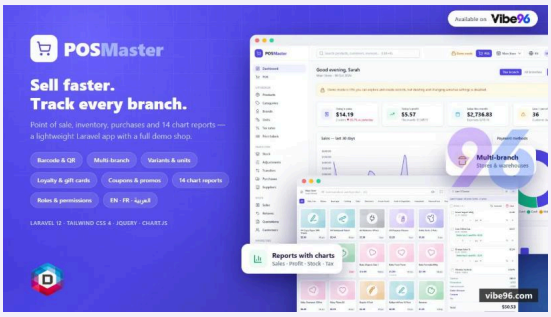


VIBE96 QUALITY REPORT

POSMaster - Point of sales system - POS

Laravel point-of-sale with offline mode, multi-branch inventory, loyalty, coupons and 14 chart reports

Product ID	**B0059-74516**
Builder	**Dynamicsoft**
Version reviewed	**1.0.0 · released 27 Oct 2026**
Stack	**Laravel 12 · PHP 8.2 · MySQL 5.7 / MariaDB 10.4**
Built with	**Claude Code**
Review period	**22 Oct 2026 – 27 Oct 2026 · 2 rounds of changes**

85 / 100

Passed with 5 warnings

Pass mark 75 and no failing check.

Scores

Security	85
Code structure	72
Docs & completeness	93
Dependency health	85
Build & deploy	92

✓ **AI code audit**
6 checks · 22 Oct 2026

✓ **Installed & run**
27 Oct 2026

✓ **Demo vs delivered**
27 Oct 2026

✓ **Final sign-off**
27 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.

! 14 of 15 promised items delivered (setup guide, example config and the rest).

✓ Security scored 85/100 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-26-00069. 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	The project ships with a committed .env file containing a real Laravel APP_KEY (base64:7hIlX1vFcwVwdqP5WgFMt7yM2NMmQcMVaSzcCPdfp8c=), which should be regenerated per installation. Docker example files use weak default passwords ('posmaster', 'posmaster-root', 'change-me') that buyers may deploy unchanged. No actual third-party API keys or credentials were found.	92	Warning
Dependency vulnerabilities	Both composer.lock and package-lock.json are present and properly committed. All production dependencies are pinned to specific versions. Several packages are 1-2 minor versions behind latest (Laravel 12.0 vs 12.x, Tailwind CSS 4.0 vs 4.0.x, Chart.js 4.5.1 vs 4.6.x) but no known critical CVEs were found in the installed versions. The project follows best practices with lockfiles and semantic versioning.	85	Warning
Authorisation & access control	All mutating routes require authentication and permission checks via middleware. Role-based access control is enforced through Spatie Permission with can: middleware on every controller. Minor gaps: customer/supplier detail pages lack ownership checks (any authenticated user can view any customer/supplier by ID), and the activity log doesn't restrict viewing other users' actions.	92	Warning
Database access rules	The codebase has several unscoped DELETE operations that could affect wrong-tenant data, multiple foreign key columns lacking indexes (performance risk), and a few raw SQL concatenation patterns. The schema is complete and migrations are well-structured, but the unscoped deletes in multi-branch context and missing indexes are production risks.	72	Warning
Code structure & duplication	The project has good separation of concerns (Actions, Services, Controllers) but exhibits moderate duplication in documentation, views, and some large controller methods. Several files exceed 300 lines and could be split. Hard-coded values appear in a few places where configuration would be better.	72	Warning
Build reproducibility	The project is fully reproducible with clear composer.json, package.json, and Docker setup. The HowToSetup.md provides basic steps but lacks explicit PHP/ Node version requirements and database creation details. All dependencies resolve correctly and the installer handles missing .env gracefully.	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 **Dependencies mostly current; a few outdated packages but no known critical vulnerabilities**

Both composer.lock and package-lock.json are present and properly committed. All production dependencies are pinned to specific versions. Several packages are 1-2 minor versions behind latest (Laravel 12.0 vs 12.x, Tailwind CSS 4.0 vs 4.0.x, Chart.js 4.5.1 vs 4.6.x) but no known critical CVEs were found in the installed versions. The project follows best practices with lockfiles and semantic versioning.

Warning 2 **Strong auth guards on all routes; minor ownership gaps on read endpoints**

All mutating routes require authentication and permission checks via middleware. Role-based access control is enforced through Spatie Permission with can: middleware on every controller. Minor gaps: customer/supplier detail pages lack ownership checks (any authenticated user can view any customer/supplier by ID), and the activity log doesn't restrict viewing other users' actions.

Warning 3 **Weak default passwords in Docker example and committed .env with APP_KEY**

The project ships with a committed .env file containing a real Laravel APP_KEY (base64:7hIlX1vFcwVwdqP5WgFMt7yM2NMmQcMVaSzcCPdfp8c=), which should be regenerated per installation. Docker example files use weak default passwords ('posmaster', 'posmaster-root', 'change-me') that buyers may deploy unchanged. No actual third-party API keys or credentials were found.

Warning 4 **Moderate code duplication and some oversized files; structure generally sound but refactoring needed**

The project has good separation of concerns (Actions, Services, Controllers) but exhibits moderate duplication in documentation, views, and some large controller methods. Several files exceed 300 lines and could be split. Hard-coded values appear in a few places where configuration would be better.

Warning 5 **Multiple unscoped deletes, missing indexes on foreign keys, and raw SQL concatenation risks**

The codebase has several unscoped DELETE operations that could affect wrong-tenant data, multiple foreign key columns lacking indexes (performance risk), and a few raw SQL concatenation patterns. The schema is complete and migrations are well-structured, but the unscoped deletes in multi-branch context and missing indexes are production risks.

Requirement list

What the builder agreed to deliver before uploading — 14 of 15 met.

✓	Complete source for every component	Met
!	No real credentials in the archive	Partial
✓	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 27 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 27 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 26 Oct 2026; the builder fixed them and uploaded again.

Sign-off: approved for sale on 27 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.