Acme Security Incident Investigation and Architecture Hardening Report

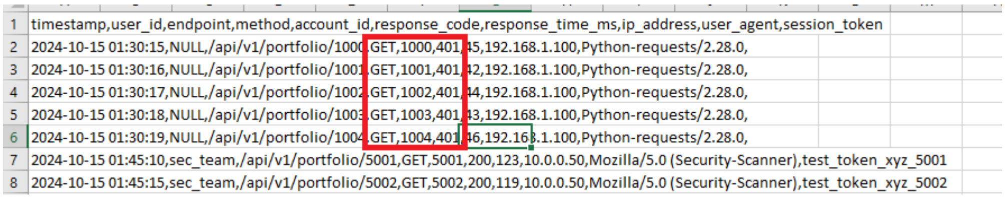
Prepared by: Ahmet Temirtekin
Position: Penetration Tester
Date: 09/11/2025

Section 1: Incident Analysis

All timestamps have been normalized to UTC

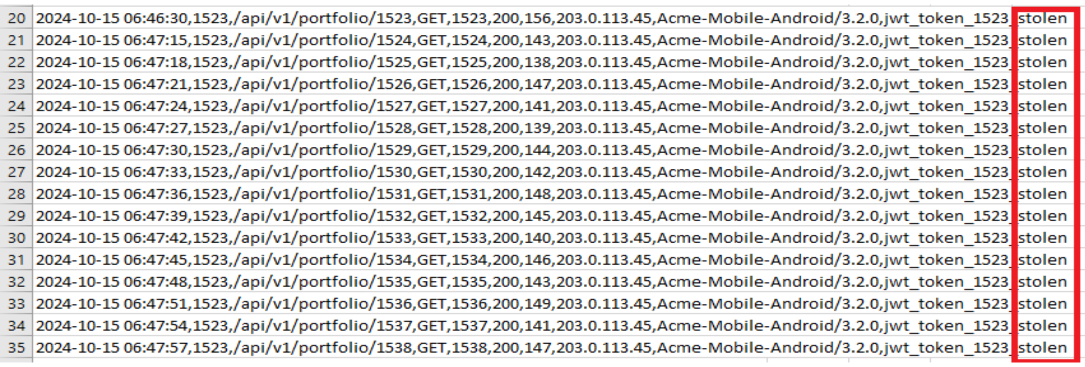
Time (UTC)	Event Description	Evidence Source	Impact Assessment
01:30-01:45	Internal security scans from 192.168.1.100; sec_team accessed test accounts 5001–5005	API logs	Benign activity, aligned with scheduled scans
06:45 – 06:48	Account 1523 login from 203.0.113.45; stolen JWT reused to access portfolios 1524–1538	API logs, WAF logs	Unauthorized portfolio access (multi-account)
09:00 – 09:01	Phishing emails sent from spoofed domain; users 1, 3, 5 clicked malicious links	Email logs, WAF logs	Likely credential/token compromise
09:18 – 09:24	SQL injection attempts against /dashboard/search; obfuscated payload bypassed WAF; large response and CSV export	WAF logs, Web logs	Potential data exfiltration via export
10:15 – 11:25	Normal web activity by accounts 4567 and 7891	Routine usage, unrelated to attack	

- **01:30–01:45** – Internal security scans from IP 192.168.1.100 generated failed login attempts; sec_team accessed test accounts 5001–5005.



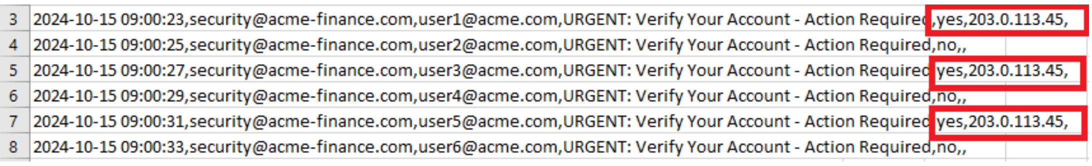
```
1  timestamp,user_id,endpoint,method,account_id,response_code,response_time_ms,ip_address,user_agent,session_token
2  2024-10-15 01:30:15,NULL,/api/v1/portfolio/1000,GET,1000,401,45,192.168.1.100,Python-requests/2.28.0,
3  2024-10-15 01:30:16,NULL,/api/v1/portfolio/1001,GET,1001,401,42,192.168.1.100,Python-requests/2.28.0,
4  2024-10-15 01:30:17,NULL,/api/v1/portfolio/1002,GET,1002,401,44,192.168.1.100,Python-requests/2.28.0,
5  2024-10-15 01:30:18,NULL,/api/v1/portfolio/1003,GET,1003,401,43,192.168.1.100,Python-requests/2.28.0,
6  2024-10-15 01:30:19,NULL,/api/v1/portfolio/1004,GET,1004,401,46,192.168.1.100,Python-requests/2.28.0,
7  2024-10-15 01:45:10,sec_team,/api/v1/portfolio/5001,GET,5001,200,123,10.0.0.50,Mozilla/5.0 (Security-Scanner),test_token_xyz_5001
8  2024-10-15 01:45:15,sec_team,/api/v1/portfolio/5002,GET,5002,200,119,10.0.0.50,Mozilla/5.0 (Security-Scanner),test_token_xyz_5002
```

- **06:45–06:48** – Account **1523** logged in from 203.0.113.45; stolen JWT reused to access portfolios

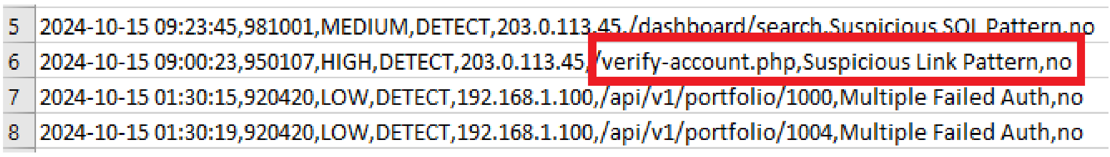


```
20 2024-10-15 06:46:30,1523,/api/v1/portfolio/1523,GET,1523,200,156,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523 stolen
21 2024-10-15 06:47:15,1523,/api/v1/portfolio/1524,GET,1524,200,143,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523 stolen
22 2024-10-15 06:47:18,1523,/api/v1/portfolio/1525,GET,1525,200,138,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523 stolen
23 2024-10-15 06:47:21,1523,/api/v1/portfolio/1526,GET,1526,200,147,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523 stolen
24 2024-10-15 06:47:24,1523,/api/v1/portfolio/1527,GET,1527,200,141,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523 stolen
25 2024-10-15 06:47:27,1523,/api/v1/portfolio/1528,GET,1528,200,139,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523 stolen
26 2024-10-15 06:47:30,1523,/api/v1/portfolio/1529,GET,1529,200,144,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523 stolen
27 2024-10-15 06:47:33,1523,/api/v1/portfolio/1530,GET,1530,200,142,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523 stolen
28 2024-10-15 06:47:36,1523,/api/v1/portfolio/1531,GET,1531,200,148,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523 stolen
29 2024-10-15 06:47:39,1523,/api/v1/portfolio/1532,GET,1532,200,145,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523 stolen
30 2024-10-15 06:47:42,1523,/api/v1/portfolio/1533,GET,1533,200,140,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523 stolen
31 2024-10-15 06:47:45,1523,/api/v1/portfolio/1534,GET,1534,200,146,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523 stolen
32 2024-10-15 06:47:48,1523,/api/v1/portfolio/1535,GET,1535,200,143,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523 stolen
33 2024-10-15 06:47:51,1523,/api/v1/portfolio/1536,GET,1536,200,149,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523 stolen
34 2024-10-15 06:47:54,1523,/api/v1/portfolio/1537,GET,1537,200,141,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523 stolen
35 2024-10-15 06:47:57,1523,/api/v1/portfolio/1538,GET,1538,200,147,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523 stolen
```

- **09:00–09:01** – Phishing emails sent from spoofed domain; users 1, 3, 5 clicked malicious links.

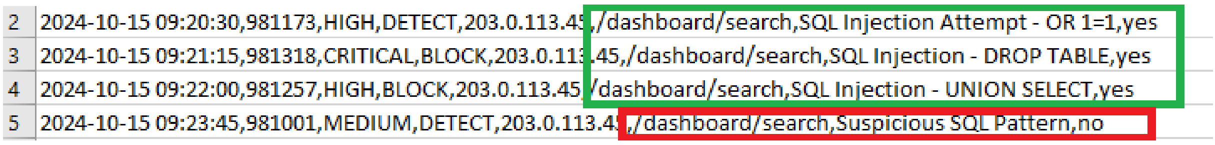


```
3 2024-10-15 09:00:23,security@acme-finance.com,user1@acme.com,URGENT: Verify Your Account - Action Required,yes,203.0.113.45,
4 2024-10-15 09:00:25,security@acme-finance.com,user2@acme.com,URGENT: Verify Your Account - Action Required,no,,
5 2024-10-15 09:00:27,security@acme-finance.com,user3@acme.com,URGENT: Verify Your Account - Action Required,yes,203.0.113.45,
6 2024-10-15 09:00:29,security@acme-finance.com,user4@acme.com,URGENT: Verify Your Account - Action Required,no,,
7 2024-10-15 09:00:31,security@acme-finance.com,user5@acme.com,URGENT: Verify Your Account - Action Required,yes,203.0.113.45,
8 2024-10-15 09:00:33,security@acme-finance.com,user6@acme.com,URGENT: Verify Your Account - Action Required,no,,
```



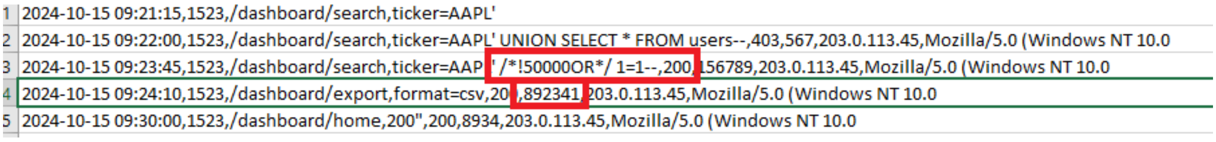
```
5 2024-10-15 09:23:45,981001,MEDIUM,DETECT,203.0.113.45,/dashboard/search,Suspicious SQL Pattern,no
6 2024-10-15 09:00:23,950107,HIGH,DETECT,203.0.113.45,/verify-account.php,Suspicious Link Pattern,no
7 2024-10-15 01:30:15,920420,LOW,DETECT,192.168.1.100,/api/v1/portfolio/1000,Multiple Failed Auth,no
8 2024-10-15 01:30:19,920420,LOW,DETECT,192.168.1.100,/api/v1/portfolio/1004,Multiple Failed Auth,no
```

- **09:18–09:24** – SQL injection attempts against /dashboard/search; obfuscated payload bypassed WAF, large response and CSV export followed.



```
2 2024-10-15 09:20:30,981173,HIGH,DETECT,203.0.113.45,/dashboard/search,SQL Injection Attempt - OR 1=1,yes
3 2024-10-15 09:21:15,981318,CRITICAL,BLOCK,203.0.113.45,/dashboard/search,SQL Injection - DROP TABLE,yes
4 2024-10-15 09:22:00,981257,HIGH,BLOCK,203.0.113.45,/dashboard/search,SQL Injection - UNION SELECT,yes
5 2024-10-15 09:23:45,981001,MEDIUM,DETECT,203.0.113.45,/dashboard/search,Suspicious SQL Pattern,no
```

&



```
1 2024-10-15 09:21:15,1523,/dashboard/search,ticker=AAPL'
2 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
3 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
4 2024-10-15 09:24:10,1523,/dashboard/export,format=csv,200,892341,203.0.113.45,Mozilla/5.0 (Windows NT 10.0
5 2024-10-15 09:30:00,1523,/dashboard/home,200",200,8934,203.0.113.45,Mozilla/5.0 (Windows NT 10.0
```

Attack Vector Identification

Attack Vector	Description	Evidence Source	Impact
Phishing Campaign	Spoofed emails tricked users into clicking links	Email logs, WAF logs	Credential/token compromise
SQL Injection	Obfuscated payload bypassed WAF	WAF logs, Web logs	Large response, data export
API Broken Access Control	Stolen JWT reused across accounts	API logs, WAF logs	Unauthorized portfolio access

The incident combined phishing, SQL injection, and API broken access control. Evidence correlates across email, WAF, web, and API logs.

Attack Classification

Owasp Table For Vulnerabilities

Owasp category	Description	Evidence in Incident
A01: Broken Access Control	API did not enforce account ownership	Stolen JWT used to access 1524–1538
A03: Injection	SQL injection payload bypassed WAF	Web logs show 156,789 bytes response
A05: Security Misconfiguration	Email gateway lacked DMARC/SPF/DKIM enforcement	Phishing emails from spoofed domain

OWASP Top 10 categories mapped to Acme incident evidence.

MITRE ATT&CK Mapping (Table)

Technique Name	Evidence in Incident
Phishing	Users clicked malicious email links
Exploit Public-Facing Application	SQL injection on /dashboard/search
Valid Accounts	Stolen JWT reused for multiple accounts

MITRE ATT&CK techniques relevant to Acme incident.”

Root Cause Analysis

The coordinated attack exploited systemic weaknesses. The Trading API validated tokens but failed to enforce ownership, enabling cross-account access. The web application lacked robust input validation, allowing obfuscated SQL payloads to bypass WAF detection. The email gateway had no strict DMARC/SPF/DKIM enforcement, increasing susceptibility to spoofed phishing emails. Together, these gaps created a chain of compromise.

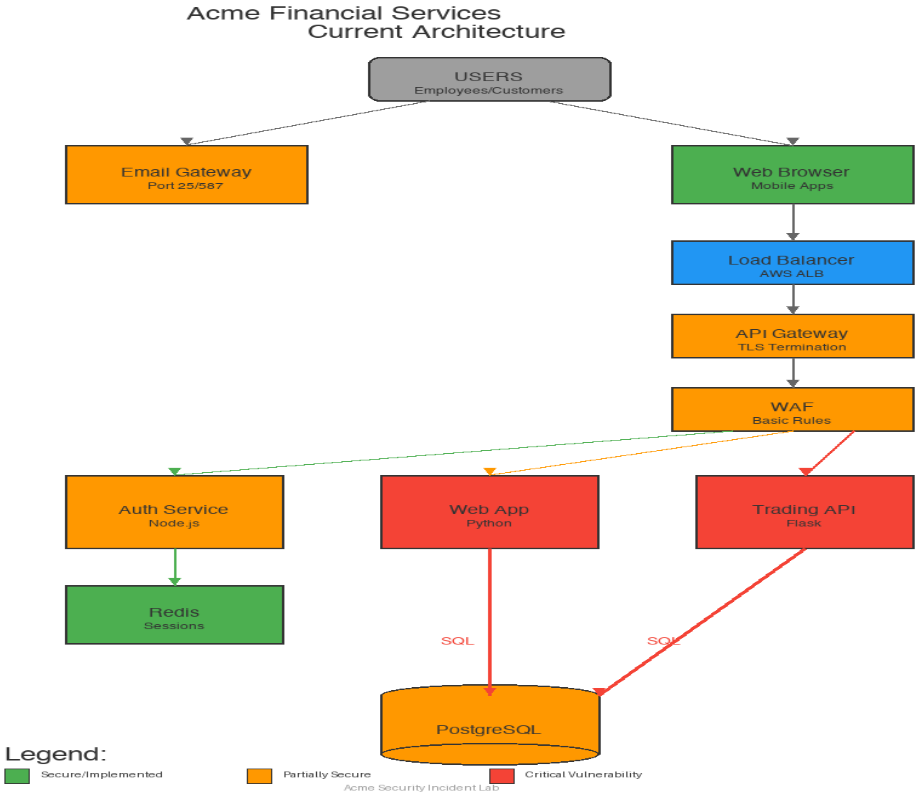
Impact Assessment

Unauthorized portfolio access across accounts 1524–1538, potential data exfiltration via CSV export, and erosion of trust in Acme's trading platform.

Impact Area	Description	Severity
Data Confidentiality	Unauthorized portfolio access (1524–1538)	Critical
Data Integrity	Potential manipulation via SQL injection	High
Availability	No direct outage observed	Low
Trust/Reputation	Customer confidence erosion	High

Section 2: Architecture Review

Current Architecture Weaknesses

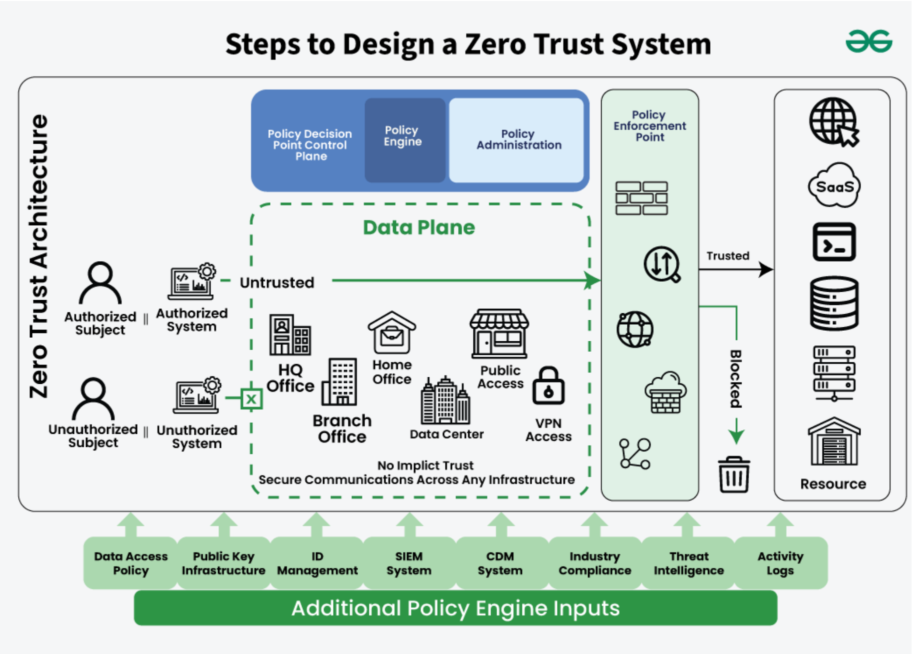


Current architecture highlighting vulnerabilities in API, Web App, and Email Gateway.

Weaknesses include missing ownership validation in API, insufficient input validation in web app, and lack of DMARC/SPF/DKIM in email gateway.

Improved Security Architecture Diagram

Defense-in-depth ensures resilience: if WAF fails, API ownership validation, SIEM monitoring, MFA, and least-privilege DB roles continue to protect the system.



Proposed Zero Trust architecture for Acme Financial Services.

This diagram illustrates the proposed Zero Trust architecture for Acme Financial Services. It emphasizes that no implicit trust is granted to any access point (HQ, branch, home, public, VPN, or data center). All requests are evaluated through a policy engine and administrator, with enforcement points protecting SaaS, PaaS, IaaS, and internal resources. Inputs such as identity management, SIEM telemetry, compliance requirements, and threat intelligence feed into the policy engine, ensuring continuous verification and defense-in-depth.

Section 3: Response & Remediation

Immediate Actions (0–24 hours)

Block malicious IP range 203.0.113.0/24, revoke compromised JWTs, rotate signing keys, disable /dashboard/export temporarily, enforce WAF rules against obfuscated payloads, and require MFA re-verification for affected users.

Short-Term Fixes (1–2 weeks)

Implement strict ownership validation, parameterized queries, rate limits, DMARC/SPF/DKIM reject policies, and phishing awareness training.

Long-Term Improvements (1–3 months)

Introduce Zero Trust API Gateway, least-privilege DB roles, JWT binding, centralized SIEM correlation, and align with OWASP ASVS, NIST 800-53, SOC 2.

Compliance Considerations

All recommendations align with OWASP ASVS, NIST 800-53, and SOC 2 Type II requirements, ensuring regulatory compliance and customer trust.

This report provides a clear roadmap for incident containment, remediation, and long-term resilience. By addressing broken access control, strengthening input validation, and improving phishing defenses, Acme Financial Services can significantly reduce exposure to future threats. The recommended Zero Trust architecture and compliance-aligned controls ensure that the organization not only mitigates current risks but also builds sustainable trust with customers and regulators.