# WWW 服务器的安全管理

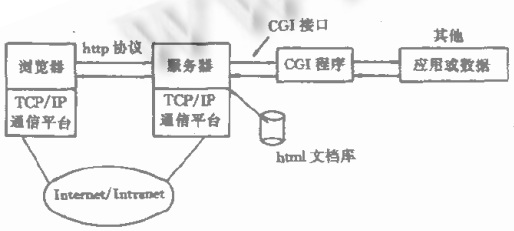
陈品德　（湘潭矿业学院自动化系　411201）
龚正虎　（国防科技大学计算机系）

**摘要**：本文通过分析 WWW 服务器的工作原理，揭示出 WEB 服务中所存在的安全问题。并以 NCSA httpd 1.3 为例，较为详细地介绍了 WWW 服务器的安全配置和管理方法。

**关键词**：www　网络安全

## 一、WWW 网络的工作原理

WWW 服务与 Internet 上的许多其他服务类型一样也是基于客户－服务器工作模式，它的实现主要依赖于以下几种技术(如图 1 所示)：




(1)http 协议。它是浏览器和服务器之间的通信协议，是一种简单、高效、无连接、无状态的应用层协议，其基本工作过程是：1. 双方利用 TCP 协议建立连接；2. 浏览器发出一个请求；3. 服务器响应请求；4. 断开连接。

(2)html 文本标记语言，在一个普通的文本文件中加入 html 标记命令便成为 html 文档。html 标记命令可以规定文本的显示格式、内置图像、超文本链等。超文本链包含一条指向其他文档、图像、声音资源位置的语句(例如：<A HREF = "http://www.xtky.whnet.edu.cn/index.htm>超文本链</A>)，当客户端用鼠标点击该处时，便可调回 URL 指向的另一文档。正是由于使用超文本链，用户在网上浏览时，可以从一个文档移到另一个文档，从一个地点移向另一个地点，而这个过程对用户来说是完全透明、浑然不觉的。

(3)URL (Uniform Resource Location)。它是一种标准化的命名方法，经由不同的协议，对 Internet 上任何地方的信息都可以用 URL 定位或取回。它的格式是：协议名://主机域名(:端口号)/ 文件路径，例如：http://www.xtky.whnet.edu.cn/pub/index.html。(4) CGI (Common Gateway Interface)。公共网关接口，CGI 是扩充 WWW 服务器功能的一个标准接口，它使得 WWW 服务器可以接受用户的输入请求，从而具有交互功能。当 WWW 服务器收到用户的输入请求后，它自己并不处理，而是将输入请求连同一些环境变量一起交给 CGI 应用程序，CGI 程序将处理后的结果重新经由 WWW 服务器返回给用户。

浏览器是 WEB 服务的客户端软件(如 Netscape, Mosaic 等)，它利用 http 协议从服务器上取回一个 MIME 类型的文档，并对其内容进行解释显示于客户端的屏面上。

浏览器向服务器发送的请求信息包括：请求方法与文档位置、浏览器支持的 MIME 类型以及与客户方有关的信息等。

服务器在收到请求后，将按如下方法将用户请求的 URL 映射到服务器上的实际文档位置：

(1)查看 URL 中是否包含了 srm.conf 配置文件中 alias 指令定义的虚拟目录(virtual directory)，若是，则将实际的路径替代虚拟目录。

(2)查看 URL 中是否含有"/user－name"，(user－name 是 WEB 服务器宿主机上的有效用户名)，若是，则转到用户目录中的公共 html 目录(如 public-html)下寻找相应的文档。

(3)否则，将服务方 DocumentRoot 指令定义的路径插入到 URL 中。

找到相应的文档位置后，还要根据存取控制文件确定用户的权限，若是合法用户，则响应用户的请求。

客户方的请求还可能是触发一个 CGI 程序，服务器根据以下因素确定，若满足以下条件之一，则转去调用



© 中国科学院软件研究所 http://www.c-s-a.org.cn

CGI 程序：

(1)在 srm.conf 配置文件中 ScriptAlias 记录指定专门存放 CGI 程序的目录(通常用虚拟路径 cgi-bin 代替实际的路径)，ScriptAlias 记录可以定义多个。例如 ScriptAlias /cgi-bin/ /serverroot/cgi-bin/，则任何对于/cgi-bin/目录下的文件请求都将导致调用一个 CGI 应用程序。

(2)若在配置文件中以 AddType 记录指定以特定的扩展名结束的文件为 CGI 程序。如 AddType application/x-httpd-cgi .cgi，则服务方每调用以.cgi 为扩展名的文件都认为是 CGI 程序而对其采取执行操作。

## 二、WWW 服务器的配置文件

WWW 服务器对用户的响应方式取决于对 WWW 服务方程序 httpd 如何进行配置，对于 WEB 服务器的安全管理也主要依赖于对 httpd 的正确配置。下面以 NCSA httpd1.3 为例介绍一下配置文件，对于其他类型的 WEB 服务器软件，其配置选项也大同小异。

NCSA httpd1.3 的配置文件有：

(1)httpd.conf 服务器主要配置文件。

(2)srm.conf 服务器资源配置文件。

(3)access.conf 全局存取控制文件。

httpd.conf 定义 httpd 的启动方法以及其他配置文件和 log 文件的名称和位置。主要有以下几个配置指令，如：

User，Group 定义了服务器运行时所使用的用户名(uid)和组名(gid)；

Port 定义了 httpd 启动后监听的端口号；

ServerRoot 定义 httpd 启动的绝对路径名，在启动时，httpd 期望在 ServerRoot 下找到相对路径文件 conf/httpd.conf；

AccessConfig 定义存取控制文件的名称和位置，默认为 conf/access.conf；

ResourceConfig 定义资源配置文件的名称和位置，默认为 conf/srm.conf；

ServerType 定义 httpd 的启动方式，默认为 standalone；

srm.conf 文件规定几个方面的内容：

(1)Alias、ScriptAlias、DocumentRoot 指令；

(2)增加支持 MIME 类型的指令；

(3)控制如何显示目录列表的指令；

(4)UserDir 记录，定义 WEB 服务器宿主机的用户目录可否提供访问，默认访问目录是 user-home/public-html；

(5)AccessFileName 指令，规定目录相关的存取控制文件名称，默认是.htaccess。

## 三、WEB 服务器的访问控制

NCSA httpd 提供了两种访问控制方法：主机过滤(以 IP 地址、IP 子网号或域名进行限制)、用户证实(以用户名和口令进行限制)。这两种方法都可以在全局性访问控制文件 conf/access.conf 及特定目录下的访问控制文件.htaccess 中加以规定。

主机过滤访问控制方法如下例：

```
<Directory /usr/local/etc/httpd/htdocs>
  Options Indexes FollowSymlinks
  AllowOverride None
  <Limit GET>
    order deny,allow
    deny from all
    allow from xtky.whnet.edu.cn
  </Limit>
</Directory>
```

<Directory>记录只能出现在全局 ACF 文件 access.conf 中，上面的意思是对于/usr/local/etc/ httpd/htdocs 这个目录只允许 xtky.whnet.edu.cn 域名中的用户访问，并且该文件不能被特定目录下的访问控制文件规定的控制方式覆盖(AllowOverride None)。

对于用户证实控制方式的使用要稍微复杂一些，举例如下：

```
<Directory /usr/local/etc/httpd/htdocs>
  Options Indexes FollowSymlinks
  AllowOverride None
  AuthUserFile /usr/local/etc/httpd/conf/.htpasswd
  AuthGroupFile /dev/null
  AuthName password!
  AuthType Basic
  <Limit GET>
  require user username
  </Limit>
</Directory>
```

其中 AuthUserFile 指明用户口令文件的位置及名



© 中国科学院软件研究所 http://www.c-s-a.org.cn

字；

AuthGroupFile 指出组定义文件的位置与名字，/dev/null 表明未使用组文件；

AuthName 定义了给用户的提示信息；

AuthType 定义授权类型，目前只能为 Basic；

另外在＜Limit GET＞中增加了 require 记录，说明允许哪些用户或组可以访问该目录。

用户的口令须用服务器端 htpasswd 程序产生，例如，加入 username1 的口令，可以如下进行：% htpasswd -c /usr/local/etc/httpd/conf/.htpasswd username1，这时系统将提示您输入口令。-c 参数（如果存在的话）表明是第一次生成.htpasswd 文件。

用户组文件可用文本编辑器生成，例如：/usr/local/etc/httpd/conf/.htgroup 文件的格式可如下：groupname: username1 username2 username3 ...

这两种控制方式也可以结合起来使用，例如：

```
＜Limit GET＞
    order deny, allow
    deny from all
    allow from xtky.whnet.edu.cn
    require group groupname
  ＜/Limit＞
```

其意义为只有 xtky.whnet.edu.cn 域中的用户才能得到用户名/口令的提示符。

口令认证方式的使用，需要具有相应功能浏览器软件的支持，当客户方访问受口令保护的文档时，将提示用户输入用户名和口令，一旦认证通过，用户在访问同一位置的其他页面时就无需重新认证。这是因为浏览器记住了服务器的主机名、路径及用户/口令对；当用户存取具有相同主机名及路径的 URL 时，用户原来输入的用户/口令对将继续起作用。

## 四、WEB 服务的安全漏洞及其防范

利用访问控制文件，可在一定程度上防范 WEB 信息的窃取。但是这里存在三个问题，一是用户名/口令在传输过程中的加密程度不高，口令仅仅以 uuencoded 格式加密；二是主机过滤存取控制方式取决于 DNS 的安全性，IP 地址也存在冒用问题；三是这两种控制方式并没有对信息本身进行加密。所以利用访问控制配置文件只能防范一般的情形。

另外还存在 WEB 服务器宿主机本身的安全性问题，由于宿主机有关信息的泄漏，给黑客以可乘之机，或者是由于 CGI 程序带来的安全性问题等，可以采取以下防范措施：

(1)限制 httpd 的运行权限，在 httpd.conf 文件中将 User 和 Group 设置为 nobody，切不可置为 root。

(2)将 httpd 的主要配置文件 httpd.conf、srm.conf、access.conf 设置为 root 用户所有，其他用户只有读权。

(3)为防止自动目录索引导致的.htaccess 等文件信息的泄漏，在 srm.conf 文件中严格限制列目录的方式。(利用 IndexIgnore 指令)例如设置：IndexIgnore */.?? * * *# */HEADER* */README*，这将使得在列目录时忽略 HeaderName、ReadmeName 以及一些隐藏文件、备份文件等。

(4)CGI 功能使得客户端可引起服务器上的程序执行，它常常是 WEB 服务器的安全隐患。可将 CGI 程序严格限制在几个规定的目录之中(利用 srm.conf 中的 ScriptAlias 指令以及在 access.conf 或.htaccess 文件中用 Options 指令规定)，尤其是限制在个人目录中执行 CGI 程序，可在 access.conf 中作如下设置：

```
＜Directory /*/public-html*＞
  AllowOverride None
  Options Indexes
＜/Directory＞
```

这样就限制了在任何 public-html 目录下执行 CGI 程序的权利，同时尽量使用可以编译成目标代码的高级语言编写 CGI 应用程序。

(5)一般情况下，浏览器访问的 html 文档位于服务器中用 Alias 或 DocumentRoot 指令规定的目录下，但是服务器上使用符号链(symbolic links)可以打破这种限制，使用户可能访问到规定目录以外的目录结构，这种情况可能在正常的文档树下发生，也可能在用户的 public-html 目录下发生。应当避免这种情况的发生，可在访问控制文件中在 Options 指令中取消 FollowSymLink 选项，或至少将其改为 SymLinksIfownerMatch。

(6)对 access.log、error.log 等文件定期分析查看，以防患于未然。

(来稿时间：1997 年 3 月)



© 中国科学院软件研究所 http://www.c-s-a.org.cn