**ASSIGNMENT – 1**

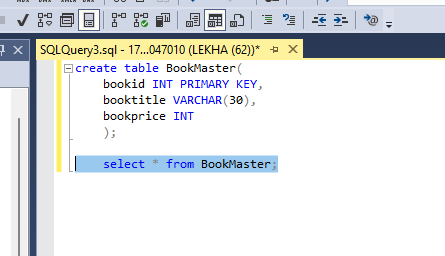
**Name –** Lekha J

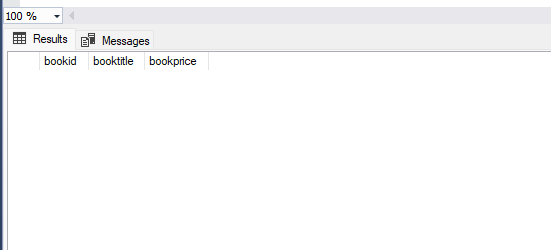
**Roll number –** 231047010

**Objective:** Illustrate the usage of Parameterized Query.

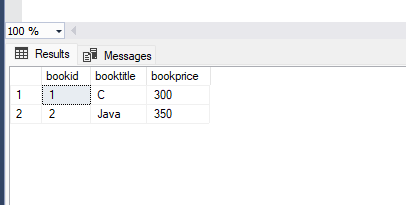
**Problem Statement:** Demonstrate through java program the concept of SQL injection and also illustrate how to avoid that through usage of parameterized query ( prepared statement in java).

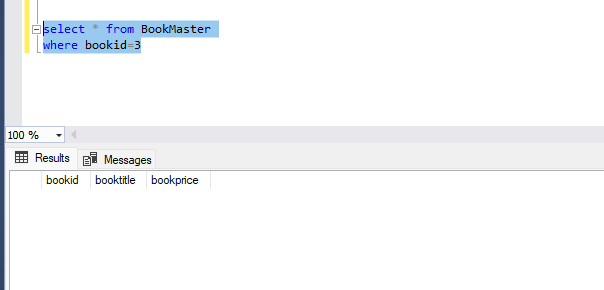
Created a table - BookMaster



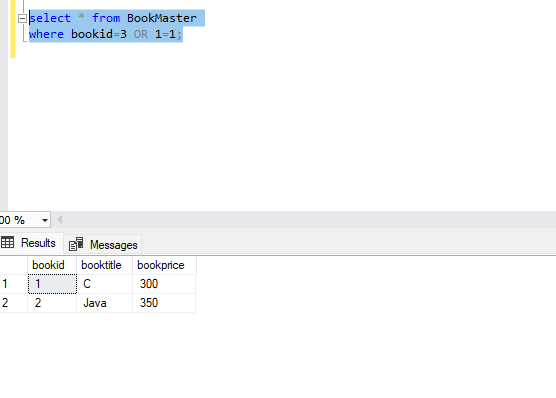


Select \* from BookMaster;





To avoid below SQL Injection parameterized query is used .



**Solution:**

**package** lekha;

**import** java.util.\*;

**import** java.sql.Connection;

**import** java.sql.DriverManager;

**import** java.sql.PreparedStatement;

**public** **class** DayCare {

**private** **static** **final** Connection ***NULL*** = **null**;

**public** **static** **void** main(String args[]) {

Connection con = ***NULL***;

Scanner sc = **new** Scanner(System.***in***);

System.***out***.println("Book Details");

**try** {

String url="jdbc:sqlserver://172.16.51.64;"+" "+"databaseName=231047010;encrypt=true;trustServerCertificate=true";

String username="lekha";

String password="lekha@321";

con=DriverManager.*getConnection*(url,username,password);

System.***out***.println("Connection established");

System.***out***.println("Enter the ID of the book");

**int** word = sc.nextInt();

System.***out***.println("Enter the name of the book");

String name=sc.next();

System.***out***.println("Enter the price");

**int** cost = sc.nextInt();

PreparedStatement stmt = con.prepareStatement("INSERT INTO BookMaster values(?,?,?)");

stmt.setInt(1, word);

stmt.setString(2, name);

stmt.setInt(3, cost);

System.***out***.println("Added succeesfully");

stmt.executeUpdate();

}**catch**(Exception e) {

System.***out***.println("Error Occured");

}

}

}

**OUTPUT:**

