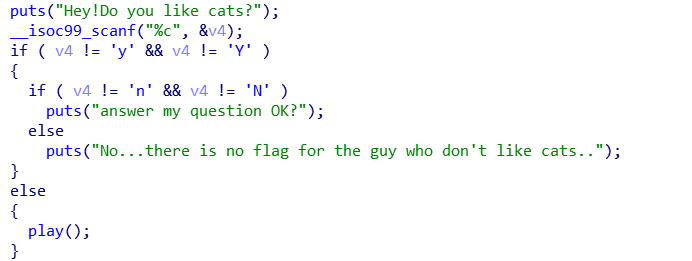
查看保护



PIE和canary都没开

IDA打开，查看程序流程



先输入’y’或’Y’进入play函数

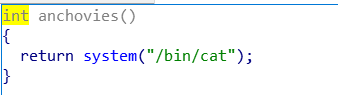


read存在栈溢出漏洞,cancary保护没开，可以直接溢出



溢出距离为0xd0

程序有后门



但这没有效果

那么可以先把puts函数的地址打印出来，求得libc的基地址，然后再求相应的‘/bin/sh’地址，system地址源程序有提供，第二次溢出时就可以获得shell

完整ex

