基于 WWW 的数据库应用

刘东 向卫平 （中国科学院计算机网络信息中心 100080）

摘要：随着信息时代的到来，WWW 越来越受到人们的重视。为了尽可能发挥其作用，非常有必要把数据库技术应用到 WWW 上。本文主要讨论通过何种方式把数据库和 WWW 连接起来，以及如何保证数据库的安全。

关键词：WWW 数据库 CGI HTTP 安全

一、Web 与数据库的连接

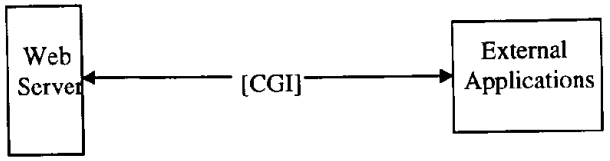
1. 为什么要使用数据库？

在 Web 服务器上，我们可以利用 Web 页面发布各种各样的信息。HTML 语言给我们提供了一个方便的途径。但是如果我们想在 Web 上提供大量的在线信息服务时，单纯的 Web 页面将不能满足这一要求。原因之一是一个 Web 页面可以存储的信息相当有限，其次是它只能提供相对静态的信息而且不便于管理。

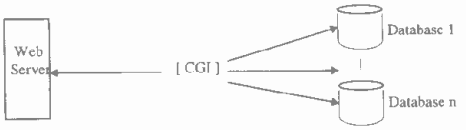
那么，该如何解决这个问题呢？我们知道，数据库具有强大的数据存储和管理能力，并且能够动态地进行数据输入与输出。如果把数据库应用于 Web 上，那么我们不但可以实现大量信息的网上发布，而且能够给客户提供动态的信息查询。正是 WWW 与数据库这两种技术的结合，给予我们解决这个问题，实现全方位信息服务的途径。

2. 公共网关接口（CGI）

公共网关接口（CGI）是 Web 服务器与外部应用程序之间的接口标准。Web 服务器可以通过 HTML 运行 CGI 程序，把数据传给它并取回它的运行结果。这个方法允许用户输入 CGI 程序需要的信息，然后点一个按钮激活程序。CGI 程序对这些信息进行处理，并执行其他一些必要的操作，最后以 HTML 格式或纯文本格式返回结果。Web 服务器接收这些结果后，根据需要进行处理，然后传给用户。与 HTML 文档不同的是，CGI 程序由用户通过请求 Web 服务器实时地执行，可以输出动态的信息。



CGI 程序在 Web 服务器与外部应用之间的交互功能使其能够很好地承担访问数据库的任务。一些数据库厂商提供了许多访问其产品的方法，比如 API、命令行方式等。CGI 的灵活性使其能够使用任何访问方法，甚至能够访问多个服务器上的多个数据库。



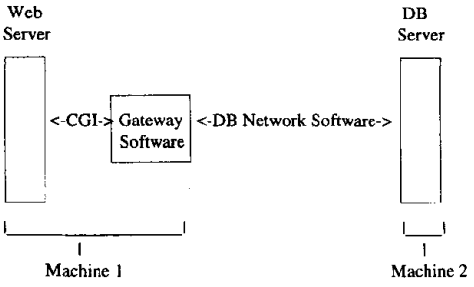
CGI 程序可以用任何语言来编写，只要它能在给定系统环境下运行，比如 C/C++、Fortran、PERL、TCL、Any Unix shell、Visual Basic、AppleScript 等。

3. 访问数据库的方式

前面讨论了 CGI 的概念及其作用，显然它能够实现 Web 与数据库的连接，也是把数据库应用于 Web 上的比较好的解决办法。不过各厂商的数据库产品在功能、访问方式、管理上各有不同，用同一种方式完成与数据库的连接是不可能的。那么，对于不同的数据库，该如何通过 CGI 对其访问呢？下面我们针对不同数据库，讨论应采取的连接方式。

·提供网络功能的数据库

这一类的数据库系统本身具有网络功能，能够通过网络实现对数据库的各种访问如管理、查询等。这样，Web 服务器可以利用数据库的网络软件来连接数据库，如下图所示。



这里，Web 服务器与数据库服务器分别位于不同的机器，数据库的网络软件安装在 Web 服务器一端。Web 服务器通过 CGI 来调用这些网络软件，与数据库交换信息。当然，两个服务器也可放到同一台机器上，但一些数据库的访问软件还是必须提供。比较有代表性的例子是一些具有 Client/Server 结构的数据库系统，它们与 Web 的连接可由 CGI 程序调用数据库的客户端工具来实现。

·没有网络功能的数据库

由于有的数据库没有网络功能，不能直接通过网络访问，Web 服务器需要与数据库系统放在同一机器上，由 CGI 程序直接调用数据库系统的 API 来连接数据库。

·利用第三方的网络软件

除了前面两种情况之外，许多第三方厂商提供了用于某些数据库的网络软件，利用这些软件可实现数据库的网络访问。因此，我们基于这第三方软件同样能够完成 Web 与数据库的连接。

这里，第三方网络软件起了 Web 服务器与数据库之间的连接桥梁作用。这个软件必须能接受通过网络对数据库的查询，把请求提交给数据库服务器，获取结果并传回给 CGI 程序，由 CGI 程序把结果送到 Web 服务器。其中，数据库一端的网络软件要能够通过数据库提供的 API 或其他数据库访问软件直接调用数据库，Web 服务器一端的网络软件能被 CGI 程序访问。

比较好的情况是，第三方网络软件能够访问多个类型的数据库并且有自己的 API，这样，在写 CGI 应用程序时，针对各种数据库，只需要调用一种 API 即可。当需要把多平台上不同类型的数据库集成到 Web 上时，这种方式是非常有用的。

所有这些方式都用到 CGI 网关过程，因而配置 Web 服务器时必须允许访问 CGI 程序。这种访问可以授权给用户，也可以对任何人（包括匿名用户）开放，不过，安全性一定要考虑。

4. **基于 Web 的数据库集成**

我们知道 Web 上大量信息的发布必须依赖数据库，为此，需要依据情况集成各种数据库。根据前面所讲，我们可以采用适当的连接方式，把数据库集成到 Web 上来。具体涉及到一个 Web 服务器与一个数据库、一个 Web 服务器与多个数据库、多个 Web 服务器与多个数据库之间的相连。由于运行于各种平台上的 web 服务器都可以方便地接入 Internet，在此基础上的数据库集成是非常灵活的。

二、Web 上数据库安全措施

Web 服务器是否能处理上百万个通过 Internet 的访问，安全性是考虑的重点。将计算机与 Intranet 连接时，可以与世界各地的人和计算机通信。这种较大的灵活性增加了冒险性－不仅自己可与其他网络上的人通信，而且其他网络上的用户也可与自己的网络开始通信。尽管 Web 服务器之间的互访通常是好的意图，但也有心存不良的人企图侵入内部网络。

尤其当数据库应用到 Web 上时，需要更加注意安全性，因为数据库一般来说保存、管理着比较重要的信息资源，不怀好意的访问将会带来巨大损失。而 CGI 是连接 Web 与数据库的主要通道，因此必须十分小心地使用 CGI 可执行程序，以防止对服务器的潜在安全性冒险。作为一项准则，在 Web 服务器上对于包含 CGI 应用程序的虚拟目录只授予执行权限。

下面以 Microsoft Internet Information Server 为例，讨论应采取的安全措施。

在 IIS 中，CGI 程序及其他应用程序一般放在 Scripts 虚拟目录下，可以通过设置 WWW 目录的访问权限来保护。操作如下：

(1)在 Internet 服务管理器中，双击 WWW 以显示其属性，然后单击“目录”选项卡。

(2)选定想要为其设置权限的目录。

(3)单击“编辑属性”。

(4)为允许 Web 客户读和下载目录中的内容，选定“读”复选框。

(5)为允许 Web 客户运行目录中的程序，选定“执行”复选框。

(6)单击“确认”，然后再单击“确认”。

虚拟目录 Scripts 包含应用程序。只有管理员可向标记为只执行的目录添加程序。这样，未授权用户在未

获得管理员访问权时不能复制恶意应用程序并在计算机上运行。另外，建议对与虚拟文件夹关联的目录上的 IUSR-computername 赋予读和执行权限，只对管理员才赋全部权限。如果只允许对已经配置的 WWW 服务器进行匿名登录，则所有远程用户的请求将使用 IUSR-computername 帐号。默认情况下，IUSR-computername 帐号不能使用 Windows NT 文件系统（NTFS）删除或更改文件，除非管理员特别授权的访问。这样，即使恶意程序复制到该计算机，它也不能对文件内容造成太大破坏，因为它只具有对计算机和文件的 IUSR-computername 访问权。

客户请求可用下面两种方法之一调用 CGI 应用程序：

·可在请求（URL）中指定可执行 CGI 文件名。示例 URL 是：

http://inetsrvr. microsoft. com/scripts/appl. exe/scripts/sample. ext? para = value

此请求要有效，文件 appl. exe 必须存储在 Web 发布目录中的某一位置，存储它的文件夹必须具有选定的执行权限。这种方法中，管理员可允许 CGI 应用程序从少量仔细监视的目录中运行。

·配置 CGI 应用程序的另一种方法是使用 Web File Extension Mapping 特性，允许可执行程序存储在 Web 发布目录以外的其他位置。示例 URL 是：

http://inetsrvr. microsoft. com/scripts/sample. ext? para = value

在本示例中，文件 sample. ext 存储在允许执行权限的 Web 发布目录的文件夹中。服务接收请求后，将使用文件名扩展映射以判定在何处查找应用程序（如 appl. exe），此应用程序可以存储在任何位置。这项技术防止用户通过在 URL 中增加参数直接调用 CGI 应用程序。因此是更安全的机制，并且对于所有 Web 应用程序很有用。

保护 CGI 程序在一定程度上防止非法用户入侵 Web 与数据库，除此之外，还可以使用 SSL 安全协议在 HTTP 协议与 TCP/IP 之间提供数据安全措施，以提高信息的安全性。SSL 协议针对一个 TCP/IP 连接能提供数据加密、服务器授权、选择客户权限、消息完整等安全措施。它可作为 Web 服务器与浏览器之间的一个数据安全协议。

三、结论

数据库在 Web 上的应用无疑增强 Web 的功能和吸引力，我们可以采用各种连接方式把 Web 与数据库相集成，达到综合信息服务的目的。CGI 是连接 Web 与数据库的一个通用的、易于实现的途径，利用它能够在各种平台上把不同类型的数据库连接到 Web 上来。安全措施需要考虑 CGI 应用程序的访问权限及保护、用户权限以及数据传输的安全性等因素，目的是最大限度地保护数据库和 web 的安全。

参考文献

[1] Berners - Lee T. The Hypertext Transfer Protocol. World - Wide Web Consortium. URL: http://www. w3. org/hypertext/WWW/Protocols/Overview. html

[2] Rob McCool. National Center for Supercomputing Applications, . University of Illinois at Urbana - Champaign Common Gateway Interface Overview. URL: http://hoohoo. ncsa. uiuc. edu/cgi/overview. html

[3] Bina E., Jones V., McCool R., and Winslett M. Secure Access to Data Over the Internet. Proceedings of the Third ACM/IEEE International Conference on Parallel and Distributed Information Systems, Austin, Texas, September 1994. URL: http://bunny. cs. uiuc. edu/CADR/pubs/SecureDBAccess. ps

（来稿时间：1997 年 12 月）