

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

Informe de auditoría SecureFix — example-bad

Estado: comprobación finalizada con hallazgos (no superada)

Agregado de severidad: alto (agregado de severidad, no es rating de riesgo) (no es rating de riesgo empresarial)

Producto: 0.2.0-phase1-alpha | Ejecución: audit_9acdef68639113f5

Resumen: 1 finding(s) (high: 1, medium: 0, low: 0)

Resumen de confianza

En qué se puede confiar:

- El resultado está vinculado a la ejecución audit_9acdef68639113f5 y al esquema 1.
- Huella del código auditado: sha256:31cb72254c3f...
- Git: unavailable (captura none)
- Hash de configuración: sha256:8055ba39cfc7...
- Alcance: . (directory); exclusiones: 42
- Etiqueta de operador: securefix-demo — no es attestation criptográfica
- Los hallazgos proceden del pipeline de herramientas; el operador puede marcar falsos positivos aparte.
- Perfil técnico de reglas: baseline (no es certificación de cumplimiento) | producto: 0.2.0-phase1-alpha

Fuera del alcance de esta auditoría:

- Pentest de infraestructura / red / nube.
- Análisis dinámico en runtime / fuzzing.
- Secretos fuera del árbol de código enviado (secretos CI, vaults).
- Certificación (ISO/SOC2) o garantía de cero vulnerabilidades.

Etapas de comprobación

Modo solicitado: standard | efectivo: standard-fail-fast

Detenido tras etapa: gosec

fmt: OK

vet: n/a

gosec: ERROR

build: n/a

test: OMITIDO

govulncheck: OK

run: OMITIDO

Hallazgos (0)

No hay hallazgos abiertos (decisiones del operador abajo).

Decisiones del operador (hallazgo original conservado)

1. [ALTO] GOSEC-G101 — Potential hardcoded credentials

en main.go:8

7: // Intentional demo finding (gosec G101).

8: const apiKey = "sk-live-hardcoded-secret-key"

9:

[accepted] nota: Confirmed true positive: intentional demo hardcoded secret (gosec G101).

alcance: finding