SQL Injection

SQL enjeksiyonu veritabanınızı yok edebilecek bir kod enjeksiyon tekniğidir.

SQL enjeksiyonu en yaygın web korsanlığı tekniklerinden biridir.

SQL enjeksiyonu, web sayfası girişi aracılığıyla SQL ifadelerinin içine kötü amaçlı kod yerleştirilmesidir.

Web Sayfalarında SQL

SQL enjeksiyonu genellikle bir kullanıcıdan kullanıcı adı/kullanıcı kimliği gibi bir girdi istediğinizde ve kullanıcı size bir ad/kimlik yerine farkında olmadan veritabanınızda çalıştıracağınız bir SQL ifadesi verdiğinde gerçekleşir.

Örneğin, bir bilgisayar korsan "1=1" gibi her zaman doğru ola ifadeleri kullanarak bir uygulamadan veri almak için SQL enjeksiyonu gerçekleştirebilir. Bu ifade he zaman doğru olduğundan, sorgu dizesi bir tablonun ayrıntılarını içeren bir yanıt döndürecektir.

Bilgisayar korsanları ayrıca “105; DROP TABLE Supplier” gibi noktalı virgüllerle ayrılmış bir dizi SQL deyiminin kullanıldığı Batched SQL enjeksiyonunu da kullanabilir. Burada noktalı virgülden sonraki ifade uygulama veri tabanından tedarikçi tablosunu silecektir.

Nasıl Önlenir

1. Parametrelendirilmiş sorgular içeren hazır deyimler: Dinamik SQL sorguları yerine statik SQL sorguları kullanarak, veri ve kod arasında ayrım yaparak SQL enjeksiyonlarını önleyin.
2. Saklı yordamlar: SQL sorgularını parametrelendirilmiş olarak oluşturan ve saklayan saklı yordamlar kullanın, ancak dinamik sorgulardan kaçının.
3. Girdi doğrulama: Kötü niyetli girdileri engellemek için sadece onaylanmış girdileri kabul eden izin listesi doğrulamasını tercih edin.
4. En az ayrıcalık ilkesi: Uygulama hesaplarına sadece gerekli erişim izinlerini vererek, potansiyel saldırılardan kaynaklanabilecek hasarı en aza indirin.