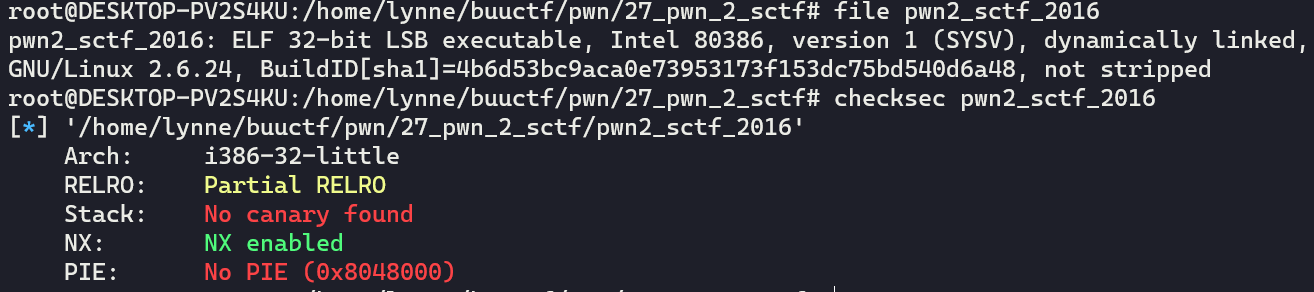
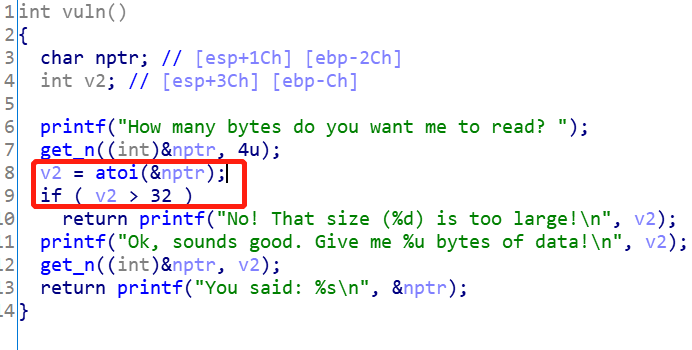
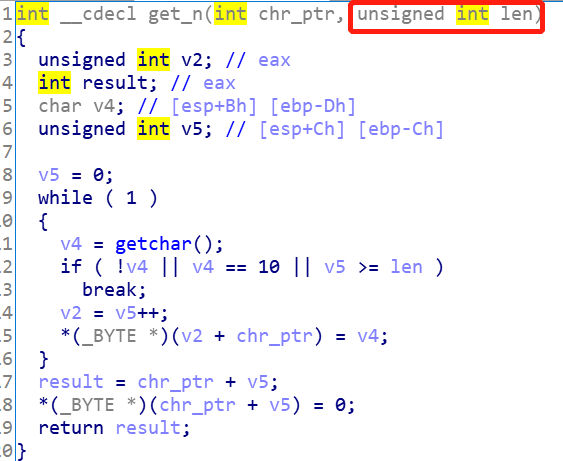
首先查看文件类型：



进IDA：



这个地方看似有个校验，然后可以传入负数：



那么思路就很简单了，给个-1，可以无限写。

然后是基本的ROP，先泄露libc的基地址，然后再调用system

