PENTESTERRA

FINTECH & BANKS

Security Testing Built for Financial Services

Financial institutions face unique attack surfaces - open banking APIs, complex business logic, and strict regulatory requirements. Pentesterra covers them all with continuous automated pentesting and evidence packages built for QSA and auditor review.

FINTECH ATTACK SURFACE COVERAGE

Open Banking API Abuse

Automated testing of OAuth flows, token scopes, and PSD2/Open Banking API endpoints.

→ IDOR, over-privileged grants, replay attacks

Credential & Session Attacks

Simulate brute-force, credential stuffing, and session token hijacking.

→ Against banking portals and mobile app backends

Business Logic Vulnerabilities

Detect IDOR, mass assignment, and bypassable workflows.

→ Payment limits, approval gates - automatic PCI-DSS scope mapping

Network & AD Lateral Movement

Map attack paths from external assets to internal payment processing systems.

→ Through Active Directory misconfigurations

Supply Chain & Developer Risk

DevGuard scans every commit pre-push.

→ Hardcoded API keys, malicious dependencies, secrets caught before production

Regulatory Evidence

PCI-DSS Req 11.3/11.4 and DORA compliance.

→ Per-cycle reports with per-finding PoCs, ready for QSA submission

PENTESTERRA

FINTECH & BANKS

WHY FINANCIAL TEAMS RUN PENTESTERRA

Business logic is tested, not just the OWASP Top 10

Payment limits, approval gates, transfer workflows, and multi-step onboarding are where financial fraud actually happens.

→ Bypassable workflows, IDOR, mass assignment

→ Each finding mapped to PCI-DSS scope

Findings are exploited before you see them

Every vulnerability is verified with a real, non-destructive exploit.

→ Your team spends time on confirmed exposure

→ Not on chasing scanner noise through change approval

Evidence is ready for the QSA, not just for you

Each cycle produces a per-finding proof-of-concept and a delta against the last assessment.

→ Export formatted for PCI-DSS Req 11.3 / 11.4 and DORA review

WHAT EVERY CYCLE DELIVERS

- ✓ Coverage of open banking / PSD2 APIs: OAuth flows, token scopes, consent replay, over-privileged grants
- ✓ Business-logic testing with automatic PCI-DSS scope mapping per finding
- ✓ Attack paths traced from an external asset to internal payment-processing systems
- ✓ Pre-push DevGuard scanning: hardcoded keys, malicious dependencies, secrets caught before they merge
- ✓ Per-cycle evidence package with per-finding PoCs, ready for QSA submission
- ✓ Continuous retest after remediation, with a stable status per finding and a full audit trail

FAQ

Does Pentesterra help with PCI-DSS and DORA specifically?

Yes. Business-logic and application findings are mapped to PCI-DSS scope automatically, and each cycle produces evidence formatted for PCI-DSS Req 11.3 / 11.4 penetration-testing requirements and DORA resilience testing, including per-finding proof-of-concept and remediation tracking.

Can it test our mobile banking app backend and open banking APIs?

Yes. API and SPA coverage includes dynamic endpoint discovery, GraphQL, OAuth and token-scope testing, and replay / consent abuse against banking portals and mobile app backends.

Is it safe to run against production banking systems?

Exploit verification is non-destructive by default - no data deletion, no denial-of-service, and nothing that reads or moves confidential data. Scopes are explicit, staging and production are isolated, and a human-in-the-loop mode can gate any active exploitation step.

How does this fit alongside our annual third-party pentest?

Most financial teams run Pentesterra continuously between annual engagements to catch regressions early, then hand the third-party tester a current, verified baseline.

Talk to a FinTech specialist

Continuous pentesting built for QSA and auditor review.

Request a Demo

info@pentesterra.com · pentesterra.com/solutions/fintech