PreparedStatements

- + eficiencia + seguridad-

Juan Diego Pérez Jiménez

ÍNDICE DE CONTENIDOS

Juan Diego Pérez Jiménez

RECORDANDO CONCEPTOS

Clase	Descripción
DriverManager	Para cargar un Driver
Connection	Para establecer conexiones con las bases de datos
Statement	Para ejecutar sentencias SQL
PreparedStatement	La ruta de ejecución está predeterminada en el servidor de base de datos lo que le permite ser ejecutado varias veces (parametrizadas)
ResultSet	Para almacenar el resultado de la consulta

PREPARED STATEMENTS

- Otra forma de realizar consultas.
- Compilación Previa (consume recursos inicialmente).
- Posteriormente es más eficiente.
- Parametrizable.
- Evita ataques SLQ Injection.

PREPARED STATEMENTS

1 -Defino la sentencia en una cadena

String sql = “select * from customers where customername= ? and country= ?”;

2 - Creo la PreparedStatement

sentencia = connection.prepareStatement(sql);

PREPARED STATEMENTS

3- Establezco los parámetros (Nombre y País)

```
sentencia.setString(1,"La Rochelle Gifts");
sentencia.setString(2,"France");
```

4 - Ejecuto la consulta

```
ResultSet rs = sentencia.executeQuery();
```

o .executeUpdate() ← Insert/Update/Delete

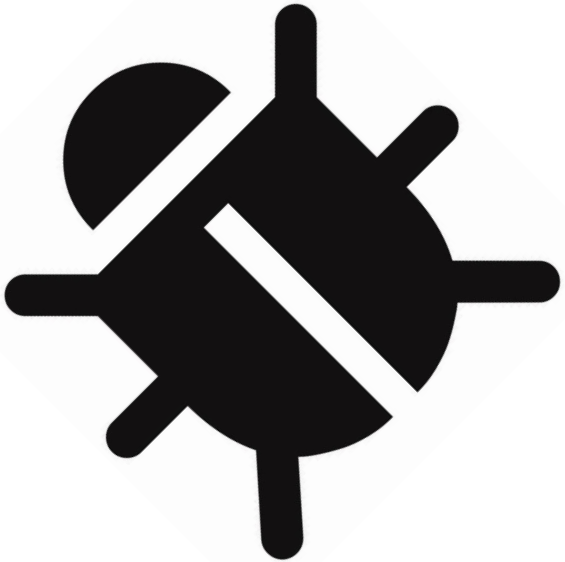
SQL Injection

> 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.

Juan Diego Pérez Jiménez

SQL Injection

where ….. or 1=1;
sql_command1; sql_command2;



El intérprete ejecuta las dos órdenes seguidas. Jugamos con eso a la hora de mandar datos a la aplicación poniendo en segundo lugar alguna orden “maliciosa”.

Juan Diego Pérez Jiménez

EJEMPLO

AVISO

USAD PREPAREDSTATEMENTS

Te evitarás problemas posteriormente

Juan Diego Pérez

END

prof.jdperez@iesalixar.org