SQL INJECTION

Ben Varghese Tharakan - 32135483

WHAT IS SQL INJECTION?

It is a common method of hijacking the database.

It is used to enter malicious code into the SQL statement to manipulate database response.

HOW DOES SQL INJECTION WORK?

When a webpage has user input section, the input is twisted to appear as a SQL statement.

When the user input is accepted by the webpage, the malicious entry by user is passed as SQL command and if the code is recognised by the database, then the user can retrieve important information from the database.

HOW DOES SQL INJECTION WORK?

The following is an example:

Username:

Here, normally, we would enter a username such as ‘admin’ for example.

A user with malicious intent could enter input like: ’ OR ‘1=1’--

When the webpage submits the response, it executes the statement. Since the 1=1 statement is present, the database will return true and will allow the user entry into the system.

HOW TO PREVENT SQL INJECTION?

To prevent SQL injection attacks, instead of making the user input in such a way that a closing inverted comma will act as the end of the input, we can change the user input so that everything inside the textbox is considered as a string.

This will make sure that there is no malicious code run by the application and thereby prevent misuse of the database.