This report has been replaced by QR-26-00057 — a newer version of the product was reviewed.

FreshNest

VIBE96 QUALITY REPORT

FreshNest

A ready-to-sell organic grocery store in Laravel storefront, Shopify-style admin, Stripe and cash on delivery.

Product ID	**B0001-73574**
Builder	**X1980 Group**
Version reviewed	**1.0.0 · released 4 Oct 2026**
Stack	**Laravel · PHP 8.x · MySQL 8.0**
Built with	**Claude Code**
Review period	**4 Oct 2026 – 4 Oct 2026**

91 / 100

Passed with 4 warnings

Pass mark 75 and no failing check.

Scores

Security	92
Code structure	78
Docs & completeness	100
Dependency health	95
Build & deploy	92

✓ **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 92/100 with no failing check.
- ! 4 open warnings — explained in part 1.

Check this report is genuine. Scan the code or open vibe96.com/report/QR-26-00003. 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. The demo admin password 'password' is a weak default that ships to buyers (a project file). Several .env.example placeholders use realistic-looking formats that could be mistaken for real values. All database passwords, API keys and secrets are properly externalized to environment variables.	**92**	Warning
Dependency vulnerabilities	All dependencies are pinned in composer.lock and package-lock.json (both present in the archive root). No known critical vulnerabilities detected in Laravel 12.69.2, PHP 8.2+, or npm packages. A few packages are slightly outdated but pose no immediate security risk.	**95**	Pass
Authorisation & access control	All admin routes are guarded by auth:admin middleware and role-checked in AuthorizeAdminArea. Mutating endpoints require authentication. Password reset is atomic and secure. Minor gaps: customer order/address reads lack explicit ownership checks in controllers (rely on Eloquent scopes), and wishlist/cart use cookies without user binding.	**92**	Warning
Database access rules	All queries use parameterized statements or Eloquent; no SQL injection paths found. Delete and update operations are properly scoped. Schema is complete and can be created from empty. A few foreign keys lack indexes (e.g. order_items.product_id, cart_items.product_id) which will cause N+1 queries under load. Missing cascade rules on some relationships could leave orphaned records.	**92**	Warning
Code structure & duplication	The codebase demonstrates solid architectural patterns with clear service/ controller/model boundaries. However, there is notable duplication in password reset logic across storefront and admin, some large controller files, and configuration values scattered across multiple locations that could be centralized.	**78**	Warning
Build reproducibility	The project is fully reproducible: composer.lock and package-lock.json pin dependencies, vite.config.js and composer.json are coherent, and docker-compose.yml is complete. README.md provides setup steps but omits the database creation command and does not specify exact PHP/Node versions. The .env.example is comprehensive and the composer setup script automates most steps correctly.	**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 demo password default and several placeholder credentials need rotation**

No real credentials found. The demo admin password 'password' is a weak default that ships to buyers (a project file). Several .env.example placeholders use realistic-looking formats that could be mistaken for real values. All database passwords, API keys and secrets are properly externalized to environment variables.

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

All admin routes are guarded by auth:admin middleware and role-checked in AuthorizeAdminArea. Mutating endpoints require authentication. Password reset is atomic and secure. Minor gaps: customer order/address reads lack explicit ownership checks in controllers (rely on Eloquent scopes), and wishlist/cart use cookies without user binding.

Warning 3 **Database access mostly safe; minor schema gaps and a few unindexed foreign keys**

All queries use parameterized statements or Eloquent; no SQL injection paths found. Delete and update operations are properly scoped. Schema is complete and can be created from empty. A few foreign keys lack indexes (e.g. order_items.product_id, cart_items.product_id) which will cause N+1 queries under load. Missing cascade rules on some relationships could leave orphaned records.

Warning 4 **Good separation of concerns with some duplication and oversized files**

The codebase demonstrates solid architectural patterns with clear service/controller/model boundaries. However, there is notable duplication in password reset logic across storefront and admin, some large controller files, and configuration values scattered across multiple locations that could be centralized.

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 4 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-26-00057	1.1.0	23 Oct 2026	**90**	Current
QR-26-00003	1.0.0	4 Oct 2026	**91**	Replaced