INTRODUCTION

Learn about the techniques and risks of SQL injection attacks.

N.ARULJOTHI,
2404001,
I-MCA

WHAT IS SQL INJECTION?

❑SQL Injection is a technique where attackers insert malicious SQL commands into input fields (like login forms or search bars) to manipulate the database.

WHY IS IT DANGEROUS ?

- ✓ It allows attackers to view, modify, or delete sensitive data.
- ✓ It can even give attackers control over the entire system.

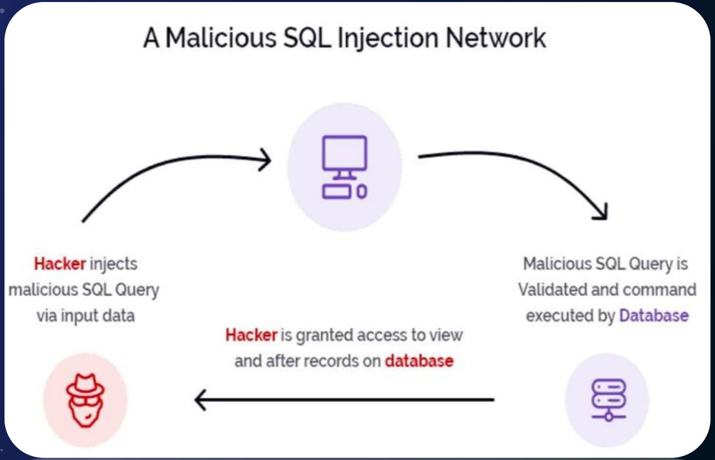
REAL-LIFE ANALOGY:-

Consider a security guard at a building who asks for an ID to grant access.

- An attacker could trick the guard by saying, 'I’m the boss OR let me in.
- ' The guard interprets this as a permission request and allows entry without proper verification.
- Similarly, SQL Injection deceives the database by entering unintended commands that the system then executes, unaware of the malicious intent behind them.

COMMON SQL INJECTION ATTACKS

✓Unauthorized Privilege Escalation
✓Privilege Abuse
✓Denial of Service (DOS)
✓Weak Authentication



A Malicious SQL Injection Network

Hacker injects malicious SQL Query via input data

Malicious SQL Query is Validated and command executed by Database

Hacker is granted access to view and after records on database

SQL INJECTION METHODS

SQL MANIPULATION

- Most common type of injection attack, change an SQL command in the application.
- Changes the SQL query to give unintended results.

Ex:- SELECT * FROM users WHERE username = 'jake' AND password = 'jakepasswd';

Injected Query: SELECT * FROM users WHERE username = 'jake' OR 'x' = 'x';

EXPLANATION:

❑ The OR 'x' = 'x' condition always returns TRUE, allowing the attacker to log in without a password.

❑ The system thinks the condition is satisfied and grants access.

CODE INJECTION

- ❖Injects extra commands into SQL queries to change how they behave.

Example: **SELECT * FROM products WHERE id = 10; DROP TABLE users;**

Explanation: The attacker inserts the DROP TABLE command, deleting the users table.

The system executes both commands, causing irreversible damage.

FUNCTION CALL INJECTION:

- Executes system or custom database functions through SQL queries.
- Example: SELECT TRANSLATE('abc', 'a', 'x') FROM dual;
- Explanation: This replaces the letter a with x in the string.
- Attackers can use similar methods to run dangerous functions that can compromise the system.

CONCLUSIONS

- In summary, understanding SQL Injection and its various types is crucial for safeguarding databases against attacks.
- Organizations must employ best practices in code validation, access controls, and regular security assessments to prevent SQL Injection vulnerabilities and protect sensitive data from malicious actors.

!!!QUIZZ SECTION!!!

What can a Function Call Injection achieve in SQL Injection?

A) Execute built-in database functions or system commands
B) Increase database storage capacity
C) Validate SQL query syntax
D) Create an additional user account

What is the goal of a Code Injection attack in SQL Injection?

A)Add extra conditions to the query
B) Modify the database schema
C) Inject malicious code to execute unauthorized commands
D) Remove duplicate records from the database

What is the primary target of a Denial of Service (DoS) attack using SQL Injection?

A) Web application frontend
B) Network firewall
C) Database server
D) User credentials

Which scenario is an example of privilege escalation through SQL Injection?

A) A guest user deletes their account
B) A user gains admin privileges by modifying the query
C) A user logs out after making changes
D) A guest user accesses public resources

Which of the following is a potential consequence of a successful SQL Injection attack?

A) Unauthorized data access or modification
B) Improved query performance
C) Automatic data backup
D) Reduced database size

What type of database object is usually the target of an SQL Injection attack?

A) Network Firewall
B) SQL Database Tables
C) Web Application Logs
D) Application Cache

In Function Call Injection, what does the attacker exploit?

A) A valid user’s credentials
B) Network firewall configurations
C) The admin’s login panel
D) Vulnerable SQL statements that execute system functions

What does Code Injection allow an attacker to do?

A) Add extra commands to an existing SQL query
B) Prevent login attempts
C) Encrypt database records
D) Modify the database schema

Which method of SQL Injection modifies the SQL query to change its logic?

A) Code Injection
B) SQL Manipulation
C) Function Call Injection
D) DoS Attack

What is the purpose of a Denial of Service (DoS) attack in the context of SQL Injection?

A) To enhance the security of the database
B) To update user privileges to admin
C) To slow down or crash the system by sending excessive requests
D) To modify query results