



java代码审计 深度解析

第四课 jdbc-修复sql注入

SQL注入-JDBC不安全的

Statment不能防止sql注入

“+”号直接拼接参数（要溯源参数user对象是否有过滤）

```
//登陆
public User login(Connection con,User user) throws Exception{
    User resultUser=null;
    String sql="select * from t_user where userName='"+user.getUserName()+"' and password='"+user.getPassword()+"'";
    java.sql.Statement stmt = con.createStatement();
    //Statement stmt=con.createStatement();
    ResultSet res = stmt.executeQuery(sql);
    if(res.next()){
        resultUser=new User();
        resultUser.setUserName(res.getString("userName"));
        resultUser.setPassword(res.getString("password"));
    }
    return resultUser;
}
```



SQL注入-JDBC不安全修复方案-预处理

PreparedStatement预处理

```
public User login(Connection con,User user) throws Exception{
    User resultUser=null;
    String sql="select * from t_user where userName=? and password=?";
    PreparedStatement pstmt=con.prepareStatement(sql);
    pstmt.setString(1, user.getUserName());
    pstmt.setString(2, user.getPassword());
    ResultSet rs=pstmt.executeQuery();
    if(rs.next()){
        resultUser=new User();
        resultUser.setUsername(rs.getString("userName"));
        resultUser.setPassword(rs.getString("password"));
    }
    return resultUser;
}
```



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, overlaid with a network of white and blue lines and dots. Scattered throughout the background are several padlock icons, some of which are open, suggesting themes of security, hacking, or digital access. The overall aesthetic is futuristic and tech-oriented.

谢谢观赏