

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

Informe de auditoría SecureFix — trial-chi-pg

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: 0.1.4-phase0 | Ejecución: audit_0c050297b97e882e

Resumen: 7 finding(s) (high: 7, medium: 0, low: 0)

Resumen de confianza

En qué se puede confiar:

- El resultado está vinculado a la ejecución audit_0c050297b97e882e y al esquema 1.
- 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: 0.1.4-phase0

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

fmt: OK
vet: OK
gosec: OK
build: OK
test: ERROR
govulncheck: ERROR
run: OMITIDO

Hallazgos (7)

1. [ALTO] TEST — Tests failed

- ? `github.com/yourusername/go-chi-postgres-starter/cmd/api` [no test files]
- ? `github.com/yourusername/go-chi-postgres-starter/cmd/api/database` [no test files]
- ? `github.com/yourusername/go-chi-postgres-starter/cmd/api/errors` [no test ...]

2. [ALTO] GOVULN-MOD-golang-org-x-net-v0-46-0 — 7 known CVEs in golang.org/x/net@v0.46.0

en go.mod
Module: golang.org/x/net@v0.46.0
OSVs (7): GO-2026-4918, GO-2026-5025, GO-2026-5026, GO-2026-5027, GO-2026-5028, GO-2026-5029, GO-2026-5030
CVEs: CVE-2026-25680, CVE-2026-25681, CVE-2026-27136, CVE-2026-33814, CVE-2026-39821, CVE-2026-42502...

3. [ALTO] GOVULN-MOD-golang-org-x-crypto-v0-43-0 — 15 known CVEs in golang.org/x/crypto@v0.43.0

en go.mod
Module: golang.org/x/crypto@v0.43.0
OSVs (15): GO-2025-4134, GO-2025-4135, GO-2026-5005, GO-2026-5006, GO-2026-5013, GO-2026-5014, GO-2026-5015, GO-2026-5016, GO-2026-5017, GO-2026-5018, GO-2026-5019, GO-2026-5020, GO-2026-5021, GO-2026-502...

4. [ALTO] GOVULN-GO-2026-5024 — Invoking integer overflow in NewNTUnicodeString in golang.org/x/sys/windows

en go.mod
OSV: GO-2026-5024
CVE: CVE-2026-39824
Fixed in: v0.44.0
Module: golang.org/x/sys@v0.37.0

5. [ALTO] GOVULN-MOD-github-com-yourusername-go-chi-postgres-starter — 2 known CVEs in github.com/yourusername/go-chi-postgres-starter

en health_handler.go:60
Module: github.com/yourusername/go-chi-postgres-starter

OSVs (2): GO-2026-5037, GO-2026-5039
CVEs: CVE-2026-27145, CVE-2026-42507
Fixed in: v1.26.4

6. [ALTO] GOVULN-MOD-github-com-jackc-pgx-v5-v5-7-4 — 2 known CVEs in github.com/jackc/pgx/v5@v5.7.4
en user_repository.go:10
Module: github.com/jackc/pgx/v5@v5.7.4

OSVs (2): GO-2026-4771, GO-2026-4772
CVEs: CVE-2026-33815, CVE-2026-33816
Fixed in: v5.9.0

7. [ALTO] GOVULN-GO-2025-3553 — Excessive memory allocation during header parsing in github.com/golang-jwt/jwt
en user_service.go:9
OSV: GO-2025-3553
CVE: CVE-2025-30204
Fixed in: v5.2.2
Module: github.com/golang-jwt/jwt/v5@v5.2.1

© 2026 Dragun Aleksandr. SecureFix.