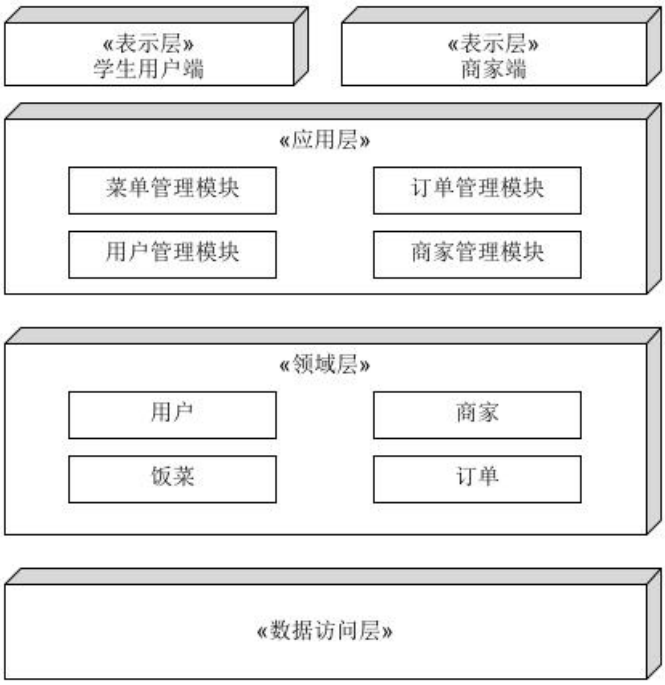
三饭订餐系统安全报告

1. 引言

本报告旨在评估我们小组开发的三饭网上订餐系统的安全性，进行风险评估，并提供相关的防护措施。

2. 系统概述

如下图所示，系统采用分层架构。



我们认为，系统可能存在的风险主要来自三个地方：

- 网络攻击者从表示层进行攻击
- 应用层内部管理不当，存在内部安全问题
- 数据访问层中，数据保密和安全性

下面我们将从这三个方面分析系统安全需求和可能遭受的具体风险威胁。

3. 安全需求

基于对系统的分析和行业标准的考虑，以下是系统的安全需求：

- 访问控制：只有经过身份验证的用户和商家才能访问系统功能
- 数据保密性：用户的个人信息和支付数据可能需要加密传输和存储
- 数据完整性：防止数据在传输和存储过程中被篡改或损坏
- 身份验证和授权：用户身份必须经过验证，并根据角色和权限进行授权
- 系统稳定性：不会因为访问量过大而崩溃，有足够空间存储用户数据

4. 风险评估

通过威胁建模的方法，我们识别出以下潜在威胁，并评估其风险

风险严重性程度高

- 身份欺骗：攻击者冒充合法用户或商家，尝试访问系统或执行未授权的操作，例如攻击者爆破获取用户密码。
- 数据修改：用户的个人信息、订单数据或支付信息可能被攻击者篡改，包括SQL注入攻击等。
- XSS（跨站脚本）攻击：攻击者通过在系统中注入恶意脚本，从而窃取用户信息或篡改网页内容。

风险严重性程度中

- 数据泄露：用户的个人信息、订单数据或支付信息可能被攻击者窃取或泄露。
- 未经授权访问：攻击者尝试绕过身份验证机制，直接访问系统资源

风险严重性程度低

- DDOS（分布式拒绝服务）攻击：攻击者通过洪水式请求，使系统过载，导致服务不可用

5. 防护措施

针对上述可能存在的风险，我们采取了以下安全控制措施：

- 强化访问控制：实施基于角色的访问控制机制，要求用户进行身份验证才能访问系统功能和数据。为了防止用户的密码过于简单，我们要求用户密码需要足够复杂，例如需要12个字符及以上，并需要同时包含数字、英文字母和符号
- 采用对象序列化保存作为持久化的方式，解决了SQL注入攻击这一风险。
- 预计采用入侵检测和防御措施，以应对DDoS攻击和未经授权的访问。
- 数据定时存储到磁盘，并对数据定时进行备份。