

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

Отчёт аудита — example-bad

Статус: проверка завершена с находками (не пройдено)

Агрегат severity: высокий (агрегат severity, не оценка риска) (не enterprise risk rating)

Продукт: 0.2.0-phase1-alpha | Запуск: audit_9acdef68639113f5

Кратко: 1 проблем(ы) (high: 1, medium: 0, low: 0)

Границы доверия

Чему можно доверять:

- Результат привязан к запуску audit_9acdef68639113f5 и схеме 1.
- Отпечаток проверенного кода: sha256:31cb72254c3f...
- Git: unavailable (захват none)
- Хеш конфигурации: sha256:8055ba39cfc7...
- Область: . (directory); исключений: 42
- Оператор (метка): securefix-demo — не криптографическая attestation
- Находки получены инструментами pipeline; оператор может отметить ложные отдельно.
- Технический профиль правил: baseline (не compliance-сертификация) | продукт: 0.2.0-phase1-alpha

Что не входило в объём:

- Пентест инфраструктуры, сети и облака.
- Динамический анализ runtime / fuzzing.
- Полная проверка секретов вне исходников (CI secrets, vault).
- Юридическая сертификация (ISO/SOC2) и гарантия отсутствия уязвимостей.

Этапы проверки

Режим запрошен: standard | факт: standard-fail-fast

Останов после стадии: gosec

fmt: ОК

vet: включено

gosec: ошибка

build: включено

test: пропуск

govulncheck: ОК

run: пропуск

Находки (0)

Открытых замечаний нет (решения оператора — ниже).

Решения оператора (исходная находка сохранена)

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

файл: main.go:8

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

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

9:

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

область: finding