SF SecureFix

Проверяем код так, как вы защищаете бизнес
We audit code the way you protect your business

SecureFix Audit Report — example-bad

Status: pipeline finished with findings (failed)
Finding severity aggregate: high (severity aggregate, not a risk rating) (not an enterprise risk rating)
Product: 0.2.0-phase1-alpha | Run: audit_9acdef68639113f5
Summary: 1 finding(s) (high: 1, medium: 0, low: 0)

Trust Summary

What you can trust:
- Result is bound to audit run audit_9acdef68639113f5 and schema 1.
- Code fingerprint of audited sources: sha256:31cb72254c3f...
- Git: unavailable (capture none)
- Config hash: sha256:8055ba39cfc7...
- Scope: . (directory); excluded patterns: 42
- Operator label: securefix-demo — not cryptographic attestation
- Findings come from the tool pipeline; operator may dismiss false positives separately.
- Technical rule profile: baseline (not a compliance certification) | product: 0.2.0-phase1-alpha

Out of scope for this audit:
- Infrastructure / network / cloud penetration testing.
- Runtime dynamic analysis / fuzzing.
- Secrets outside the submitted source tree (CI secrets, vaults).
- Certification (ISO/SOC2) or a guarantee of zero vulnerabilities.

Audit stages

Requested mode: standard | effective: standard-fail-fast
Terminated after stage: gosec
fmt: OK
vet: n/a
gosec: FAIL
build: n/a
test: SKIP
govulncheck: OK
run: SKIP

Findings (0)

No open findings (operator decisions listed below).

Operator decisions (scanner finding preserved)

1. [HIGH] GOSEC-G101 — Potential hardcoded credentials
at main.go:8
7: // Intentional demo finding (gosec G101).
8: const apiKey = "sk-live-hardcoded-secret-key"
9:
[accepted] note: Confirmed true positive: intentional demo hardcoded secret (gosec G101).
scope: finding