**APIsec**, uygulama programlama arayüzleri (API’ler) üzerinde güvenlik testleri gerçekleştirmek için kullanılan güçlü ve kapsamlı bir otomatik güvenlik test framework’üdür. Hem dahili hem de harici API’lerin güvenlik açıklarını bulmak ve raporlamak amacıyla geliştirilmiştir. Özellikle modern uygulamaların REST, GraphQL ve SOAP tabanlı API’lerini hedef alır.

Kurumsal API güvenliği için tasarlanan bu araç, zafiyet taraması, saldırı simülasyonu ve uyumluluk kontrolleri gibi birçok özelliği entegre biçimde sunar.

**Bu aracın özellikleri nelerdir?**

**Otomatik API Zafiyet Tespiti:** SSRF, IDOR, Broken Auth, XSS, SQLi gibi yaygın API açıklarını tarar.

**Swagger/OpenAPI Desteği:** API tanımlarını otomatik analiz eder.

**Blackbox ve Greybox Test:** Hem kaynak kodsuz (blackbox) hem oturum bilgili (greybox) testler yapılabilir.

**Raporlama:** OWASP API Top 10’a göre zafiyet raporları üretir.

**Saldırı Simülasyonu:** Gerçek saldırı senaryolarını test ortamında simüle edebilir.

**CI/CD Entegrasyonu:** Otomasyon hatlarına entegre edilebilir.

**Kapsamlı Loglama:** Tüm istek ve yanıtlar kayıt altına alınır.

**Bu aracı Kali Linux'a kurma ve kullanma adımları:**

**Adım 1: Toolun çalışabilmesi içn python , pip ve git paketlerine ihtiyaç duyar. Öncelikle bu paketleri şu kodu kullanarak indirmek gereklidir**

**“sudo apt update**

**sudo apt install python3 python3-pip git -y”**

**Adım 2: APIsec Kurulumu (PyPI Üzerinden)**

APIsec açık kaynak olarak paylaşılmadığından, benzer araç olan **“API-Security-Scanner”** kurulumu örnek alınabilir ve sonrasında requirements.txt dosyasını da indirmek gereklidir.

“git clone https://github.com/ajinabraham/API-Security-Scanner.git

cd API-Security-Scanner

pip3 install -r requirements.txt”

**Adım 3: Test Edilecek API Tanım Dosyasının Eklenmesi (Swagger/OpenAPI)**

APIsec ve benzeri araçlar, testlerini gerçekleştirebilmek için API’ye ait uç noktaları (**endpoint**), istek yöntemlerini (**GET, POST, PUT, DELETE**) ve parametre yapılarını bilmelidir. Bu bilgiler genellikle **Swagger (OpenAPI)** tanım dosyalarında yer alır.

Bu tanım dosyaları .json veya .yaml uzantılı olabilir.

İdeal olarak api.json adında bir dosya aşağıdaki gibi görünmelidir:

**metin, ekran görüntüsü, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu**

**Adım 4: API Testinin Başlatılması**

**“python3 apiscan.py -f api.json -o output.html” kodu ile başlat.**

* -f: Test edilecek Swagger tanım dosyası
* -o: Raporun HTML çıktısı

Komut çalıştırıldığında araç testleri başlatır, bulunan zafiyetleri analiz eder ve çıktı olarak okunabilir bir HTML raporu oluşturur.

metin, ekran görüntüsü, ekran, görüntüleme, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu