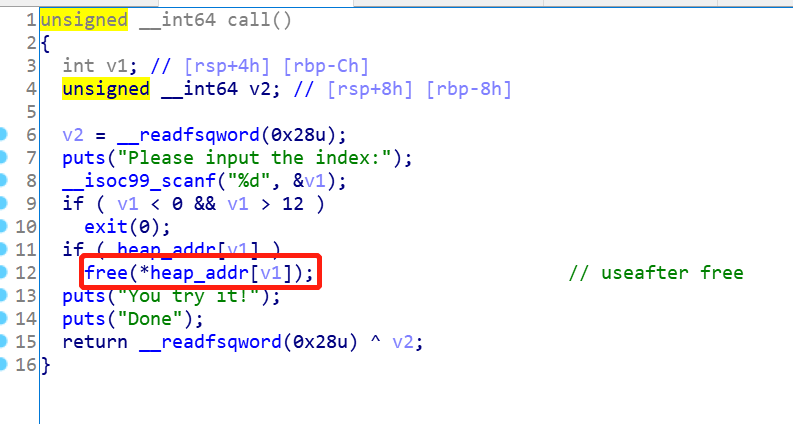


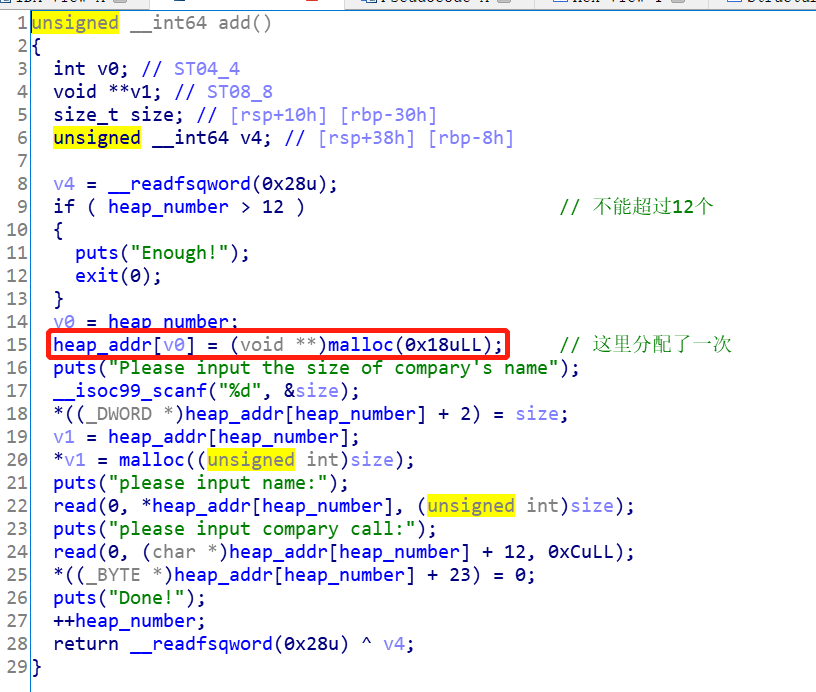
由于是UBUNTU18，所以呢，是tcache attack。

这里踩了一个坑，题目没有分析清楚，实际上还是需要边调试，边思考。

漏洞点很明显：



在add函数里面，会申请一个0x18的内存，管理堆结构。



这个结构，是没有释放掉的。所以，可以持续地输出一些信息。

攻击思路：

1. 想办法将small chunk放到unsortedbin里面去，然后show’出来地址。

2. 计算得到system地址和freehook地址

3. 由于是tcache，所以不需要伪造chunk结构，就可以直接往freehook写数据

4. 释放/bin/sh块，可以拿到shell。



