1-**How to prevent SQL injection attacks? Give six prevention techniques**

Answer: In order to prevent SQL injection attacks, which involves injecting SQL code into an open field we have to use security mechanism dedicated to preventing such attack, bellow we can find six techniques that are used for such purposes:

1. **Prepared statements**:

Force the developer to first define all the SQL code, and then pass in each parameter to the query later, so basically all the parameter from the hacker has been passed in is not equal to a value inside the database making it impossible to get processed.

1. **Stored Procedures**:

It requires the developers to build SQL statements that are parameterized.

1. **White listing:**

Only accepting input values that are known to be legit and rejecting all any other values.

1. **Typecasting:**

If a user input is Boolean, number or date then, this data can be converted into a safer form of data before it’s inputted into the query. This will make it so that only a certain type of data is submitted and not a data type that’s used in SQL injections.

1. **Escaping:**

Sanitizing and escaping user input, which will either encode/remover special characters that might allow hackers to miss with the sequel logic. For example: ‘’ , “”

1. **Web Application firewalls (WAFs):**

Implementing a web application firewall that will filter and monitor HTTP traffic between a web Application and the internet, which can detect and block SQL injection attempts.

**2- What types of SQL injections does SQL-map support? Explain**

Answer: SQL map is capable of supporting different types of injections which is what allow pen testers to check for these vulnerabilities in their sites and web applications. Some of the basics/primary types of these injections include:

1. **Classic SQL Injection (Bootlean-based injection)**:

This type of injection is based solely on exploiting Boolean-based conditions in SQL queries. SQLMap can infer the existence of a condition to be true or false just by observing changes in the application's behavior.

1. **Error-Based SQL Injection**:

SQLMap can exploit the error messages that are generated by the database to extract information about the database structure and data itself. By injecting intentionally flawed SQL code, attackers/pen testers can trigger error messages that reveal details about the underlying workings of a database.

1. **Union-Based SQL Injection:**

Union-based injections which involves leveraging the UNION SQL operator to combine the results of two or more SELECT statements. This injections is performed to retrieve information from additional database tables.

1. **Time-Based Blind SQL Injection**:

This type of injection which relies on the delay of the application's response to see the success or failure of a SQL condition, can be perform using SQL map as time-based injections by introducing time-delay functions in the injected SQL code.