Cyber Sapiens Internship Task 12

SQL Injection

What is SQL?

SQL is a domain-specific language used in programming and designed for managing data held in a relational database management system, or for stream processing in a relational data stream management system.

RDBMS is the basis for SQL, and for all modern database systems such as MS SQL Server, IBM DB2, Oracle, MySQL, and Microsoft Access.

The data in RDBMS is stored in database objects called tables. A table is a collection of related data entries and it consists of columns and rows.

Some of The Most Important SQL Commands

1. **Data Definition Language**

   DDL changes the structure of the table like creating a table, deleting a table, altering a table, etc. All the command of DDL are auto-committed that means it permanently save all the changes in the database.

   - **CREATE :** It is used to create a new table in the database.
   - **DROP :** it is used to delete both the structure and record stored in the table.
   - **ALTER :** It is used to alter the structure of the database. This change could be either to modify the characteristics of an existing attribute or probably to add a new attribute.
   - **TRUNCATE :** It is used to delete all the rows from the table and free the space containing the table.

2. **Data Manipution Language**

   - **INSERT :** The INSERT statement is a SQL query. It is used to insert data into the row of a table.
   - **UPDATE :** This command is used to update or modify the value of a column in the table.
   - **DELETE :** It is used to remove one or more row from a table.

3. **Data Control Language**

- **GRANT :** It is used to give user access privileges to a database.
- **REVOKE :** It is used to take back permissions from the user.

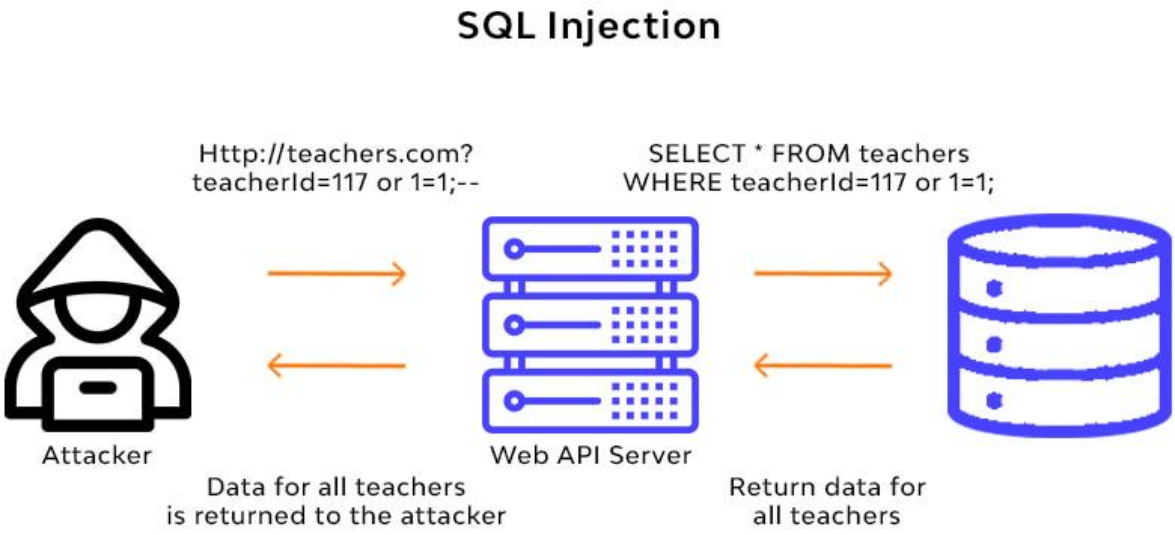
4. **Transaction Control Language**

- **COMMIT :** Commit command is used to save all the transactions to the database.
- **ROLLBACK :** Rollback command is used to undo transactions that have not already been saved to the database.
- **SAVEPOINT :** It is used to roll the transaction back to a certain point without rolling back the entire transaction.

What is SQL Injection Attack?

SQL injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

In some situations, an attacker can escalate an SQL injection attack to compromise the underlying server or other back-end infrastructure, or perform a denial-of-service attack.



Types of SQL-Injection :

1. **In-band SQL Injection:**

   In-band SQL Injection is the most common and easy-to-exploit of SQL Injection attacks. In-band SQL Injection occurs when an attacker is able to use the same communication channel to both launch the attack and gather results.

   The two most common types of in-band SQL Injection are Error-based SQLi and Union-based SQLi.

   a) **Error-based SQLi :**

   Error-based SQL injection is an In-band injection technique that enables threat actors to exploit error output from the database to manipulate its data. It manipulates the database into generating an error that informs the actor of the database's structure.

   b) **Union-based SQLi :**

   Union based SQL injection allows an attacker to extract information from the database by extending the results returned by the original query. The Union operator can only be used if the original/new queries have the same structure (number and data type of columns).

   SELECT a, b FROM table1 UNION SELECT c, d FROM table2

2. **Inferential SQL Injection :**

   Inferential SQL injection is also commonly known as blind SQL injection; it is referred to as so because, in this case, the data is not actually transferred between the web application and the attacker is not able to directly see the response of the injected queries.

a. Time-based SQLi:

Here, attackers send a SQL query to the database, making the database wait (in seconds) before it finally responds to the query as true or false**.**

If an attacker performs the above aquery, the response comes out 15s late, after executing sleep command. Hence, he can confirm that the query is executing in the background.

b. Boolean SQLi:

Here, attackers send a SQL query to the database, letting the application respond by generating either a true or false result.

3. Out-of-band SQLi:

This type of attack is executed under two circumstances—when attackers can't use the same channel to launch the attack as well as gather information or when a server is either very slow or unstable to perform these actions.

What is the impact of SQLI?

- A successful SQL injection attack can result in unauthorized access to sensitive data, such as passwords, credit card details, or personal user information.
- Many high-profile data breaches in recent years have been the result of SQL injection attacks, leading to reputational damage and regulatory fines.
- Some rare cases of SQL injection leads to remote code execution, which is a critical vulnerability.

How to prevent it?

➔ Use parameterized queries.

➔ Least privilege user.

➔ Avoid using shared database accounts.

➔ Perform input validation.

➔ Utilize a WAF preventing Injection.

References

https://www.w3schools.com/sql/sql_intro.asp
https://www.sqlcourse.com/beginner-course/what-is-sql/

https://portswigger.net/web-security/sql-injection

https://www.acunetix.com/websitesecurity/sql-injection2/