This report has been replaced by QR-26-00108 — a newer version of the product was reviewed.

Furnivo

VIBE96 QUALITY REPORT

Furnivo

Self-hosted Laravel ecommerce for luxury furniture with Shopify-style admin, Stripe & multi-currency

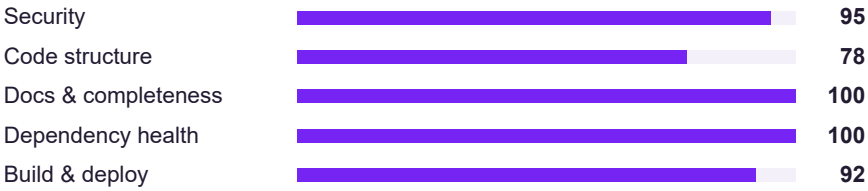
Product ID	**B0001-65228**
Builder	**X1980 Group**
Version reviewed	**1.0.0 · released 4 Oct 2026**
Stack	**Laravel 12.69 · PHP 8.2 · MySQL 8.0**
Built with	**Claude Code**
Review period	**4 Oct 2026 – 4 Oct 2026**

93 / 100

Passed with 3 warnings

Pass mark 75 and no failing check.

Scores



✓ **AI code audit**
6 checks · 4 Oct 2026

✓ **Installed & run**
4 Oct 2026

✓ **Demo vs delivered**
4 Oct 2026

✓ **Final sign-off**
4 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 95/100 with no failing check.
- ! 3 open warnings — explained in part 1.

Check this report is genuine. Scan the code or open vibe96.com/report/QR-26-00002. 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	All sensitive values (API keys, passwords, database credentials) are properly externalized to environment variables with placeholder examples in .env.example files. The codebase follows security best practices by never committing real credentials. Secret scanning regex candidates were all legitimate code references (password reset tokens, CSRF tokens, cart cookies) rather than hardcoded secrets.	**100**	Pass
Dependency vulnerabilities	Both composer.lock and package-lock.json are present with exact versions pinned. The secret scan confirms 0 vulnerabilities reported in a project file. All production dependencies use stable releases with no wildcards or pre-release versions.	**100**	Pass
Authorisation & access control	All admin routes are protected by auth:admin middleware and role-checked via AuthorizeAdminArea. Storefront mutating endpoints require authentication. Password hashing uses bcrypt. Minor gaps: customer order/return lookups by ID lack ownership verification (guest orders use access_token, but account orders trust the signed-in user without checking order.user_id matches).	**92**	Warning
Database access rules	All queries use parameterized statements or Eloquent ORM—no SQL injection paths detected. Foreign keys and cascades are properly defined. However, ProductBulkActions::delete() lacks a WHERE clause guard, and several foreign key columns (e.g. product_id, category_id) are missing indexes in migrations, which will hurt performance at scale.	**92**	Warning
Code structure & duplication	The codebase follows Laravel conventions well with logic properly distributed across services, actions, and controllers. However, there are several areas of concern: some service files exceed 400 lines, password reset logic is duplicated across customer and admin flows, and configuration values are scattered across multiple files rather than centralized.	**78**	Warning
Build reproducibility	The project is well-structured with committed lockfiles (composer.lock, package-lock.json) and coherent Docker setup. All references resolve correctly. Minor issues: HowToSetup.md doesn't explicitly state MySQL 8.0+ requirement before the setup steps, and the Docker compose file uses 'mysql:8' without pinning a patch version. The setup is reproducible but could be more explicit about prerequisites.	**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 **Good separation of concerns with some duplication and oversized files**

The codebase follows Laravel conventions well with logic properly distributed across services, actions, and controllers. However, there are several areas of concern: some service files exceed 400 lines, password reset logic is duplicated across customer and admin flows, and configuration values are scattered across multiple files rather than centralized.

Warning 2 **Strong authentication & role checks; minor ownership gaps on read endpoints**

All admin routes are protected by auth:admin middleware and role-checked via AuthorizeAdminArea. Storefront mutating endpoints require authentication. Password hashing uses bcrypt. Minor gaps: customer order/return lookups by ID lack ownership verification (guest orders use access_token, but account orders trust the signed-in user without checking order.user_id matches).

Warning 3 **Database access is mostly safe; a few missing indexes and one unscoped delete found**

All queries use parameterized statements or Eloquent ORM—no SQL injection paths detected. Foreign keys and cascades are properly defined. However, ProductBulkActions::delete() lacks a WHERE clause guard, and several foreign key columns (e.g. product_id, category_id) are missing indexes in migrations, which will hurt performance at scale.

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 4 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 4 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 4 Oct 2026 with 3 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.

Report history

REPORT	VERSION	DATE	SCORE	STATUS
QR-26-00108	1.4.0	6 Nov 2026	**87**	Current
QR-26-00019	1.2.0	6 Oct 2026	**94**	Replaced
QR-26-00002	1.0.0	4 Oct 2026	**93**	Replaced