

BookShelf — Open Tickets

AI Workshop · May 2026

These tickets are intentionally prepared for the workshop. Participants will use Claude Code (with `codebase-memory` MCP indexed) to investigate and fix.

BUG-001 — Search endpoint can be exploited

Labels	SECURITY HIGH
Reporter:	Security team
Affected:	GET /books?q=...

A pentest flagged the books search as vulnerable. Sending the query string:
`?q=' UNION SELECT username, password, NULL, NULL, NULL, NULL, NULL FROM users--`
returns user records, including passwords.

Expected: Search must not allow arbitrary SQL. Use parameterized queries.

BUG-002 — Borrowing a book never reduces available copies

Labels	DATA HIGH
Reporter:	Librarian (Bu Sari)
Affected:	POST /loans

Members keep borrowing the same single-copy book and the system never says "no copies left". Looking at the DB, `books.available_copies` is never decremented when a loan is created.

Expected: Creating a loan must atomically decrement `available_copies`. Refuse the loan if already 0.

BUG-003 — Users list pagination skips the first page

Labels	LOGIC MEDIUM
Reporter:	Admin (Pak Budi)
Affected:	GET /users?page=1&per_page=10

`page=1` returns users 11-20 instead of 1-10. `page=0` returns 1-10 (but admins don't think to pass 0). Some users on small pages get skipped.

Expected: `page=1` returns the first `per_page` records. Stop at the last page.

FEATURE-001 — Return book endpoint with overdue fine

Type:	Feature Request
Requested by:	Library operations

Add `POST /loans/:id/return` that:

- Sets `loans.returned_date = now`
- Increments `books.available_copies` by 1
- Calculates overdue fine using `utils/helpers.js -> calc_fine`
- Returns `{ ok: true, fine: <number> }`
- Only the owner of the loan or an admin can return it

FEATURE-002 — CSV export of all loans (admin)

Type:	Feature Request
Requested by:	Finance

Add `GET /loans/export.csv` (admin only) that returns a CSV file with columns:

```
loan_id, username, book_title, borrowed_date, due_date, returned_date,
overdue_days, fine
```

Hints for Trainers

- BUG-001 and BUG-003 require reading multiple files: routes + db helpers. Great showcase for codebase-memory MCP.
- BUG-002 is simple once you understand the loan flow — a good "first win" for participants.
- FEATURE-001 requires stitching helpers + routes + auth + db — perfect Lab 5 chained-skill task.
- FEATURE-002 is the stretch goal.