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

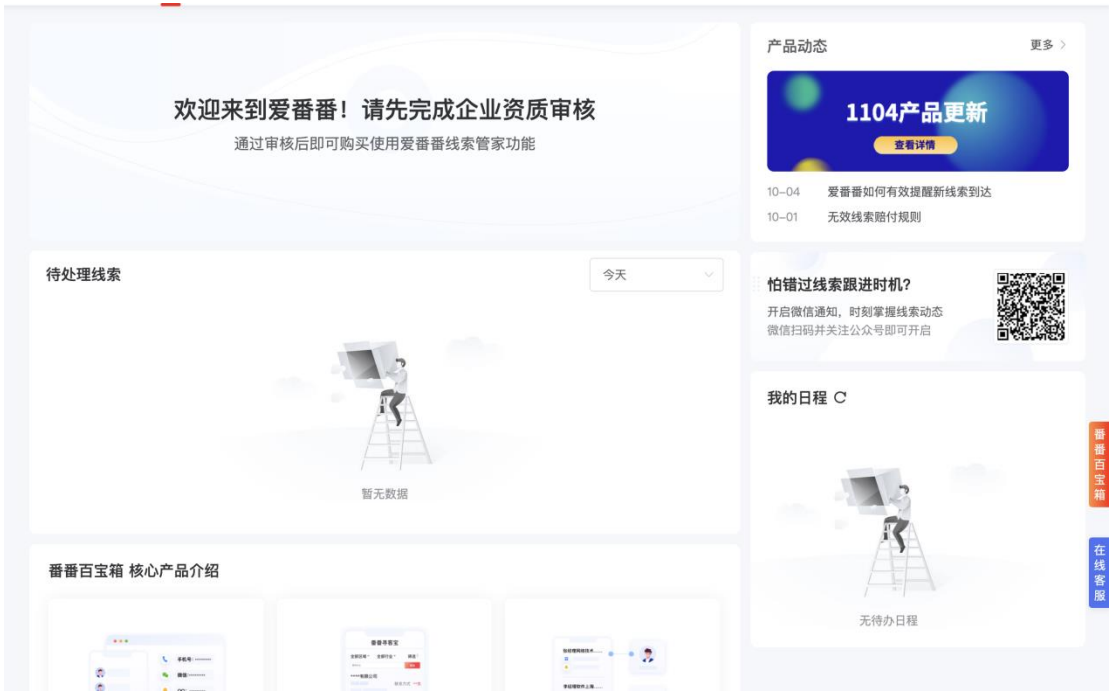
支付数据包中会包含很多的敏感信息（账号，金额，余额，优惠，订单 ID）要尝试对数据包中的各个参数进

行分析

支付的价格-支付漏洞

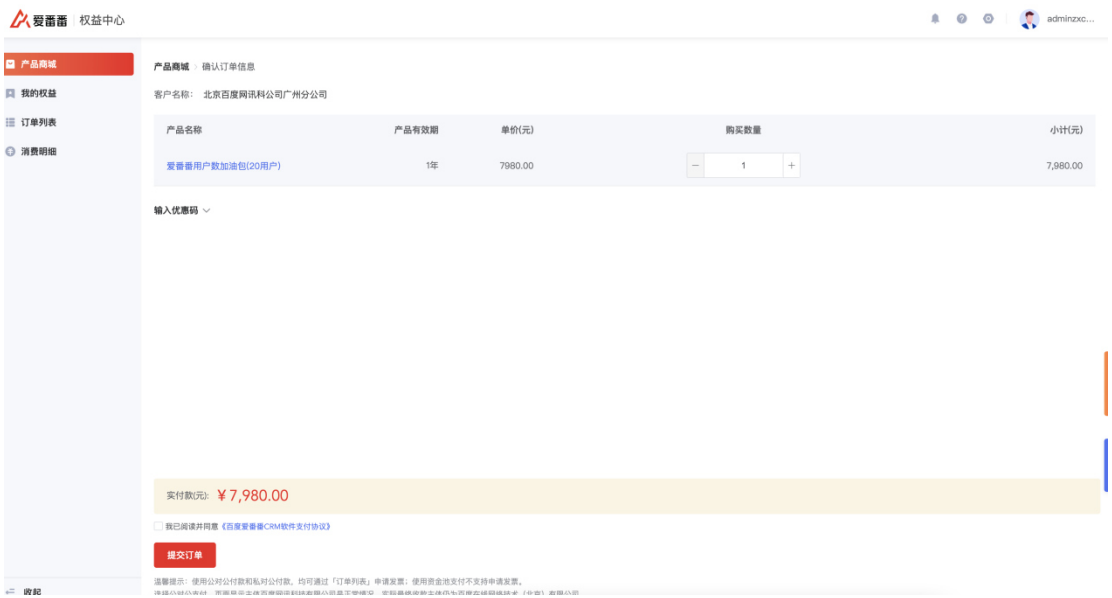
Url: https://xxxx.baidu.com/

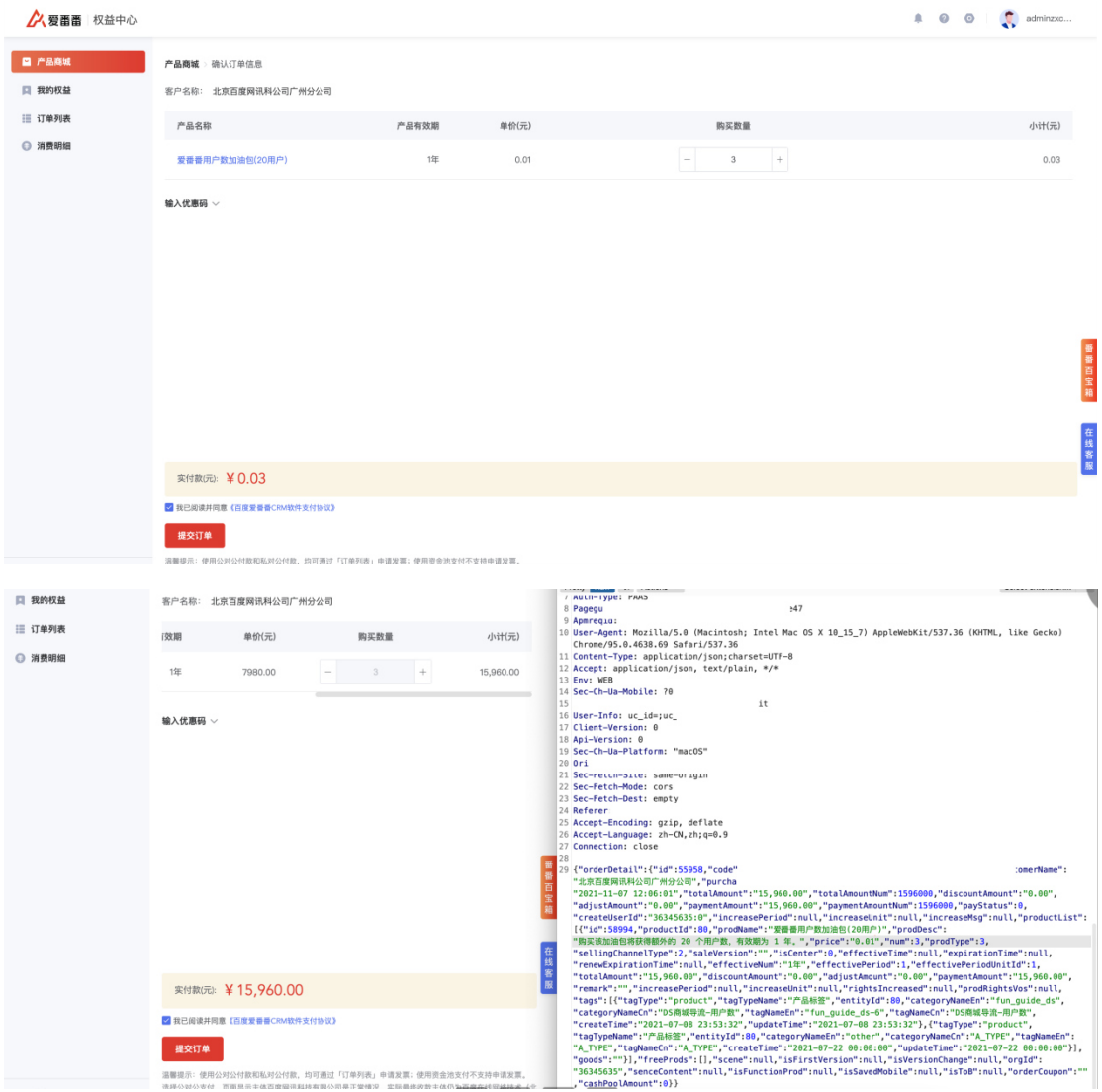
1.访问组册个企业账号



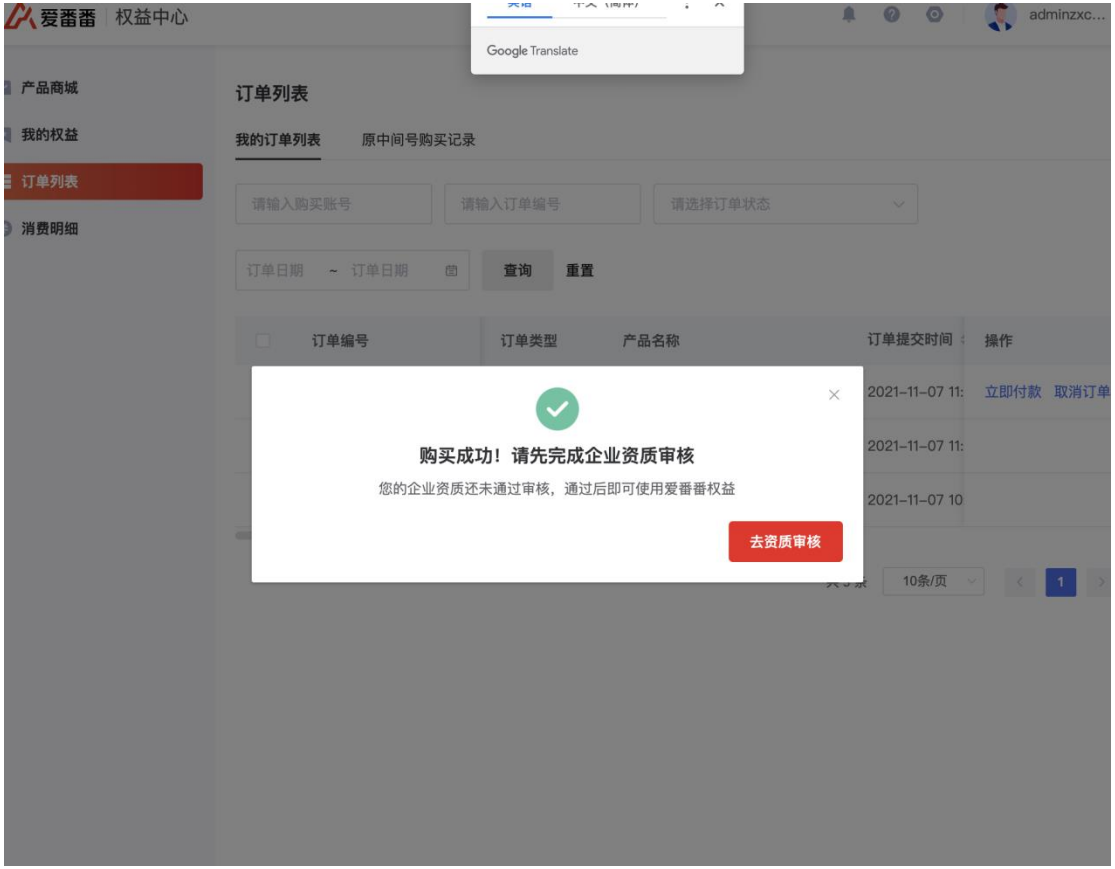
2.修改单价

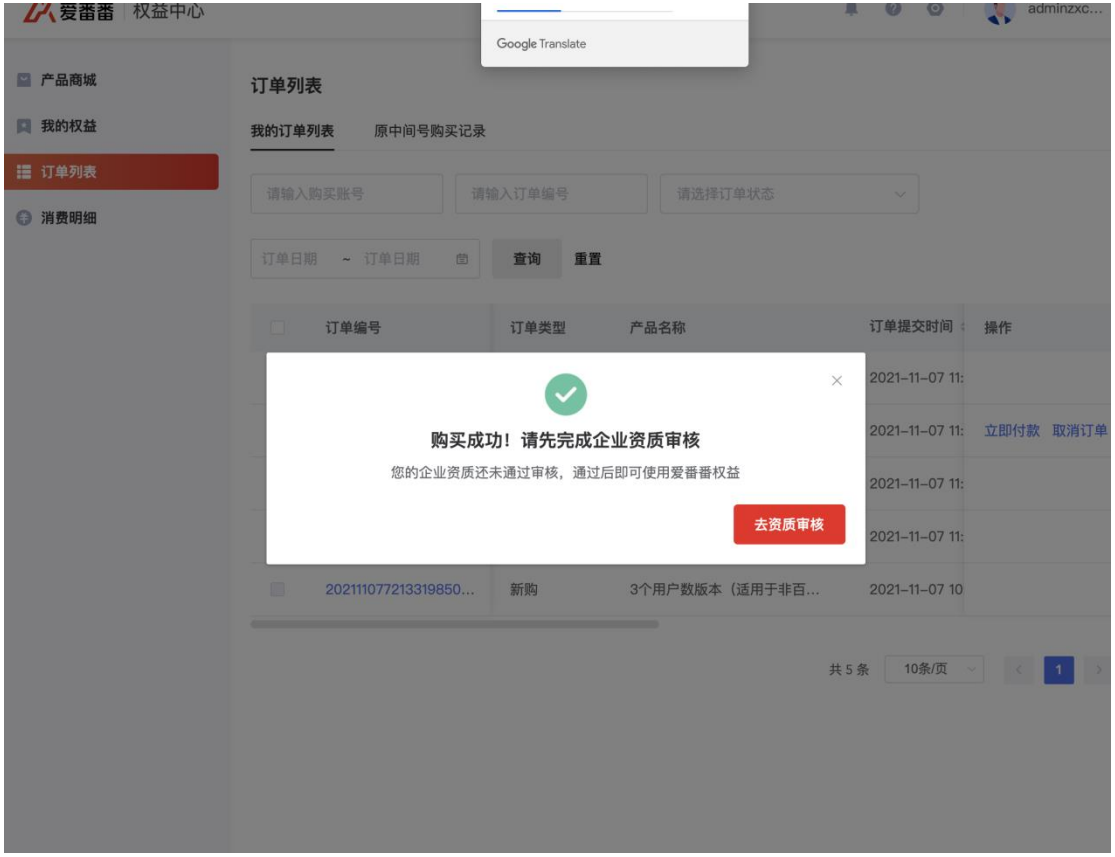
后台逻辑是 总金额 = 单价 * 数量，我们只需要修改单价即可


爱番番 权益中心
adminzxc...
产品商城
我的权益
订单列表
消费明细
产品商城 › 确认订单信息
客户名称： 北京百度网讯科公司广州分公司
产品名称
产品有效期
单价(元)
购买数量
小计(元)
爱番番用户数加油包(20用户)
1年
7980.00
1
7,980.00
输入优惠码
实付款(元): ￥7,980.00
我已阅读并同意《百度爱番番CRM软件支付协议》
提交订单
温馨提示：使用公对公付款和私对公付款，均可通过「订单列表」申请发票；使用资金池支付不支持申请发票。
收起


爱番番 权益中心
adminzxc...
产品商城
我的权益
订单列表
消费明细
产品商城 确认订单信息
客户名称： 北京百度网讯科公司广州分公司
产品名称
产品有效期
单价(元)
购买数量
小计(元)
爱番番用户数加油包(20用户)
1年
0.01
3
0.03
输入优惠码
实付款(元)： ¥ 0.03
我已阅读并同意《百度爱番番CRM软件支付协议》
提交订单
温馨提示：使用公对公付款和私对公付款，均可通过「订单列表」申请发票；使用资金池支付不支持申请发票。
客户名称： 北京百度网讯科公司广州分公司
单价(元)
购买数量
小计(元)
1年
7980.00
3
15,960.00
输入优惠码
实付款(元)： ¥ 15,960.00
我已阅读并同意《百度爱番番CRM软件支付协议》
提交订单
温馨提示：使用公对公付款和私对公付款，均可通过「订单列表」申请发票；使用资金池支付不支持申请发票。
{"orderDetail":{"id":55958,"code"
"北京百度网讯科公司广州分公司","purcha
"2021-11-07 12:06:01","totalAmount":"15,960.00","totalAmountNum":1596000,"discountAmount":"0.00",
"adjustAmount":"0.00","paymentAmount":"15,960.00","paymentAmountNum":1596000,"payStatus":0,
"createUserId":"36345635:0","increasePeriod":null,"increaseUnit":null,"increaseMsg":null,"productList":
[{"id":58994,"productId":80,"prodName":"爱番番用户数加油包(20用户)","prodDesc":
"购买该加油包将获得额外的 20 个用户数，有效期为 1 年。","price":"0.01","num":3,"prodType":3,
"sellingChannelType":2,"saleVersion":"","isCenter":0,"effectiveTime":null,"expirationTime":null,
"renewExpirationTime":null,"effectiveNum":"1年","effectivePeriod":1,"effectivePeriodUnitId":1,
"totalAmount":"15,960.00","discountAmount":"0.00","adjustAmount":"0.00","paymentAmount":"15,960.00",
"remark":"","increasePeriod":null,"increaseUnit":null,"rightsIncreased":null,"prodRightsVos":null,
"tags":[{"tagType":"product","tagTypeName":"产品标签","entityId":80,"categoryNameEn":"fun_guide_ds",
"categoryNameCn":"DS商城导流-用户数","tagNameEn":"fun_guide_ds-6","tagNameCn":"DS商城导流-用户数",
"createTime":"2021-07-08 23:53:32","updateTime":"2021-07-08 23:53:32"},{"tagType":"product",
"tagTypeName":"产品标签","entityId":80,"categoryNameEn":"other","categoryNameCn":"A_TYPE","tagNameEn":
"A_TYPE","tagNameCn":"A_TYPE","createTime":"2021-07-22 00:00:00","updateTime":"2021-07-22 00:00:00"}],
"goods":""}],"freeProds":[],"scene":null,"isFirstVersion":null,"isVersionChange":null,"orgId":
"36345635","senceContent":null,"isFunctionProd":null,"isSavedMobile":null,"isToB":null,"orderCoupon":""
,"cashPoolAmount":0}}


Bai du 百度 | 收银台
用户：炫舞之婷，已登录
订单详情：
订单号：AFF1673156647061537
订单描述：爱番番购买订单
支付方式：
个人账户支付
企业账户支付（只限企业账户选择）
支付宝
微信支付
度小满支付
请及时完成付款，避免订单取消！
支付金额：
0.03元
确认支付


爱番番 | 权益中心
Google Translate
adminzxc...
产品商城
我的权益
订单列表
消费明细
订单列表
我的订单列表
原中间号购买记录
请输入购买账号
请输入订单编号
请选择订单状态
订单日期 ~ 订单日期
查询
重置
订单编号
订单类型
产品名称
订单提交时间
操作
2021-11-07 11:
立即付款
取消订单
2021-11-07 11:
2021-11-07 10
10条/页
1
购买成功！请先完成企业资质审核
您的企业资质还未通过审核，通过后即可使用爱番番权益
去资质审核



该漏洞已修复