

Prepared Statement Advantages :-

Performance:

- i) SQL query is precompiled once and re-used.
- ii) Faster execution for repeated queries.

Security:

- i) Prevents SQL injection.
- ii) Automatically handles input sanitization.

Comparison :

Statement	Prepared Statement
i) Query compiled every time.	i) Query compiled once
ii) Vulnerable to SQL injection	ii) Secure against SQL injection.
iii) String concatenation is needed	iii) Use placeholders (?) instead of string concatenation.

Example: Insert Record Using Prepared Statement:

```
import java.sql.*;

public class insertExample {
    public static void main(String[] args) {
        try {
            Connection con = DriverManager.getConnection(
                "jdbc:mysql://localhost:3306/testdb", "user", "password");

            String sql = "INSERT INTO student(id, name) VALUES"
                "(?, ?)";

            PreparedStatement ps = con.prepareStatement(sql);

            ps.setInt(1, 101);
            ps.setString(2, "John");
            ps.executeUpdate();
            con.close();
        } catch (SQLException e) {
            System.out.println("Database error: " + e.getMessage());
        }
    }
}
```