SECURITY OPERATIONS

INCİDENT RESPONSE REPORT

Acme Financial Services Incident Analysis Report

INCİDENT DETAİLS

Incident ID:	INC-2025-001
Date:	November 9, 2025
Severity Level:	CRITICAL
Prepared by:	Ali Ekber KARA

Executive Summary

15 Ekim 2024 tarihinde Acme Finance sistemlerinde gerçekleşen olay, API katmanında başlayan ve çok aşamalı olarak ilerleyen zincirleme bir siber saldırı olarak tespit edilmiştir. Saldırgan, ilk olarak /api/v1/portfolio uç noktasında IDOR (Insecure Direct Object Reference) zafiyetinden yararlanarak kullanıcı verilerini keşfetmiş, elde ettiği bilgileri kullanarak sahte alan adından (acme-finance.com) kimlik avı (phishing) e-postaları göndermiş ve üç kullanıcının credentiallarını ele geçirmiştir. Ardından aynı IP adresiyle /dashboard/search uç noktasında SQL Injection zafiyetinden faydalanarak sistemden veri çekmiş ve /dashboard/export aracılığıyla yaklaşık 870 KB boyutunda kullanıcı verisini dışa aktarmıştır. Saldırganın, planlı penetrasyon testleri için ayrılmış 203.0.113.0/24 IP aralığını kullanarak tespiti zorlaştırması, olayın hem kimlik avı hem uygulama zafiyetlerini içermesi ve doğrudan müşteri verilerine erişim sağlaması nedeniyle olay Severity Level: Critical olarak sınıflandırılmıştır. Önerilen önlemler arasında API erişim kontrollerinin güçlendirilmesi, kullanıcı şifrelerinin sıfırlanması, MFA uygulanması, WAF kurallarının güçlendirilmesi ve phishing farkındalık eğitimlerinin artırılması yer almaktadır.

1. Incident Analysis

1.1 Incident Timeline

Tüm loglar UTC formatına normalize edilmiştir. 15 Ekim 2024 tarihinde Acme Financial Services altyapısında gerçekleşen olaylar; e-posta, WAF, API ve web uygulama loglarının korelasyonu ile incelenmiştir. Aşağıda olay dizisi, nedenleri ve ilişkili bulgularla birlikte detaylandırılmıştır.

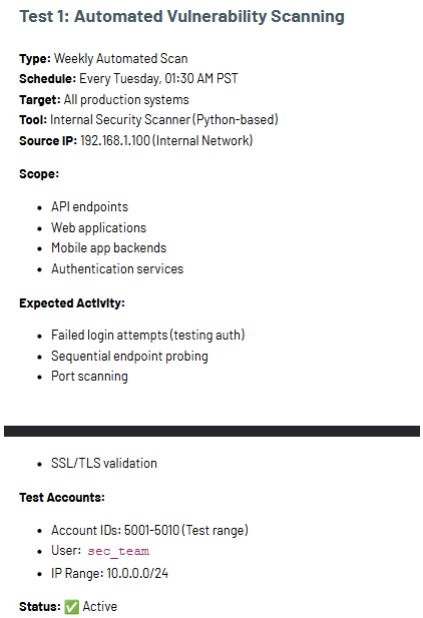
01:30 UTC – İç Ağda Otomatik Güvenlik Taraması

İç IP adresi 192.168.1.100, kurumsal güvenlik tarayıcısı tarafından planlı haftalık otomatik zafiyet taramasını başlatmıştır. Bu taramada /api/v1/portfolio/{id} uç noktalarına ardışık istekler gönderilmiş, ilk denemelerde (1000–1004) 401 yetkilendirme hatası alınmıştır. 15 dakika sonrasında aynı araç, test kullanıcı tokenları (ör. test_token_xyz_5001) ile doğrulanmış istekler yapmıştır (Şekil 1).

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	
2024-10-15 01:45:10	sec_team	/api/v1/portfolio/5001	GET	5001	200	123	10.0.0.50	Mozilla/5.0 (Security-Scanner)	test_token_xyz_5001
2024-10-15 01:45:15	sec_team	/api/v1/portfolio/5002	GET	5002	200	119	10.0.0.50	Mozilla/5.0 (Security-Scanner)	test_token_xyz_5002
2024-10-15 01:45:20	sec_team	/api/v1/portfolio/5003	GET	5003	200	127	10.0.0.50	Mozilla/5.0 (Security-Scanner)	test_token_xyz_5003
2024-10-15 01:45:25	sec_team	/api/v1/portfolio/5004	GET	5004	200	115	10.0.0.50	Mozilla/5.0 (Security-Scanner)	test_token_xyz_5004
2024-10-15 01:45:30	sec_team	/api/v1/portfolio/5005	GET	5005	200	121	10.0.0.50	Mozilla/5.0 (Security-Scanner)	test_token_xyz_5005

Şekil 1

Bu faaliyet, “Automated Vulnerability Scanning” planına uygun şekilde gerçekleştiği için false positive olarak değerlendirilmiştir (Şekil 2).



Test 1: Automated Vulnerability Scanning

Type: Weekly Automated Scan
Schedule: Every Tuesday, 01:30 AM PST
Target: All production systems
Tool: Internal Security Scanner (Python-based)
Source IP: 192.168.1.100 (Internal Network)

Scope:

- API endpoints
- Web applications
- Mobile app backends
- Authentication services

Expected Activity:

- Failed login attempts (testing auth)
- Sequential endpoint probing
- Port scanning

- SSL/TLS validation

Test Accounts:

- Account IDs: 5001-5010 (Test range)
- User: `sec_team`
- IP Range: 10.0.0.0/24

Status: ✅ Active

Şekil 2

04:15–05:33 UTC – Normal Kullanıcı Aktiviteleri

Gerçek kullanıcılar tarafından mobil uygulama (iOS ve Android) üzerinden gerçekleştirilen girişler ve portfolyo görüntüleme istekleri kaydedilmiştir. Tüm işlemler geçerli JWT tokenları ile yapılmış, IP adresleri (98.213.45.122 ve 172.89.15.67) VirusTotal üzerinde temiz olarak görünmüştür. Bu zaman aralığı, sistemin normal operasyonel trafiğini yansıtmaktadır (Şekil 3).

11	2024-10-15 04:15:30	2347	/api/v1/login	POST		200	234	98.213.45.122	Acme-Mobile-iOS/3.2.1		
12	2024-10-15 04:16:15	2347	/api/v1/portfolio/2347	GET	2347	200	145	98.213.45.122	Acme-Mobile-iOS/3.2.1	jwt_token_2347_abc	
13	2024-10-15 04:18:20	2347	/api/v1/transactions/2347	GET	2347	200	189	98.213.45.122	Acme-Mobile-iOS/3.2.1	jwt_token_2347_abc	
14	2024-10-15 04:22:45	2347	/api/v1/transfer	POST		200	456	98.213.45.122	Acme-Mobile-iOS/3.2.1	jwt_token_2347_abc	
15	2024-10-15 05:30:12	3891	/api/v1/login	POST		200	198	172.89.15.67	Acme-Mobile-Android/3.1.9		
16	2024-10-15 05:31:30	3891	/api/v1/portfolio/3891	GET	3891	200	167	172.89.15.67	Acme-Mobile-Android/3.1.9	jwt_token_3891_def	
17	2024-10-15 05:33:15	3891	/api/v1/market-data	GET		200	234	172.89.15.67	Acme-Mobile-Android/3.1.9	jwt_token_3891_def	

Şekil 3

06:47 UTC – Olası Kullanıcı Hesabı Keşfi (Account Enumeration)

WAF loglarında, 203.0.113.45 IP adresinden /api/v1/portfolio/1529–1538 aralığında hızlı ve ardışık istekler tespit edilmiştir. Bu durum "Rapid Sequential Access" ve "Possible Account Enumeration" olarak işaretlenmiştir (Şekil 4).

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

Şekil 4

İnceleme sonucunda, aynı IP adresinin birkaç saat sonra daha ciddi aktivitelerde bulunduğu görülmüştür. Bu aşama, saldırganın sistemin kullanıcı ID yapısını keşfetmeye çalıştığı ön hazırlık aşaması olarak değerlendirilmektedir. (Şekil 6).

Get Portfolio

Endpoint: `GET /api/v1/portfolio/{account_id}`

Description: Retrieve user's portfolio holdings and current values.

Parameters:

- `account_id` (path, required): User's account identifier

Headers:

`Authorization: Bearer <token>`

Success Response (200):

```
{
  "account_id": 1523,
  "user_name": "John Doe",
  "total_value": 125430.50,
  "holdings": [
    {
      "ticker": "AAPL",
      "quantity": 100,
      "avg_cost": 150.20,
      "current_price": 175.50,
      "value": 17550.00
    },
    {
      "ticker": "TSLA",
      "quantity": 50,
      "avg_cost": 220.00,
      "current_price": 245.30,
      "value": 12265.00
    }
```

Şekil 5

07:12–08:23 UTC – Normal Kullanıcı Aktivitesi

Kullanıcı oturumları (ID 4521 ve 6789) mobil uygulama üzerinden başarıyla gerçekleştirilmiştir. Bu oturumlarda JWT token'lar geçerlidir ve erişim limitleri (rate limit) dahilinde çalışmıştır. Bu trafik normal davranış olarak etiketlenmiştir (Şekil 7).

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
2024-10-15 07:15:20	4521	/api/v1/transactions/4521	GET	4521	200	145	172.89.15.67	Acme-Mobile-iOS/3.2.1	jwt_token_4521_ghi
2024-10-15 08:20:15	6789	/api/v1/login	POST		200	234	45.123.89.201	Acme-Mobile-Android/3.2.0	
2024-10-15 08:21:30	6789	/api/v1/portfolio/6789	GET	6789	200	156	45.123.89.201	Acme-Mobile-Android/3.2.0	jwt_token_6789_jkl
2024-10-15 08:23:45	6789	/api/v1/market-data	GET		200	198	45.123.89.201	Acme-Mobile-Android/3.2.0	jwt_token_6789_jkl

Şekil 6

08:55 UTC – Şüpheli Admin Aktivitesi

Admin kullanıcısı (admin_5678) sistemde /admin/users/export işlemini başlatmış ve hemen ardından harici bir e-posta adresine (external.contact@protonmail.com) "meeting_notes.pdf" adlı dosyayı göndermiştir.

İşlem, kurumsal IP (10.0.1.50) üzerinden gerçekleştirilmiş olmakla birlikte, harici alıcının ProtonMail uzantılı olması ve dosya aktarımının e-posta gönderimiyle eş zamanlı gerçekleşmesi, tesadüf ihtimalini zayıflatmaktadır. Bu nedenle aktivite şüpheli olarak değerlendirilmiştir.

Bu durum doğrultusunda ilgili kullanıcıdan teyit alınması uygun olacaktır. (Şekil 8).

2024-10-15 08:55:00	920430	LOW	DETECT	10.0.1.50	/admin/users/export	Admin Area Access	no

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 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

Şekil 7

09:00 UTC – Phishing Kampanyası Başlangıcı

Mesai saatinin başlangıcına denk gelen bu zaman diliminde, security@acme-finance.com adresinden altı farklı kullanıcıya "URGENT: Verify Your Account" konulu e-postalar gönderilmiştir. E-posta içeriği, hesapların güvenlik doğrulaması gerektiği izlenimini vererek kullanıcıları panik ortamında hızlı harekete geçmeye yönlendirmiştir.

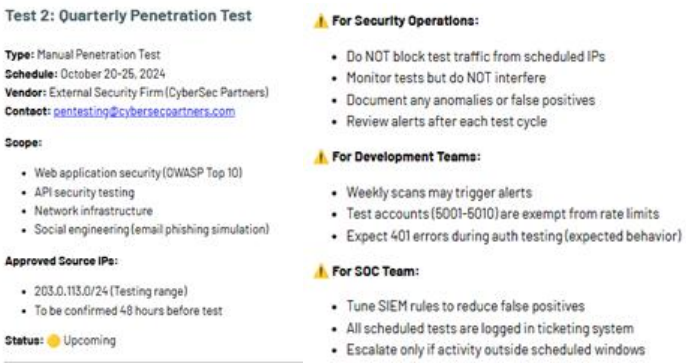
İlk bakışta kurumsal iletişim izlenimi veren bu e-posta, meşru alan adı acme.com yerine acme-finance.com sahte domainini kullanmakta olup klasik bir credential harvesting saldırısı niteliğindedir.

Kullanıcılardan üçü e-postadaki bağlantıya tıklamış, bunlardan biri (User ID 1523) daha sonra sistem üzerinde yetkisiz aktivitelerle ilişkilendirilmiştir (Şekil 8).

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	

Şekil 8

Kaynak IP adresi (203.0.113.45) planlı sızma testi için ayrılmış IP aralığında (203.0.113.0/24) yer almakla birlikte planlı testlerin 20–25 Ekim 2024 tarihleri arasında yapılması gerektiği dikkate alındığında, bu etkinliğin izin dışı bir erken test veya olası kötüye kullanım olabileceği değerlendirilmiştir (Şekil 9).



Şekil 9

Bu durum, test altyapılarının zamanlama ve erişim kontrollerinin yeterince sınırlandırılmamasının, gerçek saldırıların tespitini geciktirebileceğini göstermektedir.

09:10–09:19 UTC – Yetkisiz Girişler

Phishing e-postalarından sonra 3 farklı kullanıcı hesabı ile oturum açılmıştır.
Özellikle User ID 1523, saldırgan IP'si (203.0.113.45) üzerinden giriş yapmış ve kısa süre sonra sistem içindeki arama (search) fonksiyonlarını kötüye kullanmıştır.
Bu aşamada saldırganın, phishing e-postası yoluyla elde ettiği credentialları kullanarak gerçek kullanıcı oturumu açtığı anlaşılmıştır (Şekil 10).

3	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/6
4	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/6
5	2024-10-15 09:15:45	3421	/login		200	3421	172.89.15.67	Mozilla/5.0 (X11; Linux x86_64) Firefox/119.0
6	2024-10-15 09:16:20	3421	/dashboard		200	8745	172.89.15.67	Mozilla/5.0 (X11; Linux x86_64) Firefox/119.0
7	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
8	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

Şekil 10

09:20–09:24 UTC – SQL Injection Saldırısı ve Veri Sızdırma

WAF logları, aynı IP adresinden (203.0.113.45) gelen ardışık SQL Injection denemelerini tespit etmiştir. Denemeler sırasıyla "OR 1=1", "DROP TABLE" ve "UNION SELECT" şeklinde gerçekleştirilmiş olup bu girişimler sistem tarafından engellenmiştir. Ancak sonrasında yapılan "/*!50000OR*/ 1=1" denemesi tespit edilmesine rağmen engellenememiştir (Şekil 11).

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

Şekil 11

Bunun nedeni, WAF'ın basic kurallara göre yapılandırılmış olması ve bu ileri seviye SQL Injection patternini doğru şekilde tanımlayamamasıdır. Bu isteğin ardından /dashboard/export endpoint'ine yapılan erişimle verilerin CSV formatında dışa aktarıldığı gözlemlenmiştir. Bu aşama, olay kapsamında veri sızıntısının gerçekleştiği kritik nokta olarak değerlendirilmektedir (Şekil 12).

7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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

Şekil 12

10:15–11:25 UTC – Normal Kullanıcı Aktivitesi

WAF ve web logları bu saat diliminde anormal bir aktivite tespit etmemiştir.
Kullanıcı oturumları temiz IP adreslerinden, meşru JWT token'ları ile yürütülmüştür.
Saldırgan aktiviteleri bu saat diliminde sonlanmıştır.

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/
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/
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/
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

2024-10-15 10:15:30	920100	LOW	DETECT	45.123.89.201	/login	Normal Login Pattern	no

Şekil 13

Timeline Reconstruction

Zaman (UTC)	Kaynak	Olay	Durum
01:30	192.168.1.100	Otomatik güvenlik taraması	Beklenen
06:47	203.0.113.45	Hesap numarası keşfi	Şüpheli
08:55	10.0.1.50	Admin export & ProtonMail e-posta	Şüpheli
09:00	203.0.113.45	Phishing e-postaları	Kötü niyetli
09:19	203.0.113.45	Yetkisiz giriş (user 1523)	Kötü niyetli
09:23	203.0.113.45	SQL Injection & veri sızdırma	Kritik
10:15–11:25	Çeşitli	Normal operasyon	Normal

Şekil 14

1.2 Attack Vector Identification

Yapılan analiz sonucunda olayın birden fazla saldırı vektörü üzerinden yürütüldüğü belirlenmiştir. İlk aşamada saldırgan, API katmanındaki IDOR (Insecure Direct Object Reference) zafiyetini kullanarak /api/v1/portfolio uç noktasında kullanıcı ID'lerini keşfetmiş ve sistemin veri erişim mantığını anlamıştır. Bu aşama, hedefli saldırı için reconnaissance (keşif) evresi niteliğindedir. Elde edilen kullanıcı verileri ve kimlik bilgileri, saldırganın daha sonraki adımlarda sosyal mühendislik (phishing) faaliyetini gerçekçi şekilde yürütmesine imkân tanımıştır. Özellikle acme-finance.com sahte alan adının kullanılması, kurumsal alan adının taklit edilerek kullanıcı güvenini suistimal ettiğini göstermektedir.

Phishing yoluyla ele geçirilen kimlik bilgileri kullanılarak, saldırgan 203.0.113.45 IP adresinden sisteme geçerli kullanıcı hesaplarıyla kimlik doğrulaması gerçekleştirmiştir. Ardından, /dashboard/search uç noktasında SQL Injection zafiyetinden yararlanarak veri tabanına yetkisiz sorgular göndermiş ve /dashboard/export fonksiyonu aracılığıyla veri sızıntısını tamamlamıştır. Bu zincir, kimlik avı, uygulama zafiyeti ve erişim kontrol eksikliklerinin bir arada kullanıldığı karma bir saldırı vektörü oluşturmaktadır. Olayın planlı sızma testi IP aralığı üzerinden gerçekleştirilmiş olması, saldırganın tespitten kaçınmak için meşru ağ kaynaklarını kötüye kullandığını ve güvenlik izleme sistemlerini yanıltmayı amaçladığını ortaya koymaktadır.

1.3 Attack Classification (MITRE ATT&CK / OWASP)

Bu olay MITRE ATT&CK çerçevesinde birden fazla taktiği kapsamaktadır:

- **TA0001 Initial Access** – Phishing (T1566.002): Sahte domain üzerinden kimlik bilgisi toplama.
- **TA0006 Credential Access** – Credential Harvesting (T1555): Kullanıcı kimlik bilgilerinin ele geçirilmesi.
- **TA0009 Collection** – Data from Information Repositories (T1213): Veritabanı sorguları aracılığıyla bilgi toplama.
- **TA0010 Exfiltration** – Exfiltration Over Web Service (T1567.002): CSV formatında dışa veri aktarımı.

OWASP Top 10 2021 sınıflandırmasına göre olayın ana zafiyetleri şu kategorilere girmektedir:

- **A01: Broken Access Control** – IDOR zafiyetiyle kullanıcı verilerinin keşfedilmesi.
- **A03: Injection** – SQL Injection üzerinden veri tabanına erişim.
- **A05: Security Misconfiguration** – WAF kurallarının yetersiz yapılandırılması.
- **A07: Identification and Authentication Failures** – MFA eksikliği nedeniyle ele geçirilen credentialların doğrudan kullanılabilmesi.

1.4 Root Cause Analysis

Olayın temel nedeni, API uç noktalarında uygulanan erişim kontrollerinin yetersizliği ve güvenlik duvarı (WAF) kurallarının yalnızca temel kalıplara göre yapılandırılmış olmasıdır. Ayrıca planlı sızma testi IP aralıklarının erişim izinlerinin yanlış veya eksik kısıtlanması, saldırganın meşru trafiğe karışarak tespit edilmeden ilerlemesini sağlamıştır. Kullanıcılarda MFA eksikliği, phishing e-postalarının etkili olmasına ve kimlik bilgilerinin kolaylıkla kullanılmasına yol açmıştır. Güvenlik farkındalığı eğitimlerinin sınırlı olması da sosyal mühendislik aşamasının başarıyla sonuçlanmasında etkili olmuştur.

1.5 Impact Assessment

Gerçekleşen olay sonucunda sistemde yaklaşık 870 KB boyutunda kullanıcı verisi (isim, e-posta, portfolyo ID, işlem geçmişi gibi) dışarı sızdırılmıştır. Olayın doğrudan müşteri verilerini etkilemesi, markanın itibarına zarar verme potansiyeli ve düzenleyici otoriteler nezdinde olası yasal bildirim zorunluluklarını doğurması nedeniyle Severity Level: Critical olarak sınıflandırılmıştır. Finansal kayıp tespiti yapılmamış olmakla birlikte, kimlik bilgilerinin ele geçirilmiş olması ileride credential stuffing veya account takeover saldırılarına zemin hazırlayabilir. Bu nedenle olay, hem operasyonel hem itibari açıdan yüksek risk taşımaktadır.

2. Architecture Review

2.1 Current Architecture Weaknesses

Acme Financial Services'in mevcut altyapı mimarisi, fonksiyonel olarak tutarlı bir yapı sunsa da yaklaşan SOC 2 Type II denetimi (November 15-30) öncesinde güvenlik katmanlarının bütünsel olarak ele alınmadığı görülmektedir. Sistem, kullanıcı trafiğini Load Balancer → API Gateway → WAF → Application Server → Database hattı üzerinden yönetmekte, ancak bu zincir içinde özellikle API güvenliği ve erişim kontrolü tarafında zayıf halkalar bulunmaktadır.

İncelenen loglar ve test belgeleri mevcut mimarinin bazı yapısal güvenlik eksikliklerini ortaya koymuştur. Öncelikle WAF yapılandırması yalnızca temel imza tabanlı kurallar ile sınırlı kalmış, bu durum gelişmiş SQL Injection varyantlarının tespit edilmesini engellemiştir. API tarafında, özellikle /api/v1/portfolio/{account_id} uç noktasında token doğrulaması yapılsa bile hesap sahipliği kontrolü gerçekleştirilmemektedir. Bu tasarım hatası, IDOR zafiyetinin doğrudan ortaya çıkmasına neden olmuştur.

E-posta trafiği açısından, SPF/DKIM/DMARC kayıtlarının uygulanmadığı ve sahte domain (örneğin acme-finance.com) üzerinden gönderilen phishing e-postalarının filtrelenemediği tespit edilmiştir. Ayrıca, test altyapısında kullanılan IP aralıklarının (203.0.113.0/24) üretim ortamında yeterli şekilde sınırlandırılmaması, saldırganların planlı test trafiği görünümünde hareket etmesini kolaylaştırmıştır. Database erişim politikalarında "least privilege" prensibine uygun rol ayrımı yapılmamış, uygulama sunucuları veritabanına doğrudan erişebilmektedir. Bu da denetim öncesi kontrol matrisinde zafiyetli bir alan olarak değerlendirilmektedir.

2.2 Improved Security Architecture

Yeni tasarım, mevcut açıkları ortadan kaldırmak ve denetim uyumluluğunu (SOC 2 Type II, OWASP Top 10, NIST CSF) güçlendirmek üzere "Defense in Depth" yaklaşımına göre yeniden yapılandırılmıştır.

Kullanıcı Katmanı:
Tüm kullanıcı oturum açma işlemleri için MFA zorunluluğu getirilmelidir. E-posta trafiği için SPF, DKIM ve DMARC politikaları aktif hale getirilerek sahte domain tabanlı kimlik avı saldırılarının önüne geçilmelidir.

Ağ Katmanı:
Load Balancer arkasında, API Gateway ve Web uygulamaları farklı network segmentlerine ayrılmalı; yalnızca doğrulanmış trafik bu segmentler arasında yönlendirilebilmelidir. WAF sistemi, OWASP ModSecurity CRS v3.3.2 kuralları ve davranış tabanlı anomali tespitiyle güçlendirilmelidir.

Uygulama Katmanı:
API Gateway üzerinde claim-based authorization kontrolü uygulanmalı; token doğrulamasının yanı sıra user_id ile token.subject eşleşmesi zorunlu hale getirilmelidir. Tüm

SQL sorgularında parameterized queries veya ORM tabanlı sorgu yapısı kullanılmalıdır. Rate limit politikaları tutarlı hale getirilmeli, her API yanıtı korelasyon ID ile loglanarak denetim izi oluşturmalıdır.

Veritabanı Katmanı:
Veritabanı erişimi servis hesaplarıyla sınırlandırılmalı, "read/write" izinleri sadece gerekli tablolara verilmelidir. Database Activity Monitoring (DAM) entegrasyonu ile olağan dışı sorgular gerçek zamanlı olarak tespit edilmelidir.

Denetim ve İzleme Katmanı:
WAF, API, Auth ve SIEM sistemlerinden gelen loglar MITRE ATT&CK temelli korelasyon kuralları ile analiz edilmeli; SOAR entegrasyonu sayesinde olay müdahalesi otomatikleştirilmelidir. Tüm güvenlik testleri, belirtilen zaman dilimleriyle karşılaştırılarak yanlış alarmlar (false positive) ayrıştırılmalıdır.

2.3 Recommended Security Controls (with Justification)

Yeni güvenlik mimarisi kapsamında önerilen kontroller, hem tespit edilen zafiyetleri gidermek hem de yaklaşan denetim sürecinde kontrol etkinliği kanıtı oluşturmak amacıyla seçilmiştir.

- **MFA Entegrasyonu:** Phishing sonrası credential reuse riskini azaltır ve kimlik doğrulama güvenliğini artırır.
- **SPF/DKIM/DMARC Politikaları:** Domain sahteciliğini önler, e-posta tabanlı sosyal mühendislik saldırılarını etkisiz hale getirir.
- **WAF Kurallarının Geliştirilmesi:** Gelişmiş SQLi ve XSS varyantlarının tespitini sağlar; saldırı yüzeyini daraltır.
- **API Token Sahiplik Doğrulaması:** Kullanıcıya ait olmayan verilere erişimi engeller, IDOR riskini ortadan kaldırır.
- **Veritabanı Yetki Ayrımı:** Least privilege prensibini uygular, veri sızıntısında hasar kapsamını azaltır.
- **SIEM & SOAR Entegrasyonu:** Korelasyon bazlı uyarı sistemini güçlendirir, olay müdahale süresini kısaltır.

2.4 Defense-in-Depth Strategy

Önerilen mimari, güvenliği yalnızca tek bir katmana bırakmak yerine çok katmanlı bir savunma hattı üzerinden sağlamayı hedeflemektedir. E-posta güvenliği, kimlik doğrulama ve WAF politikaları kullanıcı tarafında saldırı yüzeyini azaltırken; API Gateway, uygulama erişim kontrolleri ve segmentasyon, sistem içi yayılmayı önler. Veritabanı seviyesinde izleme ve ayrıcalıklı erişim kısıtlamaları, olası bir ihlalin etkisini en aza indirir.

Bu yapı, Zero Trust prensiplerine uygun olarak her erişimi doğrulayan, izleyen ve sınırlandıran bir çevrimsel savunma modeli oluşturur. Böylece hem dış kaynaklı tehditler hem de iç ağdan kaynaklanabilecek hatalı erişimler denetim öncesinde minimize edilir. Yaklaşan

PwC SOC 2 Type II denetimi kapsamında bu strateji, hem kontrol etkinliğinin hem de güvenlik olgunluk seviyesinin kanıtı olarak değerlendirilecektir.

3. Response & Remediation

3.1 Immediate Actions (0–24 Hours)

Olayın tespit edilmesiyle birlikte SOC ekibi, 203.0.113.45 IP adresinden gelen tüm trafiği geçici olarak engellemeli ve olayla ilişkili kullanıcı hesaplarını karantinaya almalıdır. Phishing kampanyasıyla ele geçirilen credentialların kullanılmasının önüne geçmek amacıyla tüm aktif oturumlar sonlandırılmalı, JWT tokenları iptal edilmeli ve zorunlu parola sıfırlama süreci başlatılmalıdır. WAF loglarında SQL Injection saldırı patternlerinin bir kısmının tespit edilmediği görülmüş, bu nedenle WAF koruma modu "Blocking" seviyesine yükseltilmelidir. Aynı anda e-posta ağ geçidi filtreleri güncellenmeli, acme-finance.com sahte alan adı domain block list'e eklenmelidir.

Ayrıca **PwC** tarafından yürütülecek Kasım 2024 SOC 2 denetimi öncesinde, olaya ilişkin ilk bulgular ve alınan hızlı önlemler kayıt altına alınmalı, "Security Incident Interim Summary" başlığıyla denetim dosyasına eklenmelidir.

3.2 Short-Term Fixes (1–2 Weeks)

Olay sonrası ilk iki hafta içerisinde geliştirici ekip, /api/v1/portfolio uç noktasındaki IDOR zafiyetini gidermek için nesne tabanlı erişim kontrolü (object-level authorization) uygulamasını devreye almalıdır. API Gateway üzerinde user-to-object mapping doğrulaması zorunlu hale getirilmelidir.

Ayrıca /dashboard/search uç noktasında SQL Injection riskini ortadan kaldırmak için parametrik sorgular kullanılmalı ve ORM katmanı devreye alınmalıdır.
WAF kuralları yeniden yapılandırılarak "/*!50000OR*/" gibi gelişmiş bypass pattern'lerini tanıyacak şekilde genişletilmelidir.

SOC ekibi, planlı penetrasyon testleri için ayrılmış 203.0.113.0/24 IP aralığının erişim zamanlamasını sıkılaştırmalı, testlerin yalnızca doğrulanan zaman pencerelerinde izinli olmasını sağlamalıdır.

Kullanıcılara yönelik zorunlu MFA (Multi-Factor Authentication) etkinleştirilmelidir. Phishing olayının tekrarlanmaması için hedefli güvenlik farkındalık eğitimi düzenlenmeli ve kimlik avı simülasyonları yapılmalıdır.
Son olarak, Security Operations Team ile Development Team arasında "incident-to-remediation" süreci belgelendirilmeli ve her aşamada kanıt niteliğinde log ekran görüntüleri içeren teknik rapor hazırlanmalıdır.

3.3 Long-Term Improvements (1–3 Months)

Üç aylık dönem içerisinde Acme Financial Services güvenlik mimarisi yeniden değerlendirilmelidir.

Tüm API uç noktaları için centralized authorization middleware uygulanmalı, yetkilendirme kontrolleri kod seviyesinde değil, merkezi politika katmanında yürütülmelidir.
Data export işlemleri için anomalous activity detection mekanizması eklenmeli, olağan dışı veri hacimleri için otomatik SIEM alert'leri oluşturulmalıdır.
Ayrıca Penetration Testing Governance Policy güncellenmeli, test IP aralıklarının yalnızca yetkili personelce kullanılabilmesi için IP-based token validation mekanizması eklenmelidir.
E-posta altyapısında DMARC, DKIM ve SPF kontrolleri sıkılaştırılmalı ve sahte alan adlarının hızlı tespiti için Threat Intelligence entegrasyonu yapılmalıdır.
Geliştirme sürecinde tüm kod revizyonları için security peer-review zorunlu hale getirilmelidir.

Uzun vadede, Security Operations Center (SOC) kapasitesi artırılarak, anlık uyarıların manuel analizden ziyade otomatik olay önceliklendirme (SOAR) sistemiyle yönetilmesi hedeflenmelidir.

3.4 Compliance Considerations

Bu olay, yaklaşan SOC 2 Type II denetimi (15–30 Kasım 2024, PwC) kapsamında "Security Controls" ve "Access Management" alanlarıyla doğrudan ilişkilidir. Denetim öncesi:

- Tüm düzeltici eylemler, Change Management Ticketing System üzerinde referans numaralarıyla belgelenmelidir.
- Root Cause Analysis raporu, denetçi PwC'ye sunulacak "Corrective Action Register" içine eklenmelidir.
- Olayla ilişkili tüm log kayıtları (API, WAF, Mail Gateway) en az 180 gün süreyle arşivlenmelidir.
- Kullanıcı credentiallarının sıfırlanması ve MFA geçişi tamamlandıktan sonra, bu eylemlerin denetim notlarına "Completed Control Action" olarak işlenmesi gerekmektedir.

Bu kapsamda Acme Financial Services, olay sonrası süreçte yalnızca teknik düzeltmeler yapmakla kalmamalı, aynı zamanda denetim standartlarına uygun olarak olay yönetimi, kayıt tutma ve kontrol iyileştirme faaliyetlerini eksiksiz belgelemelidir.