Secure File Sharing Application : security controls

Project Title: Secure File Sharing App

Team: Mohsin Wazir (2022309)

Sagar kumar (2022522)

Ibrahim Imran (2022301)

Zain Ali (2022630)

Security Controls

Authentication

- OAuth 2.0 + JWT for session handling.
- Multi-Factor Authentication (MFA) using email/OTP.

Authorization

- Role-Based Access Control (RBAC)
- Principle of Least Privilege enforced using AWS IAM roles.

Encryption

- In Transit: TLS 1.3 enforced between client-server and internal components.
- At Rest:
- AES-256 encryption for S3 objects.
- PostgreSQL encryption with pgcrypto module.

Access Control

- IAM policies for S3 bucket access.
- Database access restricted to application layer (no direct external access).

- Secure cookie attributes (HttpOnly, Secure, SameSite=Strict).

Security Design Measures

- Input Validation & Sanitization: All user inputs sanitized to prevent XSS and **SQL injection**.
- Content Security Policy (CSP): Prevents injection attacks.
- Secure Logout Mechanism: Session invalidation on logout.
- Time-Limited Access URLs: For file downloads using pre-signed URLs in S3.
- Audit Logging: User actions logged for accountability (via AWS CloudTrail).
- Security Headers: HSTS, X-Content-Type-Options, X-Frame-Options enabled