记一次简简单单越权漏洞的挖掘

首先在主站点盲目的寻找功能点,然后发现一处私信

看到聊天框,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,

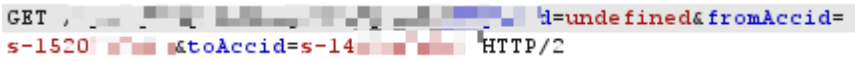
可以看到数据包,大概意思是查看 fromAccide=s-15205***44 这个 id 用户的列表是否包含 nickname=***的用户

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

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 !