Secure File Sharing Application - Risk Assessment Report

Project Title: Secure File Sharing App

Team: Mohsin Wazir

Sagar kumar

Ibrahim Imran

Zain Ali

Executive Summary

This report evaluates the risk profile of a secure file-sharing web application using IriusRisk-generated threat modeling. It documents the current and projected threats across key system components and outlines recommended security countermeasures.

Components Analyzed

- API Service
- Authentication & Authorization Module
- AWS S3
- Browser
- Login & Logout
- Other Database
- Password Manager
- User Interface

Current Risk Summary

Each component in the system is exposed to multiple threats categorized under STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege). Below are key highlights:

API Service

-Risks: Input tampering, SSRF, insecure authentication, insufficient logging, DoS.

-Status: All threats are in "Expose" state.

- Countermeasures: Parameterized queries, rate limiting, strong encryption, comprehensive logging.

Authentication & Authorization

- Risks: Elevation of privilege, SQL injections, session hijacking.

- Countermeasures: Role-based access, encryption, rate limiting, MFA.

AWS S3

- Risks: Information disclosure, misconfigurations, inadequate monitoring.

- Countermeasures: Server-side encryption, IAM-based access, AWS Macie, S3 Access Logs.

Browser

- Risks: Phishing, XSS, MitM attacks, clickjacking.

- Countermeasures: Anti-phishing, HTTPS, X-Frame-Options, CSP.

Login/Logout

- Risks: Broken auth, session fixation, CSRF.

- Countermeasures: MFA, secure logout, CSRF protection, session invalidation.

Database

- Risks: Data leakage, SQLi, outdated software.

- Countermeasures: TLS encryption, hardened configurations, parameterized queries.

Password Manager

- Risks: Data loss, privilege escalation, outdated components.

- Countermeasures: Backups, 2FA, regular updates.

User Interface

- Risks: Clickjacking, DoS, XSS.

- Countermeasures: CSP, input sanitization, load balancing.

Security Recommendations

- Enforce TLS 1.3 across all components.

- Enable audit logs using CloudWatch and CloudTrail.

- Regularly test for OWASP Top 10 vulnerabilities.

- Use AWS WAF for traffic filtering.

- Implement time-limited, signed file access URLs.

📉 Risk Ratings Overview

Component	Inherent Risk	Current Risk	Projected Risk
API Service	**Critical**	**Critical**	**Critical**
Auth Module	**High**	**High**	**High**
AWS S3	**Critical**	**Critical**	**Critical**
Browser	**Critical**	**Critical**	**Critical**
Login	**Critical**	**Critical**	**Critical**
Logout	**High**	**High**	**High**
DB	**Critical**	**Critical**	**Critical**
UI	**Critical**	**Critical**	**Critical**

✅ Conclusion

The secure file-sharing system currently operates under high inherent and current risk conditions. Implementation of the recommended countermeasures is essential to reducing the risk to an acceptable level. The projected risk, while still significant, can be mitigated through continuous security assessment, automation, and DevSecOps practices.