API LOG

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

İlgili log kaydında yer alan **IP adresi (192.168.1.100)**, TEST1 kapsamında belirtilen **iç ağ (internal network)** aralığına aittir. Bu tespit, kurumun tanımlı network segmentleriyle **doğrulanmıştır**.
Test planına göre her **Salı günü saat 01:30'da** otomatik güvenlik açığı taraması gerçekleştirilmektedir.
İncelenen log kaydının **zaman damgası**, planlı tarama zamanlaması ile **örtüşmektedir**.

- IP adresi kurum iç ağ aralığı ile **doğrulanmıştır**,
- Log kaydının zaman damgası planlı tarama zamanlaması ile **uyumludur**,
- 401 durum kodu tarama aracının kimlik doğrulaması isteğinden kaynaklanmaktadır ve **user_id = NULL** beklenen bir sonuçtur, verilen dokümantasyonda "oturum açma sırasında 401 hataları beklenen durumdur." Açıklaması yer almaktadır.
- **Herhangi bir güvenlik ihlali veya olağandışı davranış tespit edilmemiştir.**

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

Log kaydında yer alan **10.0.0.50** IP adresi, kurum dokümantasyonunda **SOC_Team'e tahsis edilen 10.0.0.0/24 ağ bloğu** içerisinde yer almaktadır.
Ayrıca kayıtta görülen **account_id'ler (5001–5005)**, aynı dokümantasyonda **test aralığı olarak tanımlanmış 5001–5010 aralığı** ile uyumludur..
Bu nedenle kayıt, **planlı ve yetkilendirilmiş SOC_Team güvenlik taraması** kapsamında değerlendirilmiş olup **herhangi bir güvenlik ihlali tespit edilmemiştir.**

2024-10-15 04:15:30	2347	/api/v1/login	POST		200	234	98.213.45.122	Acme-Mobile-iOS/3.2.1	
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
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
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

İncelenen log kaydında yer alan **98.213.45.122** IP adresi **public** olup dış ağ bağlantısı üzerinden erişim gerçekleştirilmiştir.
İlgili IP, **user_id = 2347** kullanıcısına aittir. Log kayıtlarına göre kullanıcı **Acme Mobile** uygulaması üzerinden sisteme giriş yapmış, **portfolio görüntüleme, işlem geçmişi (transactions)** ve **transfer** işlemleri gerçekleştirmiştir.
İşlemler olağan kullanıcı aktiviteleriyle uyumlu görünmekle birlikte, **transfer işlemine ilişkin oturumun bir süre izlenmesi** tavsiye edilmektedir.

2024-10-15 05:30:12	3891	/api/v1/login	POST		200	198	172.89.15.67	Acme-Mobile-Android/3.1.9	
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
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

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

Log analizine göre **172.89.15.67** IP adresi üzerinden iki farklı kullanıcı hesabı erişim sağlamıştır.
Söz konusu IP adresi **public IP aralığındadır** ve dış ağ üzerinden bağlantı yapılmıştır.
Kullanıcıların erişim kayıtları incelendiğinde birinin **Android**, diğerinin ise **iOS** cihazdan giriş yaptığı görülmektedir.
Bu durum aynı kullanıcının farklı cihazlardan erişimi veya paylaşımlı ağ (NAT) kullanımı ile açıklanabilir.
Şu aşamada olağan dışı bir aktivite tespit edilmemiştir; ancak aynı IP üzerinden birden fazla hesap erişimi **alışılmadık sıklıkta tekrarlanırsa**, detaylı gözlem önerilir.

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

İncelenen log kaydında **45.123.89.201** numaralı **public IP adresi** üzerinden **Acme Mobile** uygulaması aracılığıyla sisteme erişim sağlandığı görülmüştür.
Kullanıcı, oturum açtıktan sonra **portfolio** ve **market-data** verilerine erişim gerçekleştirmiştir.
HTTP **200** durum kodu, işlemlerin başarıyla tamamlandığını göstermektedir.
Erişim tipi ve gerçekleştirilen işlemler, sistemin normal kullanım senaryoları ile uyumlu olup **herhangi bir güvenlik ihlali tespit edilmemiştir.**

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_stole
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

Kaynak IP: **203.0.113.45** (public, üçüncü taraf test IP bloğuna ait).
Zaman damgası: **2024-10-14 06:45:10** — dokümante edilmiş onaylı test aralığı **20–25 Ekim 2024** ile çakışmıyor.
Erişim tipi: **Acme Mobile (Android v3.2.0)** user-agent'ı ile istekler.
Token göstergesi: token değeri sonunda **"stolen"** ifadesi bulunuyor → **ele geçirilmiş token** ihtimali yüksek.

Hesap erişimleri: Aynı IP'den **birden fazla hesap** (account_id 1523-1538) üzerinde erişim denemeleri ve başarılı 200 yanıtları.
Test kapsamı uyuşmazlığı: Faaliyet, sözleşme/dokümantasyonda belirtilen test onay mekanizmasına ve zamanlamaya uymuyor.
Risk: Yetkisiz veri erişimi, hesap ele geçirme, token suistimali, denetimsiz dış test faaliyeti.
Bu bulgular, planlı ve onaylı bir testten ziyade **yetkisiz/denetlenmemiş güvenlik testi veya kötü niyetli aktivite** ile daha tutarlı olup, **acil müdahale** gerektirmektedir.

Email logları

2024-10-15 08:55:12	admin@acme.com	external.contact@protonmail.com	Q3 Meeting Notes	no	10.0.1.50	meeting_notes.pdf

İncelenen log kaydında **acme.com** alan adlı kaynaktan bir **toplantı notları (PDF)** dosyasının iletildiği görülmüştür.
Dosya paylaşımı, **10.0.1.50** IP adresine sahip bir sistem üzerinden gerçekleştirilmiştir.
Söz konusu IP adresi, RFC1918 standardına göre **kurum içi (private) ağ aralığında** yer almakta olup **dış bağlantı içermemektedir.**
Log kaydında olağan dışı veya şüpheli bir etkinlik tespit edilmemiştir.

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		

Loglarda **203.0.113.45** IP adresinden gönderilen bir e-posta görülmektedir.
Gönderen adresi **acme-finans.com** olup, kurumun resmi alan adı olan **acme.com** ile uyuşmamaktadır.
Bu nedenle e-posta **şüpheli (phishing)** olarak değerlendirilmiştir.
Mesaj içeriğinde kullanıcıların "hesap doğrulaması" yapması istenmiş ve user1, user3,user5 bağlantıya **tıkladığı** görülmüştür. Bu durum, **oltalama girişimi** olasılığını güçlendirmektedir.
Sonuç:
E-posta spoofing yöntemiyle acme.com gibi davranılarak gönderilmiştir. Kullanıcıları yanıltmak için "ödül, doğrulama" gibi psikolojik tetikleyiciler kullanılmıştır. Bu log, **phishing aktivitesine işaret etmektedir** ve kullanıcı farkındalığı ile mail filtrelerinde domain kontrolü artırılmalıdır.

2024-10-15 11:45:20	it@acme.com	engineering@acme.com	Scheduled Maintenance Tonight	no	10.0.2.25

Log kayıtlarına göre **acme.com** alan adından, **engineering@acme.com** domainine sahip mühendislik ekibine bir e-posta gönderilmiştir.
E-posta içeriğinde "**bu gece planlı bakım/çalışma yapılacaktır**" ifadesi yer almaktadır.
E-posta gönderim zamanı **2024-10-15 11:45:20** olarak kaydedilmiştir.
Ancak aynı gün **203.0.113.45** IP adresinin, **saat 06:45** civarında sistemin **API loglarında erişim sağladığı** görülmüştür.
Bu durum, e-posta gönderilmeden **yaklaşık 5 saat önce** aynı IP'nin sisteme erişim gerçekleştirdiğini göstermektedir.

Waf logları

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

203.0.113.45 IP'sinin 2024-10-15 06.47.30 saatleri arasında hızlı sıralı erişim yaptığı ve Olası Hesap Numaralandırması yaptığı görülmektedir.

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

Log incelemesinde 2024-10-15 09.00.23-30 saatleri arasında **203.0.113.45** kaynağından gönderilen SQLi ve veri-tahribat (tablo silme, birleşik sorgu) denemeleri tespit edilmiştir. Bazı girişimler WAF tarafından engellenmiş, bazıları engellenmemiştir. Dokümantasyondaki "planlı test IP'leri için istisna" politikası nedeniyle engellenmeyen istekler açıklanabilir; **ancak tespit edilen aktiviteler dokümante edilmiş onaylı test tarih aralığı olan *20–25 Ekim 2024* dışında gerçekleşmemiştir**, bu nedenle olay onaysız/denetlenmemiş bir faaliyet olarak değerlendirilmelidir. Acil olarak IP doğrulaması, engellenmeyen isteklerin adli incelenmesi ve WAF kurallarının güçlendirilmesi önerilir.

Web logları

15.10.2024 08:55	admin_5678	/admin/users/export	200	15673	10.0.1.50	Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/118.0
15.10.2024 08:56	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

Loglarda **admin** hesabıyla **CSV formatında büyük bir veri dışa aktarımı** tespit edilmiştir.
Admin yetkisi nedeniyle bu işlem **beklenen/olağan** görünebilir; ancak **kesinlikle risksiz** olduğu söylenemez. Bu hareket şüpheli bir hareket gibi görünsede bunu bir yere gönderdiğine dair bir şey yok.

15.10.2024 09:18	1523	/login		200	3421	203.0.113.45	Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/118.0
15.10.2024 09:19	1523	/dashboard		200	8934	203.0.113.45	Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/118.0
15.10.2024 09:20	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
15.10.2024 09:21	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
15.10.2024 09:22	1523	/dashboard/search	ticker=AAPL' UNION SELECT * FROM	403	567	203.0.113.45	Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/118.0
15.10.2024 09:23	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
15.10.2024 09:24	1523	/dashboard/export	format=csv	200	892341	203.0.113.45	Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/118.0
15.10.2024 09:30	1523	/dashboard/home	200"	200	8934	203.0.113.45	Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/118.0

15.10.2024 09:23 kaydında ticker parametresine yerleştirilmiş SQL injection payload kullanılmış; istek **200 OK** dönmüş ve **156,789 byte** veri elde edilmiştir.
15.10.2024 09:24 kaydında `export=format=csv` görünmektedir; kısa zaman aralığı dikkate alındığında **verinin dışa aktarıldığı (exfiltration şüphesi)** kuvvetlenmiştir.
Öncesinde aynı IP ile başarılı **login + dashboard** erişimleri ve bazı sorgularda **403** cevapları kayıtlıdır.
Değerlendirme: SQLi payload'u ile filtre atılmış ve büyük miktarda veri döndürülmüştür; hemen ardından CSV export görülmesi nedeniyle olay **muhtemel veri sızdırma** olarak ele alınmalıdır.
Not: 203.0.113.45 IP'si teknik olarak planlı testleri gerçekleştirebilecek bir test IP'si olabilir; ancak kaydedilen aktiviteler **dokümante edilmiş onaylı test zaman aralığı (20–25 Ekim 2024)** ile **uyumlu değildir**. Bu nedenle söz konusu faaliyet **onaylı test** olarak kabul edilmemelidir.

Risk Değerlendirmesi ve Önerilen Önlemler

1-Veri Sızdırma Riski (SQL Injection + CSV Export)

- **Durum:** 203.0.113.45 IP'si üzerinden yapılan SQL sorgusunda hatalı veri kontrolü sonucu çok sayıda kayıt (156,789 byte) çekilmiş, ardından `export csv` işlemi yapılmış.
- **Risk:** Yetkisiz veri dışa aktarımı olabilir.
- **Öneri:**
    - Bu IP geçici olarak engellenmeli.
    - Loglar detaylı incelenmeli.
    - Export işlemleri için onay süreci (DLP veya manuel) eklenmeli.

2-Çalıntı Token Kullanımı

- **Durum:** Bazı erişimlerde "stolen" ibareli token kullanıldığı görülmüş.
- **Risk:** Başkasına ait oturumla sisteme giriş yapılmış olabilir.
- **Öneri:**
    - Tüm token'lar sıfırlanmalı.
    - Kullanıcılar yeniden giriş yapmaya zorlanmalı.
    - Token süreleri kısaltılmalı ve daha güvenli saklama yöntemi kullanılmalı.

3-Phishing (Oltalama) E-postası

- **Durum:** "acme-finans.com" adresinden gönderilen sahte e-posta, bazı kullanıcılar tarafından açılmış.
- **Risk:** Kullanıcı bilgileri çalınabilir.
- **Öneri:**
    - Kullanıcılara bilgilendirme yapılmalı.
    - Mail filtreleri ve DMARC ayarları gözden geçirilmeli.
    - Düzenli phishing farkındalık eğitimi yapılmalı.

4-Plan Dışı Test Faaliyetleri

- **Durum:** 203.0.113.45 IP'si test IP'si olabilir ancak aktivite zamanı (14 Ekim) planlı test tarihleri (20–25 Ekim) dışında.
- **Risk:** Yetkisiz test veya sızma denemesi olabilir.
- **Öneri:**
    - Firma ile test zamanlaması teyit edilmeli.
    - Bu IP'den gelen erişimler izlenmeli veya geçici olarak engellenmeli.

5-Admin Hesabı ile Büyük Veri Exportu

- **Durum:** Admin hesabı büyük miktarda CSV veri dışa aktarmış.
- **Risk:** Bilgi sızıntısı veya iç tehdit olabilir.
- **Öneri:**
    - Export işleminin amacı doğrulanmalı.
    - Gerekirse büyük export'lar için ikinci onay süreci getirilmeli.

6-Hızlı Sıralı Erişim (Olası Hesap Numaralandırması)

- **Durum:** 203.0.113.45 IP’si kısa sürede çok sayıda erişim denemesi yapmış.
- **Risk:** Hesap tarama veya brute-force denemesi olabilir.
- **Öneri:**
    - Rate-limit (hız sınırı) ve captcha kullanılmalı.
    - Anormal oturum davranışları izlenmeli.