

VIBE96 QUALITY REPORT

Velora - Car Rental Booking Platform

Multi-vendor car rental booking site with a self-hosted admin CMS, for rental operators and mobility marketplaces.

Product ID	**B0097-20004**
Builder	**MD FAHIM**
Version reviewed	**1.0.0 · released 29 Oct 2026**
Stack	**Next.js 16.4.3 (App Router) with React 19.2.8 · TypeScript 5.9.3 on Node.js 20+ (Dockerfile builds on Node 22 Alpine) · PostgreSQL 15+ (Neon serverless or standard Postgres; docker-compose uses postgres:16-alpine)**
Built with	**Claude Code, Google Antigravity**
Review period	**25 Oct 2026 – 29 Oct 2026 · 2 rounds of changes**

69 / 100

Listed after a manual review

Pass mark 75 and no failing check.

Scores

Security	73
Code structure	84
Docs & completeness	73
Dependency health	78
Build & deploy	38

✓ **AI code audit**
6 checks · 25 Oct 2026

✓ **Installed & run**
29 Oct 2026

✓ **Demo vs delivered**
29 Oct 2026

✓ **Final sign-off**
29 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.

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

! Security scored 73/100.

! 5 open warnings — explained in part 1.

Check this report is genuine. Scan the code or open vibe96.com/report/QR-26-00083. 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 live API keys, private keys or real connection strings were found. However, predictable default admin/vendor passwords are hard-coded as fallbacks in the seed script and the example env file, and docker-compose falls back to postgres/postgres. A buyer who runs the seed unchanged would deploy a publicly known admin login.	85	Warning
Dependency vulnerabilities	package-lock.json exists and no wildcard or latest versions are used, so installs are reproducible. However, all dependencies use caret ranges despite docs claiming pinned versions, and a few packages (@neon/config, @neon/env, next ^16.3.4) cannot be verified as legitimate or current. No known critical vulnerability could be confirmed from the manifest.	78	Warning
Authorisation & access control	The visible auth layer is solid: scrypt-style password hashing, hashed session tokens, httpOnly cookies, and role/superadmin helpers. However, the CRUD actions, admin pages, booking lookup, proxy and media route were not in the excerpts, so per-action guards and ownership checks (vendor scoping, booking lookup by reference) cannot be confirmed. Several visible weaknesses also remain, including the role-rank model and the open-redirect-style `next` handling.	62	Warning
Database access rules	The visible auth code uses Drizzle's parameterized builders with scoped deletes (session delete by hashed token) and hashed session tokens, with no injection path seen. Most data-access code (queries.ts, crud.ts, resources.ts, schema.ts, SQL files) was not in the excerpts, so tenant scoping, FK/index coverage and schema completeness are unverified. A few concrete risks are visible from the files that were shown.	72	Warning
Code structure & duplication	The project separates actions, queries, components and DB schema into distinct folders, which keeps boundaries mostly clear. The main costs are a few large mixed-concern files and hard-coded seed/fallback values, plus duplicated checkout/admin patterns that a buyer will have to maintain.	84	Warning
Build reproducibility	Minor points were sent to the builder to improve; none of them stopped the listing.	38	Fail

Open warnings

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

Warning 1 **No real credentials found; weak default passwords and DB credentials ship in seed, env example and compose**

No live API keys, private keys or real connection strings were found. However, predictable default admin/vendor passwords are hard-coded as fallbacks in the seed script and the example env file, and docker-compose falls back to postgres/postgres. A buyer who runs the seed unchanged would deploy a publicly known admin login.

Warning 2 **Reasonably structured Next.js codebase; some oversized files and hard-coded demo values to extract**

The project separates actions, queries, components and DB schema into distinct folders, which keeps boundaries mostly clear. The main costs are a few large mixed-concern files and hard-coded seed/fallback values, plus duplicated checkout/admin patterns that a buyer will have to maintain.

Warning 3 **Drizzle-parameterized access, but most DB code and the schema files were not visible, so key checks could not be confirmed**

The visible auth code uses Drizzle's parameterized builders with scoped deletes (session delete by hashed token) and hashed session tokens, with no injection path seen. Most data-access code (queries.ts, crud.ts, resources.ts, schema.ts, SQL files) was not in the excerpts, so tenant scoping, FK/index coverage and schema completeness are unverified. A few concrete risks are visible from the files that were shown.

Warning 4 **Lockfile present, but caret ranges, odd Neon packages, and pinned-claim mismatch need attention**

package-lock.json exists and no wildcard or latest versions are used, so installs are reproducible. However, all dependencies use caret ranges despite docs claiming pinned versions, and a few packages (@neon/config, @neon/env, next ^16.3.4) cannot be verified as legitimate or current. No known critical vulnerability could be confirmed from the manifest.

Warning 5 **Auth and password hashing look sound, but most routes and actions could not be verified for guards**

The visible auth layer is solid: scrypt-style password hashing, hashed session tokens, httpOnly cookies, and role/superadmin helpers. However, the CRUD actions, admin pages, booking lookup, proxy and media route were not in the excerpts, so per-action guards and ownership checks (vendor scoping, booking lookup by reference) cannot be confirmed. Several visible weaknesses also remain, including the role-rank model and the open-redirect-style `next` handling.

Requirement list

What the builder agreed to deliver before uploading — 11 of 15 met.

✓	Complete source for every component	Met
✓	No real credentials in the archive	Met
!	Builds from a clean machine	Partial
✓	Database script or migrations	Met
!	Authentication and roles on every mutating endpoint	Partial
!	Pinned dependencies without critical CVEs (nice)	Partial
✓	Documentation set (nice)	Met
!	Working live demo	Partial
✓	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 29 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 29 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 28 Oct 2026; the builder fixed them and uploaded again.

Sign-off: approved for sale on 29 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.