Mi az az SQL injection?

Az SQL injection egy olyan típusú támadás, amely során egy támadó rosszindulatú SQL kódot injektál egy alkalmazás vagy weboldal bemeneti mezőibe.

Az SQL injection támadás során a támadó általában arra próbál rávenni egy alkalmazást, hogy futtasson olyan SQL lekérdezéseket, amelyeket az alkalmazás fejlesztője nem tervezett vagy nem védekezett ellenük megfelelően. Ennek eredményeként a támadó képes lehet manipulálni az adatbázis lekérdezéseit, hozzáférni, módosítani vagy törölni az adatokat, vagy akár más károkat okozni.

Például, ha egy weboldalon van egy bejelentkezési űrlap, és a felhasználó nevét és jelszavát egy adatbázis lekérdezésben használják fel az azonosításhoz, egy támadó olyan értékeket adhat meg a bejelentkezési mezőkben, amelyek miatt az alkalmazás hibás SQL lekérdezést hajt végre. Ha az alkalmazás nem kezeli megfelelően ezeket az értékeket, a támadó által beszúrt SQL kód futtathatóvá válik.

Miért fontos ismerni?

Az SQL injection az egyik leggyakoribb módszer, amellyel támadók az alkalmazásokat megcélozhatják. A megfelelő védekezési módszerek alkalmazása elengedhetetlen az alkalmazásbiztonság és az adatvédelem szempontjából.

Lehetővé teszi a támadók számára az adatbázis manipulálását és személyes információkhoz való hozzáférést. Ezért fontos az ilyen típusú támadások elleni védekezés és az alkalmazások biztonságos tervezése és fejlesztése.

SQL Injection elleni védekezési módszerek

Védekezhetünk a bemeneten, a felhasználók számára megtilthatjuk az illegális karaktereket, viszont ez nem a legoptimálisabb és nem 100%-os megoldás.

A legoptimálisabb ennek bemutatására egy bejelentkező felület. Egy adott SQL lekérdezés segítségével kikeres egy felhasználónév jelszó párost az adatbázisból.

```
query = "SELECT * FROM login WHERE username='" + username + "' AND
password='" + password + "'"
cursor.execute(query)
result = cursor.fetchall()
```

Az fenti lekérdezés nem védekezik az SQL injection ellen, mert a bemeneti változók (username, password) közvetlenül kerülnek beillesztésre a lekérdezés sztringjébe, anélkül, hogy bármilyen ellenőrzést hajtanának végre rajta.
Ha a felhasználó a felhasználónév és jelszó mezőkbe az alábbi szöveget beilleszti: *' or ''='* a következő lekérdezést kapjuk:

`SELECT * FROM login WHERE username='' or AND password= '' or ''=''`, amely minden esetben igaz.

Az legjobb módszer a paraméterezett/előkészített lekérdezések használata. Ezek a módszerek automatikusan kezelik a bemeneti adatokat és megakadályozzák az SQL kód beinjektálását.
Példa paraméterezett lekérdezésre:

```
query = "SELECT * FROM adatok WHERE felhasznalo = %s AND jelszo = %s"
cursor.execute(query, (username, password))
result = cursor.fetchall()
```