SQL Injection

An SQL injection is a type of cyber-attack in which a hacker uses a piece of SQL (Structured Query Language) code to manipulate a database and gain access to potentially valuable information. ... Prime examples include notable attacks against Sony Pictures and Microsoft among others.

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.

Using SQL injection, a hacker will try to enter a specifically crafted SQL commands into a form field instead of the expected information. The intent is to secure a response from the database that will help the hacker understand the database construction, such as table names.

Steps for SQL Injection Attack

Following are some steps for SQL injection attack:

1. The attacker looks for the webpages that allow submitting data, that is, login page, search page, feedback, etc.

2. To check the source code of any website, right click on the webpage and click on “view source” (if you are using IE – Internet Explorer) – source code is displayed in the notepad. The attacker checks the source code of the HTML, and look for “FORM” tag in theHTML code. Everything between the

<FORM< and </FORM> have potential parameters that might be useful to find the vulnerabilities.

<FORM action=Search/search.asp method=post>

<input type=hidden name=A value=C></FORM>

3. The attacker inputs a single quote under the text box provided on the webpage to accept the user- name and password. This checks whether the user-input variable is sanitized or interpreted literally by the server.

4. The attacker uses SQL commands such as SELECT statement command to retrieve data from the database or INSERT statement to add information to the database

Blind SQL Injection

Blind SQL injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker. The page with the vulnerability may not be the one that displays data.

Using SQL injections, attackers can:

1. Obtain some basic information if the purpose of the attack is reconnaissance.
2. May gain access to the database by obtaining username and their password.
3. Add new data to the database.
4. Modify data currently in the database

Tools used for SQL Server penetration

1. AppDetectivePro
2. DbProtect
3. Database Scanner
4. SQLPoke
5. NGSSQLCrack
6. Microsoft SQL Server Fingerprint (MSSQLFP) Tool

How to Prevent SQL Injection Attacks

SQL injection attacks occur due to poor website administration and coding. The following steps can be taken to prevent SQL injection.

1. Input validation
2. Modify error reports
3. Other preventions