目录

1. WebKnight 简介

WebKnight 是由 AQTRONIX (http://www.aqtronix.com)开发的一款基于 IIS 服务器的免费的 Web 应用程序防火墙。它是一款开源的软件，基于 GNU 协议开放源代码。它作为 ISAPI 过滤器运行。WebKnight 被安装在 IIS 服务器的前端，根据由 Web 管理员设置的过滤规则，过滤 IIS 接收到的所有 Web 请求。它通过阻止不安全的 Web 请求（如 SQL 注入攻击等），来保护 Web 服务器的安全。WebKnight 并不是根据攻击行为模式的数据库进行识别，那样的话数据库要定期更新；相反的，WebKnight 使用每种攻击行为的关键字作为过滤规则进行攻击行为的过滤判断。这种方法保证了 Web 服务器对已知或未知的攻击行为都具有安全性。

2. WebKnight 特性

- 低负载。和其他的防火墙相比，因为 WebKnight 和 Web 服务器的关系更紧密（因为它是一个 ISAPI 过滤器），所以不会服务器造成太大的负载。
- 开源。WebKnight 是一款基于 GNU 协议的开源软件。
- 日志功能。被阻止的请求将会记录到日志中，同样，所有允许的请求也将记录下来。WebKnight 也可以以 LogOnly 的模式运行，此时将只记录日志而对请求不做任何阻止。
- 自由定制。WebKnight 可以根据不同需要灵活定制。
- 与基于 Web 的程序兼容。WebKnight 与基于 Web 的程序相兼容，如 Frontpage Extensions, WebDAV, Flash, Cold Fusion, Outlook Web Access, Outlook Mobile Access, SharePoint 等。
- SSL 保护。与传统防火墙不同的是，WebKnight 可以保护使用 HTTPS 加密

的会话。

- HTTP 错误记录。WebKinght 可以被配置用来记录来自 Web 服务器的 HTTP 错误，如‘404 Not Found’的常见错误。这么做是为了检测脚本或攻击中的错误。也可以用来发现网站中失效的链接或配置的错误。
- 实时更新。对 WebKnight 配置的改变不需要重新启动 Web 服务器，所以可以做到不妨碍用户的使用。

3. WebKnight 的安装和卸载

3.1 安装 WebKnight

WebKnight 的安装有三种方法，Windows Installer，"install.vbs" 脚本，和手工安装。

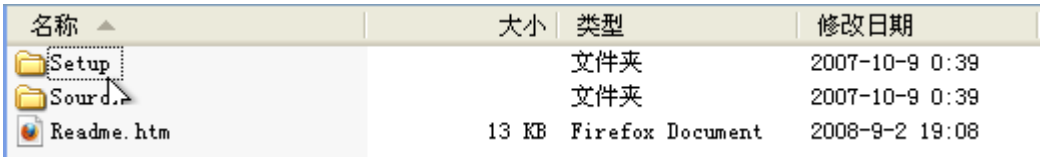
如果 Web 服务器上运行有多个网站，WebKnight 可被作为全局过滤器（global filter）安装；也可以为每个网站安装一个独立的过滤器（site filter）。

当使用 Windows Installer 和”install.vbs”脚本安装时，默认是作为全局过滤器（global filter）安装的。下面详细介绍安装步骤。

（1） 下载 WebKnight。

http://aqtronix.com/downloads/WebKnight/2008.09.02/WebKnight.zip

（2） 解压缩下载到的压缩包，可以得到如图所示的目录结构。

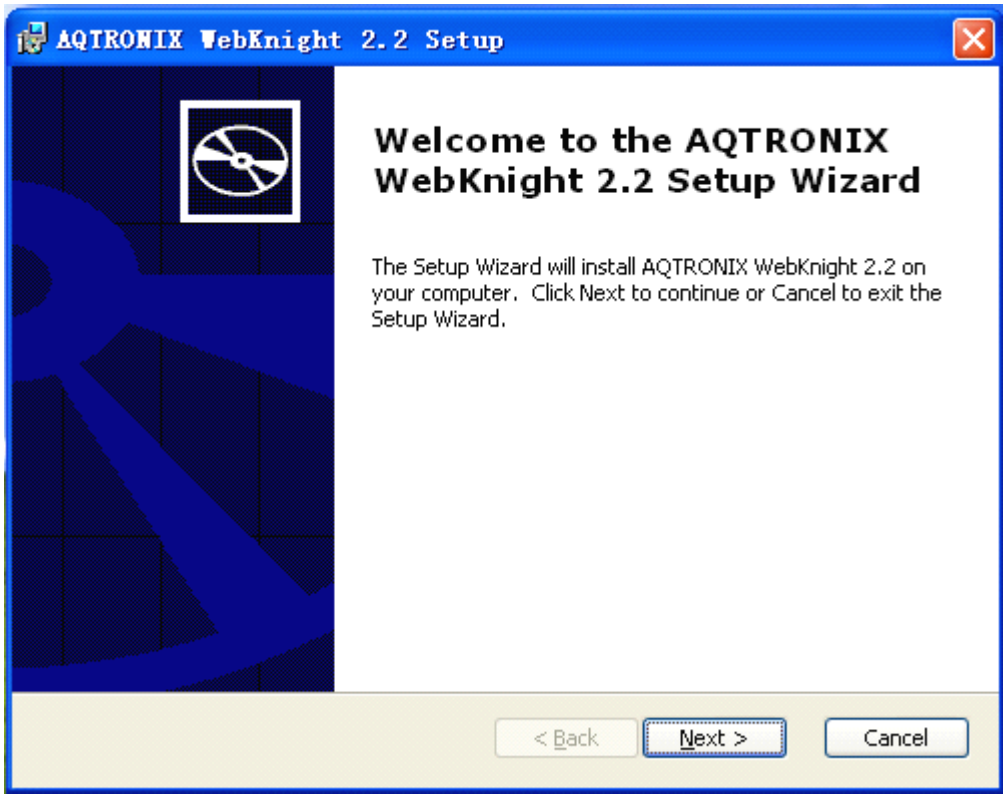


（3） Setup 文件夹下为安装所需的文件，Source 为 WebKnight 的源代码。双击 Setup 文件夹，根据自己的需要选择 32 位版本或 64 位版本。两个版本安装时区别不大，这里以 32 位版本为例，里面的文件如下图

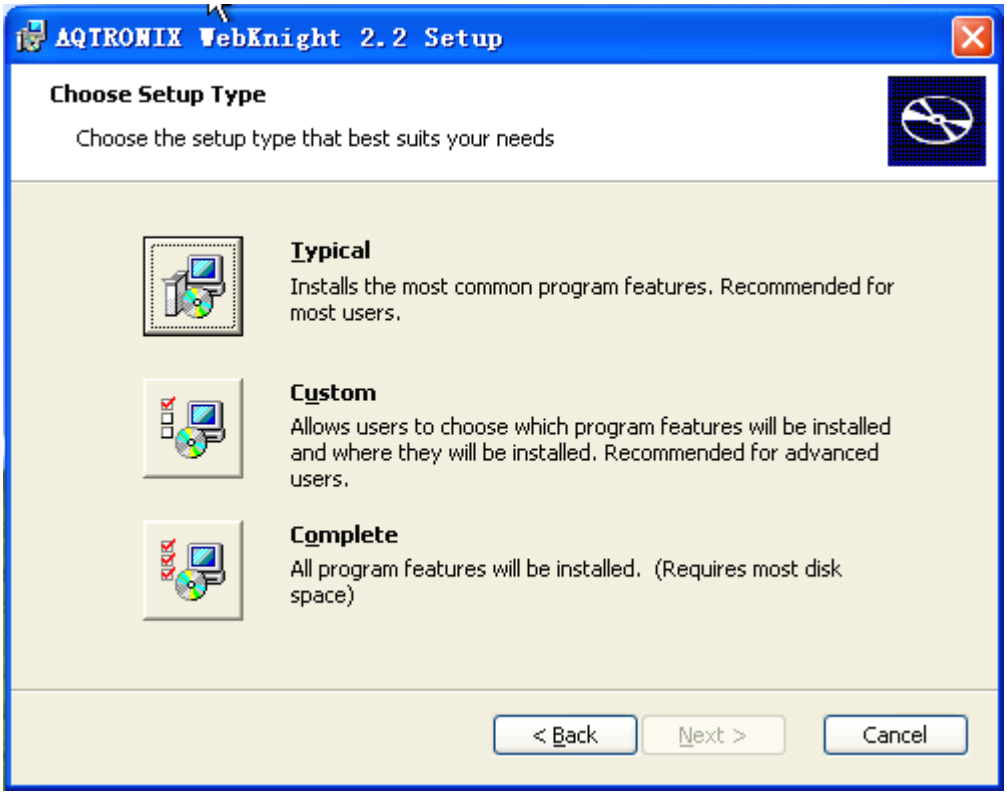
所示。

名称	大小	类型	修改日期
Config.exe	436 KB	应用程序	2008-7-9 23:25
denied.htm	2 KB	Firefox Document	2003-5-29 18:12
install.vbs	4 KB	VBScript Script...	2008-7-20 2:30
LogAnalysis.exe	424 KB	应用程序	2008-7-4 22:38
Readme.htm	13 KB	Firefox Document	2008-9-2 19:08
robots.txt	1 KB	文本文档	2006-9-13 23:33
Robots.xml	137 KB	XML 文档	2008-8-29 22:26
uninstall.vbs	3 KB	VBScript Script...	2008-7-20 2:30
WebKnight.dll	568 KB	应用程序扩展	2008-9-2 9:12
WebKnight.msi	301 KB	Windows Install...	2008-9-2 19:03
WebKnight.xml	78 KB	XML 文档	2008-9-2 9:44

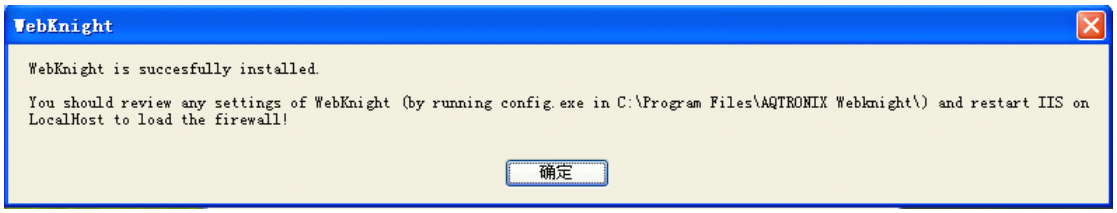
（4） 双击”WebKnight.msi”进行安装，或双击”install.vbs”运行该脚本进行安装（卸载时运行”uninstall.vbs”脚本）。下图是使用 WebKnight.msi 进行安装的界面。



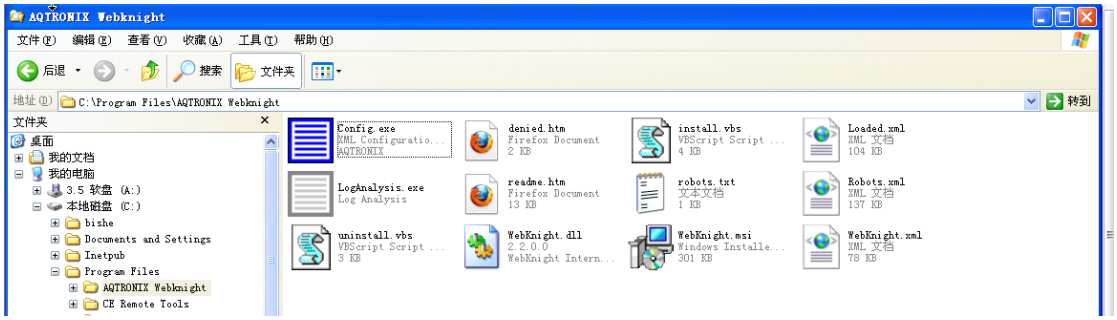
（5） 在点击了同意许可后，可以选择安装的类型。通常，选择”Typical”即可。



（6） 接下来，WebKnight 将会自动安装。安装完成后，将会出现一对话框提示安装成功。

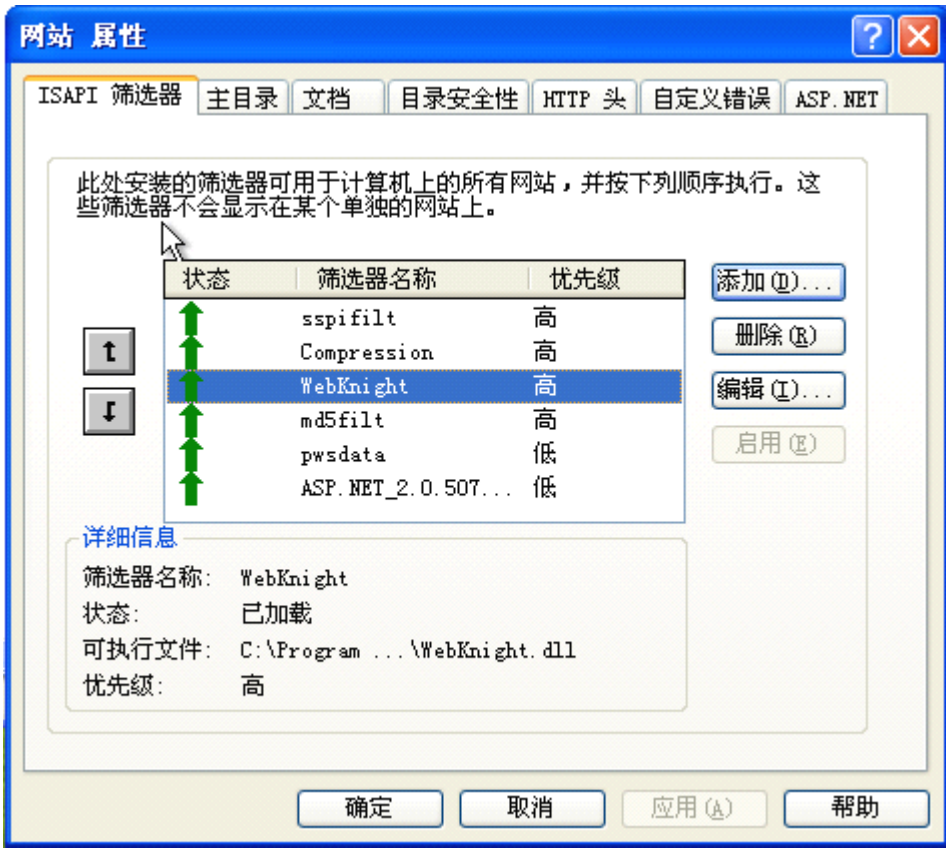


（7） WebKnight 默认被安装到 C:\Program Files\AQTRONIX WebKnight 下。请牢记这个目录位置，因为包含了 dll 文件（WebKnight.dll）、配置程序（Config.exe）、日志分析工具（LogAnalysis.exe）和日志文件。



（8） 重新启动 IIS 服务器。

（9） 如果 WebKnight 被成功的安装并重新启动了 IIS 服务器，在网站属性的 ISAPI Filter 标签页中可以看到 WebKnight 被成功加载（绿色向上箭头）。



WebKnight 可以按照上述的步骤被轻松的安装到 IIS 服务器中。如果想为不同的网站安装独立的过滤器，或自动安装无法使用，则需要按照下述步骤安装。

■ 手工安装全局过滤器

① 在服务器上建立一个本地路径，例如： C:\Program Files\AQTRONIX，复制 Setup 文件夹下所有文件至这个新建的文件夹下。

② 打开 IIS 服务器。

③ 右键单击服务器名（不是网站名），选择属性。

④ 选择 ISAPI Filter 选项卡，单击添加按钮。

⑤ 在弹出的对话框中填写过滤器的名字和 dll 文件的路径。

⑥ 单击 OK 关闭对话框。

⑦ 重新启动 IIS 服务器。

- 手工安装独立过滤器

① 在服务器上建立一个本地路径，例如：C:\Program Files\AQTRONIX\W3SVC1，复制 Setup 文件夹下所有文件到这个新建的文件夹下（每个网站一个独立的文件夹，例如 W3SVC1）。

② 打开 IIS 服务器。

③ 右键单击网站名（不是服务器名），选择属性。

④ 选择 ISAPI 选项卡，单击添加按钮。

⑤ 在弹出的对话框中填写过滤器的名字和 dll 文件的路径。

⑥ 单击 OK 关闭对话框。

⑦ 运行 Config.exe，将”Is Installed As Global Filter”按钮取消选中。

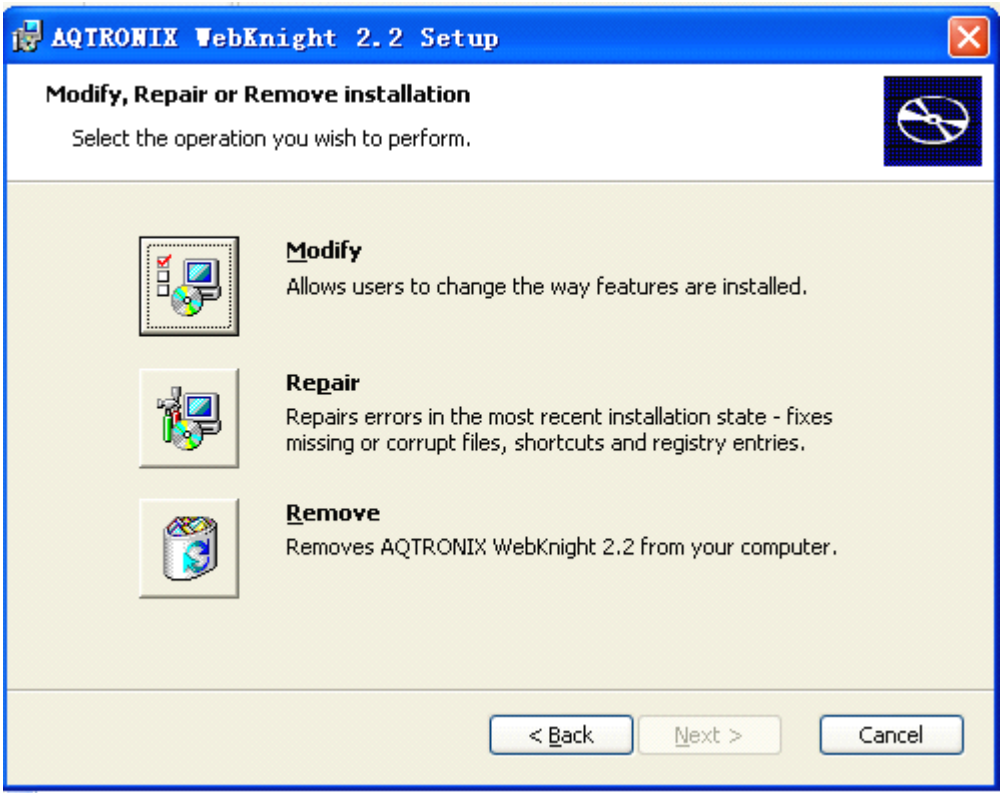
⑧ 重新启动 IIS 服务器。

3.2 卸载 WebKnight

欲卸载 WebKnight，选择下列三种方法之一，然后重新启动 IIS。

（1） 使用 Windows Installer 自动卸载（运行 WebKnight.msi）。

如果 WebKnight 安装在默认路径，运行 WebKnight.msi 后出现 Modify、Repair、Remove 选项，选择 Remove 即可卸载 WebKnight。



（2） 使用脚本自动卸载（运行 uninstall.vbs）。

如果 WebKnight 安装在默认路径，运行 C:\Program Files\AQTRONIX WebKnight\uninstall.vbs 脚本将自动卸载 WebKnight。

（3） 手动卸载。

如同手动安装的过程一样，打开 IIS 服务器，选择服务器名或网站名，右键单击选择属性，在 ISAPI Filter 选项卡中，选择 WebKnight，然后单击删除按钮。

当按上述步骤卸载 WebKnight 后，应重新 IIS 服务器。

4. WebKnigth 设置

WebKinght 提供了对 Web 攻击和尝试访问未授权文件的拦截功能。这些功能是安装时默认提供的，但有时候会阻止正常的 Web 访问。因此，WebKnight 在安装后需要对其进行自定义的设置，以使它更适合用户的使用环境。实际上，相较

安装而言，更多的时间和精力应花在配置上。配置的过程也提供了一次学习不同 Web 攻击模式的机会。

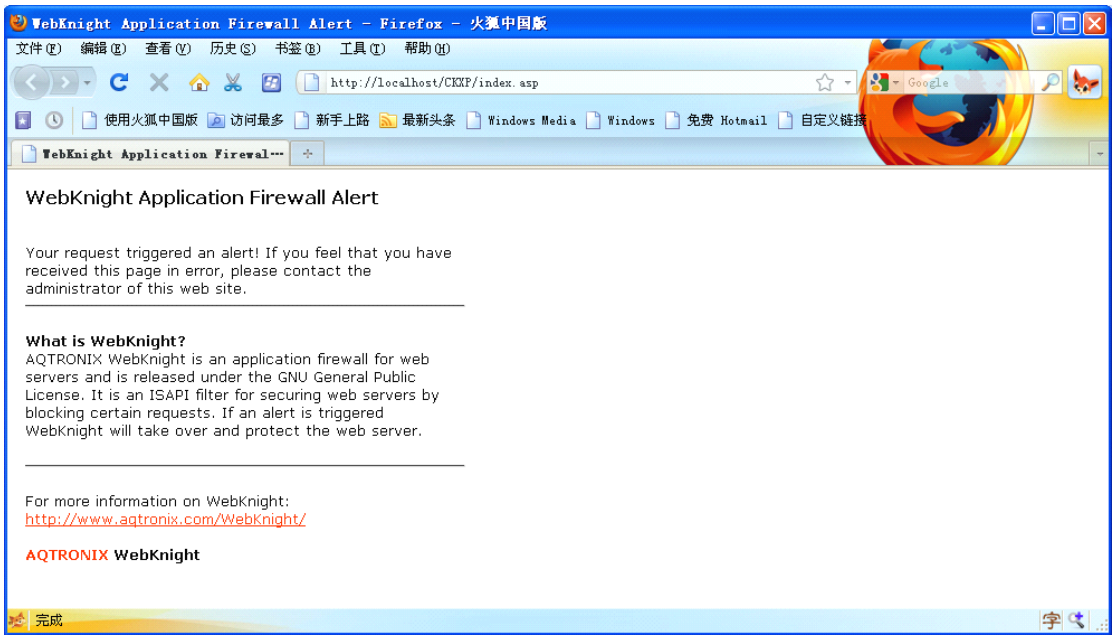
首先，在安装 WebKnight 后，应访问相应的网站，以检查 Web 请求是否正常执行和响应。如果没有发现任何阻止，应检查 WebKnight 日志文件中的相关规则。如果需要的话修改规则。

如果 WebKnight 被安装在默认目录，那么日志文件和配置程序位于：

✧ 日志文件 C:\Program Files\AQTRONIX WebKnight\LogFiles

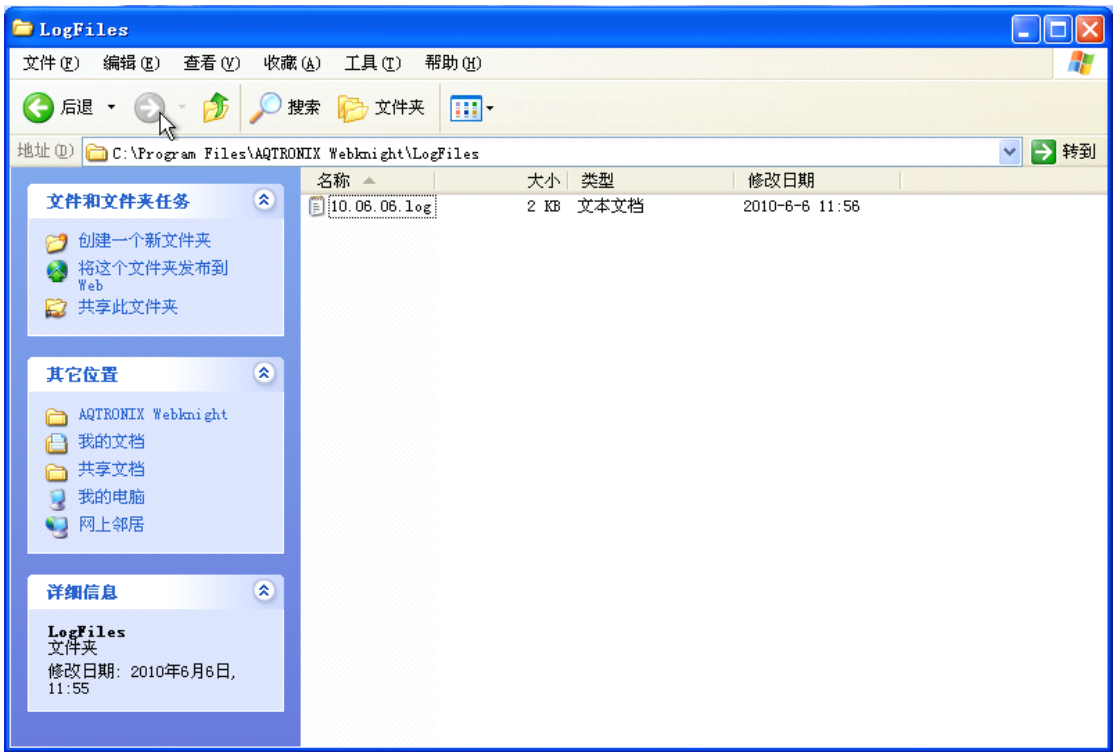
✧ 配置程序 C:\Program Files\AQTRONIX WebKnight\Config.exe

在安装 WebKnight 后，访问该网站，可能会出现如下的警告页面：



如果 WebKnight 根据过滤规则阻止了请求，这个默认的警告页面将发送到网站的浏览者。

如果正常的访问请求也出现了警告界面，那么请打开日志文件，找到“BLOCKED”信息和相应的规则。然后，在配置文件中关闭该项规则。如果是安装在默认文件夹下，“C:\Program Files\AQTRONIX WebKnight\LogFiles”文件夹将在 IIS 重新启动后建立，日志文件也将在这个文件夹下按照日期命名建立。



默认的日志文件的头域如下所示：

Time ; Site instance ; Event ; Client IP ; User name ; Additional info about request (event specific)

假设我们的正常 Web 访问被阻止，在日志文件找到如下的日志项：

05:57:42 ; W3SVC31 ; OnPreprocHeaders ; xxx.xxx.207.85 ; ; GET ;

/admin/img/deffortune.jpg ; BLOCKED: '/admin' not allowed in URL ; HTTP/1.1 ;

ASPSESSIONIDAQDBDDAD=NACAJJBAPJACHHPHNIPGDKCH

上述的日志项告诉我们 WebKnight 的规则中禁止访问/admin 文件夹，于是访问/admin/img/deffortune.jpg 的请求根据该规则也被阻止。Web 访问请求被阻止是因为原始页面被设计为从/admin 目录下读取图片文件。因此，应将原来用户访问的页面修改为不访问/admin 目录。或者，我们可以修改 WebKnight 的设置，使访问/admin 的请求不被阻止。基于日志项的定制可以帮助改进现有 Web 服务

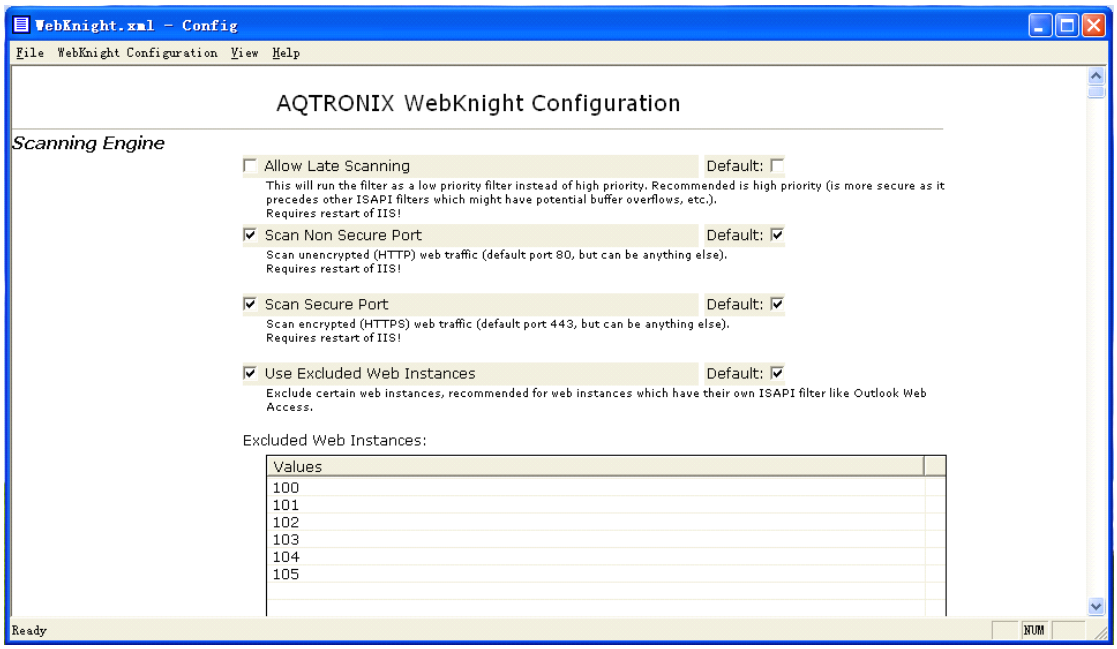
的设计。

下面的网址提供了关于 WebKnight 的安装、配置、常见问题的解答。在下一节中也提出了一些容易出现的问题和解决方法。

http://aqtronix.com/?PageID=114

在解读日志项时，应考虑到默认的时区是 GMT/UTC。如果想使用本地时间，请将“USE GMT”选项取消选中。

WebKnight 提供了一个图像化界面 Config.exe，可以方便用户自定义配置。各项的具体意义也在每项下解释的很清除，您可以参照您的需要自由定制。



5. FAQ

（1） Q：我改变了默认的设置，但是 WebKnight 阻止了所有的 Web 请求。

A：如果 WebKnight 在改变了设置后阻止了所有的合法请求，请尝试发现具体哪项设置阻止了请求。请打开日志文件并查看日志项，当你发现了“BLOCKED”信息，则表明有请求被阻止。再在配置文件中查找相似的配置项，如果你认为该项不应该被阻止，那么改变该设置即可。

（2） Q：WebKnight 没有发现配置的变化，或者还是使用默认的设置。

A：

a) 确定你编辑的配置文件是 WebKnight.xml 而不是 Load.xml（后一个文件是为了调试和观察哪些加载到内存中使用的）。

b) 确定 IIS 使用的账户（SYSTEM,NETWORK,SERVICE…）有修改 WebKnight 文件夹（包括子文件夹）的权限。

c) 出于性能的考虑，每分钟检测一次 WebKnight 配置的改变，且只有在有 Web 流量的情况下才检测。

d) 如果修改了 User-Agent 节，请注意 robots 节改变了 User-Agent 节的实际值。

（3） Q：WebKnight 阻止了 POST 请求，或文件上传。

A：

POST ; /mypage.asp ; HTTP/1.1 ; BLOCKED: Content-Type 'multipart/form-data; boundary=----------7d5281ab0594' not allowed ;

在 WebKnight1.3（包括以前版本），在 WebKnight 配置文件 Headers 节中，在“Allowed Content-Types”项中，添加“multipart/form-data”。但要注意第一行应保持空。

在 WebKnight2.0（包括之后版本），在“Web Applications”节中选中“Allow File Upload”。

（4） Q：某些文件被阻止，日志记录显示“URL is not RFC compliant”。

A：对于你的 URL，应遵循 RFC（RFC1808 和 RFC1738）标准。编码的 URL 只限于 US-ASCII。这意味着您不能在 URL 使用十六进制编码（%xx），即 ASCII 码大于 127（或 UNICODE 字符）。为了解决这个问题，您需要适当的编码您的 URL。

（5） Q：某些文件被阻止，日志显示“the URL contains high bit characters (shellcode)”或者显示“%u is not allowed”

A：WebKnight 默认的设置限制 URL 只能用 US-ASCII。您的文件名可能不是 US-ASCII 编码的，ASCII 码值大于 127 或 UNICODE 字符。在 WebKnight2.0 中，你可以在 Web Application 节中选中 Unicode 一项。在之前的版本中，你需要禁止 URL Scanning 下的 Deny High Bit Shellcode 项。为了使用 UNICODE 编码，您需要在 denied header/querystring/url/postdata 序列中移除%u。

（6） Q：IIS 根本不加载 WebKnight。

A：

- 取消选中“Is Installed As Global Filter”（在 Global Filter 节中），如果该项被选中，那么 WebKnight 将会注册 OnReadRawData 事件，这在 II6S 和 IIS7 中不是默认支持的。
- 检查 WebKnight 过滤器的权限。IIS 使用的账户（SYSTEM 或 NETWORD SERVICE）需要由写 WebKnight 文件夹的权限。
- 重新启动 IIS。
- 检查 WebKnight 日志文件，看具体是什么原因导致不能加载 WebKnight。

（7） Q：下载较大的 PDF 文件时被阻止。

A：日志文件可能显示“Range:”头太长。你在 Request Limits 节中可以改变 Range：头的限制。

（8） Q：没有日志文件。

A：WebKnight 日志有一个确定的日志文件的文件夹，如果你没有这个文件夹，或者文件夹下是空的，这意味着 WebKnight 没有访问修改该文件夹。

WebKnight 运行在 IIS 进程中，所以运行 IIS 的账户需要有修改 WebKnight 文件夹的权限（SYSTEM 或 NETWORD SERVICE 账户）。

6. 引用说明

本文的内容大都来自于 WebKnight 官方网站，以及韩国信息安全局提供的文档，本文旨在推广 WebKnight，方便中文用户的使用。

（1） WebKnight 官方网站：http://aqtronix.com/?PageID=99

（2） Korea Internet Security Center 的文档下载地址，分为英文版和韩文版：

英文版下载地址：

http://www.krcert.or.kr/english_www/inc/download.jsp?filename=TR2006003_Blocking_SQL_Injection_Attack_Using_WebKnight.pdf

韩文版下载地址：

http://www.krcert.or.kr/docDown.jsp?dn=7