```
X-FrontPage-User-Name: IUSER_MINSTAR

<html><head><title>RPC packet</title></head>
<body>
<p>method=list documents: 4.0.2.3717
<p>document_list=
<ul>
    <li>document_name=help.gif
<\ul>
```

可以从响应中看到，Web 服务器上可用文档的列表返回给了 FrontPage 客户端。在微软公司的网站上可以找到各种命令和响应的完整列表。

19.1.4 FrontPage的安全模型

任何直接访问 Web 服务器内容的发布系统都要非常注意其行为的潜在安全影响。FPSE 在极大程度上是依赖 Web 服务器来提供安全性的。

FPSE 安全模型定义了 3 种用户：管理员、作者以及浏览者，其中管理员拥有完全控制权。所有权限都是累积的，也就是说，所有的管理员都能编写和浏览 FrontPage 的网站。类似地，所有作者都有浏览权限。

对于给定的由 FPSE 扩展的网站，管理员、作者以及浏览者的列表都要定义好。所有的子 Web 可以从根 Web 继承权限，也可以自行定义。对于非 IIS 的 Web 服务器，所有的 FPSE 程序都要保存在标记为“可执行”的目录中（所有其他 CGI 程序也都有同样的限制）。Fpsrvadm，FrontPage 的服务器管理员实用工具，可以用来进行这种工作。在 IIS 服务器上，则可用 Windows 操作系统自身集成的安全模型。

在非 IIS 服务器上，Web 服务器的访问控制机制负责指定能够访问指定程序的用户。在 Apache 和 NCSA 的 Web 服务器上，访问控制文件名为 .htaccess；在 Netscape 服务器上，文件名是 .nsconfig。访问控制文件将用户、用户组以及 IP 地址与不同级别的权限关联起来：GET 是读权限，POST 是写权限，等等。例如，为了使用户在 Apache 的 Web 服务器上具有作者权限，.htaccess 文件应当允许该用户对 author.exe 进行 POST。这些访问规范文件常常是以目录为单位来定义的，这为权限定义提供了极大的灵活性。

428

在 IIS 服务器上，权限是通过给定根 Web 目录或子 Web 的根目录上的 ACL（Access Control List，访问控制列表）来制定的。当 IIS 收到请求时，首先登录，并模拟用户，接着发送请求到上述三个 DLL（Dynamic Link Library，动态链接库）之一。收到请求的 DLL 根据目标文件夹上定义的 ACL 检查所扮演用户的证书。如果检查通过，请求的操作就由扩展 DLL 来执行。否则，就向客户端发回“permission denied”