**快便支付原理**

**商户网站接入支付结果有两种方式，一种是通过浏览器进行跳转通知，一种是服务器端异步通知**

**浏览器跳转**

**基于用户访问的浏览器，如果用户在银行页面支付成功后，直接关闭了页面，**

**并未等待银行跳转到支付结果页面，那么商户网站就收不到支付结果的通知，**

**导致支付结果难以处理。而且浏览器端数据很容易被篡改而降低安全性**

**服务器端异步通知**

**该方式是支付公司服务器后台直接向用户指定的异步通知URL发送参数，采用POST或GET的方式。商户网站接收异部参数的URL对应的程序中，要对支付公司返回的支付结果进行签名验证，成功后进行支付逻辑处理，如验证金额、订单信息是否与发起支付时一致，验证正常则对订单进行状态处理或为用户进行网站内入账等**

**常见支付漏洞**

**无限创建首次优惠订单**

**修改支付的价格**

**修改订单数量**

**无限制试用**

**比如试用的参数为 2，正常购买的参数为 1**

**修改支付状态**

**订单完成 —— 未完成（傻傻分不清）**

**A 订单 - 0001 完成 ——B 订单 - 0002 未完成**

**购物app**

**购买数量：为0，小数，负数，正负值（A为-1，B为2，总值为1）**

**外卖**

**商品数量，0，负数，小数，特定值，正负数（A为-1，B为2，总值为1）**

如何挖掘

如何挖掘

支付时进行抓包，找到支付关键的数据包可能一个支付操作有三四个数据包，我们要对数据包进行挑选。

分析数据包

支付数据包中会包含很多的敏感信息（账号，金额，余额，优惠，订单ID）要尝试对数据包中的各个参数进行分析

支付的价格-支付漏洞

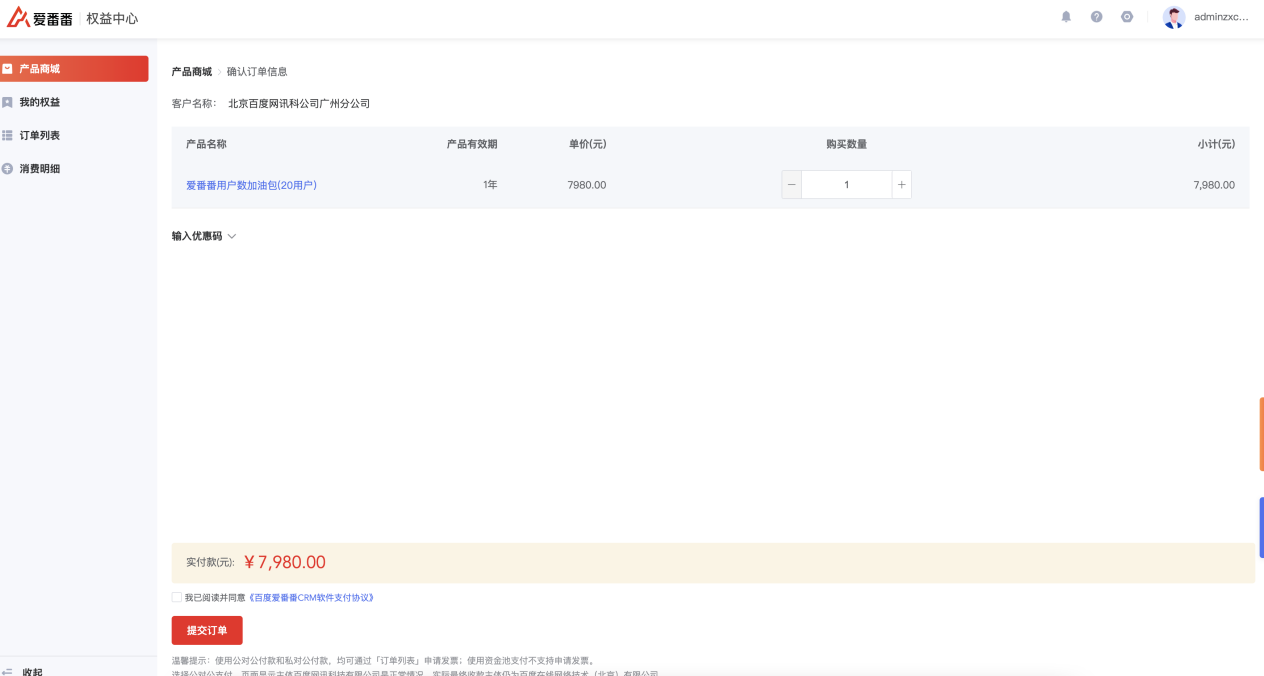
Url: https://xxxx.baidu.com/

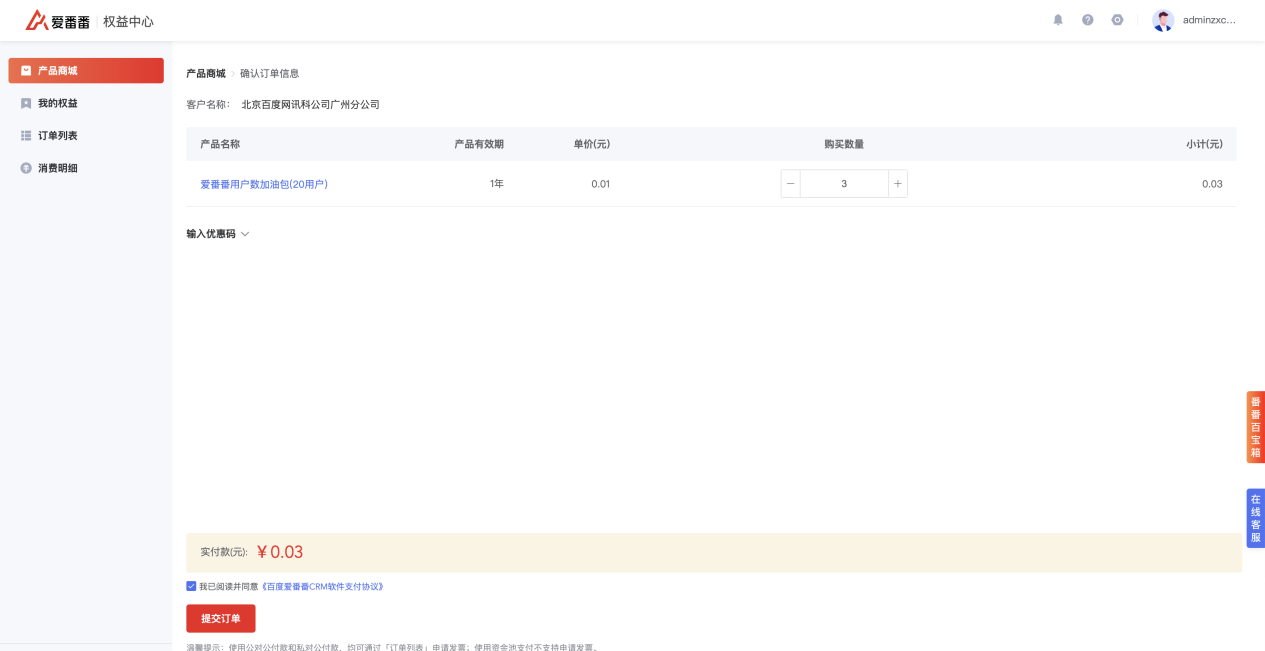
1. 访问组册个企业账号

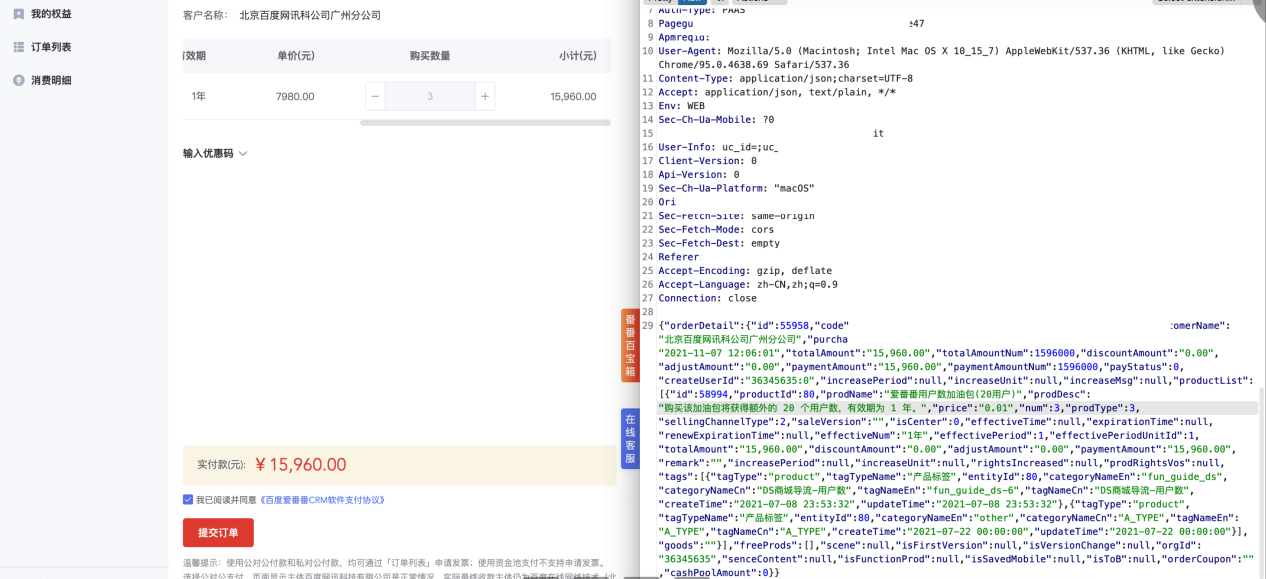


1. 修改单价

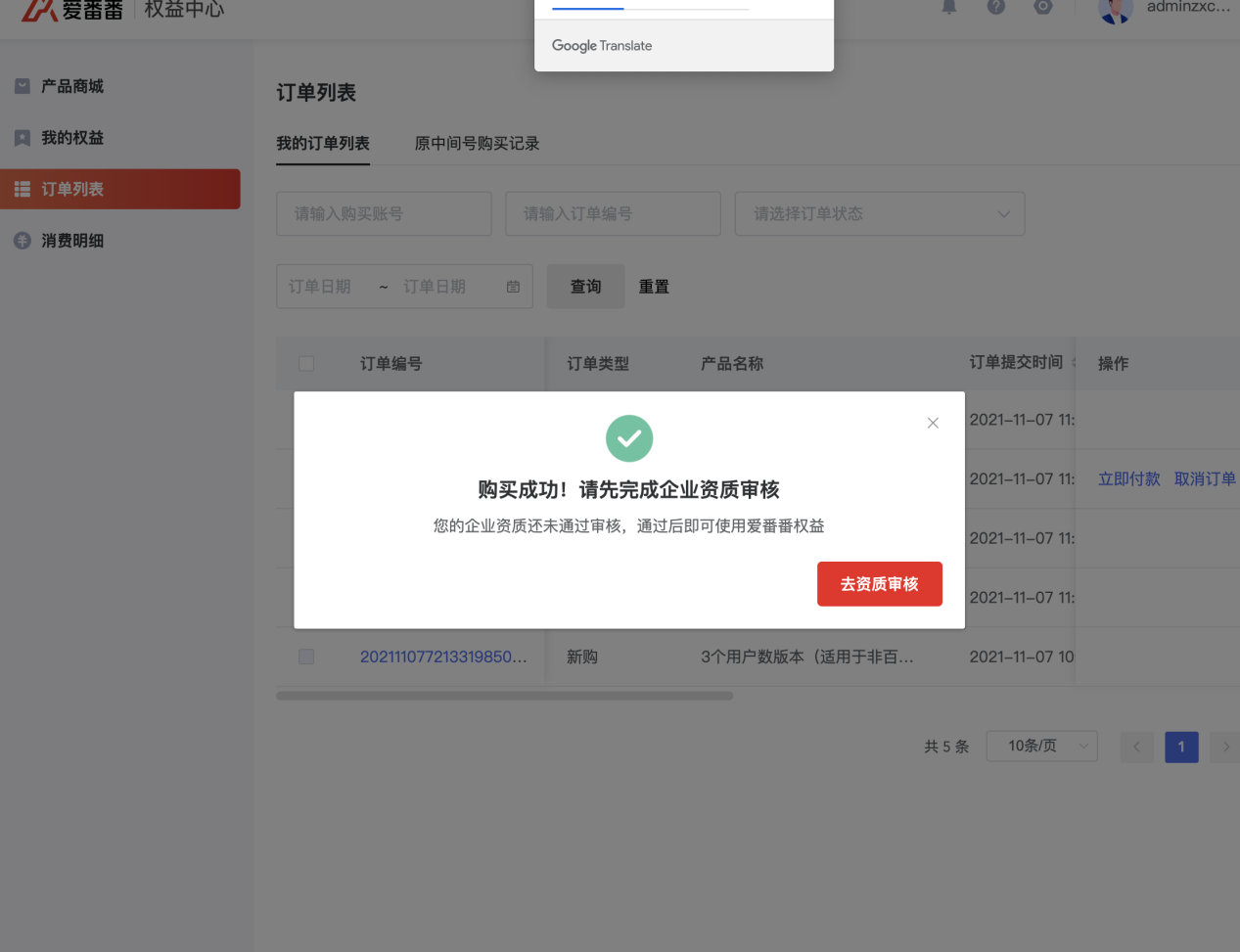
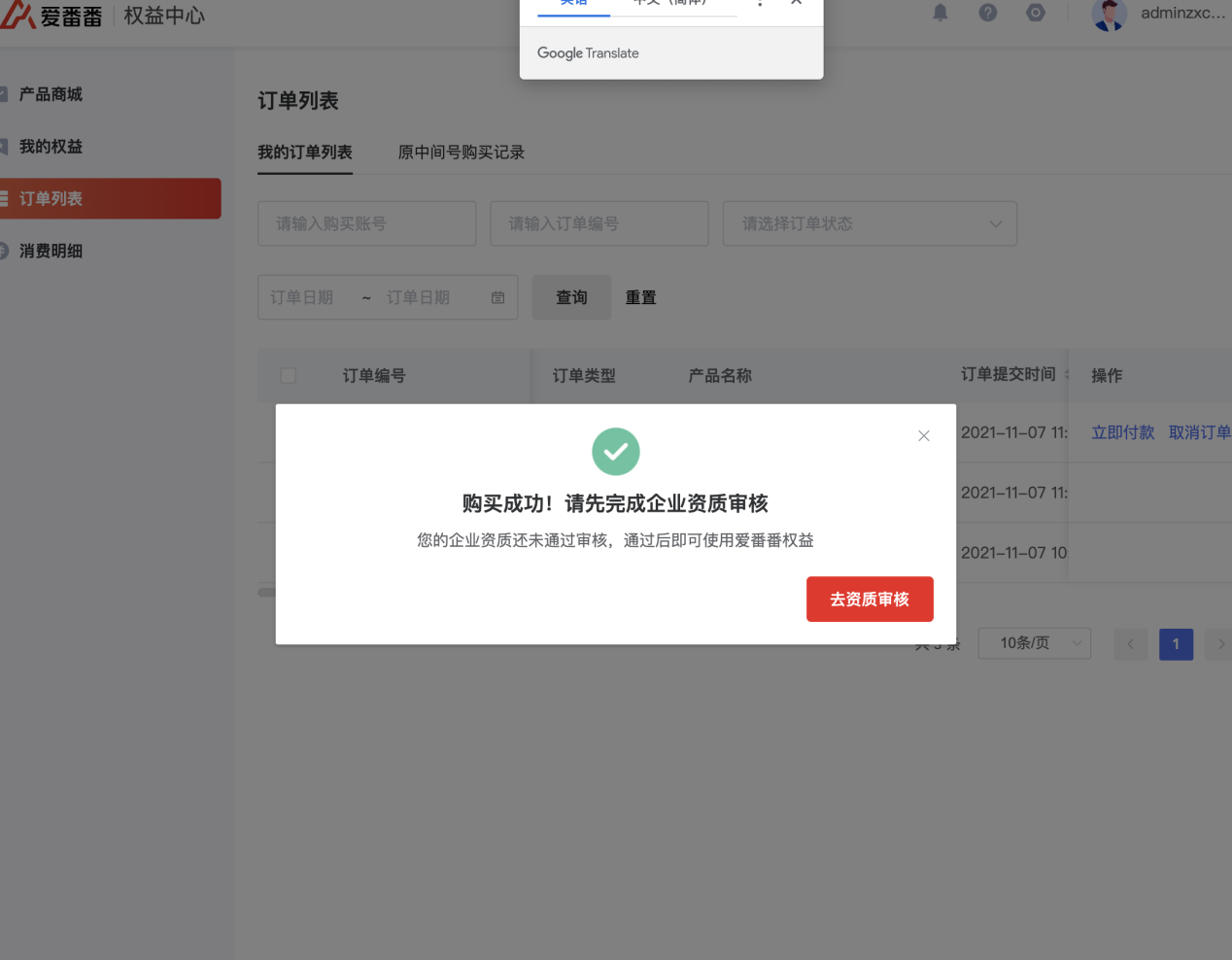
后台逻辑是 总金额 = 单价 \* 数量，我们只需要修改单价即可









、

该漏洞已修复