

这篇文章仅用于补充：[JAVA代码审计的一些Tips\(附脚本\)](#)一文中关于SQLi中不足部分

JDBC常用API

DriverManager：用于管理JDBC驱动的服务类。主要功能是获取Connection对象

```
public static Connection getConnection(String url, String user, String password) throws SQLException
    //■■■■■url■■■■■
```

Connection：代表数据库连接对象。每一个Connection代表一个物理连接会话

[illegible]

Statement：用于执行SQL语句的工具接口。该对象既可以执行DDL,DCL语句，也可以执行DML语句，还可以用于执行SQL查询

```
ResultSet executeQuery(String sql) throws SQLException;
//■■■■■■■■■■■■■■■■■■■■■ResultSet■■■■■■■■■■■■■■■■■■■■■

int executeUpdate(String sql) throws SQLException;
//■■■■■■■■DML■■■■■■■■■■■■■■■■■■■■■■DDL■■■■■■DDL■■■■■■0

boolean execute(String sql) throws SQLException;
//■■■■■■■■■■■■■■■■■■■■■■sql■■■■■■■■■■■■■■■■■■■■■ResultSet■■■■■■true■■■■■■■■■■■■■■■■■■■■■■false
```

PreparedStatement

：预编译的Statement对象，它允许数据库预编译sql语句，以后每次只改变sql命令的参数，避免数据库每次都需要编译sql语句，无需再传入sql语句，它比Statement多了以下方法

[illegible]

Hibernate框架常用API

Configuration : 负责Hibernate的配置信息。包括运行的底层信息：数据库的URL、用户名、密码、JDBC驱动类，数据库Dialect，数据库连接池等和持久化类与数据表的映射关系(*.hbm.xml文件)

```
//■■■■hibernate.properties■:
Configuration cfg = new Configuration();
//Xml■■■hibernate.cfg.xml■
Configuration cfg = new Configuration().configure();
```

SessionFactory

: Configuration对象根据当前的配置信息生成SessionFactory对象, SessionFactory对象中保存了当前数据库的配置信息和所有映射关系以及预定义的SQL语句, 同时还负责

```
SessionFactory configuration.buildSessionFactory()
    ■■SessionFactory■■
    Session sessionFactory.openSession()
```

Session

[illegible]

```
void commit()
    //■■■■■■■■session■■
void rollback()
    //■■■■■■■■
boolean wasCommitted()
    //■■■■■■■■■■
```

用于从数据源查询对象及控制执行查询的过程，Query对象包装了一个HQL查询语句。Query对象在session对象关闭之前有效，否则会抛出Sessionexception异常

```
Query setxxx()  
    //■■■■■HQL■■■■■  
  
List list()  
    //■■■■■■■■■■■■■■■■■■■■list■■■■  
  
Obect uniqueResult()  
    //■■■■■■■■■■(■■■■■■■■)  
  
int executeUpdate()  
    //■■■■■■■■■■
```

SpringJdbc常用API

[illegible]


```
//Spring Container
RepositoryFactorySupport factory = ... // Instantiate factory here
UserRepository repository = factory.getRepository(UserRepository.class)
```

Repository：是SpringData的核心接口，并不提供任何方法，用户需要自己定义需要的方法

1. public interface UserDao extends Repository<User, Long> { }
2. @RepositoryDefinition(domainClass = User.class, idClass = Long.class)
public interface UserDao { }

点击收藏 | 0 关注 | 1

[上一篇：JAVA代码审计的一些Tips\(附脚本\)](#) [下一篇：LCTF 2017 三道Web题的...](#)

1. 3 条回复



[hello_world](#) 2017-11-22 18:50:28

Heibernate框架的Criteria类没用过，所以暂时留空

0 回复Ta



[cryin](#) 2017-11-23 11:08:59

赞

0 回复Ta



[藏青](#) 2017-11-24 12:33:16

期待大佬下次更新

0 回复Ta

[登录](#) 后跟帖

[先知社区](#)

[现在登录](#)

[热门节点](#)

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)