支付漏洞四舍五入 re

前言：挖洞是一个需要思维的，而不是一成不变的模仿，做到举一反三，赏金还愁什么呢，在星球刚创立的时候我们就发布了四舍五入的支付漏洞，大家在挖掘的时候，看见的特征点就是自己的钱包的 0.00 的时候就要想到这个漏洞，但是也要学会变通。

## 0X01:发现过程：

我某天乱逛的时候看见了一个和某宝差不多可以购买 J 金的项目，然后就随手下载了 app，打开一个，发现钱包余额是 0.00 的字眼，我随手充值了 1.01 ,1.005,1.05 但是最后充值都是很正确的


然后我也放弃了这个漏洞的想法，我晚上睡觉的到时候，我又把这个 app 拿出来看（因为我买了某金嘛，我就想看看我赚没） 晚上拿出来看的时候我就发现了提线这个功能点：

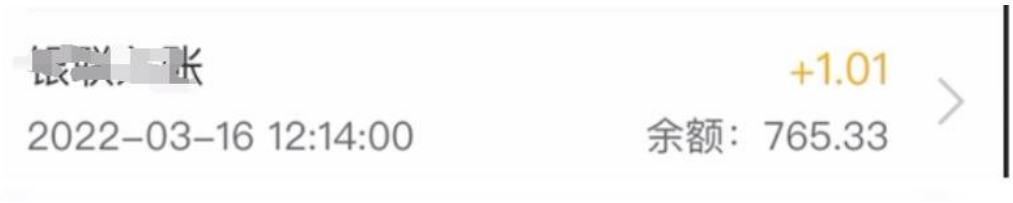

我就在想，我们充值都可以四舍五入，那么提现也可以撒!!! 于是起床开始测试：

首先提现一元的时候将数据包改为提现 1.005 看看会是什么情况：


当显示成功的时候，我看见是 1 元的时候我也以为失败了：



看到余额变成 2.04 的时候我心里也是凉凉的 但是!!!!!!!!!!!!!!!!!!!!!!
没过多久我 vx 发来了收款信息：
直接乐翻天：




这样四舍五入不就来了，直接提交！

## 0X02:反思

就是要熟悉漏洞点和经常去琢磨，就比如上面一样，四舍五入大家都知道，但是大家的思维都被作者的充值思维所局限，没有去思考，只会在充值的时候想到 4 舍五入，我的猜测就是这个项目可能在支付和提现的两个功能点都有，但是支付的被发现了，而提现的点就被放过了，所以在测试漏洞的时候，可以多思考和多笔记去分析