SQL injection

1. Brief

2. What is a Database?

3. What is SQL?

SELECT * {col_name} FROM {table} WHERE {condition} LIMIT 2,1;
{condition} → (OR, AND), LIKE 'a%'
SELECT {col_names} FROM {table1} **UNION** SELECT {col_names} FROM {table2};
INSERT INTO {table} ({col_name}, {col_name}) VALUES ('{val_1}', '{val_2}');
UPDATE {table} SET {col_1} = '{val_1}', {col_2} = '{val_2}' WHERE {condition};
DELETE FROM {table} WHERE {condition};
DELETE FROM {table} → Empty the table

4. What is SQL Injection?

Using -- & ; as user input in SQL Statement

5. In-Band SQLi:

- In-Band SQL Injection
- Error-Based SQL Injection
- Union-Based SQL Injection

0 UNION SELECT 1,2,group_concat(name, ':', password) FROM users

6. Blind SQLi - Authentication Bypass:

' OR 1=1;--

7. Blind SQLi - Boolean Based:

Trying Possibilities with LIKE operator until you found a match (return True '1')

8. Blind SQLi - Time Based:

Trying Possibilities with LIKE operator until you found a match (**Delay**)
SLEEP(5) "4961"

9. Out-of-Band SQLi:

1) An attacker makes a request to a website vulnerable to SQLI with an injection payload.
2) The Website makes an SQL query to the database which also passes the hacker's payload.

3) The payload contains a request which forces an HTTP request back to the hacker's machine

10. Remediation:

- Prepared Statements (With Parameterized Queries)
- Input Validation
- Escaping User Input