- SQL İNJECTİON
- CVE
- NVD

DUYGU KAÇAR

İçindekiler

SQL İnjection

SQL injection, bir saldırganın bir web uygulamasının veri tabanına kötü niyetli SQL sorguları enjekte ederek, yetkisiz veri erişimi sağlamasına veya veri tabanını manipüle etmesine olanak tanıyan bir güvenlik açığıdır. Bu tür saldırılar, özellikle kullanıcı girişlerinin doğrudan SQL sorgularına dahil edildiği durumlarda ortaya çıkar.

SQL injection saldırıları, aşağıdaki amaçlarla gerçekleştirilebilir:

1. **Veri Hırsızlığı**: Saldırgan, veri tabanındaki hassas bilgilere erişebilir (örneğin, kullanıcı adları, şifreler, kredi kartı bilgileri).
2. **Veri Manipülasyonu**: Saldırgan, veri tabanındaki verileri değiştirebilir veya silebilir.
3. **Yetkisiz Giriş**: Saldırgan, kullanıcı kimlik doğrulamasını atlayarak yetkisiz erişim elde edebilir.
4. **Veri Tabanı Yapısını Öğrenme**: Saldırgan, veri tabanının yapısını öğrenerek daha hedefli saldırılar gerçekleştirebilir.

SQL Injection Nasıl Gerçekleşir?

SQL injection, genellikle aşağıdaki adımlarla gerçekleştirilir:

1. **Girdi Alanlarının Manipülasyonu**: Saldırgan, web uygulamasında kullanıcıdan veri girişi alan form alanları, URL parametreleri veya HTTP başlıkları gibi yerleri kullanarak kötü niyetli SQL ifadeleri ekler.
2. **SQL Sorgularının Değiştirilmesi**: Kullanıcı girdisi doğrudan SQL sorgusuna dahil edildiğinde, saldırganın sağladığı kötü niyetli kod, sorgunun bir parçası haline gelir ve veri tabanında istenmeyen işlemler gerçekleştirilir.

Bir web uygulaması, kullanıcı adı ve şifre ile giriş yapılmasını sağlar. Kullanıcı adı ve şifreyi kontrol etmek için aşağıdaki SQL sorgusunu kullanmaktadır:

- SELECT * FROM users WHERE username = 'user' AND password = 'password';

Güvenlik Açığı

Bu sorgu, kullanıcıdan alınan giriş bilgilerini doğrudan sorguya dahil etmektedir. Eğer kullanıcı girişi uygun şekilde doğrulanmaz veya filtrelenmezse, kötü niyetli bir kullanıcı bu durumu istismar edebilir.

Bir örnek üzerinden gidersek eğer;

Bir saldırgan, kullanıcı adı alanına şu girdiyi sağlar:

- ' OR '1'='1

Ve şifre alanına herhangi bir değer girer (örneğin password):

Bu durumda, SQL sorgusu şu şekilde oluşur:

- SELECT * FROM users WHERE username = '' OR '1'='1' AND password = 'anything';

Sonuç

Bu sorguda, `username = ''` kısmı boş bir kullanıcı adı kontrol ederken, `OR '1'='1'` kısmı her zaman doğru olan bir ifade olduğundan, şifre ne olursa olsun sorgu her zaman true döner. Bu nedenle, saldırgan veri tabanındaki tüm kullanıcılara erişebilir.

Çözüm

Bu tür güvenlik açıklarını önlemek için birkaç yöntem kullanabilirsiniz:

1. **Parametrik Sorgular ve Hazır İfadeler (Prepared Statements)**: Parametrik sorgular, kullanıcı girdilerini doğrudan sorguya dahil etmek yerine parametreler kullanarak SQL injection riskini azaltır.

Örneğin, PHP ve MySQL kullanarak hazırlanan bir sorgu:

php

```
$stmt = $pdo->prepare('SELECT * FROM users WHERE username = :username AND password = :password');

$stmt->execute(['username' => $username, 'password' => $password]);

$user = $stmt->fetch();
```

2. **Girdi Doğrulama ve Temizleme**: Kullanıcı girdilerini doğrulamak ve temizlemek, kötü niyetli kodların enjekte edilmesini engeller.
3. **ORM Kullanımı**: ORM (Object-Relational Mapping) araçları, SQL sorgularını otomatik olarak oluşturur ve SQL injection riskini azaltır.
4. **SQL Injection Önleme Kütüphaneleri**: SQL injection'ı önlemeye yardımcı olan çeşitli güvenlik kütüphaneleri ve araçları kullanmak.

SQL injection, web uygulamalarında yaygın ve tehlikeli bir güvenlik açığıdır. Doğru güvenlik önlemleri alındığında, bu tür saldırılar etkili bir şekilde önlenebilir.

Common Vulnerability and Exposures (CVE)

Common Vulnerabilities and Exposures (CVE), yazılım ve donanım sistemlerindeki bilinen güvenlik açıklarını tanımlamak ve bu açıkları standart bir biçimde adlandırmak amacıyla kullanılan bir sistemdir. CVE, güvenlik açıkları hakkında bilgi paylaşımını ve karşılaştırılmasını kolaylaştırmak için tasarlanmıştır. Her bir CVE girdisi, belirli bir güvenlik açığını tanımlayan benzersiz bir kimlik numarasına sahiptir.

CVE Sistemi Nasıl Çalışır?

1. **CVE Tanımlayıcısı (ID)**: Her güvenlik açığı, CVE sisteminde benzersiz bir kimlik numarası ile tanımlanır (örneğin, CVE-2021-34527). Bu kimlik numarası, belirli bir güvenlik açığını referans almak için kullanılır.
2. **Tanım**: Her CVE girdisi, güvenlik açığının kısa ve öz bir tanımını içerir.

3. **Referanslar**: CVE girdisi, güvenlik açığı hakkında daha fazla bilgi sağlayan belgeler ve raporlara bağlantılar içerebilir.
4. **Yayınlanma**: CVE girdileri, güvenlik açığını belirleyen ve bildiren çeşitli kuruluşlar ve güvenlik uzmanları tarafından düzenli olarak güncellenir.

National Vulnerability Database (NVD)

National Vulnerability Database (NVD), ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından yönetilen, güvenlik açıkları ve bunların etkileri hakkında kapsamlı bilgi sağlayan bir veri tabanıdır. NVD, CVE (Common Vulnerabilities and Exposures) girişlerine dayalı olarak güvenlik açıkları hakkında genişletilmiş veri ve analizler sunar.

NVD'nin Temel Bileşenleri ve İşlevleri

1. **CVE Veritabanı ile Entegrasyon**: NVD, CVE girişlerini alır ve bu girişler hakkında daha ayrıntılı bilgiler sunar. CVE'nin sağladığı temel tanımlamalara ek olarak, NVD güvenlik açıklarının nasıl çalıştığını, potansiyel etkilerini ve nasıl düzeltileceğini açıklar.
2. **CVSS Puanlaması (Common Vulnerability Scoring System)**: NVD, güvenlik açıklarının ciddiyetini değerlendirmek için CVSS puanları sağlar. CVSS, güvenlik açığının potansiyel etkisini ve istismar edilebilirliğini değerlendirir ve 0 ile 10 arasında bir puan verir. Bu puanlama sistemi, kuruluşların güvenlik açıklarını önceliklendirmelerine yardımcı olur.
3. **Güvenlik Açığı Türleri ve Sınıflandırma**: NVD, güvenlik açıklarını farklı kategorilere ve türlere göre sınıflandırır. Bu sınıflandırma, kullanıcıların belirli türdeki güvenlik açıklarını daha kolay bulmasını sağlar.
4. **Yamaları ve Çözümleri İzleme**: NVD, güvenlik açıkları için mevcut olan yamalar ve çözüm yolları hakkında bilgi sağlar. Bu bilgilser, sistem yöneticilerinin güvenlik açıklarını hızlı bir şekilde düzeltmesine yardımcı olur.
5. **Güncellemeler ve Bildirimler**: NVD, güvenlik açıkları hakkında düzenli olarak güncellemeler ve bildirimler yayınlar. Bu, güvenlik uzmanlarının ve kuruluşların en son tehditler ve güvenlik açıkları hakkında bilgi sahibi olmasını sağlar.

NVD'nin Kullanım Alanları

- **Sistem Yöneticileri**: Sistemlerindeki güvenlik açıklarını belirlemek ve düzeltmek için NVD'yi kullanır.
- **Güvenlik Araştırmacıları**: Güvenlik açıklarını analiz etmek ve yeni açıklar keşfetmek için NVD'den faydalanır.
- **Geliştiriciler**: Yazılımlarındaki potansiyel güvenlik açıklarını anlamak ve güvenlik önlemleri geliştirmek için NVD'yi referans alır.
- **Risk Yönetimi Uzmanları**: Kuruluşların güvenlik risklerini değerlendirmek ve önceliklendirmek için NVD verilerini kullanır.

NVD'nin Önemi

NVD, siber güvenlik dünyasında kritik bir kaynak olarak kabul edilir. Güvenlik açıkları hakkında sağladığı ayrıntılı bilgiler ve analizler, kuruluşların güvenlik açıklarını etkin bir şekilde yönetmesine ve siber güvenlik stratejilerini geliştirmesine yardımcı olur. Ayrıca, NVD'nin sağladığı CVSS puanlaması ve sınıflandırma sistemi, güvenlik açıklarının ciddiyetini ve potansiyel etkilerini daha iyi anlamaya yardımcı olur, böylece kuruluşlar daha etkili güvenlik önlemleri alabilir.