Álvaro García Fuentes
Horas Libre Configuración
Desarrollo Aplicaciones Web

UD2 A5 Injection y sentencias parametrizadas

Álvaro García Fuentes
Horas Libre Configuración
Desarrollo Aplicaciones Web

1. **Qué es una SQL Injection. Realiza el ataque en un ejemplo que elimine un alumno por su nombre. Impleméntalo en la clase AtaqueSQLInjection.**
   Inyección SQL es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos.

   Como ejemplo, vamos a ejecutar el siguiente código:

```
import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.ResultSet;
import java.sql.SQLException;
import java.sql.SQLTimeoutException;
import java.sql.Statement;

public class AtaqueSQLInjection {

    public static void main(String[] args) {
        String url = "jdbc:mysql://127.0.0.1:3306/HLC";
        String login = "alvaro";
        String password = "macarrones";
        try {
            Connection conexion = DriverManager.getConnection(url, login, password);

            Statement st = conexion.createStatement();
            ResultSet rs = st.executeQuery("SELECT nombre FROM ALUMNOS");
            System.out.println("tabla ALUMNOS");
            while(rs.next()) {
                String nombre = rs.getString("nombre");
                System.out.println( "Nombre: " + nombre );
            }

            st = conexion.createStatement();
            int nombresEliminados = st.executeUpdate("DELETE FROM ALUMNOS WHERE nombre='fernando' OR 1=1;");
            System.out.println( "Nombres eliminados: " + nombresEliminados );

            st = conexion.createStatement();
            rs = st.executeQuery( "SELECT nombre FROM ALUMNOS" );
            System.out.println("tabla ALUMNOS");
            while(rs.next()) {
                String nombre = rs.getString("nombre");
                System.out.println( "Nombre: " + nombre );
            }


        } catch ( SQLTimeoutException e )    { System.out.print("Error de tiempo de conexion."); }
          catch ( SQLException e )           { e.printStackTrace(); }
          catch ( Exception e )              { e.printStackTrace (); }
    }
}
```

Y vemos la siguiente salida en la terminal:

```
tabla ALUMNOS
Nombre: ana
Nombre: maria
Nombre: pepe
Nombres eliminados: 3
tabla ALUMNOS
```

Álvaro García Fuentes
Horas Libre Configuración
Desarrollo Aplicaciones Web

Como vemos, se han borrado todas las entradas en la tabla alumnos.

2. **Indica cómo solucionar una SQL Injection.**
   Se puede solucionar evitando que se puedan introducir caracteres especiales (como comillas) sin haberlos transformado antes.

3. **PreparedStatement. Indica su utilidad.**
   Es una sentencia sql precompilada y se usa para prevenir sql injection.

4. **Indica alguno de los métodos para asignar los parámetros de las sentencias parametrizadas.**
   setString y setInt.

5. **En todos los métodos para asignar los prámetros setXxx el primer parámetro indica el índice el parámetro de la consulta. Indica el número del primer parámetro, ¿0 ó 1?**

   Los índices de los “set*” comienzan por 1.