Case Study: Full-Scope API Security Assessment for Fintech Platform (Anonymized)

Category: Web & API Security
Duration: 3 Weeks | **Engagement Type:** Black-box → Authenticated VAPT
Tools: Burp Suite, OWASP ZAP, Postman, CyberCLI, SQLMap, AWS Stack, ELK Stack

---

Context

A rapidly growing fintech startup handling online KYC and payment processing sought a comprehensive API-level security audit before scaling operations. Their infrastructure included public REST APIs, internal microservices, and an AWS-backed deployment with WAF protection.

The goal was to identify vulnerabilities in the authentication and authorization flow, detect injection and logic flaws, and validate resilience against automated abuse.

Approach

The assessment followed **OWASP API Security Top 10 (v2023)** and **PTES** methodology:

1. **Reconnaissance:** Enumerated 150+ API endpoints using CyberCLI, Postman, and Amass integrations.
2. **Authentication Testing:** Validated JWT token handling, password reset mechanisms, and session expiry.
3. **Authorization Testing:** Performed IDOR and BOLA exploitation attempts across multiple user roles.
4. **Injection & Input Validation:** Fuzzed JSON payloads and query params for SQLi, XSS, and path traversal.
5. **Business Logic Abuse:** Tested replay attacks and transaction manipulation.
6. **Infrastructure Validation:** Correlated WAF logs and request patterns with findings in ELK to confirm real-world exploit feasibility.

Key Findings

Severity	Count	Highlight
Critical	2	IDOR in `/api/v2/user/transactions/{id}` exposed transaction metadata
High	4	Weak JWT validation (no signature check in refresh tokens)
Medium	3	Missing rate limits on login and OTP verification APIs
Low	6	Verbose error messages leaking environment data

Remediation Summary

- Implemented **RBAC-based authorization** and **JWT signature verification** across all endpoints.
- Added **HMAC timestamping** to prevent replay attacks.
- Integrated **rate limiting (429 policy)** at the API gateway layer.
- Tuned AWS WAF managed rule groups and added regex whitelists for legitimate business endpoints.
- Deployed **ElastAlert2-based Slack notifications** for blocked requests and anomalies.

Outcome

- Reduced exploitable attack surface by **~70%**
- Improved API authentication reliability (0 reported replay incidents post-fix)
- Established continuous monitoring with **WAF + ELK + Slack** integration
- Delivered an executive summary and full 58-page report with CVSS scores and PoC payloads

---

Executive Summary

- This engagement provided a full-stack visibility into the fintech platform's API ecosystem.

- By combining manual testing, custom fuzzing, and WAF rule validation, several critical issues were remediated before public scaling.

- The collaboration also helped the client's DevOps team embed security checks into their CI/CD pipeline — establishing a **"Shift-Left" AppSec foundation** for their growing business.
