**Blind SQL Injection**

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.

**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.

**Boolean Exploited SQL Injection**

Boolean Exploitation Technique is basically an SQL Injection Exploitation technique where a set of Boolean operations are executed in order to extract juicy information regarding the tables of the database of an web application.

**Heavy query SQL Injection**

HeavyQuery SQL injection is a sophisticated form of SQL injection attack where malicious actors inject malicious SQL queries into an application's input fields. Unlike typical SQL injection attacks, HeavyQuery involves injecting complex and resource-intensive SQL queries designed to overload and exhaust the database server's resources.

**Inband 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.

**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.

**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.

**End of line comment SQL Injection**

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.

**Piggy Backed SQL QUERIES Injection**

An attacker injects additional queries into the original query used by the Grade Central site to add, modify, or delete student accounts.

**System Stored SQL Injection**

System stored SQL injection, also known as second-order SQL injection, is a type of injection attack where the payload is stored within the database itself, often in the form of a stored procedure, function, trigger, or another database object. Unlike traditional SQL injection attacks where the payload is directly injected into the application's input fields, system stored SQL injection involves injecting malicious code into the application's database, which is then executed at a later time when certain conditions are met.

**Illegal Query SQL Injection**

"Illegal query SQL injection" isn't a standard term in the realm of SQL injection attacks. However, it might refer to injecting SQL queries that are syntactically incorrect or unauthorized within an application's input fields in an attempt to exploit vulnerabilities.

**Out of Band 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.