# 系统安全和权限设计

## 6.1、安全性

### 6.1.1、Android端

在用户账户安全方面，统一采用MD5对用户密码进行加密。另外将数据存储在内部存储目录（MODE\_PRIVATE模式）或采用MD5加密对在外部储存的数据进行加密。

在接口请求方面，会设计一个请求响应拦截，根据不同的情况返回响应的http状态码，例如401状态码，表示用户必须先登录授权认证后才可以访问。

### 6.1.2、网页端

在用户账户安全方面，统一采用MD5对用户密码进行加密。采用token（不储存于浏览器）认证，有效防御CSRF跨站请求伪造。

在接口请求方面，同样会做一次拦截，一是避免sql注入，脚本攻击等，二是权限管理。

### 6.1.3、后端

采用JWT认证机制，对于前端传过来的token，首先要判断token是否合法，再来判断是否过期，这些信息都会通知用户。通过token凭证返回指定的状态码。采用云服务提供商DDoS的防御方案抵御可能来自客户端的非法大量请求。

## 6.2、健壮性

对网络请求、IO等操作进行异常捕获，并通过返回的异常信息进行无歧义的提示和有效响应。做好健壮性测试，异常测试覆盖软件健壮性设计时考虑的异常情况。

对于接口api的设计，考虑到健壮性和兼容性，当我们产品升级，添加新功能时，不应该直接在原api上进行修改，应该要考虑到旧版本。我们产品打算维护最多三个版本的api，比如有v1，v2，v3这三个版本

我们会设计一套异常处理机制，捕获开发和生产时的异常，并返回详细的信息。开发时，比如传参错误等等，生产时，比如用户登录失败，这时可以捕获到异常，并返回给用户，告知信息。

## 6.3、权限设计

网页端包括两种用户角色——超市管理员和店铺管理员，超市管理员负责订单管理和分拣，店铺管理员负责菜谱管理。