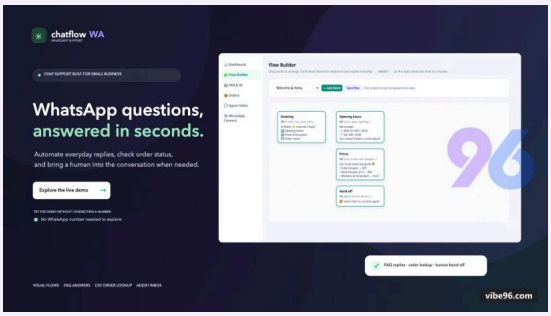


VIBE96 QUALITY REPORT

ChatFlow WA — WhatsApp Chatbot for Small Business

Self-hosted WhatsApp support bot with flow builder, FAQ AI and agent inbox for small shops and service businesses.

Product ID	**B0549-95976**
Builder	**Raj's Builder Studio**
Version reviewed	**1.0.0 · released 12 Nov 2026**
Stack	**Express 5.3.0 · JavaScript (Node.js 22+) · None: JSON file store (DATA_DIR/store.json), no SQL database**
Built with	**OpenAI Codex, Claude Code**
Review period	**3 Nov 2026 – 12 Nov 2026 · 2 rounds of changes**

72 / 100

Listed after a manual review

Pass mark 75 and no failing check.

Scores

Security	72
Code structure	42
Docs & completeness	50
Dependency health	80
Build & deploy	82

✓ **AI code audit**
6 checks · 3 Nov 2026

✓ **Installed & run**
12 Nov 2026

✓ **Demo vs delivered**
12 Nov 2026

✓ **Final sign-off**
12 Nov 2026

At a glance

! Installed and run from the delivered code — 7 of 8 checks answered yes.

✓ Live demo compared with the delivered code — 7 of 7 checks answered yes.

! 12 of 24 promised items delivered (setup guide, example config and the rest).

! Security scored 72/100 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-26-00123. 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, tokens, or private keys are committed. However, the admin password defaults to a well-known value hardcoded in server.js and pre-filled in the public login form, and a hardcoded fallback is used for session HMAC when SESSION_SECRET is unset.	82	Warning
Dependency vulnerabilities	The project has one manifest (Node a project file) and a package-lock.json, with only two production dependencies (express ^4.21.2, dotenv ^16.4.7), both current and without a known critical vulnerability. Minor issues: the Dockerfile uses npm install rather than npm ci, so the lockfile is not enforced in builds, and the lockfile contents were not available to verify installed versions.	80	Pass
Authorisation & access control	Visible admin and mutating routes (/api/admin, settings, flows, faqs, orders import, reply, resolve, analytics) use the auth middleware, and the webhook POST requires a signature. However, the single admin account uses a hardcoded fallback password compared in plaintext, the live demo pre-fills those credentials, and sessions have no CSRF or role model. Some routes are truncated in the digest and could not be fully verified.	62	Warning
Database access rules	The app uses a JSON file store (a project file) with no SQL, ORM or schema, so injection and unscoped SQL deletes do not apply. However, several admin write endpoints replace or merge whole collections from unvalidated request bodies, and the JSON file is written synchronously with no atomic write or locking, which risks data loss or corruption.	72	Warning
Code structure & duplication	The backend is one file where routing, persistence, bot matching, Meta webhook handling and OpenAI calls are interleaved, and most handlers are compressed into very long single lines. The frontend is similarly dense, with multiple views in one app.js. A buyer would struggle to change any single concern without touching the whole file.	42	Warning
Build reproducibility	The manifest, lockfile, Dockerfile and compose file are coherent, and the quick start (npm ci, copy .env, npm start) should work on Node 18+. Small gaps: Docker ignores the lockfile, there is no .dockerignore, and the webhook and persistence prerequisites are only partly spelled out. HowToSetup.md was not in the digest, so its step order could not be verified.	82	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 real credentials found; weak default admin password and session secret fallback ship to buyers**

No real API keys, tokens, or private keys are committed. However, the admin password defaults to a well-known value hardcoded in server.js and pre-filled in the public login form, and a hardcoded fallback is used for session HMAC when SESSION_SECRET is unset.

Warning 2 **Single 'server.js' holds routes, JSON store, bot logic, webhook and AI client with minified one-line handlers**

The backend is one file where routing, persistence, bot matching, Meta webhook handling and OpenAI calls are interleaved, and most handlers are compressed into very long single lines. The frontend is similarly dense, with multiple views in one app.js. A buyer would struggle to change any single concern without touching the whole file.

Warning 3 **Builds and starts from a clean machine; Docker/lockfile and setup-doc gaps**

The manifest, lockfile, Dockerfile and compose file are coherent, and the quick start (npm ci, copy .env, npm start) should work on Node 18+. Small gaps: Docker ignores the lockfile, there is no .dockerignore, and the webhook and persistence prerequisites are only partly spelled out. HowToSetup.md was not in the digest, so its step order could not be verified.

Warning 4 **No SQL, so no injection; JSON store lacks input validation and scoping on bulk writes**

The app uses a JSON file store (a project file) with no SQL, ORM or schema, so injection and unscoped SQL deletes do not apply. However, several admin write endpoints replace or merge whole collections from unvalidated request bodies, and the JSON file is written synchronously with no atomic write or locking, which risks data loss or corruption.

Warning 5 **Admin routes guarded, but default credentials, plaintext password compare and a public demo endpoint weaken access control**

Visible admin and mutating routes (/api/admin, settings, flows, faqs, orders import, reply, resolve, analytics) use the auth middleware, and the webhook POST requires a signature. However, the single admin account uses a hardcoded fallback password compared in plaintext, the live demo pre-fills those credentials, and sessions have no CSRF or role model. Some routes are truncated in the digest and could not be fully verified.

Requirement list

What the builder agreed to deliver before uploading — 12 of 24 met.

✓	Complete source in one ZIP	Met
!	Lockfile committed	Partial
✓	No real credentials	Met
!	Single example env file documented	Partial
!	HowToSetup covers two targets	Partial
!	Webhook signature verification	Partial
!	Role-gated admin and inbox	Partial
✓	Reachable demo with sample data	Met
!	Five differentiators exist in code	Partial
!	Seed data and sample CSV (nice)	Partial
!	CLAUDE.md for AI tools (nice)	Partial
!	CHANGELOG starting at 1.0.0 (nice)	Partial
!	Tests for the flow engine and webhook (nice)	Missing
!	Docs folder (optional)	Missing
✓	README.md	Met
✓	HowToSetup.md	Met
✓	Node.js a project file	Met
✓	Node.js a project file	Met
✓	.env.example	Met
✓	CLAUDE.md (nice)	Met

✓	CHANGELOG.md (nice)	Met
✓	LICENSE-NOTE.md	Met
✓	docker-compose.yml (nice)	Met
!	a project file (optional)	Missing

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 12 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	No	

Stage 2 — Live demo compared with the delivered code

Completed 12 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 10 Nov 2026; the builder fixed them and uploaded again.

Sign-off: approved for sale on 12 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.