Acme Financial Services – Security Incident Analysis Report

Report ID: AFS-GOA-2025-01
Report Date: 10 November 2025 (Istanbul)
Incident Date: 15 October 2024

1) Executive Summary

Outside the planned test window (20–25 October), a sequence of events from the same IP indicates account takeover, API Broken Access Control (BOLA), SQL injection on the web layer, and data export. Priorities: terminate active sessions, enforce ownership checks on the API, and harden WAF rules.

---

2) Scope & Method

- **Sources:** API, Web, WAF, Email logs
- **Filters:** Test IPs (192.168.1.100, 10.0.0.0/24, 203.0.113.0/24), test accounts (5001–5010), test window (20–25 Oct)
- **Approach:** Logs were consolidated with Python/pandas; events were labelled via BOLA/SQLi/Phishing/Export rules and merged into a single timeline (timeline_suspicious.xlsx).

---

3) Timeline (summary, UTC+3)

Time	Layer	Event / Request	Result	Note
06:45	API	Login (user 1523)	200 OK	Session opened
06:47–48	API	/api/v1/portfolio/1524–1538	200 OK	BOLA
09:00	Email	“Verify Your Account” (bulk recipients)	—	Phishing
09:23	WAF/Web	/*!50000OR*/ 1=1--	200 / 403	Some attempts blocked; some passed (partial bypass)
09:24	Web	/dashboard/export?format=csv	200 OK	export

Full rows and fields: **timeline_suspicious.xlsx → “Suspicious Timeline”**.

---

4) Findings

4.1 Broken Access Control (BOLA) – Critical

- 200 OK from accounts 1524–1538 using session of user 1523
- OWASP API4:2023 — Unauthorized data access risk

4.2 SQL Injection – Critical

- Patterns like /*!50000…*/, OR 1=1-- received 200 in some cases
- OWASP A03:2021 — Risk of data manipulation/exfiltration

4.3 Phishing – Critical

- "Verify Your Account" campaign from the same IP
- ISO 27001 A.8.23 / NIST PR.AT-1 — Credential harvesting risk

4.4 Monitoring/Correlation – Medium

- Chain required manual correlation; limited real-time alerting
- OWASP A09:2021, NIST DE.AE-1/2 — Longer detection/response times

---

5) Impact

- **Directly affected:** user 1523
- **Viewed accounts:** 1524–1538
- **Likely data exported:** (based on event sequence)
- **Business risk:** Customer data, compliance, reputation

---

6) Root Cause

1. Missing ownership check in API (no JWT.sub vs account_id enforcement)
2. Basic WAF rule set; obfuscated SQLi not always blocked
3. Weak identity/session hygiene (no mandatory MFA; lenient token lifecycle)
4. No SIEM chain rule (email → web → WAF → API)

---

7) Recommendations

P0 – 0–48 hours

5. Revoke tokens/sessions of user 1523; reset passwords for 1524–1538 is recommended.
6. Enforce API ownership check (return 403 when JWT.sub != account_id) is recommended.
7. Add targeted WAF rules for /*!50000, OR 1=1, UNION, DROP is recommended.
8. Apply temporary blocks to suspicious IPs and tighten rate limiting is recommended.

,P1 – 1–2 weeks

9. Use parameterized queries/ORM, input validation, and output encoding is recommended.
10. Make MFA mandatory, shorten token lifetimes, and enable session anomaly detection is recommended.
11. Define a high-priority SIEM correlation alert: Email(verify) → Web(SQLi) → WAF → API(BOLA) is recommended.

P2 – ≤3 months

12. Deploy an API Security Gateway (JWT validation, schema validation, rate-limit, IP reputation) is recommended.
13. Strengthen email security (DMARC/DKIM/SPF, sandboxing, URL analysis) is recommended.
14. Run a security awareness program and periodic phishing simulations is recommended.

---

8) Conclusion

The exploitation path progressed from a compromised session to BOLA, then SQL injection, ending with data export. Implementing the P0/P1 items should materially reduce near-term recurrence; P2 measures will shorten detection and response with measurable targets.