**SQL Injection:-**

SQL injection is a technique for exploiting web application which use client supplied data in SQL queries, but without first stripping potentially harmful characters.

SQL injection can be defined as an attack in which malicious code is embedded in a poorly designed application and then passed to the backend database. The malicious code then produce database query results or action that should never be executed. For example

Consider an application running a bank’s operation. It contains menus that may be used for searching customer details using data points such as social security number of customer. In the background the application calls a SQL query that runs in the database by passing the entered search values, as follows

SELECT client\_name, contact\_no, address, date\_of\_birth WHERE social\_security\_no= 12345

In this sample script user enters 12345 value in the application menu window, requesting the user to enter the social security number. Now by using this value a SQL query runs and interacts with database.

Here comes the malicious way of dealing the database. A user with the knowledge of SQL may understand the working of application, and then he may not enter single value in field of social security number, instead he enters a string “12345 or 1=1” which is passed to the database as follows

SELECT client\_name, contact\_no, address, date\_of\_birth WHERE social\_security\_no=12345 or 1=1.

Here where clause creates vulnerability. In a database the condition 1=1 is always true, and because the query has been specified to return social security number of client or WHERE 1=1, the query will return all rows in the table, which was not the original intension. And to prevent such attack in above mentioned example the application can be changed to accept only one numeric value.

**Detection Techniques:-**

Now a days various tools are also available to detect SQL injection attack possibility in an application. Sqlmap is one of the widely used tool for the purpose.

**SQLMAP: -** It is an open source penetration testing tool which is used to detect and exploit the SQL injection flaws and taking over the database server. It comes with a powerful detection engine and many niche features for ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to access the underlying file system and executing commands on the operating system.

Other than this acunetix, pangolin, wpoison, URL scan 3.0, Microsoft source code analyzer for SQL injection, HP scrawlr are the various tools which can be used to detect the SQL injection vulnerability, if present.

**Prevention Methods: -**

Mitigation of SQL injection vulnerability would be taking one of the two paths i.e. either using stored procedures along with callable statements or using prepared statements with dynamic SQL commands. Whichever way is adopted the data validation is must.

1. **Input Validation:** - Proper validation of the user submitted data should be done and any special/escape characters should be discarded from the search term or the URL.
2. **Use of prepared statements:** - Use a Prepared Statement to send precompiled SQL statements with one or more parameters. Parameter place holders in a prepared statement are represented by the? And are called bind variables. Prepared statement are generally immune to SQL Injection attacks as the database will use the value of the bind variable exclusively and not interpret the contents of the variable in any way.
3. **Use minimum privileges:** - Make sure that application user has specific bare minimum rights on the database server. If the application uses ROOT/SA/dbadmin/dbo on the database then it needs to be reconsidered. If an attacker gets access with the database user privileges than it can crash the whole database server rather than a single database if it has the root access.
4. **Stored Procedures:** - All SQL statements required by the application should be in stored procedures and kept on the database server. The application should execute the stored procedures using a safe interface such as Callable statements of JDBC or CommandObject of ADO.