# **4.系统安全性和权限设计**

## 4.1 **系统安全性**

我们针对几种常见的Web攻击方式，制定了几种应对策略。

1. CSRF（Cross-site request forgery）跨站请求伪造

我们通过设置SameSite Cookie属性为strict属性，使Cookie在任何情况下都不可能作为第三方Cookie，来避免CSRF攻击。

1. SQL注入

我们通过使用ORM框架，避免SQL语句直接进行字符串拼接，以避免SQL注入。

1. XSS（Cross Site Scripting）跨站脚本攻击

我们通过对特殊字符进行转义来避免XSS攻击。

## 4.2 **系统权限设计**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 权限 | 评审表评分 | 团队管理 | 学生管理 | 助教管理 | 老师管理 | 班级管理 | 创建评审表 | 重置密码 | 作业管理 | 成绩管理 |
| 组员 |  |  |  |  |  |  |  |  |  |  |
| 组长 | √ | √ |  |  |  |  | √ |  |  | √ |
| 老师 | √ | √ | √ | √ | √ | √ |  |  | √ | √ |
| 助教 | √ | √ | √ | √ | √ | √ |  |  | √ | √ |
| 超级管理员 |  | √ | √ | √ | √ | √ |  | √ |  | √ |

# **数据库设计概述**

数据库主要的表有：用户表、团队表、班级表、团队博客成绩表、结对表等。详细的数据库设计说明请参考《数据库设计说明书》

E-R 图:

