1.BLIND SQL INJECTIONS:

Blind SQL injection occurs when an application is vulnerable to SQL injection, but its HTTP responses do not contain the results of the relevant SQL query or the details of any database errors. Many techniques such as UNION attacks are not effective with blind SQL injection vulnerabilities.

PREVENTION:

Avoid dynamic SQL queries at all costs and use parameterized queries instead. Parameterized queries are prepared statements that enable you to effectively and robustly mitigate Blind SQL Injections. So, locate all dynamic SQL queries and convert them to parameterized queries.

2.TIME DELAY 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.

PREVENTION:

There are various efficient ways to patch SQL injection attacks from taking place, as well as defending against them. Data that comes from a third-party reference, like user input, should not be trusted and it should be assumed to be malicious in nature.

3.BOOLEAN EXPLOTATED SQL INJECTION:

Boolean-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the application to return a different result depending on whether the query returns a TRUE or FALSE result.

PREVENTION:

Locate all of the dynamically generated SQL queries and convert them to parameterized queries.

4.HEAVY QUERY SQL INJECTION:

A SQL injection (SQLi) is a technique that attackers use to gain unauthorized access to a web application database by adding a string of malicious code to a database query.

5.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.

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. In some cases, error-based SQL injection alone is enough for an attacker to enumerate an entire database.

7.UNIOIN 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 SQL INJECTION:

End of Line Comment: 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.

9.PIGGYBACKED QUERY SQL INJECTION:

An attacker injects additional queries into the original query to extract data, add or modify data, perform denial of service, or execute remote commands.

10.SYSTEM STORED SQL INJECTION:

SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed.

11.ILLEGAL QUERY SQL INJECTION:

SQL injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. This can allow an attacker to view data that they are not normally able to retrieve.

PREVENTION:

input validation and parametrized queries including prepared statements. The application code should never use the input directly. The developer must sanitize all input, not only web form inputs such as login forms. They must remove potential malicious code elements such as single quotes. It is also a good idea to turn off the visibility of database errors on your production sites. Database errors can be used with SQL Injection to gain information about your database.

12.OUT OF BOUND SQL INJECTION:

Out-of-band 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.

PREVENTION:

The only fully effective way to prevent all types of SQLi vulnerabilities in web applications, including out-of-band SQLi, is to use parameterized queries to access SQL databases.