SySCAN 360
I HACK THEREFORE I AM
国际前瞻信息安全会议
INFORMATION SECURITY CONFERENCE
2016.11 · SHANGHAI

Security Vulnerabilities on Online Payment: Summary and Detection

Qing Zhang(VulpeckerTeam@Qihoo 360)

Joint work with
Guangdong Bai (Faculty Member in SIT), Ye Zhou (VulpeckerTeam@Qihoo 360)

01 Web 3.0时代的安全漏洞

层出不穷的支付安全漏洞

支付协议实现的安全漏洞

IEEE S&P 2011: Rui Wang et.al. How to Shop for Free Online Security Analysis of Cashier-as-a-Service Based Web Stores

开源商店代码的安全漏洞

- NDSS 2014: Pellegrino et.al. Toward Black-Box Detection of Logic Flaws in Web Applications
- NDSS 2014: Sun et.al. Detecting Logic Vulnerabilities in E-Commerce Applications

Token泄露

Black Hat US 2016. Mendoza. Samsung Pay: Tokenized Numbers, Flaws and Issues.

为什么这么多的支付安全漏洞呢？

- 支付安全漏洞一般是涉及协议以及逻辑方面较之其他安全漏洞更难察觉。
- 电商网站使用开源代码，更新不及时，存在严重的支付安全风险。
- 开发者缺乏支付安全的知识储备与开发经验。
- 安全通信协议不安全。
- 移动端带来了新的攻击面。
- 第三方支付掉链子。

影响

由于支付过程涉及金钱，因此支付安全漏洞较之其他类型的安全漏洞具有更高的敏感性和危害性。

薅羊毛

0元支付

资金蒸发

。。。

我们的工作

1 在线支付漏洞的研究及挖掘

- 总结了15种类型的在线支付的安全漏洞
- 研究了80多个电商网站以及APP，共检测到8种新型支付漏洞（所有漏洞均已告知商家，现已修复）

2 支付漏洞的检测与防护

3 现在以及未来工作

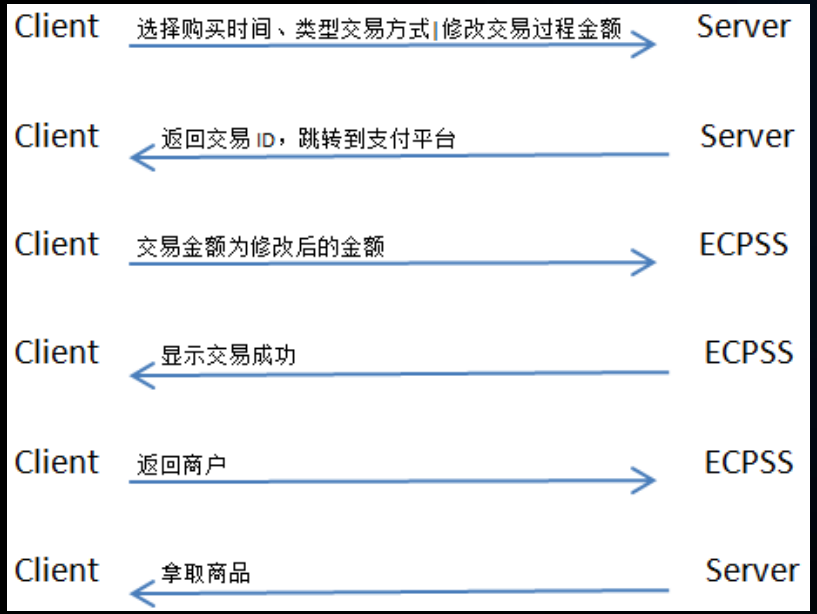
- 支付协议的形式化验证

» 02 那些“便宜的”商品

类型一：支付金额完整性 - 篡改支付金额

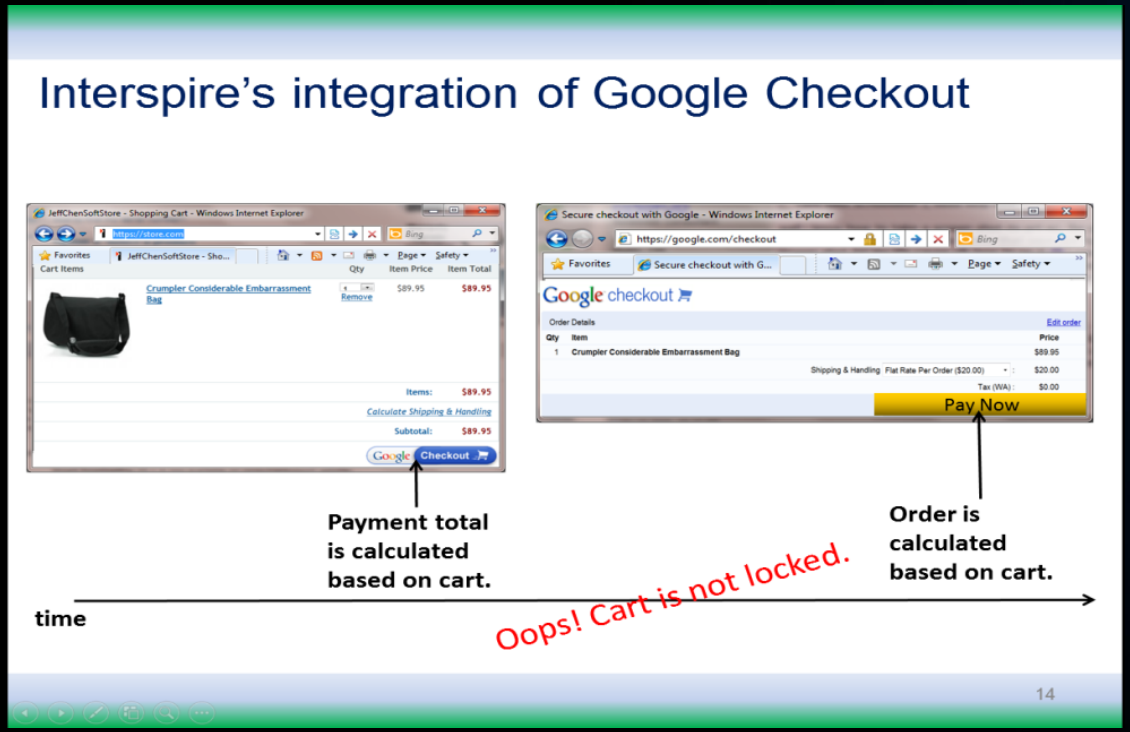
SySCAN 360
I HACK THEREFORE I AM

支付流程及攻击方式



示例一：某VPN购买网站

类型二：订单完整性 - 订单生成后加货物



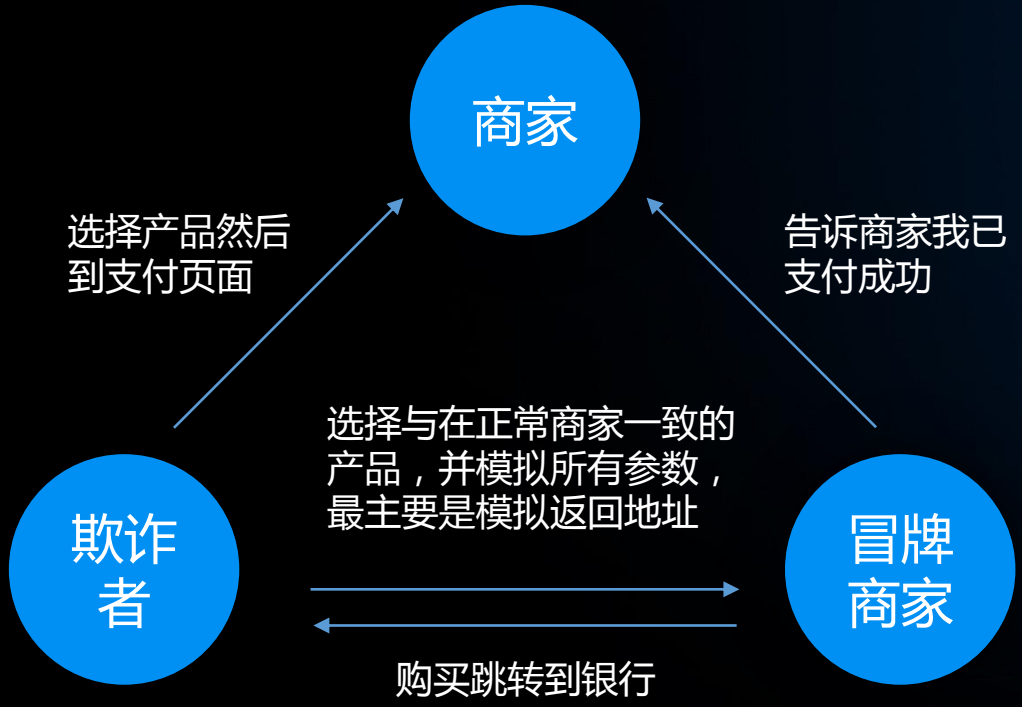
示例来源：Rui Wang et.al IEEE S&P 2011

类型三：支付凭证重放

购买成功后，会有一个从银行向商户网站跳转的过程，如果这个过程反复的重放，有可能会导致商品的反复购买和增加，但是用户不需要支付更多的金钱。

类型三：支付凭证重放 - 中间人攻击

攻击者设置一个商家，并向自己支付，然后将支付成功的消息重放到正常商家。



类型四：第三方支付漏洞导致所有商家信息泄露

漏洞原因：

- 第三方支付完成后，页面从支付网站跳转到商家网站
- 如果修改支付订单的订单号，页面自动跳转到该订单对应的商家
- 跳回的页面中含有用户在商家的订单信息
- 遍历订单号，攻击者可以获取在该第三方支付网站上支付成功的所有订单

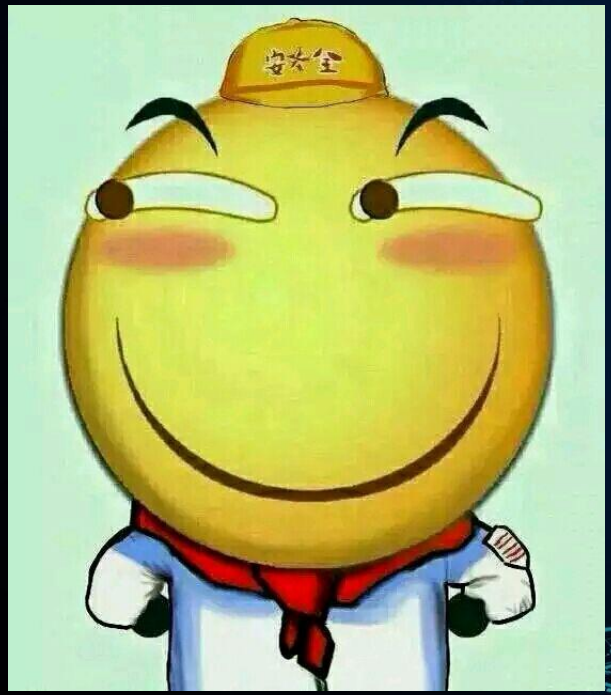
示例：X钱支付


亲爱的 newzq ，欢迎您登录本系统！
您的当前级别是： 直接客户（查看价格列表）
售前咨询 技术支持 财务问题
域名问题 网站备案 投诉建议
·您的帐户
在线充值
申请提现
转易网
可用金额 1 元
实际余额 1 元
入款总额 1 元
冻结金额 0 元
返款总额 0 元
借款金额 0 元
消费总额 0 元
优惠券 0 张
美橙互联 CNDNS.COM
将我的美橙账号和资金转移到美橙香港站
ezNet.hk
美橙香港站
www.eznet.hk
专业-可靠-稳定的互联网服务
主推香港主机空间及美国空间
您需要在行程结束后登录 东航官网 或使用 东航移动E 激活本次赠送达人券。

危害性：

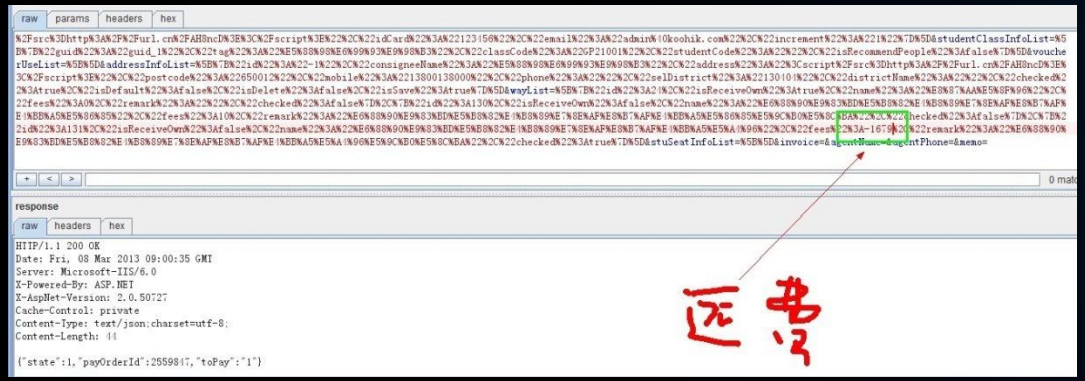
据我们统计，数千家在线购物网站受到此漏洞的影响。

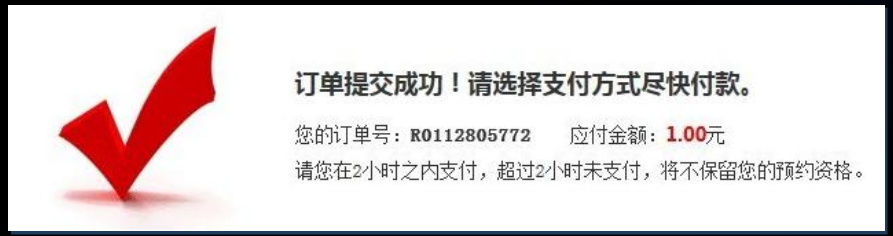
我们在X宝支付等其他第三方支付平台发现
过同样类型的漏洞。



类型五：数字签名未覆盖完整

此案例金额已经做了签名校验，但是仍然有一个未签名的参数会对最后的交易造成影响从而导致了问题的发生。@koohik





类型六：订单替换

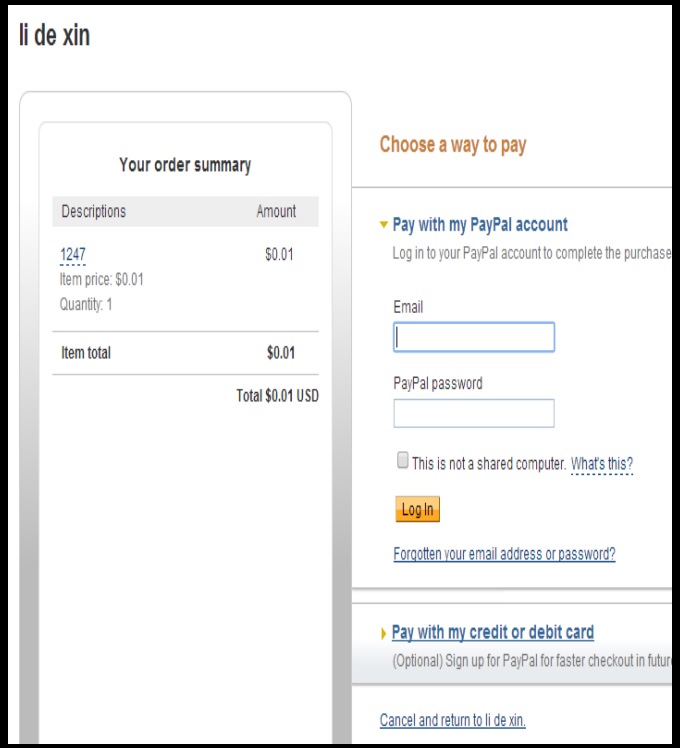

订单信息
订 单 号：1312051528064630190
订单内容：读览天下充值
应付金额：￥1元
支付必看：使用在线支付请注意，付款成功后请不要急于关闭付款页面，请依据
在线付款成功，但订单状态仍然显示未支付，或者充值未到账）。如果发生丢单情况，请
客服电话:400 606 9800 服务时间：(周一至周五9:00-18:00) 客服邮箱：service@doolan

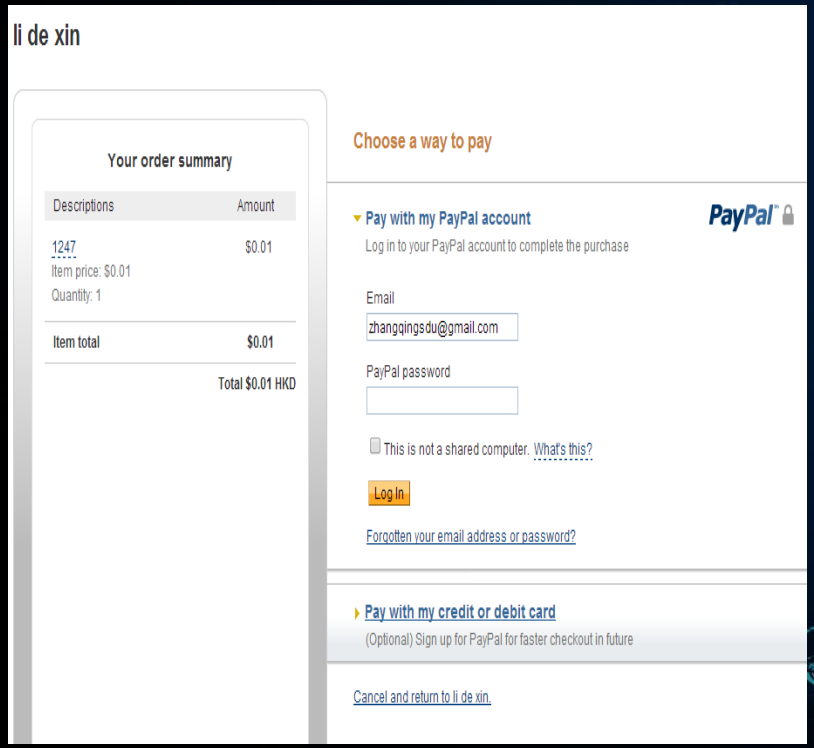

订单信息
订 单 号：1312051528504630190
订单内容：读览天下充值
应付金额：￥671元
支付必看：使用在线支付请注意，付款成功后请不要急于关闭付款页面，请依据提示点
在线付款成功，但订单状态仍然显示未支付，或者充值未到账）。如果发生丢单情况，请立即联
客服电话:400 606 9800 服务时间：(周一至周五9:00-18:00) 客服邮箱：service@dooland.net


www.dooland.com/magazine/mybank.php
读览天下
首页
杂志
图书
客户端
优惠专区
会员专区
VIP产品专区
个人中心
年终大促再续
最后15天狂欢!
温馨提示：您在会员账户中充入的充值帐项是您在读览天下网消费的预付帐，一旦充值成功，充值款项将不予退还。
点击确定后，系统将跳转到支付平台，请选择适合您的支付方式进行支付

类型七：货币单位完整性 - 货币单位替换

这种问题多发生在paypal等国际支付的场景。

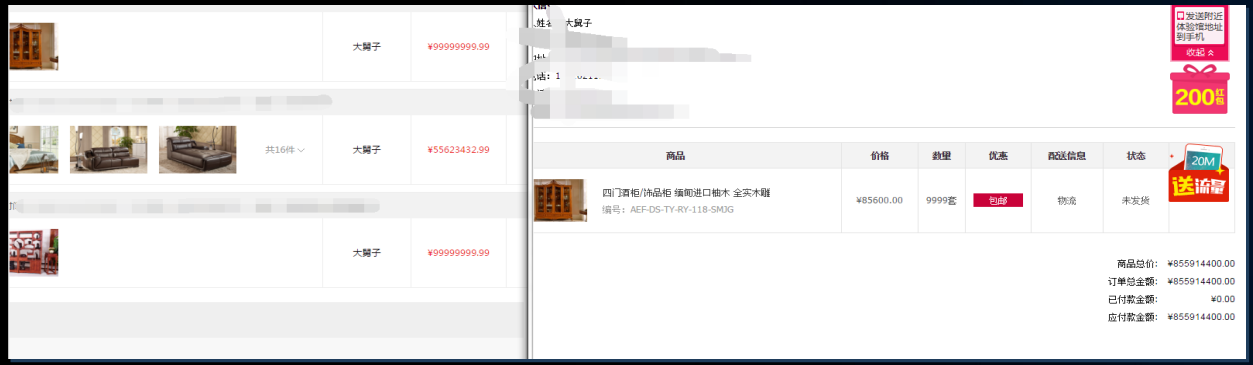




示例：这是一个印尼盾变美元的故事。。。

类型八：溢出攻击 - 金额数字溢出

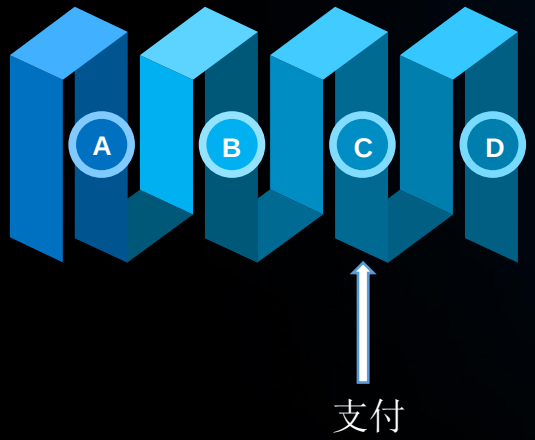
如果支付过程中没有对支付金额的上限进行安全控制，那么有可能会导致程序进入异常处理流程。比如说买不管买多少货物金额都是固定的，再严重一点就会导致0元支付。



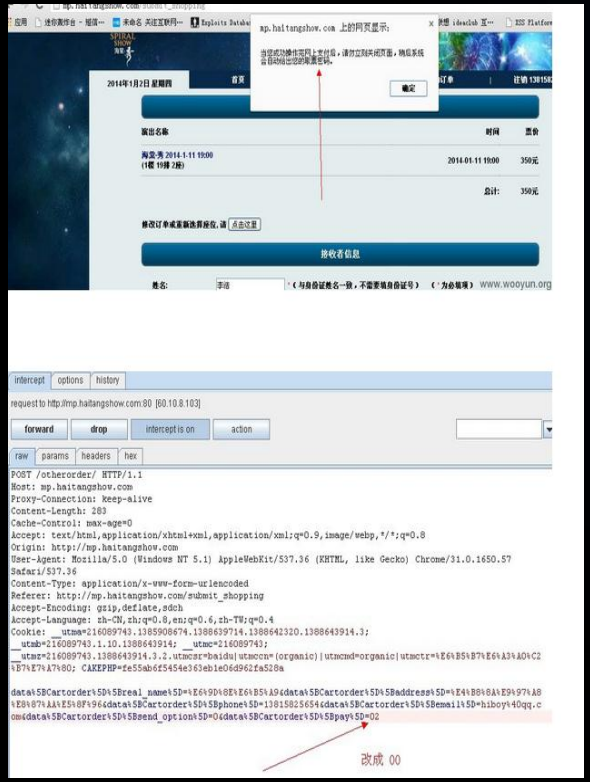
@imlonghao

类型九：顺序执行缺陷

购买过程：



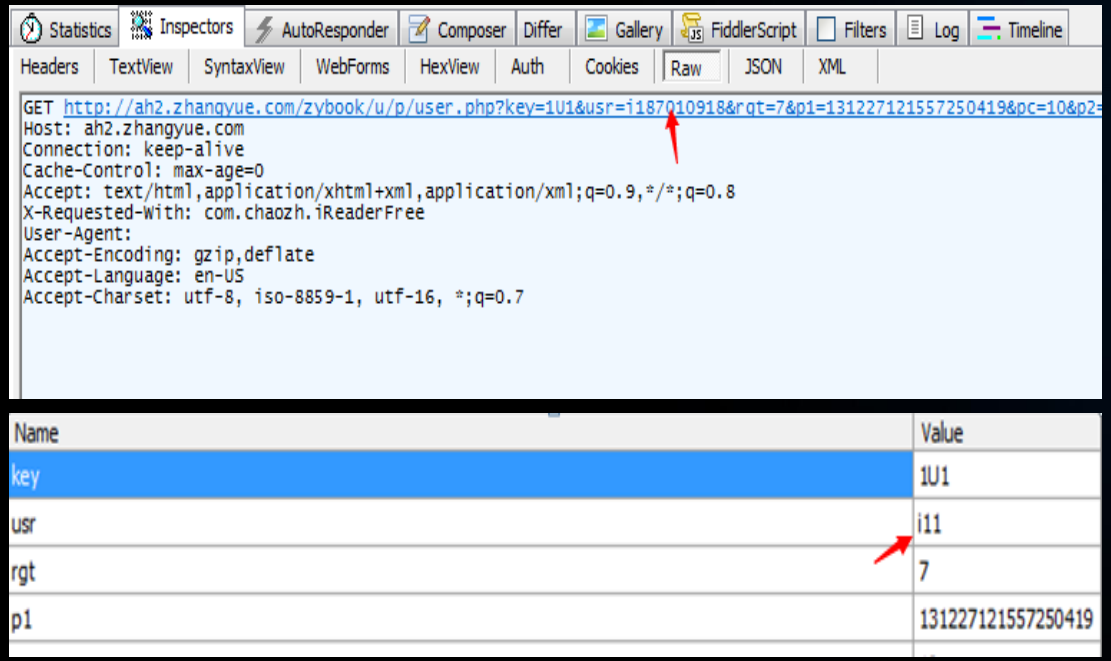
示例：轻松买票



@sex is not show

类型十：用户完整性 - 用户替换

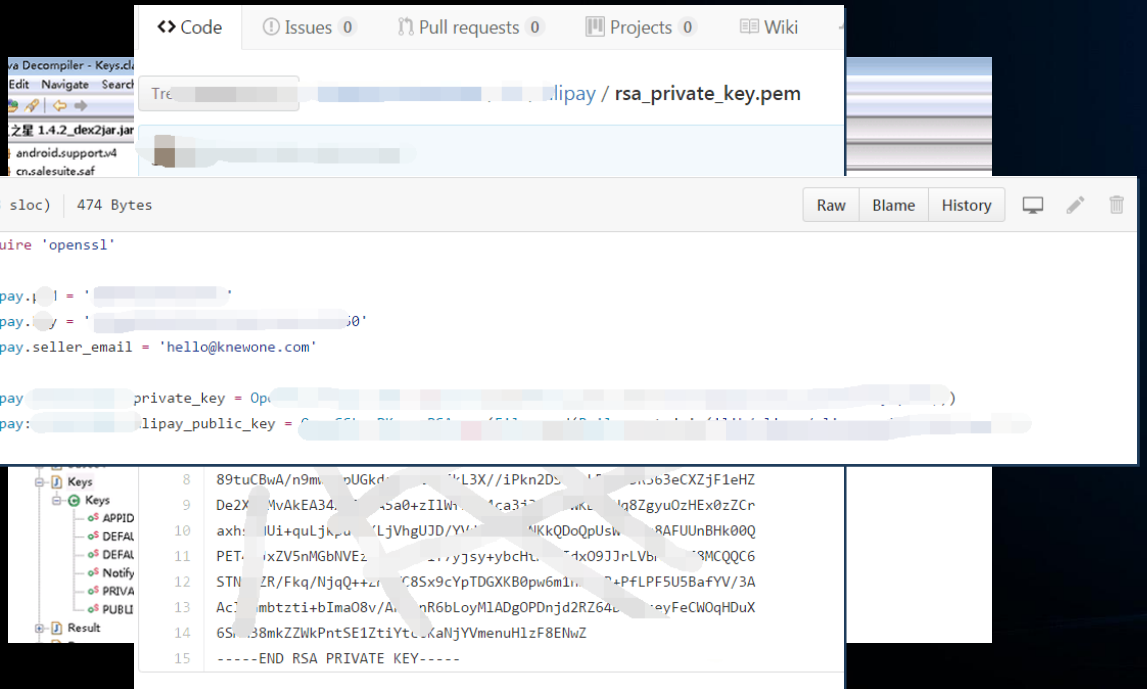
花别人的钱买自己的东西。



示例：瞬间成为初创员工有木有。。。

类型十一：密钥泄露

内置支付功能的app为了设计上的方便有可能会把私钥硬编码到代码或配置文件中，导致攻击者反编译apk之后获取密钥信息使得交易信息可以被篡改。



类型十二：函数修改

apk反编译之后的函数修改，有可能导致商家在最后一步向支付方提交订单时未验证信息的准确性，虽然此时已经对信息进行签名，但是仍然被篡改。

```
protected Integer onExecute(String[] paramArrayOfString)
{
  try
  {
    JSONObject localJSONObject1 = new JSONObject();
    localJSONObject1.put("service", "alipay");
    localJSONObject1.put("subject", OrderDetailActivity.this.currentOrder.ResvId);
    localJSONObject1.put("body", OrderDetailActivity.this.orderDetail.HotelName);
    localJSONObject1.put("totalFee", OrderDetailActivity.this.orderDetail.Amount);
    String str1 = JSON.toJSONString(localJSONObject1);
    String str2 = Md5Encrypt.getInstance().sign(str1);
    JSONObject localJSONObject2 = new JSONObject();
    localJSONObject2.put("signKey", str2);
    StringEntity localStringEntity = new StringEntity(str1, "UTF-8");
    Log.d("OrderDetailActivity", localJSONObject2.toJSONString());
    Log.d("OrderDetailActivity", "postBody : " + localJSONObject1.toString());
    String str3 = ServerURIBuilder.UriBuild("/pay/doAlipay.json", localJSONObject2, Boolean.valueOf(true), "2.0");
    HttpJsonPost localHttpJsonPost = new HttpJsonPost();
    localHttpJsonPost.makeHTTPRequest(str3, null, localStringEntity, new CommHttpClient.OnResponseReceivedListener(localHttpJsonPost)
    {
      public void onResponseReceived(InputStream paramInputStream)
      {
        try
```

示例：篡改支付信息


14:43
支付宝
单人房B全部房金
0.01元
支付宝账户
J@163.com
当前账户余额为0元
余额宝
使用银行卡付款： 0.01元
招商银行信用卡(尾号3339)
支付宝支付密码
找回支付密码
确认付款
可入住
单人房A
山东省济南市历下区解放东路60号
入住日期
15 08月 星期五
离店日期
16 08月 星期六
入住间数
1 间
入住人姓
联系人电话
订单金额 159元
价格明细
订单号 CC20140813012115
支付状态 支付成功
友情提示：
1、所有住客和访客均需携带身份证到前台登记
2、最早入住时间为入住当天早上8:00。如早于8:00到店，预订单入住日期请选择前一天

类型十三：越权获取其它订单信息

尤其是针对于虚拟商品，例如电影票，团购券，各种账号获取码等。。。

类型十四：暴力破解

如果第三方支付使用md5值作为签名校验，并且约定的密钥过短，便可以对其进行暴力破解，获取密钥值。

4.2 签名

签名是为了防止从商户系统提交的支付请求被非法篡改。

签名的方法包括使用 MD5 算法计算签名字符串的消息摘要。

在签名字符串末尾增加 MD5 密钥，密钥是在[redacted]户服务网站上设置。

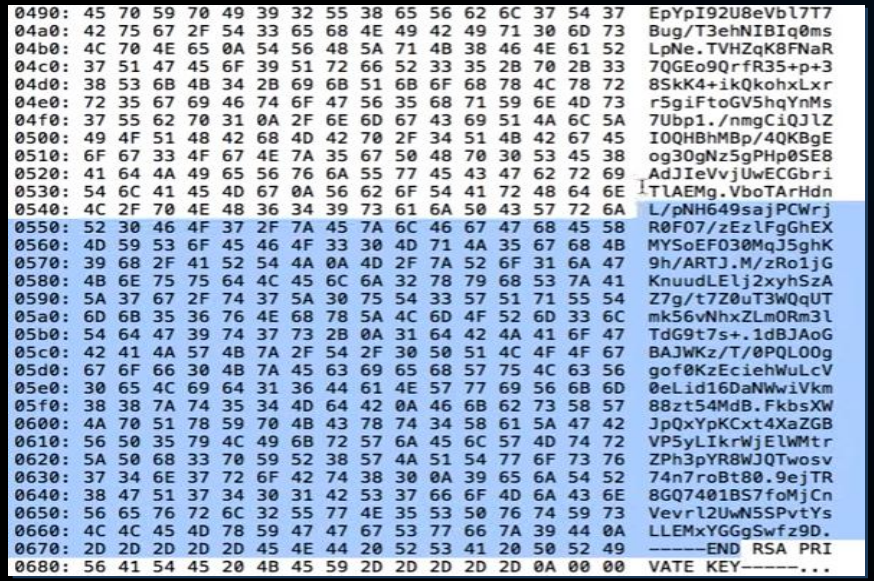
例如：

```
inputCharset=1&pickupUrl=http://192.168.1.41/demo/eshop/display-pay-result/display.do&receiveUrl=http://192.168.1.41/demo/eshop/recv-pay-result/recv.do&version=v1.0&language=1&signType=1&merchantId=100020091218001&payerName=mc&payerEmail=mc@allinpay.com&payerTelephone=13700090009&orderNo=N020100716131226&orderAmount=1&orderCurrency=0&orderDatetime=20100716131226&productName=Dell&productPrice=100&productNum=1&productId=P1005001&productDescription=Good&ext1=ext1&ext2=ext2&key=1234567890
```

使用 MD5 算法对签名字符串计算摘要，MD5 中的字母需转换为大写字母，例如上面的签名字符串所计算出的摘要为 CCFFF9C33B70FC6037677B3E9BA1A2CC，此值即为 signMsg 的字段值。

类型十五：可能影响到支付的底层漏洞

典型的例子是openSSL heart bleed漏洞。漏洞可能会导致支付过程中使用的RSA私钥被泄漏。



```
0490: 45 70 59 70 49 39 32 55 38 65 56 62 6C 37 54 37  EpYpI92U8eVbl7T7
04a0: 42 75 67 2F 54 33 65 68 4E 49 42 49 71 30 6D 73  Bug/T3ehNIBIq0ms
04b0: 4C 70 4E 65 0A 54 56 48 5A 71 4B 38 46 4E 61 52  LpNe.TVHZqK8FNaR
04c0: 37 51 47 45 6F 39 51 72 66 52 33 35 2B 70 2B 33  7QGEo9QrfR35+p+3
04d0: 38 53 6B 4B 34 2B 69 6B 51 6B 6F 68 78 4C 78 72  8SkK4+ikQkohxLxr
04e0: 72 35 67 69 46 74 6F 47 56 35 68 71 59 6E 4D 73  r5giFtoGV5hqYnMs
04f0: 37 55 62 70 31 0A 2F 6E 6D 67 43 69 51 4A 6C 5A  7Ubp1./nmgCiQJlZ
0500: 49 4F 51 48 42 68 4D 42 70 2F 34 51 4B 42 67 45  IOQHBhMBp/4QKBgE
0510: 6F 67 33 4F 67 4E 7A 35 67 50 48 70 30 53 45 38  og3OgNz5gPHp0SE8
0520: 41 64 4A 49 65 56 76 6A 55 77 45 43 47 62 72 69  AdJIeVvjUwECGbri
0530: 54 6C 41 45 4D 67 0A 56 62 6F 54 41 72 48 64 6E  TlAEMg.VboTArHdn
0540: 4C 2F 70 4E 48 36 34 39 73 61 6A 50 43 57 72 6A  L/pNH649sajPCWrj
0550: 52 30 46 4F 37 2F 7A 45 7A 6C 46 67 47 68 45 58  R0FO7/zEzlFgGhEX
0560: 4D 59 53 6F 45 46 4F 33 30 4D 71 4A 35 67 68 4B  MYSoEFO30MqJ5ghK
0570: 39 68 2F 41 52 54 4A 0A 4D 2F 7A 52 6F 31 6A 47  9h/ARTJ.M/zRo1jG
0580: 4B 6E 75 75 64 4C 45 6C 6A 32 78 79 68 53 7A 41  KnuudLElj2xyhSzA
0590: 5A 37 67 2F 74 37 5A 30 75 54 33 57 51 71 55 54  Z7g/t7Z0uT3WQqUT
05a0: 6D 6B 35 36 76 4E 68 78 5A 4C 6D 4F 52 6D 33 6C  mk56vNhxZLmORm3l
05b0: 54 64 47 39 74 37 73 2B 0A 31 64 42 4A 41 6F 47  TdG9t7s+.1dBJAoG
05c0: 42 41 4A 57 4B 7A 2F 54 2F 30 50 51 4C 4F 4F 67  BAJWKz/T/0PQLOOg
05d0: 67 6F 66 30 4B 7A 45 63 69 65 68 57 75 4C 63 56  gof0KzEciehWuLcV
05e0: 30 65 4C 69 64 31 36 44 61 4E 57 77 69 56 6B 6D  0eLid16DaNWwiVkm
05f0: 38 38 7A 74 35 34 4D 64 42 0A 46 6B 62 73 58 57  88zt54MdB.FkbsXW
0600: 4A 70 51 78 59 70 4B 43 78 74 34 58 61 5A 47 42  JpQxYpKCxt4XaZGB
0610: 56 50 35 79 4C 49 6B 72 57 6A 45 6C 57 4D 74 72  VP5yLIkrWjElWMtr
0620: 5A 50 68 33 70 59 52 38 57 4A 51 54 77 6F 73 76  ZPh3pYR8WJQTwosv
0630: 37 34 6E 37 72 6F 42 74 38 30 0A 39 65 6A 54 52  74n7roBt80.9ejTR
0640: 38 47 51 37 34 30 31 42 53 37 66 6F 4D 6A 43 6E  8GQ7401BS7foMjCn
0650: 56 65 76 72 6C 32 55 77 4E 35 53 50 76 74 59 73  Vevrl2UwN5SPvtYs
0660: 4C 4C 45 4D 78 59 47 47 67 53 77 66 7A 39 44 0A  LLEMxYGGgSwfz9D.
0670: 2D 2D 2D 2D 2D 45 4E 44 20 52 53 41 20 50 52 49  -----END RSA PRI
0680: 56 41 54 45 20 4B 45 59 2D 2D 2D 2D 2D 0A 00 00  VATE KEY-----...
```

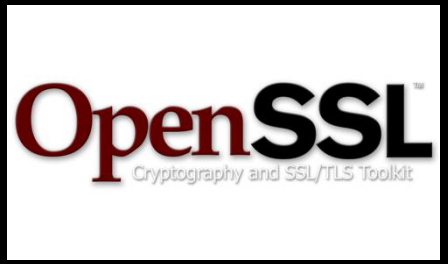

易宝支付有限公司
五年四月二十一日
易宝支付
YEEPAY.COM


亲，来微博
weibo.com
sina 新浪


交易详情
微信支付
转账金额
￥500.00
来 自
vitas


杂志
大礼包

贡献给社区



OpenSSL Software Foundation Inc.

Guangdong, your donation is now complete

PayPal Secure Payments

Confirmation number: 14N03795JN0643335.
An email with your donation details has been sent to baiguangdong@gmail.com and you can print your donation receipt.

YOUR POSTAL ADDRESS
National University of Singapore
13 Computing Drive
Singapore 117417

DONATIONS COORDINATOR CONTACT INFORMATION
OpenSSL Software Foundation Inc.

If you have forgotten your password, please reset it.

PayPal protects your privacy and security.

For more information, read our User Agreement and Privacy Policy.

Copyright © 1999-2015 PayPal. All rights reserved. Consumer advisory- PayPal, Inc., the holder of PayPal's stored value facility, does not require the approval of the Monetary Authority of Singapore. Users are advised to read the terms and conditions carefully.

» 03 全场景的支付安全保护模型

Model Checking

模型检测(model checking)是一种很重要的自动验证技术。主要通过显式状态搜索或隐式不动点计算来验证有穷状态并发系统的模态。由于模型检测可以自动执行,并能在系统不满足性质时提供反例路径，因此在工业界比演绎证明更受推崇。

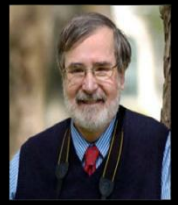
漏洞检测

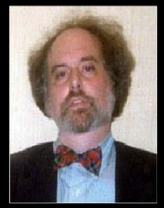
- Keyless System
- 软件设计问题，与设计模式类似
- 软件逻辑错误，比如支付逻辑错误

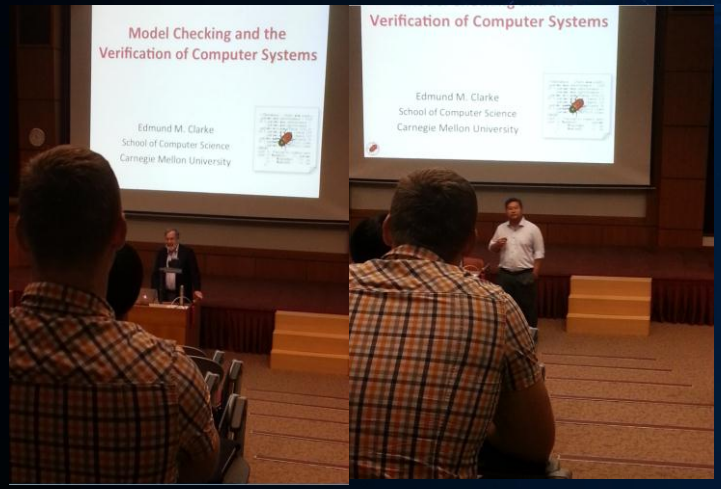
模型检验的成功之处在于它用自动搜索代替手动证明来解决验证的问题。

Edmund Clarke

Three researchers won ACM Turing Award 2007 for their pioneer work on model checking.







Intel i7 processor is verified by symbolic model checking completely without executing a single test case!

防范模型

支付前

1、检查边支付金额界值

2、检查支付数量边界值

3、金额不要直接传输

4、使用订单号的方式传输订单

5、对所有的购买信息进行签名

6、经常更换签名密钥

支付中

支付中的漏洞一般很少出现，因为由银行或者是第三方管理，目前可以利用的有SSL以及根证书欺骗等第三方支付问题。

支付后

1、检测签名是否正确

2、检测订单号是否正确

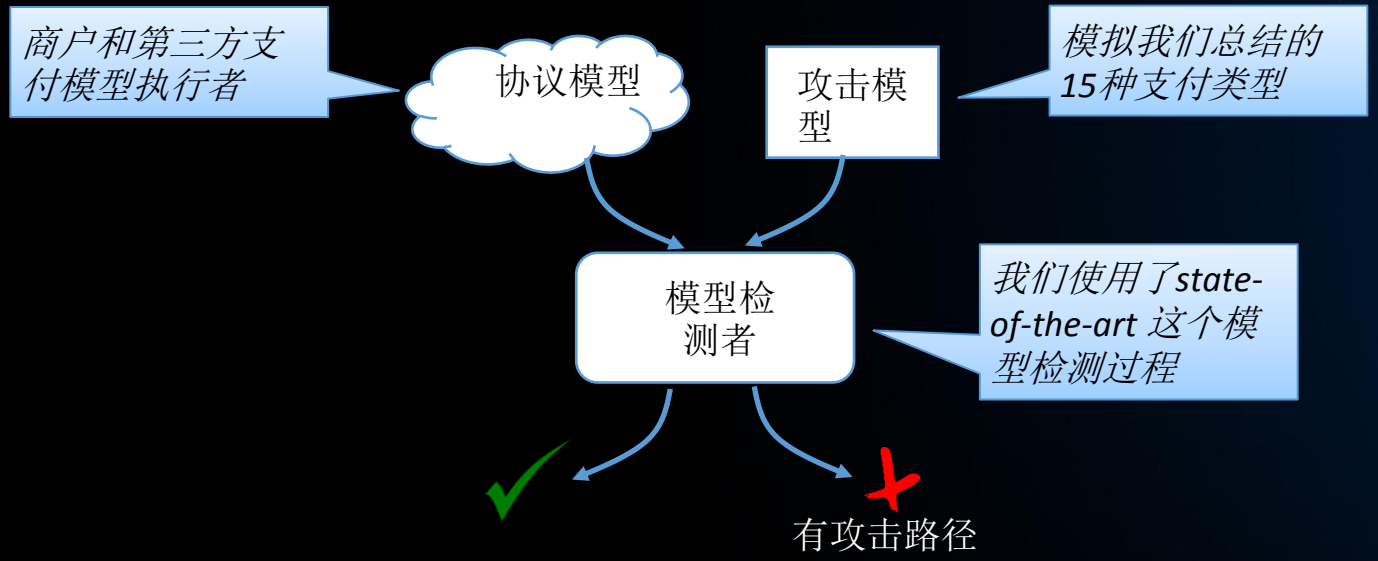
3、检测订单号对应的数量是否正确

4、检测订单号对应的金额是否正确

5、检测订单号对应的产品是否正确

6、检测收款人是否正确

方法概览


商户和第三方支付模型执行者
协议模型
攻击模型
模拟我们总结的15种支付类型
模型检测者
我们使用了state-of-the-art 这个模型检测过程
有攻击路径

Modeling Protocol in CSP#

- 每个协议的参与者(包括商家、第三方支付、以及用户）都被模拟当作一个过程
- 每个参与者都被独立和同时的运行
- 行为被模拟成事件和内联程序

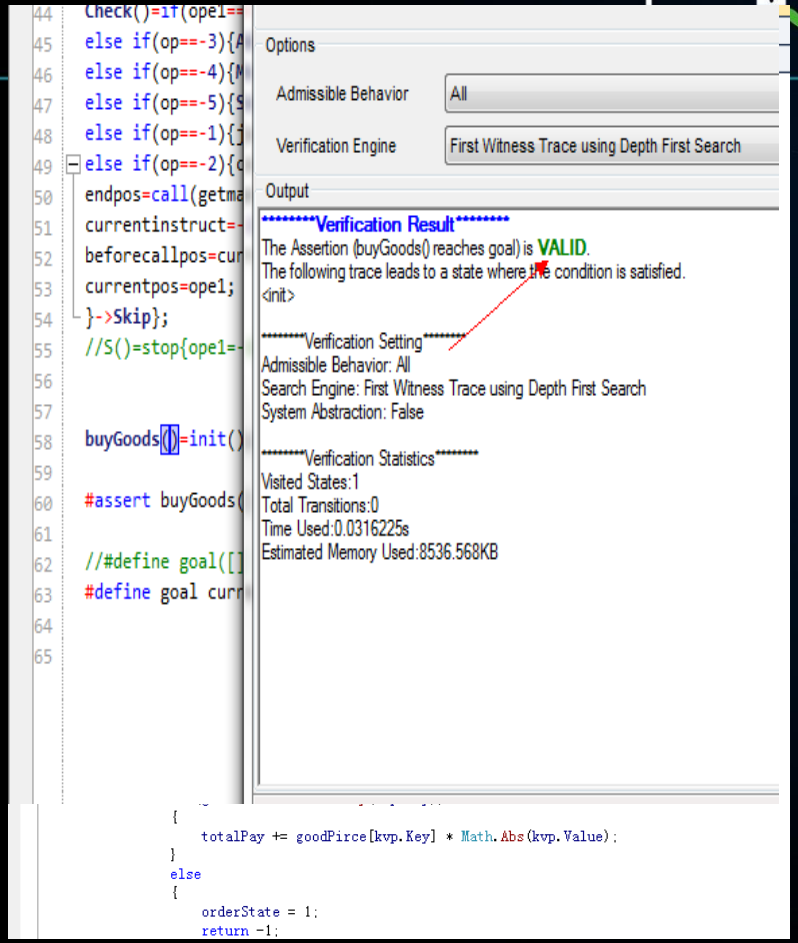
```
P ::= STOP                  (end of a process)

    | P1 ||| P2             (interleaving)
    | P1 |{X}| P2           (synchronization)
    | ch!a | ch?x           (communication
                             channels)
    | e{program} → P
                                 (event)
    | if c then P1 else P2       (conditional
                             branch)
    |P1 [] P2                    (choice)
```

检测模型&安全审计

订单号：
Order/OrderId/Order_id/out_trade_no/tradeNo/*trade*/*order*/payno*/payment_id/paymentId/merc_tranid/*tranid*
价格：
Price/*total_fee*/*amount*/*amt*
数量：
Number/*quantity*
物品ID:
itemId/item_id
用户:
User/usr
通知地址：
Notifyurl/notify_url/return_url/returnurl/show_url/showurl
商户:
Default_partner/*partner*
签名方式
Sign_type/signtype
密钥：
PRIVATE(大写)/private_key/*MD5*/*key*
签名：
Sign*/*verify_sign*/*auth*

Dooland模型

Functions
makeOrder(id, number)
EnsureOrder()
checkOrder()
Pay()
getAllGoods()
getPayType()
getShouldPay()
getPayAct()
Verification



» 04 Thanks & QA

Qing Zhang@360 VulpeckerTeam