**SQL injection**

Az SQL injection egy gyakori biztonsági rés, amely akkor keletkezik, amikor egy alkalmazás nem megfelelően kezeli a felhasználói bemeneteket az SQL lekérdezésekben. Íme egy egyszerű példa, amely bemutatja, hogyan működik az SQL injection, és miért veszélyes.

**Példa egy sebezhető SQL lekérdezésre:**

Képzeljük el, hogy van egy egyszerű bejelentkezési rendszer, amely a felhasználónevet és a jelszót ellenőrzi egy adatbázisban. Az alábbi kód egy sérülékeny változata ennek:

<?php

$username = $\_POST['username'];

$password = $\_POST['password'];

// SQL lekérdezés, amely sérülékeny az SQL injection-re

$query = "SELECT \* FROM users WHERE username = '$username' AND password = '$password'";

$result = mysqli\_query($conn, $query);

Ebben a példában a $\_POST['username'] és $\_POST['password'] értékei közvetlenül beillesztésre kerülnek az SQL lekérdezésbe anélkül, hogy megtisztítanánk vagy ellenőriznénk őket.

**SQL Injection támadásra példa:**

Egy rosszindulatú felhasználó megpróbálhatja kihasználni ezt a sebezhetőséget úgy, hogy a következőket adja meg a username és password mezőkben:

* **Felhasználónév**: ' OR '1'='1
* **Jelszó**: nem számít

Ez a bemenet az alábbi SQL lekérdezést eredményezi:

SELECT \* FROM users WHERE username = '' OR '1'='1' AND password = 'nem számít';

Ebben a lekérdezésben a username = '' OR '1'='1' kifejezés mindig igaz lesz, így az SQL szerver minden felhasználót visszaadhat, lehetővé téve a bejelentkezést érvényes hitelesítés nélkül.

**Védekezés SQL Injection ellen:**

A legjobb védekezési mód az előkészített (prepared) lekérdezések használata, amely megakadályozza az SQL injection támadásokat azáltal, hogy elkülöníti a kódot a bemeneti adatokról.

<?php

$query = "SELECT \* FROM users WHERE username = ? AND password = ?";

$stmt = mysqli\_prepare($conn, $query);

mysqli\_stmt\_bind\_param($stmt, "ss", $username, $password);

mysqli\_stmt\_execute($stmt);

$result = mysqli\_stmt\_get\_result($stmt);

Ezzel a megközelítéssel a username és password paraméterek megfelelően kezelve lesznek, megakadályozva a káros SQL kód befecskendezését a lekérdezésbe.