Sql Injection

What is sql Injection?

Sql injection is a web-based vulnerability which allows the user to submit queries which interfaces with the data base. This grants access to information that is otherwise hidden to the user. This includes data which could belong to users or data which that application has access to.

If SQL injection is successful, then the user could remove or edit entries within the database itself. Most attacks recently have been due to sql injection resulting in some major damage and even fines. If the sql injection is not resolved and fixed, then it could be used as a backdoor into the server which the database is on and could cause major damage.[1]

How to sql Inject

Injecting sql into a program is very easy. Say we have a program where we can search through the data base for a specific user, this is how we would do it:  
txtUsrId = getRequestString(“UsrId”)

searchSql = “SELECT \* FROM Users WHERE UserId = ” + txtUsrId;

This command allows us to enter in a user ID and it will search everything inside the Users table until it finds the given user. If instead of entering in the user ID of a user e.g., “Usr30005218”, we enter in a quire such as “5214 OR 1=1” This will then make the statement:

“SELECT \* FROM Users WHERE UserId = 5214 OR 1=1”

As 1=1 is true this results in every user being displayed within the program with all their private information. This is however the most basic way of sql injection.

Another way sql injection can occur is via the “=” operand. This occurs if you have a login screen where the user needs to enter in their username and password. If you enter in your details into the representative textboxes this is what the code would look like:  
UsrName = getRequestString(“Tb\_Username”);

UsrPassword = getRequestString(“Tb\_Password”);

“SELECT \* FROM Users WHERE Name= +”UsrName” + AND Pass=+ ”UsrPass”+”

Normally entering in your details here would either grant you access to your account or display an error message, but if you instead include the “=” operand then just like the example above all the account details will be displayed to the user.

Both problems we will be facing within our program and will need to create some code to prevent this from occurring. [2]

How to prevent sql injection

Prevent a sql injection attack is rarther simple to do. It can be as easy as writing a fiew lines of code to applying additional programs to work all together: Here are some ways that we will be trying to reduce Sql attacks on our program.

One way we can reduce sql injections attack sis reducing the amount of access points. When constructing our program, we should only have the amount of sql interactions needed for our program to run. If we have to many then this could be a sign of weakness and could be abused. We could also reduce the number of text boxes for user input so that the user has less limited area to attack.

Using a variety of hard coding and dynamic sql commands reduces the about of possible sql injection attacks. The main area for sql injection is via the user input so if we reduce the need for user input and have pre-generated queries, this results in less ways off attacks. Of cause the program could not run properly if everything is hard coded so having a variety of both is a good procedure.

One of the main ways is having code which catches the sql attack attempt. This can be done by many ways. As we are using SQLite it comes with a pre generated function called “string sqlite\_escape\_string()”. This function will escape any query being made if it detects any characters which are deemed special via SQLite.[3][4]

References

1.PortSwigger *SQL Injection.* Available at: <https://portswigger.net/web-security/sql-injection> (Accessed at:26/01/20201)

2.w3schools *SQL Injection.* Available at: <https://www.w3schools.com/sql/sql_injection.asp> (Accessed at:26/01/2021)

3.Rubens, P. (2018) *How to Prevent SQL Injection Attacks* Available at: <https://www.esecurityplanet.com/threats/how-to-prevent-sql-injection-attacks/> (Accessed at: 27/01/2021)

4.tutorialspoint *SQLite – Injection.* Available at <https://www.tutorialspoint.com/sqlite/sqlite_injection.htm> (Accessed at: 27/01/2021)