Acme Financial Services Incident Response Report

TTP Classification: T1190, T1566, T1078

Date: 10/11/2025

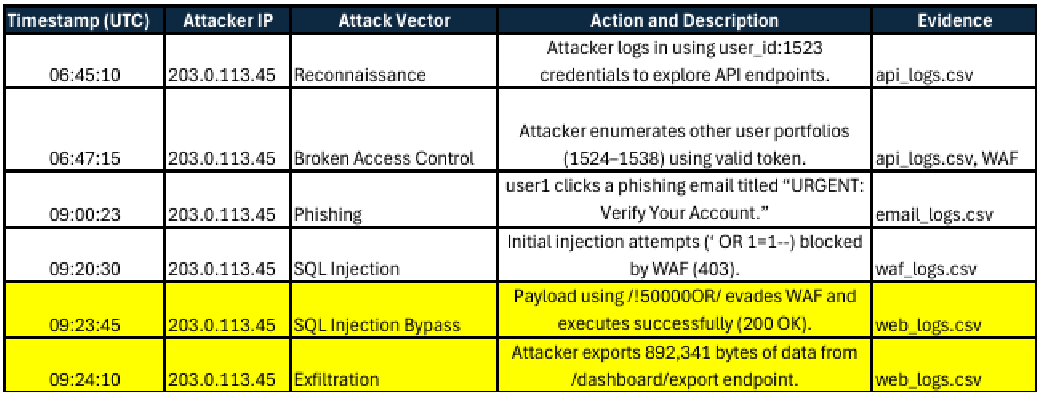
Analyst: Mikail Burak Doğru

Investigation Period: 07/11/2025 - 10/11/2025

Keywords: Incident Response, SQL Injection (A03), Broken Access Control (A01), Phishing (T1566), WAF Bypass (T1190), MITRE ATT&CK, OWASP

Incident Analysis

Timeline Reconstruction



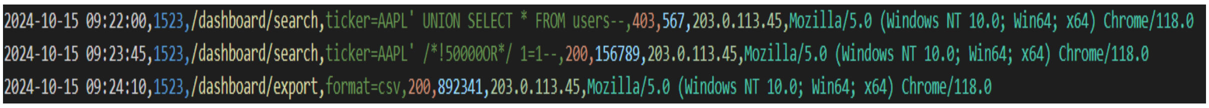
Timestamp (UTC)	Attacker IP	Attack Vector	Action and Description	Evidence
06:45:10	203.0.113.45	Reconnaissance	Attacker logs in using user_id:1523 credentials to explore API endpoints.	api_logs.csv
06:47:15	203.0.113.45	Broken Access Control	Attacker enumerates other user portfolios (1524–1538) using valid token.	api_logs.csv, WAF
09:00:23	203.0.113.45	Phishing	user1 clicks a phishing email titled "URGENT: Verify Your Account."	email_logs.csv
09:20:30	203.0.113.45	SQL Injection	Initial injection attempts (' OR 1=1--) blocked by WAF (403).	waf_logs.csv
09:23:45	203.0.113.45	SQL Injection Bypass	Payload using /!50000OR/ evades WAF and executes successfully (200 OK).	web_logs.csv
09:24:10	203.0.113.45	Exfiltration	Attacker exports 892,341 bytes of data from /dashboard/export endpoint.	web_logs.csv

This timeline shows the attack progression from reconnaissance to exfiltration, with each step documented by system logs and web evidence.

Attack Vector Identification

Phishing: At 09:00:23, the attacker sent phishing emails from IP 203.0.113.45. This IP was intended for a penetration test scheduled for Oct 20-25 but was misused five days prior, confirming malicious activity.

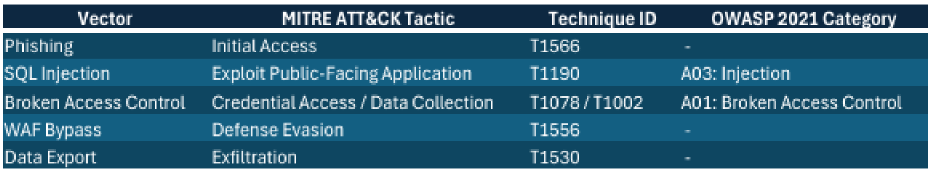
SQL Injection: The attacker targeted the `/dashboard/search` endpoint. Initial payloads were blocked by the WAF, but at 09:23:45, a MySQL comment obfuscation payload (`/*!50000OR*/`) successfully bypassed protections, retrieving 156,789 bytes of sensitive data.



```
2024-10-15 09:22:00,1523,/dashboard/search,ticker=AAPL' UNION SELECT * FROM users--,403,567,203.0.113.45,Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/118.0
2024-10-15 09:23:45,1523,/dashboard/search,ticker=AAPL' /*!50000OR*/ 1=1--,200,156789,203.0.113.45,Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/118.0
2024-10-15 09:24:10,1523,/dashboard/export,format=csv,200,892341,203.0.113.45,Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/118.0
```

Broken Access Control: At 06:47, while authenticated as `user_id:1523`, the attacker accessed other user accounts (1524-1538) through API endpoints. The system lacked proper object-level authorization checks, creating a critical security gap.

Attack Classification (MITRE ATT&CK & OWASP)



Vector	MITRE ATT&CK Tactic	Technique ID	OWASP 2021 Category
Phishing	Initial Access	T1566	-
SQL Injection	Exploit Public-Facing Application	T1190	A03: Injection
Broken Access Control	Credential Access / Data Collection	T1078 / T1002	A01: Broken Access Control
WAF Bypass	Defense Evasion	T1556	-
Data Export	Exfiltration	T1530	-

This classification maps the observed actions to known frameworks, confirming both the attack methods and their severity.

Root Cause Analysis

1. **Authorization Gaps:** Authentication was verified, but token ownership validation was missing, allowing `user_id:1523` to access multiple accounts.
2. **Unsecured Query Handling:** The web app did not enforce parameterized queries, relying solely on WAF protection, which was bypassed.
3. **Weak WAF Configuration:** Basic WAF rules failed to detect obfuscated SQL payloads.
4. **Unrestricted IP Whitelisting:** Email gateway allowed the vendor IP outside the designated test window, enabling early phishing attacks.

Impact Assessment

- **Data Exposure:** 892,341 bytes of user portfolio data were stolen.
- **User Impact:** PII and financial information of multiple users were compromised.
- **Regulatory Breach:** The incident triggered SOC 2 and GDPR compliance concerns.

Architecture Review

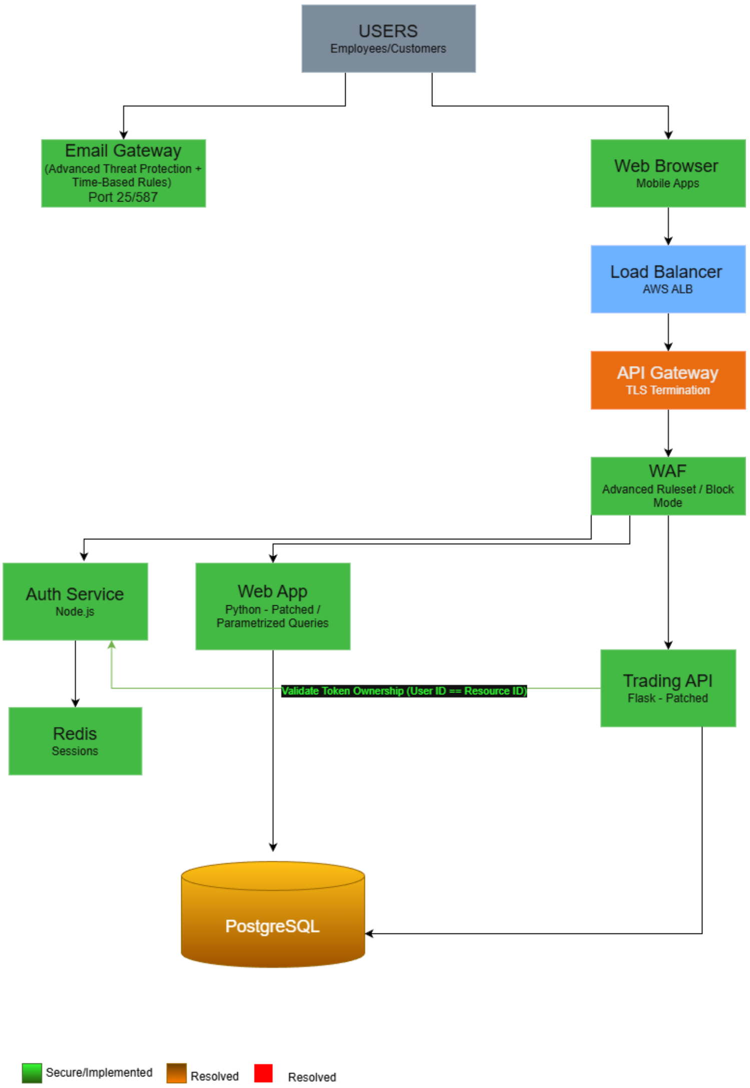
Current Architecture Weaknesses

- **WAF:** Basic rules, easily bypassed.
- **Web App & API:** Vulnerable endpoints lacked input validation and authorization enforcement.
- **Email Gateway:** Trusted IPs without time-based restrictions, enabling phishing attempts.

Improved Security Architecture Diagram

The redesigned architecture introduces multiple security layers, each providing independent controls:

- **WAF with advanced rule sets** to block obfuscated attacks.
- **Web Application** using parameterized queries for SQLi defense.
- **API** enforcing token ownership and object-level authorization.
- **Email Gateway** with time-based whitelist validation.



Recommended Security Controls (with Justification)

1. **WAF (Advanced Ruleset / Block Mode):** Blocks complex attack patterns and obfuscated payloads.
2. **Web App (Parameterized Queries):** Ensures defense-in-depth by neutralizing SQL injection attacks at the application layer.
3. **API (Token Ownership Validation):** Prevents unauthorized account access by validating user identity against requested resources.
4. **Email Gateway (Time-Based Rules):** Limits vendor IP trust to defined windows, preventing phishing attacks outside authorized periods.

Defense-in-Depth Strategy

Layered defenses ensure that a single failure does not lead to a data breach. Even if the WAF is bypassed, the Web App and API remain secure, containing potential attacks and protecting sensitive information.

Response & Remediation

Immediate Actions (0-24 Hours)

- Block attacker IP (203.0.113.45) across all networks.
- Invalidate compromised session tokens and disable user accounts.
- Deploy virtual WAF patches to block obfuscated SQLi payloads.
- Audit all web logs for the extent of exfiltrated data.
- Preserve forensic evidence for investigation.

Short-Term Fixes (1-2 Weeks)

- Refactor endpoints to use parameterized queries.
- Apply API-level object authorization checks.
- Upgrade WAF to advanced rules with block mode.
- Enforce time-based IP validation for trusted vendors.

Long-Term Improvements (1-3 Months)

- Provide secure coding training to developers aligned with OWASP Top 10.
- Enhance SIEM to detect WAF bypass attempts and large-scale data exports.
- Conduct independent security audits and penetration tests.
- Review vendor security policies to prevent misuse of trusted IPs.

Compliance Considerations

- **SOC 2:** Breach of Confidentiality and Integrity principles.

- **GDPR:** Violates Article 32 (Security of Processing); immediate reporting is required.
- Engage legal and compliance teams to initiate formal breach notifications.