**SQLMap Nedir?**

SQLMap, otomatikleştirilmiş bir SQL enjeksiyon (SQL injection) aracıdır. Açık kaynak kodludur ve Python ile yazılmıştır. Temel amacı, web uygulamalarındaki veri tabanı açıklıklarını tespit etmek ve bu açıklıkları istismar ederek veri tabanına erişim sağlamaktır. SQLMap, birçok farklı veritabanı yönetim sistemi (DBMS) ile uyumlu çalışabilir. MySQL, Oracle, PostgreSQL, Microsoft SQL Server, SQLite ve daha fazlasını destekler.

SQL enjeksiyonu, kötü niyetli kullanıcıların veri tabanına doğrudan müdahale etmesini sağlayan tehlikeli bir güvenlik açığıdır. SQLMap, bu açığı tespit etmekle kalmaz, aynı zamanda saldırganların neler yapabileceğini de test eder. Bu özelliğiyle hem saldırı hem de savunma tarafında kullanılabilir; güvenlik uzmanları bu aracı sistemlerini test etmek için kullanırken, saldırganlar istismar amacıyla kullanabilir.

**Özellikleri**

SQLMap, aşağıdaki gelişmiş özellikleriyle dikkat çeker:

* **Veritabanı Tanıma:** Hedef sistemde hangi veritabanı yönetim sisteminin (DBMS) kullanıldığını otomatik olarak tespit edebilir.
* **Veritabanı Sürümünü Öğrenme:** DBMS sürüm bilgisini çıkarabilir.
* **Veritabanı Yapısını Gösterme:** Hangi veritabanlarının, tabloların ve sütunların mevcut olduğunu listeleyebilir.
* **Veri Çekme:** Belirli tablolar veya sütunlardan veri çekebilir.
* **Kabuk Erişimi:** Uygun koşullarda sistem kabuğuna erişim sağlayabilir (örneğin --os-shell gibi seçeneklerle).
* **Şifre Kırma:** Hashlenmiş şifreleri bulabilir ve parola kırma araçlarıyla çözebilir.

**Temel Kullanımı**

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.**

Bu komut, verilen URL üzerindeki “id” parametresinde SQL enjeksiyon açıklığı olup olmadığını test eder.  
Bazı yaygın SQLMap seçenekleri şunlardır:

* --dbs: Sunucudaki veritabanlarını listeler.
* --tables -D <veritabani>: Belirli bir veritabanındaki tabloları listeler.
* --columns -D <veritabani> -T <tablo>: Belirli bir tablonun sütunlarını gösterir.
* --dump: Belirli bir sütunun içeriğini veritabanından çeker.
* --os-shell: İşletim sistemi kabuğu açmaya çalışır.
* --passwords: Tespit edilen kullanıcı parolalarını gösterir.
* --level ve --risk: Test derinliği ve risk seviyesini ayarlamak için kullanılır (1–5 arası).

**SQLMap ile Güvenlik Testi**

SQLMap sadece saldırı aracı değildir. Beyaz şapkalı güvenlik uzmanları (etik hackerlar) SQLMap'i kullanarak uygulama testleri (pentest) yapar ve sistem açıklarını önceden tespit edip kapatırlar. Güvenli yazılım geliştirme sürecinde SQLMap gibi araçlarla düzenli testler yapılması, potansiyel tehditlere karşı koruma sağlar.

Ayrıca geliştiriciler için SQLMap kullanımı, güvenlik farkındalığı açısından oldukça önemlidir. Çünkü uygulamanızın ne kadar savunmasız olabileceğini bu araçla görüp gerekli önlemleri alabilirsiniz.

**SQLMap’in Avantajları**

* Otomatikleştirilmiş saldırı mekanizması sayesinde kullanıcıdan çok az bilgi gerektirir.
* Çok sayıda veritabanı ve işletim sistemi ile uyumludur.
* Açık kaynak olması nedeniyle geliştirilmeye açıktır.
* Detaylı çıktı ve log sistemi sayesinde saldırı süreci takip edilebilir.

**Dikkat Edilmesi Gerekenler**

SQLMap, güçlü ve tehlikeli bir araçtır. Yetkisiz sistemlerde kullanılması **kanunen suçtur**. Sadece kendi sisteminizde ya da izin aldığınız sistemlerde etik testler amacıyla kullanılmalıdır. Aksi takdirde ciddi cezai sonuçlarla karşılaşabilirsiniz.