The Verification Layer for AI-Built Software

VERIFICATION REPORT

GEC_Tracker · Run #1

WK-4-E8B17DFD · Nov 13, 2026 · 17:33 UTC

VERIFICATION VERDICT

NOT PRODUCTION READY

Significant issues must be resolved before production release.

EXECUTIVE SUMMARY

Weurkico evaluated 54 of 68 framework controls on 50 code files (~12,990 lines) (27 passed, 9 failed; 14 not verified automatically). 31 issues were found (2 critical, 10 high) across 68 locations. Significant issues must be resolved before production release.

VERIFICATION DETAILS

APPLICATION **GEC_Tracker**	RUN **#1 (id 4)**	SOURCE **GEC_App.zip**	SCOPE **Production**
FRAMEWORK **v1.4**	STARTED **Nov 13, 2026 · 16:51 UTC**	HUMAN REVIEW **Not performed (automated only)**	VERSION **GEC_App.zip sha256:e8b17dfd**
FILES ANALYZED **50 code files · 12,990 LOC**	FILES IN ARCHIVE **23,526 files · 230 MB**	VERIFICATION ID **WK-4-E8B17DFD**	GENERATED **Nov 13, 2026 · 17:33 UTC**
VERIFY THIS REPORT **https://weurkico.com/verify/WK-4-E8B17DFD**			

APPLICATION PROFILE

LANGUAGES	FRAMEWORKS	AUTOMATED TESTS	CI PIPELINE
JavaScript 99%	**React, Tailwind CSS**	**None detected**	**None detected**

TECHNOLOGIES DETECTED

JavaScript · React · Tailwind CSS · npm · Firebase Auth · No Dockerfile · No CI config · No test files

COVERAGE

68	54	27	9	14	31
FRAMEWORK	EVALUATED	PASSED	FAILED	NOT VERIFIED	ISSUES FOUND



● 2 critical ● 10 high ● 10 medium ● 9 low

9 control(s) not applicable to this application: `business_logic.payment_logic` (no payment processing detected in this application), `ai_security.prompt_injection` (no AI/LLM integration detected in this application), `ai_security.model_permissions` (no AI/LLM integration detected in this application), `ai_security.data_to_models` (no AI/LLM integration detected in this application), `ai_security.tool_calling` (no AI/LLM integration detected in this application), `ai_security.output_handling` (no AI/LLM integration detected in this application), `ai_security.credentials` (no AI/LLM integration detected in this application), `ai_security.agent_autonomy` (no AI/LLM integration detected in this application), `ai_security.ai_dependent_logic` (no AI/LLM integration detected in this application)

FINDINGS

SEVERITY	FINDING	CATEGORY	LOCATION	STATUS
CRITICAL	**Secret key in your code** (2 occurrences) CONFIDENCE 90% · EVIDENCE: STRONG	Security	`.env:3`, `firebase.js:8`	open

SEVERITY	FINDING	CATEGORY	LOCATION	STATUS
CRITICAL	**Unscoped data access (potential cross-user exposure)** (4 occurrences) CONFIDENCE 40% · EVIDENCE: PARTIAL	Data	`firestore.js:281, firestore.js:39, firestore.js:44, firestore.js:83`	open
HIGH	**Password in your code** (2 occurrences) CONFIDENCE 90% · EVIDENCE: STRONG	Security	`Register.jsx:85, create-admin.js:24`	open
HIGH	**firebase 9.23.0 has known vulnerabilities** CONFIDENCE 85% · EVIDENCE: STRONG	Dependencies	`package.json`	open
HIGH	**postcss 8.4.38 has known vulnerabilities** CONFIDENCE 85% · EVIDENCE: STRONG	Dependencies	`package.json`	open
HIGH	**vite 5.2.12 has known vulnerabilities** CONFIDENCE 85% · EVIDENCE: STRONG	Dependencies	`package.json`	open
HIGH	**Environment file committed: .env** CONFIDENCE 95% · EVIDENCE: STRONG	Infrastructure	`.env:1`	open
HIGH	**Account lifecycle operation invoked directly from client/application code** (3 occurrences) CONFIDENCE 65% · EVIDENCE: PARTIAL	Business Logic	`AdminDashboard.jsx:95, AuthContext.jsx:92, create-admin.js:32`	open
HIGH	**Sensitive data written to logs** (2 occurrences) CONFIDENCE 60% · EVIDENCE: PARTIAL	Security	`create-admin.js:46, create-admin.js:47`	open
HIGH	**Sensitive business operation requires server-side authorization rule** (9 occurrences) CONFIDENCE 60% · EVIDENCE: PARTIAL	Business Logic	`AdminDashboard.jsx:758, Classes.jsx:423, Modules.jsx:179, Modules.jsx:183 +5 more`	open
HIGH	**Critical workflows lack automated verification or schema validation** CONFIDENCE 75% · EVIDENCE: PARTIAL	Business Logic	`project-wide`	open
HIGH	**Firestore used without committed security rules (firestore.rules)** CONFIDENCE 80% · EVIDENCE: PARTIAL	Security	`project-wide`	open
MEDIUM	**Privilege or role assignment in application code** CONFIDENCE 65% · EVIDENCE: PARTIAL	Security	`create-admin.js:26`	open
MEDIUM	**Multi-step data write without atomic transaction** (2 occurrences) CONFIDENCE 60% · EVIDENCE: PARTIAL	Business Logic	`Announcements.jsx:117, Feedback.jsx:327`	open
MEDIUM	**Unescaped HTML injection sink** (2 occurrences) CONFIDENCE 60% · EVIDENCE: PARTIAL	Security	`Modules.jsx:385, StudentModules.jsx:105`	open
MEDIUM	**No automated tests detected** CONFIDENCE 90% · EVIDENCE: PARTIAL	Business Logic	`project root - no test files found`	open
MEDIUM	**No reproducible deployment definition** CONFIDENCE 70% · EVIDENCE: PARTIAL	Infrastructure	`project root - no Dockerfile or deployment manifest found`	open
MEDIUM	**No backup configuration or script detected in repository** CONFIDENCE 75% · EVIDENCE: PARTIAL	Data	`project-wide`	open
MEDIUM	**Hard-coded external URLs alongside environment config** CONFIDENCE 50% · EVIDENCE: PARTIAL	Infrastructure	`AdminDashboard.jsx:95`	open
MEDIUM	**Database access without visible error handling** (2 occurrences) CONFIDENCE 45% · EVIDENCE: PARTIAL	Reliability	`History.jsx, Layout.jsx`	open

SEVERITY	FINDING	CATEGORY	LOCATION	STATUS
MEDIUM	**Potentially expensive query (Unbounded…)** (6 occurrences) CONFIDENCE 50% · EVIDENCE: PARTIAL	Performance	`Announcements.jsx:28, Classes.jsx:216, Dashboard.jsx:73, Feedback.jsx:37 +2 more`	open
MEDIUM	**Outbound call without a timeout** CONFIDENCE 55% · EVIDENCE: PARTIAL	Reliability	`AdminDashboard.jsx:95`	open
LOW	**No CI pipeline detected** CONFIDENCE 85% · EVIDENCE: PARTIAL	Infrastructure	`project root - no CI configuration found`	open
LOW	**No rollback or migration downgrade strategy detected** CONFIDENCE 75% · EVIDENCE: PARTIAL	Infrastructure	`project-wide`	open
LOW	**No health check or monitoring hook detected** CONFIDENCE 75% · EVIDENCE: PARTIAL	Reliability	`project-wide`	open
LOW	**Possible N+1 query inside a loop** (9 occurrences) CONFIDENCE 40% · EVIDENCE: PARTIAL	Performance	`AdminDashboard.jsx:1183, ClassPage.jsx:198, Classes.jsx:64, Dashboard.jsx:68 +5 more`	open
LOW	**No retry or idempotency policy on outbound calls** CONFIDENCE 50% · EVIDENCE: PARTIAL	Reliability	`project-wide`	open
LOW	**Copy-pasted code blocks across 18 files** CONFIDENCE 70% · EVIDENCE: PARTIAL	Quality Maintainability	`AdminDashboard.jsx`	open
LOW	**Oversized file (1746 lines)** (4 occurrences) CONFIDENCE 85% · EVIDENCE: PARTIAL	Quality Maintainability	`AdminDashboard.jsx, ClassPage.jsx, Classes.jsx, firestore.js`	open
LOW	**No change-approval artifact in the repository** CONFIDENCE 60% · EVIDENCE: PARTIAL	Quality Compliance	`(repository)`	open
INFO	**Unused packages (3): lucide-react, react-quill, tailwind-merge** (3 occurrences) CONFIDENCE 55% · EVIDENCE: PARTIAL	Dependencies	`dependency manifest`	open

REMEDIATION PRIORITIES

1. **Google API key committed to the repository (2 occurrences)**
   Move the secret to environment variables or a secrets manager; rotate it.

2. **Unscoped data access (potential cross-user exposure) (4 occurrences)**
   Scope every query to the current user/tenant.

3. **Hard-coded password committed to the repository (2 occurrences)**
   Move the secret to environment variables or a secrets manager; rotate it.

4. **firebase 9.23.0 has known vulnerabilities**
   Upgrade to a patched version listed in the advisory.

5. **postcss 8.4.38 has known vulnerabilities**
   Upgrade to a patched version listed in the advisory.

6 **vite 5.2.12 has known vulnerabilities**
Upgrade to a patched version listed in the advisory.

7 **Environment file committed: .env**
Remove the file, add it to .gitignore, rotate the secrets it contained.

8 **Account lifecycle operation invoked directly from client/application code (3 occurrences)**
Move privileged account lifecycle calls to a protected backend endpoint.

9 **Sensitive data written to logs (2 occurrences)**
Remove sensitive fields or redact them before logging.

10 **Sensitive business operation requires server-side authorization rule (9 occurrences)**
Enforce explicit role and ownership checks on the server before executing sensitive business actions.

LIMITATIONS & NOT VERIFIED

- Static analysis may miss vulnerabilities reachable only at runtime.
- Deep data-flow analysis (CodeQL) was not run - results rely on pattern and heuristic checks.
- No automated test suite existed, so behaviour was not regression-tested.
- AI analysis is an assistive layer; every AI-derived finding is escalated for human review.
- This report reflects the code at the analyzed commit/archive only.
- Not verified: Test coverage tooling, Test/source ratio, Functional / e2e tests, API contract tests, Test isolation, Test suite execution, Regression safety net, API input validation, API error handling, API documentation, Requirement-to-test traceability, Test data management, Authentication, Injection.
- Not verified: Runtime behaviour under real production load.
- Not verified: Third-party accounts/secrets values validity.
- Not verified: Business workflows not observable from static code analysis.
- Not verified: Expert review is not included in your plan - upgrade to unlock human verification..

The verdict is computed deterministically by the Weurkico Verification Framework from scanner evidence and human review. AI-assisted analysis, when enabled, is advisory only and never produces the verdict.

WHAT HAPPENS NEXT

Address the remediation priorities above, then start a new verification run on the updated code to refresh this verdict.