## What is SQL Injection?

SQL injection is a cyber attack that can destroy your database. It is one of the most common website hacking technique in which your sensitive data is exposed to the intruder by exploiting your database. The hacker places a malicious code inside your SQL statement through the web input, and then he has complete access to your site's data.

### What can it do?

If a cyber attack of SQL injection is successful, then your sensitive data is at risk. The hacker can modify your database and perform operations such as insert, update, and delete. Furthermore, he can execute administrative operations such as shut down your database management system. The range of malicious activities does not end here because a hacker can further recover any DBMS content. The worst case is when the hacker can issue commands to your operating system via this cyber attack.

## How Does It Work?

There are many ways to run an SQL injection for a cyber attack. Interestingly, most of these methods are very simple. Some of the most common methods are below:

### The 1=1 Logic

A ubiquitous method of SQL injection is by exploiting the rule of 1=1. If there is no method to stop a user from entering a wrong input, they can manipulate the input data and launch a cyber attack. If the user enters input like *100 OR 1=1* then it will be correct. When this statement of user reaches your code, the ‘OR’ plays the role of a binary operator.

Thus, the statement 1=1 is true, and your database will return true, which will allow the hacker to enter it. It can be dangerous if your database contains passwords of your users or any other sensitive information.

### The Batched SQL Statements

Some developers use batched SQL statements, which refer to a group of SQL statements linked together. In such statements, the result of one database prompts an action to another database. If the hacker smartly puts an input with command to stimulate action to another database then it will be correct.

For instance your batched SQL statement drops table supplier. Then, the user input of *105; DROP TABLE Suppliers* will be valid. Thus, the hacker now has access to your database of supplier.

## Conclusion

SQL injection is a smart and simple way for a hacker to get hold of your database. However, you can prevent your website from a cyber attack of SQL injection by using SQL parameters.