**SARA HACHECHE 5672186**

1/

The SQL injection is a new technique used by a category of people and this operation risks destroying our data bases it is used for piracy and hacking .

2/4 examples of sql injection:

1/

SELECT ItemName, ItemDescription  
FROM Items  
WHERE ItemNumber = 999 OR 1=1

this code means that it is an attacker who executed an sql injection to exploit non-validated entries in the database and the 1=1 statement is always true, the query returns all product names and descriptions in the database, even those that you may not have permission to access.

<https://www.imperva.com/learn/application-security/sql-injection-sqli/>

2/

SELECT ItemName, ItemDescription  
FROM Items  
WHERE ItemID = '999' UNION SELECT Username, Password FROM Users;

the union and select request means that this person is trained to try to combine the request for the name and the description of the element mentioned in the request

<https://www.imperva.com/learn/application-security/sql-injection-sqli/>

3/

sql = "SELECT id FROM users WHERE username='" + user + "' AND password='" + pass + "'"

it is an attacker who bypasses the authentication of an application to obtain access such as username and passwords

<https://brightsec.com/blog/sql-injection-attack/>

4/

SELECT id, firstname, lastname FROM authors

the latter is a simple user-based sql injection attack the hacher uses a formulaire that requires the firstname and lastname

<https://brightsec.com/blog/sql-injection-attack/>

3/

sql injection attacks represent a great danger for the cyberecuitre and indeed there are solutions to avoid not being hacked

\_ Using prepared statements and parameterized queries : means that the developer when he uses queries for his work he must define the entire SQL code, then pass each parameter as the attacker can never modify.

\_ Using Stored Procedures: the developer must define SQL statements using parameters stored in the database this technique is an alternative to the use of prepared statements, it can help us in our work and this method is effective.

\_ Using Input Validation in the Allow List: when the developer is making these requests he can define an expected value, such as the authorized name of a table or a column, doing this method an unapproved user cannot add or modify anything.

\_ Install the latest software versions and security patches as soon as they are released

\_ companies should avoid using shared accounts to prevent attackers from gaining additional access in the event of an account compromise

\_ companies should avoid sending error messages from the database to the browser because attackers can use some technical details of the database and they can easily attack .

and that's for sure there are still several security measures to protect the database against SQL injection I have quoted a few

[https://www.crowdstrike.fr/cybersecurity-101/sql-injection/#:~:text=Par%20exemple%2C%20les%20mesures%20de,SQL%2C%20puis%20passer%20chaque%20param%C3%A8tre](https://www.crowdstrike.fr/cybersecurity-101/sql-injection/" \l ":~:text=Par%20exemple%2C%20les%20mesures%20de,SQL%2C%20puis%20passer%20chaque%20param%C3%A8tre).

4/ In conclusion

As a software tester, it is very important for me to understand SQL Injection because it is one of the most common and dangerous attacks that can affect the security of an databases. SQL Injection is an attack technique where attackers exploit the slightest flaws in the database of a web application to manipulate SQL queries and obtain unauthorized access to sensitive data or perform unauthorized operations. for the security of databases it is important to carry out security tests to better protect you never know In addition to the tests, it is important to set up a proactive response plan. This ensures that you are able to react adequately in the event of an SQL injection attack.

And it is important for a tester to know sql injection as it helps and contributes to data security

<https://www.ranorex.com/blog/the-importance-of-sql-injection-testing/>