Title	WHAT IS SQL INJECTION AND HOW SHOULD WE PREVENT IT?
Description	Intro
Date	2022 20 Augus
Author	Arashtad
Author URI	https://Arashtad.com

The SQL injection attack involves manipulating backend databases with malicious SQL code in order to gain access to information that wasn't meant to be displayed. This information includes sensitive company data, user lists, and private customer information. A successful SQL injection can have a far-reaching impact on a business. In some cases, an attacker may gain administrative rights to a database if they successfully view user lists, delete entire tables, or gain access to entire databases. These things are highly detrimental to a company. If personal information, such as phone numbers, addresses, and credit card numbers, is stolen, it can result in the loss of customer trust. SQLi can be used to attack any SQL database, but websites tend to be the most common targets.

HOW DO WE QUERY FROM SQL?

A SQL query is a query that executes commands, such as retrieving data, updating records, and removing records. SQL is a standardized language for accessing and manipulating databases; We use it to build personalized data views for each user. And execute these tasks by different SQL elements, for example, queries implementing the SELECT statement to retrieve data according to user-provided parameters. Generally, We query data from a database as below:

```
SELECT CustomerName, CustomerEmail
FROM Customer
WHERE CustomerNumber = CustomerNumber
```

From this, the web application builds a string query that is sent to the database as a single SQL statement:

```
sql_query= "
SELECT CustomerName, CustomerEmail
FROM Customer
WHERE CustomerNumber = " & Request.QueryString("CustomerID")
```

A user-provided input http://www.ShoppingCenter.com/customer/customers.asp?customerid=78 can then generate the following SQL query:

```
SELECT CustomerName, CustomerEmail
FROM Customer
WHERE CustomerNumber = 78
```

As you can see from the code, this query provides the name and email of customer number 78.

DIFFERENT KINDS OF SQL INJECTION:

You can classify SQL injections based on their methods of accessing backend data and their damage potential. There are three types of SQL injections: In-band SQLi (Classic), Inferential SQLi (Blind), and Out-of-band SQLi.

IN-BAND SQLI

An SQLi attack that uses the same channel of communication for both launching and gathering results is called an in-band SQLi attack, which is simple and efficient. It has two subvariations:

ERROR-BASED SQLI

A database attack occurs when the attacker causes it to produce error messages. The attacker can potentially use the data provided by these errors to gather information about the database structure. The attacker can alter the SQL commands by exploiting incorrectly filtered characters, including semicolons which we use in order to separate two fields. The below example illustrates how the attacker can delete the entire user database:

```
SELECT ItemName, CustomerEmail
FROM Customers
WHERE CustomerNumber = 78; DROP TABLE USERS
```

As you can see the semicolon creates an error, resulting in the execution of the DROP TABLE USERS command.

UNION-BASED SQLI

In this technique, the attacker uses the UNION SQL operator to assemble multiple select statements generated by the database into a single HTTP response. The response may contain data that can be exploited. UNION SELECT statement combines two unrelated SELECT queries to retrieve data from different database tables. You can the example below:

```
SELECT CustomerName, CustomerEmail
FROM Customers
WHERE CustomerID = '78' UNION SELECT Username, Password FROM Users;
```

This query makes use of the UNION SELECT statement to combine the name and email of customer 78 with names and passwords for all users.

INFERENTIAL (BLIND) SQLI

In order to understand the server's structure, the attacker sends data payloads to it and observes its behavior and response. Due to the fact that the website database transfers no data to the attacker, the attacker cannot see information about the attack in-band. As a result of their reliance on the response or behavior of the server, blind SQL injections are typically slower to execute but may be equally damaging. Blind SQL injections can be any one of the following types:

BOOLEAN:

In boolean SQLi, The attacker sends a SQL query to the database, asking the application to return a result. Depending on whether the query is true or false, the information within the HTTP response will change or remain unchanged. By analyzing the response, the attacker can determine whether it generated a true or false result.

TIME-BASED:

In a time-based SQLi, As the attacker sends a SQL query to the database, the database waits (for a period of a few seconds) before it can respond. The attacker can determine whether a query is true or false by the time the database takes to respond. If the message returned true or false, an HTTP response will be generated instantly or after a waiting period. Therefore, the attacker does not need to rely on database data.

OUT-OF-BAND SQLI:

An attacker can only conduct this type of attack if certain features of the database server used by the web application are enabled. this form of attack is primarily used to replace in-band and inferential SQLi attacks. When the attacker is unable to use the same channel to launch the attack and gather information, or when the server is too slow or unstable for this to take place, out-of-band SQLi is used. These techniques rely on the server’s ability to create DNS or HTTP requests to transfer data to an attacker.

HOW TO PREVENT SQL INJECTION ATTACKS:

The first step in preventing SQLI attacks is input validation (or sanitization), which is the process of writing code that detects illegitimate inputs. Though input validation is always a good practice, it is rarely foolproof. The reality is that, in most cases, it is simply not feasible to map out all legal and illegal inputs-at least not without causing a large number of false positives, which interfere with the user experience and the functionality of the application.

It is for this reason that web application firewalls (WAFs) are commonly used to block SQLI attacks and other online threats. To perform this task, a WAF typically relies on a large, and constantly updated, list of meticulously crafted signatures that allow it to surgically weed out malicious SQL queries. The signatures in such a list usually address specific attack vectors, and they are regularly patched so that newly discovered vulnerabilities can be blocked. Additionally, modern web application firewalls often integrate with other security solutions. These firewalls do this by allowing them to receive additional information that will further enhance their security.

WRAPPING UP:

In this article, you got familiar with one of the most important subjects in web security and SQL-based databases known as SQLi (SQL Injection). Furthermore, you learned about the different types of SQL Injection attacks with some examples for some of them. In the end, we talked about the ways you can follow to prevent these attacks.

FOLLOW US