**OWASP – A03: 2021 Injection**

## **Description:**

Injection is an OWASP vulnerability which involves an attacker submitting an untrusted input string to a program/website which modifies the commands being delivered to an interpreter.

## **Impact of exposure:**

A successful attacker may carry out the following actions on an exploited target:

* Bypass authentication,
* Steal, modify, corrupt or delete data,
* Run shady code,
* Gain root access to the system

## **Priority/Severity:**

Applications often aim to inject their shady code into databases. SQL injections have the capability to be extremely harmful to any company or person if they are successfully carried out. It may be very difficult to fully recover after sensitive data has been compromised.

## **How it works:**

The most common example of injection is an SQL injection. Wherever you have a login field or a potential search field for items, it is most likely that it uses some SQL code. Some of that code isn’t secure and because of that, we can insert a string such as:  
“injecting’ OR ‘StaffID’ = 1 OR 1 =’”  
Which ends up becoming (The example below is from my own test database):  
“SELECT \* FROM ‘customer’ WHERE ‘StaffUsername’ = ‘injecting’ OR ‘StaffID’ = 1 OR 1 = ‘ ’ AND ‘StaffPassword’ = ‘password’”  
By passing a ‘ in the staff username field we can modify the query itself and by adding an OR we are able to execute additional conditions without having all of them to be true.

## **Pre/Post refactored code:**

Because the user input is combined with the query directly, the following code is vulnerable to an SQL injection:  
String query = "SELECT \* FROM products WHERE category = '"+ input + "'";  
Statement statement = connection.createStatement();  
ResultSet resultSet = statement.executeQuery(query);

This code may be quickly changed to prevent user input from interfering with the structure of the query into:  
PreparedStatement statement = connection.prepareStatement("SELECT \* FROM products WHERE category = ?");  
statement.setString(1, input);  
ResultSet resultSet = statement.executeQuery();

## **Examples of injection in the past:**

A Hacker has gained access to the app store database and Learning Lodge of Vtech, a company that specialized in electronic toys and educational material for children. Vtech said that on the 14th of November 2022, there was “unauthorized access” to the database using an SQL injection. A large volume of data that appeared to have come from the attack has been seen online but ended up being concealed. Sensitive information such as names, surnames, dates of birth and even address information also appeared to have been included.

## **References:**

https://owasp.org/www-community/Injection\_Theory/  
https://www.acunetix.com/blog/articles/injection-attacks/  
https://www.rapid7.com/fundamentals/sql-injection-attacks/  
https://portswigger.net/web-security/sql-injection/  
https://www.bbc.com/news/technology-34944140/