

Code 帮帮队

系统设计说明书

组员：陈尚斌、杨文渊、林怡杰、鄢灿、
吕东剑、许俊翔、陈禹帆、吴康明

指导老师：汪璟玢

Code 帮帮队编写

2025 年 10 月 17 日

目录

1. 文档介绍	4
1.1. 文档目的	4
1.2. 阅读对象	4
1.3. 文档约定	5
2. 总体设计	6
2.1. 软件结构	6
2.1.1. 系统架构	6
2.1.2. 软件功能结构	7
3. 系统功能模块	8
3.1. 首页模块	8
3.2. 个人中心模块	8
3.3. 错题本录入模块	9
3.4. 错题列表模块	10
3.5. 错题详情模块	11
3.6. 错题分析模块	11
3.7. 复习计划模块	12
3.8. 登录注册模块	13
4. 接口设计	14
4.1. 接口规范	14
4.1.1. 接口命名规范	14
4.1.2. 响应状态码规定	15
4.1.3. 注意事项	16
4.1.4. 协议约定	18
4.2. 接口总览	19
4.3. 接口文档	20
4.3.1. 用户模块	20

4.3.2. 首页模块	23
4.3.3. 个人中心模块	25
4.3.4. 错题录入模块	27
4.3.5. 错题本列表模块	30
4.3.6. 错题本详情模块	31
4.3.7. 错题本分析模块	32
4.3.8. 复习计划模块	35
4.3.9 用户管理	38
4.3.10 数据概览	41
4.3.11 标签管理	43
4.3.12 系统维护	46
4.3.12.1 查看系统日志	46
5. 权限设计	48
6. 安全性、健壮性与可扩展性	50
6.1. 安全性	50
6.1.1. 防 SQL 注入	50
6.1.2. CSRF 防御	50
6.1.3. XSS 防御	51
6.1.4. DDOS 防御	51
6.1.5. 多因素认证	52
6.1.6. 用户密码安全	52
6.1.7. 基于 RSA 的用户数据保护	53
6.2. 健壮性	53
6.2.1. 状态码	53
6.2.2. 响应时间	54
6.2.3. 数据库操作限制	54
6.2.4. 输入检测	55

6.2.5. 数据转换	55
6.3. 可扩展性	55
6.3.1. 系统功能模块化	55

1. 文档介绍

1.1. 文档目的

本系统设计说明书旨在明确项目目标与需求，详细阐述系统架构设计、功能模块定义、技术选型与标准、性能与安全要求、运维与监控方案。文档通过全面规划，确保开发团队对视频网站系统的整体设计有清晰理解，促进项目高效有序进行。同时，为运维人员、开发人员及用户提供必要的操作手册和文档支持，确保系统上线后能顺利运行并得到有效维护。本说明书是视频网站项目成功实施的关键基石，为系统后续的开发、运维及扩展提供坚实基础。

1.2. 阅读对象

本视频网站系统设计说明书的阅读对象涵盖了项目生命周期中的多个关键角色，他们各自拥有不同的职责和关注点。具体而言，这些阅读对象包括但不限于：

- (1) 项目负责人与产品经理：他们是项目的决策者和规划者。通过阅读本说明书，他们能够全面把握项目的整体目标、预期成果、市场定位及用户需求，从而进行有效的项目管理和产品规划。同时，他们还能了解项目的关键里程碑、资源分配及风险管理策略，确保项目按时、按质、按量完成。
- (2) 开发团队：包括前端开发工程师、后端开发工程师、数据库管理员、移动应用开发者等。他们负责系统的具体实现。通过深入阅读本说明书，开发团队能够明确系统的技术选型、功能模块划分、接口定义及数据交互方式。这有助于他们制定详细的开发计划、进行代码编写、单元测试及集成测试，确保系统的稳定性和可靠性。
- (3) 测试团队：他们负责系统的质量保障。通过阅读本说明书，测试团队能够了解系统的功能需求、性能要求、安全标准及用户体验期望。在此基础上，他们能够制定全面的测试计划，包括功能测试、性能测试、安全测试及兼容性测试等，确保系统满足用户需求及业务目标。
- (4) 运维团队：他们负责系统的日常运行和维护。通过阅读本说明书，运维团队能够熟悉系统的架构设计、部署方案、运维工具及监控策略。这有助于他们进行系统的日常监控、性能调优、故障排查及数据备份恢复等工作，确保系统稳定运行并快速响应问题。
- (5) 利益相关者与客户：他们可能包括项目投资者、合作伙伴、最终用户等。通过阅读本说明书，他们能够了解系统的核心功能、用户体验及业务价值，从而对项目的进展和成果进行评估和反馈。这有助于项目团队及时调整策略，满足用户需求及市场变化。

1.3. 文档约定

文档约定主要是指本设计说明书的排版约定，文档风格为：

标题 1：宋体，二号，粗体；

标题 2：宋体，三号，粗体；

标题 3：宋体，四号，粗体；

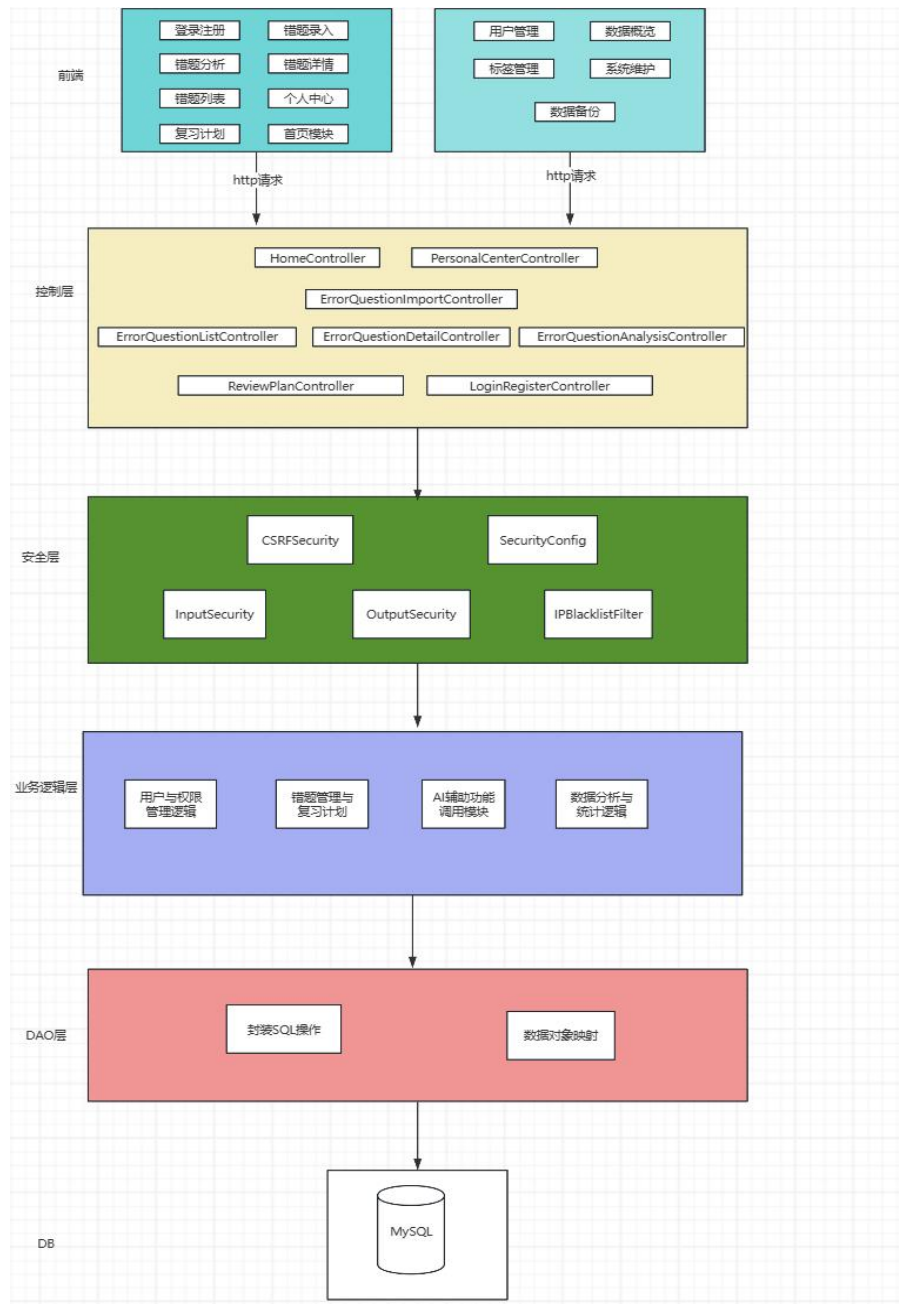
标题 4：宋体，四号，粗体；

正文：宋体，小四号，单倍行距；

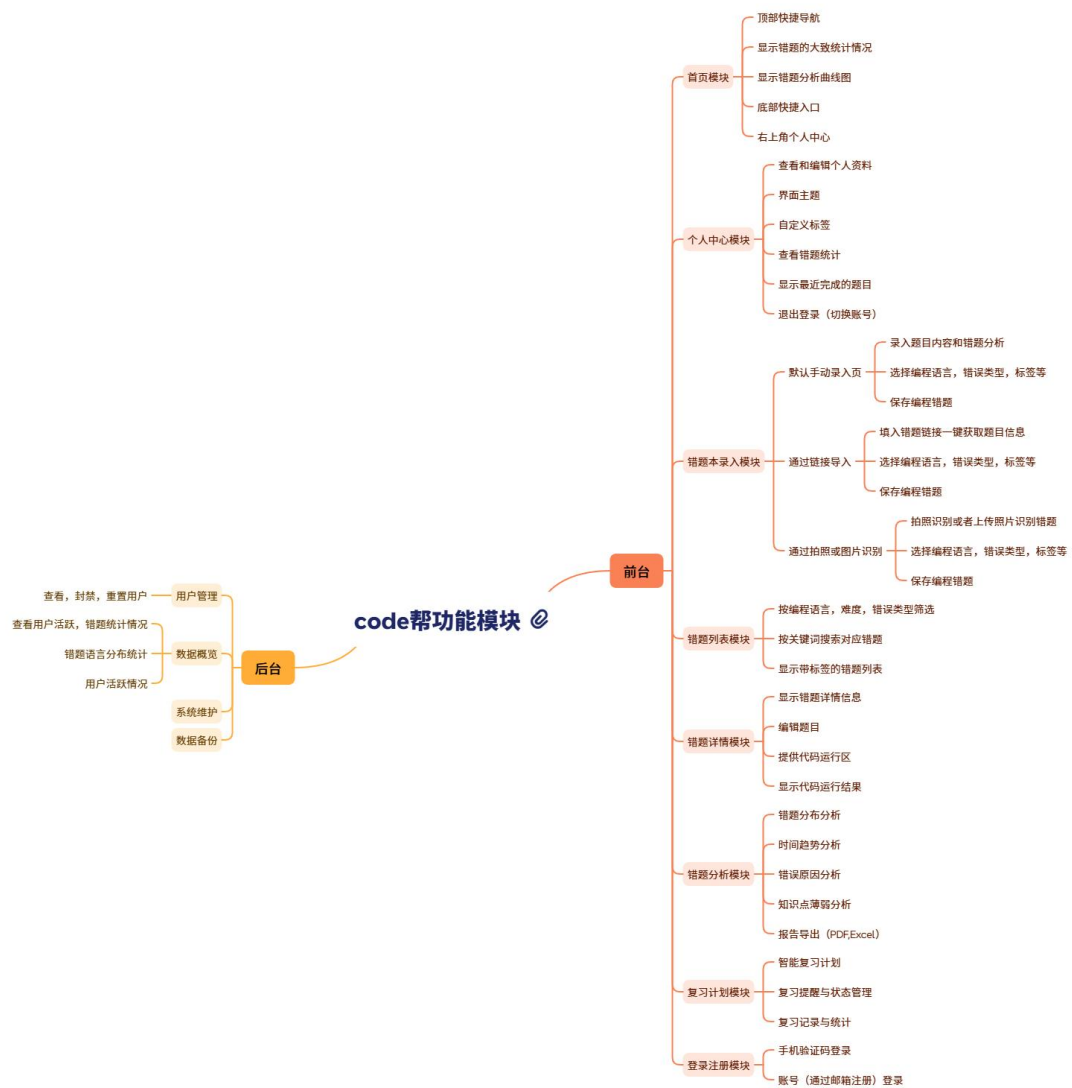
2. 总体设计

2.1. 软件结构

2.1.1. 系统架构



2.1.2. 软件功能结构



Presented with xmind

3. 系统功能模块

3.1. 首页模块

首页的功能模块由顶部快捷导航、显示错题的大致统计情况、显示错题分析曲线图、底部快捷入口、右上角个人中心等子功能模块组成，各个模块功能如下：



顶部快捷导航：可在首页、错题本、分析错题页面之间快速跳转，提升操作效率。

显示错题的大致情况：展示总错题数、已掌握错题数、需复习错题数、近期待复习错题数，并与上周数据对比，更直观呈现错题掌握情况变化。

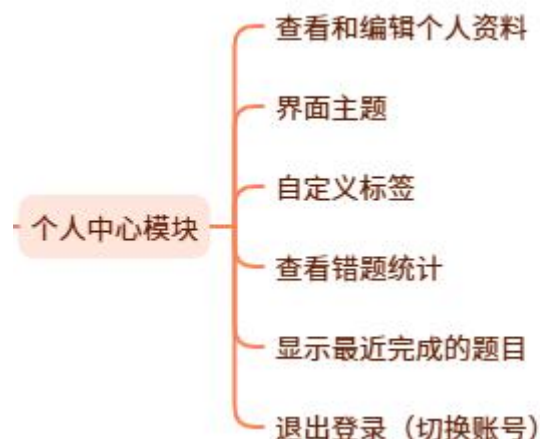
显示错题分析曲线图：支持按周、月、年的维度，展示总错题数与复习数量的趋势，助力用户把握错题变化规律。

底部快捷入口：提供错题录入、错题列表、错题数据分析页面的快速访问通道，简化操作路径。

个人中心：点击可进入个人中心模块，便于进行个人信息管理与设置

3.2. 个人中心模块

个人中心的功能模块由查看和编辑个人资料、界面主题、自定义标签、查看错题统计、显示最近完成的题目、退出账号（切换账号）等子功能模块组成，各个模块功能如下：



查看和编辑个人资料：用户可在这里查看、更新自己的个人信息。

界面主题：支持用户根据个人喜好切换界面主题风格，打造舒适的使用视觉体验。

自定义标签：允许用户根据自身学习节奏与需求，灵活自定义错题标签。

查看错题统计：通过错题统计功能，用户能清晰了解自己的薄弱环节，从而更高效地进行查漏补缺。

显示最近完成的题目：可快速回顾最近完成的题目，便于及时复盘学习内容，巩固知识记忆。

退出账号（切换账号）：为有多个账号需求的用户提供便利，可轻松退出当前账号或切换至其他账号，满足不同使用场景。

3.3. 错题本录入模块

错题本录入的功能模块由手动输入错题、链接导入错题、拍照或图片识别录入错题功能模块组成



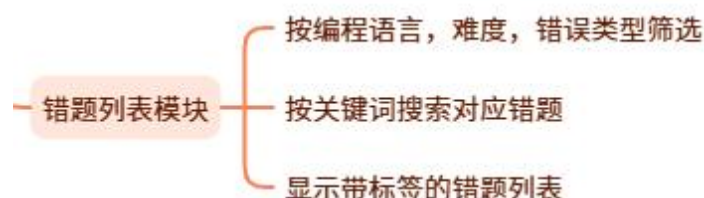
手动录入：在默认手动录入页，用户可自主录入题目内容，还能为错题选择编程语言、错误类型、知识点标签等分类信息，最后完成编程错题的保存。这种方式适合需要深度梳理错题思路、手动细化内容的场景。

链接导入：只需填入错题链接，就能一键获取题目信息；随后同样可选择编程语言、错误类型、标签等分类项，进而保存编程错题。该方式大幅节省了手动输入题目的时间，便捷性更强。

拍照或图片识别录入：通过拍照识别或上传照片识别错题，系统会智能提取相关内容；之后选择编程语言、错误类型、标签等，即可完成编程错题的保存。对于纸质题目、无法复制链接等场景，这种智能识别的方式尤为实用。

3.4. 错题列表模块

错题列表模块是对已录入错题进行高效管理与便捷查找的核心区域，通过多种灵活方式助力用户快速定位目标错题，提升复习效率。



错题列表模块支持按编程语言、难度、错误类型进行精准筛选，能让用户快速聚焦某一类特征的错题（如仅查看 Java 语言、高难度的逻辑错误类错题）；

也可按关键词搜索对应错题，借助题目中的关键信息（如知识点名称、代码片段关键词等），快速锁定相关错题；同时，还能显示带标签的错题列表，依托前期为错题设置的标签，更直观地基于分类标签梳理错题，让错题查找与复习更具针对性，为后续高效复习提供清晰指引。

3.5. 错题详情模块

错题详情模块由显示错题详情信息、编辑题目、提供代码运行区、显示代码运行结果等子功能模块组成，各个模块功能如下：



显示错题详情信息：可清晰呈现错题的完整维度内容，包括题目描述、错误代码片段、错因分析等关键信息，让用户快速回溯错题场景与核心问题。

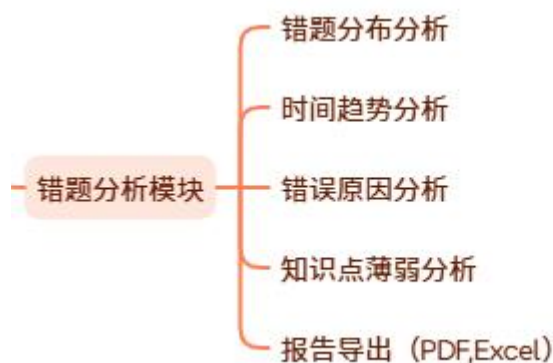
编辑题目：功能支持对题目内容、错因标注等进行修改与完善，便于用户在复盘时补充细节、优化记录，使错题信息更精准契合学习需求。

提供代码运行区：搭建了便捷的代码编写与调试环境，方便用户针对错题中的代码问题，即时开展修改、验证等实操性操作。

显示代码运行结果：直观呈现代码运行后的输出反馈，帮助用户快速判断修改后的代码是否符合预期，高效完成代码层面的错题纠错与思路优化。

3.6. 错题分析模块

错题分析模块由错题分布分析、时间趋势分析、错误原因分析、薄弱知识点分析、报告导出等子功能模块组成，各个模块功能如下：



错题分布分析：错题分布分析可从编程语言、错误类型、题目难度等维度，直观呈现错题在不同类别下的分布格局，让用户快速知晓哪类错题占比更高。

时间趋势分析：时间趋势分析以时间为轴线，展现错题数量、错误率等指标的动态变化趋势，辅助用户把握学习状态的起伏（如近期错题是增多还是减少，学习效果是否稳定）。

错误原因分析：错误原因分析会对错题的根源进行归类总结，像语法错误、逻辑漏洞、知识点误解等类型，精准定位犯错的核心诱因。

知识点薄弱分析：知识点薄弱分析则基于错题关联的知识点，梳理出用户掌握不扎实的知识板块，明确后续复习的重点方向。

报告导出：支持将分析结果以 PDF 或 Excel 格式导出，方便用户留存、分享或进一步整理，为学习规划提供更灵活的依据。

3.7. 复习计划模块

复习计划模块由智能复习计划、复习提醒与状态管理、复习记录与统计等子功能模块组成，各个模块功能如下：



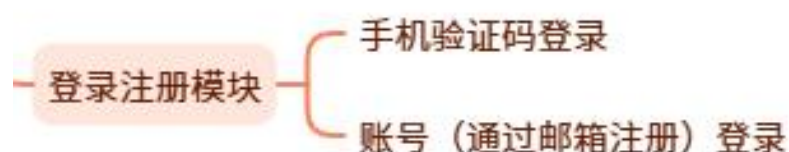
智能复习计划：可依据用户的错题特征（如知识点分布、掌握薄弱程度等），自动生成个性化的复习方案，合理规划复习内容与时间，让复习更具针对性，避免盲目性。

复习提醒与状态管理：能设置定时复习提醒，督促用户按计划执行复习任务；同时实时管理复习进度与状态，清晰展示“已复习 / 待复习”等阶段情况，保障复习的持续性与连贯性。

复习记录与统计：会全程记录复习行为，并通过统计分析呈现复习效果的变化趋势，助力用户评估复习策略的有效性，进而优化后续复习安排。

3.8.登录注册模块

登录注册模块由手机验证码登录和账号（通过邮箱注册）登录等子功能模块组成。



用户填写信息进行注册和登录

3.9.后台



用户管理：支持对用户进行“查看、封禁、重置”等操作，便于规范用户体系，灵活管理用户账号状态。

数据概览：可呈现多维度平台数据，包括用户活跃情况、错题统计情况（如错题语言分布统计）等，为运营策略制定、功能迭代方向提供数据依据。

系统维护：承担系统整体运行状态的维护工作，及时排查并处理潜在问题，保障前端各业务模块（如错题录入、分析、复习计划等）稳定可用。

数据备份：对用户信息、错题数据等核心数据进行备份存储，有效防范数据丢失风险，确保数据安全性与可恢复性。

4. 接口设计

4.1. 接口规范

4.1.1. 接口命名规范

- 基础 URL：需要有某个路径表示版本号，如 `https://api.example.com/v1`
- 资源命名：使用小写字母，如 `/user`、`/order`。
- 数据格式：请求可以是 HTTP 的不同类型（如 Header、Query），响应均使用 JSON 格式。

4.1.2. 响应状态码规定

暂定以下状态码

HTTP 状态码	响应状态码	状态码描述
200	0	成功
200	1001	系统内部错误
200	1002	第三方调用错误
200	1004	数据库调用错误
200	1008	文件系统错误
200	2001	access_token 无效
200	2002	access_token 过期
200	2004	access_token 废弃（密码重置）
200	3001	该接口已废弃
200	3002	网络调用错误
200	4001	参数不合法
200	4002	数据验证失败
200	5001	资源不存在
200	5002	资源冲突
200	6001	权限不足
200	7001	MFA 认证失败
4xx	-	客户端错误响应
5xx	-	服务端错误响应

表 6-1 状态码表

4.1.3. 注意事项

4.1.3.1. 接口规范

- 对于文档中提供的 GET 请求, 无特殊要求
- 对于文档中提供的 POST 请求, body 中的参数应以 JSON 字符串形式写入
- 当以 JSON 传递数据时候, 需要设置请求头 "content-type":
"application/json"

4.1.3.2. 资源文件规范

4.1.3.2.1. 图片资源

- (1) 图片格式要求支持的图片格式：JPEG、PNG、GIF、BMP（建议优先使用 JPEG 和 PNG 格式，因为它们在压缩率和质量之间提供了良好的平衡）。

- (2) 图片大小限制

最大文件大小：单张图片不超过 5MB

尺寸限制：建议图片宽度不超过 2000 像素，高度不超过 2000 像素

- (3) 图片质量要求

分辨率：图片应具有较高的分辨率，以确保在缩放时保持清晰度。

压缩率：在保证图片质量的前提下，尽量使用适当的压缩率来减小文件大小。

- (4) 色域和颜色模式

色域：建议使用 sRGB 色域，因为它是 Web 上最常用的色域。

颜色模式：图片应为 8 位/通道 RGB 颜色模式（对于 PNG 和 GIF 格式，可支持透明通道）。

- (5) 其他要求

无水印：上传的图片不应包含任何水印或广告信息。

无版权问题：确保上传的图片不侵犯任何第三方的版权。

内容合法：图片内容应符合相关法律法规和平台规定，不包含敏感、违法或不良信息。

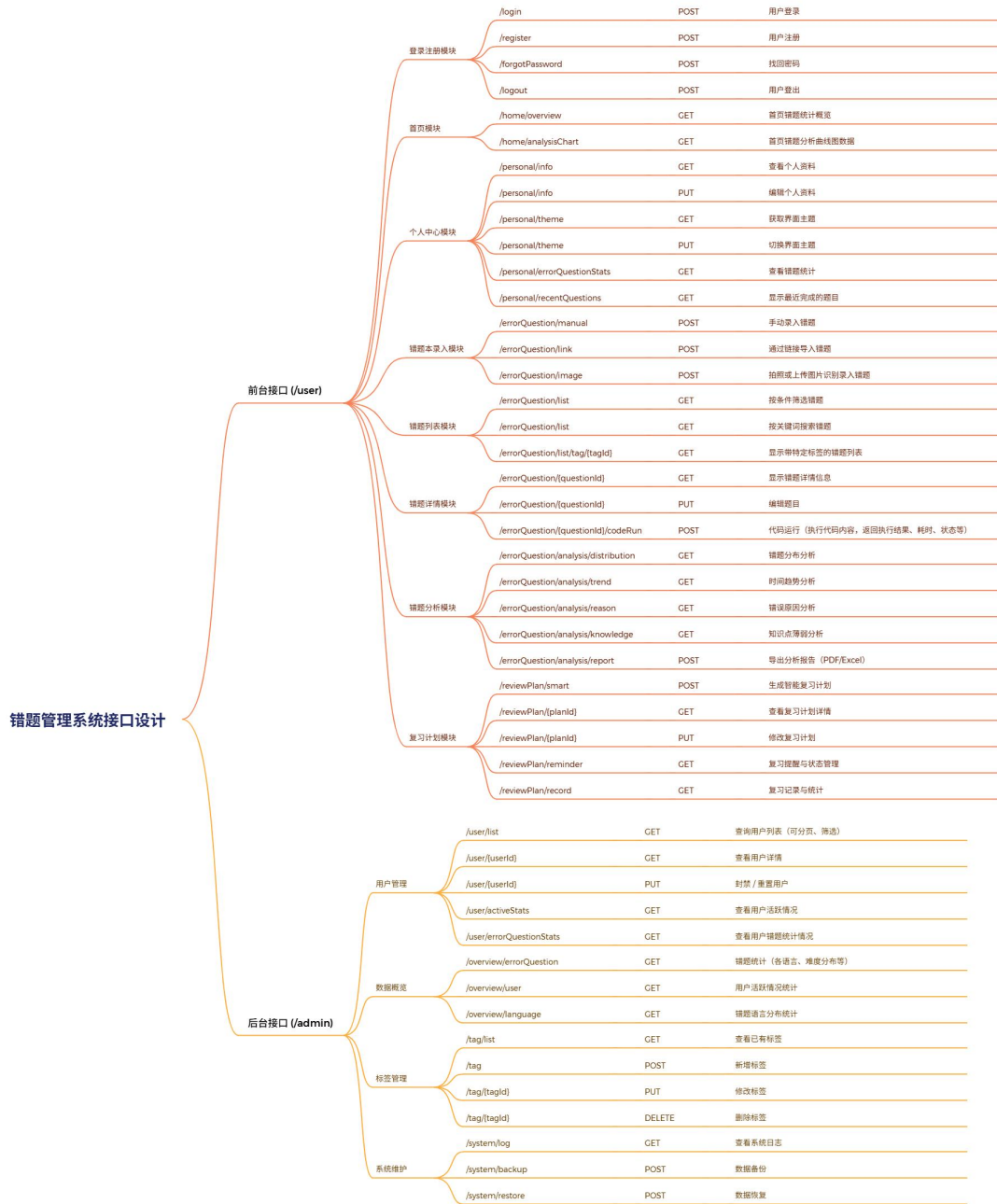
- (6) 备注

本平台会对部分图片进行压缩，请务必保证原图片**清晰度充足**。

4.1.4. 协议约定

- 所有请求皆为 http/https 请求
- 所有 url 参数请注意 URL encode (中文字符适配)
- 所有字符编码采用 UTF-8 编码

4.2. 接口总览



Presented with xmind

4.3. 接口文档

4.3.1. 用户模块

4.3.1.1. 用户注册

简要描述

- 用户注册接口

请求 URL

- /api/v1/user/register

请求方法

- POST

注意事项

- 邮箱不可重复
- 手机号不可重复
- 邮箱格式必须符合规范
- 密码具备安全强度权限要求
- 无请求参数

HTTP 参数类型	参数名	参数类型	必选	描述
Body	phone	string	是	手机号绑定
				符以内)
	password	string	是	用户密码 (需拥有足够安全密码强度, 比如特殊字符、大小写字母)

	email	string	是	绑定邮箱（需满足邮箱格式）

表 6-3 用户注册请求参数表

5.3.1.2. 用户使用账号登录

简要描述

- 用户账号登录接口

请求 URL

- /api/v1/user/login

请求方法

- POST

注意事项

- 允许用户名或邮箱登录
- 无请求参数

HTTP 参数类型	参数名	参数类型	必选	描述
Body	username/email	string	是	用户名（也可用 email）
	password	string	是	用户密码

5.3.1.3. 上传头像

简要描述

- 上传头像接口
- 返回一个 URL 供上传

请求 URL

- /api/v1/user/avatar/upload

请求方法

- GET

注意事项

- 无权限要求
- 已登录用户请求参数

HTTP 参数类型	参数名	参数类型	必选	描述
Header	avatar_url	string	是	头像 URL

5.3.1.4. 忘记密码

简要描述

- 忘记密码接口

请求 URL

- /api/v1/user/security/password/retrieve

请求方法

- POST

注意事项

- 无权限要求
- 无请求参数

HTTP 参数类型	参数名	参数类型	必选	描述
Body	otype	string	是	重置方式（目前用邮箱）
	oid	string	是	重置方式的对象字符串

5.3.1.5. 重置密码

简要描述

- 重置密码接口

请求 URL

- /api/v1/user/security/password/reset

请求方法

- POST

注意事项

- 无权限要求
- 无请求参数

HTTP 参数类型	参数名	参数类型	必选	描述
Body	otype	string	是	重置方式（目前用邮箱）
	oid	string	是	重置方式的对象
	code	string	是	验证码
	password	string	是	新密码（需满足安全密码强度，比如特殊字符、大小写字母）

4.3.2. 首页模块

4.3.2.1. 错题概览

简要描述

- 首页错题概览

请求 URL

- /api/v1/user/home/overview

请求方法

- GET

注意事项

- 无

权限要求

- 无请求参数

4.3.2.2. 首页错题分析曲线图数据

简要描述

- 首页错题分析曲线

请求 URL

- /api/v1/user/home/analysisChart

请求方法

- GET

参数名	位置	类型	必选	描述	示例
groupBy	query	string	否	聚合粒度	week
startDate	query	string	否	开始日期	2025-07-01
endDate	query	string	否	结束日期	2025-10-19

4.3.3. 个人中心模块

4.3.3.1. 查看个人资料

请求 URL: /api/v1/user/personal/info

请求方法: GET

注意事项: 需登录

4.3.3.2. 编辑个人资料

简要描述

- 编辑个人资料
- 请求 URL
- /api/v1/user/personal/info

请求方法

- PUT

注意事项

- 无权限要求
- 无请求参数

参数名	位置	类型	必选	描述	示例
username	body	string	否	新用户名	jack2025
avatarUrl	body	string	否	新头像	https://...
phone	body	string	否	手机号	13800138000
notifyEnable	body	boolean	否	是否接收提醒	TRUE

4.3.3.3. 切换界面主题

简要描述

- 切换界面主题

请求 URL

- /api/v1/user/personal/theme

请求方法

- PUT

注意事项

- 无权限要求
- 无请求参数

参数名	位置	类型	必选	描述	示例
theme	body	string	是	主题枚举	light / dark

4.3.3.4. 设置自定义复习参数

简要描述

- 设置自定义复习参数

请求 URL

- /api/v1/user/personal/reviewParams

请求方法

- PUT

参数名	位置	类型	必选	描述	示例
dailyTarget	body	integer	否	每日目标题数	15

strategy	body	string	否	策略	spaced
hour	body	integer	否	每日提醒小时	21
spacedDays	body	array	否	间隔天数	\[1,2,7,15]

4.3.3.5. 查看近期错题统计

请求 URL: /api/v1/user/personal/errorQuestionStats

请求方法: GET

请求参数: 无

返回数据结构:

4.3.3.6. 查看近期完成题目

请求 URL: /api/v1/user/personal/recentQuestions

请求方法: GET

参数名	位置	类型	必选	描述	示例
size	query	integer	否	返回条数	5 (默认 5)

4.3.4. 错题录入模块

4.3.4.1. 手动录入错题

简要描述

- 手动录入

请求 URL

/api/v1/user/errorQuestion/manual

请求方法

- POST

参数名	位置	类型	必选	描述	示例
title	body	string	是	题目标题	两数之和
content	body	string	是	题目描述	给定一个整数数组 nums ...
wrongCode	body	string	是	错误代码	def twoSum():...
correctCode	body	string	否	正确代码	def twoSum():...
language	body	string	是	编程语言	python
errorType	body	string	是	错误类型	logic
difficulty	body	string	是	难度枚举	easy
tags	body	array[string]	否	知识点标签	["数组","哈希表"]
hint	body	string	否	解题提示	可用字典降低复杂度

sourceUrl	body	string	否	来源链接	<https://leetcode.cn/>...
-----------	------	--------	---	------	---------------------------

4.3.4.2. 链接导入错题

简要描述

- 链接导入错题

请求 URL

- /api/v1/user/errorQuestion/link

请求方法

- POST

参数名	位置	类型	必选	描述	示例
url	body	string	是	题目链接	<https://leetcode.cn/problems/two-sum/>
language	body	string	是	语言	python
errorType	body	string	是	错误类型	logic
tags	body	array[string]	否	标签	\[]

4.3.4.3. 拍照上传

简要描述

- 拍照上传

请求 URL

- /api/v1/user/errorQuestion/image

请求方法

- POST

注意事项

- 无

参数名	位置	类型	必选	描述	示例
image	body	file	是	图片文件	.jpg / .png
language	body	string	是	编程语言	python
errorType	body	string	是	错误类型	syntax

4.3.5. 错题本列表模块

4.3.5.1. 多条件筛选

简要描述

- 多条件筛选

请求 URL

- /api/v1/user/errorQuestion/list

请求方法 : GET

参数名	位置	类型	必选	描述	示例
language	query	string	否	编程语言	python
difficulty	query	string	否	难度	easy
errorType	query	string	否	错误类型	logic
tag	query	string	否	标签名	递归

4.3.5.3. 按关键词搜索

简要描述

- 按关键词搜索

请求 URL

- /api/v1/user/errorQuestion/search

请求方法

参数名	位置	类型	必选	描述	示例
keyword	query	string	是	关键词	二叉树 遍历
page/size	query	integer	否	分页	1/20

4.3.6. 错题本详情模块

4.3.6.1. 错题本详情

简要描述

- 错题本详情

请求方法: GET

注意事项: 仅返回自己的错题

参数名	位置	类型	必选	描述	示例
questionId	path	string	是	错题主键 ID	123

4.3.7. 错题本分析模块

4.3.7.1. 错题本分布分析

简要描述

- 按语言、难度、错误类型、标签等多维度聚合，返回错题分布饼图/柱状图

数据

请求 URL

- /api/v1/user/errorQuestion/analysis/distribution

请求方法

- GET

参数名	位置	类型	必选	描述	示例
language	query	string	否	编程语言	python
difficulty	query	string	否	难度	easy
errorType	query	string	否	错误类型	logic
tag	query	string	否	标签名	递归

4.3.7.2. 错题时间趋势

简要描述

- 给定时间区间，返回每日/周错题新增与复习数量折线数据

请求 URL

- /api/v1/user/errorQuestion/analysis/trend

请求方法

- GET

参数名	位置	类型	必选	描述	示例
startDate	query	string	是	开始日期	2025-09-01
endDate	query	string	是	结束日期	2025-10-19
granularity	query	string	否	粒度 day/week	day

4.3.7.3. 知识点薄弱分析

简要描述

- 根据错题标签与错误频率，计算薄弱知识点 Top-N

请求 URL

- /api/v1/user/errorQuestion/analysis/knowledge

请求方法

- GET

参数名	位置	类型	必选	描述	示例
top	query	int	否	返回前 N 个	10

4.3.7.4. 错误原因分析

简要描述

- 按错误类型聚合，展示各原因占比及平均复习次数

请求 URL

- /api/v1/user/errorQuestion/analysis/reason

请求方法

- GET

参数名	位置	类型	必选	描述	示例
language	query	string	否	编程语言	python
difficulty	query	string	否	难度	easy
tag	query	string	否	标签名	递归

4.3.7.5. 分析报告导出

简要描述

- 生成 PDF / Excel 综合分析报告并提供下载链接

请求 URL

- /api/v1/user/errorQuestion/analysis/report

请求方法

- POST

参数名	位置	类型	必选	描述	示例
format	query	string	是	导出格式 pdf/excel	pdf
language	query	string	否	编程语言	python
difficulty	query	string	否	难度	easy

tag	query	string	否	标签名	递归
-----	-------	--------	---	-----	----

4.3.8. 复习计划模块

4.3.8.1. 生成智能复习计划

简要描述

- 依据艾宾浩斯算法与用户错题难度、错误频率、最近掌握度，自动生成未来 30 日复习任务

请求 URL

- /api/v1/user/reviewPlan/smart

请求方法

- POST

参数名	位置	类型	必选	描述	示例
days	query	int	否	计划天数（默认 30）	30
dailyLimit	query	int	否	每日最大题量（默认 20）	20

4.3.8.2. 查看复习计划详情

简要描述

- 返回计划基本信息及任务列表（分页）

请求 URL

- /api/v1/user/reviewPlan/{planId}

请求方法

- GET

参数名	位置	类型	必选	描述	示例
-----	----	----	----	----	----

planId	path	long	是	计划主键	42
page	query	int	否	页码 (从 1 起)	1
pageSize	query	int	否	每页条数 (≤100)	20

4.3.8.3. 修改复习计划

简要描述

- 仅计划拥有者可改；支持增删题、调整间隔

请求 URL

- /api/v1/user/reviewPlan/{planId}

请求方法

- PUT

参数名	位置	类型	必选	描述	示例
planId	path	long	是	计划主键	42
name	body	string	否	新名称	春招强化版
addQuestionIds	body	array<long>	否	新增错题 ID	\[128,129]
removeQuestionIds	body	array<long>	否	移除错题 ID	\[123]
intervals	body	array<int>	否	全新闻隔序列	\[1,2,4,7,15]

4.3.8.4. 复习提醒

简要描述

- 返回当日/逾期待复习任务概览，供首页小红点使用

请求 URL

- /api/v1/user/reviewPlan/reminder

请求方法

- GET

参数名	位置	类型	必选	描述	示例
todayOnly	query	bool	否	仅查今日	true

4.3.8.5. 复习记录及统计

简要描述

- 按日期/计划维度查看已完成任务统计

请求 URL

- /api/v1/user/reviewPlan/record

请求方法

- GET

参数名	位置	类型	必选	描述	示例
planId	query	long	否	指定计划（缺省查全部）	42
startDate	query	string	否	开始日期	2025-09-01

endDate	query	string	否	结束日期	2025-10-19
groupBy	query	string	否	聚合维度 date/plan	date

4.3.9 用户管理

4.3.9.1 查询用户列表

简要描述

- 分页+多条件检索，支持倒序/正序

请求 URL

- /api/v1/admin/user/list

请求方法

- GET

参数名	位置	类型	必选	描述	示例
page	query	int	否	页码 (从 1 起)	1
pageSize	query	int	否	每页条数 (≤ 200)	20
keyword	query	string	否	用户名/邮箱/手机号模糊搜索	test
role	query	string	否	角色过滤 user/admin	admin
status	query	string	否	账号状态 normal/banned	normal
sortField	query	string	否	排序字段 created_at/last_login_at	last_login_at

sortOrder	query	string	否	排序方向 asc/desc	desc
-----------	-------	--------	---	---------------	------

4.3.9.2 查看用户详情

简要描述

- 返回用户基础信息、错题统计、活跃数据

请求 URL

- /api/v1/admin/user/{userId}

请求方法

- GET

参数名	位置	类型	必选	描述	示例
userId	path	long	是	用户主键	10086

4.3.9.3 封禁/重置用户

简要描述

- 一键封禁：强制下线并禁止登录；重置后恢复

请求 URL

- /api/v1/admin/user/{userId}/status

请求方法

- PATCH

参数名	位置	类型	必选	描述	示例
userId	path	long	是	用户主键	10086
action	body	string	是	ban/unban	ban
reason	body	string	否	封禁原因 (≤255)	广告刷屏

4.3.9.4 用户活跃统计

简要描述

- 按日期区间统计日活、周活、月活折线数据

请求 URL

- /api/v1/admin/user/activeStats

请求方法

- GET

参数名	位置	类型	必选	描述	示例
startDate	query	string	是	开始日期	2025-09-01
endDate	query	string	是	结束日期	2025-10-19
dimension	query	string	否	统计维度 d/w/m (日/周/月)	d

4.3.9.5 用户错题统计

简要描述

- 返回各用户错题总量、语言分布、最近 7 日新增

请求 URL

- /api/v1/admin/user/errorQuestionStats

请求方法

- GET

参数名	位置	类型	必选	描述	示例
page	query	int	否	页码	1
pageSize	query	int	否	每页条数 (≤ 100)	50
top	query	int	否	返回前 N 名 (与分页二选一)	20

4.3.10 数据概览

4.3.10.1 错题总览

简要描述

- 全局错题量级、语言/难度/错误类型分布饼图数据

请求 URL

- /api/v1/admin/overview/errorQuestion

请求方法

- GET

参数名	位置	类型	必选	描述	示例
language	query	string	否	按语言过滤	python
difficulty	query	string	否	按难度过滤	hard
errorType	query	string	否	按错误类型过滤	逻辑错误

4.3.10.2 用户活跃总览

简要描述

- 注册趋势、日活/周活/月活、留存率折线数据

请求 URL

- /api/v1/admin/overview/user

请求方法

- GET

参数名	位置	类型	必选	描述	示例
startDate	query	string	是	开始日期	2025-07-01
endDate	query	string	是	结束日期	2025-10-19

dimension	query	string	否	统计粒度 d/w/m	w
-----------	-------	--------	---	------------	---

4.3.10.3 语言分布统计

简要描述

- 近 30 日各语言新增错题量、占比、同比增幅

请求 URL

- /api/v1/admin/overview/language

请求方法

- GET

参数名	位置	类型	必选	描述	示例
recentDays	query	int	否	最近天数 (默认 30)	30
compare	query	bool	否	是否返回环比数据	true

4.3.11 标签管理

4.3.11.1 查看已有标签

简要描述

- 分页返回系统全部标签，含引用次数、创建时间

请求 URL

- /api/v1/admin/tag/list

请求方法

- GET

参数名	位置	类型	必选	描述	示例
page	query	int	否	页码 (从 1 起)	1
pageSize	query	int	否	每页条数 (≤ 200)	50
keyword	query	string	否	标签名模糊搜索	递归
sortField	query	string	否	排序字段 ref_count/created_at	ref_count
sortOrder	query	string	否	排序方向 asc/desc	desc

4.3.11.2 新增标签

简要描述

- 管理员创建全局标签，自动去重

请求 URL

- /api/v1/admin/tag

请求方法

- POST

参数名	位置	类型	必选	描述	示例
name	body	string	是	标签名 ≤20 字	动态规划
color	body	string	否	十六进制颜色	#007bff

4.3.11.3 修改标签

简要描述

- 重命名或更换颜色，同步更新用户错题关联

请求 URL

- /api/v1/admin/tag/{tagId}

请求方法

- PUT

参数名	位置	类型	必选	描述	示例
tagId	path	long	是	标签主键	15
name	body	string	否	新名称 ≤20 字	贪心
color	body	string	否	新颜色	#28a745

4.3.11.4 删除标签

简要描述

- 仅当未被任何错题引用时才可物理删除；否则返回 422

请求 URL

- /api/v1/admin/tag/{tagId}

请求方法

- DELETE

参数名	位置	类型	必选	描述	示例
tagId	path	long	是	标签主键	15

4.3.12 系统维护

4.3.12.1 查看系统日志

简要描述:

- 分页检索运行日志与错误日志

请求 URL:

- /api/v1/admin/system/log

请求方式:

- GET

参数名	位置	类型	必选	描述	示例
page	query	int	否	页码 (从 1 起)	1

pageSize	query	int	否	每页条数 (≤500)	50
logLevel	query	string	否	日志级别 INFO/WARN/ERROR	ERROR
startTime	query	string	否	开始时间 (ISO8601)	2025-09-01T00:00:00Z
endTime	query	string	否	结束时间 (ISO8601)	2025-10-19T23:59:59Z

4.3.12.2 数据备份

简要描述:

- 立即触发全库备份并返回下载链接

请求 URL:

- /api/v1/admin/system/backup

请求方式:

- POST

参数名	位置	类型	必选	描述	示例
backupType	query	string	否	备份类型 full/incremental	full

4.3.12.3 数据恢复

简要描述:

- 上传备份文件执行恢复

请求 URL:

- /api/v1/admin/system/restore

请求方式:

- POST

参数名	位置	类型	必选	描述	示例
file	form	file	是	备份文件 (.sql/.zip)	-

5. 权限设计

(1) 系统管理员 (System Administrator)

全局数据修改权限: 可以对所有错题、用户、日志表执行任意增删改查操作, 不受行级限制。

数据库结构修改权限: 可创建、修改或删除数据库、表、索引、视图、存储过程、触发器, 也可调整字段类型与约束。

用户和角色管理权限: 能够创建、修改、删除数据库账户, 授予或回收任意权限, 维护角色与权限的映射关系。

系统监控与维护权限: 可执行全量/增量备份、时点恢复、性能监控、杀进程、flush 日志、修改数据库参数等运维命令。

审计日志访问权限: 拥有审计表 (audit_log) 及相关系统表的查询与导出权, 可追踪所有登录与权限变更事件。

(2) 数据库管理员 (Database Administrator)

数据库结构修改权限：可在业务库内新增、修改、删除表结构与索引，进行分区或性能优化。

数据查询与修改权限：能读写生产库所有业务数据，用于统计、修复或批量订正。

用户权限管理权限：可对业务相关账号授予或回收对象级（表级/列级）SELECT/INSERT/UPDATE/DELETE 权限。

数据备份与恢复权限：可发起逻辑或物理备份，执行整体或单表恢复，并验证备份完整性。

(3) 开发者 (Developer)

数据查询权限：在测试库可读取全部表结构及数据，用于接口调试与单元测试。

数据修改权限（受限）：仅允许在测试环境执行 INSERT/UPDATE/DELETE；对生产库仅有只读权。

数据库结构查询权限：可查看表结构、索引、视图定义，方便编写 SQL 与 ORM 映射。

调试与诊断权限：可使用 EXPLAIN、SHOW PROFILE、慢查询日志等工具进行性能诊断，禁止直接修改线上数据。

(4) 普通用户 (User)

数据查询权限（受限）：通过行级视图仅能看到属于自己的错题、复习记录与个人信息。

数据修改权限（受限）：只能对自有数据执行 INSERT/UPDATE/DELETE；禁止批量导出全表。

数据导出权限（受限）：经应用层授权后，可导出个人错题集为 CSV/PDF，单次上限 1000 条。

6. 安全性、健壮性与可扩展性

6.1. 安全性

6.1.1. 防 SQL 注入

防止 SQL 注入是确保数据库安全的关键环节，它要求开发者在设计和实现数据库交互功能时，采取一系列预防措施来抵御攻击者通过输入恶意 SQL 代码来操控数据库的行为。SQL 注入攻击通常发生在应用程序未能对用户输入进行充分验证和过滤的情况下，攻击者可以在输入框中插入或“注入”恶意的 SQL 语句，从而绕过正常的安全控制，执行非法的数据库查询、更新或删除操作，甚至可能窃取、篡改或破坏数据库中的敏感数据。

为防止 SQL 注入，需要确保所有用户输入都被视为潜在的攻击源，并对其严格的验证和过滤。这包括检查输入数据的格式、类型和长度，以及使用适当的转义字符来处理特殊字符，以防止它们被解释为 SQL 语句的一部分。此外，采用参数化查询或预编译语句是防止 SQL 注入的最有效方法之一，因为它们允许将用户输入作为参数传递给 SQL 语句，而不是直接将其拼接到 SQL 代码中，从而避免了恶意输入被解释为 SQL 命令的风险。

同时，还应遵循最小权限原则，为数据库用户分配最小必要的权限，以降低 SQL 注入攻击成功后的潜在危害。通过这些综合措施的实施，可以有效地保护数据库免受 SQL 注入攻击的威胁。

6.1.2. CSRF 防御

防御 CSRF（跨站请求伪造）攻击需采取多层次的安全措施。首先，验证 HTTP Referer 字段是一个基本方法，通过检查请求的来源地址，判断其是否来自可信的网站。然而，Referer 字段并非总是可靠，因为它可以被伪造或在某些情况下被省略。

更为有效的方法是使用 CSRF Token。服务器在用户登录时为其生成一个唯一的 Token，并将其存储在用户会话中。每当用户提交表单或进行敏感操作时，服务器要求客户端在请求中包含这个 Token，并进行验证。这种方法可以确保请求的真实性和合法性，是防御 CSRF 攻击的最佳实践。

此外，自定义 HTTP 头验证、双因素身份验证、严格的安全策略、输入验证和过滤也是重要的防御手段。自定义 HTTP 头验证通过在请求中添加额外的验证信息来增加安全性；多因素身份验证（MFA）对于敏感操作提供了额外的安全保障；严格的安全策略如内容安全策略和 HTTP 严格传输安全策略，可以减少攻击者利用漏洞的机会；输入验证和过滤则能确保用户输入的数据格式和类型符合预期，防止恶意数据的注入。

最后，定期更新和维护应用程序和依赖库，以修复已知的安全漏洞，也是防御 CSRF 攻击的重要一环。同时，对数据库进行定期备份和恢复测试，可以在发生安全事件时迅速恢复数据，减少损失。综上所述，通过采取这些多层次的安全防护措施，可以有效地降低 CSRF 攻击的风险。

6.1.3. XSS 防御

XSS（Cross-Site Scripting，跨站脚本攻击）是一种网络安全漏洞，它允许攻击者将恶意脚本代码注入到正常的网页中，当用户访问这些被注入恶意代码的网页时，脚本会在用户的浏览器中执行。这些恶意脚本可以窃取用户的敏感信息，如 cookies、session IDs 等，从而劫持用户会话，模拟用户身份执行非法操作。此外，XSS 攻击还可以用于钓鱼攻击，诱导用户输入敏感信息，或者恶意重定向用户到恶意网站，破坏页面结构并显示虚假信息。

为了有效防御 XSS 攻击，需要采取一系列措施。首先，对用户输入的数据进行严格的验证和过滤是关键。通过检查输入数据的长度、字符类型等，并过滤掉可能导致脚本执行的特殊字符，可以有效防止恶意脚本的注入。同时，对输出到页面的内容进行适当的编码处理，如将 HTML 特殊字符进行转义，可以防止恶意脚本在浏览器中执行。

此外，使用安全的 HTTP 头部也是防御 XSS 攻击的重要手段。例如，设置 Content-Security-Policy（CSP）HTTP 头部，可以限制网页上能执行的脚本和加载的资源，从而阻止恶意脚本的执行。同时，定期更新应用程序及其依赖的库和框架，以修复已知漏洞，也是必不可少的。健壮性

6.1.4. DDOS 防御

对于 DDOS 攻击，本产品打算采用 Sentinel 作为防御手段。

Sentinel 作为一个高可用、高扩展、高稳定性的开源流量控制和熔断降级框架，主要通过其流量控制功能来防御 DDoS（分布式拒绝服务）攻击。

DDoS 攻击的原理是通过发送大量请求来占用系统资源，导致服务无法响应正常请求。而 Sentinel 能够实时监控服务的调用情况，根据预定义的规则对流量进行限制。这些规则可以基于多种维度来设置，如每秒查询率（QPS）、线程数等，从而确保服务在面临异常流量时能够保持稳定。

在实际应用中，Sentinel 通过定义流控规则来限制服务的请求量。当服务的请求量超过预设的阈值时，Sentinel 会触发相应的流控策略。这些策略包括但不限于直接拒绝请求、延迟处理请求或进行流量整形等。通过这些策略，Sentinel 能够有效地减缓 DDoS 攻击对后端服务的影响，保护服务不被过载崩溃。

此外，Sentinel 还支持多种流控模式，如快速失败、预热（Warm Up）和匀速排队等。这些模式可以根据服务的实际情况和攻击的特点进行灵活配置，从而进一步增强防御 DDoS 攻击的效果。例如，在预热模式下，服务在启动时会有一个逐渐增加流量的过程，这有助于防止服务在启动时因突然增加的流量而崩溃。

6.1.5. 多因素认证

MFA（Multi-Factor Authentication，多因素认证）是一种先进的身份验证机制，它要求用户在登录或进行敏感操作时提供两种或更多不同类型的身份验证因素，从而显著提升账户的安全性。其中，基于时间的一次性密码（Time-Based One-Time Password，TOTP）算法是 MFA 中常用的一种技术。

TOTP 算法的核心在于结合时间变量生成一次性密码，这种密码仅在特定时间段内有效，过期即失效。具体而言，TOTP 算法基于预共享的密钥和当前时间戳生成一次性密码。用户在初始化 MFA 时，会在身份验证应用中设置一个密钥，这个密钥只有用户和认证服务器知道。认证服务器和用户的身份验证应用会根据固定的时间步长（通常为 30 秒）生成一次性密码。使用 HMAC-SHA1 算法，将当前时间戳除以时间步长得到一个计数值，然后使用密钥对计数值进行哈希计算，得到的哈希结果就是一次性密码的一部分。

在认证过程中，用户的身份验证应用会显示生成的一次性密码，用户需要在一定时间内使用这个密码进行登录或认证。当用户输入一次性密码后，认证服务器会在当前时间戳的前后几个时间步长内计算一次性密码，并与用户输入的密码进行比较。如果匹配，则认证成功；如果不匹配，则认证失败。

由于 TOTP 算法生成的一次性密码具有时效性，且每次生成的密码都不同，因此即使密码被泄露，攻击者也无法在有效时间内再次使用。此外，由于动态口令只存在于用户绑定的设备上，攻击者难以通过网络攻击获取到动态口令。这些因素共同使得 MFA 采用 TOTP 算法能够为用户提供更为安全的身份验证机制。

6.1.6. 用户密码安全

为了防止用户密码泄露，可以采取 MD5 加密入库与用户密码加盐的综合防护方法。

首先，MD5 加密是一种广泛应用的哈希算法，它可以将任意长度的数据转换为固定长度的哈希值。在用户注册时，系统可以获取用户输入的明文密码，并使

用 MD5 算法对其进行加密处理，然后将加密后的哈希值存储到数据库中。这样，即使数据库被攻击者非法访问，他们也无法直接获取用户的明文密码。

然而，MD5 加密也存在一定的安全风险，如碰撞漏洞等。为了进一步提高密码的安全性，可以采用加盐的方法。具体而言，在加密用户密码之前，先生成一个随机的盐值，并将其与用户密码进行拼接。然后，对拼接后的字符串进行 MD5 加密处理，并将加密后的哈希值以及盐值一起存储到数据库中。这样，即使两个用户使用了相同的密码，由于盐值的不同，他们在数据库中存储的哈希值也会不同。

6.1.7. 基于 RSA 的用户数据保护

RSA 加密算法在保护用户聊天信息方面发挥着至关重要的作用。作为一种非对称加密算法，RSA 使用一对密钥——公钥和私钥，来确保信息的机密性和完整性。

在用户聊天场景中，RSA 加密的应用主要体现在信息的传输过程中。发送方会使用接收方的公钥对聊天信息进行加密，生成一段无法被轻易解读的密文。这段密文在传输过程中即使被第三方截获，也无法直接获取其中的原始信息，因为解密需要接收方的私钥，而私钥是保密的，仅由接收方掌握。

当接收方收到这段密文后，会使用自己的私钥进行解密，还原出原始的聊天信息。这种加密解密的过程确保了只有真正的信息接收者才能解读聊天内容，从而有效防止了信息泄露的风险。

RSA 算法的安全性主要基于大数分解的数学难题，即给定一个大合数（由两个大质数相乘得到），目前没有已知的高效算法能够在合理时间内分解出它的质因数。因此，在合理选择密钥长度和参数的情况下，RSA 算法具有很高的安全性。此外，RSA 算法还可以用于数字签名，确保信息的完整性和来源的可靠性。发送方可以使用自己的私钥对聊天信息进行签名，接收方使用发送方的公钥进行验证。如果签名验证通过，说明信息在传输过程中没有被篡改，且确实来自声称的发送方。

6.2. 健壮性

6.2.1. 状态码

除了 HTTP 协议中的几个基本状态码以外，本产品保证每个请求都能在响应 JSON 中获取状态码与状态信息。状态码能够清晰地传达请求的处理结果。无论是成功还是失败，后端都可以通过返回特定的状态码来告知前端请求的处理状态。这对于前端开发者来说，是判断后续操作的重要依据。

考虑到用户体验，通过返回明确的状态码和相应的错误信息，前端可以为用户提供更加友好的错误提示。这不仅可以减少用户的困惑和不满，还可以提高用户对系统的信任度和满意度。一个基本的状态码如下：

```
{  
  
  "code": 1001,  
  
  "msg": "系统内部错误"  
  
}
```

6.2.2. 响应时间

本产品对所有接口的响应设置超时时间，并在超时后抛出异常同时在用户界面显示错误信息。

设置超时时间能够防止系统因长时间等待响应而陷入僵死状态。在异步请求中，如果后端服务处理时间过长或出现故障，前端可能会一直等待响应，导致用户界面无法继续操作。通过设置超时时间，系统能够在等待超过一定时长后自动中断请求，避免资源被无效占用，从而保持系统的响应性和可用性。

超时后抛出异常并显示错误信息，有助于快速定位和解决问题。当请求超时后，系统能够立即捕捉到异常，并通过用户界面向用户展示错误信息。这不仅可以让用户了解请求失败的原因，还可以为开发者提供调试和排查问题的线索，从而加快问题的解决速度。通过及时显示错误信息，用户能够了解请求失败的原因，并采取相应的措施。同时，这也能够向用户展示系统对于异常情况的处理能力，增强用户对系统的信任度和满意度。

6.2.3. 数据库操作限制

在实际应用中，若不对接口操作数据库表项的数量加以控制，可能会导致数据库负载过高，进而影响其响应时间。特别是在高并发场景下，大量接口请求同时访问数据库，若每个请求都涉及大量表项操作，数据库将难以承受如此巨大的压力，响应时间将显著延长，甚至可能导致系统崩溃。

通过限制接口对数据库表项的操作数量，可以有效避免数据库过载，确保其响应时间保持在合理范围内。这一措施能够防止因数据库负载过高而导致的性能瓶颈，从而维护系统的稳定性和可靠性。

限制接口操作数量还有助于提升系统的可扩展性和容错性。在系统设计时，可以预留一定的冗余资源，以应对突发的高并发请求。当数据库操作请求激增时，系统可以通过动态调整接口操作限制，确保数据库在高负载下仍能保持稳定运行。同时，这一措施还能为数据库维护和数据备份等操作提供便利，进一步提升系统的健壮性。

6.2.4. 输入检测

对所有输入内容进行检测限制，是提升系统健壮性的重要手段。通过对输入内容进行严格的校验，可以及时发现并处理超出输入范围或不符合要求的内容，避免其引发系统错误或异常。这种预防措施能够显著降低系统因输入问题而崩溃或表现异常的风险，提升系统的稳定性和可靠性。同时，向用户提供清晰的输入提示，也能增强用户体验，减少因输入错误而导致的操作失败。

6.2.5. 数据转换

对数据格式转换的处理过程进行详尽的规划和明确，是确保系统健壮性的关键环节。明确数据转换前后的格式，能够确保数据在传输和处理过程中保持一致的语义和结构，避免因格式不匹配而导致的解析错误或数据丢失。这有助于维护数据的完整性和准确性，提升系统的可靠性。转换规则不仅指导数据如何从一个格式转变为另一个格式，还确保转换过程中的逻辑正确性和一致性。这有助于避免数据在转换过程中被错误地修改或解释，从而减少系统错误和异常的发生。边界值处理能够确保系统在处理极端或特殊数据时不会崩溃或表现异常，从而增强系统的稳定性和容错能力。

6.3. 可扩展性

6.3.1. 系统功能模块化

在功能模块的设计与开发过程中，高内聚低耦合的原则被视为构建高效、可维护且可扩展系统的基石。这一原则不仅关乎当前系统的稳定性与性能，更为未来的业务扩展和技术升级奠定了坚实的基础。

高内聚强调的是模块内部功能的紧密关联与协同工作。一个高度内聚的模块，其内部组件和函数应紧密围绕一个核心目标或功能进行组织，共同实现该目标。这样的设计使得模块内部逻辑清晰、结构紧凑，易于理解和维护。同时，高内聚还能减少模块间的交互复杂度，降低因模块间通信不畅或误解而导致的错误率。当需要对某个功能进行改进或优化时，只需关注该模块内部，无需过多考虑与其他模块的交互，从而提高了开发效率和系统的稳定性。

低耦合则要求模块之间的依赖关系尽可能简单、松散。一个低耦合的系统，

其模块间的交互应尽可能通过标准化的接口或协议进行，避免直接依赖对方的具体实现。这样的设计使得模块间的依赖关系更加清晰、易于管理，同时也为系统的未来扩展提供了更大的灵活性。当需要添加新功能或修改现有功能时，只需关注相关模块，无需对整个系统进行大规模的重构或调整。

在遵循高内聚低耦合原则的基础上，设计功能模块时还需充分考虑未来业务的扩展需求。随着业务的不断发展，系统可能需要从单体式架构向分布式架构转型，以适应更高的并发量和更复杂的业务场景。因此，在设计之初就应引入分布式系统的思想，如微服务架构、事件驱动架构等，为系统的未来扩展预留足够的空间。

为实现这一目标，可以采取一系列技术手段来增强系统的可扩展性。例如，通过接口抽象和依赖注入技术，可以降低模块间的直接依赖关系，使得系统在面对新业务需求时更加灵活和可配置。同时，模块化设计也是提升系统可扩展性的重要手段之一。通过将系统划分为多个独立的模块，每个模块都可以独立开发、测试和维护，从而降低了系统的整体复杂度，提高了开发效率和系统的可维护性。