著名的SQL流量注入(SQL注入)攻击法 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/353/2021_2022__E8_91_97_E5_90_8D_E7_9A_84S_c97_353591.htm 我们在编程过程中，经常会把用户输入的数据拼成一个SQL语句，然后直接发送给服务器执行，比如：string SqlStr = "0select * from customers where CompanyName Like %" textBox1.Text "%".这样的字符串连接可能会带来灾难性的结果，比如用户在文本框中输入：a or 1=1 --那么SqlStr的内容就是：0select * from customers where CompanyName like %a or 1=1 --%这样，整个customers数据表的所有数据就会被全部检索出来，因为1=1永远true，而且最后的百分号和单引号被短横杠注释掉了。如果用户在文本框中输入：a EXEC sp_addlogin John ,123 EXEC sp_addsrvrolemember John,sysadmin --那么SqlStr的内容就是：0select * from customers where CompanyName like %a EXEC sp_addlogin John,123 EXEC sp_addsrvrolemember John,sysadmin --这个语句是在后台数据库中增加一个用户John，密码123，而且是一个sysadmin账号，相当于sa的权限。如果用户在文本框中输入：a EXEC xp_cmdShell(format c:/y) --运行之后好像是格式化C盘！还有很多更危险的操作，不过都没试过。还是存储过程好用啊，存储过程的参数把用户的输入当成真正的字符串处理，既安全，又快速！ 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com