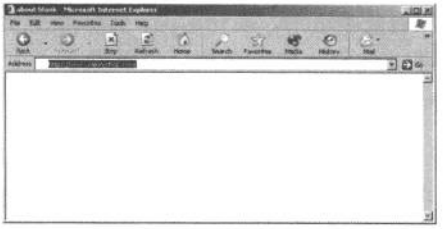
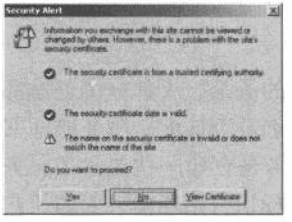


(a) 由于站点是虚拟主机站点，而证书的主机名为*.securesites.com，所以这个URL（www.cajun-shop.com）中的主机名与证书中的名称不匹配。




(b)对话框警告用户站点证书的日期有效，而且来自有效的证书颁发机构，但证书中所列名称与URL所请求的站点不相符。


（c）为了获取更详细的信息，用户点击了“查看证书”按钮，看到证书是一个通配证书，主机名为*.securesites.com。有此信息之后，用户就可以判定是该接受还是该拒绝这个证书了。


(d)接受证书，通过安全HTTPS协议装载页面。为避免此类用户错误，这个特定的站点将所有 HTTPS流量都导向了主机别名cajun-shop.securesites.com。这个虚拟主机名与ISP在其商业包中提供的证书名字相符。

图 14-18　证书名不匹配引发的证书错误对话框

## 14.8.1　OpenSSL

OpenSSL 是 SSL 和 TLS 最常见的开源实现。OpenSSL 项目由一些志愿者合作开发，目标是开发一个强壮的、具有完备功能的商业级工具集，以实现 SSL 和 TLS 协议以及一个全功能的通用加密库。可以从 http://www.openssl.org 上获得 OpenSSL 的相关信息，并下载相应软件。

328