淘世界交易平台—商城
开发计划书

班级：　11403202

学号：　1140320206

姓名：　霍峻杰

时间：　2017.3.1

1. 题目：淘世界交易平台—商城 开发计划书

2. 意义

网站实现会员注册机制，注册的会员可以在淘世界交易平台上购买自己喜欢的二手商品。当今社会商品种类激增，人们生活水平上升的同时也导致了资源的浪费。一些新型商品的价格比较贵，价位在一些人不能承受的范围内，而二手交易市场的出现，不仅使资源分配更加和谐，也使资源得到了重用，增加了商品的价值。二手交易市场已经逐渐兴起，市场上逐渐出现了一些二手交易平台，如瓜子二手车直卖网。淘世界二手交易平台集众家之所长，汇集了各类商品的二手商品，认证支付手段也十分新颖方便快捷，拥有其他平台没有的众多优势。

3. 需求分析：

基本原则：会员制、订单制、购物车机制、加密信息原则，快捷支付原则，防抵赖机制

我们根据上述原则及网络商品支付的基本信息流程总结出一些基本的商城功能，包括如下：

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) 会员管理：管理员后台管理用户信息，其中重要的信息（密码等重要信息需要加密存储，管理员也不能获取）
3) 登录认证：用户的注册信息会在数据库中存储，注册信息中的敏感信息（如密码）需要 RSA 加密后传输。在服务端解密后，密码经过加盐处理后经过 SHA-256 加密散列后存储（散列值+盐）。即使公司内部人员获取到 RSA 私钥，也无法解析密码。登录认证时，进行的是服务器端认证，获取登陆用户输入的密码，加盐后 SHA-256 后与数据库中密码验证。网络中不传输密码明文，而传输的是 RSA 加密的数据。
4) 商品展示：分类展示（生活用品，运动器材等），数据存储在数据库中点击显示商品的详细信息。
5) 商品搜索：搜索商品，字符串过滤，防止 sql 注入
6) 库存显示：提示顾客二手商品的剩余库存量
7) 加入购物车：顾客输入数字进行限制（0 < n <= 库存）,可进入查看购物车界面，删除购物车中样品（支持选中批量删除功能）
8) 支付认证（有精力的话会支持选择多种支付方式）：
   将订单支付唯一标识号（每次进行交易都会根据交易时间，交易方式等信息生成一个唯一的交易标识号，防止网上银行抵赖），商户的银行卡号,用户真实姓名以及一个发送信息的当前时间戳生成 json 格式后，用网上银行的公钥加密数据，再将加密结果用商城的私钥进行加密，得到的加密字符串以二维码形式展示。需要用网上银行的扫一扫功能，数据传输后在网上银行数字签名认证和私钥解密，用户输

入支付密码进行支付（这段是网上银行细节信息，详见网上银行篇）。根据返回信息（成功或失败信息的 json 形式）进行相应页面的跳转。解密出来的时间戳用于进行支付时间验证，与当前时间对比，两者之差超过 5min，验证信息失效，返回支付失败界面。

9) 交易信息记录：

将交易的信息交易时间，订单号，订单信息等）记录在相应的数据库中（年终对账记录以及防止顾客抵赖），还可以根据顾客需求打印相关的信息发票

10) 防中间人攻击：采用开启 ssl，用 https 协议进行传输，防止中间人攻击。

性能需求：

1） 同时满足 1000 人交易操作。

2） 登录及身份认证操作需要在 10 秒钟内完成

4. 概要设计：

4.1 硬件环境

一个真实物理 IP 地址，真实域名 www.taoshijie.top。网络带宽不低于 100Mbps。内存 16G，硬盘 750G，双 CPU 高性能服务器。

4.2 开发环境

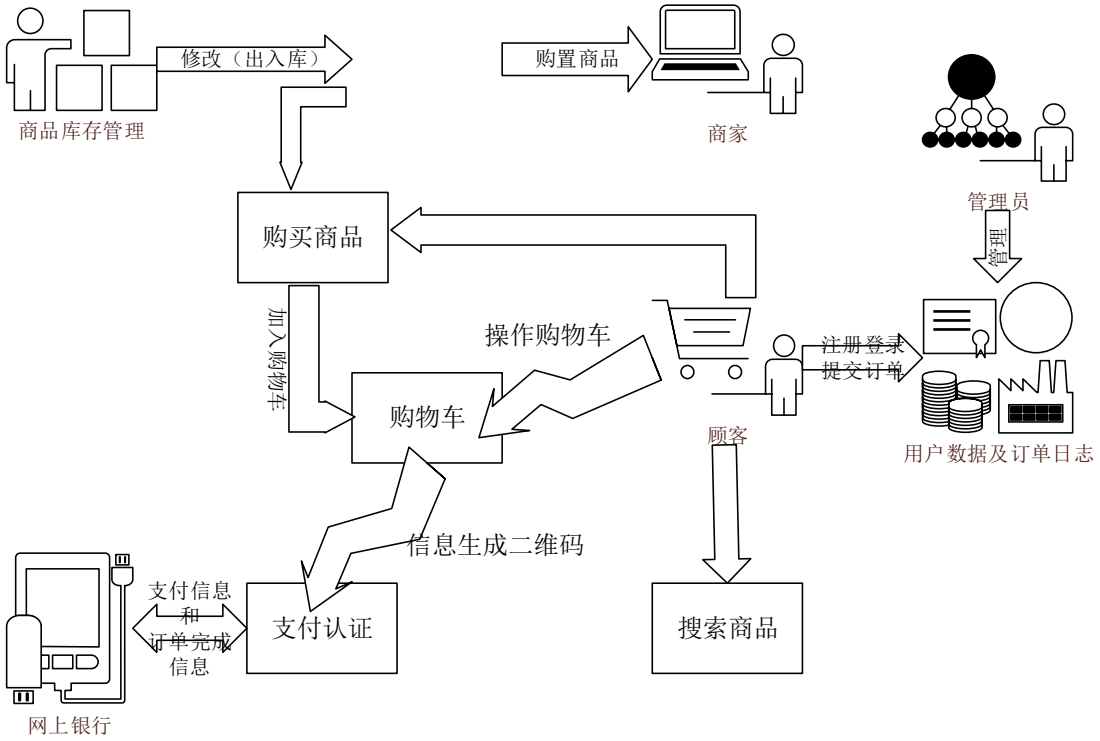
操作系统：Linux
数据库：Mysql
Web 服务器：Tomcat
程序设计语言：java、javascript、jquery

4.3 用户环境：

操作系统：windows xp 及以上
客户端：IE、Firefox、chrome

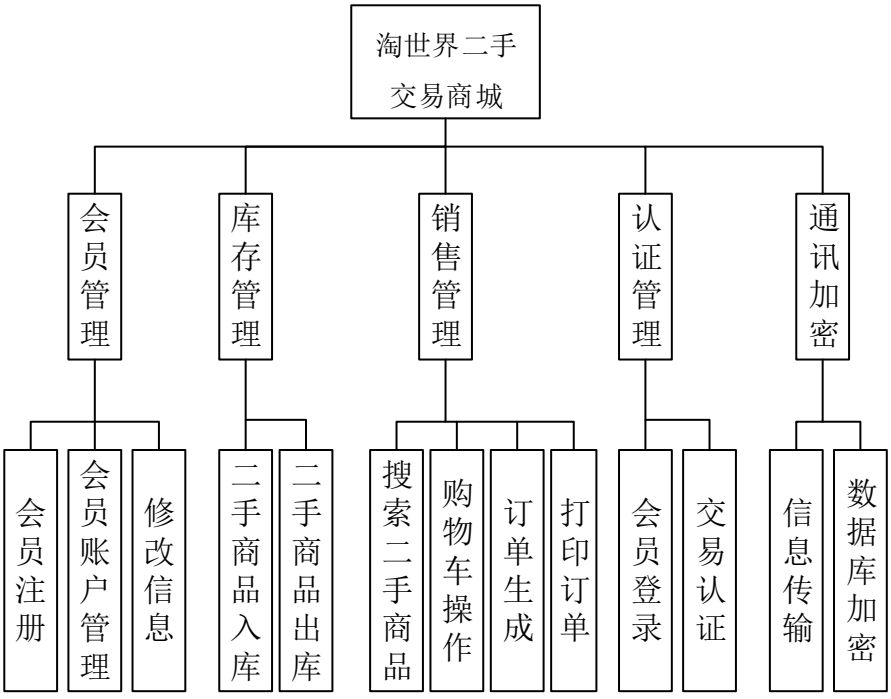
4.4 业务数据流

根据需求进行业务逻辑分析，得到下列业务数据流图：



4.5 功能模块划分

根据业务处理逻辑进性功能模块划分如下：



4.6 功能模块定义

4.6.1 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。

4.6.2 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。

4.6.3 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。

4.6.4 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。

4.6.5 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。

4.7 数据库设计

4.7.1 管理员帐户

表名 ts_admin

表项	类型	说明
admin_user	String	管理员用户名
admin_pwd	String	管理员密码
admin_id	int	管理员 id
last_log	String	最后登录时间

4.7.2 会员信息表

表名：ts_member

表项	类型	说明
userid	Int	会员唯一 id
username	String	用户名
pwd	String	密码
phone_num	String	手机号
real_name	String	真实姓名
gender(Optional)	Char	性别
nickname(Optional)	String	昵称

4.7.3 订单日志表

表名：ts_log

表项	类型	说明
userid	int	用户 id
phone_num	String	手机号
date	String	订单日期

log_message	String	订单信息
code	int	订单成功提交与否

4.7.4 商品库存表

表名：ts_store

表项	类型	说明
mer_id	Int	商品唯一 id
count	Int	剩余库存
mer_name	String	商品名称
sale	Float	价格

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 rsa 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，且只有网上银行可以解出，所以在信息经过数字证书加密前，需要将数据进行一次共要加密，保证传输过程中的信息保密性。
3. 思考了如何防止中间人技术时，发现一些学到的方法不能防中间人攻击。而有效地防止中间人攻击（篡改，重放等）需要经过多次握手的协议，于是我们就不把精力放在这里了，直接采用基于 ssl 的 https 协议来防中间人攻击。所以这个算是利用的 ssl 的加密认证。

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。

5.4 网站 CDN 技术接入

开通 CDN 服务，隐藏服务器 ip 的同时，使服务器压力缓解，达到万人，甚至十万人使用流畅。

6. 任务进度表

第 8~9 周：
第 10 周：