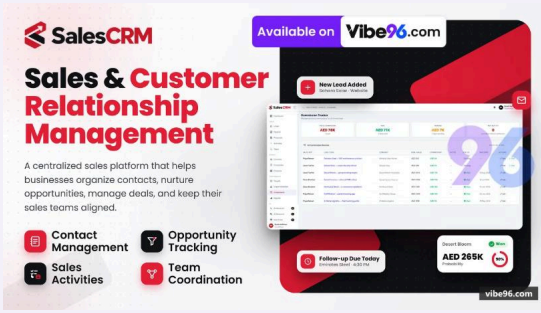


VIBE96 QUALITY REPORT

SalesCRM

Self-hosted B2B sales CRM with AI assistant, deal scoring, training academy and offline mobile app

Product ID	**B0006-53130**
Builder	**Build Nest**
Version reviewed	**1.0.0 · released 9 Oct 2026**
Stack	**Laravel 12 · PHP 8.2 · MySQL 8.0.16**
Built with	**OpenAI Codex, Claude Code**
Review period	**7 Oct 2026 – 9 Oct 2026**

93 / 100

Passed with 3 warnings

Pass mark 75 and no failing check.

Scores

Security	93
Code structure	82
Docs & completeness	100
Dependency health	100
Build & deploy	92

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

✓ **Installed & run**
7 Oct 2026

✓ **Demo vs delivered**
7 Oct 2026

✓ **Final sign-off**
9 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 93/100 with no failing check.
- ! 3 open warnings — explained in part 1.

Check this report is genuine. Scan the code or open vibe96.com/report/QR-26-00032. 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 API keys or credentials were found in the codebase. However, the .env.example files contain weak placeholder passwords ('your_secure_database_password_here' and 'your_secure_root_password_here') that could be mistaken for actual passwords by inexperienced users. All other secrets are proper placeholders or environment variable references.	**92**	Warning
Dependency vulnerabilities	composer.lock pins every dependency to exact versions. The project declares 'composer audit --locked' passes in DEPENDENCIES.md and runs it in the 'composer check' script. No known vulnerabilities found in the locked versions of Laravel 12.69, PHPUnit 11.5.57, or any transitive dependencies.	**100**	Pass
Authorisation & access control	All mutating routes are protected by authentication and role checks. Password hashing uses bcrypt. The middleware is declared both on routes and in controllers. Minor gaps: a few read-only endpoints (analytics, reports, team performance) lack explicit ownership checks, allowing any signed-in user to see team-wide data regardless of role.	**95**	Warning
Database access rules	The application uses Eloquent ORM throughout with proper scoping (visibleTo() and owner checks). All destructive operations have WHERE clauses. The schema has 73 foreign keys with cascade rules, but 3 foreign keys lack indexes. One raw SQL call in SqlFile.php is safe (reads a file, no user input). Password hashes use bcrypt, SMTP passwords are encrypted. Minor: add indexes on unindexed foreign keys.	**92**	Warning
Code structure & duplication	The project demonstrates good architectural discipline with single-responsibility classes, clear separation of concerns, and appropriate use of services and traits. However, there is some duplication in validation logic, a few hard-coded values that should be configuration, and one oversized controller that could be split.	**82**	Pass
Build reproducibility	The project is fully reproducible: composer.lock pins all dependencies, Docker setup is complete, and database schema/seed files are present. HowToSetup.md covers both server and Docker paths clearly. Minor deductions for missing explicit PHP extension installation steps in the server setup path and no mention of running the test suite to verify the build.	**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 default passwords in example files; no real credentials found**

No real API keys or credentials were found in the codebase. However, the .env.example files contain weak placeholder passwords ('your_secure_database_password_here' and 'your_secure_root_password_here') that could be mistaken for actual passwords by inexperienced users. All other secrets are proper placeholders or environment variable references.

Warning 2 **Database access is mostly safe; a few unindexed foreign keys and one raw SQL call need attention**

The application uses Eloquent ORM throughout with proper scoping (visibleTo() and owner checks). All destructive operations have WHERE clauses. The schema has 73 foreign keys with cascade rules, but 3 foreign keys lack indexes. One raw SQL call in SqlFile.php is safe (reads a file, no user input). Password hashes use bcrypt, SMTP passwords are encrypted. Minor: add indexes on unindexed foreign keys.

Warning 3 **Access control is comprehensive with minor gaps on read-only endpoints**

All mutating routes are protected by authentication and role checks. Password hashing uses bcrypt. The middleware is declared both on routes and in controllers. Minor gaps: a few read-only endpoints (analytics, reports, team performance) lack explicit ownership checks, allowing any signed-in user to see team-wide data regardless of role.

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 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 9 Oct 2026 with 3 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.