SQL Injection (Issue and it's countermeasure)

What is SQL Injection?

SQL injection is one of the most common web attack mechanisms utilized by attackers to steal sensitive data from organizations. While SQL Injection can affect any data-driven application that uses a SQL database, it is most often used to attack websites.

SQL Injection is a code injection technique that hackers can use to insert malicious SQL statements into input fields for execution by the underlying SQL database. This technique is made possible because of improper coding of vulnerable web applications.

These flaws arise because entry fields made available for user input unexpectedly allow SQL statements to go through and query the database directly.

Issues - Yu, Yazhi

01

Code injection technique that is the most common security issue plaguing many web applications in the past (and present!).

An attacker is able to execute their own malicious SQL statement against the web application should a vulnerability be exploited.

Easy to exploit when applications are reliant on user input data which is used in conjunction with an SQL database.

02

SQL injection usually occurs when you ask a user for input, like their username/userid, and instead of a name/id, the user gives you an SQL statement that you will unknowingly run on your database.Example:

txtUserId = getRequestString("UserId");

txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId,;

the SQL statement will look like this:

SELECT * FROM Users WHERE UserId = 105 OR 1=1;

Above we made WHERE always true, so WHERE in this query has no effect.

Countermeasure - Miji, Yimeng

01

Don't use dynamic SQL when it can be avoided

Apply patches and updates

Consider a web application firewall (WAF) – either software or appliance based

02

Preventing SQL Injections with JPA

Working with Passwords-Password Hashing/salting

Sanitizing and validating the input field

Thank you.