

SECURITY OPERATIONS

INCIDENT RESPONSE REPORT

# Acme Financial Services

## Incident Analysis Report

### INCIDENT DETAILS

Incident ID:	INC-20241015-001
Date:	November 9, 2025
Severity Level:	CRITICAL
Prepared by:	Ali Ekber KARA

# Executive Summary

The incident that occurred in Acme Financial Services systems on October 15, 2024, has been identified as a chained cyber attack that began at the API layer and progressed in multiple stages. The attacker first exploited an IDOR (Insecure Direct Object Reference) vulnerability at the /api/v1/portfolio endpoint to discover user data. Using the information obtained, the attacker sent phishing emails from a fake domain name (acme-finance.com) and compromised the credentials of three users. Then, using the same IP address, they exploited an SQL Injection vulnerability at the /dashboard/search endpoint to extract data from the system and exported approximately 870 KB of user data via /dashboard/export. The incident was classified as Critical Severity because the attacker used the 203.0.113.0/24 IP range, reserved for planned penetration tests, to make detection difficult, and because the incident involved both phishing and application vulnerabilities and provided direct access to customer data. Recommended measures include strengthening API access controls, resetting user passwords, implementing MFA, strengthening WAF rules, and increasing phishing awareness training.

## 1. Incident Analysis

### 1.1 Incident Timeline

All logs have been normalized to UTC format. Events that occurred on October 15, 2024, in the Acme Financial Services infrastructure were investigated by correlating email, WAF, API, and web application logs. The sequence of events, causes, and related findings are detailed below.

#### 01:30 UTC – Automated Vulnerability Scanning

The internal IP address 192.168.1.100 initiated a scheduled weekly automated vulnerability scan by the corporate security scanner. During this scan, sequential requests were sent to the /api/v1/portfolio/{id} endpoints, and 401 authorization errors were received in the first attempts (1000–1004). After 15 minutes, the same tool made authenticated requests using test user tokens (e.g., test\_token\_xyz\_5001). (api\_logs.csv)

This activity was classified as a false positive because it occurred in accordance with the “Automated Vulnerability Scanning” plan. (security\_test\_schedule.pdf)

#### 04:15–05:33 UTC – Normal User Activities

Logins and portfolio viewing requests made by real users via the mobile application (iOS and Android) have been recorded. All transactions were performed with valid JWT tokens, and the IP addresses (98.213.45.122 and 172.89.15.67) appeared clean on VirusTotal. This time frame reflects the system's normal operational traffic. (api\_logs.csv)

#### 06:47 UTC – Possible Account Enumeration

In the WAF logs, rapid and sequential requests were detected from the IP address 203.0.113.45 in the range /api/v1/portfolio/1529–1538. This situation has been flagged as “Rapid Sequential Access” and “Possible Account Enumeration”. (api\_logs.csv)

The investigation revealed that the same IP address was involved in more serious activities a few hours later. This stage is considered to be a preparatory phase in which the attacker attempted to discover the system's user ID structure. (api\_docs.pdf)

## **07:12–08:23 UTC – Normal User Activity**

User sessions (ID 4521 and 6789) were successfully completed via the mobile application. JWT tokens were valid for these sessions and operated within access limits (rate limit). This traffic has been labeled as normal behavior. (api\_logs.csv)

## **08:55 UTC – Suspicious Admin Activity**

The admin user (admin\_5678) initiated the /admin/users/export process in the system and immediately sent the file named “meeting\_notes.pdf” to an external email address (external.contact@protonmail.com).

Although the process was performed via the corporate IP (10.0.1.50), the fact that the external recipient has a ProtonMail extension and that the file transfer occurred simultaneously with the email sending weakens the possibility of coincidence. Therefore, the activity has been assessed as suspicious.

In light of this situation, it would be appropriate to obtain confirmation from the relevant user. (web\_logs.csv, email\_logs.csv)

## **09:00 UTC – Phishing Campaign Launch**

During this time frame, which coincided with the start of business hours, emails with the subject line “URGENT: Verify Your Account” were sent to six different users from the address security@acme-finance.com. The email content gave the impression that the accounts needed security verification, prompting users to act quickly in a state of panic. (email\_logs.csv)

At first glance, this email appeared to be corporate communication, but it used the fake domain acme-finance.com instead of the legitimate domain acme.com, constituting a classic credential harvesting attack.

Three users clicked on the link in the email, one of whom (User ID 1523) was later associated with unauthorized activities on the system.

The source IP address (203.0.113.45) is within the IP range (203.0.113.0/24) reserved for the planned penetration test. However, considering that the planned tests are scheduled to take place between October 20–25, 2024, this activity has been assessed as a potentially unauthorized early test or possible misuse. (security\_test\_schedule.pdf)

This situation demonstrates that insufficiently restricted timing and access controls in test infrastructures can delay the detection of real attacks.

## **09:10–09:19 UTC – Unauthorized Access**

After the phishing emails, three different user accounts were logged in.

Specifically, User ID 1523 logged in via the attacker's IP address (203.0.113.45) and shortly thereafter misused the search functions within the system.

At this stage, it was determined that the attacker used the credentials obtained through the phishing email to open a real user session. (web\_logs.csv)

## **09:20–09:24 UTC – SQL Injection Attack and Data Exfiltration**

WAF logs detected consecutive SQL Injection attempts originating from the same IP address (203.0.113.45). The attempts were carried out in the following order: “OR 1=1”, “DROP TABLE”,

and “UNION SELECT”, and these attempts were blocked by the system. However, the subsequent attempt “!/50000OR/ 1=1” was detected but could not be blocked.

The reason for this is that the WAF is configured according to basic rules and cannot correctly identify this advanced SQL Injection pattern. Following this request, it was observed that data was exported in CSV format by accessing the /dashboard/export endpoint. This stage is considered the critical point where data leakage occurred within the scope of the incident. (waf\_logs.csv)

### **10:15–11:25 UTC – Normal User Activity**

WAF and web logs have not detected any abnormal activity during this time period. User sessions were conducted from clean IP addresses with legitimate JWT tokens. Attacker activity has ceased during this time period.

## **1.2 Attack Vector Identification**

The analysis revealed that the incident involved multiple attack vectors. First, the attacker exploited an IDOR (Insecure Direct Object Reference) vulnerability in the API layer at the /api/v1/portfolio endpoint to discover user IDs and understand the system's data access logic, constituting the reconnaissance phase. Using the obtained user data and credentials, the attacker conducted social engineering via phishing with the fake domain acme-finance.com, exploiting user trust by imitating the corporate domain. With the stolen credentials, the attacker authenticated into the system from IP 203.0.113.45 and then exploited an SQL injection vulnerability at /dashboard/search, sending unauthorized queries and exfiltrating data through /dashboard/export. This chain of actions combines phishing, application vulnerabilities, and access control weaknesses. Furthermore, the use of a planned penetration test IP range indicates that the attacker misused legitimate network resources to evade detection and bypass security monitoring.

## **1.3 Attack Classification (MITRE ATT&CK / OWASP)**

This incident involved several MITRE ATT&CK tactics, including phishing (T1566.002), credential harvesting (T1555), data from information repositories (T1213), and exfiltration over web service (T1567.002).

According to OWASP Top 10 2021, the main vulnerabilities were A01: Broken Access Control (IDOR), A03: Injection (SQL Injection), A05: Security Misconfiguration (WAF rules), and A07: Identification and Authentication Failures (use of stolen credentials without MFA).

## **1.4 Root Cause Analysis**

The root cause of the incident was insufficient access controls implemented at the API endpoints and web application firewall (WAF) rules configured only according to basic patterns. Furthermore, incorrect or insufficient restrictions on access permissions for planned penetration testing IP ranges allowed the attacker to progress undetected by blending in with legitimate traffic. The lack of MFA among users led to phishing emails being effective and credentials being easily exploited. Limited security awareness training also contributed to the success of the social engineering phase.

## **1.5 Impact Assessment**

As a result of the incident, approximately 870 KB of user data (such as name, email, portfolio ID, transaction history) was leaked from the system. The incident has been classified as Severity Level: Critical due to its direct impact on customer data, its potential to damage the brand's reputation, and the possible legal reporting obligations to regulatory authorities. Although no financial loss has been

identified, the compromise of identity information could pave the way for credential stuffing or account takeover attacks in the future. Therefore, the incident carries a high risk from both an operational and reputational perspective.

## 2. Architecture Review

### 2.1 Current Architecture Weaknesses

Although Acme Financial Services' current infrastructure is functional, it appears that security layers have not been fully addressed ahead of the upcoming SOC 2 Type II audit (November 15–30). The system operates in the Load Balancer → API Gateway → WAF → Application Server → Database chain, but there are weaknesses, particularly in API security and access controls. Reviews have revealed that the WAF is limited to basic signature-based rules and cannot detect advanced SQL injection attempts. Although token verification is performed at API endpoints, account ownership is not verified, leading to an IDOR vulnerability. SPF/DKIM/DMARC records are missing in the email infrastructure, and phishing emails from fake domains cannot be filtered. Test IP ranges (203.0.113.0/24) were not sufficiently restricted in the production environment, and role separation and the “least privilege” principle were not applied to database access. These points are considered critical vulnerability areas prior to the audit.

### 2.2 Improved Security Architecture

The new design has been restructured using a “Defense in Depth” approach to address existing vulnerabilities and strengthen compliance (SOC 2 Type II, OWASP Top 10, NIST CSF).

#### User Layer:

MFA should be mandatory for all user logins; SPF, DKIM, and DMARC policies should be enabled for email traffic to prevent phishing attacks based on fake domains.

#### Network Layer:

API Gateway and web applications behind the Load Balancer should be separated into different network segments, and only verified traffic should be routed between segments. WAF should be enhanced with OWASP ModSecurity CRS v3.3.2 rules and behavior-based anomaly detection.

#### Application Layer:

Claim-based authorization should be implemented on the API Gateway; in addition to token verification, the `user_id` must match the `token.subject`. All SQL queries should be parameterized queries or ORM-based, rate limit policies should be consistent, and every API response should be logged with a correlation ID to create an audit trail.

#### Database Layer:

Access should be restricted to service accounts, and “read/write” permissions should only be granted to necessary tables. Unusual queries should be monitored in real time with Database Activity Monitoring (DAM) integration.

#### Audit and Monitoring Layer:

WAF, API, Auth, and SIEM logs should be analyzed using MITRE ATT&CK-based correlation rules; incident response should be automated with SOAR integration. All security tests should be compared against scheduled time intervals to filter out false positive alerts.

## **2.3 Recommended Security Controls (with Justification)**

The controls proposed under the new security architecture have been defined to address identified vulnerabilities and provide evidence of control effectiveness for the upcoming audit. MFA integration enhances authentication security by reducing the risk of credential reuse after phishing. SPF, DKIM, and DMARC policies prevent domain spoofing, rendering email-based social engineering attacks ineffective. Developing WAF rules reduces the attack surface by detecting advanced SQL Injection and XSS variants. API token ownership verification eliminates IDOR risk by preventing access to data that does not belong to the user. Database privilege separation limits damage in potential data leaks by applying the least privilege principle. SIEM and SOAR integration strengthens the correlation-based alert system and shortens incident response time.

## **2.4 Defense-in-Depth Strategy**

The recommended architecture aims to ensure security through a multi-layered defense rather than relying on a single layer. Email security, authentication, and WAF policies reduce the attack surface on the user side, while API Gateway, application access controls, and network segmentation prevent internal propagation. Database-level monitoring and privileged access restrictions minimize the impact of potential breaches. This approach offers a circular defense model that verifies, monitors, and restricts every access in line with Zero Trust principles. Thus, both external threats and potential misaccesses originating from the internal network are minimized prior to auditing and can be evaluated as proof of control effectiveness and security maturity in the upcoming PwC SOC 2 Type II audit.

# **3. Response & Remediation**

## **3.1 Immediate Actions (0–24 Hours)**

The SOC team must block all traffic from IP 203.0.113.45 and quarantine affected accounts. All active sessions must end, JWT tokens must be revoked, and users must reset their passwords. WAF must be upgraded to “Blocking” mode, and the fake domain acme-finance.com must be blocked in email filters. All actions must be recorded in the “Security Incident Interim Summary” for the SOC 2 Type II audit.

## **3.2 Short-Term Fixes (1–2 Weeks)**

The development team must implement object-level authorization at /api/v1/portfolio and validate user-to-object mapping. SQL queries must use ORM or parameterized queries to prevent SQL Injection. WAF must detect advanced patterns like /!50000OR/. The SOC team must restrict test IP range usage to official windows. MFA must be enabled, and phishing training must be given. The incident-to-remediation process must be documented with log evidence.

## **3.3 Long-Term Improvements (1–3 Months)**

Acme Financial Services must implement centralized API authorization and enforce access controls at a central layer. Anomaly detection must monitor data exports, and SIEM must alert on unusual activity. Penetration testing policies must include IP-based verification. Email security must use SPF, DKIM, and DMARC, and Threat Intelligence must detect fake domains. Peer code review must be required. SOC must use SOAR for automatic incident alerts.

### **3.4 Compliance Considerations**

All corrective actions must be documented in the Change Management system. Root Cause Analysis must be added to the Corrective Action Register for PwC. Logs must be archived for at least 180 days. MFA and password resets must be recorded as “Completed Control Action” in audit notes. Acme Financial Services must fully document post-incident processes to comply with SOC 2 Type II standards.