ACME SECURITY - INCIDENT LAB REPORT

1 Incident Analysis

1.1 Timeline reconstruction (UTC normalized)

	A	B	C	D	E	F
1	Timeline (PST)	Timeline (UTC)	Log Type	Affected user / account	Event Summary	Critical Analysis
2	06:45:10	14:45:10	API	user_id: 1523	POST /api/v1/login (Status: 200)	The attacker successfully logged into the API with the user_id:1523 account.
3	06:47:15 - 06:47:57	14:47:15 - 14:47:57	API & WAF	account_id: 1524 to 1538	GET /api/v1/portfolio/{account_id} requests	BAC (Broken Access Control) Exploit. Attacker successfully leaked portfolio information for 15 different accounts. WAF only alerted (DETECT [MEDIUM]).
4	08:55:00	16:55:00	WEB & WAF	/admin/users/export	admin area access	Successful access to admin account. Phishing is now possible.
5	08:55:12	16:55:12	EMAIL	external.contact@protonmail.com	Phishing	meeting_notes.pdf is a phishing campaign sent.
6	09:00:23-09:00:33	17:00:23 - 17:00:33	EMAIL & WAF	user1, user3, user5	The phishing link URGENT was clicked.	The WAF app detected the problem [DETECT] but did not block it. The phishing campaign was successful. Login information of three different accounts was stolen. It is believed that the attacker used these new accounts to access the web application.
7	09:18:30	17:18:30	WEB	user_id: 1523	200 /login (Web Application Login)	The attacker also successfully logged into the web application using the 1523 ID that was previously used in the API.
8	09:20:30	17:20:30	WEB & WAF	/dashboard/search	ticker=AAPL' OR 1=1--	SQL Injection Blocked. WAF correctly blocked the dangerous query with the BLOCK [HIGH] action.
9	09:21:15	17:21:15	WEB & WAF	/dashboard/search	ticker=AAPL'; DROP TABLE users--	SQL Injection Blocked. WAF correctly blocked the dangerous query with the BLOCK [CRITICAL] action.
10	09:22:00	17:22:00	WEB & WAF	/dashboard/search	ticker=AAPL' UNION SELECT * FROM users--	SQL Injection Blocked. WAF correctly blocked the dangerous query with the BLOCK [HIGH] action.
11	09:23:45	17:23:45	WEB & WAF	/dashboard/search	ticker=AAPL' /*!50000OR*/ 1=1-- (Status: 200)	WAF Bypass and SQLi Success. The attacker bypassed the WAF using obfuscated syntax. The web application returned 200 OK. This is a successful data access.
12	09:24:10	17:24:10	WEB	/dashboard/export	format=csv (Status: 200)	Right after the successful SQLi, the attacker used the export feature to steal the data they got from the system.

1.2 Attack vector identification

The attack was carried out by exploiting multiple vectors targeting three different critical security control points of the system using a single source IP address (203.0.113.45). The three primary vectors and log evidence are presented below.

1.2.1 Mobile API broken access control

This represents the earliest and most effective vector of attack. The attacker initially gained access to the API using a valid session token associated with user_id 1523. The attacker began sending requests via the GET /api/v1/portfolio/account_id endpoint at 14:47:15 UTC. API logs confirm fifteen consecutive and systematic requests were made to this endpoint, ranging from 1524 to 1538. Each of these requests returned a successful 200 response despite not matching the identity of the authorized token holder. As a result, the API failed to properly enforce authorization checks between the user_id and the requested account_id, allowing one user to access sensitive portfolio data belonging to another.

1.2.2 Web application SQL injection

Approximately two and a half hours after the API leak, the attacker shifted to this vector and successfully bypassed the Web Application Firewall (WAF). The target was the ticker parameter in the /dashboard/search endpoint. Initially, the first malicious attempts were intercepted by the WAF, which blocked the actions containing DROP TABLE and UNION SELECT commands, generating a BLOCK [CRITICAL] alert at 09:21:15 UTC. However, at 09:23:45 UTC, the attacker modified the payload and used an obfuscated query — ticker=AAPL' /!50000OR/ 1=1-- — which caused the WAF to trigger only a DETECT [MEDIUM] alert without blocking the request. Web logs show that this attempt received a Status: 200 response, indicating successful execution. As a result of the WAF bypass, the web application's database became exposed, and within seconds, approximately 892 KB of bulk data was exfiltrated through the /dashboard/export endpoint.

1.2.3 Phishing campaign targeting employees

This vector provided the attacker with additional credentials that could be used to access the web application. The target in this phase was user credentials. Email logs indicate that, during a fake campaign titled "URGENT: Verify Your Account" launched at 09:00:23 UTC, users user1, user3, and user5 clicked on a fraudulent link and unknowingly submitted their login information to the attacker. This incident represented a critical stage in expanding unauthorized access to corporate systems and revealed a significant gap in basic identity protections, particularly the absence of Multi-Factor Authentication (MFA) enforcement.

1.3 Attack classification (MITRE ATT&CK, OWASP)

The multi-vector attack exposed both technical and human vulnerabilities in existing defense architectures. The classification identifies the attack methods, intent, and resulting application vulnerabilities.

1.3.1 MITRE ATT&CK

	A	B	C	D
1	**Tactics**	**Technical IDs**	**Technical Description**	**Events**
2	Initial Access	T1566 / T1078	Phishing and use of valid accounts.	Accessing the API and three account information with user_id 1523.
3	Collection	T1005	Collecting data from system.	Collecting 15 account data and files after SQL injection using BAC exploit.
4	Exfiltration	T1041 / T1537	Data leakage via application functionality	Exporting data using API GET requests and Web /dashboard/export function.

1.3.2 OWASP Top 10

	A	B	C	D
1	Category ID	Category Name	Associated Vector	Impact Level
2	A01:2021	Broken Access Control	Mobile API (IDOR)	Critical
3	A03:2021	Injection	Web App. (SQLi)	Critical
4	A07:2021	Identification and Authentication Failures	Phishing Campaign	High

1.4 Root cause analysis

Lack of authorization control in the API: Because Object Level Authorization (OLA) was not implemented, account data of 15 different users was leaked using an authorized user token (log evidence: 06:47:15).

An injection vulnerability in the web application: User input was not handled according to secure coding principles, prepared statements were not used, and therefore the attacker gained access to the database by directly incorporating the input into the query (log evidence: 09:23:45).

Gaps in WAF (Web Application Firewall) configuration: Advanced and obfuscated query evasion rules were missing. As a result, the attacker bypassed the WAF using special syntax.

MFA (Multi-Factor Authentication): Because MFA is not required for all accounts, the impact of phishing attacks has increased, allowing stolen credentials to be used without restriction.

1.5 Impact assessment

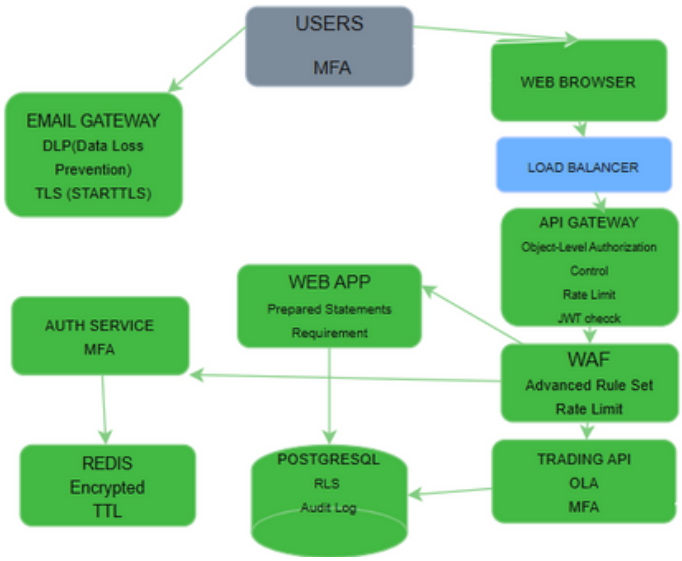
An API Deficiency in Authorization Check (IDOR) and a Web SQL Injection bypass resulted in the unauthorized exfiltration of 15 customer account details and 892KB of bulk transaction data. The theft of three employee credentials increases the risk of lateral expansion within the corporate network, threatening operational integrity.

2 Architecture Review

2.1 Current architecture weaknesses

The incident demonstrates the existence of deep security vulnerabilities at multiple layers of the architecture. These vulnerabilities allowed the cyber attacker to advance unhindered through three main vectors: API, Web, and Identity. The most critical vulnerabilities are at the code level: In the mobile API, the complete lack of an Object Level Authorization (OLA) check, which verifies whether the user is authorized to access the requested resource, directly led to the IDOR vulnerability. In the web application, the lack of Prepared Statements during development was the technical root cause of the SQL injection attack. These code vulnerabilities were reinforced by environmental and identity management vulnerabilities; the WAF was bypassed due to a lack of rulesets against the obfuscated SQL syntax used by the attacker. Furthermore, the lack of a Multi-Factor Authentication (MFA) requirement for corporate accounts ensured the success of the phishing campaign.

2.2 Improved security architecture diagram



2.3 Recommended security controls (with justification)

Vulnerability Area	New Control / Solution	Rationale
IDOR (Insecure Direct Object Reference)	Mandatory OLA (Object-Level Authorization)	Ensures that every API request verifies ownership of the requested resource. Prevents data leakage at the root cause.
SQL Injection	Prepared Statements	Forces all database queries in the application code to separate data inputs from code logic, eliminating injection risks.
MFA Weakness	MFA for All Accounts	Ensures that stolen credentials from phishing attacks are useless and prevents unauthorized access.
Detection/Monitoring Deficiency	Advanced SIEM Correlation and Logging	The new OLA module collects logs from all critical control points. Detects abnormal-speed IDOR scans in real time and automatically responds.

2.4 Defense-in-depth strategy

Layer	Control Point	Secondary Defense (If Primary Fails)	Root Cause Solution
1. Identity	Mandatory MFA	Risk-Based Session Termination	Renders credentials stolen via Phishing useless.
2. Perimeter (API)	API Rate Limiting	Enhanced WAF (BLOCK Mode)	Slows down rapid IDOR scanning; WAF prevents evasion attempts.
3. Authorization (App)	OLA Control Module	Mandatory Prepared Statements	Prevents unauthorized users from accessing other accounts (IDOR) with a 403 response.
4. Data	Prepared Statements	Principle of Least Privilege	Neutralizes all remaining SQLi attempts by treating input as data, not code.
5. Visibility	SIEM Correlation	SOAR Automated Response	Connects failure events from all layers (e.g., OLA errors, WAF detects) and automatically terminates the session upon suspicious activity.

3 Response & Remediation

3.1 Immediate Actions (0–24 Hours)

Attacker Access Disablement: All JWT tokens for the stolen account used in the attack, user_id: 1523, must be immediately revoked, and the password for this account must be reset.
Immediate Blocking in WAF Rules: The WAF rule that detected the obfuscated syntax used by the attacker for SQLi has been upgraded from the "Suspicious SQL Pattern" [DETECT] action to the definitive BLOCK action. This closes the immediate leak vector.
Evidence Protection: During the period of the incident (specifically 06:45 - 09:30 UTC), all API, WAF, Web, and Email logs have been copied and isolated for forensic analysis, ensuring their integrity is intact.

3.2 Short-Term Fixes (1–2 Weeks)

IDOR Vulnerability Remedy (OLA): The Object Level Authorization (OLA) Module is integrated between the API Gateway and the Application Server. This enforces the matching of the token owner and the requested resource owner for every request to the /portfolio/{account_id endpoint.
SQL Injection Vulnerability Remedy: Prepared Statements are strictly used in all queries interacting with the database in the web application. This ensures that user input is processed as data, not as a query.
MFA Requirement: Multi-Factor Authentication (MFA) is immediately mandatory for all corporate accounts, admin panels, and critical users.
Phishing Awareness Training: All employees receive practical training, particularly on identifying phishing URLs and email triggers.

3.3 Long-Term Improvements (1–3 Months)

Zero Trust Architecture Completion: Implemented OLA, MFA, and Prepared Statements controls are extended and standardized across all critical APIs and applications across the organization.
SIEM/SOAR Integration and Automation: New OLA and MFA logs are integrated into the SIEM system. Rules are created to instantly detect rapid IDOR scanning or anomalous login/authorization chains. Automatic session termination capability is added with SOAR for critical alarms.
Penetration Test Validation: An independent external security firm (CyberSec Partners) conducts a penetration test targeting all newly implemented security controls.

3.4 Compliance Considerations

SOC 2 Audit Focal Point: In preparation for the upcoming SOC 2 Type II Audit (November 15-30), the Auditor (PwC) will be contacted. All improvements made and lessons learned from this incident will be presented as primary evidence during the audit, under access control and logging headings.

Audit Evidence Chain: All intervention steps, technical decisions, log analysis reports, and code changes must be documented to create a complete and intact chain of evidence for legal and audit processes.