Index.html

```
<html>
	<head>
		<title>Sql Injection</title>
	</head>
	<body>

		<h3>Example 1 - <em>' OR '' = '</em></h3>
		<h3>Example 2 - <em>x'; INSERT INTO tbl_users(username, password) VALUES
('evilhacker','hello');</em></h3>

		<form action="app.php" method="post">
			<input type="text" placeholder="Username" name="username" size="100" /><br />
			<input type="text" placeholder="Password" name="password" size="100" /><br />
			<input type="submit" />
		</form>

	</body>
</html>
```

App.php

```
<?php

require_once('db.php');

$username = $_POST['username'];

$sql = "SELECT * FROM tbl_users WHERE username = '$username'" ;

echo '<h3>Query</h3>';
echo '<pre>';
echo $sql;
echo '</pre>';

$stmt = $db->prepare($sql);
$stmt->execute();
$result = $stmt->fetchAll(PDO::FETCH_ASSOC);

echo '<h3>Resultaat</h3>';
var_dump($result);

?>
```

Db.php

```
<?php
$db = new PDO('mysql:dbname=sqlinj;host=localhost', 'root', '');
?>
```