# SQL Injection

Created by Dyussembayev Alisher
To professor Grace Kennedy

# Content

What's SQL Injection? And how's it work?

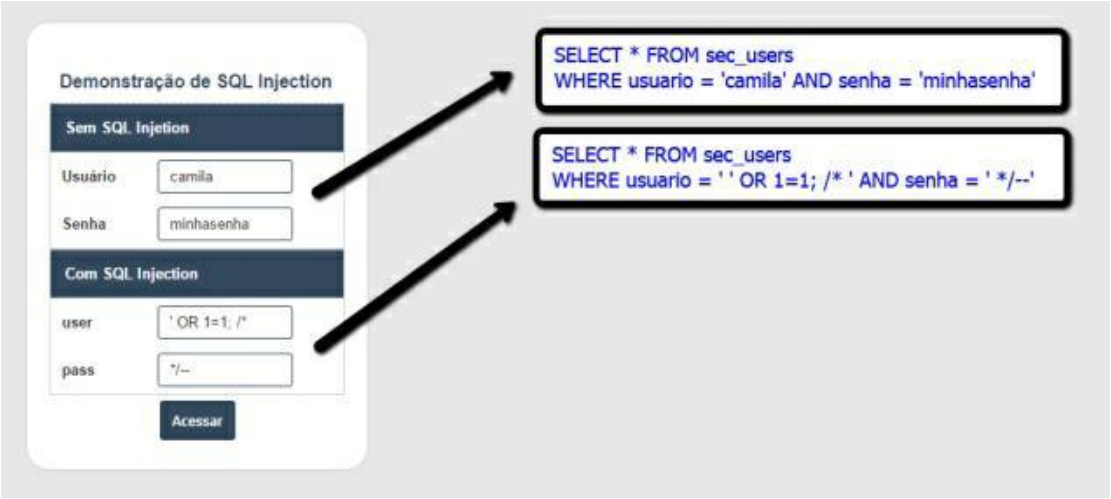
Ways of solving the problems of SQL Injection

Does SSL protect against SQL injection?

Examples of SQL Injection dictionary

# What's SQL Injection? And how's it work?

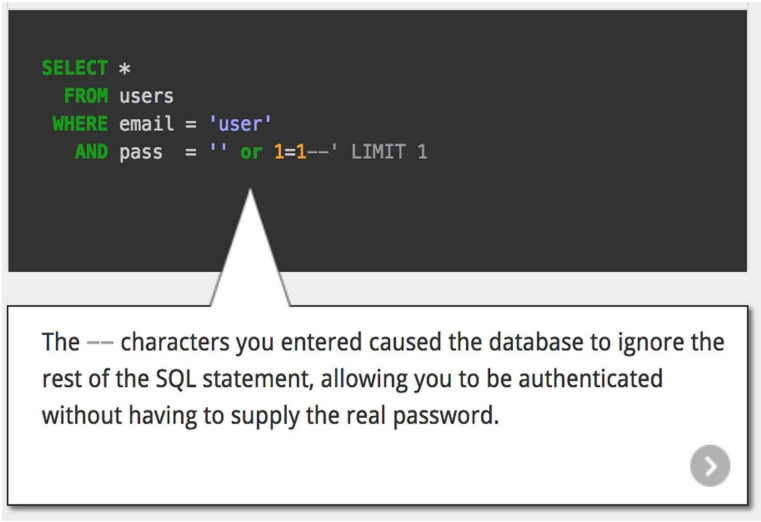
SQL injection (SQLi) is a type of cyberattack against web applications that use SQL databases such as IBM Db2, Oracle, MySQL, and MariaDB. As the name suggests, the attack involves **the injection of malicious SQL statements to interfere with the queries sent by a web application to its database.**



# Ways of solving the problems of SQL Injection

Developers can prevent SQL Injection vulnerabilities in web applications by utilizing parameterized database queries with bound, typed parameters and careful use of parameterized stored procedures in the database.

This can be accomplished in a variety of programming languages including Java, .NET, PHP, and more.



# Does SSL protect against SQL injection?

No, SSL does nothing to prevent SQL injection attacks.

# Examples of attack dictionary

| Parameter mutations |
| --- |
| ” or 1=0 – |
| ” or 1=1 – |
| ” or 1=1 or ””=” |
| ’ or (EXISTS) |
| ’ or uname like ’% |
| ’ or userid like ’% |
| ’ or username like ’% |
| ’ UNION ALL SELECT |
| ’ UNION SELECT |
| char%2839%29%2b%28SELECT |
| char%4039%41%2b%40SELECT |
| " or 1=1 or ""=" |
| ' or ''=' |