# 交易支付逻辑漏洞小总结—安全小课堂第三十六期

2016-12-02 京东安全应急响应中心

点击上方蓝字"京东安全应急响应中心"一起玩耍

#### 安全小课堂第三十六期

支付漏洞的理解通常都是篡改价格。比如,一分钱买任何东西。少收款、企业收费产品被免费使用,直接造成企业的经济损失。本期我们来聊一聊交易支付逻辑漏洞。

本期我们邀请到

JSRC资深白帽子

种田、紫霞仙子

ر\*°∨°\*)∠





豌豆妹

先说说支付流程出现逻辑漏洞的严重性吧~





支付漏洞的理解通常都是篡改价格。比如,一分钱买任何东西。少收款、企业收费产品被免费使用,直接造成企业的经济损失。





### 豌豆妹

交易支付逻辑漏洞的呈现形式有哪些呢?



支付成功后,实际价格与支付价格不相等。可以举一些案例以助于更好地理解。 例一,充值的时候,程序只判断订单有没有充值成功,但没有判断金额,例如:生成订 单跳至支付宝页面,在原网站上点支付失败,这时可以修改订单,改成更大的金额(订 单号没变),回到支付宝支付页面,支付成功。程序并没有重新核对支付宝实际的金 额,只是把订单改为已支付。

例二:使用余额支付,把数量改为负数,总金额也为负数,扣除余额时,负负得正,这 时余额增加。





#### 豌豆妹

那如何测试交易支付是否存在逻辑漏洞呢?





- 1、在购买产品过程中修改产品数量、价格;
- 2、在支付时修改总价格或者优惠价格;
- 3、订单生成后,编辑订单把A商品的价格改成B商品的价格,实现低价支付。 测试时,修改数量、单价,优惠价格参数为负数、小数,无限大,看是否能生成订单, 能生产进入支付即说明存在逻辑漏洞了。



## 豌豆妹

能说说交易支付漏洞的几种常见类型么?



- 1、修改金额;
- 2、修改商品数量;
- 3、修改优惠金额;
- 4、修改数量、单价,优惠价格参数为负数、小数,无限大;
- 5、商品价格更改;
- 6、支付key泄露等。

实际安全中会有一些比较特别的,反正各种能改的参数都去尝试。个数\*单价-优惠券个数\*单价=总额,每个值都可能存在问题,就看服务自身处理是否有问题了。





豌豆妹

能说说支付漏洞的修复方案么?



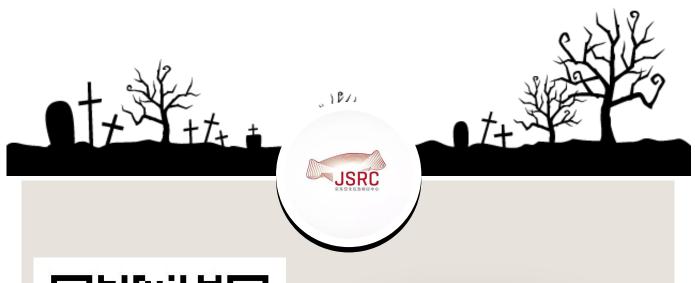
1、在后端检查订单的每一个值,包括支付状态;

- 2、校验价格、数量参数,比如产品数量只能为整数,并限制最大购买数量;
- 3、与第三方支付平台检查,实际支付的金额是否与订单金额一致;
- 4、另外,如果给用户退款,要使用原路、原订单退回。比如:退押金,按用户原支付订单原路退回;
- 5、MD5 加密、解密、数字签名及验证,这个可以有效的避免数据修改,重放攻击中的各种问题;
- 6、金额超过指定值,进行人工审核等。



豌豆妹

好哒~大家有其他感兴趣的话题,也可以在后台留言给本宝宝哟~感谢大家的持续关注!





微信公众号:jsrc\_team

新浪官方微博:

京东安全应急响应中心

固定栏目

技术分享 | 安全意识 | 安全小课堂