I - Information Disclosure (Bilgi İfşası)

Hedef: Hassas verilerin (kullanıcı PII, şifreler, sistem detayları) yetkisiz kişilerin eline geçmesi.

1. Saldırı Ağacı - Kullanıcı Verisi Sızıntısı (BOLA/IDOR)

Hedef: Diğer Kullanıcıların Şarj Verilerini ve Konumlarını Görmek

Adım 1: Meşru Bir Hesapla API Trafiğini İzlemek
Alt Adım 1a: Saldırgan, kendi hesabıyla mobil uygulamaya giriş yapar.
Alt Adım 1b: (Burp Suite gibi) bir proxy aracıyla uygulama ve API arasındaki trafiği izler.

Adım 2: Hassas Bir API Endpoint'i Tespit Etmek
Alt Adım 2a: Şarj geçmişini görüntülerken GET /api/v1/users/54321/transactions şeklinde bir API isteği tespit eder (54321 kendi ID'si).

Adım 3: ID Parametresini Manipüle Etmek (BOLA/IDOR)
Alt Adım 3a: İsteği tekrarlar ancak ID'yi 54322 olarak değiştirir.

Adım 4: Yetkisiz Veriye Erişmek
Alt Adım 4a: API, "403 Yasak" hatası vermek yerine, 54322 ID'li kullanıcının tüm şarj geçmişini (tarih, saat, maliyet, istasyon konumu) JSON formatında döndürür.
Sonuç: Saldırgan, tüm kullanıcı ID'lerini tarayarak (enumeration) herkesin verisini çekebilir.

2. Sömürü Senaryoları

Şarj Davranış Pattern'leri: Saldırgan (belki bir veri ihlali yoluyla) toplu veri sızıntısı elde ederse, bir kullanıcının (örn. bir politikacı veya CEO) "hafta içi her gün saat 18:00'de A konumunda, 09:00'da B konumunda" şarj ettiğini tespit ederek bu kişiyi fiziksel olarak takip edebilir veya nerede olduğunu ifşa edebilir.

Sunucu Tarafı İstek Sahteciliği (SSRF): CSMS'teki (örn. "İstasyon Durumu Kontrol Et" özelliği) zafiyetli bir URL giriş alanı aracılığıyla, sunucunun iç ağına (örn. http://192.168.1.10/db_admin) istek gönderilerek iç ağdaki servislerin varlığı ifşa edilebilir.

Fiziksel İfşa: İstasyonun kapağını açan bir saldırgan, UART/JTAG gibi hata ayıklama portlarına bağlanarak veya flash belleği sökerek, belleğe düz metin olarak yazılmış CSMS bağlantı parolasını, API anahtarlarını veya mTLS özel anahtarını (private key) ifşa edebilir.

3. Azaltma Stratejileri (Mitigation)

API Yetkilendirme Kontrolü (BOLA/IDOR): Her API isteğinde, isteği yapan kullanıcının kimliğini (token'dan gelen ID) ile erişilmek istenen kaynağın sahibinin (URL'deki veya gövdedeki ID) aynı olup olmadığını sunucu tarafında zorunlu olarak kontrol etmek.

Veri Minimizasyonu ve Anonimleştirme: CSMS'in, şarj pattern analizi için sadece anonimleştirilmiş (kullanıcı ID'sinden bağımsız) verileri kullanması. PII (Kişisel Tanımlanabilir Bilgi) verilerinin sadece faturalandırma gibi zorunlu modüllerde ve şifreli (at-rest) olarak saklanması.

Güvenli Anahtar Depolama (Donanım): İstasyonun özel anahtarı (private key) veya CSMS parolası gibi kritik bilgilerin, TPM (Trusted Platform Module) veya Güvenli Eleman (SE) gibi donanımsal güvenlik yongalarında saklanması.

4. Tespit Mekanizmaları (Detection)

API Anomali Tespiti: Bir IP adresinin veya kullanıcının, kısa süre içinde çok sayıda farklı kullanıcı ID'sini (örn. /users/1, /users/2, /users/3...) deneyerek istek atmasını (enumeration) tespit etmek ve bu IP'yi geçici olarak engellemek.

WAF (Web Application Firewall): file:///etc/passwd, 169.254.169.254 (Bulut meta-verisi) veya 192.168.* gibi bilinen SSRF ve LFI (Local File Inclusion) payload'larını içeren API isteklerini engellemek.

I - Information Disclosure DREAD Değerlendirmesi

Tehdit Senaryosu: "API'de BOLA/IDOR ile Kullanıcı Verisi Sızıntısı"

(Meşru bir kullanıcının, API isteğindeki userID'yi değiştirerek başka bir kullanıcının şarj geçmişine ve konumlarına erişmesi.)

D - Damage Potential (Zarar Potansiyeli): 8
Gerekçe: Çok ciddi KVKK/GDPR ihlali. Binlerce kullanıcının PII (Kişisel Bilgi), şarj

geçmişi ve lokasyon verisi (ev/iş adresi rutinleri) ifşa olabilir. Yüksek yasal cezalar ve itibar kaybı.

R - Reproducibility (Tekrarlanabilirlik): 10
Gerekçe: Zafiyet varsa, her zaman %100 tekrarlanabilir. Saldırı kolayca otomatize edilerek tüm veritabanı taranabilir.

E - Exploitability (İstismar Edilebilirlik): 3
Gerekçe: İstismar etmesi çok kolaydır. Sadece bir proxy aracı (örn. Burp Suite) ve API isteğindeki userID parametresini değiştirecek kadar temel bilgi gerektirir.

A - Affected Users (Etkilenen Kullanıcılar): 10

Gerekçe: Potansiyel olarak sistemdeki *tüm* kullanıcılar etkilenir.

D - Discoverability (Keşfedilebilirlik): 8

Gerekçe: Bu, API pentestlerinde bakılan ilk ve en yaygın zafiyetlerden biridir. Mobil uygulama trafiğini izleyen herkesin tespiti çok kolaydır.

Risk Skoru: 39/50 (Çok Yüksek Risk)

Sacide Aişenur Direk