越权（一）

————支付收获地址越权

前言：在我挖掘漏洞的时候，其实越权是普遍存在，一个 get 请求中的显眼参数，一个 post 请求中不明显的参数，这些都是需要我们去思考的。

0X01 身份鉴权不严的挖法

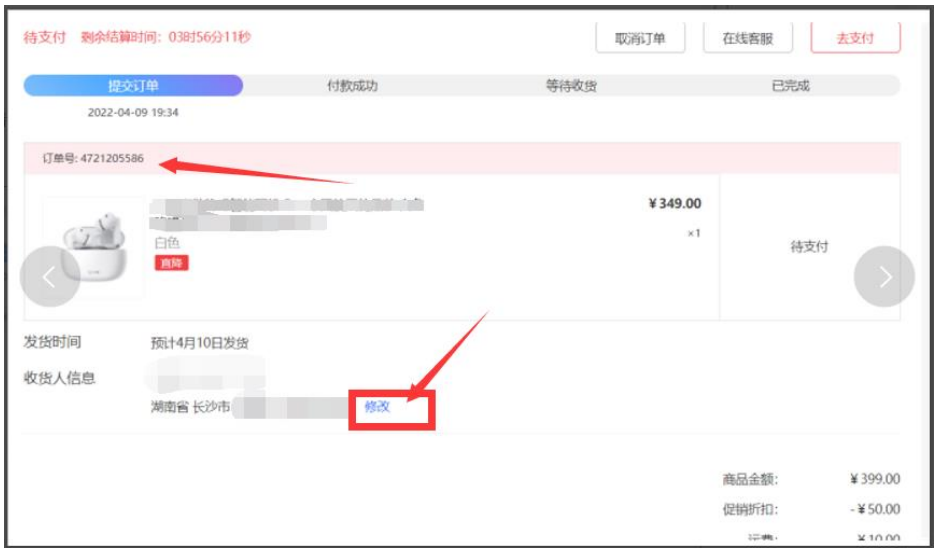
身份鉴权不严（原理就不解释了）这个漏洞点可以说存在整个 web 站点的任何一个地方，所以我们挖漏洞的时候，**一定要养成保存数据包的习惯，这是我们挖越权很重要的思路，再者就是 A 页面不存在越权，但是保不准 B 页面就不存在越权，所以我们在挖掘的时候，不要放过任何地方，总而言之就是：善于观察参数**

0X02 电商站点的越权处（一）

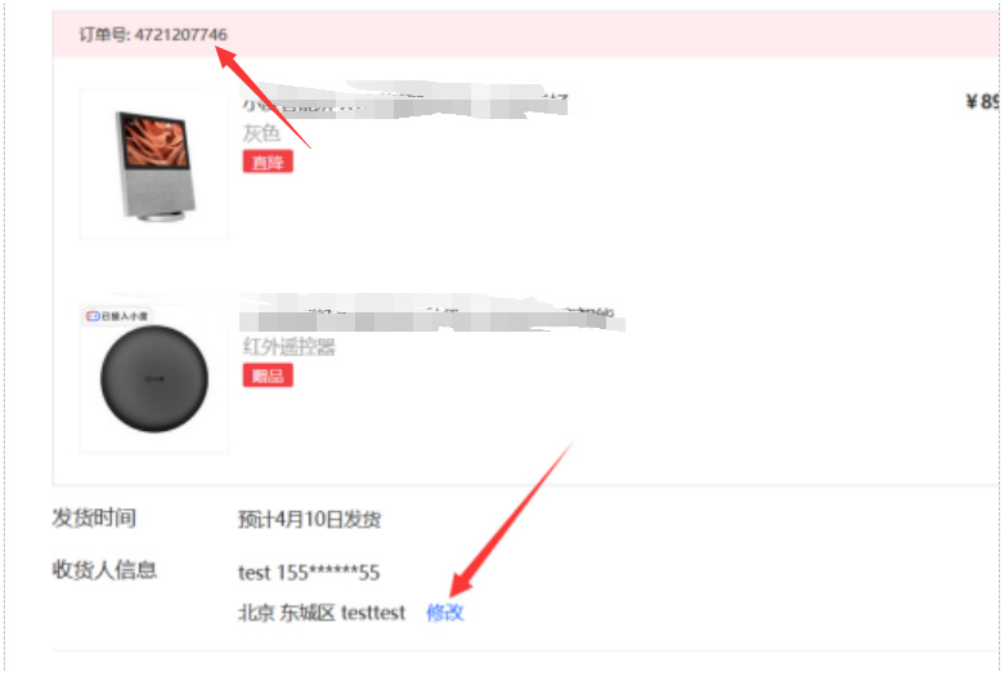
当我们在测试电商站点的时候，往往都有一个收货地址，在收货地址这个功能点下面一般有增加地址，修改地址，和删除地址，这几个功能点，这几个功能点就是我们测试越权的关键点，如果增加地址和修改地址存在越权，那么你说高危是不是就来了？

0X03 案例

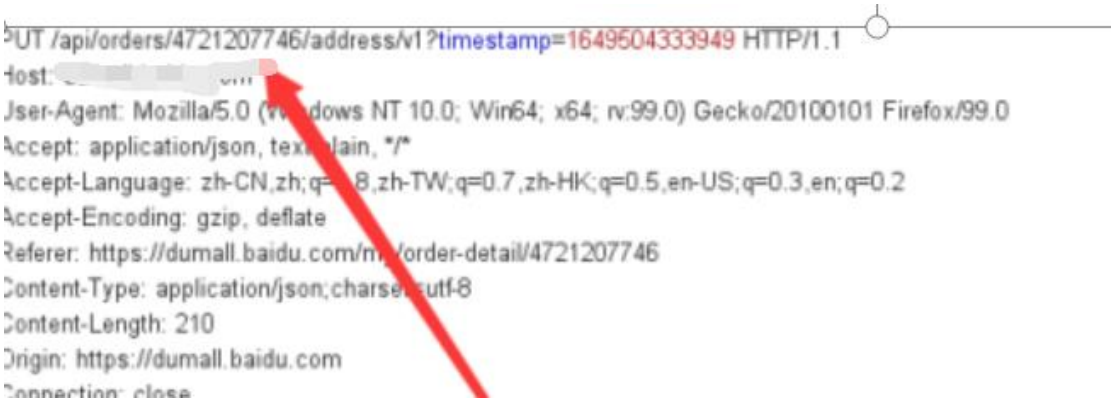
某度的商城我们点击付款的页面时看见了订单号和修改地址这个功能点



然后我们准备另外一个账号购买相同的物品，然后生成订单记住订单号：



然后我们抓包，换成我们另一个账号的订单：



放包，就成功为我们第一个账号的地址：