RISK ASSESSMENT

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **TITOLO** | **LIVELLO SEVERITA’** | **ASSET COINVOLTO** | **IMPATTO** | **PROBABILITA’** | **AZIONE** |
| Errori nella gestione dello stato letto/non letto | **Medio** | **Database, logica backend** | Visualizzazione e filtraggio errati | **Alta** | Test approfonditi, validazione stato al salvataggio |
| Perdita dati o corruzione del catalogo | **Alto** | Database (es: SQLite, Mongo) | Perdita definitiva dei dati utente | **Bassa** | Backup regolari, meccanismi di rollback e controlli di integrità |
| Vulnerabilità lato client (XSS, CSRF) | **Alto** | Interfaccia utente | Possibili attacchi a sessione utente o furto dati | **Media** | Input sanitization, token CSRF, header di sicurezza |
| Accessi non autorizzati alla modifica dei libri | **Alto** | Autenticazione/autorizzazione | Modifica o cancellazione non autorizzata | **Media** | Implementare login sicuro, autorizzazioni per ruolo utente |
| Interfaccia utente poco chiara per gestione stato e filtri | **Medio** | **Frontend** | Esperienza utente compromessa | **Alta** | Test con utenti, interfaccia intuitiva, feedback visivo sullo stato dei libri |
| Problemi di compatibilità tra browser | **Bassa** | Frontend (HTML/CSS/JS) | Rendering scorretto o malfunzionamenti | **Media** | Test cross-browser, uso di framework standard (Bootstrap, React, ecc.) |
| Cache del browser obsoleta | **Bassa** | |  | | --- | |  | | Cache lato client | | Visualizzazione temporanea di dati non aggiornati | **Media** | Forzare refresh o utilizzare versioning risorse statiche |

TITOLO: Gestione errata delle statistiche

LIVELLO SEVERITA’: Medio

ASSET COINVOLTO: Database, logica backend

IMPATTO: Statistiche non affidabili o errate

PROBABILITA’: Media

AZIONE: Test unitari su calcolo statistiche, validazione dati

TITOLO: Vulnerabilità nella gestione delle impostazioni utente

LIVELLO SEVERITA’: Alto

ASSET COINVOLTO: Backend, DB

IMPATTO: Possibile esposizione dati personali

PROBABILITA’: Media

AZIONE: Controlli di sicurezza, crittografia dei dati sensibili

TITOLO: Debolezza nella procedura di cambio password

LIVELLO SEVERITA’: Alto

ASSET COINVOLTO: Autenticazione

IMPATTO: Accessi non autorizzati se la procedura non è sicura

PROBABILITA’: Media

AZIONE: Forzare password robuste