# SQL-injektio

SQL-injektiolla 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-taulusta tietyn asiakkaan tiedot id:n perusteella:

```php
<?php
// sql-inject.php
require_once("/home/ara/db-config/db-init.php");

echo "<code style='background-color: #eeb;'>$_GET['id'] = {$_(

$sql = "SELECT * FROM customer WHERE id = '{$_GET['id']}'";
echo "<code style='background-color: #eeb;'>SQL: $sql</code><b


$results = $db->query($sql);


echo "<table border='1'>";
while($row = $results->fetch(PDO::FETCH_ASSOC)) {
  echo "<tr><td>{$row['id']}</td><td>{$row['name']}</td></tr>
}
echo "</table>";

?>
```

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

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

tällöin kysely on muotoa

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

jolloin tulostuu asiakkaan id=2 tiedot.

Mutta jos kysely muotoillaankin:

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

suoritettava SQL-lause saa muodon

```
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.

```
© #AriRantala
```