Incident Report: Unauthorized Penetration Testing Activity

Prepared by: Mert ACAR
Report Date: November 8, 2025

1 Incident Analysis

On October 15, 2024, multiple security events were observed across email, API, WAF, and web application logs, initially flagged as potential compromise. Subsequent correlation with the Q4 2024 Scheduled Security Testing document revealed these activities to be unscheduled penetration testing conducted by CyberSec Partners using the approved IP range 203.0.113.0/24. Despite written approval of the IP block, no 48-hour pre-confirmation was provided, violating procedural controls.

1.1 Timeline Reconstruction (UTC Normalized)

All timestamps have been normalized to UTC for consistency:

- **2024-10-15 06:46:30 UTC**: API request to `/api/v1/portfolio/1523` returns 200 OK from IP 203.0.113.45 using JWT token `jwt_token_1523_stolen`.
- **2024-10-15 06:46:30 – 06:47:57 UTC**: 16 sequential GET requests to `/api/v1/portfolio/1523` through `/api/v1/portfolio/1538`, all returning 200 OK. No rate limiting enforced.
- **2024-10-15 06:47:30 – 06:47:57 UTC**: WAF triggers `Rule 942100` (Rapid Sequential Access) and `Possible Account Enumeration` on same endpoints.
- **2024-10-15 09:00:23 UTC**: Phishing email link clicked by `user1@acme.com` from 203.0.113.45.
- **2024-10-15 09:00:27 UTC**: `user3@acme.com` clicks link.
- **2024-10-15 09:00:31 UTC**: `user5@acme.com` clicks link.
- **2024-10-15 09:00:23 UTC**: WAF logs access to `/verify-account.php` (Suspicious Link Pattern).
- **2024-10-15 09:18:30 UTC**: Web login by user ID 1523 from 203.0.113.45.
- **2024-10-15 09:20:30 – 09:22:00 UTC**: Three SQL injection attempts blocked (`OR 1=1`, `DROP TABLE`, `UNION SELECT`).
- **2024-10-15 09:23:45 UTC**: Successful SQL injection using MySQL inline comment bypass: `ticker=AAPL' /*!50000OR*/ 1=1-` returns 200.
- **2024-10-15 09:24:10 UTC**: CSV export of dashboard data downloaded.

1.2 Attack Vector Identification

The primary vector was **assumed breach via credential harvesting**. The penetration testing team leveraged pre-shared test credentials to simulate phishing success, then exploited Insecure Direct Object Reference (IDOR) in the Trading API. Subsequent web application compromise was achieved through SQL injection with WAF bypass. The email vector (`security@acme-finance.com`) was not listed in the testing document, indicating an unapproved sender domain.

1.3 Attack Classification

- **MITRE ATTCK**:
  - `T1190` – Exploit Public-Facing Application (SQLi)
  - `T1550.002` – Use Alternate Authentication Material (JWT)
  - `T1078` – Valid Accounts
  - `T1110` – Brute Force (sequential ID enumeration)
  - `T1566` – Phishing
- **OWASP Top 10**:
  - `A01:2021` – Broken Access Control (IDOR)
  - `A03:2021` – Injection (SQLi)
  - `A05:2021` – Security Misconfiguration (WAF bypass, rate limit)

1.4 Root Cause Analysis

The root cause is **insufficient defense-in-depth and procedural non-compliance**. While the IP range was approved, lack of pre-confirmation led to false positive incident escalation. Technical root causes include:

- Absence of account ownership validation in `GET /api/v1/portfolio/{id}`
- Incomplete rate limiting implementation
- WAF rule deficiency against MySQL versioned comments
- No multi-factor authentication (MFA) enforcement
- Direct SQL query execution in web application

1.5 Impact Assessment

Although no production data was compromised (test accounts used), the exercise demonstrated **full system compromise potential** from a single credential. Successful data exfiltration via CSV export and complete account enumeration represent critical risk. Financial, reputational, and regulatory impact could exceed million dollars in a real breach.

2 Architecture Review

The current architecture provides layered security but fails in execution. The Email Gateway allowed phishing simulation, API Gateway validated tokens without ownership checks, and WAF was bypassed using advanced SQL injection techniques.

2.1 Current Architecture Weaknesses

The Trading API and Web Application both execute direct SQL queries and lack input validation. Rate limiting is documented but not enforced across all endpoints. The WAF does not block MySQL inline comments (`/*!50000...*/`). Authentication relies solely on JWT without MFA. The email domain `security@acme-finance.com` was not pre-approved.

2.2 Improved Security Architecture with DMZ

2.3 Recommended Security Controls

1. **DMZ Implementation**: Isolate public-facing services (Web App, API) from internal database.
2. **MFA Enforcement**: Require TOTP or WebAuthn for all logins.
3. **IDOR Mitigation**: Server-side ownership check in API.
4. **WAF Rule**: Block `/\*\!\d{5}.*?\*\/`.
5. **Prepared Statements**: Enforce ORM usage.

2.4 Defense-in-Depth Strategy

Implement multiple overlapping controls: prevent phishing at the email gateway (DMARC), block exploitation at WAF, detect anomalies via rate limiting, isolate public services in DMZ, and contain damage through least-privilege database access and MFA.

3 Response & Remediation

3.1 Immediate Actions (0–24 Hours)

1. Contact CyberSec Partners to confirm activity and demand immediate cessation until re-approval.
2. Place IP 203.0.113.45 in temporary WAF block list.
3. Invalidate all JWT tokens issued to user ID 1523.
4. Notify SOC to downgrade incident priority to informational.

3.2 Short-term Fixes (1–2 Weeks)

1. Deploy WAF rule to block MySQL inline comments.
2. Implement server-side IDOR checks in Trading API.
3. Enforce MFA for all internal and test accounts.
4. Update rate limiting to cover all API endpoints.

3.3 Long-term Improvements (1–3 Months)

1. Migrate all database interactions to ORM with prepared statements.
2. Implement DMARC `p=reject` policy and full SPF/DKIM alignment.
3. Establish formal pre-confirmation process for penetration testing IPs and domains.
4. Conduct red team exercise with full procedural compliance.

3.4 Compliance Considerations

This incident triggers review under SOC 2, PCI DSS, and GDPR. The lack of pre-confirmation violates change management controls. All penetration testing must now include signed Rules of Engagement with 48-hour notification and approved sender domains.

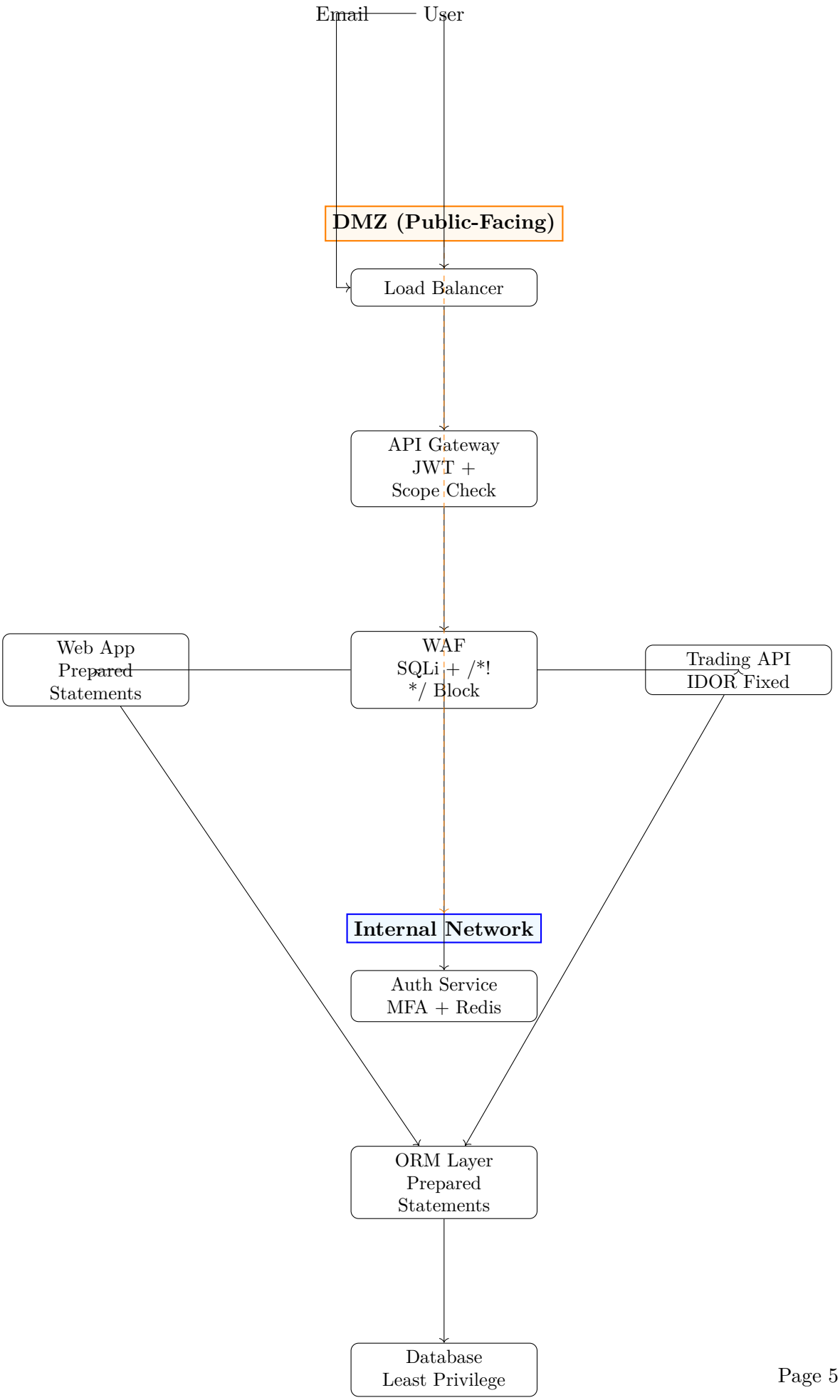

Figure 1: Improved Architecture with DMZ Isolation and Defense-in-Depth