Güvenlik Olayı Analiz Raporu

(Uzman Yardımcısı Adayı Raporu)

Ekim 2024

Raporu Hazırlayan (Analist)	Halil ALİSA
Olay Başlangıç Tarihi	15.10.2024
Olay Bitiş Tarihi	15.10.2024
Onaylayan / SOC Yöneticisi	-
Kurum / Sistem Adı	Acme Financial Services
Olay	Token Reuse > Broken Access Control (IDOR) > Phishing > SQL İnjection

Bu rapor Acme SOC tarafından hazırlanmıştır. İlgili birimlere e-posta yoluyla iletilmelidir.

Bölüm 1: Olay Analizi

Özet

15.10.2024 Tarihinde Acme Finansal Hizmetleri Ticaret Platformuna koordineli çok yönlü siber saldırı gerçekleşmiştir. Saldırı kapsamında kurumun maruz kalmış olduğu saldırı vektörleri aşağıda yer almaktadır:

- Sosyal Mühendislik (Oltalama Tekniği) : Çalışanları hedefleyen kimlik avı kampanyası
- Token Reuse : Broken Access Control (IDOR), tekniği kullanılarak API istismari
- SQL Injection : Web Uygulaması İstismarı

Saldırgan, tüm aşamaları 203.0.113.45 IP'si üzerinden gerçekleştirmiş. WAF, 8 saldırının 3/8 olmak üzere kısmı bloklama yapmış. API üzerinde ise yeterli kontroller olmadığından ötürü IDOR zafiyeti üzerinden ve WEB Uygulaması üzerinden eksik konfügrasyondan ötürü SQL Injection üzerinden veri sızıntısı gerçekleşmiştir.

Zaman Çizelgesi

Zaman	Aşama	Olay	Kaynak IP	Durum
01:30:15 - 01:30:19	Recon	192.168.1.100 API kaba kuvvet	192.168.1.100	Tespit Edildi
06:45:10 - 06:47:57	Istismar	jwt_token_1523_stolen ile 15 hesap sorgulandı	203.0.113.45	Başarılı
09:00:23	İlk Erişim	Phishing kampanyası (acme-finance.com)	203.0.113.45	Kullanıcılar (1,3,5) Etkilendi
09:18:30	Oturum açma	user 1523 web'e giriş yaptı	203.0.113.45	Yetkili Erişim
09:20:30 - 09:23:45	İstismar	/dashboard/search SQLi zinciri (VEYA 1=1 → DROP TABLE → UNION SELECT)	203.0.113.45	Kısmen Bloklandı
09:24:10	Veri Hırsızlığı	/dashboard/export → 892 KB CSV çıktı	203.0.113.45	Başarılı
10:15:30 - 11:25:45	Normal Trafik	Diğer kullanıcı aktiviteleri	45.123.89.201, 172.89.15.67	Normal

Teknik Bulgular

1. **Script Çalışması**
   Şekil 1'de görüleceği üzere LAN 192.168.1.100 IP'sinde iç ağda, Python Script'i çalıştırılmış. Script 1'er saniye arayla çalışıp, 1000-1004 ID numaralı Account'lar için API'ye istek atmakta, Response olara ise 401 dönmektedir. Şekil 1.2 ise WAF ynıtları görmekte ancak LAN IP'si olduğu için bloke etmemektedir.

192.168.1.100

	timestamp	user_id	endpoint	method	account_id	response_code	response_time_ms	ip_address	user_agent	session_token
2	2024-10-15 01:30:15	NULL	/api/v1/portfolio/1000	GET	1000	401	45	192.168.1.100	Python-requests/2.28.0	
3	2024-10-15 01:30:16	NULL	/api/v1/portfolio/1001	GET	1001	401	42	192.168.1.100	Python-requests/2.28.0	
4	2024-10-15 01:30:17	NULL	/api/v1/portfolio/1002	GET	1002	401	44	192.168.1.100	Python-requests/2.28.0	
5	2024-10-15 01:30:18	NULL	/api/v1/portfolio/1003	GET	1003	401	43	192.168.1.100	Python-requests/2.28.0	
6	2024-10-15 01:30:19	NULL	/api/v1/portfolio/1004	GET	1004	401	46	192.168.1.100	Python-requests/2.28.0	

Şekil 1 (API Log'ları)

192.168.1.100

	timestamp	rule_id	severity	action	source_ip	uri	signature	blocked
7	2024-10-15 01:30:15	920420	LOW	DETECT	192.168.1.100	/api/v1/portfolio/1000	Multiple Failed Auth	no
8	2024-10-15 01:30:19	920420	LOW	DETECT	192.168.1.100	/api/v1/portfolio/1004	Multiple Failed Auth	no

Şekil 1.2 (WAF Log'ları)

2. **Sosyal Mühendislik (Oltalama Tekniği)**
   Saldırgan, Şekil 2'de görüleceği üzere security@acme-finance.com ve 203.0.113.45 üzerinden kurum çalışanlarına, Oltalama saldırı gerçekleştirmiştir. 6 hedeften, 3'ü linke tıklayıp oltalama saldırısına maruz kalmıştır. Maruz kalan kullanıcılar 1, 3 ve 5'dir. Oltalama Saldırısına maruz kalan saldırganların bilgileri ele geçirilmiştir.

   Güvenlik Önlemi : Kurum çalışanlarına Siber Güvenlik Farkındalığı Eğitimi Verilmelidir.

security@acme-finance.com

	timestamp	from	to	subject	link_clicked	ip_address	attachment
3	2024-10-15 09:00:23	security@acme-finance.com	user1@acme.com	URGENT: Verify Your Account - Action Required	yes	203.0.113.45	
4	2024-10-15 09:00:25	security@acme-finance.com	user2@acme.com	URGENT: Verify Your Account - Action Required	no		
5	2024-10-15 09:00:27	security@acme-finance.com	user3@acme.com	URGENT: Verify Your Account - Action Required	yes	203.0.113.45	
6	2024-10-15 09:00:29	security@acme-finance.com	user4@acme.com	URGENT: Verify Your Account - Action Required	no		
7	2024-10-15 09:00:31	security@acme-finance.com	user5@acme.com	URGENT: Verify Your Account - Action Required	yes	203.0.113.45	
8	2024-10-15 09:00:33	security@acme-finance.com	user6@acme.com	URGENT: Verify Your Account - Action Required	no		

Şekil 2 (Email Log'ları)

3. **API Saldırısı**
   IDOR zafiyetinden yararlanan saldırgan, 1523 ID sahip kullanıcı ile sisteme giriş yapmaktadır. Giriş yaptıktan sonra /portfolio/{1524–1538} arasında yer alan 15 kullanıcının, pörtfolyosuna erişim sağlayak istismari gerçekleştirmektdir. Token olarak 15 kullanıcı için "jwt_token_1523_stolen" tokeni belirtilmiş.
   Güvenlik Önlemi : Kontrol mekanizmasına **"**if g.current_user.account_id != account_id:" kodu eklenerek. user_id ile account_id eşleşmesinin kontrolü sağlanmalıdır.

203.0.113.45

	timestamp	user_id	endpoint	method	account_id	response_code	response_time_ms	ip_address	user_agent	session_token
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

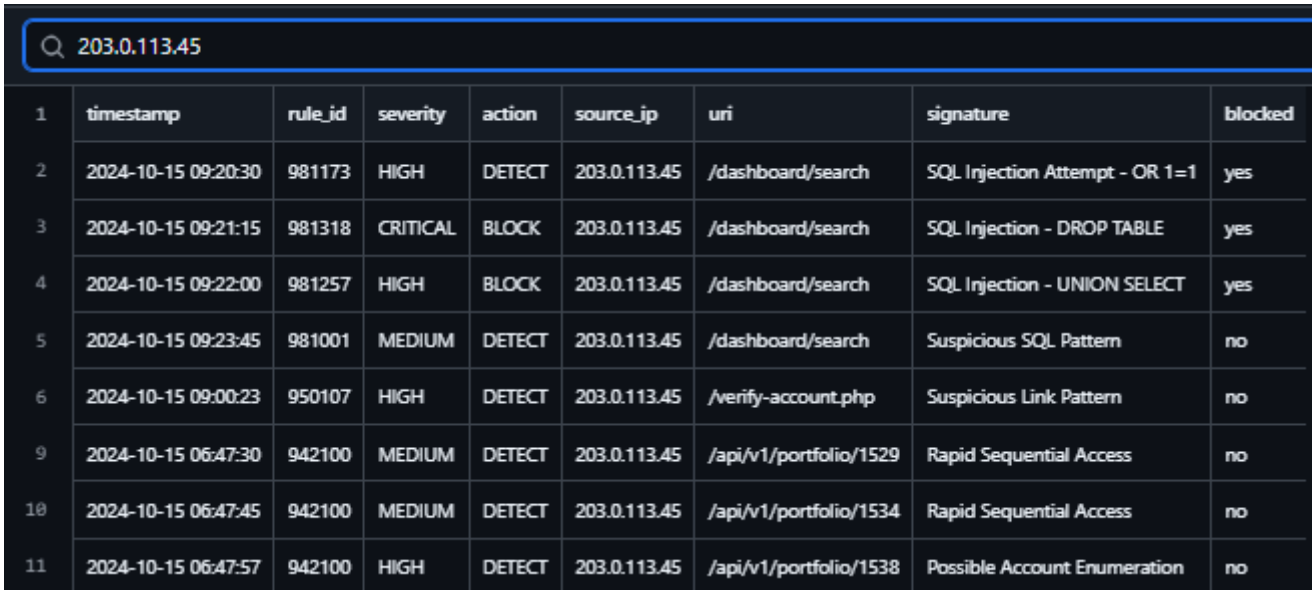
Şekil 3 (API Log'ları)

4. Web Saldırısı

Web Saldırısında, saldırganın ilk 3 denemesi Şekil 4 ve 4.1 görüleceği üzere saldırılar başarısız olmuş bulunmaktadır. İstekler WAF tarafından, bloke edilerek 403 yanıtı döndürülmüştür. Ancak "/!50000OR/ 1=1--" sorgusu ile WAF bypass edilip, SQL Injection başarılı bir şekilde gerçekleşmiş. "/dashboard/export" yanıtında görüleceği üzere, 892 KB veri, CSV formatında sızdırılmıştır.

```
1  timestamp,user_id,endpoint,query_params,response_code,response_size_bytes,ip_address,user_agent
2  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
3  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
4  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/605.1
5  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/605.1
6  2024-10-15 09:15:45,3421,/login,,200,3421,172.89.15.67,Mozilla/5.0 (X11; Linux x86_64) Firefox/119.0
7  2024-10-15 09:16:20,3421,/dashboard,,200,8745,172.89.15.67,Mozilla/5.0 (X11; Linux x86_64) Firefox/119.0
8  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
9  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
10 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
11 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
12 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
13 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
14 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
15 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
16 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
17 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/605.1
18 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/605.1
19 2024-10-15 11:20:15,7891,/login,,200,3421,172.89.15.67,Mozilla/5.0 (X11; Linux x86_64) Firefox/119.0
20 2024-10-15 11:21:30,7891,/dashboard,,200,8934,172.89.15.67,Mozilla/5.0 (X11; Linux x86_64) Firefox/119.0
21 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
```

Şekil 4



203.0.113.45

	timestamp	rule_id	severity	action	source_ip	uri	signature	blocked
2	2024-10-15 09:20:30	981173	HIGH	DETECT	203.0.113.45	/dashboard/search	SQL Injection Attempt - OR 1=1	yes
3	2024-10-15 09:21:15	981318	CRITICAL	BLOCK	203.0.113.45	/dashboard/search	SQL Injection - DROP TABLE	yes
4	2024-10-15 09:22:00	981257	HIGH	BLOCK	203.0.113.45	/dashboard/search	SQL Injection - UNION SELECT	yes
5	2024-10-15 09:23:45	981001	MEDIUM	DETECT	203.0.113.45	/dashboard/search	Suspicious SQL Pattern	no
6	2024-10-15 09:00:23	950107	HIGH	DETECT	203.0.113.45	/verify-account.php	Suspicious Link Pattern	no
9	2024-10-15 06:47:30	942100	MEDIUM	DETECT	203.0.113.45	/api/v1/portfolio/1529	Rapid Sequential Access	no
10	2024-10-15 06:47:45	942100	MEDIUM	DETECT	203.0.113.45	/api/v1/portfolio/1534	Rapid Sequential Access	no
11	2024-10-15 06:47:57	942100	HIGH	DETECT	203.0.113.45	/api/v1/portfolio/1538	Possible Account Enumeration	no

Şekil 4.1

Saldırının Başarılı Olmasının Kök Nedenleri

- MFA zorunluluğu yoktu → phishing ile oturum bilgileri çalındı.
- API'de hesap sahipliği doğrulama eksikliği.
- WAF bazı kurallarda “Detect” modda kaldı.
- SOC korelasyon kuralları IP bazlı zincirleri izlemedi.
- Kurum çalışanlarının farkındalığı yok

MITRE ATT&CK Eşlemesi

Taktik	Teknik	Açıklama
İlk Erişim	T1566.002 – Kimlik Avı Bağlantısı	Kullanıcılar kandırıldı
Kimlik Bilgisi Erişimi	T1556.003 – Web Portalı Kimlik Avı	Token sızıntısı
Yanal Hareket	T1550.001 – Web Belirteci Kullanımı	API'de token reuse
Koleksiyon	T1213.003 – Depolardan Gelen Veriler	Diğer kullanıcı verileri çekildi
Sızma	T1041 – Web Servisleri Üzerinden Veri	/export CSV ile veri sızdı
Etki	T1485 – Veri İmha Girişimi	DROP TABLE ifadesiyle veri silme denemesi

OWASP Eşlemesi

Teknik	Başlık	Açıklama
A01	Bozuk Erişim Kontrolü	API IDOR
A03	Enjeksiyon	SQL Injection
A05	Güvenlik Yanlış Yapılandırması	WAF Yanlış Algılama
A07	Tanımlama & Kimlik Doğrulama Hataları	MFA eksikliği
A09	Arızaları Kaydetme & İzleme	SOC korelasyonu yok

IOC Listesi

Tür	Değer	Açıklama
IP	203.0.113.45	**Saldırgan IP’si**
Alan Adı	acme-finance.com	Phishing alan adı
E-posta	security@acme-finance.com	**Kullanılan E-posta**
Token	jwt_token_1523_stolen	**Kullanılan JWT Token**
Url	/dashboard/search	SQL Injection hedefi

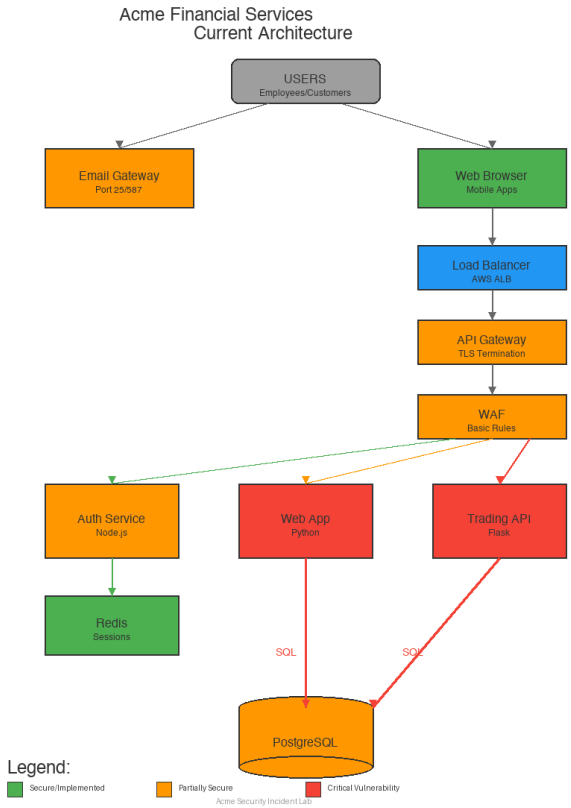
Dosya	user_export.csv	Sızdırılan veri

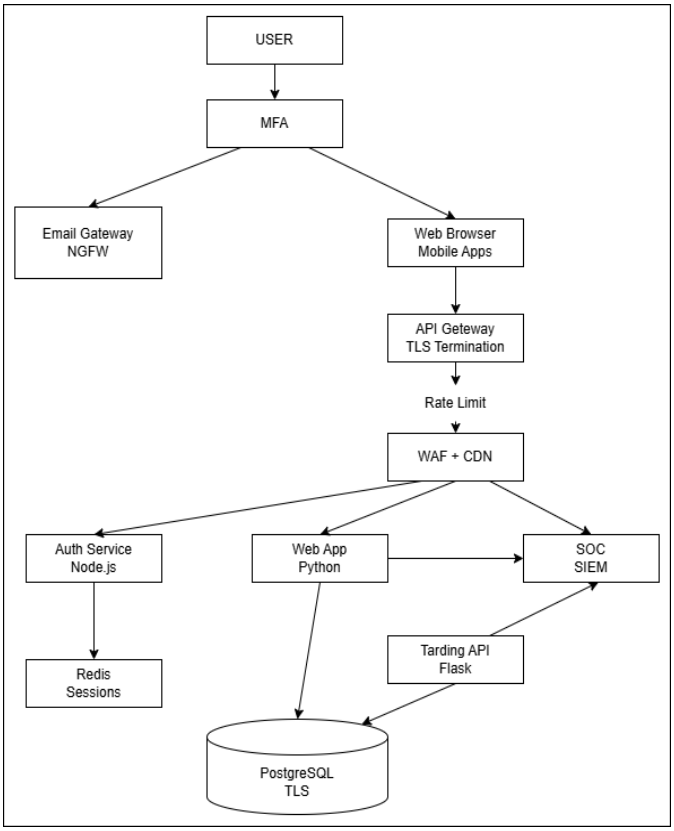
Etki Değerlendirmesi

- Veri Gizliliği : Kullanıcıların verileri sızdırılmış
- Veri Bütünlüğü : Drop Table komutu ile veri bütünlüğü bozulmaya çalışmış ancak WAF tarafından istek bloke edilmiş.
- Sistem Güvenliği : Yanlış yapılandır, MFA, eksik kontrol nedeni ile sisteme sızılmıştır.
- Ris seviyesi 5/5 olarak belirlenmiştir.

Bölüm 2: Mimari İnceleme

Mevcut Mimari	Geliştirilmiş Mimari





Bölüm 3: Yanıt & İyileştirme

- Anında eylemler (0-24 saat)
  - IP karantinaya alınıp, SIEM üzerinden blackliste dahil edilmeli
  - Kullanıcı oturumları sonlandırılmalı ve tüm JWT revoke edilmeli
  - Oltalamaya saldırısına maruz kalan kullanıcı hesapları, bloke edilip askıya alınmalı
- Kısa vadeli düzeltmeler (1-2 hafta)
  - /portfolio/{id} endpointlere sahiplik durum kontrolü eklenmeli
  - Rate Limit Eklenmeli ve tüm kullanıcılar için MFA zorunlu kılınmalı
- Uzun vadeli iyileştirmeler (1-3 ay)
  - WAF + API logları SIEM'e entegre edilmeli
  - Kurum için farkındalık eğitimi verilip, phishing tatbikatı yapılmalı
  - SQL Injection önlemek için WAF kuralları revize edilmeli

Sonuç

Saldırgan, "Token Reuse > Broken Access Control (IDOR) > Phishing > SQL İnjection" çok yönlü zincirleme saldırısını kullanarak, sisteme erişim sağlamayı başarmış bulunmaktadır. Erişim sonrası "/export" CSV ile veri sızıntısı gerçekleştirmiş bulunmaktadır. Bu zincir saldırı katmanlı SOC ve entegre bir yapı olmadığından ötürü tespit edilememiştir. Alınacak önlemler ile aynı saldırı zincir vektörlerinin tekrarlanması önlenebilir.