java代码审计深度解析

第十一课　jdbc-like-修复sql注入

SQL注入-JDBC遇到like-正确写法

当预处理遇到like—正确处理方法

```
public ResultSet gradeList(Connection con,PageBean pageBean,Grade grade)throws Exception{
    StringBuffer sb=new StringBuffer("select * from t_grade");
    int apd = 0;
    if(grade!=null && StringUtil.isNotEmpty(grade.getGradeName())){
        sb.append(" and gradeName like ?");
        apd += 1;
    }
    if(pageBean!=null){
        sb.append(" limit ?,?");
        apd += 2;
    }
    PreparedStatement pstmt=con.prepareStatement(sb.toString().replaceFirst("and", "where"));
    if(apd == 3){
        pstmt.setString(1, "%"+grade.getGradeName()+"%");
        pstmt.setLong(2, pageBean.getStart());
        pstmt.setLong(3, pageBean.getRows());
    }else if(apd == 2){
        pstmt.setLong(1, pageBean.getStart());
        pstmt.setLong(2, pageBean.getRows());
    }else if(apd == 1){
        pstmt.setString(1, "%"+grade.getGradeName()+"%");
    }

    return pstmt.executeQuery();
}
```

谢谢观赏