CIE406 – Keamanan Informasi
Vulnerability Assessment Report
Library Management System

1. Overview
This document analyzes potential vulnerabilities in the Laravel 12 + Filament-based Library Management System and the countermeasures implemented to protect the application.

2. Authentication & Authorization
Risk: Unauthorized users accessing protected areas.
Mitigation: Laravel's auth system and middleware ensure only valid sessions access protected routes.

3. Input Validation
Risk: SQL Injection, XSS attacks.
Mitigation: Laravel uses Eloquent ORM and built-in validation; Filament also sanitizes input fields.

4. Password Storage
Risk: Plain-text password leaks.
Mitigation: Laravel hashes passwords using bcrypt by default.

5. Role Escalation
Risk: Users manipulating requests to gain admin access.
Mitigation: Authorization policies and middleware prevent access without correct roles.

6. File Upload / Exposure
Risk: Sensitive files (env, config) being publicly accessible.
Mitigation: Laravel's folder structure isolates public and private files; `.env` never committed.

7. Logging and Monitoring
Risk: Undetected misuse or attacks.
Mitigation: Actions such as borrowing/returning are logged; Laravel's logs provide history.

8. Conclusion
The system implements strong default protections from Laravel + Filament. Remaining risks can be mitigated further with rate-limiting, audit trails, and real-time monitoring in production.