prepareStatement对象防止sql注入的方式是**把用户非法输入的单引号用\反斜杠做了转义**，从而达到了防止sql注入的目的

**PreparedStatement是预编译的**,**对于批量处理可以大大提高效率**. **也叫JDBC存储过程**

使用 Statement 对象，在对数据库只执行**一次性存取的时侯**，用 Statement 对象进行处理。**PreparedStatement 对象的开销比Statement大**，对于一次性操作并不会带来额外的好处。

1. String updateString = "UPDATE COFFEES SET SALES = 75 " + "WHERE COF\_NAME LIKE ′Colombian′";
2. stmt.executeUpdate(updateString);

PreparedStatement updateSales = con.prepareStatement("UPDATE COFFEES SET SALES = ? WHERE COF\_NAME LIKE ? ");

updateSales.setInt(1, 75);

1. updateSales.setString(2, "Colombian");
2. updateSales.executeUpdate();