

因为 12 月份团队师傅们都在忙着百度的比赛，1 月份过年也比较忙所以更新的比较少，而我准备升学考试这几个月可能没时间更新了。废话就不多说了进入主题



在企业 src 里面支付业务肯定是必不可少的，那么有业务肯定就有漏洞，今天就来讲一下

我们用余额充值为例，余额都是保留到分(也就是 0.00)当然有些区块链的网站可能会更精确

那么如果我们充值 0.001 会怎么样呢，那么开发一般会前端判断我们输入的数字，或者直接把后一位四舍五入了

我们来试试



The screenshot displays the Alipay 'Balance Recharge' (余额充值) interface. At the top, there is a 'pay' logo, the title '余额充值', and a 'Return' (返回) button. Below this, there are two main options: 'Online Recharge' (在线充值) and 'Recharge Code Exchange' (充值码兑换). The 'Online Recharge' option is highlighted with a blue background and a smartphone icon. Below these options, there is a dashed horizontal line. Underneath the line, there is a numeric input field containing the value '0.001'. To the right of the input field is a small up/down arrow icon. At the bottom right of the interface, there is a blue button labeled 'Confirm Payment' (确认支付).

支付宝直接报错，因为第三方支付是只能充值到分的

收银台

支付单号: 6663F3DE

充值: 0元

待支付



订单信息有错误, 建议联系卖家

错误码: TOTAL_FEE_EXCEED

请使用支付宝扫描
二维码以完成支付

那我们就可以尝试一下充值 0.019 看看会发生什么事



我们可以看到显示的是 0.01 后面的 9 直接忽略了，因为第三方支付只能判断到分

支付单号: 60CC72AC

充值: 0.01元

待支付

请从以下选项选择一个支付方式

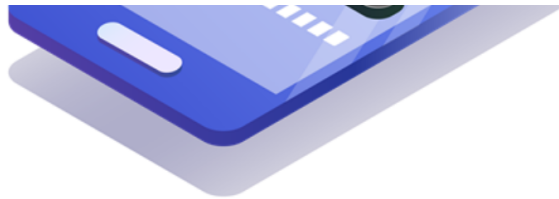


支付宝
生活好 支付宝



微信
推荐 更快更安全

我们支付看看



成功充值 0.02 元

返回主页

充值了 0.02，是不是惊喜，那么漏洞不就出来了吗？

利用四舍五入的性质就可以实现半价充值了

那么在企业 src 中也是很常见的，主要是利用这个四舍五入的性质来欺骗服务器。