系统设计说明书

**评了么小组**

**2021.4.15**

目录

[1.引言 2](#_Toc18690)

[1.1编写目的 2](#_Toc21379)

[1.2项目背景 2](#_Toc5809)

[1.3参考资料 2](#_Toc22534)

[1.4 缩写定义 2](#_Toc6806)

[2. 系统结构设计 2](#_Toc2471)

[2.1 系统架构设计 2](#_Toc30948)

[2.1.1 架构概述 2](#_Toc5072)

[2.1.2 架构说明 3](#_Toc28497)

[2.2 系统功能模块设计 3](#_Toc25967)

[2.2.1 功能模块设计 3](#_Toc224)

[2.2.2 功能模块层次图 4](#_Toc11809)

[3. 接口设计 4](#_Toc31955)

[3.1 状态码规定 4](#_Toc19916)

[3.2接口列表 4](#_Toc8801)

[4.系统安全性和权限设计 13](#_Toc4625)

[4.1 系统安全性 13](#_Toc28387)

[4.2 系统权限设计 13](#_Toc14391)

[5. 数据库设计概述 14](#_Toc21136)

# 1.**引言**

## 1.1编写目的

评了么项目旨在提供一个在线评分系统，帮助助教提高作业评分效率，提供比现有方式更好的课堂答辩评审体验，同时减轻助教的工作量并降低助教工作复杂度。

## 1.2项目背景

软件名称：评了么评分系统

项目任务提出者：单红老师

项目开发者：评了么团队

## 1.3参考资料

1. (美)Roger S.Pressman 著，郑人杰等译.软件工程[M].第八版. 北京：机械工业出版,2017.
2. 邹欣.构建之法[M].第二版. 北京：人民邮电出版社，2015.

## 1.4 缩写定义

评了么评分系统下称“本系统”。

# **系统结构设计**

## 2.1 **系统架构设计**

### 2.1.1 **架构概述**

本系统使用MVC模式设计架构，进行前后端分离。视图层和业务层分离，这样就允许更改视图层代码而不用重新编译模型和控制器代码，业务流程或者规则的改变只需要对前端代码进行改动即可。也可以很容易地改变应用程序的数据层和业务规则。

### 2.1.2 **架构说明**

根据MVC模式，本系统主要可分为Model（模型），View（视图），Controller（控制器）三个层次。

1. Model层

本层主要负责数据库的结构映射，数据库增删改查等直接对数据库进行操作的行为。向提供接口的方式允许其他层间接地访问数据库。

1. View层

本层的分为前端与后端两个部分。前端负责Web界面的显示与逻辑。后端负责接收前端请求并根据前端请求返回前端所需的数据。

1. Controller层

本层负责绝大多数的业务逻辑。在接收到前端请求的时候，对请求进行处理。处理业务逻辑过程中，通过Model层间接对数据库进行访问，并且通过View层将处理结果返回给前端，并在前端展示给用户。

## 2.2 **系统功能模块设计**

### 2.2.1 **功能模块设计**

本系统的功能模块大体上围绕四种不同类型的用户来设计的。

1. 超级管理员

超级管理员模块由登陆、教师管理、密码重置组成。超级管理员模块主要负责危险数据的访问，如增加教师与密码重置。

1. 教师/助教

教师/助教模块由学生管理，班级管理，助教管理，作业管理，评分管理，成绩管理等组成。学生管理允许对学生进行导入，以及信息的修改。班级管理、助教管理负责对班级进行创建、增加助教等。作业管理、评分管理、成绩管理可以新建发布作业，对评审表进行评分，对个人成绩、团队成绩进行管理。

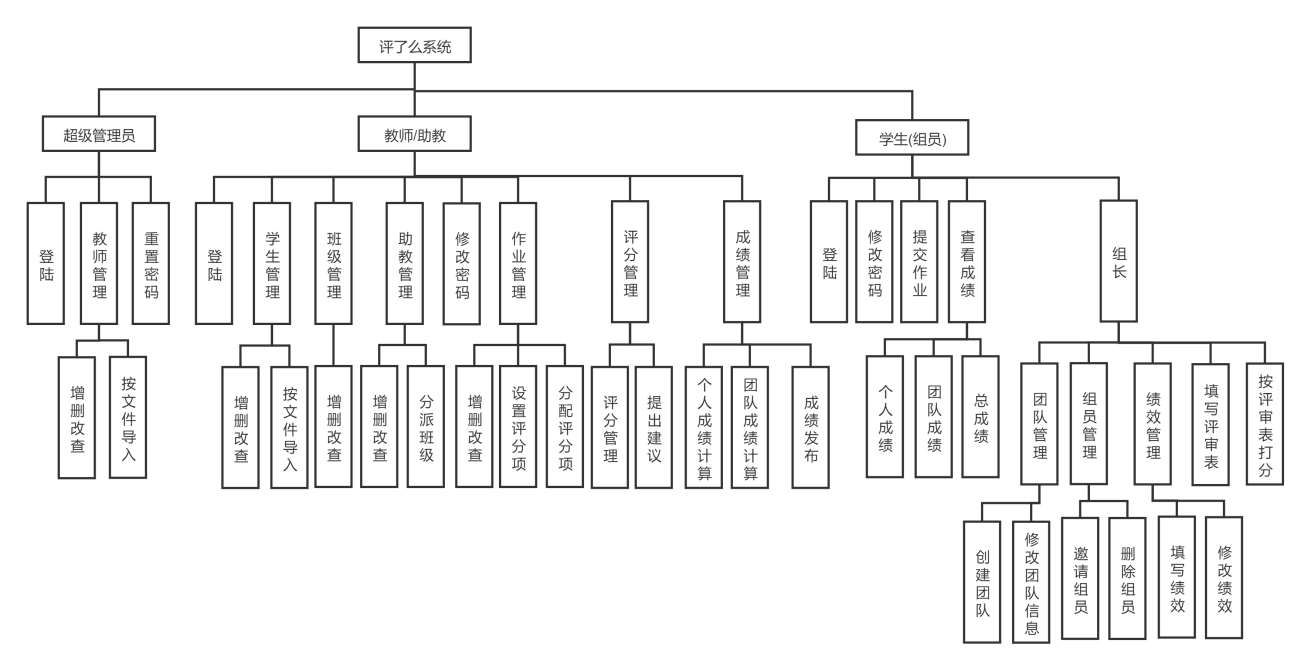
1. 用户-普通组员

普通组员模块主要功能是查看成绩，如个人成绩，团队成绩。

1. 用户-组长

组长模块由团队管理，组员管理，绩效管理，评审表新建、评审表打分组成。

### 2.2.2 **功能模块层次图**



# **接口设计**

## **3.1 状态码规定**

未登录：401  
未授权访问：403  
数据库操作失败：50001  
加密失败：50002  
参数错误：40001

## **3.2接口列表**

注：URL前均省略“/api/v1/”。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| login | POST | { "uid": 学号, "password": 密码 } | { "code": 0, "data": { "uid": 学号, "identity":教师0、助教1、学生2 }, "msg": "Success" } { "code": 40001, "msg": "账号或密码错误" } | 用户登录 |
| user/information | GET | { "identity": 0、1 } | { "code": 0, "data": { "uid":教师工号或学生学号, "nickname": 昵称, "password":加密密码 }, "msg": "Success" } { "code": 40001, "msg": "数据获取错误" } | 个人信息 |
| user/information | GET | { "identity": 2 } | { "code": 0, "data": { "nickname": 姓名, "uid":学号, "student1\_id":结对学生ID,没有则返回"尚未结对" "name":团队名,没有则返回"尚无团队" "password":加密密码 }, "msg": "Success" } { "code": 40001, "msg": "数据获取错误" } | 个人信息 |
| user/pairing\_edit | GET | { "uid": 学号 } | { "code": 0, "msg": "结对成功！" } { "code": 0, "msg": "结对失败！对方已结对！" } { "code": 40001, "msg": "数据获取错误" } | 填写结对信息 |
| user/group\_create | GET | { "group\_name": 团队名称 } | { "code": 0, "msg": "创建团队成功！" } { "code": 0, "msg": "创建团队失败！该名称已被使用！" } { "code": 40001, "msg": "数据获取错误" } | 创建团队 |
| user/password\_edit | POST | { "uid": 学号, "password": 密码 } | { "code": 0, "msg": "修改成功！" } { "code": 40001, "msg": "出现错误" } | 修改密码 |
| logout | DELETE |  |  | 用户登出 |
| user/member\_add | GET | { "uid": 学号 } | { "code": 0, "msg": "增加组员成功！" } { "code": 0, "msg": "增加组员失败！该学生已有团队！" } { "code": 0, "msg": "增加组员失败！该用户不为学生！" } { "code": 40001, "msg": "数据获取错误" } | 增加组员 |
| user/member\_delete | GET | { "uid": 学号 } | { "code": 0, "msg": "删除成功！" } { "code": 40001, "msg": "数据出现错误" } | 删除组员 |
| user/evaluation\_create | GET | { "name": 团队名 } | { "code": 0, "ID":评审表ID, "msg": "创建成功！" } { "code": 40001, "msg": "数据出现错误" } | 创建评审表 |
| user/evaluation\_get | GET | { "name": 团队名, "ID":评审表ID } | { "code": 0, "data": { "content": 空, "score":空, "suggest":空, }, "msg": "Success" } { "code": 40001, "msg": "获取错误" } | 获取评审表 |
| user/evaluation\_edit | GET | { "content":内容, "score":分数, "suggest":建议, } | { "code": 0, "msg": "填写成功！" } { "code": 40001, "msg": "数据修改错误！" } | 填写评审表 |
| user/merit\_edit | GET |  | { "code": 0, "msg": "填写成功！" } { "code": 40001, "msg": "数据修改错误！" } | 填写绩效 |
| user/homework | GET | { "uid": 学号 } | { "code": 0, "data": { homework\_list:[ { "title":作业标题, "content":作业内容, "start\_time":开始时间, "end\_time":结束时间, }, { "title":作业标题, "content":作业内容, "start\_time":开始时间, "end\_time":结束时间,  } ] }, "msg": "Success" } { "code": 40001, "msg": "数据获取错误" } | 查看作业列表 |
| user/homework\_score | GET | { "uid": 学号 } | { "code": 0, "data": { "total\_score":总分, "homework\_list":[ { "title":作业标题, "content":作业内容, "start\_time":开始时间, "end\_time":结束时间, "score":成绩 }, { "title":作业标题, "start\_time":开始时间, "end\_time":结束时间,  "score":成绩 } ] }, "msg": "Success" } { "code": 40001, "msg": "数据获取错误" } | 获取作业列表与对应成绩及总成绩 |
| student/import | POST | PS：暂时不写 |  | 批量导入学生 |
| student/add | POST | { "uid":学号, "name":姓名, "class\_id":班级编号, } | { "code": 0, "msg": "Success" } { "code": 40001, "msg": "数据获取错误" } | 批量添加学生 |
| teacher/create | POST | { "uid":教师编号, "name":姓名, "class\_id":班级编号, } | { "code": 0, "msg": "Success" } { "code": 40001, "msg": "数据获取错误" } | 创建助教 |
| teacher/setclass | POST | { "uid":教师编号, "class\_id":班级编号, } | { "code": 0, "msg": "Success" } { "code": 40001, "msg": "数据获取错误" } | 设置助教的班级 |
| homework/create | POST | { "class\_id":班级编号, "homework\_name":作业名, "homework\_item":[ { item\_id:"评分项编号", item\_name:"评分项名称", item\_comment:"评分项注释", item\_parentID:"评分项父级id",[ TODO ] }  ], } | { "code": 0, "msg": "Success" } { "code": 40001, "msg": "数据获取错误" } | 创建作业 |
| homework/preview/:id | GET | URL参数 | { "code": 0, "data": { { "homework\_id":作业编号, "item":[ { item\_id:"评分项编号", item\_name:"评分项名称", item\_comment:"评分项注释", item\_parentID:"评分项父级id", }  ], } "msg": "Success" } { "code": 40001, "msg": "数据获取错误" } | 显示作业预览及评分项 |
| score/edit | POST | { "homework\_id":作业编号, "score":[ { item\_id:"评分项编号", item\_score:"评分项得分", item\_comment:"评分项备注", }  ], "homework\_comment":"作业备注", } | { "code": 0, "msg": "Success" } { "code": 40001, "msg": "数据获取错误" } | 提交评分结果及备注 |
| homeworkList/get | GET | { "class\_id":班级编号, } | { "code": 0, "data": { "homework\_list":[ { "title":作业标题, } ] }, "msg": "Success" } { "code": 40001, "msg": "数据获取错误" } | 获取某班级的作业列表 |
| homework/import | POST | PS：暂时不写 |  | 批量导入作业 |
| admin/password/reset | POST | { "uid":用户账号, } | { "code": 0, "msg": "Success" } { "code": 40001, "msg": "数据获取错误" } | 重置密码 |
| teacher/add | POST | { "uid":教师编号, "name":姓名, } | { "code": 0, "msg": "Success" } { "code": 40001, "msg": "数据获取错误" } | 增加老师 |
| class/create | POST | { "class\_id":班级编号, "class\_name":班级名字, } | { "code": 0, "msg": "Success" } { "code": 40001, "msg": "数据获取错误" } | 创建班级 |
| student/list/:class\_id | GET | URL参数 | { "code": 0, "data": { "stu\_list":[ { "stu\_name":"学生姓名", "stu\_id":"学号" } ] }, "msg": "Success" } { "code": 40001, "msg": "数据获取错误" } | 查看班级学生列表 |
| student/class/change | POST | { "uid":学号, "class\_id":班级编号, } | { "code": 0, "msg": "Success" } { "code": 40001, "msg": "数据获取错误" } | 改变学生的班级 |
| teacher/list | GET |  | { "code": 0, "data": { "teacher\_list":[ { "teacher\_name":"老师姓名", "teacher\_id":"老师编号" } ] }, "msg": "Success" } { "code": 40001, "msg": "数据获取错误" } | 查看老师的账号 |

# **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**

本系统使用基于角色的权限访问控制RBAC（Role-Based Access Control）方式进行权限控制。每个用户都对应以下的某个角色，每种角色拥有自己特定的权限。

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 角色/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:

