Tillora - Multi-Tenant POS & Inventory SaaS

VIBE96 QUALITY REPORT

Tillora - Multi-Tenant POS & Inventory SaaS

Multi-tenant point-of-sale and inventory platform for running your own retail subscription business

Product ID	**B0055-72183**
Builder	**Asad**
Version reviewed	**1.0.0 · released 18 Oct 2026**
Stack	**Laravel 13.0 · PHP 8.3 · MySQL 8.0 / MariaDB 10.5**
Built with	**Claude Code**
Review period	**17 Oct 2026 – 19 Oct 2026**

81 / 100

Passed with 6 warnings

Pass mark 75 and no failing check.

Scores

Security	82
Code structure	72
Docs & completeness	100
Dependency health	85
Build & deploy	78

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

✓ **Installed & run**
19 Oct 2026

✓ **Demo vs delivered**
18 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.
- ✓ 15 of 15 promised items delivered (setup guide, example config and the rest).
- ✓ Security scored 82/100 with no failing check.
- ! 6 open warnings — explained in part 1.

Check this report is genuine. Scan the code or open vibe96.com/report/QR-26-00043. 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 API keys or secrets found. However, weak default passwords ('change-me-db', 'change-me-root') ship in docker-compose.yml and demo account credentials ('password') are documented in multiple files. These defaults could be deployed unchanged by buyers who skip the setup guide.	75	Warning
Dependency vulnerabilities	Both PHP (composer.lock) and Node.js (a project file) lockfiles are present and committed. No known critical vulnerabilities detected in the declared versions. Several packages are outdated (Laravel 13.0 is current, Stripe PHP SDK, Next.js 16.4.0, React 19.3.0 are recent). A few dev dependencies could be updated but pose no security risk. No wildcard or unpinned production dependencies found.	85	Warning
Authorisation & access control	All mutating endpoints are properly guarded with Sanctum auth and role middleware. Passwords use bcrypt. Route permission enforcement is active. Minor issues: a few read endpoints (customer display token lookup, some admin list routes) lack explicit ownership checks, and the public customer display endpoint accepts tokens without rate limiting.	92	Warning
Database access rules	The codebase uses parameterized queries and Eloquent ORM correctly, avoiding SQL injection. However, multiple controllers perform delete/update operations without explicit tenant or user scoping (relying on global scopes that can be bypassed). Additionally, many foreign key columns in migrations lack indexes, which will cause performance issues at scale. No plain-text password storage detected.	78	Warning
Code structure & duplication	The codebase demonstrates good architectural separation with clear service/repository layers, but contains notable duplication in token handling, permission checking, and API response patterns. Several files exceed 400 lines and could benefit from extraction. Hard-coded values are mostly confined to config files, though some magic strings appear in controllers.	72	Warning
Build reproducibility	The project can be built from source but HowToSetup.md omits the frontend build step (npm run build in Tillora/frontend/) before starting the server, risking a 404 for /app. Docker compose references TILLORA_DB_PASSWORD/ ROOT_PASSWORD without documenting them in .env.example or the setup guide. No lockfile version pins for npm (package-lock.json missing from digest). Setup steps are otherwise correct.	78	Warning

Open warnings

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

Warning 1 **Dependencies mostly current; a few outdated packages but no known critical vulnerabilities**

Both PHP (composer.lock) and Node.js (a project file) lockfiles are present and committed. No known critical vulnerabilities detected in the declared versions. Several packages are outdated (Laravel 13.0 is current, Stripe PHP SDK, Next.js 16.4.0, React 19.3.0 are recent). A few dev dependencies could be updated but pose no security risk. No wildcard or unpinned production dependencies found.

Warning 2 **Weak default credentials and demo passwords ship to production buyers**

No real API keys or secrets found. However, weak default passwords ('change-me-db', 'change-me-root') ship in docker-compose.yml and demo account credentials ('password') are documented in multiple files. These defaults could be deployed unchanged by buyers who skip the setup guide.

Warning 3 **Moderate code duplication and some oversized files; business logic generally well-separated**

The codebase demonstrates good architectural separation with clear service/repository layers, but contains notable duplication in token handling, permission checking, and API response patterns. Several files exceed 400 lines and could benefit from extraction. Hard-coded values are mostly confined to config files, though some magic strings appear in controllers.

Warning 4 **Several unscoped deletes/updates and missing indexes on foreign keys reduce safety**

The codebase uses parameterized queries and Eloquent ORM correctly, avoiding SQL injection. However, multiple controllers perform delete/update operations without explicit tenant or user scoping (relying on global scopes that can be bypassed). Additionally, many foreign key columns in migrations lack indexes, which will cause performance issues at scale. No plain-text password storage detected.

Warning 5 **Strong auth/authz with minor ownership gaps on read endpoints and one public display token route**

All mutating endpoints are properly guarded with Sanctum auth and role middleware. Passwords use bcrypt. Route permission enforcement is active. Minor issues: a few read endpoints (customer display token lookup, some admin list routes) lack explicit ownership checks, and the public customer display endpoint accepts tokens without rate limiting.

Warning 6 **Build reproducible with gaps: missing frontend build in setup, Docker env unclear, no version pins**

The project can be built from source but HowToSetup.md omits the frontend build step (npm run build in Tillora/frontend/) before starting the server, risking a 404 for /app. Docker compose references TILLORA_DB_PASSWORD/ROOT_PASSWORD without documenting them in .env.example or the setup guide. No lockfile version pins for npm (package-lock.json missing from digest). Setup steps are otherwise correct.

Requirement list

What the builder agreed to deliver before uploading — 15 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	Met
✓	Pinned dependencies without critical CVEs (nice)	Met
✓	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 18 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

None — approved on the first round.

Sign-off: approved for sale on 19 Oct 2026 with 6 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.