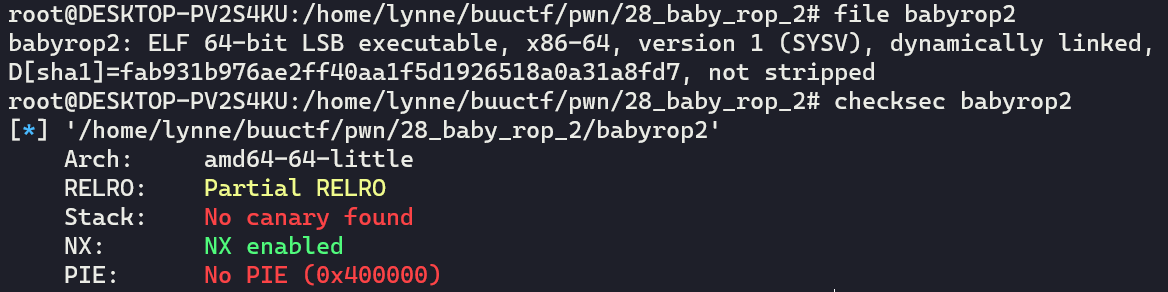
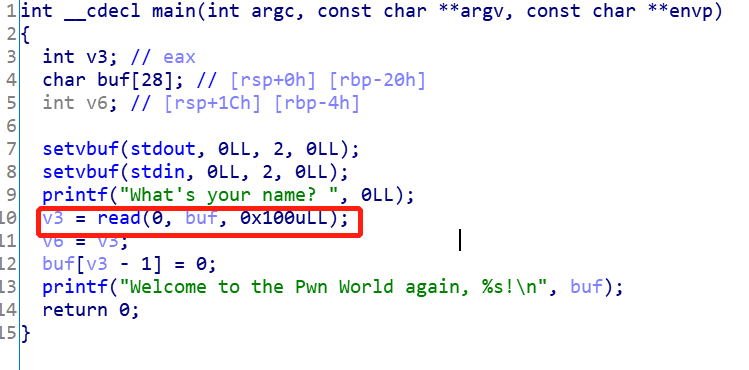
首先看下文件：



看main函数：



非常基础的ROP，开写吧！

注意64位的泄露姿势和32位是不一样的，必要的时候，加上ret，保持栈平衡。

好吧，本地不行，远程可以，不知道为啥！

