SQL Injection

-SQL injection is a type of cyber attack where an attacker exploits vulnerabilities in a web application's database query handling.
-By injecting malicious SQL code into an input field, an attacker can manipulate the SQL query executed by the server.
-This can lead to unauthorized access, data retrieval, modification, or even deletion of database records.

How SQL Injection Works

1. **Input Manipulation**: The attacker provides malicious input, often through web forms, URL parameters, or cookies, that is intended to be included in an SQL query.

2. **Query Modification**: The malicious input alters the structure of the SQL query.

3. **Execution and Damage**: The modified query is executed by the database, leading to various potential consequences:
   Unauthorized Access
   Data Theft
   Data Manipulation
   System Compromise

Types of SQL Injection Attacks

Classic SQL Injection: Directly manipulates the SQL query.

Blind SQL Injection: The attacker can't see the results of the SQL query directly, but can infer information based on the behavior of the application

Union-based SQL Injection: Uses the UNION SQL operator to combine results from multiple queries, allowing attackers to retrieve additional data.

Error-based SQL Injection: Leverages error messages returned by the database to gain information about the database structure and contents.

Preventing SQL Injection

Prepared Statements: Use parameterized queries.

Input Validation: Implement strict validation rules.

Least Privilege: Restrict database user privileges to minimize the impact of a successful injection.

Error Handling: Avoid exposing detailed error messages to users.

Web Application Firewalls (WAF): Deploy WAFs to detect and block malicious SQL injection attempts.