SQL Injection

- By Pravesh N

- Means Structured Query Language (SQL) is injected as anomalous to the Database.
- It has more types, such as Data Manipulation Language (DML), Data Definition Language (DDL), and Data Control Language (DCL).

SQL types:

1. DML

- used to retrieve/delete, update and insert any data into the database.
- It can violate confidentiality if an attacker uses these methods

(eg, update employees set department='Sales' where first_name='Tobi')

2. DDL

- Used to define a database's schema(overall structure)
- Can do operations like create, alter and drop into the database
- It can violate the integrity of the information if an attacker gains access to these organisations' sensitive resources

3. DCL

- Used to implement access control to the database.
- Can do operations like grant and revoke to change the access or privileges
- It violates both confidentiality and availability of the system.
  (Eg. GRANT SELECT, INSERT, UPDATE, DELETE ON grant_rights TO unauthorized_user;)

SQL injections:

1. "SELECT * FROM users WHERE name = '" + userName + "'"; → it injects the any username given by the client, and will return all the data that contains "appropriate/same name"
   Eg. Smith' OR '1' = '1

results in SELECT * FROM users WHERE name = 'Smith' OR TRUE;
→ it returns all the entries from the table.

Consequences:

- Read and modify the data from the database
- Recover the content and move it to any other location
- Access to grant rights to the table or the logs

Note:

The rest all performed through hands-on tasks!