【外部】飞书安全 - Blog站点

房超 王霖 | 昨天修改

AI 速览

本文讨论了飞书安全的Blog站点项目，该项目作为"开发者最佳练手项目"，旨在锻炼学生多方面设计能力以发掘优秀学生，介绍了项目交付清单、考核标准等内容。关键要点包括：

1. **项目交付**：交付内容有Blog站点WEB端、需求分析等文档类、项目源代码，汇报演示非必须。
2. **普通用户注册**：可通过用户名、密码或手机号+验证码注册，有格式校验、唯一性校验等安全防护，注册成功3 - 5s跳转至登录页。
3. **普通用户登录**：支持账密或手机号+验证码登录，1min内连续登录失败超3次需滑块验证，可正常退登。
4. **普通用户Blog操作**：创作有富文本编辑器，发布需内容检测；可编辑/删除自有文章，支持文章导出PDF、关键词搜索文章，个人空间可修改部分信息。
5. **管理员内容管理**：维护敏感词库，可下架文章，用户可重新编辑发布。
6. **管理员账号管理**：可查看账号信息、新增、踢蹬、封禁、解封、查询账号。
7. **异常感知与指导课程**：超管可查询账号异常登录信息；指导课程涵盖RESTful API设计等多方面知识。

项目背景

Blog站点作为"开发者最佳练手项目"，涵盖用户体系、内容管理、个人中心等通用模块，其技术方案可无缝迁移至电商、社交、CMS等复杂场景。互联网产品核心架构与博客系统存在技术同源性，通过该项目旨在锻炼学生的前端/后端/算法等多方面的设计能力，从而发掘优秀学生。

项目交付

交付清单

- 产品
  - Blog站点WEB端
- 文档类
  - 需求分析文档；
  - 框架设计与流程设计；
  - 项目管理文档；
  - 其他技术会议文档整理；
- 代码
  - 项目源代码；
- 汇报演示（非必须，如有更好）
  - 以 PPT 或 文档形式，包括：产品介绍、分工、设计思路、思考复盘等；

考核标准

评价标准（合格-60分）	评价标准（优秀-80分）	评价标准（超出期望-90分以上）
• **普通用户视角** ◦ **注册模块** 用户可以自行通过用户名、密码进行注册，注册成功后，3-5s可自动跳转至登录页； ▪ 格式校验： • 字段规则：如用户名长度（6-20字符）、密码复杂度（含大小写字母+数字，长度6-16） ▪ 唯一性校验：提交前需查询是否存在同名用户，若存在则提示"用户名已占用" ▪ 安全防护： • 密码禁止明文存储	• **普通用户视角** ◦ **注册模块** 用户可以自行通过用户名、密码进行注册，注册成功后，3-5s可自动跳转至登录页； ▪ 格式校验： • 字段规则：如用户名长度（6-20字符）、密码复杂度（含大小写字母+数字，长度6-16） • 前端实时提示：通过JavaScript动态检测输入合法性 ▪ 唯一性校验：提交前需查询是否存在同名用户，若存在则提示"用户名已占用"	• **普通用户视角** ◦ **注册模块** 用户可以自行通过用户名、密码进行注 注册成功后，3-5s可自动跳转至登录页 ▪ 格式校验： • 字段规则：如用户名长度（6- 符）、密码复杂度（含大小写 +数字，长度6-16） • 前端实时提示：通过JavaScrip 检测输入合法性 ▪ 唯一性校验：提交前需查询是否有 名用户，若存在则提示"用户名已占

- **登录模块**
  - 账密登录：普通用户能够使用自己注册的用户名/密码进行登录
    - 登录时，如果1min内连续登录失败超过3次，后续登录时，需要做 滑块验证，验证成功后才可做登录逻辑；
  - 可以在使用完平台功能后，正常退登；
- **Blog内容创作**
  - Blog创作：
    - 提供富文本编辑器（支持Markdown语法、图片上传、代码高亮），可设置文章分类/标签，支持草稿自动保存
    - 发布时，需要自动做内容检测，仅当内容满足安全合规的要求时，才可完成发布；否则，给出当前内容不合规的原因提示用户进行更正；
  - 内容管理：
    - 用户可编辑/删除自有文章，操作需二次确认。
  - Blog查看
    - 登录后可以正常查看到 其账号下自己管理的Blog列表；
- **个人空间：**
  - 用户头像、简介、注册时间
  - 可修改密码/头像/简介

- **管理员视角**
  - **Blog内容管理**
    - 可主动下架某篇文章，下架后用户侧可重新编辑后再次发布
  - **账号管理**
    - 账号列表：超管可以看到目前平台侧允许登录的所有账号信息，涉及 基本信息、当前是否已登录的信息；
    - 新增账号：超管可以在平台创建账号，并将账号信息分享给有需要的普通用户；
    - 账号踢蹬：超管可以针对疑似被盗用的账号进行踢蹬处理，踢蹬后、用户侧会被重定向到登录页；
    - 账号封禁：超管可以针对恶意账号做封禁处理，封禁后、用户侧会被重定向到登录页，并且用户再次登录时，提示账号已被封禁，无法正常登录；
    - 账号解封：超管可以针对已封禁的账号进行解封，账号解封后，可以完成正常的用户登录流程；
    - 账号查询：可以指定账号查看账号详情，比如注册时间等等；
  - **异常感知**
    - 账号异常登录
      - 超管可以查询指定时间范围内，发生过账号异常登录的信息；账号异常登录指：在较短的时间内（如1min）发生3次账号密码错误的登录失败问题；

- 安全防护：
  - 防止自动化脚本批量注册
  - 密码禁止明文存储
- **登录模块**
  - 账密登录：普通用户能够使用自己注册的用户名/密码进行登录
    - 登录时，如果1min内连续登录失败超过3次，后续登录时，需要做 滑块验证，验证成功后才可做登录逻辑；
  - 可以在使用完平台功能后，正常退登；
- **Blog内容创作**
  - Blog创作：
    - 提供富文本编辑器（支持Markdown语法、图片上传、代码高亮），可设置文章分类/标签，支持草稿自动保存
    - 发布时，需要自动做内容检测，仅当内容满足安全合规的要求时，才可完成发布；否则，给出当前内容不合规的原因提示用户进行更正；
  - 内容管理：
    - 用户可编辑/删除自有文章，操作需二次确认。
  - Blog查看
    - 登录后可以正常查看到 其账号下自己管理的 Blog列表；
- **个人空间：**
  - 用户头像、简介、注册时间
  - 可修改密码/头像/简介

- **管理员视角**
  - **Blog内容管理**
    - 维护敏感词库，用于发布时文章合规检测
    - 可主动下架某篇文章，下架后用户侧可重新编辑后再次发布
  - **账号管理**
    - 账号列表：超管可以看到目前平台侧允许登录的所有账号信息，涉及 基本信息、当前是否已登录的信息；
    - 新增账号：超管可以在平台创建账号，并将账号信息分享给有需要的普通用户；
    - 账号踢蹬：超管可以针对疑似被盗用的账号进行踢蹬处理，踢蹬后、用户侧会被重定向到登录页；
    - 账号封禁：超管可以针对恶意账号做封禁处理，封禁后、用户侧会被重定向到登录页，并且用户再次登录时，提示账号已被封禁，无法正常登录；
    - 账号解封：超管可以针对已封禁的账号进行解封，账号解封后，可以完成正常的用户登录流程；
    - 账号查询：可以指定账号查看账号详情，比如注册时间等等；
  - **异常感知**
    - 账号异常登录
      - 超管可以查询指定时间范围内，发生过账号异常登录的信息；账号异常登录指：在较短的时间内（如2min）发生3次账号密码错误的登录失败问题；

- 安全防护：
  - 防止自动化脚本批量注册
  - 密码禁止明文存储
  - 支持手机号+验证码注册
- **登录模块**
  - 账密登录：普通用户能够使用自己的用户名/密码进行登录
    - 登录时，如果1min内连续登录超过3次，后续登录时，需要做块验证，验证成功后才可做登辑；
    - 支持手机号+验证码登录
  - 可以在使用完平台功能后，正常退
- **Blog内容创作**
  - Blog创作：
    - 提供富文本编辑器（支持Mark语法、图片上传、代码高亮），设置文章分类/标签，支持草稿保存
    - 发布时，需要自动做内容检测当内容满足安全合规的要求时可完成发布；否则，给出当前不合规的原因提示用户进行更
  - 内容管理：
    - 用户可编辑/删除自有文章，二次确认。
    - 支持文章导出为PDF格式
  - Blog查看
    - 登录后可以正常查看到 其账号己管理的 Blog列表；
    - 支持关键词搜索相关文章
- **个人空间：**
  - 用户头像、简介、注册时间
  - 可修改密码/头像/简介

- **管理员视角**
  - **Blog内容管理**
    - 维护敏感词库，用于发布时文章合测
    - 可主动下架某篇文章，下架后用户重新编辑后再次发布
  - **账号管理**
    - 账号列表：超管可以看到目前平台许登录的所有账号信息，涉及 基本息、当前是否已登录的信息；
    - 新增账号：超管可以在平台创建账并将账号信息分享给有需要的普通户；
    - 账号踢蹬：超管可以针对疑似被盗账号进行踢蹬处理，踢蹬后、用户被重定向到登录页；
    - 账号封禁：超管可以针对恶意账号禁处理，封禁后、用户侧会被重定登录页，并且用户再次登录时，提号已被封禁，无法正常登录；
    - 账号解封：超管可以针对已封禁的进行解封，账号解封后，可以完成的用户登录流程；
    - 账号查询：可以指定账号查看账号情，比如注册时间等等；

- **异常感知**
  - 账号异常登录
    - 超管可以查询指定时间范围内
      生过账号异常登录的信息；账
      常登录指：在较短的时间内（
      2min）发生3次账号密码错误
      失败问题；

指导课程：

1. RESTful API设计原则
   a. HTTP方法规范
   b. 状态码语义化
2. 系统安全专题
   a. 密码存储
      i. 彩虹表攻击
      ii. 加盐方式
   b. CSRF/CSS 攻击与防御
3. 项目部署与运维
   a. Docker容器化部署
4. 敏捷开发与流程
   a. Git 使用
   b. 单元测试