1. **系统安全性问题**

安全性是设计和实施中的一个重要方面，如何确保学生和教师的隐私和数据安全是系统需要考虑的问题。为了确保学生和教师的隐私和数据安全，系统采取了一系列防御措施来防止未经授权的访问。

* 1. **用户权限分类**

系统实现了细粒度的权限管理，确保不同角色具有相应的访问权限：

1. 学生权限：可以查看自己的考勤记录、提交请假申请、查看课程表等。
2. 教师权限：可以管理学生的考勤记录、审批请假申请、发布考勤等。
   1. **接口参数安全**

为了保护系统免受恶意攻击，所有接口参数都经过严格的安全检查：

1. 输入验证：对所有用户输入进行格式、类型和范围的验证，确保它们符合预期的规范。
2. 防止注入攻击：通过参数化查询和适当的数据清洗，防止SQL注入攻击。
3. 防止跨站脚本攻击：对用户输入的内容进行编码和过滤，避免XSS攻击。
   1. **DoS攻击防护**

系统设计了专门的机制来抵御拒绝服务（DoS）攻击：

1. 请求频率限制：通过限制每个用户或IP地址在特定时间内的请求次数，防止恶意用户通过大量请求来耗尽系统资源。
2. 负载均衡：使用负载均衡技术分散网络流量和请求，提高系统的处理能力和抗攻击能力。
3. 异常流量监控：实时监控网络流量和请求模式，快速识别并阻断异常流量，减轻DoS攻击的影响。
   1. **防止未经授权的访问**

为了确保学生和教师的隐私和数据安全，系统采取了一系列防御措施来防止未经授权的访问：

1. 身份验证机制：系统实施了多因素身份验证机制，要求用户在登录时提供至少两种验证信息，如密码加手机验证码或者密码加生物识别信息（指纹或面部识别）。这种多层次的验证过程大大增加了账户安全性。
2. 数据加密技术：所有敏感数据，包括个人信息和考勤记录，都通过强加密算法进行加密存储。在数据传输过程中，使用SSL/TLS等安全协议确保数据在客户端和服务器之间安全传输。
3. 访问控制策略：系统根据角色基础的访问控制（RBAC）模型，为不同的用户角色（如学生、教师）定义了明确的权限。每个角色都有特定的访问权限，确保用户只能访问对应的资源和数据。