支付漏洞

【学习目标】

1. 支付漏洞的概念
2. 支付的原理
3. 支付漏洞的利用
4. 支付漏洞的防御

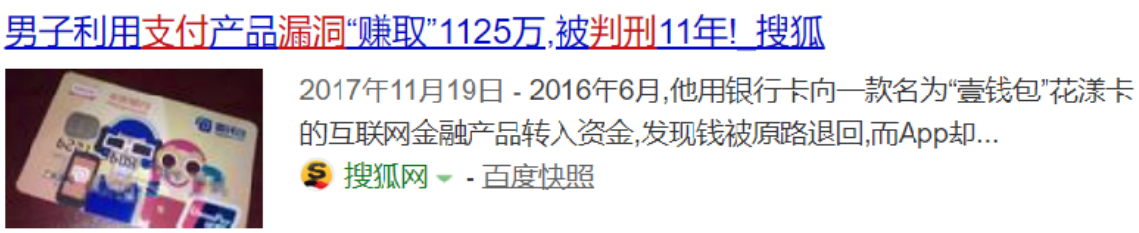
【重难点知识】

1. 支付的原理
2. 支付漏洞的利用

支付漏洞的概念

支付漏洞一直以来就是是高风险，对企业来说危害很大，对用户来说同样危害也大。就比如我用他人账户进行消费，这也属于支付漏洞中的越权问题。那么支付漏洞一般存在在哪些方面呢，根据名字就知道，凡是涉及购买、资金、积分、优惠价兑换等方面的功能处就有可能存在支付问题。

相对于其他漏洞来说，支付漏洞应该是很容易理解的，比如一分钱购买手机（但是大家渗透测试要有分寸）



支付漏洞也属于逻辑漏洞，挖掘这类漏洞有发散（QiPa）思维，往往有事半功倍的效果，简单来说就是不按常理出牌。

主要造成的危害：

对企业和用户的危害极大(主要是钱。。。。)

支付的原理

PHP演示基础支付流程

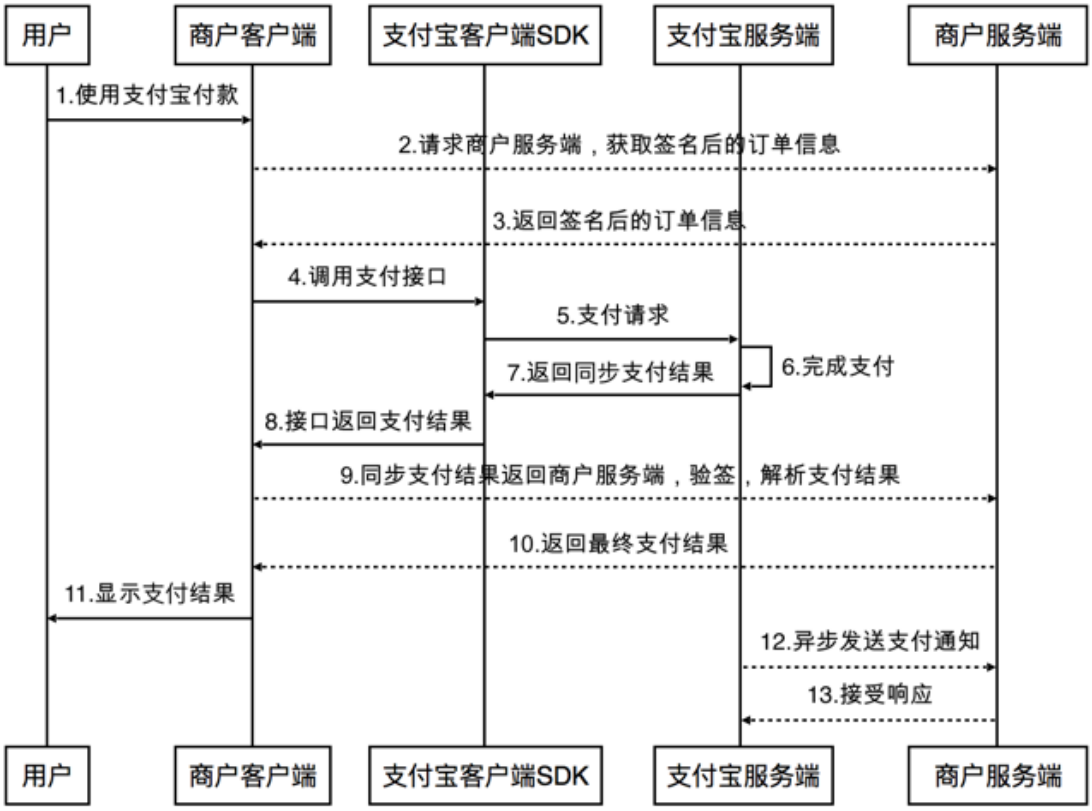
PHP先演示最简单的支付。

支付宝支付流程

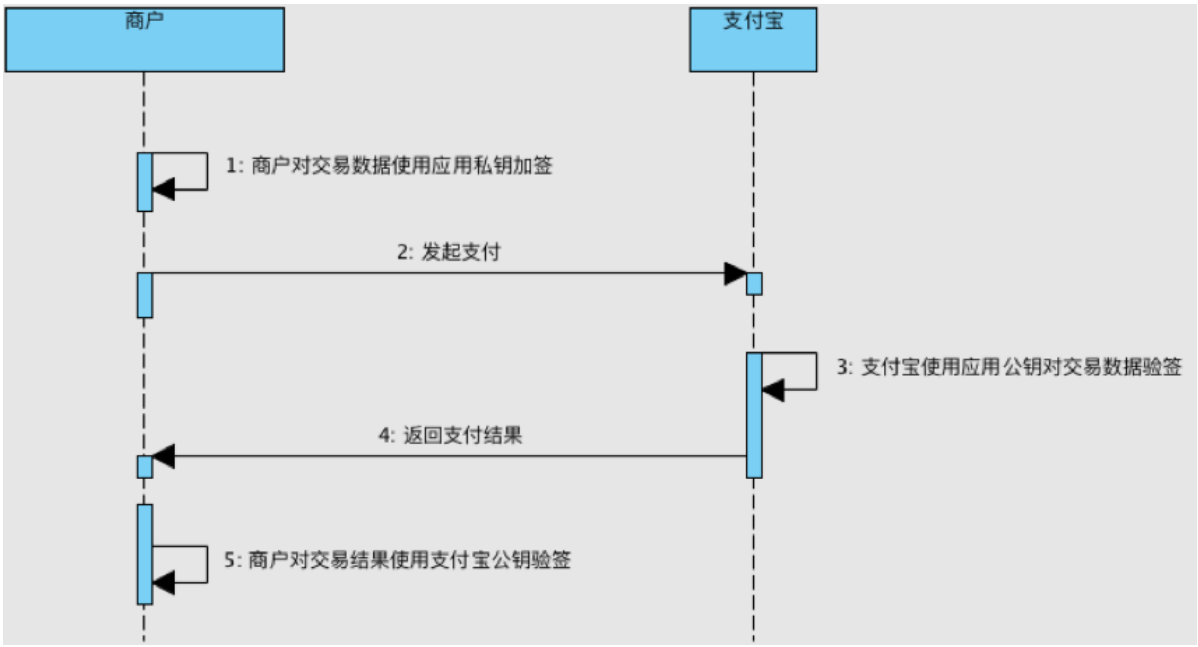
基本流程：


商家APP
1. 下单
商家后台
2. 返回订单信息
3. 根据订单唤起
钱包进行支付
6. 返回支付结果
7. 异步通知支付结果
支付宝App
4. 支付
支付宝支付后台
5. 返回支付结果

详细流程：


用户
商户客户端
支付宝客户端SDK
支付宝服务端
商户服务端
1.使用支付宝付款
2.请求商户服务端，获取签名后的订单信息
3.返回签名后的订单信息
4.调用支付接口
5.支付请求
6.完成支付
7.返回同步支付结果
8.接口返回支付结果
9.同步支付结果返回商户服务端，验签，解析支付结果
10.返回最终支付结果
11.显示支付结果
12.异步发送支付通知
13.接受响应
用户
商户客户端
支付宝客户端SDK
支付宝服务端
商户服务端

密钥体系：


商户
支付宝
1: 商户对交易数据使用应用私钥加签
2: 发起支付
3: 支付宝使用应用公钥对交易数据验签
4: 返回支付结果
5: 商户对交易结果使用支付宝公钥验签

支付漏洞的利用

利用前提：

- 目标网站有支付系统
- 在支付流程中，对于用户、商品、平台和（或）商家、支付公司四个重要因素之间有漏洞。

如何挖掘：

寻找网站的支付系统，或兑换系统，抓包判断有没有敏感信息可以修改。

修改支付价格

在支付当中，购买商品一般分为三步骤：订购、确认信息、付款。

那么这个修改价格具体是修改哪一步的价格呢？可以在这三个步骤当中的随便一个步骤进行修改价格测试，如果前面两步有验证机制，那么你可在最后一步付款时进行抓包尝试修改金额，如果没有在最后一步做好检验，那么问题就会存在，其修改的金额值你可以尝试小数目或者尝试负数。

相关例子：

- http://wy.zone.ci/bug_detail.php?wybug_id=wooyun-2016-0215059
- http://wy.zone.ci/bug_detail.php?wybug_id=wooyun-2016-0211806

修改支付状态

这个问题是没有对支付状态的值跟实际订单支付状态进行校验，导致点击支付时抓包修改决定支付或未支付的参数为支付状态的值从而达到支付成功。

修改商品数量

在支付的过程中，数量也同时决定着价格，比如：1个数量商品对应的是100，2个数据就是200，那么当你修改这个值数量值为负数时，那么其金额也会变为负数，最后就会导致支付问题的产生。

http://wy.zone.ci/bug_detail.php?wybug_id=wooyun-2015-0163435

http://wy.zone.ci/bug_detail.php?wybug_id=wooyun-2015-0161722

修改附属值

比如在很多购买的时候都可以利用积分或者优惠券等等进行代替金额付款，那么就容易存在问题。在这里我把附属值分为几类进行讲述。

1.修改优惠券金额

优惠券其基本都是优惠一半，一般用优惠券进行消费一般出现在第二个步骤当中：确认购买信息，在这个步骤页面当中，你可以选择相关优惠券，然后直接修改金额大于或等于商品的价格就可以，或者直接修改其为负值进行尝试，最后进行支付，如果对这点没有加以验证，那么问题就会产生，直接支付成功。

2.修改积分金额

有些网站有积分，比如你消费多少，评论多少就可以拥有一定的积分数量，这个积分可以在你付款的时候进行折扣其订单金额，如果这个没有做好积分金额的校验，那么当你在支付当中选择用积分为账户减一些金额的时候，可以抓包修改其积分金额为任意数或负金额，然后可0元支付成功。

http://wy.zone.ci/bug_detail.php?wybug_id=wooyun-2016-0167386

http://wy.zone.ci/bug_detail.php?wybug_id=wooyun-2015-0156253

修改支付接口

比如一些网站支持很多种支付，比如自家的支付工具，第三方的支付工具，然后每个支付接口值不一样，如果逻辑设计不当，当我随便选择一个点击支付时进行抓包，然后修改其支付接口为一个不存在的接口，如果没做好不存在接口相关处理，那么此时就会支付成功。

重复支付

一些交易市场有一类似于试用牌子或者其它，这个试用牌子可以依靠签到获得，而这个牌子的作用可以去试用一些商品，在你进行试用的时候会扣掉你的试用牌子，当你试用完成或者主动取消试用时，试用牌子会返回到账户当中。如果没有进行对订单多重提交的校验，那么就可导致无限制刷牌子，比如，你试用时抓包，然后你每次试用都会产生一个订单号，然后利用刚抓到的数据包进行批量提交，你就可以看到每次提交的订单号不一样，然后这时你再看订单可以看到同一个商品的无数订单，但试用牌子数只扣了你第一个试验时的牌子数，那么这时你申请批量退出试用，那么这么多订单，每退一个就会退相应的牌子数量到账户当中，这就构成了无限制刷得问题。

最大额支付

以前也是看到过相关的例子，一些网站比如你购买商品，这里有2个思路修改值，1是直接修改支付金额值为最大值，比如999999999，或者修改附属值，如优惠卷，积分等为999999999，如果这里逻辑设计有问题，那么其支付金额会变为0。

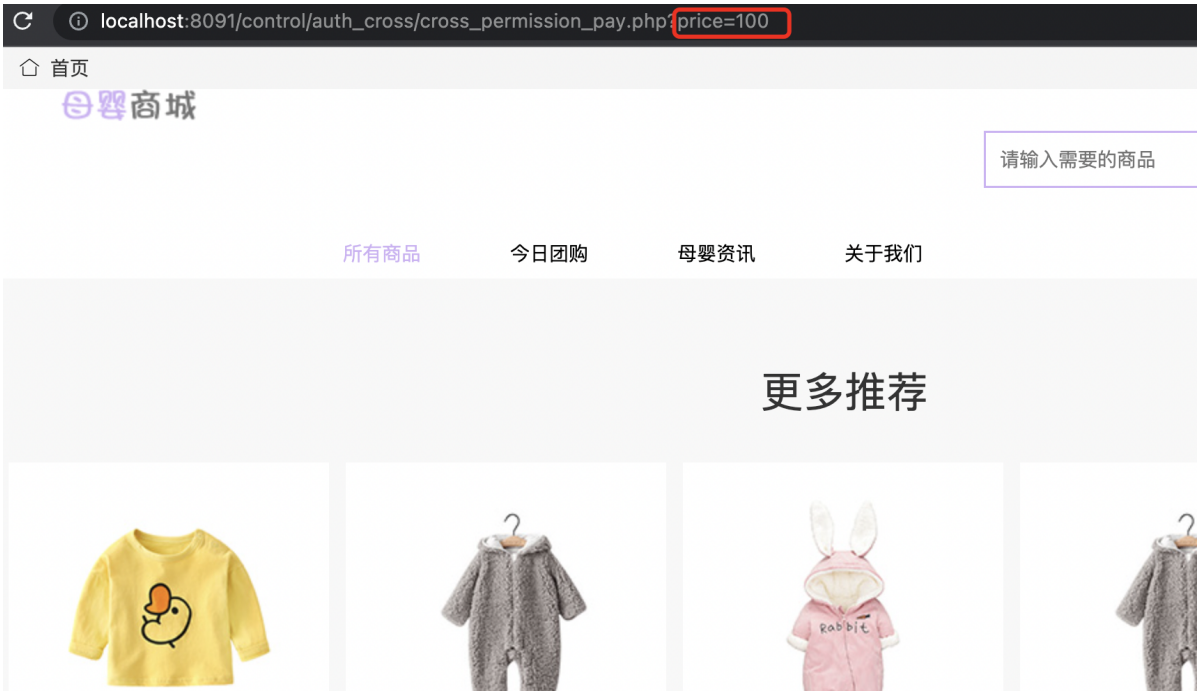
无限制试用

一些网站的一些商品，比如云系列产品支持试用，试用时期一般为7天或者30天，一个账户只能试用一次，试用期间不能再试用，但如果这个试用接口没做好分配那么很容易导致问题的发生。

越权支付

在支付当中会出现当前用户的ID，比如：username=XXXXX，如果没有加以验证，其支付也是一次性支付没有要求输入密码什么的机制，那么就可以修改这个用户ID为其它用户ID，达到用其他用户的账号进行支付你的商品。

WEBBUG支付漏洞



支付漏洞防御

- 对支付流程的每个环节进行校验，并且防止跳过某一个环节。
- 用户确认购买后，立即验证商品价格（商品单价、商品数量、折扣优惠）、订单价格和到账金额。
- 对一些优惠券、折扣券的使用方式进行测试。
- 修复防范网站其他漏洞。