JWTD Lab Assignment-6

SQL Injection

Athul u c

211047022

Main code:

1.lab6.java

**package** lab61;

**import** java.sql.Connection;

**import** java.sql.DriverManager;

**import** java.sql.PreparedStatement;

**import** java.sql.ResultSet;

**import** java.sql.SQLException;

**import** java.sql.Statement;

//import java.sql.Statement;

**public** **class** lab6 {

**public** **static** **void** getConnection(**int** userId, String pswd) {

//Connection initialization

Connection conn = **null**;

**try** {

//Connection parameters

String dbURL1 = "jdbc:sqlserver://LAPTOP-R07JHSTN:1433;databaseName=sqlinjection;encrypt=true;trustServerCertificate=true;";

String user = "athul";

String pass = "athul";

//Getting the connection

conn = DriverManager.*getConnection*(dbURL1, user, pass);

**if** (conn != **null**) {

//Statement Declaration

Statement sta = conn.createStatement();

//ResultSet for Statement

ResultSet rs = sta.executeQuery("select \* from login where user\_ID="+userId+"and passwd='"+pswd+"'" );

//Prepared Statement Declaration

//PreparedStatement sta = conn.prepareStatement("select \* from login where user\_ID = ? and passwd = ?");

//Passing the parameters to the prepared statement

//sta.setInt(1, userId);

//sta.setString(2, pswd);

//ResultSet for Prepared Statement

// ResultSet rs = sta.executeQuery();

**if**(rs.next()) {

//Storing the userName locally

//String USerName = rs.getString("userName");

System.***out***.println("True\nWelcome user");

//break;

} //endif

**else** {

System.***out***.println("Invalid credentials\n");

} //end else

}

} **catch** (SQLException ex) {

ex.printStackTrace();

} **finally** {

**try** {

**if** (conn != **null** && !conn.isClosed()) {

conn.close();

}

} **catch** (SQLException ex) {

ex.printStackTrace();

}

}

}

}

2.injection.java

**package** \_211047022;

**import** java.util.Scanner;

//import sql.impl.\*;

//import sql.op.\*;

**import** lab61.lab6;

**public** **class** injection {

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

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

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

System.***out***.println("Enter UserID\n");

**int** userId = scan.nextInt();

System.***out***.println("Enter Password\n");

String pswd = sc.nextLine();

//System.out.println("Please Wait\n");

lab6.*getConnection*(userId, pswd);

scan.close();

sc.close();

}

}

OUTPUT:

Login with proper credentials

Graphical user interface, text, application

Description automatically generated

Login with invalid credentials

Text

Description automatically generated

SQL injection

Graphical user interface

Description automatically generated with medium confidence

SQL injection with prepared statements

Graphical user interface, text, application

Description automatically generated