SQL INJECTION INTERVIEW QUESTIONS

1.What is SQL?

Answer: SQL (Structured Query Language) is a standard programming language used to manage and manipulate relational databases. It allows users to query, update, insert, and delete data.

2.What are the main types of SQL statements?

Answer: The main types of SQL statements include Data Query Language (DQL) for retrieving data (e.g., SELECT), Data Manipulation Language (DML) for modifying data (e.g., INSERT, UPDATE, DELETE), Data Definition Language (DDL) for defining database structures (e.g., CREATE, ALTER, DROP), and Data Control Language (DCL) for controlling access to data (e.g., GRANT, REVOKE).

3.What is a primary key in SQL?

Answer: A primary key is a column or a set of columns in a table that uniquely identifies each row in that table. Primary keys must contain unique values and cannot contain NULLs.

4.What is a foreign key in SQL?

Answer: A foreign key is a column or a set of columns in one table that refers to the primary key columns in another table, creating a relationship between the two tables.

5.What is a JOIN in SQL?

Answer: A JOIN is an SQL operation used to combine rows from two or more tables based on a related column between them. Common types of joins include INNER JOIN, LEFT JOIN, RIGHT JOIN, and FULL OUTER JOIN.

6.What is an SQL injection attack?

Answer: SQL injection is a code injection technique where an attacker inserts malicious SQL code into an input field, allowing them to manipulate the database to access, modify, or delete data, or execute administrative operations.

7.How does a basic SQL injection attack work?

Answer: In a basic SQL injection attack, an attacker provides input that includes SQL syntax, which the application mistakenly executes as part of a legitimate query. For example, entering ' OR '1'='1 into a login field might manipulate the SQL query to always return true, bypassing authentication.

8.What are some common types of SQL injection attacks?

Answer: Common types include:

In-band SQLi: Using the same communication channel for injection and retrieval (e.g., error-based or union-based).

Inferential (Blind) SQLi: No direct data retrieval; attackers deduce information by observing responses (e.g., boolean-based or time-based).

Out-of-band SQLi: Using different channels for injection and retrieval (e.g., through DNS or HTTP requests).

9.What is a union-based SQL injection?

Answer: Union-based SQL injection exploits the UNION SQL operator to combine the results of two or more SELECT statements into a single result, allowing attackers to retrieve additional data from other tables.

10.What is an error-based SQL injection?

Answer: Error-based SQL injection leverages error messages returned by the database server to gain insights into the structure of the database and extract sensitive information.

11.What are SQL injection evasion techniques?

Answer: Evasion techniques are methods used by attackers to bypass security measures and evade detection. These techniques include obfuscation, encoding, and using different variations of SQL syntax.

12.What is SQL obfuscation in the context of evasion?

Answer: SQL obfuscation involves modifying the SQL injection payload to evade detection by security mechanisms. This can include using comments, white spaces, and different SQL syntax variations.

13.How can encoding be used as an evasion technique in SQL injection?

Answer: Attackers can encode their payloads using URL encoding, hexadecimal encoding, or other encoding schemes to bypass input filters that only look for specific patterns.

14.What is the purpose of using comment markers in SQL injection evasion?

Answer: Comment markers (e.g., --, /* ... */) can be used to truncate or alter the intended SQL query structure, making it more difficult for security mechanisms to detect the malicious payload.

15.Explain how timing attacks can be used to evade detection in SQL injection.

Answer: Timing attacks (time-based blind SQL injection) involve sending SQL queries that trigger a time delay in the database response, allowing attackers to infer information based on the time it takes to receive a response, evading immediate detection.

16.What are some effective countermeasures against SQL injection attacks?

Answer: Effective countermeasures include using prepared statements (parameterized queries), input validation, stored procedures, ORM frameworks, least privilege principle, and web application firewalls (WAFs).

17.How do prepared statements prevent SQL injection?

Answer: Prepared statements use parameterized queries, separating SQL code from user input. This ensures that user input is treated as data only, not executable SQL code, preventing injection attacks.

18.Why is input validation important in preventing SQL injection?

Answer: Input validation ensures that only properly formatted data is accepted by the application. This helps to reject malicious input that could be used for SQL injection attacks.

19.What role do web application firewalls (WAFs) play in defending against SQL injection?

Answer: WAFs monitor and filter incoming traffic to web applications, blocking malicious requests, including SQL injection attempts, based on predefined security rules and patterns.

20.How can the principle of least privilege help mitigate the impact of SQL injection attacks?

Answer: By ensuring that database accounts have the minimum permissions necessary for their tasks, the principle of least privilege limits the damage an attacker can do if they successfully exploit an SQL injection vulnerability.