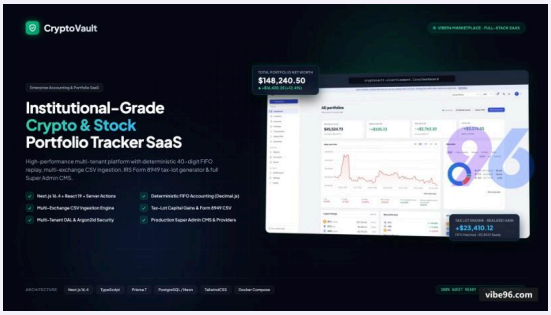


VIBE96 QUALITY REPORT

Crypto, Trading and Stock Portfolio Tracker SaaS for Investors and Multi-portfolio Holders

Multi-tenant crypto and stock portfolio tracker SaaS with FIFO/ average-cost P&L, CSV import and an admin panel.

Product ID	**B0097-80438**
Builder	**MD FAHIM**
Version reviewed	**1.0.0 · released 20 Nov 2026**
Stack	**Next.js 16.4 (App Router) with React 19.3 · TypeScript 5 on Node.js 22+ · PostgreSQL 14+ (Neon or self-hosted; Docker uses Postgres 16)**
Built with	**Claude Code, Google Antigravity**
Review period	**10 Nov 2026 – 20 Nov 2026 · 1 round of changes**

72 / 100

Listed after a manual review

Pass mark 75 and no failing check.

Scores

Security	73
Code structure	84
Docs & completeness	73
Dependency health	72
Build & deploy	62

✓ **AI code audit**
6 checks · 10 Nov 2026

✓ **Installed & run**
20 Nov 2026

✓ **Demo vs delivered**
20 Nov 2026

✓ **Final sign-off**
20 Nov 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 with no failing check.

! 5 open warnings — explained in part 1.

Check this report is genuine. Scan the code or open vibe96.com/report/QR-26-00151. 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	None of the regex candidates are real credentials: the .claude/skills hits are documentation reading process.env, and .env.example uses placeholders. However docker-compose.yml hardcodes a realistic-looking encryption key, scheduler secret, admin password and default DB/MinIO credentials that would ship to buyers and could be deployed unchanged.	80	Warning
Dependency vulnerabilities	package-lock.json exists, so installs are reproducible, and I cannot confirm any known critical (RCE / auth bypass) vulnerability in the declared versions. However, nearly all dependencies use caret ranges, some packages look suspicious (the 'cn' package, 'shadcn' in runtime deps), and the Docker image and compose file ship with default credentials. I could not verify the installed versions against advisory databases from the digest, so this is a calibrated warning.	72	Warning
Authorisation & access control	The visible architecture is sound: Argon2id password hashing, hashed session tokens, an authed() wrapper with permission keys, and a tenant-scoped DAL. The bodies of the admin actions, /internal/cron, /media/[id] and the other actions were not provided, so ownership and role checks cannot be confirmed for them. Because of that, the score is capped in the warning band.	70	Warning
Database access rules	The visible code uses Prisma ORM with a documented tenant-scoped DAL, a sensible FK cascade on Session and PasswordResetToken, and migrations plus a standalone schema.sql. The excerpts omit the DAL, raw queries (job queue FOR UPDATE SKIP LOCKED), admin actions and schema.sql, so injection safety, unscoped deletes and schema completeness cannot be confirmed. Scoring is capped until those files are reviewed.	70	Warning
Code structure & duplication	The project separates server actions, server modules, UI components and accounting logic into distinct folders, following a documented structure in CLAUDE.md. The digest is truncated, so file-size and duplication claims cannot be fully verified, and a few hard-coded values and repeated locale lists are visible.	84	Pass
Build reproducibility	The package manifest, lockfile and Prisma migrations are present, and the build script runs prisma generate before next build. However, the Dockerfile and compose file have coherence problems (no migrations, no bucket creation, dev-only DB init, source copied into the runner), and HowToSetup.md could not be verified for prerequisites or step order from the digest.	62	Warning

Open warnings

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

Warning 1 **No live credentials found; docker-compose ships weak, hardcoded default secrets and admin password**

None of the regex candidates are real credentials: the .claude/skills hits are documentation reading process.env, and .env.example uses placeholders. However docker-compose.yml hardcodes a realistic-looking encryption key, scheduler secret, admin password and default DB/MinIO credentials that would ship to buyers and could be deployed unchanged.

Warning 2 **Prisma-based access looks scoped, but most DB code was not visible and delete cascades are unverified**

The visible code uses Prisma ORM with a documented tenant-scoped DAL, a sensible FK cascade on Session and PasswordResetToken, and migrations plus a standalone schema.sql. The excerpts omit the DAL, raw queries (job queue FOR UPDATE SKIP LOCKED), admin actions and schema.sql, so injection safety, unscoped deletes and schema completeness cannot be confirmed. Scoring is capped until those files are reviewed.

Warning 3 **Authz design looks sound, but most actions and routes were not shown, so it cannot be fully verified**

The visible architecture is sound: Argon2id password hashing, hashed session tokens, an authed() wrapper with permission keys, and a tenant-scoped DAL. The bodies of the admin actions, /internal/cron, /media/[id] and the other actions were not provided, so ownership and role checks cannot be confirmed for them. Because of that, the score is capped in the warning band.

Warning 4 **Lockfile present, but caret ranges throughout and a few dated or odd packages; no confirmed critical CVE**

package-lock.json exists, so installs are reproducible, and I cannot confirm any known critical (RCE / auth bypass) vulnerability in the declared versions. However, nearly all dependencies use caret ranges, some packages look suspicious (the 'cn' package, 'shadcn' in runtime deps), and the Docker image and compose file ship with default credentials. I could not verify the installed versions against advisory databases from the digest, so this is a calibrated warning.

Warning 5 **Mostly reproducible, but Docker runner, Prisma generate path and setup doc gaps risk a failed clean build**

The package manifest, lockfile and Prisma migrations are present, and the build script runs prisma generate before next build. However, the Dockerfile and compose file have coherence problems (no migrations, no bucket creation, dev-only DB init, source copied into the runner), and HowToSetup.md could not be verified for prerequisites or step order from the digest.

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 20 Nov 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 20 Nov 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 13 Nov 2026; the builder fixed them and uploaded again.

Sign-off: approved for sale on 20 Nov 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.