1. 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。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。

这种方式可以参考这个案例：

<https://bbs.ichunqiu.com/forum.php?mod=viewthread&tid=8236>

1. 修改购买数量

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。

1. 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劵等等进行代替金额付款，那么就容易存在问题。在这里把附属值分为几类进行讲述。

①：修改优惠劵金额

优惠劵其基本都是优惠一半，一般用优惠劵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劵，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：修改优惠劵金额及业务逻辑问题

这个漏洞也是逻辑问题导致了成功利用，同样在是在第二部确认购买信息当中有可选择优惠劵进行支付，但是，当你修改其优惠劵值为任意值或负值想要支付的时候，会回显支付失败，或者金额有误等一些提示，可能这时很多白帽子会很失望然后就会去其它点找问题了，但当你找到个人中心，点击订单详情，如果存在这个逻辑问题，那么此时在你刚刚修改优惠劵金额后点击下一步支付的时候，其实这时候就已经产生了订单了，你在订单详情内就可以看到支付金额为0，因为你刚刚修改了优惠劵金额嘛，然后点击支付就可以支付成功。

当然，这里还要说下小技巧，有可能会支付失败，但是如果找到的这个问题是一个一般业务分站点，如果有自带的一个钱包功能，那么就可以利用这个只带的钱包功能去支付这个订单，而不要利用其它支付类型，那么就可以支付成功！

③：修改积分金额

有些网站有积分，比如消费多少，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。

1. 最大额支付

以前也是看到过相关的例子，一些网站比如购买商品，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。

1. 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。

1. 无限试用

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会做好分配那么很容易导致问题的发生。

比如：在支付的时候它URL后面的支付接口是3，而试用接口是4，那么此时你已经使用过了，复制下确认试用时的URL，修改后面的支付接口为3，那么此时就会调用购买支付接口，但是由于本身这个产品就是试用的，其相应值绑定了这个试用商品，那么金额就肯定是0，那么最后点击支付，就可以看到支付成功，试用成功，又重复试用了一次，然后他们的试用时间会累加在一起，这就导致了可无限制购买任何产品了。

1. 修改优惠价格

比如一些商品有优惠价，优惠多少多少，那么在支付时抓包，修改这个优惠价就可造成支付问题的产生。

1. 多并发

多线程并发问题就是没有实时的处理各种状态所导致的问题，之前挖掘过刷钱问题，就是利用该思路，比如很多平台有自家的钱包，而这个钱包是一个迷你钱包，这个钱包作用也仅是用于这当前一个业务平台网站，在提现时，没有任何验证码或者校验机制，只要输入体现金额就可以提现，并且是秒到账，如果什么负数，修改金额都测试过了都不行，那么你就可以试试多线程并发问题，提现时抓包，比如现在钱包内有0.1元，那么按理说每提0.01可以体现10次，也就是发送10次进程，但是利用这个问题可以达到多发现几次成功的进程，提现时抓包，然后把数据包发送到BurpSuite工具的Intruder当中，进行批量发送18次，然后可以看到成功的提现到了12次。

这里是从0开始到11截止，账户内只有0.1 而这里体现了0.12 也就是提现的进程为12次，369为提现成功，349为提现失败的长度值，从这里就可以看出这个问题的危害了，当然此时账户的金额肯定是为负的了，如果把这个提现金额变大，是一笔不小的数字

多线程也可以在其它功能处进行测试，比如利用积分换礼品，一个账户只能进行总换一次，利用这个问题，可以多几次总换，一些转账功能，提现功能，购买功能等等很多。