INCIDENT REPORT

AYŞE AKIN

7.11.2025 – 10.11.2025

SUMMARY

The suspicious IP address is included in the IP range specified in the Manual Penetration Test section, but the test did not take place on the scheduled date and has not yet been officially approved.

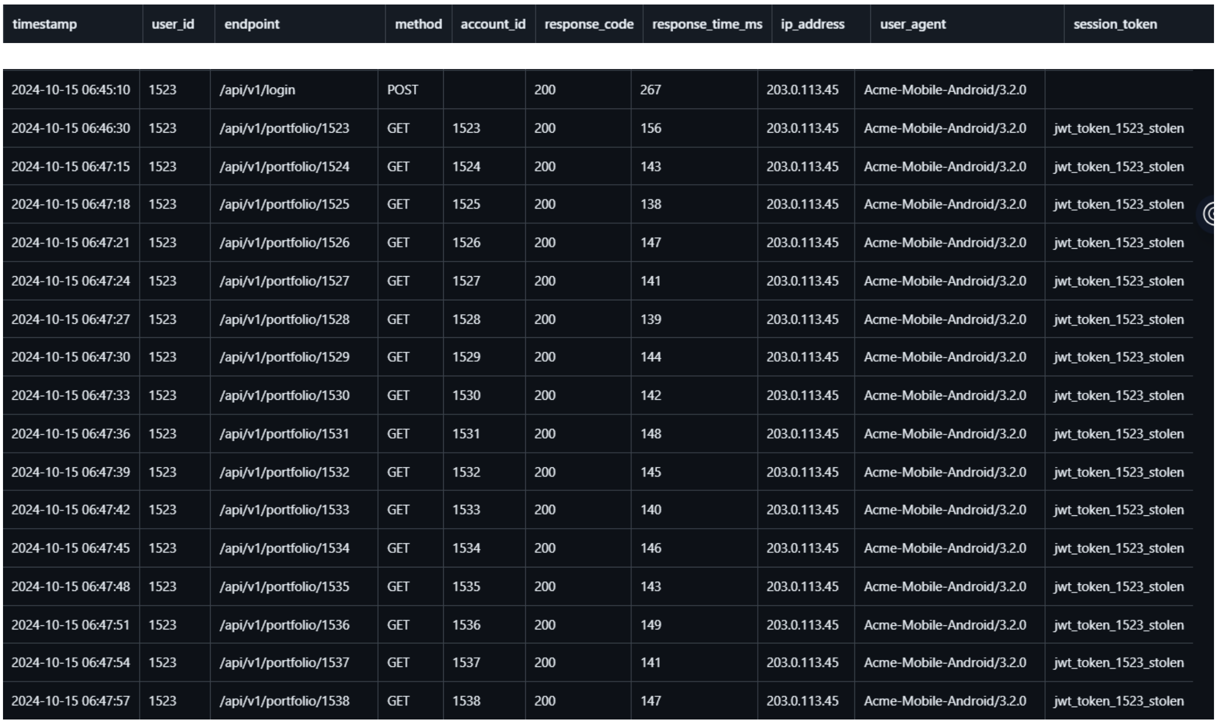
IDOR: User 1523 was able to query other user IDs with their own token and gained unauthorized access. This vulnerability allows unauthorized access to users' accounts or data.

Phishing: The credentials of user1, user3, and user4 accounts were compromised via emails sent from security@acme-finance.com. This allowed the attacker to log into the user1 account.

SQL Injection: Attempts were made to gain unauthorized access to the database and manipulate data using the payloads provided in the report. Some payloads were blocked by the WAF, while others bypassed the WAF.

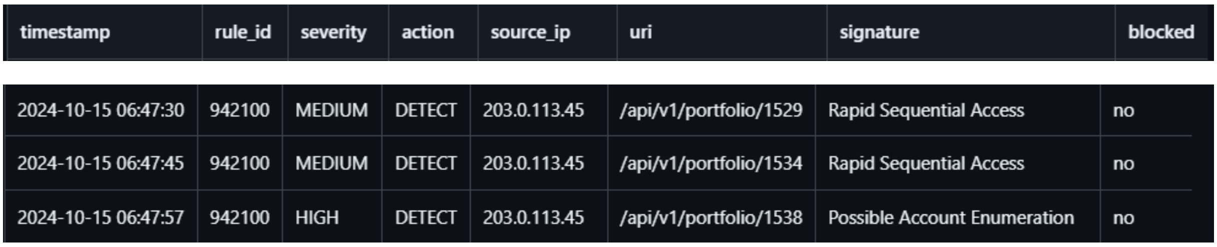
Suspicious IP Address: 203.0.113.45

FINDINGS



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 1: api_logs.csv



timestamp	rule_id	severity	action	source_ip	uri	signature	blocked
2024-10-15 06:47:30	942100	MEDIUM	DETECT	203.0.113.45	/api/v1/portfolio/1529	Rapid Sequential Access	no
2024-10-15 06:47:45	942100	MEDIUM	DETECT	203.0.113.45	/api/v1/portfolio/1534	Rapid Sequential Access	no
2024-10-15 06:47:57	942100	HIGH	DETECT	203.0.113.45	/api/v1/portfolio/1538	Possible Account Enumeration	no

Figure 2: waf_logs.csv

1) The user with ID 1523 successfully logged into the system. After logging in, they queried their own user ID, and this operation was successful. Subsequently, they queried other user IDs using the same token information, and all queries were successful (Figure 1-2).

Vulnerability:

IDOR: Insecure Direct Object References (IDOR) occur when an application provides direct access to objects based on user-supplied input. As a result of this vulnerability, attackers can bypass authorization and access resources in the system directly, for example database records or files. Insecure Direct Object References allow attackers to bypass authorization and access resources directly by modifying the value of a parameter used to directly point to an object. Such resources can be database entries belonging to other users, files in the system, and more. This is caused by the fact that the application takes user supplied input and uses it to retrieve an object without performing sufficient authorization checks (OWASP).

Impact:

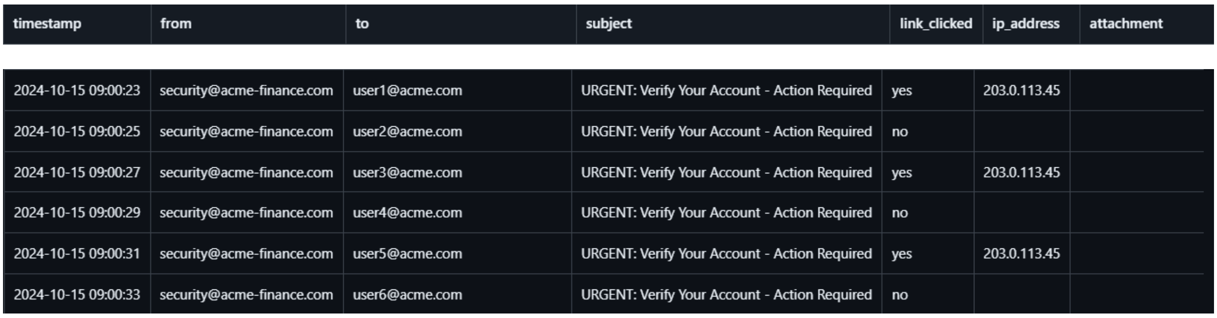
This vulnerability allows access to different users' token information and enables unauthorized actions on user accounts.

Risk Level:

High

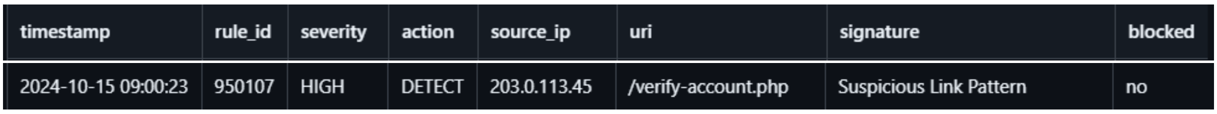
Recommendation:

Object Level Authorization checks should be applied for every object access; the user's token information should be compared with the data to be accessed, and access should be denied if there is no match. Additionally, when multiple different user ID query attempts are detected with the same token, an alarm should be generated on the SIEM.



timestamp	from	to	subject	link_clicked	ip_address	attachment
2024-10-15 09:00:23	security@acme-finance.com	user1@acme.com	URGENT: Verify Your Account - Action Required	yes	203.0.113.45	
2024-10-15 09:00:25	security@acme-finance.com	user2@acme.com	URGENT: Verify Your Account - Action Required	no		
2024-10-15 09:00:27	security@acme-finance.com	user3@acme.com	URGENT: Verify Your Account - Action Required	yes	203.0.113.45	
2024-10-15 09:00:29	security@acme-finance.com	user4@acme.com	URGENT: Verify Your Account - Action Required	no		
2024-10-15 09:00:31	security@acme-finance.com	user5@acme.com	URGENT: Verify Your Account - Action Required	yes	203.0.113.45	
2024-10-15 09:00:33	security@acme-finance.com	user6@acme.com	URGENT: Verify Your Account - Action Required	no		

Figure 3: email_logs.csv



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

Figure 4: waf_logs.csv

2) A phishing email was sent to users from the address security@acme-finance.com. user1, user3, and user4 clicked on the link in this email. At the same time, suspicious login activity was detected in the WAF logs, and it was determined that the attacker gained unauthorized access to the user1 account (Figure 3-4).

Vulnerability:

Compromise of user credentials via phishing email.

Impact:

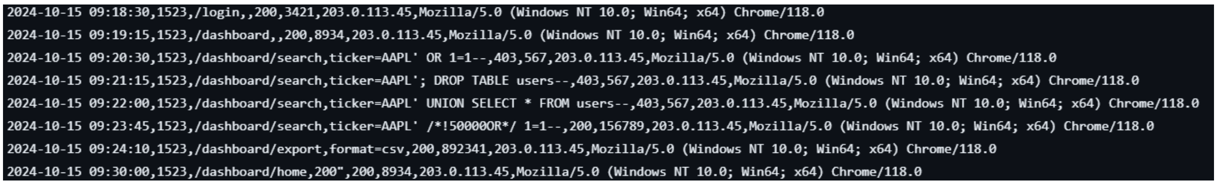
Unauthorized access allows access to user account information and modification of the account.

Risk Level:

High

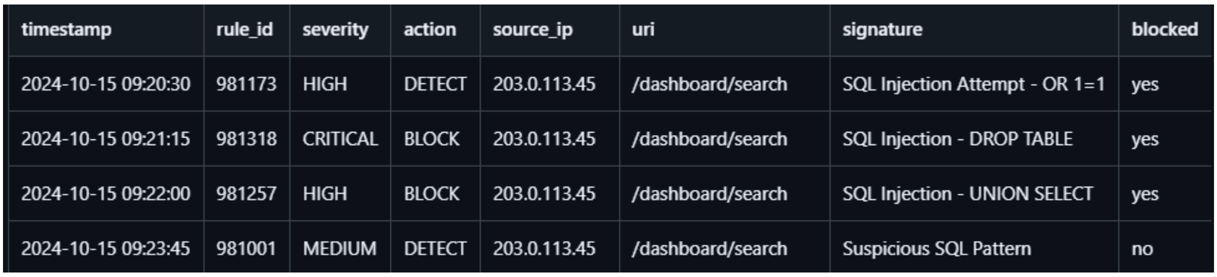
Recommendation:

MFA (Multi-Factor Authentication) should be enabled, suspicious messages should be detected with an email filtering system, and alerts should be created on SIEM for such incidents.



```
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
```

Figure 5: web_logs.csv



timestamp	rule_id	severity	action	source_ip	uri	signature	blocked
2024-10-15 09:20:30	981173	HIGH	DETECT	203.0.113.45	/dashboard/search	SQL Injection Attempt - OR 1=1	yes
2024-10-15 09:21:15	981318	CRITICAL	BLOCK	203.0.113.45	/dashboard/search	SQL Injection - DROP TABLE	yes
2024-10-15 09:22:00	981257	HIGH	BLOCK	203.0.113.45	/dashboard/search	SQL Injection - UNION SELECT	yes
2024-10-15 09:23:45	981001	MEDIUM	DETECT	203.0.113.45	/dashboard/search	Suspicious SQL Pattern	no

Figure 6: waf_logs.csv

3) The “OR 1=1” payload shown in Figure 5 is a classic SQL injection attempt sent to test whether filtering exists in the system and aims to retrieve records from the database. The “DROP TABLE users” command is a destructive attempt to delete the users table. The “UNION SELECT * FROM users” payload aims to combine users data from different tables and leak unauthorized data. The “/*!50000OR*/ 1=1” expression is an evasion technique used to bypass WAF signatures. Initial attempts were detected and blocked by the WAF using rule_id; however, the attacker's query containing evasion was not blocked by the WAF (Figure 6).

Vulnerability:

SQL Injection — Malicious SQL queries can be injected via data sent by the client.

Impact:

User data can be altered, all database content can be exposed or deleted; this leads to data loss and privacy/integrity breaches.

Risk Level:

High

Recommendations:

Database user permissions should be set according to the least privilege principle. The WAF should be strengthened against evasion techniques. Attempting the same payloads used in the SQL injection method multiple times from the same IP address should trigger a SIEM alert.

CONCLUSION

The identified vulnerabilities critically threaten user information and system integrity. The recommended measures should be implemented promptly, and the security status should be monitored continuously.

ARCHİTECTURAL RECOMMENDATİON

Instead of connecting directly to the Web App and Trading API database, an ORM service layer should be added. This reduces the risk of SQL injection and prevents users from accessing the database.

WAF alone is insufficient, so SIEM should be added. With SIEM, alerts can be generated and the system can be made more secure.