1)Blind Sql injection:
When an attacker executes a successful malicious query, they take control over the database server. This leads to data theft (e.g., credit card numbers).
the case of a Content-based Blind SQL Injection attack, the attacker makes different SQL queries that ask the database TRUE or FALSE questions. Then they analyze differences in responses between TRUE and FALSE statements.

2)Time dealy sql injection:

Time-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the database to wait for a specified amount of time (in seconds) before responding. The response time will indicate to the attacker whether the result of the query is TRUE or FALSE.

3) Boolean sql injection:
Boolean-based SQL injection is a technique that relies on sending an SQL query to the database based on which the technique forces the application to return different results. The result allows an attacker to judge whether the payload used returns true or false.
If an application is vulnerable to SQL injection, it will not return anything, and the attacker will next inject a query with a true condition (1=1). In this time if not true then return false.

4) heavy query sql injection :
For different reasons, it might happen that it is impossible to use time delay functions or procedures in order to achieve a classic time delay injection. In these situations, the best option is to simulate it with a heavy query that will take noticeable time to get executed by the database engine.

5)In band sql injection:
In-band SQL injection is a type of SQL injection where the attacker receives the result as a direct response using the same communication channel. For example, if the attacker performs the attack manually using a web browser, the result of the attack will be displayed in the same web browser. In-band SQL injection is also called classic SQL injection.

6) error based sql injection:
Error-based SQLi is an in-band SQL Injection technique that relies on error messages thrown by the database server to obtain information about the structure of the database.

7)union based sql injection:
Union-based SQLi is an in-band SQL injection technique that leverages the UNION SQL operator to combine the results of two or more SELECT statements into a single result which is then returned as part of the HTTP response.

8)end of line comment injection:
1.After injecting code into a particular field, legitimate code that follows if nullified through usage of end of line comments: SELECT * FROM user WHERE name = 'x' AND userid IS NULL; --'; Comments in a line of code are often denoted by (--), are ignored by the query.A placeholder for a numeric value must be immediately preceded by a minus.

2.There must be a second placeholder for a string value after the first placeholder on the same line.Both parameters must be user controlled.

9)PiggyBacked Query injection:

1.SELECT * FROM customers; TRUNCATE TABLE customers.The server receives, and potentially executes multiple queries.

2.It happens when you do not validate your input. Never ever use dynamic statements embedded in your code, use parametrised queries; always validate your input.

10) system stored sql injection:

1.A system stored sql injection is prepared SQL code that you save.

2.So that code be reused over and over again. So if you have an SQL query that you write over and over again, save it as a stored procedure, and then just call it to execute it.

11) illegal query sql injection:

1. Illegal query sql injection is used to SQL injection on someone else's website is considered illegal.

2.SQL injections are a type of computer attack in which malicious code is inserted into a database in order to gain access to sensitive information..

12)out band sql injection:

Out-of-ba
nd SQL injection (OOB SQLi) is a type of SQL injection where the attacker does not receive a response from the attacked application on the same communication channel but instead is able to cause the application to send data to a remote endpoint that they control.