ACME FINANCIAL SERVICES

Incident Analysis and Security Assessment Report

(Within the scope of Q4 2024 Security Tests)

Prepared by: Sude Nur Karakin Date: November 2025

1. **Introduction and General Information**

Acme Financial Services is an online platform that provides financial transaction and investment services. It consists of a web application, mobile API and corporate e-mail system.

During the fourth quarter of 2024, planned safety tests were conducted, and unusual activities outside the scope of testing were detected. This situation showed that there may be unauthorized access attempts and data exfiltration attempts in the system.

2. **Scope and Purpose**

This report aims to analyze unusual activities identified during Acme Financial Services' security tests conducted in the fourth quarter of 2024, identify the root causes of vulnerabilities, and recommend corrective measures. Work; e-mail, web application, WAF and API logs, and evaluations were carried out within the framework of ISO/IEC 27001, NIST SP 800-61 and OWASP Top 10 standards. The main goal of the analysis is to prevent the recurrence of similar attacks by revealing security breaches that occur outside of planned testing and to increase the overall security maturity of the organization.

3. **Executive Summary**

On October 15, 2024, while scheduled security tests were underway on the Acme Financial Services platform, unusual activities outside the scope of testing were detected. Through investigation, it was determined that the incident was a coordinated attack chain consisting of three successive phases:

a) Phishing Emails

Employees were sent emails that appeared to be Acme's official communications, and user credentials were compromised.

b) Web Application Attack (SQL Injection)

Accessing the system with the compromised credentials, the attacker gained access to the database using a custom SQL query in the /dashboard/search endpoint that bypassed the WAF.

c) API Access Control Vulnerability (IDOR/BOLA)

Unauthorized access was made to other users' portfolio data via API calls using the web session. As a result of the log correlation, it was determined that all these activities were carried out from a single attack infrastructure connected to the IP address 203.0.113.45. The main purpose of the incident was considered to be data exfiltration.

4. **Recommendation Summary**

As a result of the analysis, the main causes of the incident were determined as technical security vulnerabilities, misconfigurations and lack of user awareness.

." The "Defense in Depth" strategy should be adopted. (E.g. Network layer IDS, application firewall, etc.)

Finding 1: Phishing Attack

Effectiveness: High

Domain: Email / User Accounts

Finding Description

Acme Financial Services employees were asked to verify their identity through fraudulent emails that appeared to have been sent by the in-house security team. In the e-mails sent, a fake login link ("Verify Your Account") was found and the credentials of the users who clicked on this link were transmitted to the attacker's server.

As a result of log analysis, it was determined that user1@acme.com, user3@acme.com and user5@acme.com users accessed the phishing link through the same IP address (203.0.113.45).

IP Correlation

This IP represents a proxy or command server (C2 server) controlled by the attacker. This suggests that the attack was coordinated by a single person or group

Evidence Table (Email Logs)

	A	B	C	D	E	F	G
1	timestamp	from	to	subject	link_clicked	ip_address	attachment
2	15.10.2024 08:55	admin@acme.com	external.contact@protonmail.com	Q3 Meeting Notes	no	10.0.1.50	meeting_notes.pdf
3	**15.10.2024 09:00**	**security@acme-finance.com**	**user1@acme.com**	**URGENT: Verify Your Account - Action Required**	**yes**	**203.0.113.45**	
4	15.10.2024 09:00	security@acme-finance.com	user2@acme.com	URGENT: Verify Your Account - Action Required	no		
5	**15.10.2024 09:00**	**security@acme-finance.com**	**user3@acme.com**	**URGENT: Verify Your Account - Action Required**	**yes**	**203.0.113.45**	
6	15.10.2024 09:00	security@acme-finance.com	user4@acme.com	URGENT: Verify Your Account - Action Required	no		
7	**15.10.2024 09:00**	**security@acme-finance.com**	**user5@acme.com**	**URGENT: Verify Your Account - Action Required**	**yes**	**203.0.113.45**	
8	15.10.2024 09:00	security@acme-finance.com	user6@acme.com	URGENT: Verify Your Account - Action Required	no		
9	15.10.2024 09:15	support@acme.com	customer1@example.com	Re: Account inquiry	no	10.0.2.30	
10	15.10.2024 10:30	hr@acme.com	all-staff@acme.com	Team Building Event Next Week	no	10.0.2.15	
11	15.10.2024 11:45	it@acme.com	engineering@acme.com	Scheduled Maintenance Tonight	no	10.0.2.25	
12							

Figure 1: (user1,user3,user5) users are seen clicking on the malicious link from the same IP address. *(email_logs.png)*

Analysis Details

- Multiple clicks from the same IP address indicate that the attacker is using a single control server or proxy device.
- The credential collection page is an exact replica of Acme's official login page.
- The attack aimed to create user interaction through "social engineering" methods.

Potential Hazards

- Obtaining user credentials
- Abuse of internal login privileges
- Gaining unauthorized access to the web application or API system

Conclusion and Recommendation

- This incident underscores the importance of user awareness and the inadequacy of email security controls.
- Authentication policies and phishing simulation tests should be made mandatory in corporate communication infrastructure.

Finding 2: SQL Injection (Web Application)

Impact Rating: Critical

Domain: Web Application/Database

Finding Description

A SQL injection vulnerability was detected in the /dashboard/search endpoint due to user inputs not being filtered.On October 15, 2024, requests from IP address 203.0.113.45 circumvented WAF signatures using the payload /*!50000OR*/ 1=1--.

Evidence Table (Web Logs)

	A	B	C	D	E	F	G	H
1	timestamp	user_id	endpoint	query_params	response_code	response_size_bytes	ip_address	user_agent
2	15.10.2024 08:55	admin_5678	/admin/users/export		200	15673	10.0.1.50	Mozilla/5.0 (Windows NT 10.0
3	15.10.2024 08:56	admin_5678	/admin/download/user_export.csv		200	245890	10.0.1.50	Mozilla/5.0 (Windows NT 10.0
4	15.10.2024 09:10	2145	/login		200	3421	98.213.45.122	Mozilla/5.0 (Macintosh
5	15.10.2024 09:11	2145	/dashboard		200	8934	98.213.45.122	Mozilla/5.0 (Macintosh
6	15.10.2024 09:15	3421	/login		200	3421	172.89.15.67	Mozilla/5.0 (X11
7	15.10.2024 09:16	3421	/dashboard		200	8745	172.89.15.67	Mozilla/5.0 (X11
8	15.10.2024 09:18	1523	/login		200	3421	203.0.113.45	Mozilla/5.0 (Windows NT 10.0
9	15.10.2024 09:19	1523	/dashboard		200	8934	203.0.113.45	Mozilla/5.0 (Windows NT 10.0
10	**15.10.2024 09:20**	**1523**	**/dashboard/search**	**ticker=AAPL' OR 1=1--**	**403**	**567**	**203.0.113.45**	**Mozilla/5.0 (Windows NT 10.0**
11	**15.10.2024 09:21**	**1523**	**/dashboard/search**	**ticker=AAPL'**				
12	**15.10.2024 09:22**	**1523**	**/dashboard/search**	**ticker=AAPL' UNION SELECT * FROM users**	**403**	**567**	**203.0.113.45**	**Mozilla/5.0 (Windows NT 10.0**
13	**15.10.2024 09:23**	**1523**	**/dashboard/search**	**ticker=AAPL' /*!50000OR*/ 1=1--**	**200**	**156789**	**203.0.113.45**	**Mozilla/5.0 (Windows NT 10.0**
14	**15.10.2024 09:24**	**1523**	**/dashboard/export**	**format=csv**	**200**	**892341**	**203.0.113.45**	**Mozilla/5.0 (Windows NT 10.0**
15	**15.10.2024 09:30**	**1523**	**/dashboard/home**	**200"**	**200**	**8934**	**203.0.113.45**	**Mozilla/5.0 (Windows NT 10.0**
16	15.10.2024 10:15	4567	/login		200	3421	45.123.89.201	Mozilla/5.0 (Macintosh
17	15.10.2024 10:16	4567	/dashboard		200	8934	45.123.89.201	Mozilla/5.0 (Macintosh
18	15.10.2024 10:18	4567	/dashboard/portfolio		200	12345	45.123.89.201	Mozilla/5.0 (Macintosh
19	15.10.2024 11:20	7891	/login		200	3421	172.89.15.67	Mozilla/5.0 (X11
20	15.10.2024 11:21	7891	/dashboard		200	8934	172.89.15.67	Mozilla/5.0 (X11
21	15.10.2024 11:25	7891	/dashboard/search	ticker=TSLA	200	5432	172.89.15.67	Mozilla/5.0 (X11
22								

Figure 2: SQL Injection trials and WAF reactions are seen. (web_logs.png)

Analysis Details

- The first attempts were blocked by WAF, but evasive payload passed successfully.
- Afterwards, there was a suspicion of data leakage with an "export" request.

Conclusion and Recommendation

The lack of input control and WAF signature inadequacy at the application layer created a vulnerability that could lead to data exfiltration.

- Switching to parametric queries - SQL injections are avoided.
- Update WAF ruleset – Evasive payloads should be detected.

Finding 3: WAF Signature Evasion

Impact: MediumDomain: WAF / Edge Security

Finding Description

A large number of SQLi attempts from source 203.0.113.45 have been detected in WAF logs. Some variants (e.g., /*!50000OR*/) circumvent signature-based rules; therefore, the WAF provided only partial protection.

Evidence Table

	A	B	C	D	E	F	G	H
1	timestamp							
2	15.10.2024 09:20	981173	HIGH	DETECT	203.0.113.45	/dashboard/search	SQL Injection Attempt - OR 1=1	yes
3	15.10.2024 09:21	981318	CRITICAL	BLOCK	203.0.113.45	/dashboard/search	SQL Injection - DROP TABLE	yes
4	15.10.2024 09:22	981257	HIGH	BLOCK	203.0.113.45	/dashboard/search	SQL Injection - UNION SELECT	yes
5	15.10.2024 09:23	981001	MEDIUM	DETECT	203.0.113.45	/dashboard/search	Suspicious SQL Pattern	no
6	15.10.2024 09:00	950107	HIGH	DETECT	203.0.113.45	/verify-account.php	Suspicious Link Pattern	no
7	15.10.2024 01:30	920420	LOW	DETECT	192.168.1.100	/api/v1/portfolio/1000	Multiple Failed Auth	no
8	15.10.2024 01:30	920420	LOW	DETECT	192.168.1.100	/api/v1/portfolio/1004	Multiple Failed Auth	no
9	15.10.2024 06:47	942100	MEDIUM	DETECT	203.0.113.45	/api/v1/portfolio/1529	Rapid Sequential Access	no
10	15.10.2024 06:47	942100	MEDIUM	DETECT	203.0.113.45	/api/v1/portfolio/1534	Rapid Sequential Access	no
11	15.10.2024 06:47	942100	HIGH	DETECT	203.0.113.45	/api/v1/portfolio/1538	Possible Account Enumeration	no
12	15.10.2024 08:55	920430	LOW	DETECT	10.0.1.50	/admin/users/export	Admin Area Access	no
13	15.10.2024 10:15	920100	LOW	DETECT	45.123.89.201	/login	Normal Login Pattern	no

Figure 3: Evasive payload detections and 200 OK responses in WAF logs. (waf_logs.png)

Analysis Details

- WAF signature-based rulesets block most standard payloads.
- Evasive techniques (obfuscation / comment-encoding, etc.) have circumvented some signatures and led to the achievement of practice.
- This shows the limitation of WAF working only with static signatures.

Conclusion and Recommendation

- Update the WAF ruleset and add evasive patterns (immediate hotfix).
- Enable anomaly/behavioral mode in WAF; Apply rate-limiting.
- Send the detected payload samples to SIEM in a protected manner, create a correlation rule.
- Schedule periodic red-team/evading-tests and automate the WAF tuning process.

Finding 4: API (IDOR / BOLA) Vulnerability

Effectiveness: High

Domain: Mobile API / Authentication

Finding Description

In the API logs, it was seen that user 1523 sent a request to access portfolio information for different accounts (1524–1538). This indicates that there is a "Broken Object Level Authorization (BOLA)" or "Insecure Direct Object Reference (IDOR)" vulnerability in the system. The attacker was able to access the data of different users using the same JWT token.

Potential Hazards

- Disclosure of customer portfolio information
- Violation of user privacy
- Risk of unauthorized financial transactions

Conclusion and Recommendation

- This vulnerability in API access control directly threatens the privacy of user data. In order to prevent such vulnerabilities, the "object-level authorization" mechanism should be made mandatory.
- An authorization layer should be added, and user ID ≠ account ID should be checked for each API call.
- The JWT token structure should be redesigned, User-specific permission information should be added to the token.

References and Resources

Standards and Frameworks

1. ISO/IEC 27001:2022 — Information Security Management System (ISMS)

It is based on incident management, risk assessment and corrective action processes.

2. NIST SP 800-61 Rev.2 — *Computer Security Incident Handling Guide*

The framework for incident analysis, detection, response, and remediation steps is in line with this standard.

3. OWASP Top 10 (2021) — *Web Application Security Risks*

In particular, the A03:2021 Injection and API4:2023 Broken Object Level Authorization categories were evaluated.

4. OWASP API Security Top 10 (2023)

BOLA/IDOR and authentication vulnerabilities are classified according to this list.

5. SOC 2 Type II — Security, Access Control, and Monitoring requirements (included in the Acme test plan).

Corporate Documents

- Acme Financial Services — Scheduled Security Testing (Q4 2024)
  By Security Operations Team
  Date: 01 October 2024

Test scope, planned activities, and safety procedures are based on this document.

- Acme Architecture Diagram — "Current Architecture" (2024)

It shows the flow of system components and vulnerability points during incident analysis.

Log and Analysis Resources

Source	Explanation
email_logs.csv	It was used in the analysis of the phishing campaign.
web_logs.csv	It was used to detect SQL Injection attempts.
waf_logs.csv	It was used in blocking/detection data and signature circumvention analysis.
api_logs.csv	It was used in mobile API access controls (BOLA/IDOR) events.

Additional Resources

- Microsoft Security Blog — "Defending Against Modern Phishing Campaigns", 2023.
- OWASP Cheat Sheet Series — "SQL Injection Prevention" and "Authorization Testing".
- Cloudflare WAF Ruleset Documentation, 2024.
- MITRE ATT&CK Framework — *T1190: Exploit Public-Facing Application*.

REPORT PRIVACY NOTICE