

快便支付原理

商户网站接入支付结果有两种方式，一种是通过浏览器进行跳转通知，一种是服务器端异步通知

浏览器跳转

基于用户访问的浏览器，如果用户在银行页面支付成功后，直接关闭了页面，并未等待银行跳转到支付结果页面，那么商户网站就收不到支付结果的通知，导致支付结果难以处理。而且浏览器端数据很容易被篡改而降低安全性

服务器端异步通知

该方式是支付公司服务器后台直接向用户指定的异步通知 **URL** 发送参数，采用 **POST** 或 **GET** 的方式。商户网站接收异步参数的 **URL** 对应的程序中，要对支付公司返回的支付结果进行签名验证，成功后进行支付逻辑处理，如验证金额、订单信息是否与发起支付时一致，验证正常则对订单进行状态处理或为用户进行网站内入账等

如何挖掘

如何挖掘

支付时进行抓包，找到支付关键的数据包可能一个支付操作有三四个数据包，我们要对数据包进行挑选。

分析数据包

支付数据包中会包含很多的敏感信息（账号，金额，余额，优惠，订单 ID）要尝试对数据包中的各个参数进行分析

支付的价格-支付漏洞

Url: <https://xxxx.xxxx.com/>

1.修改单价

后台逻辑是 总金额 = 单价 * 数量, 我们只需要修改单价即可

产品名称	产品有效期	单价(元)	购买数量	小计(元)
<div></div> <div>用户)</div>	1年	7980.00	<div>-</div> <div>1</div> <div>+</div>	7,980.00

输入优惠码

实付款(元): **¥7,980.00**

提交订单

产品名称	产品有效期	单价(元)	购买数量	小计(元)
户)	1年	0.01	<div><div>-</div><div>3</div><div>+</div></div>	0.03

实付款(元):

¥0.03

修改单价

有效期	单价(元)	购买数量	小计(元)
1年	7980.00	<input type="text" value="3"/>	15,960.00

输入优惠码 ▾

实付款(元): **¥ 15,960.00**

提交订单

```

7 Au
8 Pa
9 Ap
10 Us
11 Ch
12 Co
13 Ac
14 En
15 Se
16 Us
17 Cl
18 Ap
19 Se
20 Or
21 Se
22 Se
23 Se
24 Re
25 Ac
26 Accept-Language: en-us;q=0.8
27 Connection: close
28
29

```

```

1,"increaseUnit":null,"increaseMsg":null,"productL
数加油包(20用户)","prodDesc":
"price":"0.01","num":3,"prodType":3,
P":0,"effectiveTime":null,"expirationTime":null,
"
:1
"U
"
"
+1

```

订单详情:

支付方式:

请及时完成付款，避免订单取消!

支付金额: **0.03**元

确认支付

×

全部账单

商家

-0.30

我的订单列表

请输入购买账

订单日期

~

订单日期

图

查询

重置



订单编号

订单类型

产品名称

订单提交时间



购买成功!

共 5 条

10条/页

