This report has been replaced by QR-26-00114 — a newer version of the product was reviewed.

Look Fashion

VIBE96 QUALITY REPORT

Look Fashion

Complete fashion e-commerce platform with bilingual storefront and Shopify-style admin for clothing retailers

Product ID	**B0002-47813**
Builder	**Buildify**
Version reviewed	**1.0.0 · released 7 Oct 2026**
Stack	**Laravel 12.69 · PHP 8.2+ · MySQL 8 / MariaDB 10.11**
Built with	**Claude Code**
Review period	**7 Oct 2026 – 7 Oct 2026**

84 / 100

Listed after a manual review

Pass mark 75 and no failing check.

Scores



✓ **AI code audit**
6 checks · 7 Oct 2026

✓ **Installed & run**
7 Oct 2026

✓ **Demo vs delivered**
7 Oct 2026

✓ **Final sign-off**
7 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 92/100.
- ! 4 open warnings — explained in part 1.

Check this report is genuine. Scan the code or open vibe96.com/report/QR-26-00029. 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 archive contains only placeholders and example values. However, weak default passwords appear in demo setup commands and example environment files that could be deployed unchanged. The demo admin password mechanism and example .env files should require explicit user input before deployment.	**92**	Warning
Dependency vulnerabilities	Minor points were sent to the builder to improve; none of them stopped the listing.	**40**	Fail
Authorisation & access control	All admin routes require authentication via auth:admin middleware and role-based authorization through AuthorizeAdminArea. Storefront mutating endpoints are properly guarded. Password handling uses bcrypt with configurable rounds. Minor gaps: customer order/return lookups by ID lack ownership verification, allowing one customer to view another's data by changing the ID parameter.	**92**	Warning
Database access rules	No SQL injection or unscoped deletes found. All queries use parameter binding or Eloquent. Schema is complete with foreign keys and cascades. However, several foreign key columns lack indexes (e.g. product_id, category_id, user_id in various tables), which will hurt performance as data grows.	**92**	Warning
Code structure & duplication	The codebase demonstrates solid architectural patterns with clear service/controller/model boundaries. However, there is notable duplication in payment gateway implementations, password reset logic across guards, and some files exceed 300 lines. The structure is maintainable but could benefit from extracting common patterns.	**78**	Warning
Build reproducibility	The project is fully reproducible with clear dependencies in composer.json and package.json. HowToSetup.md provides comprehensive installation paths (XAMPP, Linux, Docker, SQL). Minor issues: the setup document doesn't specify exact PHP/Node versions matching composer.json platform requirement (8.2.0) and package.json doesn't lock Node version; Docker nginx.conf references a path that may not exist without prior setup.	**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 **Database access is safe; minor schema gaps (missing indexes on foreign keys)**

No SQL injection or unscoped deletes found. All queries use parameter binding or Eloquent. Schema is complete with foreign keys and cascades. However, several foreign key columns lack indexes (e.g. product_id, category_id, user_id in various tables), which will hurt performance as data grows.

Warning 2 **Weak default passwords in demo setup and example files**

No real credentials found. The archive contains only placeholders and example values. However, weak default passwords appear in demo setup commands and example environment files that could be deployed unchanged. The demo admin password mechanism and example .env files should require explicit user input before deployment.

Warning 3 **Strong authentication guards; minor ownership gaps on read-only customer endpoints**

All admin routes require authentication via auth:admin middleware and role-based authorization through AuthorizeAdminArea. Storefront mutating endpoints are properly guarded. Password handling uses bcrypt with configurable rounds. Minor gaps: customer order/return lookups by ID lack ownership verification, allowing one customer to view another's data by changing the ID parameter.

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 payment gateway implementations, password reset logic across guards, and some files exceed 300 lines. The structure is maintainable but could benefit from extracting common patterns.

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	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)	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 7 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 7 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 7 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-26-00114	1.9.0	11 Nov 2026	**81**	Current
QR-26-00029	1.0.0	7 Oct 2026	**84**	Replaced