信息安全设计与实践

淘世界二手交易平台--商城篇

学院：计算机科学与技术学院

专业：信息安全

班级：11403202

学号：1140320206

姓名：霍峻杰

【摘要】：当今社会，科技的发展使人们的生活变得越来越便捷，随着网络的覆盖与普及，网上的一些交易也赢然而生。网购逐渐成为多数人选择的购物方式，网上商城也如雨后春笋般出现在大众的视野中。人们在方便的使用这些网购平台时，一些不法分子也渐渐的瞄准了网购平台，在网络安全意识普遍低下的情况下，他们通过网站的漏洞，盗取他人虚拟货币等一些违法行为。我们或多或少都听说过0元购等一些手段，但是还是有一些网站的安全机制不是非常的完善。

本次作品，我们通过模拟一个网购平台和一个网上银行的交互行为，来进行安全方面的认证，加密传输等。本次作品，我们的网上商城是网页版的，而网上商城是android端的，交易信息的传递通过android端扫描商城端生成的含有双重签名加密的二维码进行信息的加密传递。二维码方便快捷，可存储大量信息，是当前认证的主流方式。双重签名可以保证信息的加密传输，也能做身份的认证，防止他人生成恶意二维码。

创新性：将双重签名的信息应用于二维码传递信息，通过扫码，将信息从网页商城端安全的传递到手机网上银行端。二维码的信息易于传递，可以通过转发二维码来进行代付等其他操作，我们采用的加密和认证机制也非常的安全，保证了交易的安全性和完整性。

应用前景：电子商务越来越发达，网购平台的安全性需要得到保证，在保证安全的同时，也不能忽略了网上交易的便捷性。我们的项目在保证了信息传递的安全同时，也保留了网购的快捷属性，并且也方便大家进行代付等后续操作，实现了集快捷和安全于一身的较完整的安全加密和认证体系。

【关键词】：二维码，双重签名，RSA，Android，网上商城，网上银行

目录

**1 作品概述1**

1.1 应用背景2

1.1 作品简析2

1.1 作品前景3

**2 系统简介4**

2.1 系统概述5

2.2功能模块6

**3 系统详细设计与实现7**

3.1 开发环境8

3.2 安全网络通信10

3.3 注册和登陆验证13

3.4 用户支付认证14

**4 商城端结果展示16**

**5 关键技术26**

**6 总结27**

1 作品概述

1.1 应用背景

近年来，随着网络的急速发展，网上购物的方便和快捷使其成为了大多数用户的购物方式的选择。而一些网购平台在运营过程中，没有一套良好的安全认证机制和信息保护措施，是得用户的权益受到不同程度的侵害。世界上总是不缺少破坏者，他们利用网购商城的漏洞，对网购商城的商家或某个用户进行违规操作，使其利益受损。

这里简单介绍一些漏洞及利用：

a. 网站本身存在sql注入，攻击者会利用注入点进行对数据库文件的越权读取，严重者可写入webshell，控制整个网站。

b. 零元购，这个大家应该会比较耳熟，所谓的零元购就是通过商城的交易漏洞，在订单处可修改自己的单价为0，这样将免费买到的商品，这个是之前某大网购平台出现的低级漏洞。

c. 负元购，商城没有验证用户填入的商品数量是否为负，导致恶意用户故意填入数量为负的数据，使自己的账户余额不减反增，同时对数据库的库存管理数据进行了数据污染。

以上简单的列举出了一些网购平台的常见漏洞及利用，通过具体的例子，我们发现，网购平台的安全性极其重要，此刻需要一套可靠的信息保护和身份认证机制来保护用户和商城的利益。

另一方面，为什么网购平台能够发展的如此迅速，主要的原因是他的便捷性，而在一些安全机制添加后，网购商城的便捷性受到了伤害，普通平台的其他服务，如他人代取也不是很安全。

针对以上问题，我们模拟了商城和网上银行之间的交互，保证了安全性和快捷性的结合，同时，在商城和银行分别与用户交互（注册，登陆等操作），我们进行了完善，使各处认证的安全达到滴水不漏。

1.2 作品简介

我这边做的是商城的系统，商城的安全认证需要很多方面，下面分几个方面来谈。

a. 用户的注册

这里采用邮箱注册，即用户需要输入正确的邮箱，商城向邮箱中发送验证码，用户通过邮箱中的验证码来完成注册验证，筛选出了一些非活跃用户（即，用户需要有效的邮箱来进行注册）

b. 注册信息的数据库存储

这里采用用户在注册时，会随机生成一段盐，用来进行撞库混淆，用户注册后的密码会与随机盐拼接进行sha256哈希，然后一起存入到数据库中，保证了即使管理员或登录到数据库的恶意用户，无法反解出密码的明文信息。

c. 商城端与后台的信息传输加密

在每一个新的会话（session）的开始，都会通过rsa协商出一个des密钥，deskey的传播加密使用了rsa加密，保证deskey无法被截获后反解。在商量出deskey后，注册信息，登陆信息等重要信息的传递就都使用这个协商好的deskey进行信息的加密和解密。

d. 商城的安全限制

一些基本的安全限制，如当前用户购买商品数量不能为负数，数量不能超过库存等。

e. 访问限制

当用户没有进行登录时，会限制用户的一些访问，比如，没有登录，不允许进入自己的购物车，更不允许提交订单。在用户登陆后，购物车中没有商品时，不允许提交订单，防止恶意ddos攻击，或空订单信息污染订单数据库等问题。

f. 订单支付加密认证

在网上商城与网上银行进行订单支付加密认证的时候，我们采用了对订单信息的双重签名，先用商城私钥对订单信息进行签名，在对签名后的信息用网上银行的公钥进行加密。这样保证了订单信息的加密传输，而且通过商城的签名，网上银行可以对支付方进行身份认证，从而防止了恶意用户的行为。

e. 二维码信息传递

我们的另一特色就是采用二维码传输加密的信息，二维码已经成为了主流的信息传递和身份验证方式，它具有方便快捷安全的优点，这里我们只需要在网上银行端进行扫一扫，就可以获取到商城发来的订单信息。同时，用户的付款行为由被动变为主动，大大提高了支付的安全性。

g. 完善的后台管理

一个好的商城系统不可缺少完善的后台管理系统，我的后台管理分三个部分:

(1) 用户管理：

管理员可以查看用户的一些基本的信息，除删除操作权限（用来清理长期不活跃用户或恶意用户），外其他操作的权限不赋给管理员，如修改用户信息。

(2) 商品管理：

管理员可以对商品进行相应的操作，更改库存，单价，添加，删除商品等，不具有其他权限。

(3) 订单信息管理：

管理员仅能查看和删除订单信息，不能拥有其他权限。

1.3 作品前景

当今的电子商务的发展非常的迅猛，网购平台也是百花齐放，在这个信息流通十分广大的时代，信息的传递重要性不可而喻，尤其是当信息涉及到交易信息时，需要格外的保护。我们做的这一套购物支付系统有很好的安全性，便捷性和可移植性，任何需要的企业，公司都可以使用这套安全认证和加密传输机制，使网购平台的安全性大大提高，让人们都能安全方便的在网上进行购物而不会有任何的风险。

2 系统简介

2.1 系统概述

2.1.1 应用示意图



Fig1: 应用示意图

应用主要分为三个主体

1. 用户

2. 商城

3. 管理员

应用流程介绍：

1. 用户通过在商城页面进行注册和登陆，从而获得购买商品的权利。用户在登录认证通过后，开始浏览商品，并将需要购买的商品加入自己的独享的购物车中。

2. 当用户选择完毕后，进入到自己的购物车，进行订单提交

3. 提交订单后，点击生成二维码，生成自己的支付二维码支付

4. 用户打开网上银行进行扫一扫操作，在银行端完成支付后，商城端获得支付完成（成功或失败）信息，若成功，则将订单信息写入到数据库。

5. 商城的后台管理员可以查看和删除用户的信息，还可以对商城的订单信息进行查看和删除。

6. 商品的库存管理者可以通过购置货物，增加库存，修改商品单价等操作修改数据库中商品的信息。

2.1.2 功能模块图



Fig2：功能模块图

2.2 功能模块

I会员管理

1. 主要功能：

1) 会员注册：完成用户身份信息的输入、记录。包括注册者用户名，密码，手机号绑定。注册方式也可以是手机验证码注册。

2）会员账户管理：管理员通过后台管理系统对用户的信息进行管理（审核，删除长期不活跃用户等）。同时，管理员操作的会员密码也是对管理员保密的（保存的是hash值）。

3) 修改信息：用户修改注册账号的密码，须通过手机验证的方式来进行密码的修改，如支持昵称等功能，可以支持修改昵称等信息。

2. 与其他模块的关系：

会员管理涉及到销售管理的订单方面，注册的会员每次交易成功的订单都会有相应的记录。

会员管理还涉及认证管理，需要通过后台对登录用户的身份进行认证，才可以登陆，再进行后续操作。

会员登录还涉及到通讯管理的数据库加密部分，用户的一些敏感信息必须加密后（或散列）存储，保证管理员也很难获取或被撞库后，也很难解出密码。

II库存管理

1. 主要功能

1) 二手商品入库：商城二手商品购进，增加库存数量

2) 二手商品出库：顾客提交订单后，商场发出商品后，将对应商品的库存数量减少，并反映到库存显示上。

2. 与其他模块的关系：

库存管理与销售管理的购物车模块有关，库存剩余量需要在用户购买商品时进行显示，如果库存为0则不能将商品加入到购物车。

III销售管理

1. 主要功能：

1) 搜索二手商品：通过搜索框对想要的商品进行关键词搜索，商品的排序可根据用户的需求自定义（按销量，按库存量）

2) 购物车操作：将物品添加至购物车，进入购物车，对商品进行批量删除，或直接清空购物车。可以在购物车中点击商品来查看商品的详细信息。

3) 订单生成：包括订单号，购买者，购买者手机号（尾号），收货地址，商品，商品价钱，快递公司，运费，总金额，订单支付时间。

4) 打印订单：将生成的订单按顾客需求打印

2. 与其他模块的关系：

销售模块与库存管理模块的关系体现在销售的商品数量要相应在库存中减去。

销售模块会调用认证模块的支付认证，在购物车中会提供支付功能，通过网上银行方面的身份和支付认证，完成交易的付款。

支付认证时涉及信息传输加密，这里采用R[商城私钥](R[银行公钥](信息))来进行认证后加密传输。

IV认证管理

1. 主要功能：

1) 会员登录：会员登录操作时，需要在后台服务器运行认证校验，若数据库查询失败，则提示顾客先行注册操作。

2) 交易认证：将加密信息生成指定的二维码，需要网上银行扫码操作来进行信息的传输，支付细节在网上银行介绍。

2. 与其他模块的关系：

认证管理需要对会员登录进行认证。

认证管理与信息传输加密密不可分，对一些敏感信息进行加密后传输， 保证传输信息（支付信息）的安全。

V通讯加密

1. 主要功能：

1) 信息传输：信息在网络上的传输都需要进行加密传输，禁止明文传输，这里区分用户登录信息的信息加密传输和支付信息的加密传输方式。两者的信息发送接收端不同，所以采用不同的信息加密。

2) 数据库加密：用户的基本信息，订单信息都需要存储在数据库中，一些次要的信息可以进行明文存储，但是敏感信息（如 密码，支付唯一标识码等）需要进行相应的加密处理。使信息即使被泄露，破解还原也非常的困难，使撞库损失降到最低。

2. 与其他模块的关系：

通讯加密模块和会员管理模块的会员登录有关，用户上传的登录信息需要被加密进行传输。

通讯加密模块还与支付模块紧密相关，支付信息需要很强的加密手段，防止中间人攻击，破解攻击，重放攻击等攻击，保证信息安全的到达，且不被成功窃取信息。

3 系统详细设计与实现

3.1 开发环境

开发环境： Microsoft Windows 8.1

开发工具： MyEclipse

Java 1.8

Tomcat

Mysql 5.16

测试工具： Windows主机本地测试

3.2 安全网络通信

3.2.1 设计

商城前端和服务器间的信息传输使用des加密（des密钥的传输使用rsa进行加密传输协商）。

商城和网上银行支付时使用双重签名，保证信息的加密传输和身份认证的双重保护。

数据库将敏感信息进行哈希存储，防止他人进行恶意读取

限制管理员的一些操作权限，防止管理员有意或无意的对数据库信息造成不可弥补的损失。

3.2.2 实现

可参照下面的具体实现。

3.3 注册和登陆验证

3.3.1 具体流程



Fig3：注册登录流程图

3.3.2 注册

1）用户填写相应的信息，在填入邮箱后，点击发送邮箱验证码

2）用户将收到的验证码填入注册信息中

3）用户提交信息，经过前端des加密传输到后台进行验证

4）验证成功则注册成功，可进行后续登陆操作，否则返回注册，这里设置了验证码有效时间，若超过一定时间，验证码即失效。

5）后台验证成功后，将用户的信息写入到数据库，其中密码信息通过与一段随机的盐拼接在一起，进行sha256哈希后，存入数据库。

3.3.3 登陆

1）用户提交登录信息

2）前端des加密后传送到后台

3）后台des解密，查找数据库，将用户提交密码与用户所拥有的盐拼接进行sha256哈希

4）与数据库中的用户密码哈希值进行对比，若一致，则登陆成功，将用户登录信息存入session

5）若用户处于未登录状态，则有些界面不能让用户进入，如用户的购物车等敏感界面，这些界面不会对游客开放。

3.4 用户的支付认证

3.4.1 支付认证流程图



Fig4：支付认证流程图

3.4.2 支付认证流程

1）用户选择好购物车中的商品时，点击提交订单

2）服务器对提交的信息进行双重签名

① 用商城的私钥进行RSA签名

② 用网上银行的公钥对签名后的信息进行RSA加密

3）将双重签名后的信息生成一个支付二维码

4）用户扫描二维码，在网上银行Android端进行支付

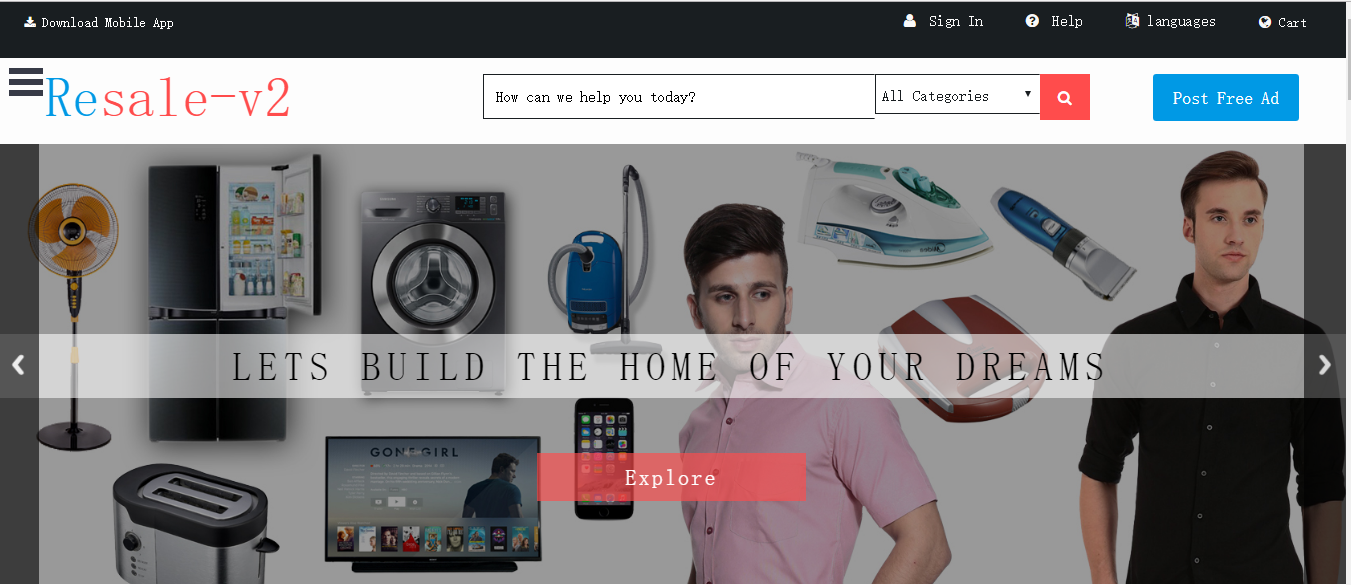
5）返回支付成功或失败信息

6）网购商城端进行提示验证和订单信息写入数据库操作

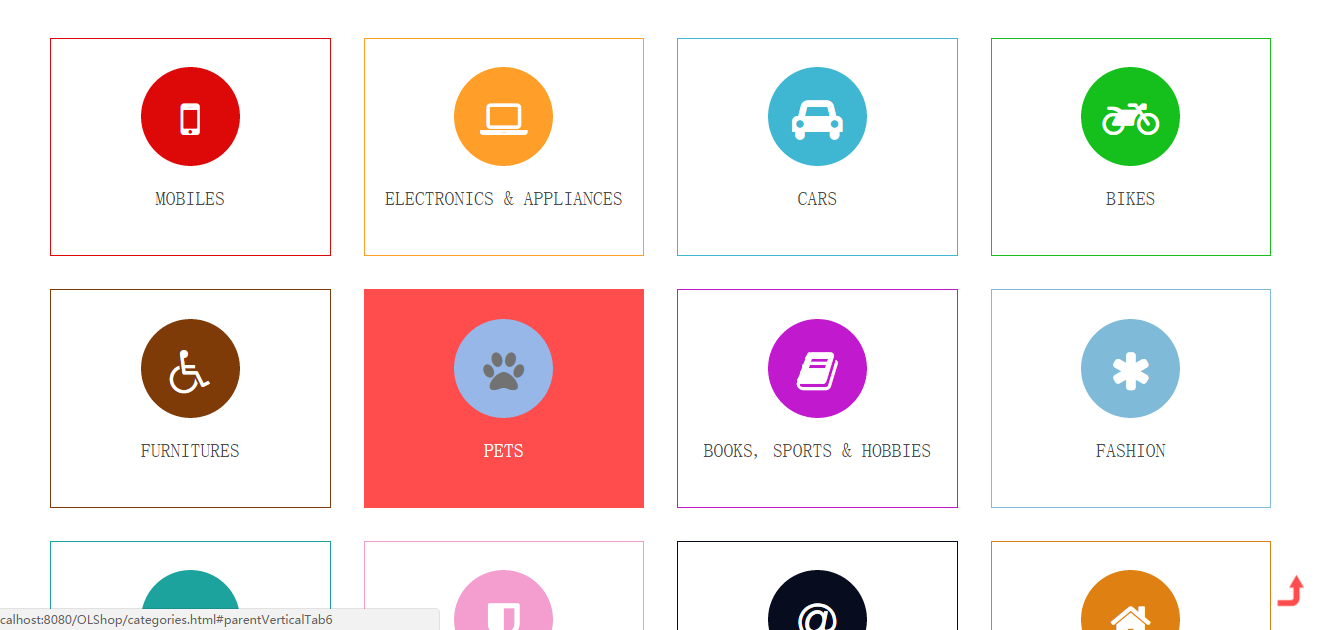
4 商城端成果展示

4.1 商城页面总览

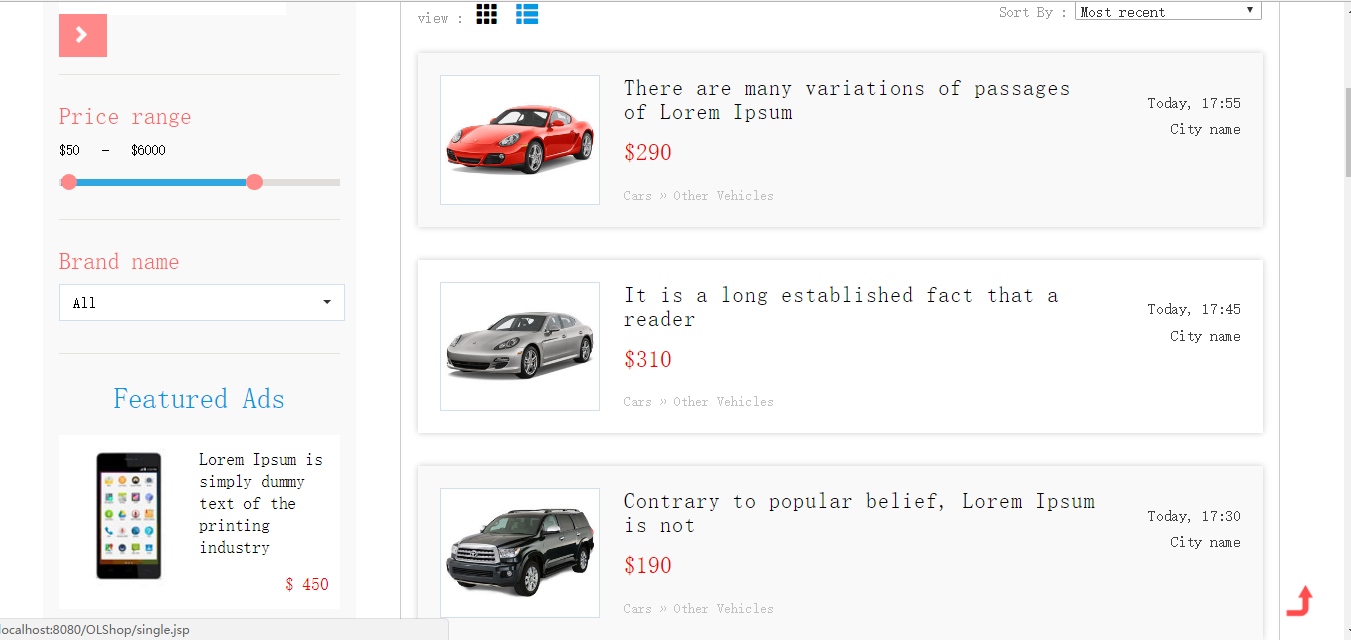
4.1.1 初始欢迎界面



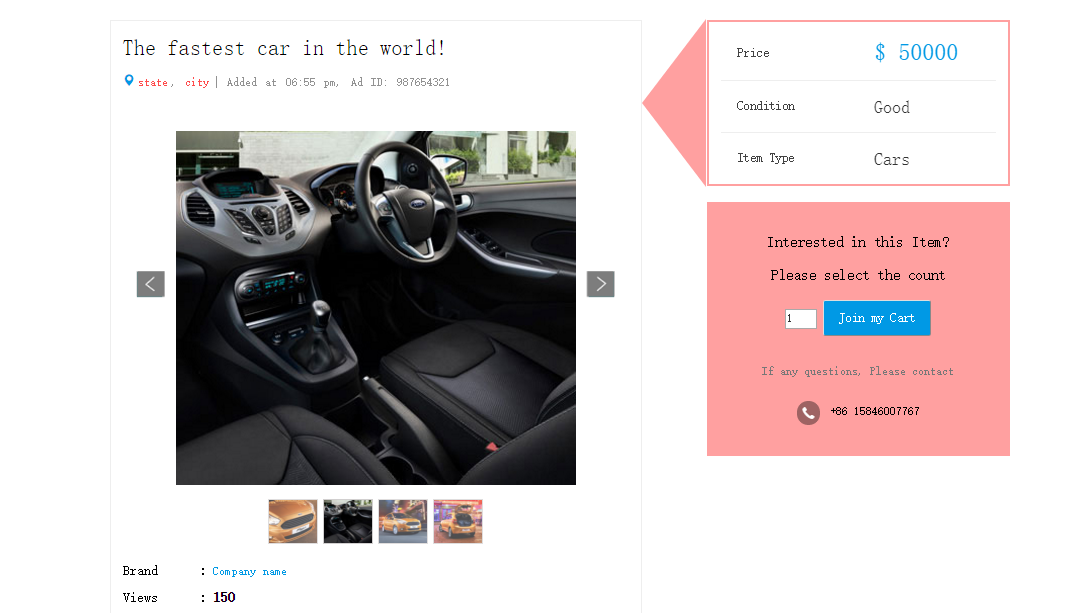
4.1.2 购物分类



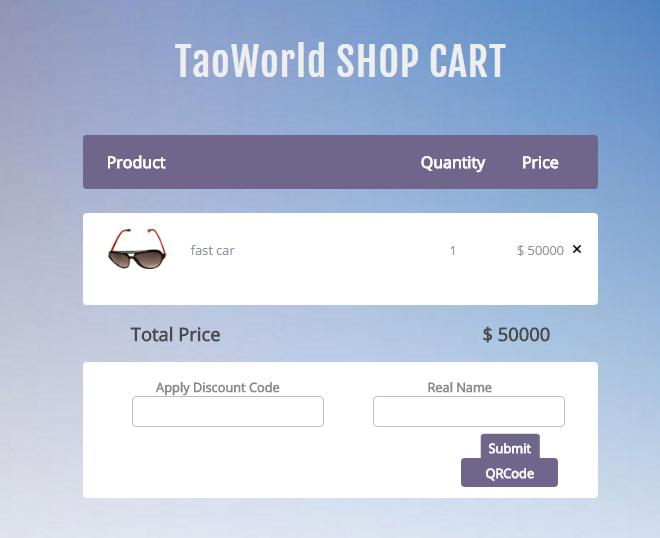
4.1.3 购物列表



4.1.4 购物界面



4.1.5 购物车



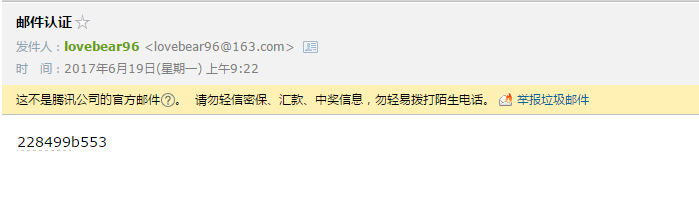
4.2 注册与登陆

4.2.1 注册

1）填写信息，获取邮件验证码



2）收到邮件验证码



3）填写验证码完成注册

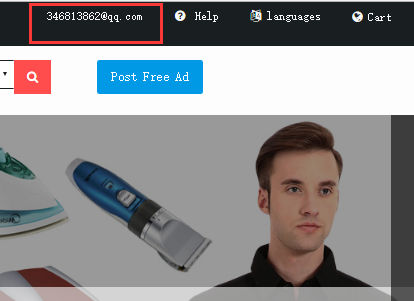
注册成功会跳转到登录页面

4.2.2 登陆

1）输入注册信息登陆

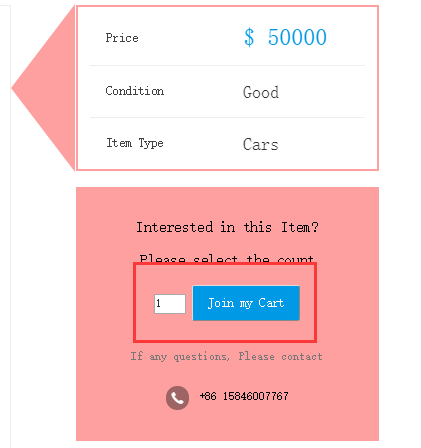


2）登陆成功后，signin按钮变为用户的邮箱信息

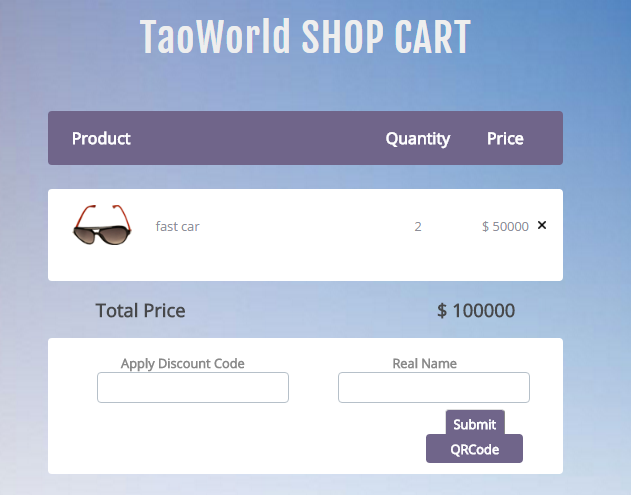


4.3 购买商品

1）选择商品，加入购物车，可以选择购买数量

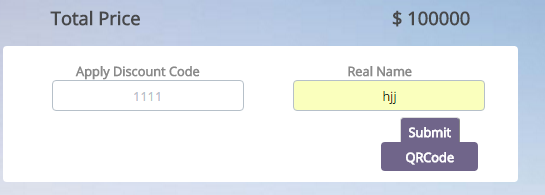


2）购买完成后，查看购物车



4.4 提交订单

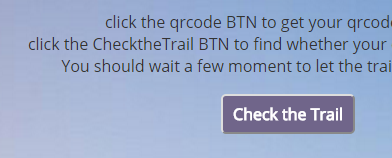
1）输入用户的ID卡号和真实姓名用于银行端验证



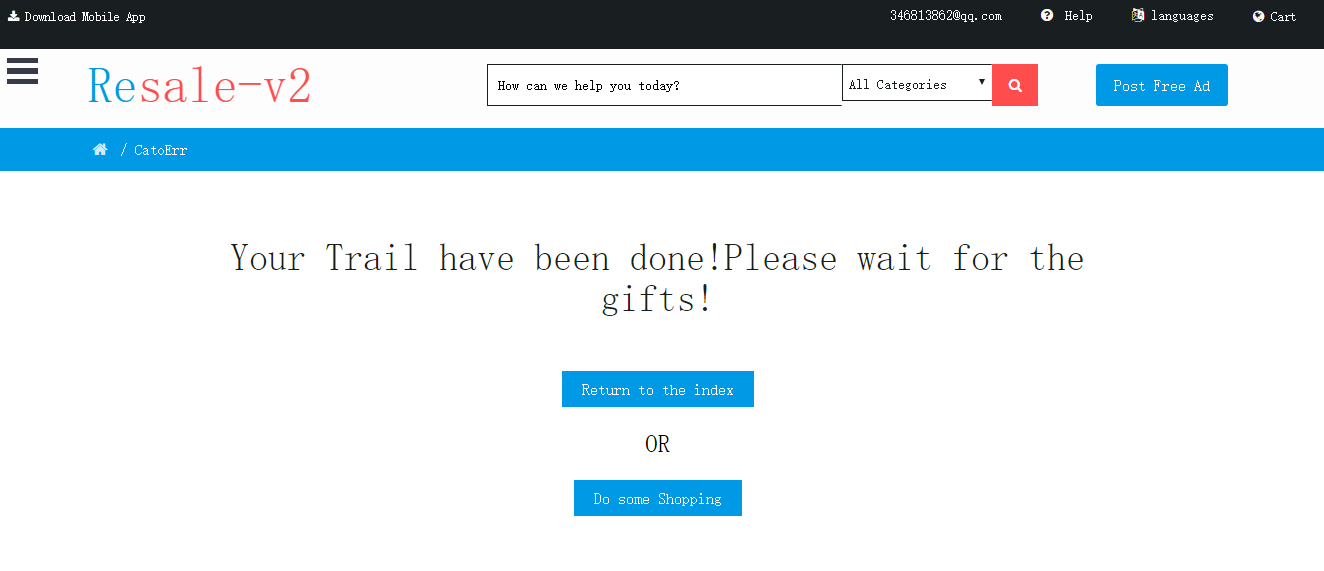
2）提交订单后，查看生成的二维码



3）查看交易是否完成



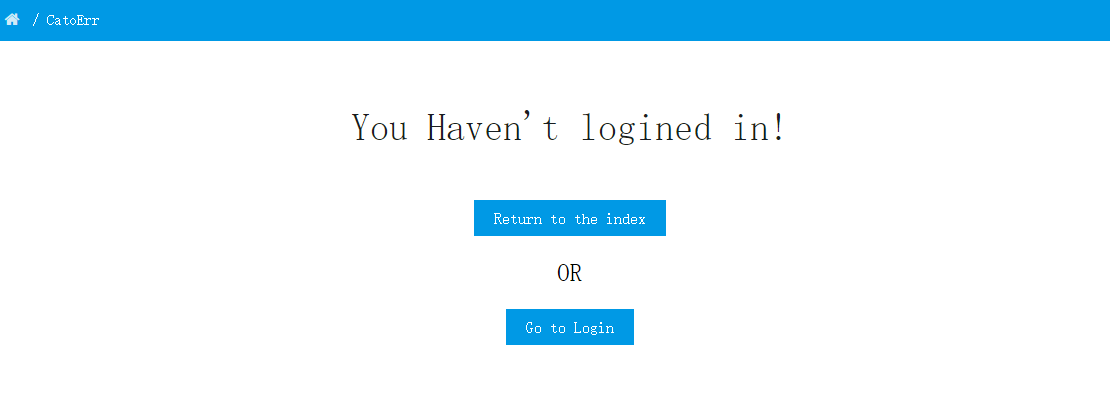
4）查看结果



4.5 错误情况页面

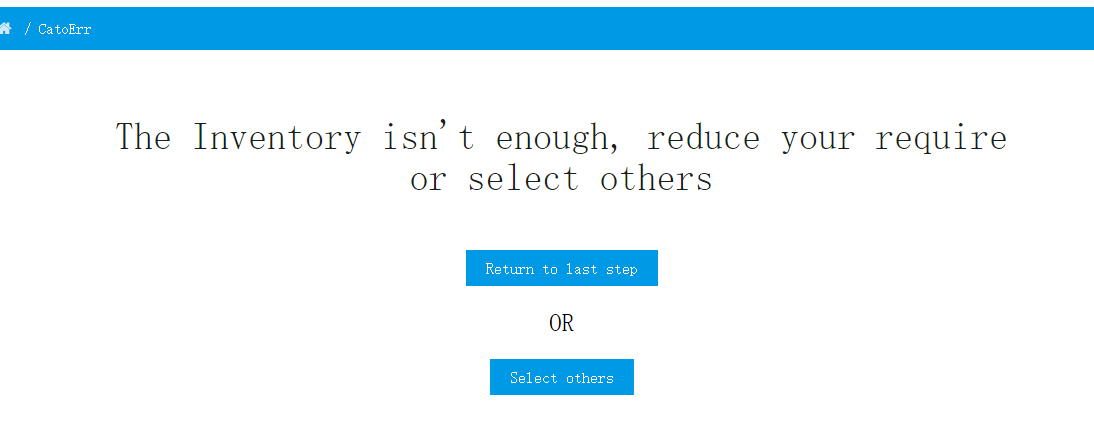
4.5.1 用户未登录

若用户未登录，后续操作将被阻止（购物，进入购物车等），弹出返回主页或跳转到登录界面两个选项

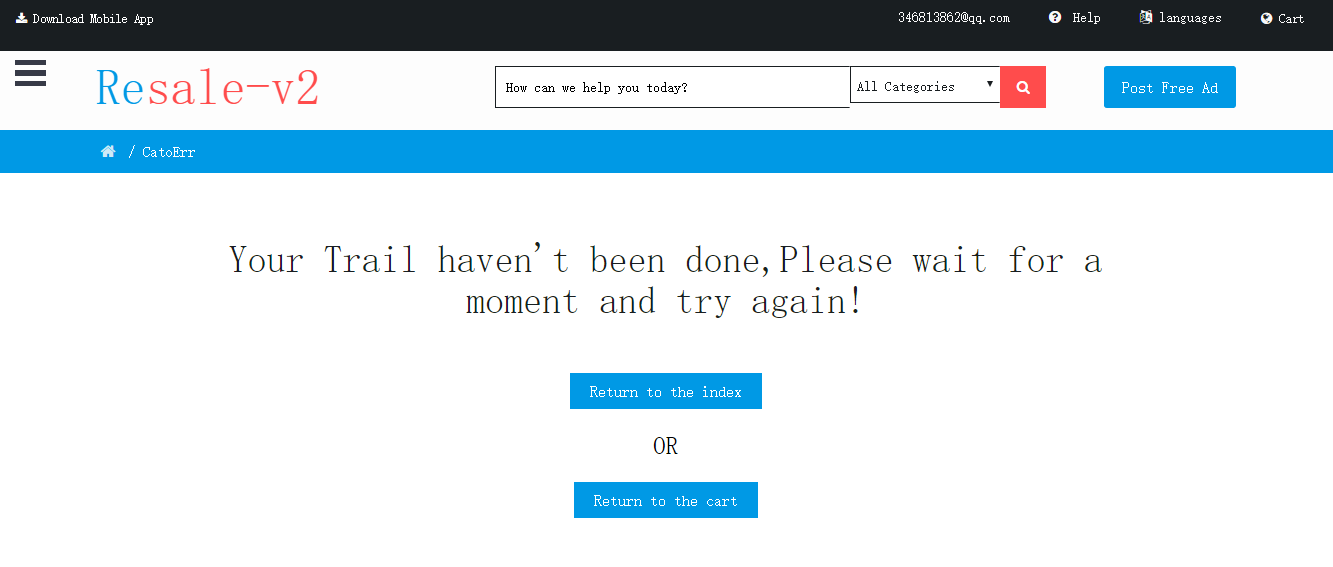


4.5.2 用户购买数量超过库存

返回提示库存不够

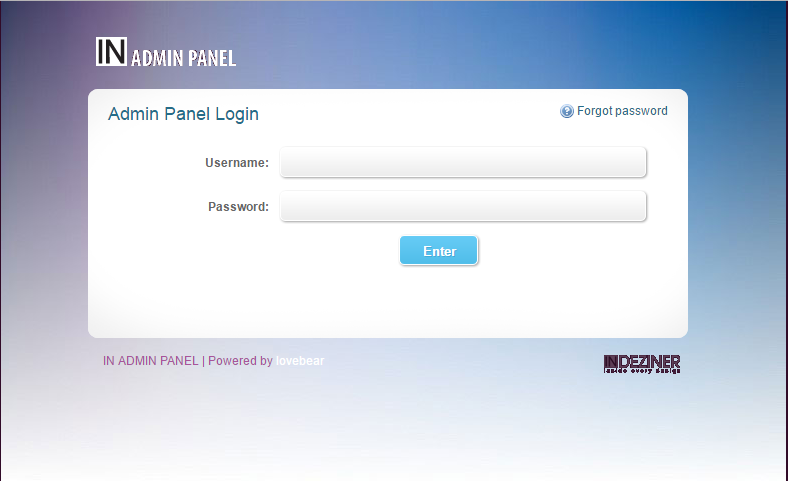


4.5.3 用户交易未成功

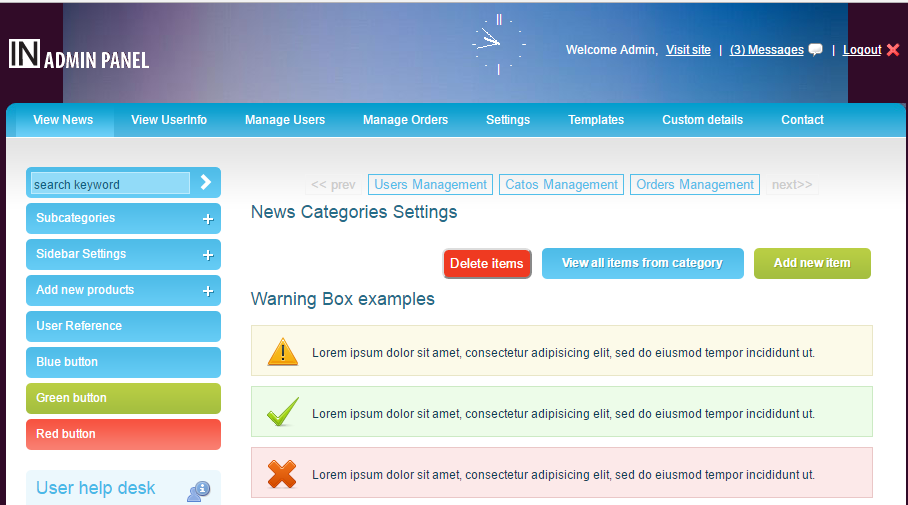


4.6 管理员后台

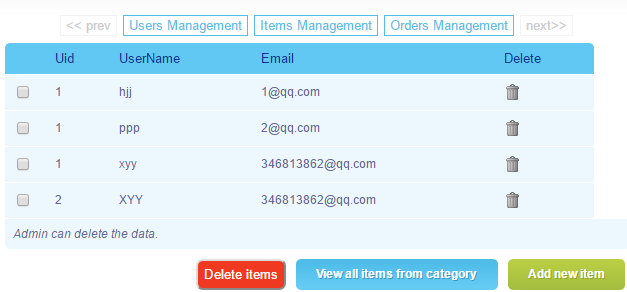
4.6.1 登录界面



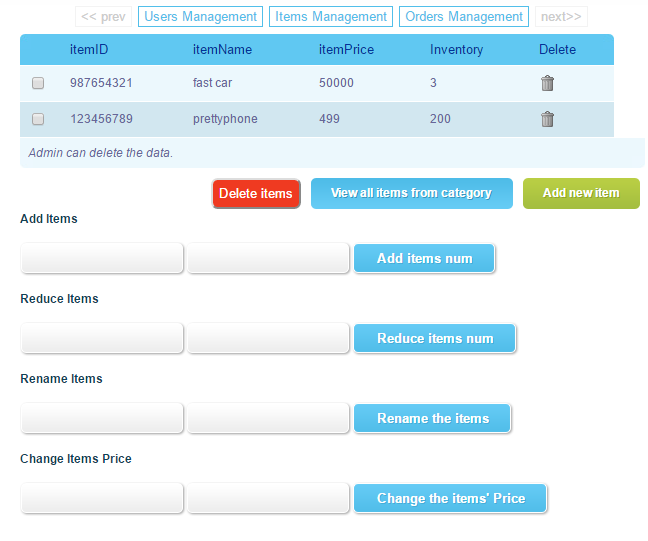
4.6.2 登陆成功



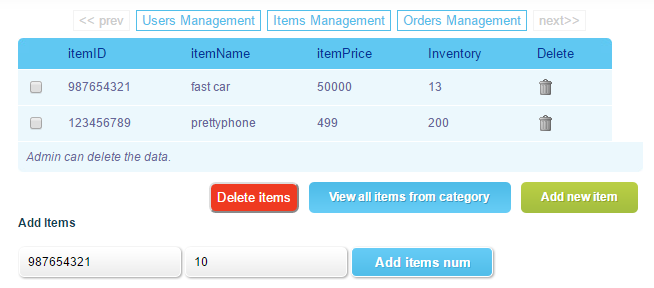
4.6.3 注册用户



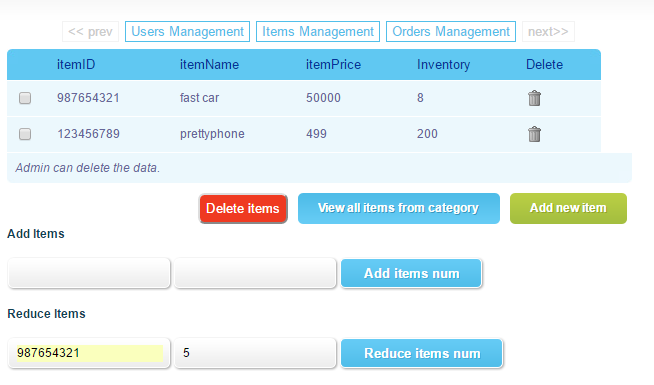
4.6.4 商品信息及操作



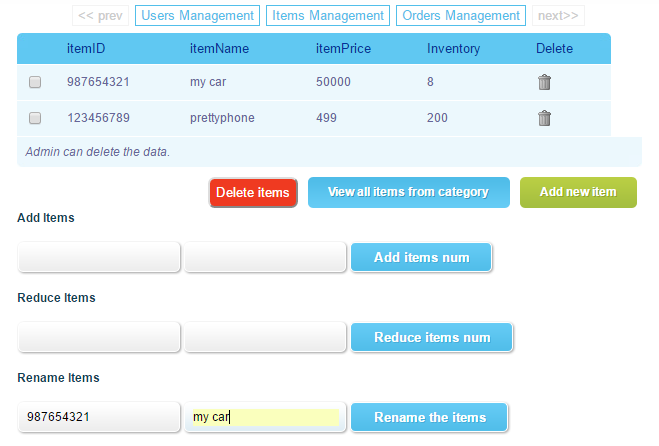
1）增加库存



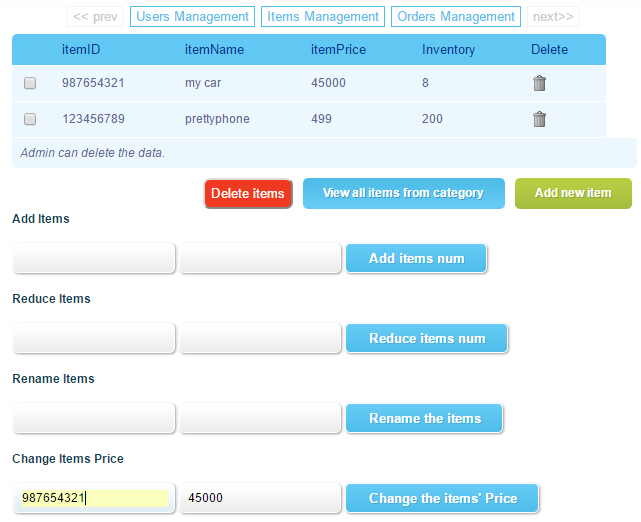
2）减少库存



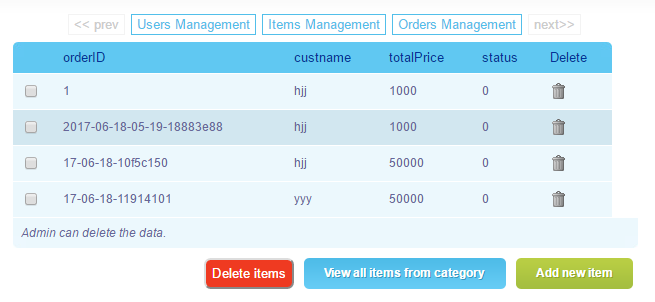
3）更改商品名字



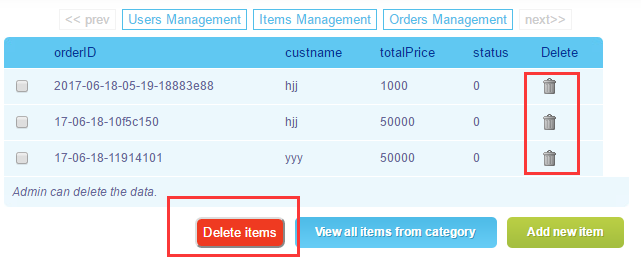
4）改商品价格



4.6.5 写入订单信息



4.6.6 删除信息



可多选进行批量删除。

5 关键技术

5.1 认证技术

1. 用户登录时，采用的是后台信息对比认证，即，后台用户名密码一致，即为登陆成功。

2. 支付信息传送时，采用数字证书的方式，使网上银行明确待支付用户的身份为商城，而不是某个伪造的信息

3. 通过二维码进行消息的传输和认证，网上银行在后台认证支付者信息，来确保是支付者提交的支付信息。

5.2 加密技术

1. 用户登录时，首先将用户的信息采用des加密，将加密的信息传 输。保证在网络上，敏感信息不会明文传输。

2. 用户支付时，需保证生成二维码中的信息也不是明文，将明文的 订单信息先用商城的私钥进行签名，达到认证身份的作用，再将 签名后的信息进行网上银行共钥加密，保证传输的信息加密。

5.3 注册信息保护

1. 密码等信息传到服务器后，服务器rsa解密得到密码，随机生成 一个“盐”，密码加盐处理后进行SHA-256散列，得到的散列值与 “盐”一起保存在数据库中。这样，即使拿到用户的密码表项（撞 库，或社工），破解起来也是相当的困难。

2. 在一些用户的搜索等提交表单的地方，进行用户输入的严格过 滤，防止恶意用户的sql注入和xss攻击。

3. 数据库权限配置合理，分配给数据库能正常工作的最小权限，包 括管理员权限也是这样。

6 总结

当今社会网路越来越发达，网购也在我们身边渐渐普及开来，逐渐成为一种新型的主流购物方式。随之而来的是网购安全方面的大量需求，我们抓住了这个重点，结合了网购本身带来的优点（如便捷性等），使加密认证方式变得既安全又便捷。

在商城方面，我们考虑了各种可能出现的安全认证问题，防止了普通用户的越权访问一些敏感内容。

注册时，我们采用了邮箱认证，可以大大降低低价值用户的注册，也可以有效地防止在注册端的ddos攻击（需要大量有效邮箱）

登陆时，验证的是数据库中的哈希值，这样，即使管理员也不能看见用户的密码。

购物时，对零元购，负元购等漏洞进行了修补

整个网站的sql不存在sql注入，防护sql注入做到极致，网站前端与服务器交互信息的时候，使用了session刚开始用RSA协商的deskey，做到了一次交换，多次使用的简便安全策略。

提交订单是通过双重签名将订单信息加密（商城私钥签名，银行公钥加密）。生成一个含有加密信息的二维码。二维码可以存储大量的加密信息，并且在认证时，有安全便捷的效果。

银行端交易完成后，将返回给商城交易状态信息，商城判断交易是否成功就可以将订单信息写入持久化数据库。

我们的这一套系统是一套相对比较完善的安全加密认证思路，通过简单的二维码，将网页端与手机端连接通信，达到方便快捷又不失安全的效果。在未来的网购平台安全中，我们的思路可能会更加开阔，将这个思路变得更加的完善，积极为互联网安全贡献出自己的能量。