

# java代码审计 深度解析



# 第五课 jdbc-in-分析sql代码漏洞原因

## SQL注入-JDBC遇到in-不正确写法

当预处理遇到in

```
public int gradeDelete(Connection con,String delIds)throws Exception{  
    String sql="delete from t_grade where id in("+delIds+")";  
    PreparedStatement pstmt=con.prepareStatement(sql);  
    return pstmt.executeUpdate();  
}
```



## SQL注入-JDBC遇到in-正确写法

当预处理遇到in

```
//安全的删除方法
public int gradeDelete(Connection con,String delIds)throws Exception{
    String num = "";
    String[] spl = delIds.split(",");
    for(int i=0;i<spl.length;i++){
        if(i==0){
            num += "?";
        }else{
            num += "?.?";
        }
    }
    String sql = "delete from t_grade where id in("+num+")";
    PreparedStatement pstmt=con.prepareStatement(sql);
    try {
        for(int j=0;j<spl.length;j++){
            pstmt.setInt(j+1,Integer.parseInt(spl[j]));
        }
        return pstmt.executeUpdate();
    } catch (Exception e) {
        // TODO: handle exception
    }

    return 0;
}
```



The image features a central figure of a person wearing a black hoodie, with their right hand pressed against their forehead in a gesture of stress or contemplation. The background is a vibrant blue digital landscape. It includes a glowing globe on the right side, a network of interconnected nodes and lines, and several padlock icons scattered throughout, suggesting themes of cybersecurity or digital privacy. A horizontal semi-transparent bar is positioned across the middle of the image, containing the text.

谢谢观赏