Security & Access Control

Security Overview

Security Objectives

- Protect user data and privacy
- Secure financial transactions
- Prevent unauthorised access to system resources
- Maintain data integrity and availability

Threat Model

Potential Threats:

- Unauthorised access to user accounts
- SQL injection attacks
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Session hijacking
- Brute force attacks
- Data breaches
- Payment fraud
- Malicious vendor uploads
- Denial of Service (DoS) attacks
- Man-in-the-middle attacks
- Insecure direct object references
- Information disclosure

Authentication & Authorisation

User Authentication

Registration Process:

- Strong password requirements:
  - Minimum 8 characters
  - Must contain uppercase, lowercase, number, and special character
  - Check against common password lists
  - Password strength indicator during registration
- Email verification required before account activation
- CAPTCHA on registration form to prevent bot signups
- Rate limiting on registration attempts (max 3 per hour per IP)

Session Management:

- Secure session cookies with HttpOnly and Secure flags
- SameSite=Strict cookie attribute to prevent CSRF
- Session timeout after 30 minutes of inactivity

- Absolute session timeout after 24 hours
- Session regeneration after authentication
- Logout clears all session data
- Concurrent session limit: 3 active sessions per user
- Device tracking for suspicious login detection

Password Reset:

- Password reset via email with time-limited token (1 hour expiry)
- Token single-use only
- Secure token generation (minimum 32 bytes of random data)
- Rate limiting on password reset requests (max 3 per hour)
- Email notification when password is changed
- Previous password cannot be reused