越权让他人支付

<https://forum.butian.net/share/1125>

四舍五入半价购

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。)



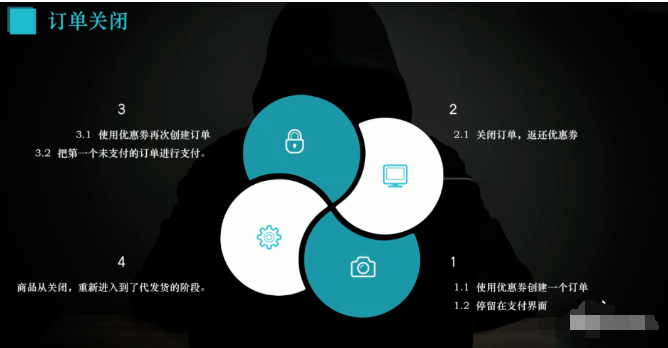


并发提前全签到

1. 采用时间验证，修改当前设备时间绕过
2. 未采用验证，直接修改数据包对应发包



循环利用优惠券



支付签约多逻辑



大家都知道有些软件推出了新用户的会员签约功能，新的用户首次签约付费时能以低价购买会员，这个时候就尝试想白嫖多个月的低价会员了。于是开始第一次测试——使用支付宝打开签约界面，然后使用微信也同时打签约界面，然后再依次支付，支付后系统提示，无法重复签约。

我想难到系统有检测？舍不得孩子套不到狼，于是申请个新号再次进行测试：

* 还是同时支付宝和微信都打开了签约界面，但这次先签约其中一个比如先签约微信；
* 微信支付成功并签约完成后，在微信取消签约，然后再去支付宝点击签约；

这个时候奇迹就发生了，系统成功到账了2个月的低价会员！

也就是说服务器虽然校验了同一新用户不能同时多次低价签约，但是对于新用户同时发起的多个支付签约页面的请求，服务器没有校验解约后再次签约的情况，导致成功白嫖！以上的一个业务逻辑流程大致如下图：

