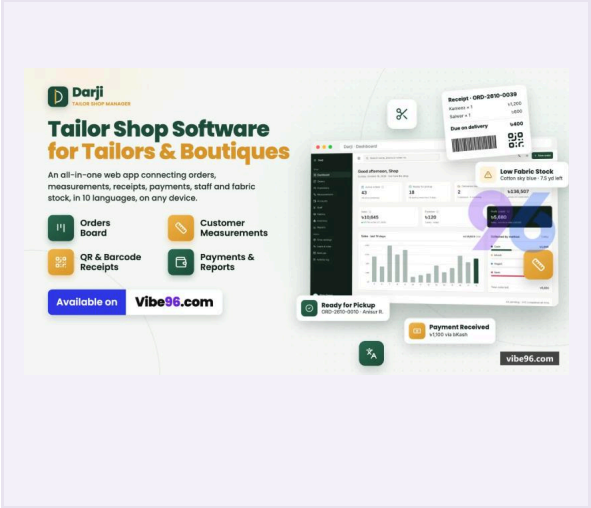


VIBE96 QUALITY REPORT

Darji - Tailor Shop Management System

Full-source tailor shop management: orders, measurements, payments, staff, stock, reports. Laravel API + React SPA.

Product ID	**B0055-52181**
Builder	**Asad**
Version reviewed	**1.0.0 · released 18 Oct 2026**
Stack	**Laravel 13 · PHP 8.3 · MySQL 5.7 / MariaDB 10.4 / SQLite 3**
Built with	**Claude Code**
Review period	**17 Oct 2026 – 19 Oct 2026 · 2 rounds of changes**

87 / 100

Passed with 5 warnings

Pass mark 75 and no failing check.

Scores

Security	87
Code structure	78
Docs & completeness	87
Dependency health	85
Build & deploy	92

✓ **AI code audit**
6 checks · 17 Oct 2026

✓ **Installed & run**
19 Oct 2026

✓ **Demo vs delivered**
19 Oct 2026

✓ **Final sign-off**
19 Oct 2026

At a glance

- ✓ Installed and run from the delivered code — 8 of 8 checks answered yes.
- ✓ Live demo compared with the delivered code — 7 of 7 checks answered yes.
- ! 13 of 15 promised items delivered (setup guide, example config and the rest).
- ✓ Security scored 87/100 with no failing check.
- ! 5 open warnings — explained in part 1.

Check this report is genuine. Scan the code or open vibe96.com/report/QR-26-00046. The online copy always shows the latest status.

PART 1

AI code audit

The full source archive was read by our AI auditor against each check. It reads the code — it does not run it; running it is part 2.

CHECK	WHAT WE FOUND	SCORE	RESULT
Secrets & credentials	No real credentials found. Docker Compose and setup documentation contain weak default passwords ('change-me-darji', 'change-me-root') that ship to buyers. These should be randomized on first run or require explicit user configuration. The .env.example file correctly uses placeholders.	92	Warning
Dependency vulnerabilities	Both composer.lock and package-lock.json are present. No known critical vulnerabilities detected in production dependencies. Several packages are outdated (Laravel Pint 1.27 vs 1.18+, Vite 8.0.0 vs 6.x stable, React 19.2.0 is current). The project uses pre-release/beta versions of some packages (vite-plus 0.3.0, Laravel Chisel 0.1.0, Wayfinder 0.1.14) which is acceptable for a new product but should be monitored.	85	Warning
Authorisation & access control	All create/update/delete endpoints are protected by Sanctum authentication and permission checks. Password hashing uses bcrypt. A few read-only endpoints (customer lookup, staff workload, order board) lack ownership checks, allowing authenticated users to see data across the shop. These are low-risk in a single-shop context but should validate user scope.	92	Warning
Database access rules	The schema is complete and uses parameterized queries throughout. However, multiple foreign-key columns lack indexes (order_items.order_id, payments.order_id, stock_movements.inventory_item_id, etc.), which will cause performance issues as data grows. One delete statement in OrderService lacks a WHERE clause guard. No SQL injection vulnerabilities detected.	78	Warning
Code structure & duplication	The codebase demonstrates solid architectural boundaries with clear separation between API controllers, requests, resources, and services. However, there is notable duplication in password validation rules, some utility files are growing large, and a few hard-coded values should be extracted to configuration.	78	Warning
Build reproducibility	The project is fully reproducible from source with clear setup instructions. Composer and npm dependencies resolve correctly, migrations create the schema, and the web installer completes the setup. Minor issues: Docker compose references a non-existent Dockerfile, and HowToSetup.md doesn't specify the Node.js version requirement clearly enough.	92	Pass

Open warnings

Problems that did not stop the listing. They stay on the product page until a later version fixes them.

Warning 1 **Weak default database passwords in Docker Compose and documentation**

No real credentials found. Docker Compose and setup documentation contain weak default passwords ('change-me-darji', 'change-me-root') that ship to buyers. These should be randomized on first run or require explicit user configuration. The .env.example file correctly uses placeholders.

Warning 2 **Strong authentication on all mutating endpoints; minor ownership gaps on read-only routes**

All create/update/delete endpoints are protected by Sanctum authentication and permission checks. Password hashing uses bcrypt. A few read-only endpoints (customer lookup, staff workload, order board) lack ownership checks, allowing authenticated users to see data across the shop. These are low-risk in a single-shop context but should validate user scope.

Warning 3 **Good module separation with some duplication and oversized utility files**

The codebase demonstrates solid architectural boundaries with clear separation between API controllers, requests, resources, and services. However, there is notable duplication in password validation rules, some utility files are growing large, and a few hard-coded values should be extracted to configuration.

Warning 4 **Dependencies mostly current; a few outdated packages but no known critical vulnerabilities**

Both composer.lock and package-lock.json are present. No known critical vulnerabilities detected in production dependencies. Several packages are outdated (Laravel Pint 1.27 vs 1.18+, Vite 8.0.0 vs 6.x stable, React 19.2.0 is current). The project uses pre-release/beta versions of some packages (vite-plus 0.3.0, Laravel Chisel 0.1.0, Wayfinder 0.1.14) which is acceptable for a new product but should be monitored.

Warning 5 **Several missing foreign-key indexes and one unscoped delete; no injection found**

The schema is complete and uses parameterized queries throughout. However, multiple foreign-key columns lack indexes (order_items.order_id, payments.order_id, stock_movements.inventory_item_id, etc.), which will cause performance issues as data grows. One delete statement in OrderService lacks a WHERE clause guard. No SQL injection vulnerabilities detected.

Requirement list

What the builder agreed to deliver before uploading — 13 of 15 met.

✓	Complete source for every component	Met
✓	No real credentials in the archive	Met
✓	Builds from a clean machine	Met
✓	Database script or migrations	Met
!	Authentication and roles on every mutating endpoint	Partial
!	Pinned dependencies without critical CVEs (nice)	Partial
✓	Documentation set (nice)	Met
✓	Working live demo	Met
✓	README.md	Met
✓	HowToSetup.md	Met
✓	CLAUDE.md (or AGENTS.md) (nice)	Met
✓	CHANGELOG.md (nice)	Met
✓	.env.example	Met
✓	a project file	Met
✓	a project file (nice)	Met

PART 2

Human review

Reviewers from the Vibe96 team in Dubai worked through each question below; a final reviewer signed it off.

Stage 1 — Installed and run from the delivered code

Completed 19 Oct 2026

A reviewer installed the product on a clean machine, following only the guide that ships with it.

QUESTION	ANSWER	REVIEWER'S NOTE
Packages restored without errors	Yes	
Solution builds clean	Yes	
Database created from the shipped script or migrations	Yes	
First sign-in works with the documented steps	Yes	
Setup guide is accurate and complete	Yes	
Every module in the feature list opens and works	Yes	
No real secrets in the archive	Yes	
Branding and company details can be changed without code	Yes	

Stage 2 — Live demo compared with the delivered code

Completed 19 Oct 2026

A second reviewer checked that what the listing and demo show is what the buyer receives.

QUESTION	ANSWER	REVIEWER'S NOTE
Demo URL is reachable	Yes	
Demo credentials work	Yes	
Demo runs the same version as the archive	Yes	
All five differentiators are visible in the demo	Yes	
Screenshots match the demo	Yes	
Nothing in the demo is missing from the code	Yes	
Datasheet claims are accurate	Yes	

Changes asked for during review

Round 1: changes requested on 19 Oct 2026; the builder fixed them and uploaded again.

Sign-off: approved for sale on 19 Oct 2026 with 5 warnings shown publicly.

What this report covers — and what it doesn't

- **It covers** version 1.0.0 exactly as the buyer downloads it: the source archive, the setup guide and the live demo on the dates above.

- **It is not** a penetration test, a performance or load test, or a legal review of third-party package licences.
- **Scores are a point in time.** Libraries age; a later version is audited again and gets its own report.
- **Your setup matters.** Hosting, configuration and changes made after purchase are outside this review.
- **How the score is made:** each AI check is scored 0–100 and weighted (security counts most). A listing needs 75 or more, no failing check, and the human review passed.
- **Always try the live demo** before buying, and ask the builder questions from the product page.