支付逻辑漏洞思路小集合

支付漏洞算是一个高危漏洞，毕竟和钱沾边就轻不了，下面也是总结汇总了一些支付漏洞可能存在的操作点。(因为没有图所以可能比较枯燥，但我还是尽量用自己的话简单理了一遍)

一.直接的价格修改

这个在我高中的时候就发生过，某某商城一分钱撸手机，直接使用fd抓包，当时把存在这种漏洞的网站叫线报，自己也尝试过，不过没有成功(成功我估计就进去了)。
现在这种漏洞基本没有了，但是还是要简单说一下的。

在支付当中，购买商品一般分为三步骤：订购、确认信息、付款。
而我们修改哪一步呢？你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，修改金额我们同样也可以修改为负数等。

Plain Text 复制代码

```
实战案例：2k套餐0.5元拿下
http://wooyun.2xss.cc/bug_detail.php?wybug_id=wooyun-2016-0226613
```

二.修改支付状态

这个就类似于我们之前说的登录的一些逻辑漏洞一样，网站直接通过响应码判断是否成功。例如200成功，400失败等。
此外还有，例如A订单-0001完成——B订单-0002未完成
付款时尝试把订单B的单号给成订单A，也可能会导致未付款直接显示完成。

三.修改购买数量

在支付中，例如你买一个蜜汁小汉堡为十块钱，十个就是10*10=100，如果我们修改数量为-10个，那么是不是平台要反要倒给我们100，利用这个漏洞，我们就可以很便宜买到东西。

Plain Text 复制代码

```
实战案例：阿三商城数量修改引起的支付漏洞
https://www.freebuf.com/vuls/212089.html
```

四：支付附属值修改

我们在支付的时候，常会给你一些优惠券呀，积分呀，满减等等，而这些值同样都是没有操作的点。

①：修改优惠券金额

我们可以直接对数据包中优惠价的价格数量等进行操作，如果服务器对其没有验证，就会导致漏洞产

生。

②：修改优惠券金额及业务逻辑问题

有时候我们明明修改成功了，但是在支付时可能会失败或者显示金额不正确，这里不要放弃，我们还可以试试其他操作，虽然支付失败了，但是订单可能创建了，价格还是原来的价格，我们照样可以进行支付。
此外，很多平台可能存在一个钱包的功能，我们先充一点钱，然后选择用自带的钱包进行支付，那么也是有可能直接成功的。

③：修改积分金额

有些网站支付时可以使用积分，积分又可以抵现，我们也可以尝试修改这个地方，进行测试；此外我们也可以反向操作，例如下单10元送1积分，我们直接梭哈，修改个100，这样不也是一样嘛。

④：满减修改

例如每次双十一的跨店满减，300减100，我们可以对300修改，例如修改到101减100，降低满减门槛等等操作。

```Plain Text
实战案例：一夜成为凤凰书城最富的用户
http://wooyun.2xss.cc/bug_detail.php?wybug_id=wooyun-2016-0214319
```

同时也可以用到运费等其他支付附属值，都可以进行修改。

五：订单替代支付

举例：我们创建一个A订单为10元，创建一个B订单为100元，如果在支付过程中，我们将B的订单号改为A，服务器没有对其进行其他校验的话，我们是可以支付成功的，相当于10元撸到了100元的东西。

```
1  实战案例：顺丰宝支付逻辑漏洞
2  http://wooyun.2xss.cc/bug_detail.php?wybug_id=wooyun-2011-02272
```

这个操作简单就是说由于没有其他验证，我们可以先记下充值一元的单号，然后再替换0.01的单号，这样我们支付0.01就变成了充值一元，可以看到账号又多了一块钱。

六：支付接口替换

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。

七：重复支付

到这个有人可能会说，支付一次搞个数据包不久行了，为什么要重复支付，多花钱。
这里举一个例子，京东存在试用商品卡，一张卡可以试用一个商品，我们可以将这个试用商品的数据包进行多次提交，如果服务端没有进行校验的话就会产生很多订单，而如果我们将这个订单退掉，那么这个试用卡就会退回，如果我们将这些订单全部退掉，是不是就能获得很多试用卡呢?

八.最小额支付及最大支付(金额溢出)

①：最小支付

在很多白帽子测试支付的漏洞时候，修改的金额往往都是0.01等或者负数，我想说这很容易错失掉一些潜在的支付问题，因为有些厂商在设计时最低支付金额就是1元，低于这个全部算支付失败，所以我们在测试时不能直接修改太低，哪怕比原始金额少一元，也是可以证明存在支付漏洞的。

②：最大支付(金额溢出)

一般在开发当中，商品的金额都会用int 型来定义，那么 int 的最大值为2147483647，可以尝试修改为2147483648。看是否造成整数溢出，有可能支付状态异常，从而导致支付成功。
利用公式：2147483647/物品单价+1=物品数量

九.四舍五入导致支付漏洞

这个漏洞上次看小伙伴交的补天，获得了厂商1.2k的奖金，如何操作呢，我们来分析分析。

我们以充值为例，余额值一般保存到分为止，那么如果我充值0.001元也就是1厘，一般开发会在前端判断我们的数字，或者将最后一位四舍五入，使用支付宝充值是直接报错的，因为第三方一般只支持到分。

那我们如果充值0.019呢，由于支付宝只判断到分，所以导致只能支付0.01，而由于我们支付成功，前端会将9四舍五入，直接变成0.02，所以等于直接半价充值。(这个漏洞京东也是有的，不过后来修复了。)

十.首单优惠，无限重购

很多厂家为了留住用户，都会有一个首月半价，或者是免费等等的活动，我们可以抓取这个数据包，进行多次支付，就可以一直优惠购买。(百度云去年有这个漏洞，可以无限6元一月超级会员。)

十一.越权支付

这个问题很早之前有过，现在可能很少存在这类问题，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。

或者使用CSRF漏洞操作等等。

十二.并发数据包

这个思路就是在买一个商品的时候，支付操作抓包，高并发环境下反复多次购买，有可能会造成比如10块钱的东西，高并发操作下，花10块钱买了很多个。有些环境下要先满足兑换条件，例如兑换2次，一次1元，首先余额要够4元才可以。
(发散思路：退款等等也同样是可以并发操作的。)

十三.盲盒类抽奖

现在由于盲盒类的兴起，在线盲盒也多了起来，我们拿一个简单的举例，例如现在有三个盲盒，两个普通款，一个隐藏款，那我们如何100%能获得隐藏款呢，我们可以尝试修改盲盒的属性，例如隐藏款对应的id为1，普通款都为2，我们就可以将所有抽到id为2的修改为1即可。

十四.直播打赏类

一些直播平台的礼物可能还是根据id值来进行划分，其中就有可能存在一些内部测试的礼物，我们可以尝试对礼物的id值进行一个遍历，查看是否有其他隐藏信息。
暂时就简单总结这么多，这种支付类逻辑漏洞现在也有点难挖，厂商很多都有token、加密等，但是这类漏洞其实又很好挖，因为很多时候看你的思路有多宽，骚套路有多深，漏洞就能挖多深。
此外，支付类漏洞适可而止，搞太多可能还是会被请进去的。