在挖掘一些业务的时候，很多系统都会放在一个统一认证中去访问，你只有登录统一认证才能去访问某个系统，那么当我们在挖掘的时候，遇见这样的环境怎么办呢？

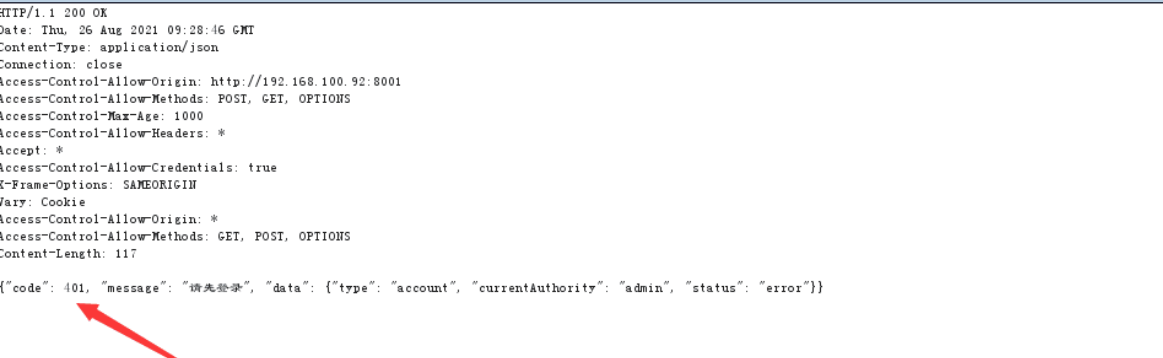
当然是最简单的修改返回包查看是否可以未授权查看内容，当然很多时候都是白给，但是我们还是要尝试一下撒。

当我们扫描出xxxx.com存在一个子域名，我们去访问站点http://stde.xxxx.com发现他要跳转到一个统一认证的页面，此时我们进行抓包对每一个数据包进行分析：

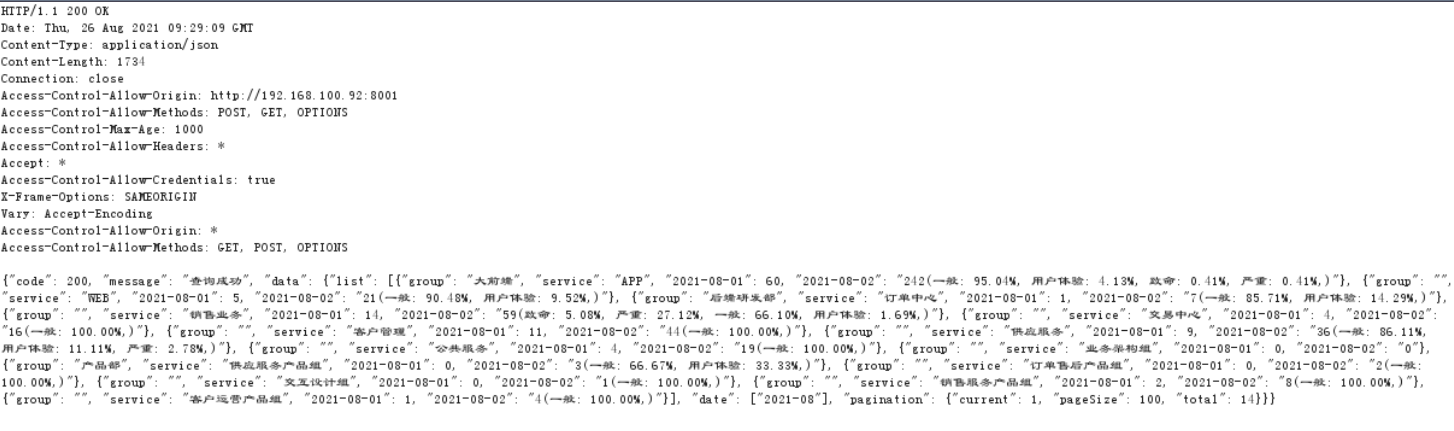
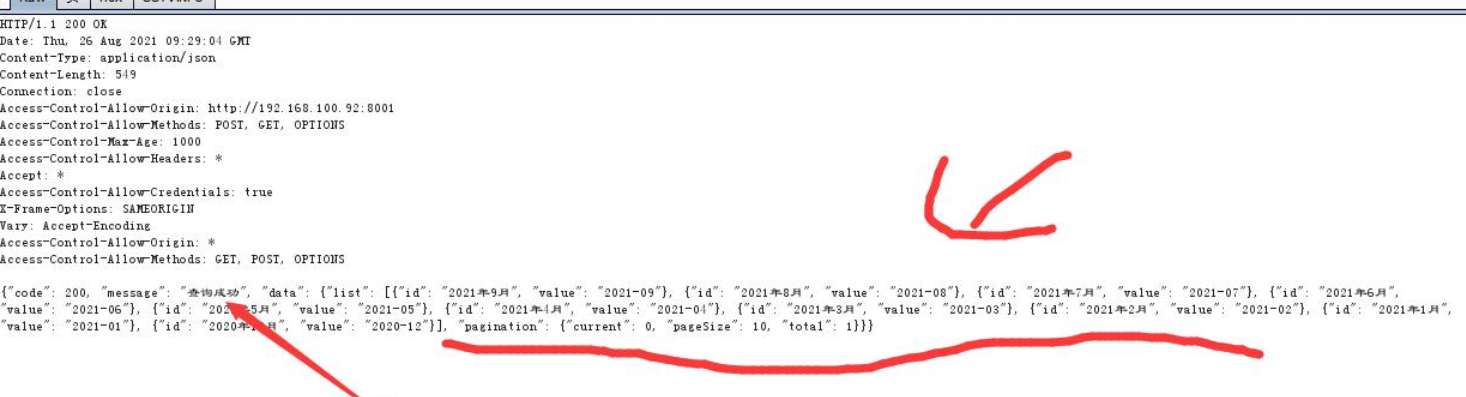


每一次放包都会自动跳转，但是发现该数据包时，我将箭头所指的{}删掉，发现就可以进入系统卡死在功能点页面，因为页面只有功能点没有数据，我就继续点击功能点

点击任意功能点继续抓包：出现如图的数据包的时候将401，提示我们需要先登录才能进行访问



常规操作，将401改为200，发现居然成功访问数据：



可以发现整个站点功能点都可以用这个方法查看数据:

