Non-Functional Requirements (NFR) – Library Management System

Application Name: Library Management System

Project Type: Web Application

Group No: 5

1. Security

1.1 Authentication and Authorization

- Role-Based Access: The system defines roles such as Member and Admin, each with defined permissions.
- Access Restrictions: Members can only manage their own accounts and transactions. Admins manage inventory, complaints, and reports.

1.2 Password Security

- Passwords are encrypted using standards like bcrypt.
- First-time login requires changing default credentials.
- Password strength enforced: minimum 8 characters, uppercase, lowercase, number, special character.

1.3 Data Protection

- SQL Injection Protection via parameterized queries.
- XSS Protection through input sanitization.
- Session Management includes login session handling and inactivity timeouts.
- Redirects are validated to trusted URLs only.

2. Navigation & User Interface

2.1 User-Friendly Navigation

- Fixed navigation bar includes role-based modules.
- Clear navigation for Members (Home, Books, Donate, Profile) and Admins (Dashboard, Management Panels).

2.2 Flow Management

- Members access only their own data.
- Admins access and manage entire system content.

3. Performance

3.1 System Responsiveness

- Page load time < 2 seconds.
- Search and transactions respond within 1 second under normal conditions.

3.2 Query Optimization

- Indexed queries used for efficient retrieval.
- Pagination used in listings and reports.

4. Consistent UI

- Standard font, button, and color themes across all pages.
- Real-time field validation with standard error messages.

5. Exception Handling

- Use of try-catch for backend processes.
- Friendly error messages; no internal details exposed.

6. Validation and Input Handling

6.1 Client-Side Validation

- Real-time validation on forms with helpful error prompts.

6.2 Server-Side Validation

- All user inputs are validated again on the server before saving.

6.3 Error Feedback

- Inline error messages near the form fields for guidance.

7. Data Management

7.1 Data Integrity

- All transactions are tied to valid users.
- Soft delete used for complaints and member data.

7.2 Data Backup

- Daily automated backups configured.

7.3 Audit Logs

- Log of major operations with timestamps maintained.

8. Scalability & Maintainability

- Modular MVC architecture supports extensibility.
- Admin panel supports filtering, sorting, and bulk actions.

9. Cross-Browser & Platform Compatibility

- Tested on Chrome, Firefox, Edge (desktop and mobile).
- Responsive UI supports desktop, tablet, and mobile views.

10. Compliance and Usability

10.1 Usability
- Tooltips, placeholders, and confirmation dialogs enhance usability.

10.2 Compliance
- Follows general security and data privacy guidelines.