越权漏洞扩大战果（任意用户信息修改+xss 后门+重置任意用户密码）
1.我们选择购买一张会员卡；
2.点击提交来到信息设置页面；
3.填写相关信息点击提交并抓包，得到如下数据信息，数据包中的 uid 参数引起了我的注意；
4.我们准备了另一个用户，填写信息；
5.将数据包中的 uid 参数修改为 47706624 并提交，之后返回该用户页面刷新，发现信息各项信息被成功修改，并且成功给该用户种植了一个存储型 XSS；
6.既然邮箱信息被成功修改，那么我们就可以直接对该用户进行密码重置，知道用户 uid 可通过论坛等多个途径获取对应 uid 用户的用户名信息，这里拿自己的注册的帐号演示；
7.对该用户填入我们修改后的邮箱帐号，成功发送了密码重置链接请求到我们修改的邮箱；
8.登陆对应的邮箱获取到密码重置链接请求；
9.成功验证进入密码重置环节；
10.填入我们想要重置的密码，即可完成该用户的密码重置；