1. 后端启用https加密连接，保证数据在传输过程中的安全性

2. 登录校验采用 jwt的形式，有效避免csrf攻击

3. 前端和后端对数据进行双重校验，保证数据的合法性

4. 后端操作数据库使用预编译SQL语句，防止SQL注入攻击

5. 权限模型采用简化版的 RBAC 权限管理模型，设计简单，易于扩展，每名用户拥有角色，用户和角色之间为多对多，目前角色暂时分为登录用户和管理员两类。