**AttackForge**, sızma testi (penetration testing) projelerinin daha etkili, merkezi ve ekip bazlı yürütülmesini sağlayan **web tabanlı bir platformdur**. Test sürecinin planlanmasından raporlamaya kadar olan tüm aşamaları yönetmeye yardımcı olur. Genellikle kırmızı takım (red team) ve danışmanlık ekipleri tarafından tercih edilir.

AttackForge, test sürecini takip etmeyi kolaylaştıran, müşterilerle iletişimi merkezi hale getiren, bulguları yapılandırılmış şekilde raporlayan ve iş birliğini artıran güçlü bir araçtır.

**Bu aracın özellikleri nelerdir?**

**Merkezi Raporlama**: Tüm güvenlik açıklarını merkezi bir yerden raporlamanızı sağlar.

**Proje ve Test Planı Yönetimi**: Hedef sistemler, test adımları, tarihler ve sorumlular tanımlanabilir.

**Ekip İçi İşbirliği**: Aynı anda birden fazla güvenlik uzmanı aynı proje üzerinde çalışabilir.

**Müşteri Portali**: Test süreci hakkında müşterilere şeffaf bilgi akışı sağlar.

**API Desteği**: Otomasyon sistemleriyle kolay entegrasyon için REST API sağlar.

**Kendi Sunucuna Kurulum**: Bulut servisi veya on-premise (kendi sistemine) kurulum seçeneği mevcuttur.

**Entegre Word/PDF Raporlama**: Bulgular tek tuşla dışa aktarılabilir.

**Aktif Geliştirici Topluluğu**: GitHub üzerinden aktif olarak güncellenir ve destek alabilirsiniz.

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

**Adım 1: Gerekli Bağımlılıkları Kurun**

Docker ve Node.js bu araç için temel gereksinimlerdir.

“sudo apt install git curl docker.io docker-compose nodejs npm -y”

**Adım 2: AttackForge’u Klonlayın**

Bu komut, AttackForge’un API tabanlı açık kaynak kodlarını Github üzerinden sisteminize klonlar.

**“git clone https://github.com/AttackForge/attackforge-api.git**

**cd attackforge-api”**

**Adım 3: Yapılandırma Dosyasını Oluşturun**

Proje klasörü içinde .env adında bir yapılandırma dosyası oluşturun veya örnek .env.example dosyasını kopyalayın:

“cp .env.example .env”

Ardından bu .env dosyasını bir metin düzenleyiciyle açarak veritabanı, port ve e-posta ayarlarını yapın:

“nano .env”

Port ayarı

AttackForge’un hangi port üzerinden çalışacağını burada belirlersin. Örnek satır:

“PORT=8080”

SMTP (E-posta) Ayarları

AttackForge, şifre sıfırlama, proje bildirimi gibi işlemler için e-posta gönderir. Bunun için SMTP bilgilerini girmelisin. Örnek:

metin, yazı tipi, ekran görüntüsü içeren bir resim

Açıklama otomatik olarak oluşturuldu

**Adım 4: Docker Konteynerlerini Başlatın**

“sudo docker-compose up –build”

Bu komut ile:

* PostgreSQL veritabanı
* Node.js tabanlı API sunucusu
* Diğer servisler (örneğin mail, servis proxy)

otomatik olarak ayağa kaldırılır.

**Adım 5: Web Arayüzüne Erişin**

Docker konteynerleri başlatıldıktan sonra, web tarayıcınızdan şu adresle erişebilirsiniz:

“<http://localhost:8080>”

Varsayılan olarak gelen kullanıcı bilgileri terminalde görüntülenir veya .env dosyasına göre oluşturulur.

Örnek Terminal çıktısı :

metin, yazı tipi, ekran görüntüsü içeren bir resim

Açıklama otomatik olarak oluşturuldu