ACME SECURITY INCIDENT REPORT

Incident ID: INC2025-1109-222

Incident Severity: High

Incident Status: Unresolved

Reporter: Merve Delal YILDIRIM

Report Date: 09.11.2025

Index

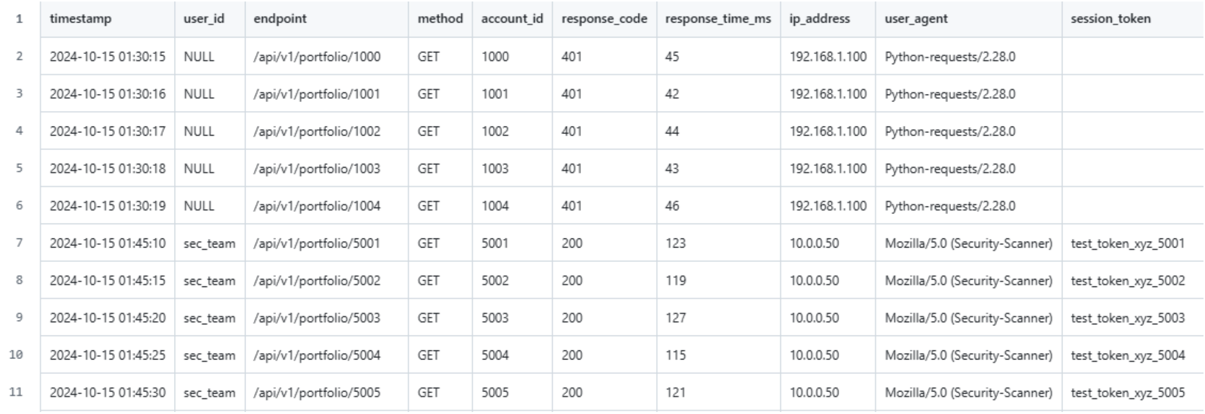
1. General Timeline

Date/Time (UTC)	Activity	Source
2024-10-15 06:46:30	/api/v1/portfolio/1523	api_logs.csv
2024-10-15 06:47:15	/api/v1/portfolio/1524	api_logs.csv
2024-10-15 06:47:18	/api/v1/portfolio/1525	api_logs.csv
2024-10-15 06:47:21	/api/v1/portfolio/1526	api_logs.csv
2024-10-15 06:47:24	/api/v1/portfolio/1527	api_logs.csv
2024-10-15 06:47:27	/api/v1/portfolio/1528	api_logs.csv
2024-10-15 06:47:30	/api/v1/portfolio/1529	api_logs.csv
2024-10-15 06:47:30	/api/v1/portfolio/1529	waf_logs.csv
2024-10-15 06:47:33	/api/v1/portfolio/1530	api_logs.csv
2024-10-15 06:47:36	/api/v1/portfolio/1531	api_logs.csv
2024-10-15 06:47:39	/api/v1/portfolio/1532	api_logs.csv
2024-10-15 06:47:42	/api/v1/portfolio/1533	api_logs.csv
2024-10-15 06:47:45	/api/v1/portfolio/1534	api_logs.csv
2024-10-15 06:47:45	/api/v1/portfolio/1534	waf_logs.csv
2024-10-15 06:47:48	/api/v1/portfolio/1535	api_logs.csv
2024-10-15 06:47:51	/api/v1/portfolio/1536	api_logs.csv
2024-10-15 06:47:54	/api/v1/portfolio/1537	api_logs.csv
2024-10-15 06:47:57	/api/v1/portfolio/1538	api_logs.csv
2024-10-15 06:47:57	/api/v1/portfolio/1538	waf_logs.csv

2024-10-15 08:55:00	/admin/users/export	waf_logs.csv
2024-10-15 08:55:00	/admin/users/export	web_logs.csv
2024-10-15 08:55:12	Q3 Meeting Notes	email_logs.csv
2024-10-15 08:56:30	/admin/download/user_export.csv	web_logs.csv
2024-10-15 09:00:23	/verify-account.php	waf_logs.csv
2024-10-15 09:00:23	URGENT: Verify Your Account - Action Required	email_logs.csv
2024-10-15 09:00:25	URGENT: Verify Your Account - Action Required	email_logs.csv
2024-10-15 09:00:27	URGENT: Verify Your Account - Action Required	email_logs.csv
2024-10-15 09:00:29	URGENT: Verify Your Account - Action Required	email_logs.csv
2024-10-15 09:00:31	URGENT: Verify Your Account - Action Required	email_logs.csv
2024-10-15 09:00:33	URGENT: Verify Your Account - Action Required	email_logs.csv
2024-10-15 09:20:30	/dashboard/search,ticker=AAPL' OR 1=1--	web_logs.csv
2024-10-15 09:21:15	/dashboard/search,ticker=AAPL'; DROP TABLE users--	web_logs.csv
2024-10-15 09:22:00	/dashboard/search,ticker=AAPL' UNION SELECT * FROM users--	web_logs.csv
2024-10-15 09:23:45	/dashboard/search	waf_logs.csv
2024-10-15 09:23:45	/dashboard/search,ticker=AAPL' /*!50000OR*/ 1=1--	web_logs.csv
2024-10-15 09:24:10	/dashboard/export,format=csv	web_logs.csv

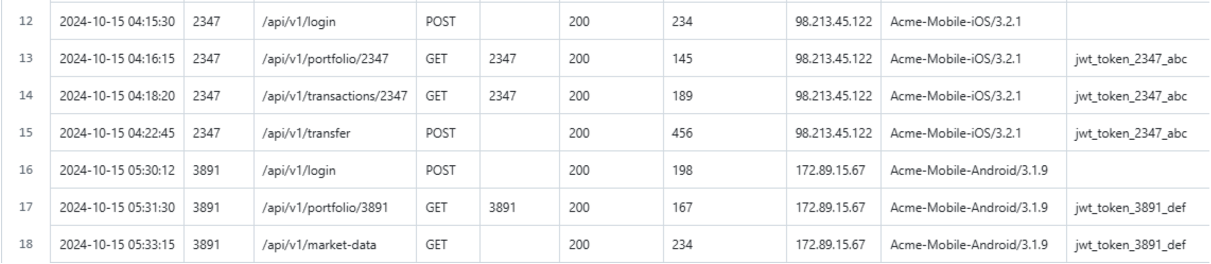
2. Technical Details

2.1 API Log Details

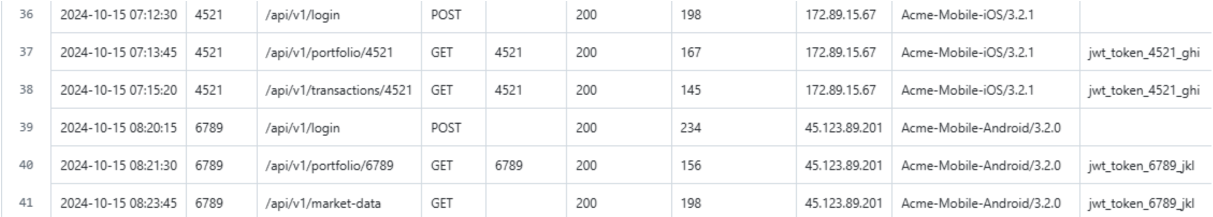


timestamp	user_id	endpoint	method	account_id	response_code	response_time_ms	ip_address	user_agent	session_token
2024-10-15 01:30:15	NULL	/api/v1/portfolio/1000	GET	1000	401	45	192.168.1.100	Python-requests/2.28.0	
2024-10-15 01:30:16	NULL	/api/v1/portfolio/1001	GET	1001	401	42	192.168.1.100	Python-requests/2.28.0	
2024-10-15 01:30:17	NULL	/api/v1/portfolio/1002	GET	1002	401	44	192.168.1.100	Python-requests/2.28.0	
2024-10-15 01:30:18	NULL	/api/v1/portfolio/1003	GET	1003	401	43	192.168.1.100	Python-requests/2.28.0	
2024-10-15 01:30:19	NULL	/api/v1/portfolio/1004	GET	1004	401	46	192.168.1.100	Python-requests/2.28.0	
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
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
2024-10-15 01:45:20	sec_team	/api/v1/portfolio/5003	GET	5003	200	127	10.0.0.50	Mozilla/5.0 (Security-Scanner)	test_token_xyz_5003
2024-10-15 01:45:25	sec_team	/api/v1/portfolio/5004	GET	5004	200	115	10.0.0.50	Mozilla/5.0 (Security-Scanner)	test_token_xyz_5004
2024-10-15 01:45:30	sec_team	/api/v1/portfolio/5005	GET	5005	200	121	10.0.0.50	Mozilla/5.0 (Security-Scanner)	test_token_xyz_5005

The log start time **(01:30:15)** closely aligns with the test's scheduled start time of 01:30 AM PST. The **IP address 192.168.1.100 matches the source IP** specified in the test report. The **user_agent field in the logs, specifying Python-requests/2.28.0**, confirms that the activity originates from the internal security scanner, which is documented as being Python-based. The **401 Unauthorized response code** in the logs supports the test's expected activity of "Failed login attempts (testing auth)". Furthermore, the sequential endpoint queries (/1000, /1001, etc.) are consistent with the "Sequential endpoint probing" activity. Crucially, the activity targeted the "API endpoints" which are **within the documented scope of the test**. All technical parameters and the timing of the activity have been validated against "Test 1: Automated Vulnerability Scanning," which was planned and documented by the internal security team. No malicious external attack or unauthorized internal activity has been detected. The logs reflect the expected and approved operation of the vulnerability scanning tool.

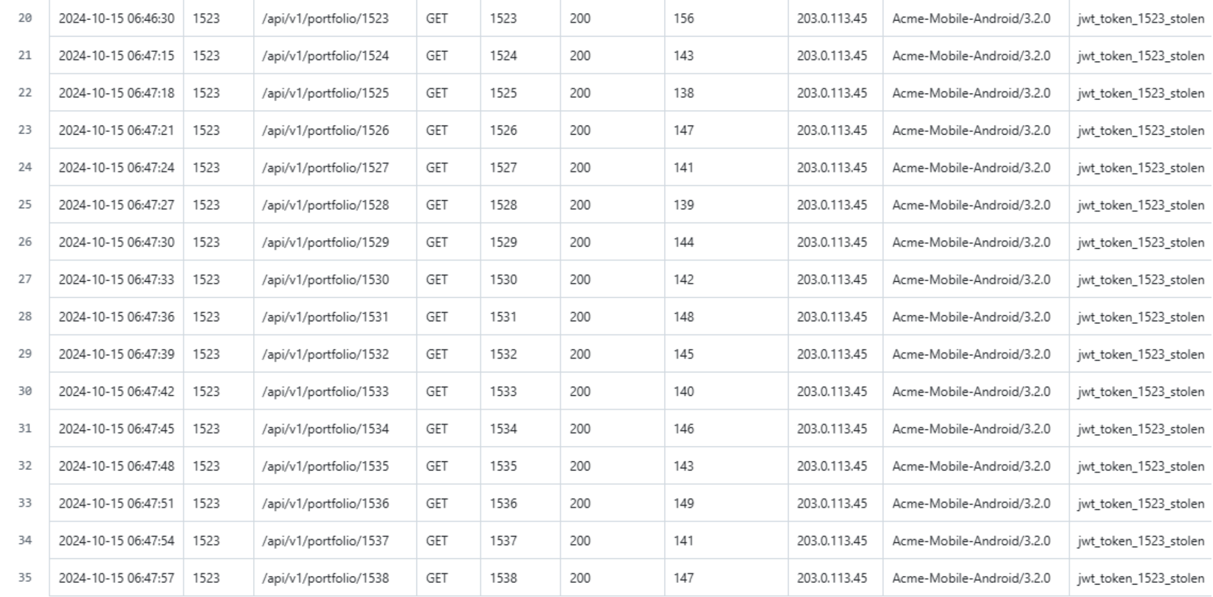


12	2024-10-15 04:15:30	2347	/api/v1/login	POST		200	234	98.213.45.122	Acme-Mobile-iOS/3.2.1	
13	2024-10-15 04:16:15	2347	/api/v1/portfolio/2347	GET	2347	200	145	98.213.45.122	Acme-Mobile-iOS/3.2.1	jwt_token_2347_abc
14	2024-10-15 04:18:20	2347	/api/v1/transactions/2347	GET	2347	200	189	98.213.45.122	Acme-Mobile-iOS/3.2.1	jwt_token_2347_abc
15	2024-10-15 04:22:45	2347	/api/v1/transfer	POST		200	456	98.213.45.122	Acme-Mobile-iOS/3.2.1	jwt_token_2347_abc
16	2024-10-15 05:30:12	3891	/api/v1/login	POST		200	198	172.89.15.67	Acme-Mobile-Android/3.1.9	
17	2024-10-15 05:31:30	3891	/api/v1/portfolio/3891	GET	3891	200	167	172.89.15.67	Acme-Mobile-Android/3.1.9	jwt_token_3891_def
18	2024-10-15 05:33:15	3891	/api/v1/market-data	GET		200	234	172.89.15.67	Acme-Mobile-Android/3.1.9	jwt_token_3891_def



36	2024-10-15 07:12:30	4521	/api/v1/login	POST		200	198	172.89.15.67	Acme-Mobile-iOS/3.2.1	
37	2024-10-15 07:13:45	4521	/api/v1/portfolio/4521	GET	4521	200	167	172.89.15.67	Acme-Mobile-iOS/3.2.1	jwt_token_4521_ghi
38	2024-10-15 07:15:20	4521	/api/v1/transactions/4521	GET	4521	200	145	172.89.15.67	Acme-Mobile-iOS/3.2.1	jwt_token_4521_ghi
39	2024-10-15 08:20:15	6789	/api/v1/login	POST		200	234	45.123.89.201	Acme-Mobile-Android/3.2.0	
40	2024-10-15 08:21:30	6789	/api/v1/portfolio/6789	GET	6789	200	156	45.123.89.201	Acme-Mobile-Android/3.2.0	jwt_token_6789_jkl
41	2024-10-15 08:23:45	6789	/api/v1/market-data	GET		200	198	45.123.89.201	Acme-Mobile-Android/3.2.0	jwt_token_6789_jkl

These log activities demonstrate a successful login, data viewing, and transfer flow performed by legitimate users utilizing the mobile application.



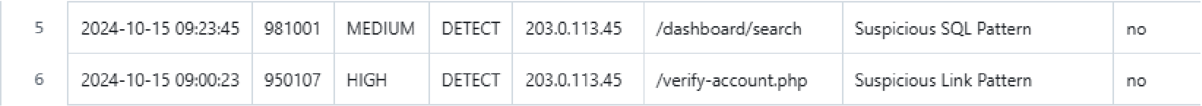
20	2024-10-15 06:46:30	1523	/api/v1/portfolio/1523	GET	1523	200	156	203.0.113.45	Acme-Mobile-Android/3.2.0	jwt_token_1523_stolen
21	2024-10-15 06:47:15	1523	/api/v1/portfolio/1524	GET	1524	200	143	203.0.113.45	Acme-Mobile-Android/3.2.0	jwt_token_1523_stolen
22	2024-10-15 06:47:18	1523	/api/v1/portfolio/1525	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

The **HTTP Response Code 200** on these access attempts indicates that the token granted access not only to its own user_id but also to **other user IDs**. From /api/v1/portfolio/1523 to /1538, the attacker attempted **horizontal access** by manipulating the object ID (user_id) in the URL path. Specifically, the attacker targeted the GET /api/v1/portfolio/{user_id} endpoint with the **compromised token** and successfully accessed the data of unauthorized users by sequentially changing the {user_id} field (e.g., 1523, 1524, 1525...). This is further supported by the **external origin of the Source IP**. Furthermore, **16 requests in approximately 90 seconds** strongly suggest the use of an automated script or tool.

2.1.1 Attack Vector Indenfitication and Classification

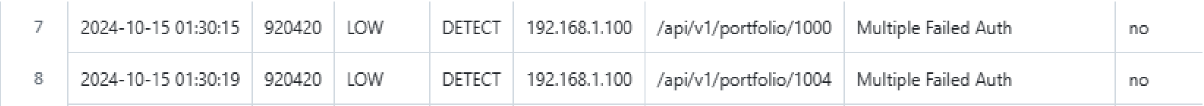
API IDOR/BOLA: Concurrently, the critical Broken Access Control vulnerability **(OWASP A01:2021/BOLA)** on the Trading API was exploited through sequential **account_id** attempts, a **MITRE ATT&CK T1083 (Resource Enumeration) technique**, and portfolio data was collected using the **T1530 (Data from Central Repository) technique.**

2.2 WAF Log Details



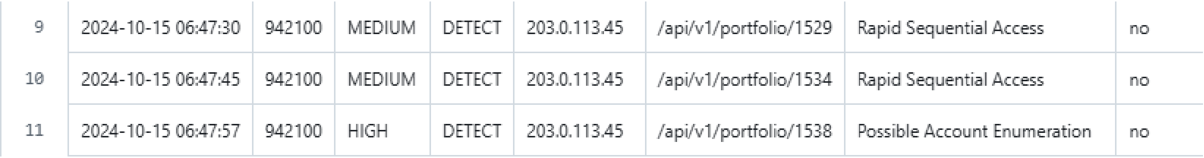
5	2024-10-15 09:23:45	981001	MEDIUM	DETECT	203.0.113.45	/dashboard/search	Suspicious SQL Pattern	no
6	2024-10-15 09:00:23	950107	HIGH	DETECT	203.0.113.45	/verify-account.php	Suspicious Link Pattern	no

The **Web Application Firewall (WAF) successfully detected (DETECT)** suspicious activities (**Suspicious SQL Pattern and Suspicious Link Pattern**) originating from the external source (203.0.113.45). However, the **'no' value in the logs indicates that the traffic was not blocked (BLOCK)** as a WAF rule action. This suggests that the WAF remained in detection mode, allowing an **active SQL Injection (SQLi) or link manipulation attempt to pass through** to the system. This constitutes a **security control failure requiring immediate (HIGH) intervention**.



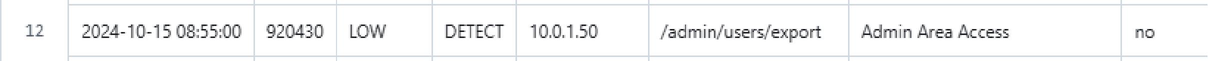
7	2024-10-15 01:30:15	920420	LOW	DETECT	192.168.1.100	/api/v1/portfolio/1000	Multiple Failed Auth	no
8	2024-10-15 01:30:19	920420	LOW	DETECT	192.168.1.100	/api/v1/portfolio/1004	Multiple Failed Auth	no

The referenced log entries originate from the internal IP address **192.168.1.100**. This source IP, along with the **'Multiple Failed Auth'** alert, aligns perfectly with the activity expected from the documented **'Test 1: Automated Vulnerability Scanning.'** As detailed in the test plan, this Python-based scanning tool is anticipated to generate such **LOW-severity** alerts during its operation. Consequently, this activity is not deemed suspicious.



9	2024-10-15 06:47:30	942100	MEDIUM	DETECT	203.0.113.45	/api/v1/portfolio/1529	Rapid Sequential Access	no
10	2024-10-15 06:47:45	942100	MEDIUM	DETECT	203.0.113.45	/api/v1/portfolio/1534	Rapid Sequential Access	no
11	2024-10-15 06:47:57	942100	HIGH	DETECT	203.0.113.45	/api/v1/portfolio/1538	Possible Account Enumeration	no

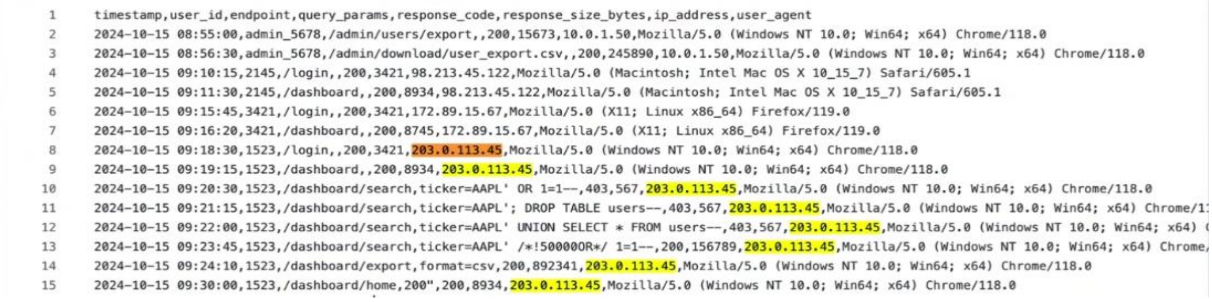
The **Web Application Firewall (WAF) detected** suspicious API access attempts originating from the **attacker's IP address (203.0.113.45)**. The alerts, specifically **'Rapid Sequential Access'** and 'Possible Account Enumeration,' corroborate the observed **Broken Object Level Authorization (BOLA) exploitation attempt** detailed in the API logs. However, the **DETECT action** and the corresponding 'no' value indicate that the WAF remained in detection-only mode instead of blocking this critical activity. This confirms that the WAF **failed to prevent the successful unauthorized accesses (HTTP 200)** observed in the API logs (Rows 20-35), necessitating an immediate review of the WAF rule's enforcement action.



12	2024-10-15 08:55:00	920430	LOW	DETECT	10.0.1.50	/admin/users/export	Admin Area Access	no

Access to the administrative panel endpoint (/admin/users/export) was detected originating from the **internal IP address 10.0.1.50**. This activity triggered an 'Admin Area Access' rule and potentially resulted in the **exportation of all user data**. The WAF classified this activity as **LOW-severity and failed to block it** (indicated by 'no' action), likely due to its internal origin. While this action may have been performed by an authorized administrator, the bulk exportation of user data is inherently suspicious and highly sensitive under corporate policy. Given the **potential for Insider Threat**, immediate verification of the account associated with the 10.0.1.50 IP and the justification for this data export is mandatory.

2.3 WEB Log Details



```
1    timestamp,user_id,endpoint,query_params,response_code,response_size_bytes,ip_address,user_agent
2    2024-10-15 08:55:00,admin_5678,/admin/users/export,,200,15673,10.0.1.50,Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/118.0
3    2024-10-15 08:56:30,admin_5678,/admin/download/user_export.csv,,200,245890,10.0.1.50,Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/118.0
4    2024-10-15 09:10:15,2145,/login,,200,3421,98.213.45.122,Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) Safari/605.1
5    2024-10-15 09:11:30,2145,/dashboard,,200,8934,98.213.45.122,Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) Safari/605.1
6    2024-10-15 09:15:45,3421,/login,,200,3421,172.89.15.67,Mozilla/5.0 (X11; Linux x86_64) Firefox/119.0
7    2024-10-15 09:16:20,3421,/dashboard,,200,8745,172.89.15.67,Mozilla/5.0 (X11; Linux x86_64) Firefox/119.0
8    2024-10-15 09:18:30,1523,/login,,200,3421,203.0.113.45,Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/118.0
9    2024-10-15 09:19:15,1523,/dashboard,,200,8934,203.0.113.45,Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/118.0
10   2024-10-15 09:20:30,1523,/dashboard/search,ticker=AAPL' OR 1=1--,403,567,203.0.113.45,Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/118.0
11   2024-10-15 09:21:15,1523,/dashboard/search,ticker=AAPL'; DROP TABLE users--,403,567,203.0.113.45,Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/1
12   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) (
13   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,
14   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
15   2024-10-15 09:30:00,1523,/dashboard/home,200",200,8934,203.0.113.45,Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/118.0
```

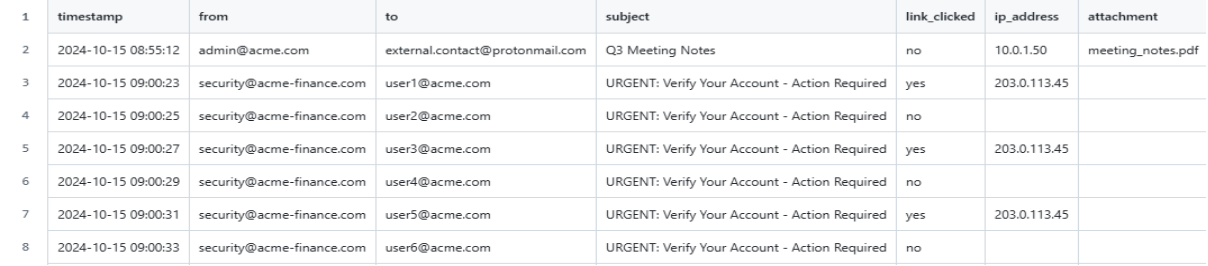
In rows 2-3, **user admin_5678** may have exported the user list from the admin panel via the **internal IP 10.0.1.50**. The log shows the file download **(download/user_export.csv)**. This activity is associated with the previously observed WAF alert for 'Admin Area Access.' The **WAF's failure to block this internal action** may have led to a potential **Insider Data Leakage risk**. In rows 8-15, the **attacker (203.0.113.45) successfully logged in** at 09:18:30 using **user_id 1523** (/login, response_code: 200). The attacker targeted the /dashboard/search?ticker=... endpoint. In row 11, **destructive commands such as DROP TABLE USERS** were attempted, indicating an intent to **compromise database integrity**.

In row 12, the attacker executed a **successful SQL Injection** using the command **UNION SELECT * FROM users**. This command shows an attempt to access **all user data** that the application should not normally return, **confirming that data compromise occurred**. Data Exfiltration happened in row 14: after the SQLi was successful, the attacker performed **data export in CSV format** (/dashboard/export, format=csv). This indicates that the attacker **successfully exfiltrated the compromised data** from the system.

2.3.1 Attack Vector Indenfitication and Classification

SQL Injection: The attacker injected the **//!50000OR/ payload** into the **/dashboard/search endpoint** (OWASP A03:2021), **bypassing WAF defenses** using the **MITRE ATT&CK T1055 (Defense Evasion) technique**, and exploiting the public-facing application via the T1190 (Exploit Public-Facing Application) technique.

2.4 Email Log Details



1	timestamp	from	to	subject	link_clicked	ip_address	attachment
2	2024-10-15 08:55:12	admin@acme.com	external.contact@protonmail.com	Q3 Meeting Notes	no	10.0.1.50	meeting_notes.pdf
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		

At **08:55:12 UTC**, a potential **data exfiltration occurred** as a file (meeting_notes.pdf), possibly related to the exported user data, was sent from **admin@acme.com** via the **internal IP 10.0.1.50** to a **suspicious external recipient (external.contact@protonmail.com)**. This transaction **reinforces the Insider Threat potential** observed in the bulk data export activity (/admin/users/export).

Users were targeted with **'URGENT: Verify Your Account' phishing emails** sent from a domain (**security@acme-finance.com**) external to the corporate domain (acme.com). Crucially, the **external IP 203.0.113.45**, which was **linked to the prior SQLi and BOLA attacks**, was **immediately used to access the accounts of users who clicked the link** (user1, user3, user5). This confirms a **strong association** between the 203.0.113.45 attacker and the phishing campaign designed to harvest user credentials.

2.4.1 Attack Vector Indenfitication and Classification

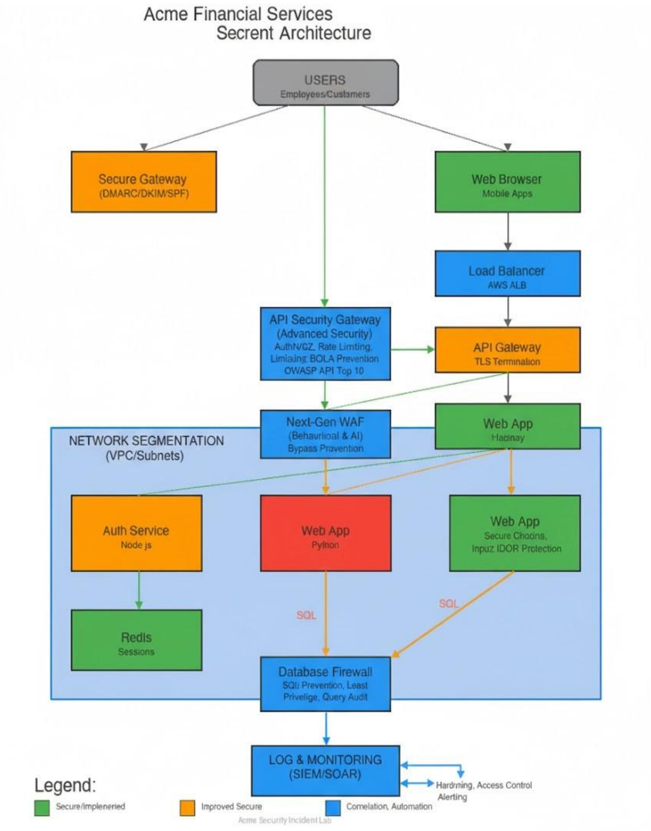
Phishing: The **threat actor utilized the false identity of security@acme-finance.com** to send **"URGENT" emails**, implementing the **MITRE ATT&CK T1566.002 (Spearphishing Link) technique**, thereby aiming to bypass the organization's **authentication controls (OWASP A07:2021)**.

3. Architecture Rewiew

3.1 Current Architecture Weaknesses

Critical API Vulnerabilities: Both the Web App and Trading API are susceptible to SQL Injection and BOLA/IDOR due to their use of direct SQL connections to the database.

WAF Failure and Remediation: The WAF exhibited a **critical defense failure** by only **DETECTING** high-priority attacks and **failing to BLOCK** them. Remediation requires implementing a **Next-Gen WAF** with **behavioral analysis** and bypass prevention capabilities, moving beyond basic rule sets.



Advanced API Security: Upgrade the API Gateway beyond just TLS termination to incorporate **BOLA/IDOR prevention**, rate limiting, and OWASP API Top 10 protections.

Email Security: Utilize a Secure Email Gateway with **DMARC, DKIM, and SPF** configurations for advanced phishing and spoofing protection.

Centralized Monitoring & Response: Establish a central **SIEM/SOAR** platform for log collection, correlation, and automated response triggering.

3.2 Improved Security Architecture Diagram

Advanced API Security: Upgrade the API Gateway beyond just TLS termination to incorporate BOLA/IDOR prevention, rate limiting, and OWASP API Top 10 protections.

Next-Gen WAF: Implement a Next-Gen WAF with **behavioral analysis** and bypass prevention capabilities, moving beyond basic rule sets.

Database Protection: Position a **Database Firewall (DBF)** in front of the database to audit all SQL queries and enforce the **Least Privilege** principle.

Network Segmentation: Establish **strict network segmentation** (VPC/Subnets) between all layers (Web, API, DB), enforced by firewall rules.

Email Security: Utilize a Secure Email Gateway with **DMARC, DKIM, and SPF** configurations for advanced phishing and spoofing protection.

Centralized Monitoring & Response: Establish a central **SIEM/SOAR** platform for log collection, correlation, and automated response triggering.

4. Response & Remediation

4.1 Immediate Actions

Network Blocking Permanently block the attacker's IP address **(203.0.113.45)** across all security layers **(WAF, Firewall)**. Account Suspension Immediately suspend the compromised account **(User ID 1523)** and the suspected Insider Threat account **(admin_5678)**. Terminate all active sessions (session tokens) belonging to the suspended accounts. Mandatory Reset Force password resets and terminate active sessions for users who clicked the phishing link **(user1, user3, and user5)**. System Offline Place the **/api/v1/portfolio/** and **/dashboard/search** endpoints into maintenance mode until short-term fixes are deployed.

4.2 Short-Term Fixes

API (IDOR) Fix Implement **server-side authorization** on /api/v1/portfolio/{account_id} to **verify that the user_id in the JWT token matches the requested account_id**. Web (SQLi) Fix Rewrite the SQL query for the /dashboard/search endpoint using **parameterized queries (prepared statements)**. WAF Hardening **Update the WAF rule set**. Change the action for critical rules (e.g., "Possible Account Enumeration," "Suspicious SQL Pattern") from **DETECT to BLOCK**. Insider Threat Investigation Initiate a **full forensic analysis** of the **admin_5678 account** and the device with IP 100150. Awareness Alert Issue an **alert to all personnel** regarding the **phishing attack** from security@acme-financecom.

4.3 Long-Term Improvements

Secure SDLC **Integrate mandatory security testing (SAST/DAST)** into the Software Development Lifecycle (**SDLC**). DLP Solution Implement a **Data Loss Prevention (DLP) solution** to automatically detect and **prevent the exfiltration of critical data** to external email addresses. SIEM/SOAR Integration Establish a **centralized SIEM solution** with **correlation rules** (WAF DETECT + API 200 OK) to enable **automated response**. Advanced API Gateway Implement a **modern API Security Gateway** to enforce **BOLA/IDOR protection**, advanced rate limiting, and anomaly detection. Network Segmentation Apply **strict network segmentation** between the application layers (Web, API, DB) to **restrict lateral movement**. Security Training Conduct **mandatory and regular security awareness training**, including practical **phishing simulations**.