# 记一次简简单单越权漏洞的挖掘

Author p1ng by ACT-Team

前言:

每天看大佬们冲榜乱杀羡慕死弟弟了,于是菜鸡如我也去尝试了一波SRC漏洞的挖掘,很幸运的收获了一个越权漏洞,于是分享给米娜桑

首先在主站点盲目的寻找功能点,然后发现一处私信,看着做的这么粗糙的前端,于是男人的第十感告诉我,这里必定会有漏洞



看到聊天框,我先进行搜索联系人的越权测试,首先的想法是,替换查找用户联系人列表的id,看能否将其他用户的联系人进行查看,也就是越权查看其他用户的联系人,



可以看到数据包,大概意思是查看fromAccide=s-15205\*\*\*44这个id用户的列表是否包含nickname=\*\*\*的用户

此时我们就可以替换fromAccide,查看别的用户的联系人列表

经测试,替换成功,可以直接越权查看别人的联系人列表

但是,我们此时危害是不是不够大,看别人联系人列表而已啦,小洞小洞



既然搜索联系人有,那么旁边的搜索聊天记录是不是存在一样的越权漏洞呢?



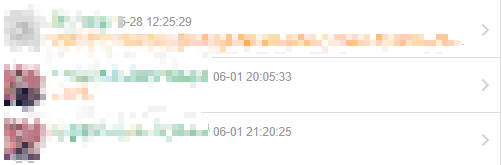
那么继续抓包,



发现有两个参数fromAccid和toAccide

哦?替换一个fromAccid,替换为别人的,然后放包

直接查看别人聊天记录!高危害越权不就来了嘛?



然后提交审核,虽然最后只给了250块你妹的

