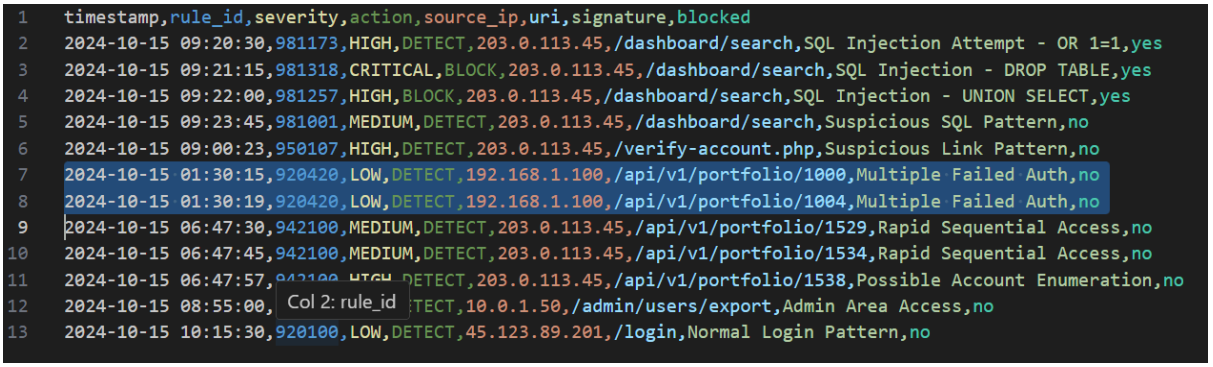
Section 1 - Incident Analysis

The timeline of the attack on Acme Financial Services systems, which occurred on October 15, 2024, was reconstructed by combining data from the api_logs, web_logs, waf_logs, email_logs, security_test_schedule, and api_docs files. The analysis focused on the attacker's actions originating from the IP address "**203.0.113.45**."

Under normal circumstances, the attacker IP address "**203.0.113.45**" is specified in the "**security_test_schedule**" document as the approved IP address within the **"203.0.113.0/24**" test range as part of the three-month penetration test scheduled for October 20-25, 2024. However, it was determined that the attack, via "**203.0.113.45**," occurred earlier than planned, on October 15, 2025.

When the WAF logs were examined, it was determined that the activities with the rule ID "**929420**" coming from the IP address "**192.168.1.100**" at 01:30:15 (Image -1) were a planned automatic security scan verified with the "**security_test_schedule**" document and were evaluated as 'false positive'.



```
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
2024-10-15 09:00:23,950107,HIGH,DETECT,203.0.113.45,/verify-account.php,Suspicious Link Pattern,no
2024-10-15 01:30:15,920420,LOW,DETECT,192.168.1.100,/api/v1/portfolio/1000,Multiple Failed Auth,no
2024-10-15 01:30:19,920420,LOW,DETECT,192.168.1.100,/api/v1/portfolio/1004,Multiple Failed Auth,no
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
2024-10-15 08:55:00,
Col 2: rule_id
TECT,10.0.1.50,/admin/users/export,Admin Area Access,no
2024-10-15 10:15:30,920100,LOW,DETECT,45.123.89.201,/login,Normal Login Pattern,no
```

Image - 1

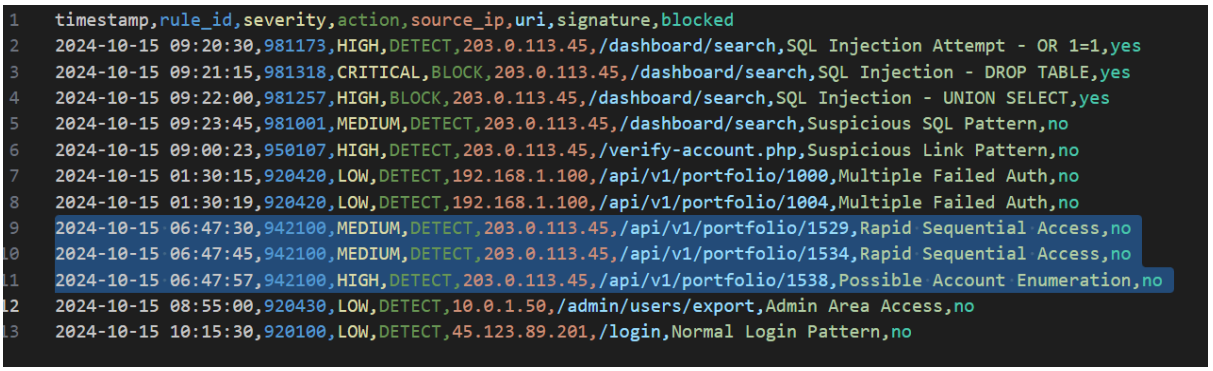
Examining the API logs, it was confirmed that the actual attack chain started at **06:45:10**, with the attacker successfully logging in using the user id account "**1523**" **(/api/v1/login,POST,200)**.

After viewing his own portfolio, the attacker discovered the broken access control attack at **06:47:15** (Image - 2) and accessed the portfolio information of 15 different accounts from **/api/v1/portfolio/1524** to **/api/v1/portfolio/1538.**

```
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
2024-10-15 07:12:30,4521,/api/v1/login,POST,,200,198,172.89.15.67,Acme-Mobile-iOS/3.2.1,
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
```

Image - 2

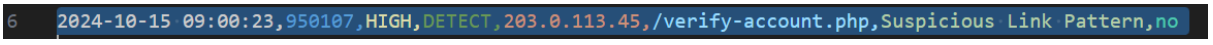
As seen in the WAF logs (Image - 3), the Broken Access Control attack is consistent with the "**Rapid Sequential Access**" and "**Possible Account Enumeration**" logs with rule id "**942100**" arriving at **06:47**. WAF detected these activities (Detect) but did not block them (Blocked: no).



```
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
2024-10-15 09:00:23,950107,HIGH,DETECT,203.0.113.45,/verify-account.php,Suspicious Link Pattern,no
2024-10-15 01:30:15,920420,LOW,DETECT,192.168.1.100,/api/v1/portfolio/1000,Multiple Failed Auth,no
2024-10-15 01:30:19,920420,LOW,DETECT,192.168.1.100,/api/v1/portfolio/1004,Multiple Failed Auth,no
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
2024-10-15 08:55:00,920430,LOW,DETECT,10.0.1.50,/admin/users/export,Admin Area Access,no
2024-10-15 10:15:30,920100,LOW,DETECT,45.123.89.201,/login,Normal Login Pattern,no
```

Image - 3

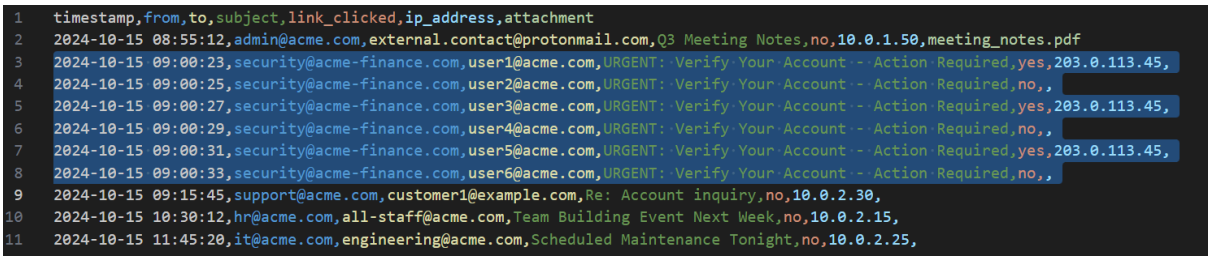
As seen in the WAF logs (Image - 4), the attacker started the phishing attack with the "**Suspicious Link Pattern**" log, triggered by the rule id "**950107**" at **09:00:23**. This attack could not be blocked by the WAF (Blocked: no).



```
2024-10-15 09:00:23,950107,HIGH,DETECT,203.0.113.45,/verify-account.php,Suspicious Link Pattern,no
```

Image - 4

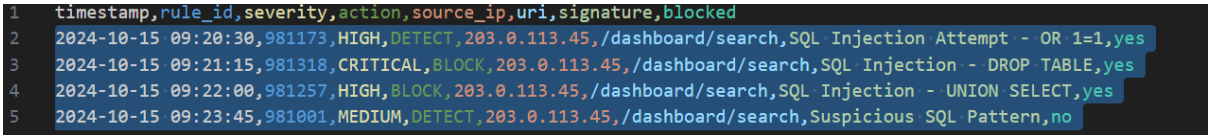
The phishing attack was carried out by 3 employees clicking on the fake link (link_clicked: yes) directed to the page “**/verify-account.php**” targeting 6 employees, with the title **“URGENT: Verify Your Account - Action Required**” coming from a fake sender named “security@acme-finance.com” with the same timestamp as the rule id “**950107**” in the WAF log, as seen in the email logs (Image - 5).



```
timestamp,from,to,subject,link_clicked,ip_address,attachment
2024-10-15 08:55:12,admin@acme.com,external.contact@protonmail.com,Q3 Meeting Notes,no,10.0.1.50,meeting_notes.pdf
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,,
2024-10-15 09:15:45,support@acme.com,customer1@example.com,Re: Account inquiry,no,10.0.2.30,
2024-10-15 10:30:12,hr@acme.com,all-staff@acme.com,Team Building Event Next Week,no,10.0.2.15,
2024-10-15 11:45:20,it@acme.com,engineering@acme.com,Scheduled Maintenance Tonight,no,10.0.2.25,
```

Image - 5

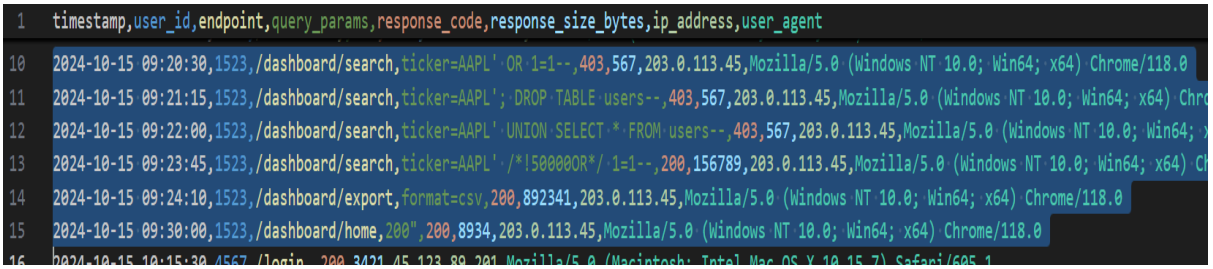
As seen in the third and final phase of the attack, WAF logs (Image - 6) show, SQLi attacks were detected on the **/dashboard/search** uri. Three of these attacks were blocked by WAF, but the log with rule id "**981001**" was not blocked.



```
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
```

Image - 6

SQLi attacks can be seen in more detail in the web logs at the same timeframe (Image - 7). The attack, which was not blocked by the WAF at **09:23:45**, was carried out with the parameter "**ticker=AAPL' /*!50000OR*/ 1=1–**". (/*! ... */) is a disguised SQL injection attempt. The 156kb response size indicates that it successfully retrieved all the data from the ticker table. The log record seen at **09:24:10** is the final stage of the attack, and the data leak was achieved by exporting the obtained data as CSV.



```
timestamp,user_id,endpoint,query_params,response_code,response_size_bytes,ip_address,user_agent
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) Chro
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; x
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) Ch
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
```

Image - 7

API Broken Acces Control	
Attack Classification	**OWASP**: A01:2021 - Broken Access Control. API1:2023 BOLA The system is not checking authorization, as stated in the api_docs.pdf file ("Authorization checks validate token but may not verify account ownership"). **Mitre Attack**: T1213 - Data from Information Repositories Discovered other accounts (1524, 1525, etc.) via API. This was also triggered by WAF as "Possible Account Enumeration."
Root Cause	Coding Error. While developing the API, it was discovered that the API performed "Authentication" but not "Authorization".
Impact Assessment	Data Privacy Breach. Sensitive portfolio information (stocks, balance, etc.) of at least 15 clients was directly stolen.

Phishing Attack	
Attack Classification	**OWASP:** A07:2021 Identification and Authentication Failures The purpose of a phishing attack is credential theft, which falls into this category. **Mitre Attack**: T1566.002 Sending a specially prepared link to a targeted group.
Root Cause	Inadequate Email Security. Email Gateway's "Partially Secure" status was unable to filter emails from a fake/suspicious domain (acme-finance.com).
Impact Assessment	Persistent Threat. The credentials of 3 employees are now in the attacker's hands.

Web Application SQL Injection	
Attack Classification	**OWASP:** A05:2021 Security Misconfiguration and A03:2021 - Injection It is a security configuration error that WAF is configured only with "Basic Rules" and cannot prevent hidden attacks such as /*!...*/. **Mitre Attack**: T1027 Obfuscated Files or Information is the use of an obfuscated command like /*!50000OR*/ instead of the standard OR 1=1 to bypass WAF. T1190: Exploit Public-Facing Application
Root Cause	Lack of Secure Software Development. The development team is not sanitizing user input on the server side or using parameterized queries..
Impact Assessment	Mass Data Leak 892KB has the potential to leak the entire database content returned by the query /*!...OR 1=1*/ as a CSV.

Section 2 - Architecture Review

The architectural structure of Acme Financial Services systems is clearly stated in the “current_architecture.png” file. In this context;

Insufficient WAF Configuration: The "Basic Rules" specified in the diagram did not prevent the attacker from using the obfuscated /*!50000OR*/ 1=1-- SQLi payload.

Lack of API Authorization: The architecture lacked authorization controls at the API Gateway level or in the application code that prevented a user from accessing another customer's data. This is confirmed by the note in the api_docs.pdf file ("...may not verify account ownership").

Lack of Segmentation: Since both Web App (Python) and Trading API (Flask) services share the same PostgreSQL database, an SQLi attack via the Web App could also put critical trading data (Trading API) at risk.

Inadequate Email Security: Email Gateway allowed phishing emails from a spoofed domain to land unfiltered in the inboxes of 6 employees.

Section 3 - Response & Remediation

Emergency Actions (0-24 Hours)	Block the attacker IP address (203.0.113.45). Suspend and reset passwords for all accounts that were breached (user_id: 1523) and clicked on the phishing email. Disable the (/dashboard/export) endpoint used for data exfiltration until the vulnerability is fixed.
Short-Term Corrections (1-2 Weeks)	Fix A01 (BAC): Add a mandatory authorization check to the Trading API code that matches the requesting user_id with the requested account_id. Update the WAF rule set to also block stealthy attacks (e.g. OWASP Core Rule Set).
Long-Term Improvements (1-3 Months)	Plan mandatory security awareness training against phishing. Implement database segmentation into separate database roles or tables for Web App and Trading API.