SECURITY INCIDENT RESPONSE REPORT

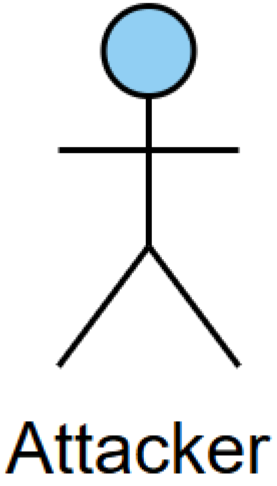
ORGANIZATION: ACME FINANCIAL SERVICES

Metehan Çevik

INCIDENT OVERVIEW

16 accounts, 1.14 MB data, 4 attack phases

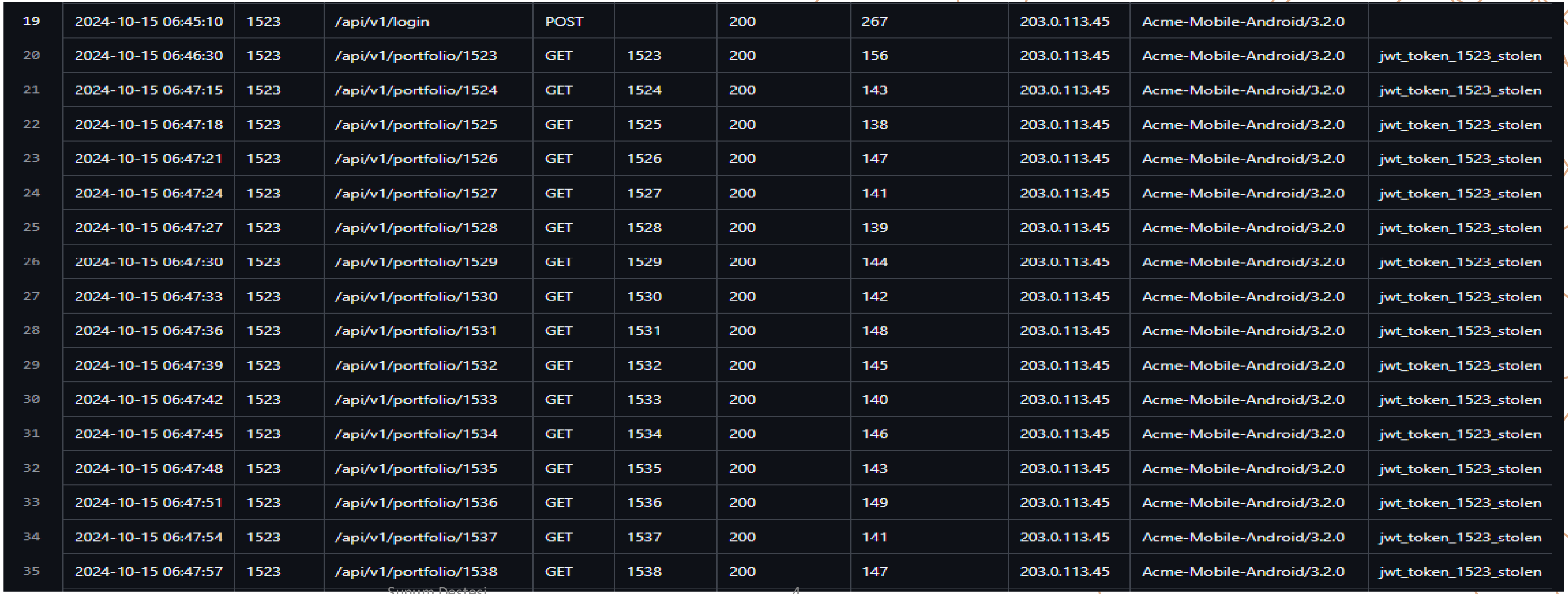
PHASE 0



IP 203.0.113.45

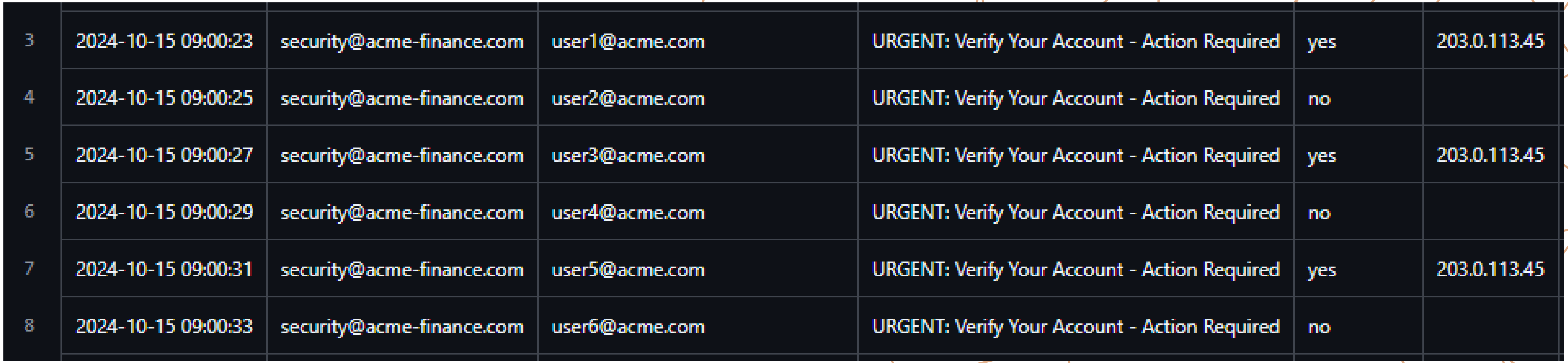
Customer Id: 1523

PHASE 1



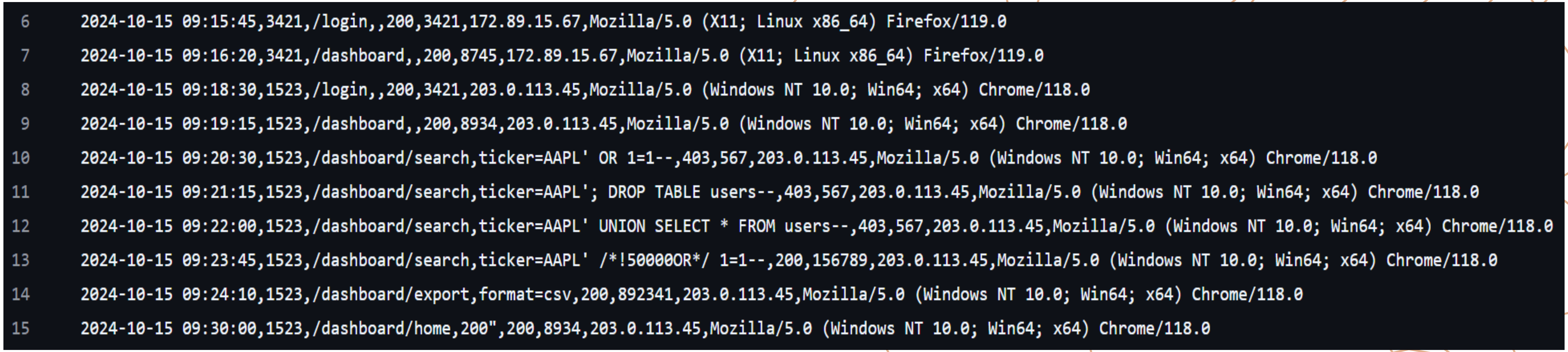
19	2024-10-15 06:45:10	1523	/api/v1/login	POST		200	267	203.0.113.45	Acme-Mobile-Android/3.2.0	
20	2024-10-15 06:46:30	1523	/api/v1/portfolio/1523	GET	1523	200	156	203.0.113.45	Acme-Mobile-Android/3.2.0	jwt_token_1523_stolen
21	2024-10-15 06:47:15	1523	/api/v1/portfolio/1524	GET	1524	200	143	203.0.113.45	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

PHASE 2



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	

PHASE 3 AND PHASE 4

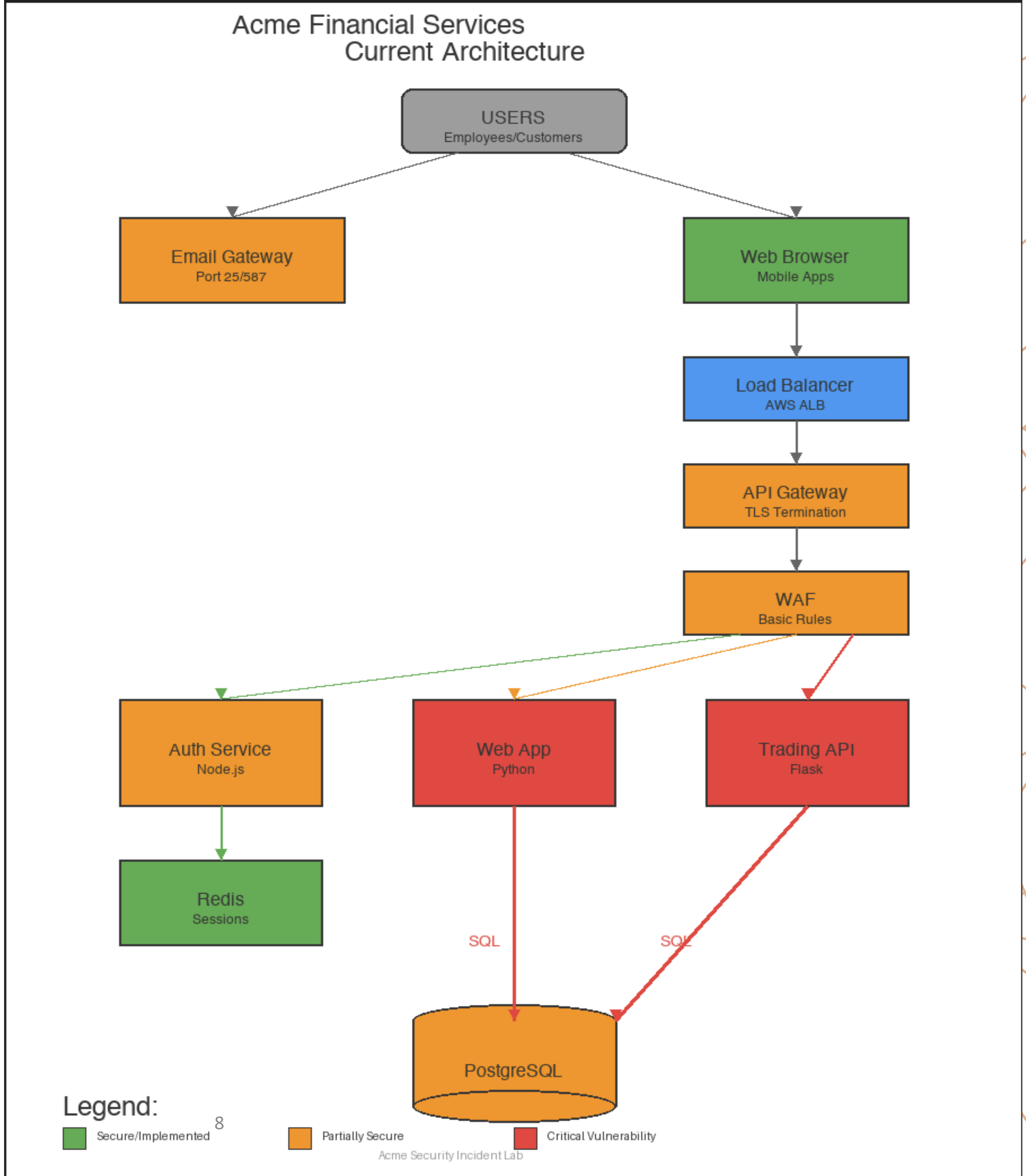


```
2024-10-15 09:15:45,3421,/login,,200,3421,172.89.15.67,Mozilla/5.0 (X11; Linux x86_64) Firefox/119.0
2024-10-15 09:16:20,3421,/dashboard,,200,8745,172.89.15.67,Mozilla/5.0 (X11; Linux x86_64) Firefox/119.0
2024-10-15 09:18:30,1523,/login,,200,3421,203.0.113.45,Mozilla/5.0 (Windows NT 10.0; Win64; 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
```

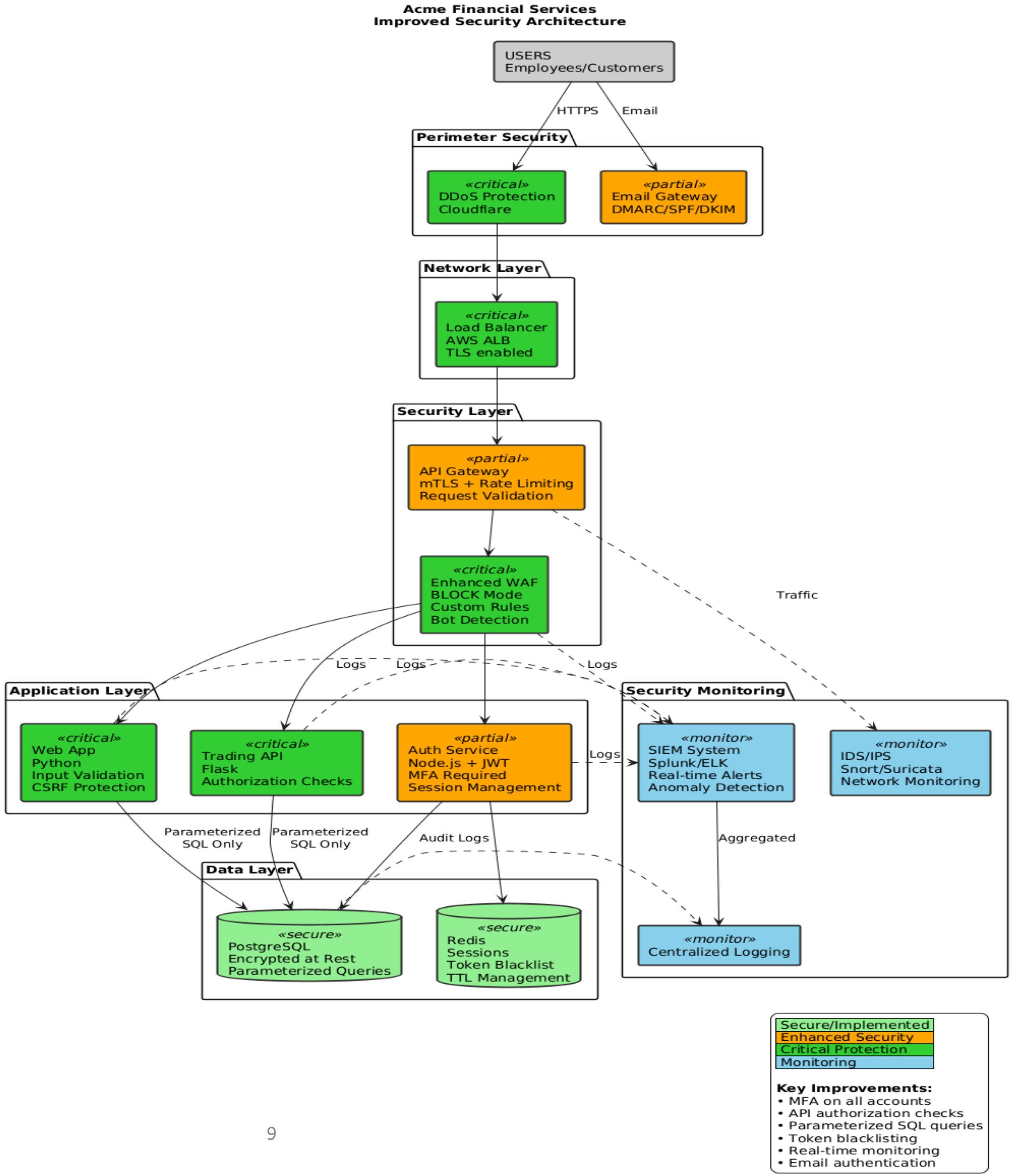
ROOT CAUSE ANALYSIS

- Token control is not being performed correctly
- Data input is not properly verified and sanitized
- Monitoring and Email Security

CURRENT ARCHITECTURE WEAKNESSES



IMPROVED SECURITY ARCHITECTURE



Acme Financial Services
Improved Security Architecture

USERS
Employees/Customers

HTTPS

Email

Perimeter Security

«critical»
DDoS Protection
Cloudflare

«partial»
Email Gateway
DMARC/SPF/DKIM

Network Layer

«critical»
Load Balancer
AWS ALB
TLS enabled

Security Layer

«partial»
API Gateway
mTLS + Rate Limiting
Request Validation

«critical»
Enhanced WAF
BLOCK Mode
Custom Rules
Bot Detection

Traffic

Logs

Logs

Logs

Application Layer

«critical»
Web App
Python
Input Validation
CSRF Protection

«critical»
Trading API
Flask
Authorization Checks

«partial»
Auth Service
Node.js + JWT
MFA Required
Session Management

Logs

Security Monitoring

«monitor»
SIEM System
Splunk/ELK
Real-time Alerts
Anomaly Detection

«monitor»
IDS/IPS
Snort/Suricata
Network Monitoring

Aggregated

«monitor»
Centralized Logging

Parameterized
SQL Only

Parameterized
SQL Only

Audit Logs

Data Layer

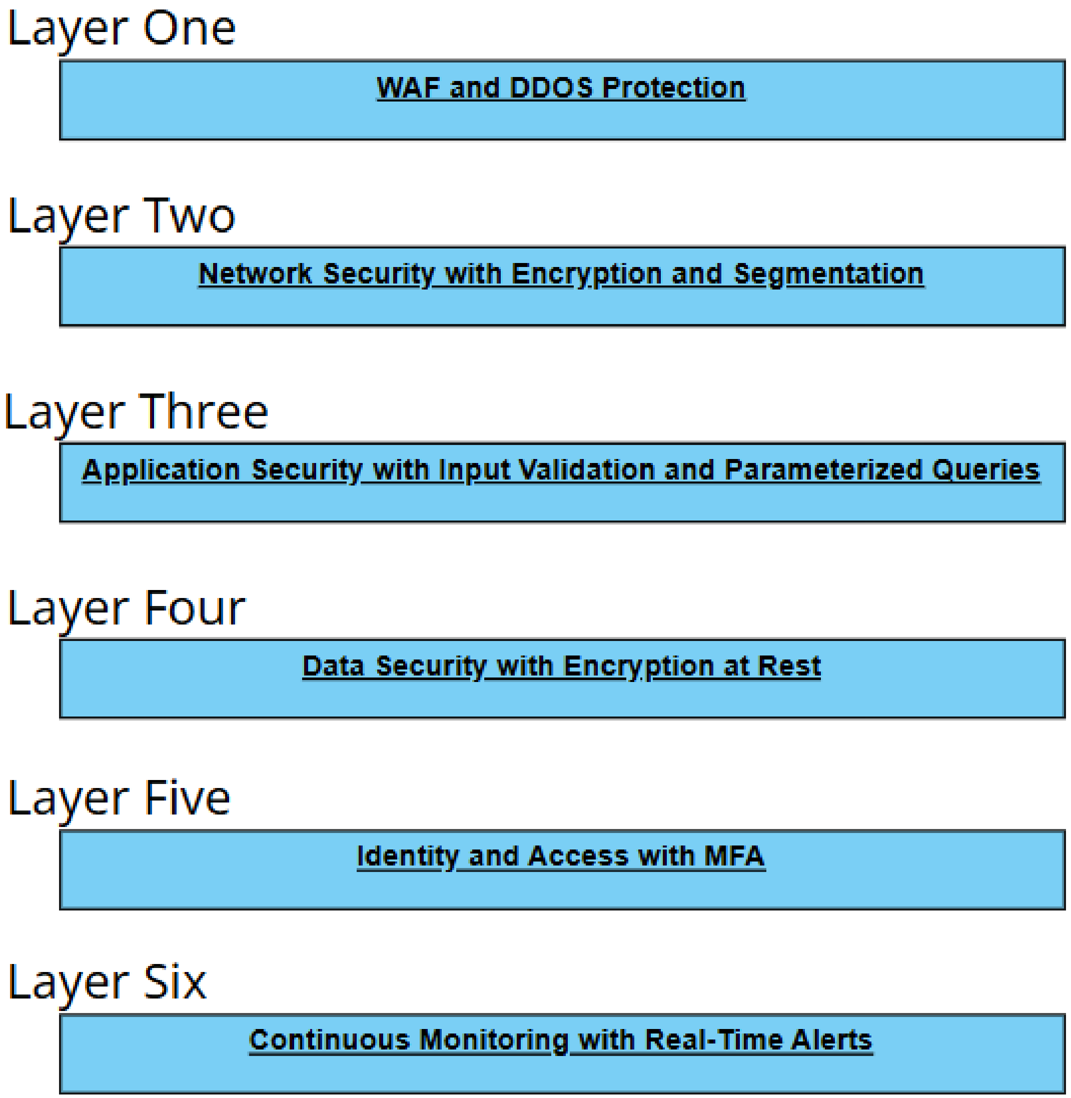
«secure»
PostgreSQL
Encrypted at Rest
Parameterized Queries

«secure»
Redis
Sessions
Token Blacklist
TTL Management

Secure/Implemented
Enhanced Security
Critical Protection
Monitoring

Key Improvements:
- MFA on all accounts
- API authorization checks
- Parameterized SQL queries
- Token blacklisting
- Real-time monitoring
- Email authentication

DEFENSE-IN-DEPTH STRATEGY



Layer One

WAF and DDOS Protection

Layer Two

Network Security with Encryption and Segmentation

Layer Three

Application Security with Input Validation and Parameterized Queries

Layer Four

Data Security with Encryption at Rest

Layer Five

Identity and Access with MFA

Layer Six

Continuous Monitoring with Real-Time Alerts

CHECKLIST WITH THREE TOP PRIORITIES

Number one: Implement proper API authorization.

Number two: Convert all SQL queries to parameterized statements.

Number three: Deploy MFA for all accounts and set up SIEM for real-time monitoring.

SHORT-TERM FIXES

-Rate limiting of 40 requests per minute.

-Automatic token blacklisting for suspicious patterns.

-DMARC, SPF, and DKIM.

-Updating WAF rules

LONG-TERM STRATEGY

-DevSecOps practices.

-Penetration tests.

-Security training for developers.

-Phishing simulations

CLOSING SUMMARY

To summarize: an attacker exploited BOLA, SQL injection, and email spoofing to access 16 accounts and steal 1.14 megabytes of financial data. We've identified all root causes and are implementing comprehensive fixes across authentication, authorization, input validation, and monitoring.

All improvements are tracked with monthly progress reports to management until complete. We're transforming our security posture from reactive to proactive.