Northvale

VIBE96 QUALITY REPORT

Northvale

Laravel website & CMS with six switchable homepage designs for marketing agencies and consultancies

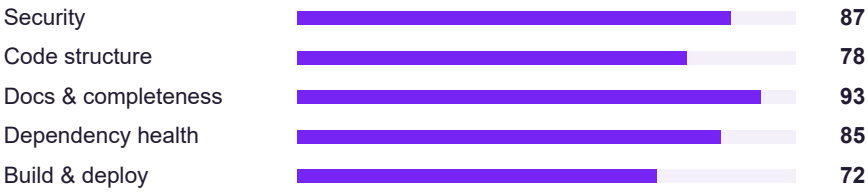
Product ID	**B0002-30326**
Builder	**Buildify**
Version reviewed	**1.0.0 · released 19 Oct 2026**
Stack	**Laravel 12 + Livewire 4 · PHP 8.2+ · MySQL 8 / MariaDB 10.6+**
Built with	**Claude Code**
Review period	**15 Oct 2026 – 19 Oct 2026**

84 / 100

Passed with 6 warnings

Pass mark 75 and no failing check.

Scores



✓ **AI code audit**
6 checks · 15 Oct 2026

✓ **Installed & run**
19 Oct 2026

✓ **Demo vs delivered**
19 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.
- ! 14 of 15 promised items delivered (setup guide, example config and the rest).
- ✓ Security scored 87/100 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-26-00045. 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. However, docker-compose.yml ships with weak default passwords ('change-me-db', 'change-me-root') that buyers might deploy unchanged. The .env.example also contains 'change-me' placeholders that are too generic. These should be replaced with stronger examples or random generation instructions.	75	Warning
Dependency vulnerabilities	The project uses Laravel 12 and Livewire 4 with recent versions. No known critical vulnerabilities detected in package.json or composer.json dependencies. However, composer.lock is missing from the digest (only composer.json provided), which prevents verification of exact installed versions. Several npm packages are slightly outdated but not vulnerable.	85	Warning
Authorisation & access control	Every admin route requires authentication via middleware and Livewire components re-check user roles on each request. Public write endpoints (contact form, newsletter, analytics beacon) are CSRF-protected, validated and rate-limited. Minor: analytics collection endpoint accepts any page_id without ownership validation, though it only increments counters and stores no user data.	95	Warning
Database access rules	All queries use Eloquent or the query builder with proper parameterization—no SQL injection paths found. One unscoped delete in the demo reset command could affect production data if demo mode is accidentally enabled. Several foreign key columns lack indexes (page_id, post_id, user_id on various tables), which will slow joins and cascades as data grows.	92	Warning
Code structure & duplication	The project has good module boundaries with clear separation between CMS rendering, admin Livewire components, and controllers. However, there is notable duplication in admin Livewire components (similar validation, toast patterns, permission checks), some large files approaching 400+ lines, and hard-coded values scattered across multiple files that should be centralized in config.	78	Warning
Build reproducibility	The archive includes compiled admin assets (public/build) but HowToSetup.md omits the Node build step entirely, creating confusion about whether npm is required. Database setup instructions are scattered and incomplete—no clear guidance on creating the database before migration. Demo mode credentials are hardcoded in docker-compose.yml and .env.example with placeholder values that could be deployed unchanged.	72	Warning

Open warnings

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

Warning 1 **Strong auth guards on all mutating endpoints; minor ownership gaps on read-only analytics**

Every admin route requires authentication via middleware and Livewire components re-check user roles on each request. Public write endpoints (contact form, newsletter, analytics beacon) are CSRF-protected, validated and rate-limited. Minor: analytics collection endpoint accepts any page_id without ownership validation, though it only increments counters and stores no user data.

Warning 2 **No critical vulnerabilities; some outdated packages and missing composer.lock**

The project uses Laravel 12 and Livewire 4 with recent versions. No known critical vulnerabilities detected in package.json or composer.json dependencies. However, composer.lock is missing from the digest (only composer.json provided), which prevents verification of exact installed versions. Several npm packages are slightly outdated but not vulnerable.

Warning 3 **Weak default passwords in docker-compose.yml and example files**

No real credentials found. However, docker-compose.yml ships with weak default passwords ('change-me-db', 'change-me-root') that buyers might deploy unchanged. The .env.example also contains 'change-me' placeholders that are too generic. These should be replaced with stronger examples or random generation instructions.

Warning 4 **Database access is mostly safe; a few missing indexes and one unscoped delete**

All queries use Eloquent or the query builder with proper parameterization—no SQL injection paths found. One unscoped delete in the demo reset command could affect production data if demo mode is accidentally enabled. Several foreign key columns lack indexes (page_id, post_id, user_id on various tables), which will slow joins and cascades as data grows.

Warning 5 **Moderate code duplication and some oversized components; generally well-structured but refactoring opportunities exist**

The project has good module boundaries with clear separation between CMS rendering, admin Livewire components, and controllers. However, there is notable duplication in admin Livewire components (similar validation, toast patterns, permission checks), some large files approaching 400+ lines, and hard-coded values scattered across multiple files that should be centralized in config.

Warning 6 **Build reproducible with gaps: missing Node build step, unclear DB setup, demo password exposed**

The archive includes compiled admin assets (public/build) but HowToSetup.md omits the Node build step entirely, creating confusion about whether npm is required. Database setup instructions are scattered and incomplete—no clear guidance on creating the database before migration. Demo mode credentials are hardcoded in docker-compose.yml and .env.example with placeholder values that could be deployed unchanged.

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 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 19 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.