ASP.NET中如何防范SQL注入式攻击 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/137/2021_2022_ASPNET_E4_B8_AD_c98_137820.htm 一、什么是sql注入式攻击 所谓sql注入式攻击，就是攻击者把sql命令插入到web表单的输入域或页面请求的查询字符串，欺骗服务器执行恶意的sql命令。在某些表单中，用户输入的内容直接用来构造（或者影响）动态sql命令，或作为存储过程的输入参数，这类表单特别容易受到sql注入式攻击。常见的sql注入式攻击过程类如：⑴ 某个asp.net web应用有一个登录页面，这个登录页面控制着用户是否有权访问应用，它要求用户输入一个名称和密码。⑵ 登录页面中输入的内容将直接用来构造动态的sql命令，或者直接用作存储过程的参数。下面是asp.net应用构造查询的一个例子： system.text.stringbuilder query = new system.text.stringbuilder("0select * from users where login = ’ ") .append(txtlogin.text) .append(" ’ and password= ’ ") .append(txtpassword.text).append(" ’ "). ⑶ 攻击者在用户名字和密码输入框中输入" ’ 或 ’ 1 ’ = ’ 1"之类的内容。⑷ 用户输入的内容提交给服务器之后，服务器运行上面的asp.net代码构造出查询用户的sql命令，但由于攻击者输入的内容非常特殊，所以最后得到的sql命令变成： 0select * from users where login = ’ ’ or ’ 1 ’ = ’ 1 ’ and password = ’ ’ or ’ 1 ’ = ’ 1 ’ ⑸ 服务器执行查询或存储过程，将用户输入的身份信息和服务器中保存的身份信息进行对比。⑹ 由于sql命令实际上已被注入式攻击修改，已经不能真正验证用户身份，所以系统会错误地授权给攻击者。 如果攻击者知道应用会将表单中输入的

内容直接用于验证身份的查询，他就会尝试输入某些特殊的sql字符串篡改查询改变其原来的功能，欺骗系统授予访问权限。 系统环境不同，攻击者可能造成的损害也不同，这主要由应用访问数据库的安全权限决定。如果用户的帐户具有管理员或其他比较高级的权限，攻击者就可能对数据库的表执行各种他想要做的操作，包括添加、删除或更新数据，甚至可能直接删除表。 二、如何防范 好在要防止asp.net应用被sql注入式攻击闯入并不是一件特别困难的事情，只要在利用表单输入的内容构造sql命令之前，把所有输入内容过滤一番就可以了。过滤输入内容可以按多种方式进行。 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