sql注入及常用防护方法计算机等级考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/645/2021_2022_sql_E6_B3_A8_E5_85_A5_E5_c97_645395.htm SQL 注入简介： SQL注入是最常见的攻击方式之一,它不是利用操作系统或其它系统的漏洞来实现攻击的,而是程序员因为没有做好判断,被不法 用户钻了SQL的空子,下面我们先来看下什么是SQL注入: 比如在一个登陆界面,要求用户输入用户名和密码: 用户名: or 1=1 -- 密码: 点登陆,如若没有做特殊处理,而只是一条带条件的查询语句如: String sql="0select * from users where username=" userName " and password=" password " " 那么这个非法用户就很得意的登陆进去了.(当然现在的有些语言的数据库API已经处理了这些问题) 这是为什么呢?我们来看看这条语句,将用户输入的数据替换后得到这样一条语句: 0select * from users where username= or 1=1 -- and password= 为了更明白些，可以将其复制到SQL分析器中，将会发现，这条语句会将数据库的数据全部读出来，为什么呢？ 很简单,看到条件后面 username= or 1=1 用户名等于 或 1=1 那么这个条件一定会成功，然后后面加两个-，这意味着 什么？没错，注释，它将后面的语句注释，让他们不起作用，这样就可以顺利的把数据库中的数据读取出来了。 这还是比较温柔的，如果是执行 0select * from users where username= .DROP Database (DB Name) -- and password= .....其他的您可以自己想象。。。 那么我们怎么来处理这种情况呢？下面我以java为列给大家两种简单的方法： 第一种采用预编译语句集，它内置了处理SQL注入的能力，只要使用它的setString方法传值即可： String sql= "0select * from users where

username=? and password=?. PreparedStatement preState = conn.prepareStatement(sql). preState.setString(1, userName).