GRUPO FARINA · STAGE 1 DELIVERABLE SAMPLE

Payments & API Security Readiness Diagnostic

Reference target: SecurePay (Java 25 · Spring Boot 4 · PostgreSQL 18) | Baseline audit: Oct 21, 2026 → Remediated verification: Oct 26, 2026 (120 automated tests). Note: This readiness diagnostic identifies technical gaps and verifies controls; formal PCI DSS / ISO 27001 certification requires an accredited QSA or certification body.

1. Executive Summary & Scope

Stage 1 evaluates payment APIs and backend services across four axes: (1) Idempotency & PostgreSQL concurrency, (2) Authentication, BOLA/ownership & rate limiting (OWASP API Top 10 / PCI DSS Req. 6 & 8), (3) Container & runtime hardening, and (4) DevSecOps CI supply-chain gates (Gitleaks, SpotBugs/FindSecBugs, Trivy, CycloneDX SBOM).

2. Prioritized Findings & Remediation Tracking (Stage 1 → Stage 2)

ID / Severity	Finding & Regulatory Mapping	Baseline Risk (Oct 21)	Remediation & Evidence (Oct 26)
SP-01 High	Dual auth configuration (DemoUsersConfig Basic Auth vs. JWT) OWASP API2 / PCI DSS 8.2	Conflicting UserDetailsService beans and inline demo credentials in docs.	**CLOSED (PR #30–#32):** Unified BCrypt + signed Bearer JWT (HS256); inline secrets removed; Gitleaks active.
SP-02 High	Missing rate limiting on /auth/login and /api/payments OWASP API4:2023	Exposed to credential stuffing and payment creation bursts.	**CLOSED (PR #34 & #36):** Token-bucket filter (429 + Retry-After) by IP and customer; X-Forwarded-For spoofing tests.
SP-03 Medium	BOLA / Ownership & JWT payload tampering coverage OWASP API1:2023	Needed full HTTP matrix for cross-customer reads and forged customerId fields.	**CLOSED (Days 23–25):** Verified 401/403/404 parity, foreign customerId rejection and SQL injection literal safety.
SP-04 Medium	Container & OS package vulnerabilities (musl / brotli) PCI DSS Req. 6.3	Alpine runtime layer flagged by Trivy for CVE-2026-107891 & CVE-2026-111497.	**CLOSED (PR #35 & #39):** Digest-pinned Temurin 25 JRE image, UID 10001, read-only rootfs, 0 High/Critical CVEs.
SP-05 Low	Swagger / OpenAPI permitAll in SecurityConfig under prod profile OWASP API8:2023	Springdoc was disabled in prod YAML, but SecurityConfig still had permitAll.	**CLOSED:** SecurityConfig gates Swagger matchers on springdoc properties; verified by ProdSwaggerSecurityTest (401/404).

3. Verified Engineering & Observability Controls (Days 36–41)

• **Idempotency & Concurrency:** Customer-scoped Idempotency-Key + SHA-256 payload fingerprint verified against concurrent race conditions in PostgreSQL 18.6.
• **Observability & Traceability:** Structured JSON logs with validated X-Correlation-Id, bounded Micrometer payment metrics (restricted to ADMIN), and OpenTelemetry spans with W3C Trace Context propagation.
• **Resilience Probes:** Isolated Compose outage test confirms /actuator/health/readiness transitions to 503 during PostgreSQL outage while /liveness stays 200 UP, recovering automatically upon DB restart.
• **Residual Roadmap (Next Stage):** Migration from manual HS256 filter to Spring OAuth2 Resource Server / external OIDC IdP, distributed Redis rate limiting for multi-replica deployments, and provider webhook reconciliation.

Grupo Farina · Rosario, Argentina — nicolasfarina@outlook.com — https://www.nicolasfarina.com