Easy云盘Web应用安全性防护方案

1. 安全性隐患深度分析

**核心功能风险**

|  |  |
| --- | --- |
| **功能模块** | **主要安全隐患** |
| **用户认证** | **弱密码策略、会话劫持风险、多设备登录缺乏验证** |
| **文件上传** | **恶意文件上传（木马/脚本）、分片注入攻击、未限制文件类型和大小** |
| **文件分享** | **分享链接可预测性、未授权访问、XSS注入风险（分享描述）** |
| **回收站机制** | **权限绕过（访问他人回收站）、软删除文件未物理隔离** |
| **文件预览** | **恶意文件解析漏洞（Office/PDF）、目录遍历风险** |
| **数据库交互** | **SQL注入风险（文件搜索/用户管理）、敏感数据泄露** |

OWASP Top 10相关风险

1. 失效的访问控制（文件权限、回收站访问）

2. 加密机制失效（密码存储、传输加密）

3. 注入漏洞（SQL/XSS）

4. 不安全设计（分享链接生成机制）

5. 安全配置错误（服务器信息泄露）

二、防护策略体系

1. 认证授权安全强化

**密码安全策略**：

* 强制8位以上复杂密码（字母+数字+特殊字符）
* BCrypt高强度加密存储（工作因子≥12）
* 登录失败5次锁定账户30分钟

**会话管理**：

* HTTPS强制传输
* 会话固定防护（登录后更新Session ID）
* 闲置30分钟自动退出

**多设备管理**：

* 新设备登录需短信验证
* 实时显示在线设备列表
* 支持远程会话终止

2. 文件操作安全

**上传防护**：

* 文件类型白名单（仅允许文档/图片/视频）
* 单文件大小限制（≤2GB）
* 病毒扫描引擎（ClamAV集成）

**分享安全**：

* 不可预测分享链接（UUID+时间戳哈希）
* 分享有效期控制（默认7天）
* 密码保护选项（敏感文件）

**回收站加固**：

* 物理隔离存储（专用安全分区）
* 严格权限验证（仅所有者可访问）
* 自动清理机制（30天后永久删除）

3. 注入攻击防护

**SQL注入防护**：

* 全站参数化查询
* 敏感字符过滤（'; --等）
* 最小化数据库权限

**XSS防护**：

* 输入输出双重过滤
* CSP（内容安全策略）头部署
* 富文本内容沙箱处理

4. 安全基础设施

**网络层：**

* WAF（Web应用防火墙）部署
* DDoS防护服务
* 定期端口扫描

**服务器安全：**

* 最小化开放端口
* 定期安全补丁更新
* 关键目录写权限禁用

**监控审计**：

* 异常操作实时告警
* 完整操作日志记录
* 月度安全审计报告

三、安全性测试方案

1. 核心测试用例

|  |  |  |
| --- | --- | --- |
| 测试类型 | 测试场景 |  |
| XSS | 文件评论插入`<script>alert(1)</script>` | 显示转义文本，无脚本执行 |
| SQL注入 | 文件搜索输入`' OR 1=1--` | 返回0结果或错误页面 |
| CSRF | 伪造删除文件请求（无CSRF Token） | 拒绝执行并记录异常 |
| 权限提升 | 普通用户直接访问管理员API | 403权限不足 |

**漏洞修复流程**

典型漏洞处理

|  |  |
| --- | --- |
| 漏洞类型 | 修复方案 |
| XSS | 部署全局XSS过滤器 + CSP策略 + 输出编码 |
| SQL注入 | 启用预编译语句 + 数据库操作审计 + 错误信息模糊化 |
| 文件泄露 | 禁用目录列表 + 资源访问权限校验 + 敏感路径屏蔽 |
| 配置泄露 | 关闭调试模式 + 自定义错误页面 + 服务器信息隐藏 |
| CSRF | 全站启用Anti-CSRF Token + 关键操作二次验证 |

|