Security Incident Analysis Report

(Assistant Specialist Candidate Report)

October 2024

Report Prepared by (Analyst) Halil AL	SA
Event Start Date	October 15, 2024
Event End Date	October 15, 2024
Approved by / SOC Manager -	
Institution / System Name	Acme Financial Services
Event	Token Reuse > Broken Access Control (IDOR) > Phishing > SQL Injection

This report was prepared by Acme SOC. It should be emailed to the relevant departments.

Machine Translated by Google

Part 1: Event Analysis

Summary

On October 15, 2024, a coordinated, multi-pronged cyber attack occurred on the Acme Financial Services Trading Platform. The attack vectors to which the institution was exposed within the scope of the attack are listed below:

- Social Engineering (Phishing Technique): Phishing campaign targeting employees
- Token Reuse: API exploitation using Broken Access Control (IDOR) technique
- SQL Injection: Web Application Exploitation

The attacker carried out all steps via the IP address 203.0.113.45. The WAF blocked 3/8 of the 8 attacks. Data leaks occurred through the IDOR vulnerability due to insufficient API controls, and through SQL injection due to incomplete configuration in the WEB Application.

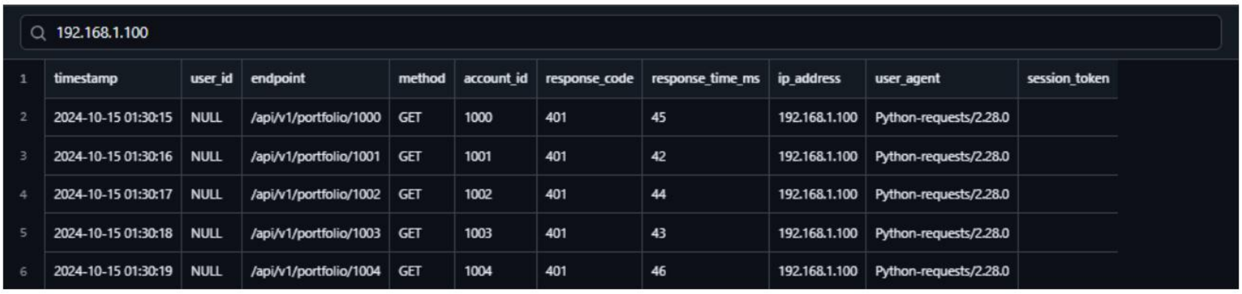
Timeline

Time	Stage		Source IP	Situation
01:30:15 - 01:30:19	Recon	Incident 192.168.1.100 API brute	192.168.1.100	Detected
06:45:10 - 06:47:57	Exploitation	force jwt_token_1523_stolen was used to query 15 accounts	203.0.113.45	Successful
09:00:23	First Access	Phishing campaign (acme-finance.com)	203.0.113.45	Users (1,3,5) Affected
09:18:30	Log in	user 1523 logged into the web	203.0.113.45	Authorized Access
09:20:30 - 09:23:45	Exploitation	/dashboard/search SQLi chain (OR 1=1 ÿ DROP TABLE ÿ (UNION SELECT)	203.0.113.45	Partially Blocked
09:24:10	Data Theft	/dashboard/export ÿ 892 KB CSV output	203.0.113.45	Successful
10:15:30 - 11:25:45	Normal Traffic	Other user activities	45.123.89.201, 172.89.15.67	Normal

Technical Findings

1. Script Work

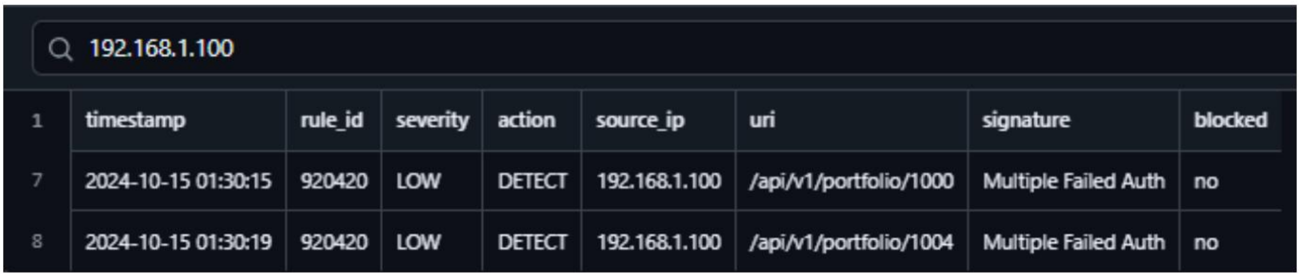
As can be seen in Figure 1, a Python script was run on the internal network at LAN IP 192.168.1.100. The script runs at 1-second intervals, sending API requests for accounts with IDs 1000-1004, and returns a 401 response. In Figure 1.2, the WAF sees the responses but doesn't block them because they are LAN IP addresses.



192.168.1.100

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	

Figure 1 (API Logs)



192.168.1.100

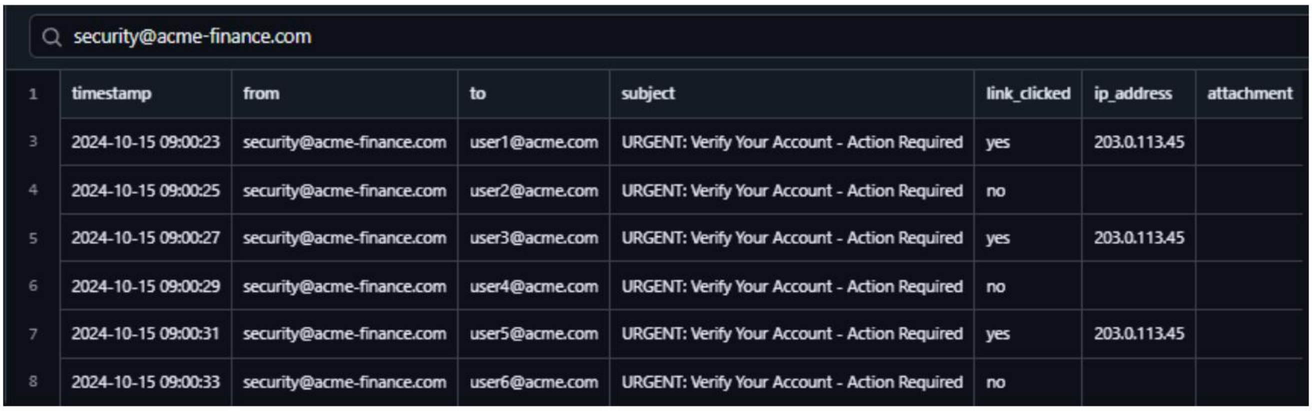
1	timestamp	rule_id	severity	action	source_ip	uri	signature	blocked
7	2024-10-15 01:30:15	920420	LOW	DETECT	192.168.1.100	/api/v1/portfolio/1000	Multiple Failed Auth	no
8	2024-10-15 01:30:19	920420	LOW	DETECT	192.168.1.100	/api/v1/portfolio/1004	Multiple Failed Auth	no

Figure 1.2 (WAF Logs)

2. Social Engineering (Phishing Technique)

As can be seen in Figure 2, the attacker conducted a phishing attack on company employees via security@acme-finance.com and 203.0.113.45. Three of the six targets clicked the link and were exposed to the phishing attack. The exposed users are users 1, 3, and 5. The information of the attackers exposed to the phishing attack was obtained.

Security Measure: Cyber Security Awareness Training should be given to the institution's employees.



security@acme-finance.com

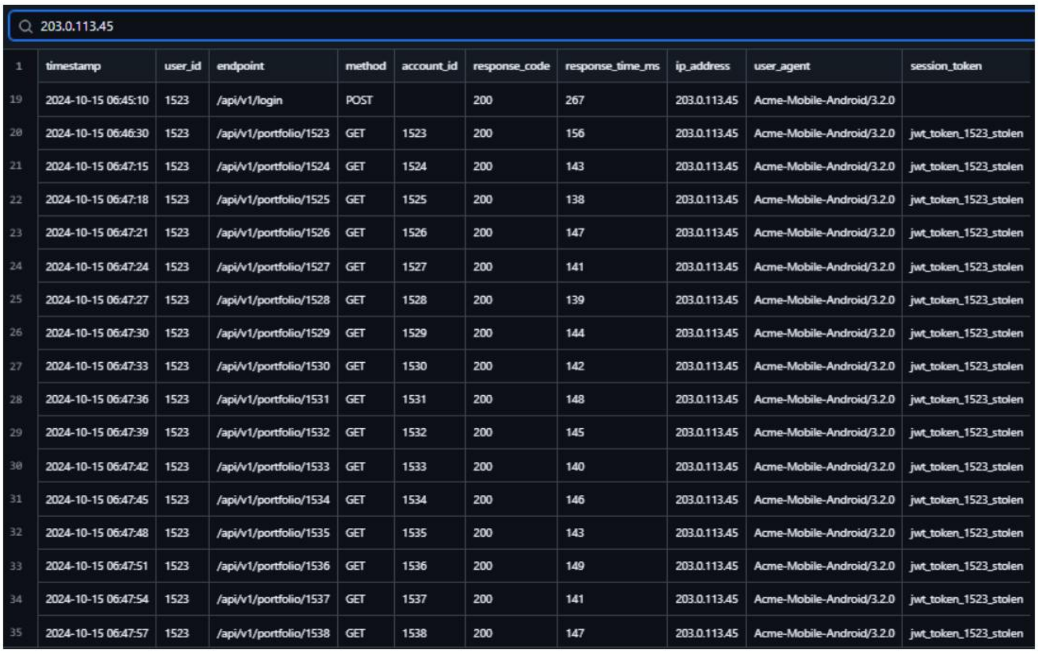
1	timestamp	from	to	subject	link_clicked	ip_address	attachment
3	2024-10-15 09:00:23	security@acme-finance.com	user1@acme.com	URGENT: Verify Your Account - Action Required	yes	203.0.113.45	
4	2024-10-15 09:00:25	security@acme-finance.com	user2@acme.com	URGENT: Verify Your Account - Action Required	no		
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		

Figure 2 (Email Logs)

3. API Attack

The attacker exploiting the IDOR vulnerability logs into the system with the user ID 1523. After logging in, the attacker accesses the portfolios of 15 users located between /portfolio/{1524–1538} and performs the exploit. The token used for the 15 users is "jwt_token_1523_stolen."

Security Measure: The code “if g.current_user.account_id != account_id:” should be added to the control mechanism to ensure the user_id and account_id match.



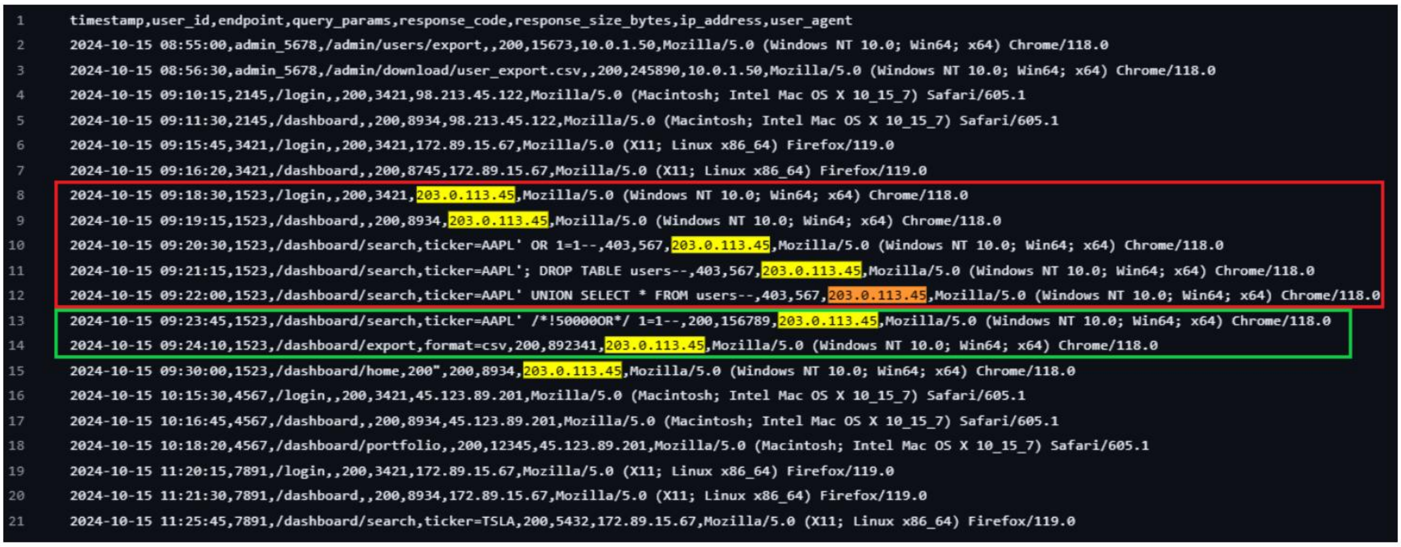
203.0.113.45

timestamp	user_id	endpoint	method	account_id	response_code	response_time_ms	ip_address	user_agent	session_token
2024-10-15 06:45:10	1523	/api/v1/login	POST		200	267	203.0.113.45	Acme-Mobile-Android/3.2.0	
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Figure 3 (API Logs)

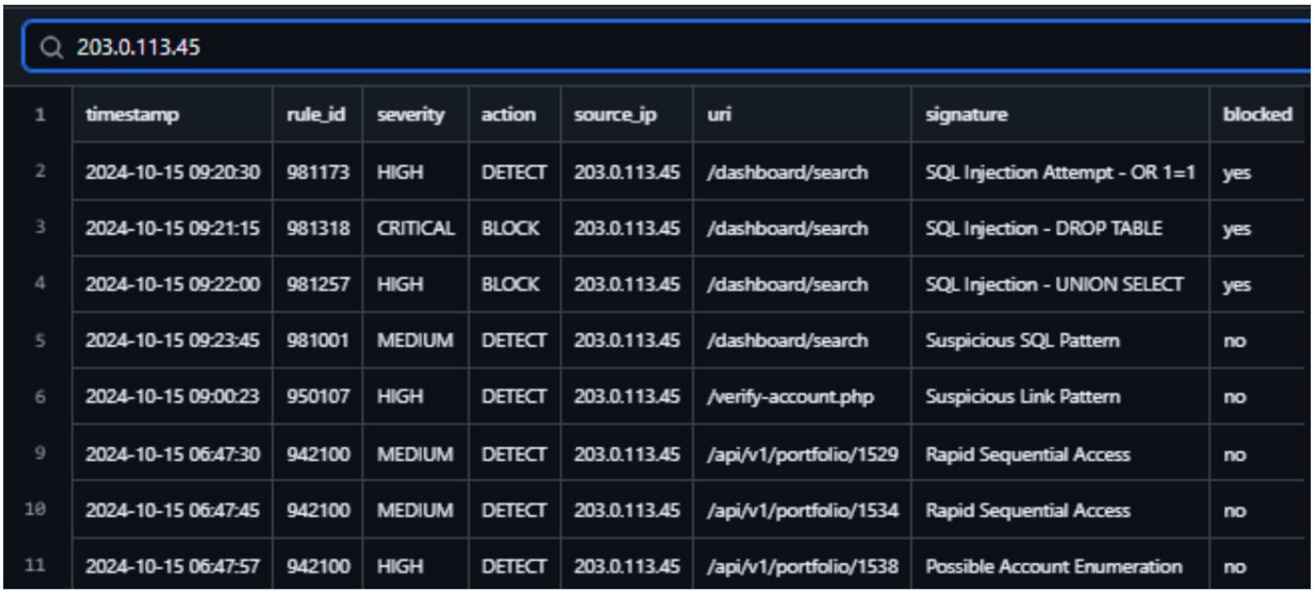
4. Web Attack

In the Web Attack, the attacker's first three attempts failed, as seen in Figures 4 and 4.1. The WAF blocked the requests and returned a 403 response. However, the WAF was bypassed with the query "/!50000OR/ 1=1--", and the SQL injection was successfully executed. As can be seen in the "/dashboard/export" response, 892 KB of data was exfiltrated in CSV format.



```
timestamp,user_id,endpoint,query_params,response_code,response_size_bytes,ip_address,user_agent
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
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
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
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
2024-10-15 09:15:45,3421,/login,,200,3421,172.89.15.67,Mozilla/5.0 (X11; Linux x86_64) Firefox/119.0
2024-10-15 09:16:20,3421,/dashboard,,200,8745,172.89.15.67,Mozilla/5.0 (X11; Linux x86_64) Firefox/119.0
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
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
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
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/118.0
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) Chrome/118.0
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/118.0
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
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
2024-10-15 10:15:30,4567,/login,,200,3421,45.123.89.201,Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) Safari/605.1
2024-10-15 10:16:45,4567,/dashboard,,200,8934,45.123.89.201,Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) Safari/605.1
2024-10-15 10:18:20,4567,/dashboard/portfolio,,200,12345,45.123.89.201,Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) Safari/605.1
2024-10-15 11:20:15,7891,/login,,200,3421,172.89.15.67,Mozilla/5.0 (X11; Linux x86_64) Firefox/119.0
2024-10-15 11:21:30,7891,/dashboard,,200,8934,172.89.15.67,Mozilla/5.0 (X11; Linux x86_64) Firefox/119.0
2024-10-15 11:25:45,7891,/dashboard/search,ticker=TSLA,200,5432,172.89.15.67,Mozilla/5.0 (X11; Linux x86_64) Firefox/119.0
```

Figure 4



203.0.113.45

1	timestamp	rule_id	severity	action	source_ip	uri	signature	blocked
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
6	2024-10-15 09:00:23	950107	HIGH	DETECT	203.0.113.45	/verify-account.php	Suspicious Link Pattern	no
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

Figure 4.1

Root Causes of the Attack's Success

- There was no MFA requirement ÿ session information was stolen through phishing.
- Lack of account ownership verification in API.
- WAF stuck in “Detect” mode for some rules.
- SOC correlation rules did not follow IP-based chains.
- Lack of awareness among institution employees

MITRE ATT&CK Mapping

Tactics	Technical	Explanation
First Access	T1566.002 – Phishing Link T1556.003 –	Users were deceived
Credential Access	Web Portal Phishing	Token leak
Lateral Movement	T1550.001 – Web Token Usage	token reuse in API
Collection	T1213.003 – Data from Repositories Other user data was withdrawn	
Infiltration	T1041 – Data leaked via Web Services / export CSV	
Effect	T1485 – Data Destruction Attempt	Attempting to delete data with the DROP TABLE statement

OWASP Mapping

Technical	Title	Explanation
A01	Broken Access Control	API IDOR
A03	Injection	SQL Injection
A05	Security Misconfiguration	WAF False Detection
A07	Identification & Authentication Errors	Lack of MFA
A09	Recording & Monitoring Faults	No SOC correlation

IOC List

Type	Value	Explanation
ROPE	203.0.113.45	**Attacker IP**
Domain Name	acme-finance.com	Phishing domain name
Email	security@acme-finance.com	**Email Used**
Token	jwt_token_1523_stolen	**JWT Token used**
URL	/dashboard/search	SQL Injection target

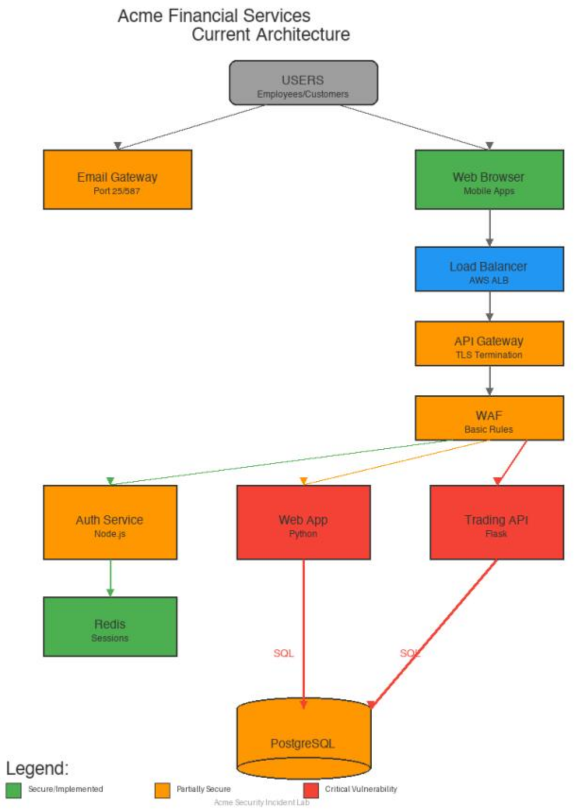
File	user_export.csv	Leaked data

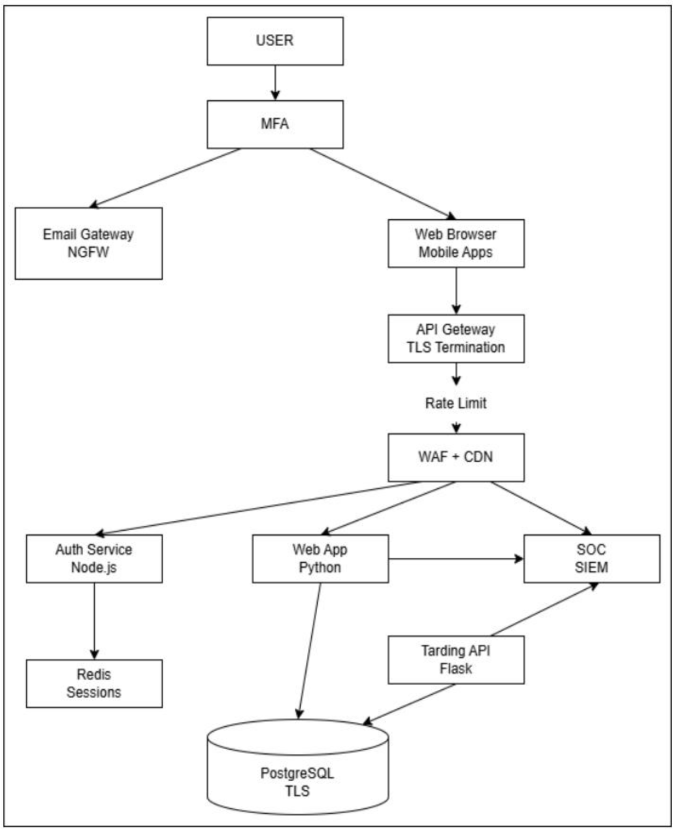
Impact Assessment

- Data Privacy: Users' data has been leaked
- Data Integrity: An attempt was made to disrupt data integrity with the Drop Table command, but the request was blocked by the WAF.
- System Security: The system was infiltrated due to incorrect configuration, MFA, and incomplete control.
- Risk level was determined as 5/5.

Chapter 2: Architectural Review

Current Architecture	Improved Architecture





Chapter 3: Response & Recovery

- Instant actions (0-24 hours)

  The IP should be quarantined and blacklisted via SIEM.
  User sessions must be terminated and all JWTs must be revoked.

  User accounts that are subject to phishing attacks should be blocked and suspended.
- Short-term corrections (1-2 weeks)

  o /portfolio/{id} endpoints should have ownership status checks added

  o Rate Limit should be added and MFA should be required for all users
- Long-term improvements (1-3 months)

  o WAF + API logs should be integrated into SIEM

  o Awareness training should be provided for the institution and phishing drills should be conducted.

  WAF rules should be revised to prevent SQL Injection

Conclusion

The attacker gained access to the system using a multi-pronged chain attack: "Token Reuse > Broken Access Control (IDOR) > Phishing > SQL Injection." After access, the attacker used the "/export" command .

Data leaks were made using CSV. This attack chain was not detected due to the lack of a layered SOC and an integrated structure. Taking precautions can prevent the recurrence of the same attack chain vectors.