IIS、A .NET和SQLServer的安全性问题 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/259/2021_2022_IIS_E3_80_81A_N_c98_259351.htm SQL Server、Internet 信息服务器和 ASP.NET 引擎都提供了坚实可靠的安全模型，它们可以很好地在一起协同工作。为了保证用户数据和应用程序的安全，Microsoft 还为每项服务的默认设置设置了相当低的值。 大多数开发人员面临的挑战是如何使用 SQL Server、IIS 和 ASP.NET 在应用程序和数据之间设置适当的信任级别，而不会留下可被别人轻易攻入的安全漏洞。由于涉及三类服务（SQL Server、IIS 和 ASP.NET），所以需要采取三个关键的步骤来确保解决方案的安全。本部分讨论一种为 Web 应用程序设置足够权限和信任级别的更常用（且可靠）的方法。 定义 DotNetKB 自定义 IIS 用户帐户 保证 Web 应用程序安全性的最安全的方法是定义一个权限有限的自定义用户，然后对 IIS 进行配置，使之能够在执行您的 Web 应用程序时能作为自定义用户运行。这是相当容易实现的，可以确保访问您的 Web 应用程序的每个访问者都只具有您希望他们具有的权限。 第一步是生成一个新的 Windows 用户（本例中称为 DotNetKB），为其设置一个增强型密码，然后将其添加到 Windows 来宾组 (Guest Windows Group) 中。同时，确保选中 Password never expires（密码永不过期）和 User cannot change password（用户不能更改密码）复选框。这样将生成一个权限有限的用户，在 IIS 中运行您的 Web 应用程序时，您可以将其用作标识(参见图 1）。 然后，调用 Internet 信息服务器管理员并选择承载这些网页的 Web 应用程序。在本例中，您

可以选择承载前文所生成的测试页的 Web 应用程序 (DotNetKB_WebSite)。在树视图中的 Web 应用程序上单击鼠标右键，然后从上下文相关菜单中选择 Properties...（属性...）。然后选择 Directory Security（目录安全性）并单击该对话框 Anonymous access and authentication control（匿名访问和验证控制）部分中的 Edit（编辑）按钮。最后，输入自定义用户名 (DotNetKB)，取消选择 Allow IIS to control password（允许 IIS 控制密码）复选框，并输入该自定义用户帐户的密码。完成所有这些工作之后，单击 OK（确定）按钮，将这些更改保存到 IIS 配置数据库中（参见图 2）。 