

# SQL-injektio

SQL-injektioilla tarkoitetaan sitä kun SQL-lauseita sisältävään ohjelmakoodiin voidaan injektoida ei-toivottua SQL-toiminnallisuutta. SQL-injektion avulla voidaan mm. tulostaa, muokata tai poistaa enemmän informaatiota kuin ohjelman määrittelyssä oli tarkoituksena.

## Esimerkki 2101: sql-inject.php

Tarkoituksena on näyttää customer-tilusta tietyn asiakkaan tiedot id:n perusteella:

```
1  <?php
2  // sql-inject.php
3  require_once("/home/ara/db-config/db-init.php");
4
5  echo "<code style='background-color: #eeb;'>{$_GET['id']} = {"
6
7  $sql = "SELECT * FROM customer WHERE id = '{$_GET['id']}'";
8  echo "<code style='background-color: #eeb;'>SQL: $sql</code><br>"
9
10
11 $results = $db->query($sql);
12
13
14 echo "<table border='1'>";
15 while($row = $results->fetch(PDO::FETCH_ASSOC)) {
16     echo "<tr><td>{$row['id']}</td><td>{$row['name']}</td></tr>"
17 }
18 echo "</table>";
19
20 ?>
```

Esimerkiksi asiakkaan, jonka id=2, tiedot voidaan hakea kutsumalla em. skriptiä URLilla

```
1 | http://localhost/sql-inject.php?id=2
```

tällöin kysely on muotoa

```
1 | SELECT * FROM customer WHERE id='2'
```

jolloin tulostuu asiakkaan id=2 tiedot.

Mutta jos kysely muotoillaankin:

```
1 | http://localhost/sql-inject.php?id=2'+OR+1+OR+id='1
2 | tai URL-koodattuna
3 | http://localhost/sql-inject.php?id=2%27+OR+1+OR+id%3D%271
```

suoritettava SQL-lause saa muodon

```
1 | SELECT * FROM animals WHERE id='2' OR 1 OR id='1'
```

jolloin näytetään tietueet seuraavien ehtojen perusteella

- id=2 TAI
- 1 (1 on AINA TOSI) TAI
- id=1

**LOPPUTULOS:** Koska keskimmäinen ehto (arvo 1) on aina tosi, näytetään kaikki tietueet. Tämä oli selvästi jotakin enemmän kuin haluttiin näyttää.