IBM Security AppScan Standard
V 9.0.3.4

入门指南

SC43-3707-00

目录

第 1 章 安装

系统需求

运行 AppScan Standard 所需最低硬件和软件的摘要。

硬件需求

硬件	最低需求
处理器	Core 2 Duo 2 GHz（或同等处理器）
内存	4 GB RAM
磁盘空间	30 GB
网络	1 NIC 100 Mbps（针对具有已配置 TCP/IP 的网络通信）

操作系统和软件需求

软件	详细信息
操作系统	支持的操作系统： • Microsoft Windows Server 2012：Essentials、Standard 和 Datacenter • Microsoft Windows Server 2012 R2：Essentials、Standard 和 Datacenter • Microsoft Windows Server 2008：Standard 和 Enterprise，SP2 • Microsoft Windows Server 2008 R2：Standard 和 Enterprise（含或不含 SP1） • Microsoft Windows 10：Pro 和 Enterprise • Microsoft Windows 8.1：Pro 和 Enterprise • Microsoft Windows 8：Standard、Pro 和 Enterprise • Microsoft Windows 7：Enterprise、Professional 和 Ultimate（含或不含 SP1） **注：**支持 32 位和 64 位版本，但首选 64 位版本。
浏览器	Microsoft Internet Explorer 11
License Key Server	Rational® License Key Server 8.1.1、8.1.2、8.1.3、8.1.4
其他	Microsoft .NET Framework 4.5.2 （可选）需要 Adobe Flash Player for Internet Explorer 才能执行 Flash（以及查看某些建议中的指示视频）。支持 V9.0.124.0 到 14.0.0.125。不支持较低的版本，且某些版本可能需要进行配置。 （可选）用于定制报告模板的 Microsoft Word 2007、2010、2013

要点：在其机器上没有本地许可证的客户在使用 AppScan 时需要与其许可服务器进行网络连接。

要点：与 AppScan 运行在同一计算机上的个人防火墙可阻止通信，并导致结果不正确和性能降低。为了获得最佳结果，请不要在运行 AppScan 的计算机上运行个人防火墙。

Glass box 服务器需求

Glass box 扫描功能需要在应用程序服务器上安装 glass box 代理程序。有关更多详细信息，请参阅联机帮助，或者是在主 glass box 文件夹中找到的 Glass Box 用户指南，缺省情况下该指南位于：

```
C:\Program Files (x86)\IBM\AppScan Standard\Glass box
```

Java 平台：在 Java 平台上，支持以下服务器平台和技术。

软件	详细信息
操作系统	受支持的 Microsoft Windows 系统（32-bit 位和 64-bit 位版本）： • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2008 SP2 • Microsoft Windows Server 2008 R2 受支持的 Linux 系统： • Linux RHEL 5、6、6.1、6.2、6.3、6.4 • Linux SLES 10 SP4、11 SP2 受支持的 UNIX 系统： • UNIX AIX® 6.1、7.1 • UNIX Solaris (SPARC) 10、11
Java™ EE 容器	JBoss AS 6、7；JBoss EAP 6.1；Tomcat 6.0、7.0；WebLogic 10、11、12；WebSphere 7.0、8.0、8.5、8.5.5

.NET 平台：在 .NET 平台上，支持以下系统和技术：

项	详细信息
操作系统	受支持的操作系统（32-bit 位和 64-bit 位版本）： • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2008 SP2 • Microsoft Windows Server 2008 R2
其他	Microsoft IIS 7.0 或更高版本 必须安装 Microsoft .NET Framework 4.0 或 4.5，并且必须在根级别配置 IIS，才能用于此版本的 ASP.net

注：在服务器上运行应用程序时，用户必须具有管理员特权。

注：应在服务器上成功安装了您要测试的应用程序之后安装代理程序。

安装

安装向导用于指导您完成这一快速而简单的过程。

过程

1. 关闭任何已打开的 Microsoft Office 应用程序。
2. 启动 AppScan 安装。

   将启动"InstallShield 向导"，并检查您的工作站是否满足最低安装需求。然后将显示 AppScan® 安装向导欢迎屏幕。
3. 请按照向导指示信息来完成 AppScan 安装。

   注：将询问您是否要安装或下载 GSC（通用服务客户机）。如果要浏览 Web Services 以配置 Web Services 扫描，GSC 是必要的，但如果不用扫描 Web 服务，那么 GSC 就不是必要的）。

静默安装

使用命令行进行无人照管安装的指示信息。

您可以使用命令行和以下参数"静默地"安装 AppScan：

```
AppScan_Setup.exe /l"LanguageCode" /s /v"/qn INSTALLDIR=\"InstallPath\""
```

要点： 如果在安装 Rational AppScan 的同时想要安装"通用服务客户机"（扫描 Web Service 所必需的，但不是只扫描 Web 应用程序），您必须运行包含两个安装 (.exe) 文件的文件夹中的命令行。

参数	功能
/l	语言代码。选项有： • 英语：**1033** • 中文（繁体）：**1028** • 中文（简体）：**2052** • 法语：**1036** • 德语：**1031** • 意大利语：**1040** • 日语：**1041** • 韩语：**1042** • 葡萄牙语：**1033** • 西班牙语：**1034**
/s	激活"静默方式"（否则将启动常规安装）。 **注：**必须与 /v"/qn" 结合使用（请参阅下一行）

参数	功能
/v	设置其他 MSI 属性，如 UI 模式和 AppScan 将安装到的路径。 **UI 模式：** 对于"静默方式"，包含 /qn 作为参数（在两边加引号）。 **路径：** 如果您未定义安装路径，那么安装将使用缺省路径：...Program Files\IBM\AppScan Standard\ 要定义其他安装路径，请添加 INSTALLDIR=\"InstallPath\" 作为参数（在两边加上引号）。路径可能包括空格。 示例： /v"/qn INSTALLDIR=\"D:\Program Files\AppScan\""

示例：

- 要以静默方式将 AppScan 的英文版本安装在缺省目录中，请输入：

  ```
  AppScan_Setup.exe /s /v"/qn"
  ```

- 要以静默方式将 AppScan 的日语版本安装在缺省目录中，请输入：

  ```
  AppScan_Setup.exe /l"1041" /s /v"/qn"
  ```

- 要以静默方式将 AppScan 的韩文版本安装在 D:\Program Files\AppScan\ 中，请输入：

  ```
  AppScan_Setup.exe /l"1042" /s /v"/qn INSTALLDIR=\"D:\Program Files\AppScan\""
  ```

许可证

对许可证类型、安装和管理的描述。

AppScan 安装中包含一个缺省许可证，此许可证允许扫描 IBM 定制设计的 AppScan 测试 Web 站点 (demo.testfire.net)，但不允许扫描其他站点。为了扫描您自己的站点，您必须安装 IBM® 提供的有效许可证。在完成此操作之前，AppScan 将会装入和保存扫描和扫描模板，但不会对您的站点运行新的扫描。

Rational 许可证

从 V7.8 开始，AppScan 许可证从 Rational 许可证密钥中心下载。有三种类型的许可证：

"浮动"许可证
这些许可证安装到 IBM Rational License Server（可与运行 AppScan 的机器相同）。在其上使用 AppScan 的任何服务器均必须具有与许可证服务器的网络连接。用户每次打开 AppScan 时，都会检出一个许可证，而关闭 AppScan 时，会重新检入该许可证。

"令牌"许可证
这些许可证安装到 IBM Rational License Server（可与运行 AppScan 的机器相同）。在其上使用 AppScan 的任何服务器均必须具有与许可证服务器的网络连接。用户每次打开 AppScan 时，都会检出所需数量的令牌，而关闭 AppScan 时，会重新检入这些令牌。

"节点锁定"许可证
这些许可证安装到运行 AppScan 的机器上。每个许可证被分配到单个机器。

许可证状态

要查看许可证状态，请执行以下操作：

- 单击**帮助 > 许可证**。会打开"许可证"对话框，显示许可证状态和以下选项：

装入 IBM Rational 许可证	如果您拥有 IBM Rational 许可证（在您的计算机上或在其他网路服务器上），请单击此处以打开 AppScan License Key Administrator，您可以从这里装入和管理许可证。此外，也可从以下位置打开该程序： `..\IBM\RationalRLKS\common\licadmin8.exe`
添加 AppScan Enterprise 许可证	如果您的组织具有 AppScan Enterprise 许可证（允许扫描本地 AppScan Standard 许可证允许的站点外的其他站点），那么除了现有许可证外，还可导入这些许可权以在本地机器上使用。 **注：**仅当装入完整的 AppScan Standard 许可证（而非演示许可证）之后，该选项才可用。
查看许可证协议	单击此处以查看许可证协议。

注：可以通过单击  来刷新该对话框中显示的许可证信息。

注：如果已验证浮动或令牌许可证，但是许可证服务器后来变为不可用，那么 AppScan 可在"断开连接方式"下最多运行三天。在这段时间里，您可以照常扫描应用程序。

测试运行

如果您拥有 AppScan 的评估副本（即，未购买许可证），那么可以通过扫描 IBM 的"AltoroMutualBank"Web 站点（该站点是针对演示用途而创建）来"测试运行"该产品。使用以下 URL 和登录凭证：

URL	http://demo.testfire.net/
用户名	jsmith
密码	demo1234

注：如果您正在使用 AppScan 的评估副本，那么 AltoroMutual Bank Web 站点是您可以扫描的唯一站点。

另见第 10 页的『样本扫描』。

第 2 章 基本原则

扫描步骤和扫描阶段

"AppScan 全面扫描"包含两个"主要"阶段：探索和测试。尽管扫描过程的绝大部分对于用户来说实际上是无缝的，并且直到扫描完成几乎不需要用户输入，但理解其后的原则仍然很有帮助。

- **"探索"阶段：**在第一个阶段中，会探索站点并构造应用程序树。这就是"探索"阶段。AppScan 会分析它所发送的每个请求的响应，查找潜在漏洞的任何指示信息。AppScan 接收到可能指示有安全漏洞的响应时，它将自动创建测试，并记录验证规则（这些规则是确定哪些结果构成漏洞以及所涉及到安全风险的级别时所需的验证规则）。
- **"测试"阶段：**在"测试"阶段，AppScan 会发送其在"探索"阶段创建的上千条定制测试请求。它会记录和分析应用程序的响应，以识别安全问题并将其按安全风险的级别进行排名。
- **"扫描"阶段：**实践中，"测试"阶段会频繁显示站点内的新链接和更多潜在安装风险。因此，完成"探索"和"测试"的第一个"阶段"后，AppScan 将自动开始一个新的"阶段"，以处理新的信息。（缺省阶段数是 4。）

Web 应用程序与 Web Service

首先通过探索站点来扫描站点，然后根据探索阶段响应对站点进行测试。有其他方式来收集"探索数据"。在所有情况下，一旦收集了数据之后，AppScan 就将用于向站点发送测试。

在没有 web 服务的情况下探索站点

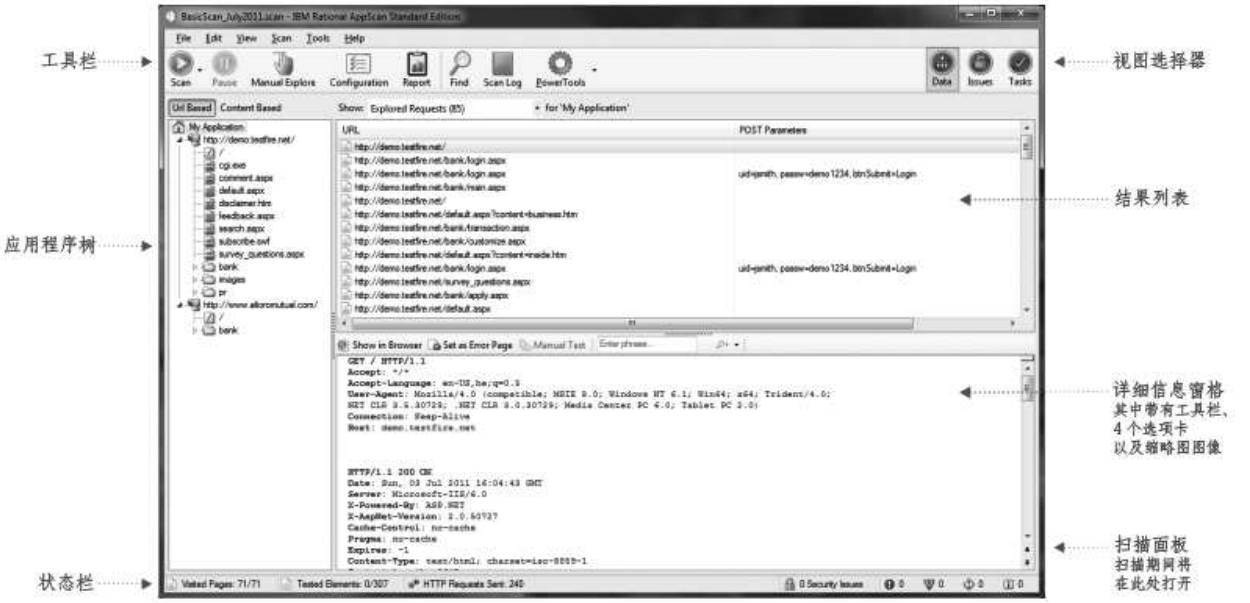
- 如果是没有 Web 服务的站点，那么为 AppScan 提供起始 URL 和登录认证凭证通常足以使其能够测试站点。
- 如有必要，还可以通过 *AppScan* 手动搜寻站点，以便能够访问仅通过特定用户输入才能到达的区域。

探索 web 服务

- 为了扫描 web 服务，可设置 AppScan 作为用探索服务的设备（例如移动电话或模拟器）的记录代理。这样，AppScan 就可以分析收集到的探索数据，并发送相应的测试。
- 如果您具有 web 服务（例如 SOAP web 服务）的 WSDL 文件，那么 AppScan 安装可以有选择地包含单独的工具，此工具使用户能够查看已合并到该 Web Service 中的各种方法，对输入数据进行控制，以及检查来自该服务的反馈。您首先需要为 AppScan 提供服务的 URL。集成的"通用服务客户机（GSC）"使用 WSDL 文件以树格式显示可用的单独方法，并且会创建用户友好的 GUI 来向服务发送请求。您可以使用此界面输入参数和查看结果。此过程由 AppScan 进行"记录"，并且用于在 AppScan 扫描站点时创建针对服务的测试。

主窗口

主屏幕包含菜单栏、工具栏、视图选择器和三个数据窗格：**应用程序树**、**结果列表**和**"详细信息"窗格**。下图显示使用扫描的数据进行填充的主屏幕。



视图选择器	单击三个按钮中的其中一个，以选择在三个主窗格中显示的数据类型。
应用程序树	会随着扫描进度填充应用程序树。扫描完成时，该树显示在应用程序中所找到的所有文件夹、URL 和文件。
结果列表	显示应用程序树中选定节点的相关结果。
详细信息窗格	显示三个选项卡（"咨询"、"修订建议"和完整的"请求/响应"）中的结果列表内选定节点的相关详细信息。

工作流程

此部分描述使用"扫描配置向导"的简单工作流程，对新用户或带有额外配置扫描模板的用户最适合。更多的高级用户可能喜欢使用扫描配置对话框来配置其扫描，手动探索某些站点（ 以显示 AppScan 某些典型的用户行为），然后启动扫描。

使用下列向导扫描：

1. 选择扫描模板。（您可以稍后按照要求调整配置。）
2. 打开"扫描配置"向导并选择扫描类型：

探索选项	描述
AppScan（自动或手动）	对大多数 web 应用程序扫描选择该选项。通过从 AppScan 发送到应用程序的请求手动和/或自动探索应用程序。
外部设备/客户机（用 AppScan 作为记录代理）	选择该选项可使用 AppScan 作为记录代理，并使用移动设备、模拟器或仿真器手动探索 web 服务。AppScan 在其外部流量记录器中显示域和请求，并根据输入发送相应的测试。

探索选项	描述
通用服务客户机 (WSDL)	对带有 WSDL 文件的 web 服务选择该选项。通用服务客户机 (GSC) 使用 Web 服务的 WSDL 文件来显示一个简单界面以在其中显示可用的服务，还使您能够输入参数并查看结果。使用 GSC 界面可手动探索 Web Service，以便 AppScan 能够使用您的输入来创建相应的测试。 **注：**如果在安装 AppScan 时未安装 GSC，那么选择该选项时将提示您进行安装。

3. 遵循向导步骤来探索应用程序：

   AppScan：

   a. 输入起始 URL。

   b. （推荐）记录登录过程。

   c. （可选）复审"测试策略"。

   外部设备：

   a. 将 AppScan 配置为记录代理。

   b. （如果服务器使用 HTTPS：）本地或在设备上安装 AppScan SSL 证书。

   c. 记录登录过程。

   d. （可选）复审和编辑"测试策略"。

   e. 将请求从使用 AppScan 作为记录代理的设备发送到服务器。

   f. 编辑域和请求的列表以用于测试阶段。

   GSC：

   a. 输入 WSDL 文件位置。

   b. （可选）复审"测试策略"。

   c. 使用"通用服务客户机"（该客户机会自动打开）以向服务发送请求，同时，AppScan 会记录您的输入和接收到的响应。

      注：您必须向服务发送至少一个请求，以便 AppScan 能够对其进行测试。

4. （可选，仅应用程序）运行 **Scan Expert**：

   a. 运行 Scan Expert 以复审对正在扫描的应用程序的配置是否有效。

   b. 复审建议的配置更改并选择性地应用这些更改。

   注：启动扫描时，您可以配置 Scan Expert 以自动执行其分析并应用部分建议。

5. 启动自动扫描：
   - （应用程序：）全面自动扫描（探索和测试）
   - （服务：）仅测试

6. 复审结果以评估站点的安全状态，以及
   - 手动探索其他链接
   - 打印报告
   - 复审补救任务
   - 向您的缺陷跟踪系统记录缺陷

样本扫描

样本扫描可帮助您感受 AppScan 的用法以及扫描结果的内容。

可在安装 AppScan 时将三个样本扫描保存到您的机器。可打开这些扫描以查看如何对它们进行配置以及如何在 AppScan 中显示结果。它们可在主 AppScan Standard 文件夹中找到，其缺省位置为：

```
C:\Program Files (x86)\IBM\AppScan Standard
```

扫描包括：

demo.testfire.net.scan

这是 AppScan 演示测试站点的扫描。您可以复审配置和结果。还可以向站点发送其他请求并使用新数据继续扫描。

Glass_Box_DotNet_Demo.scan and Glass_Box_Java_Demo.scan

这两个扫描是分别使用 .NET 应用程序服务器和 Java 服务器的 glass box 扫描的示例。您可以复审配置并向下钻取到单个问题以查看 glass box 结果的内容。

注：Glass box 需要正在扫描的应用程序的服务器上代理程序的访问权，而且您没有用于该扫描的代理程序的访问权，因此无法继续扫描。

GSC_demo.testfire.scan

这是 AppScan 演示测试站点的 Web Service 扫描。您可以复审配置和结果。如果已安装了 GSC（通用服务客户机），那么可将其用于向站点发送其他请求并使用新数据继续扫描。

第 3 章 配置期间

关于此任务

本部分描述使用该向导来进行标准应用程序扫描配置。要获取高级配置方法和 Web Service 扫描配置的详细信息，请参阅主要的用户指南和在线帮助。

过程

1. 启动 AppScan。
2. 在"欢迎屏幕"上，单击**创建新扫描**。
3. 在"新建扫描"对话框中，验证是否已选择"启动向导"复选框。
4. 在"预定义的模板"区域，单击**常规扫描**以使用缺省模板。（如果您正在使用 AppScan 扫描具有专用预定义模板的其中一个测试站点，那么请选择该模板：Demo.Testfire、Foundstone 或 WebGoat。）
5. 选择 **Web 应用程序扫描**并单击**下一步**，以进行三个步骤设置的第一步。
6. 在扫描开始处输入 **URL**。

   注：如果您需要添加其他服务器或域，那么请单击"高级"。
7. 单击**下一步**以继续进行下一步骤。
8. 选择**记录的登录**，然后单击**新建**。 这时会显示描述记录登录过程的消息。
9. 单击**确定**。 这时会打开嵌入式浏览器，其中的"记录"按钮已按下（呈灰色）。
10. 浏览登录页面，记录有效的登录序列，然后选择浏览器。
11. 在"会话信息"对话框中，复审登录序列并单击**确定**。
12. 单击**下一步**以继续进行下一步骤。 在这一步骤，您可以复审将用于扫描的"测试策略"（即，哪一类别会用于扫描）。

    注：缺省情况下，会使用所有除侵入式测试以外的测试。

    注：高级按钮使您能够控制其他测试选项，其中包括特权升级（测试在不具有充分的访问特权时，用户可访问特权资源的程度）和多阶段扫描。
13. 缺省情况下会选择**会话中检测**复选框，并且会突出显示指示响应处于"会话中"状态的文本。在扫描过程中，AppScan 会发送脉动信号请求，检查此文本的响应，以验证其是否仍处于登录状态（并在需要时重新登录）。验证突出显示的文本是否确实能够证明会话的有效性。
14. 单击**下一步**。
15. 选择适当的单选按钮以启动**自动扫描**，使用**手动探索**或**稍后**来启动（可以通过单击工具栏上的"启动"图标来稍后启动扫描）。
16. （可选）缺省情况下，会选择 Scan Expert 复选框，以便在完成向导时运行 Scan Expert。您可以清除此选择，以直接进入扫描步骤。
17. 单击**完成**以退出该向导。

Scan Expert

"扫描配置向导"中的其中一个选项适用于 Scan Expert，可指导其运行简短扫描，以评估特定站点的新配置的效率。

运行 Scan Expert 时，会在屏幕的顶部打开 Scan Expert 面板，并且由于 Scan Expert 探索站点，应用程序树将会开始出现在左边的窗格中。

在简短评估结束时， Scan Expert 会为您建议可以接受或拒绝的配置更改。（您可以单独查看各个建议，也可以选择自动应用建议。）

注：部分更改只能由 Scan Expert 手动进行应用，因此，当选择自动选项时，可能不会应用部分更改。

- 要手动运行 Scan Expert，请通过简短"探索"阶段进行（如果尚未有"探索"结果），请单击**扫描 > 运行"Scan Expert 评估"**。
- 要在现有"探索"阶段结果上手动运行 Scan Expert，请单击**扫描 > 只运行"Scan Expert 分析"**。
- 要将 Scan Expert 配置为在扫描开始前自动运行，请单击**工具 > 选项 > 首选项**，然后选择**扫描开始前运行 Scan Expert**。
- 要配置运行哪个 Scan Expert 模块，请单击**配置 > Scan Expert**。

手动探索

关于此任务

通过单击链接并输入数据，"手动探索"使您能够自行浏览应用程序。AppScan 会记录您的操作，并使用该数据来创建测试。有三种可能的原因让您想要进行手动探索：

- 为了传递反自动化机制（如要求输入随机字以作为图像显示）
- 为了探索特定的用户进程（在某种情况下，用户将访问的 URL、文件和参数）
- 由于在扫描过程中发现了交互式链接，并且您想要填写所需数据以启用更加详尽的扫描

注：创建"手动探索"后，您可能想要继续自动"探索"步骤，以便扫描可覆盖您的整个应用程序。

过程

1. 单击**扫描 > 手动探索**

   这时会打开嵌入式浏览器。
2. 浏览站点，然后单击链接并按要求填写字段。
3. 完成后关闭浏览器。

   注：您可以通过单击**暂停**，浏览至其他位置，然后单击**记录**来恢复记录，从而创建包含多个过程的手动探索。

   这时会显示**已探索的 URL** 对话框，其中显示您所访问的 URL。
4. 单击**确定**。
5. AppScan 会检查您的所有输入是否适合添加到"自动表单填充器"，显示列表，以及询问如果这样询问，您想要添加**全部**、**无**还是**选定的参数**。
   - 如果您想要将部分输入添加到"自动表单填充器"，那么请单击**添加选定的输入**。然后在"临时表单参数"列表中选择项，并单击**移动**（以将其移动到"现有表单参数"列表）。然后单击**确定**。
6. 单击**确定**。 AppScan 分析已搜寻的 URL，并基于该分析来创建测试。
7. 要运行新测试，请单击**扫描 > 继续扫描**。

第 4 章 扫描

扫描开始时，"进度面板"会出现在屏幕的顶部，并与状态栏（靠着屏幕的底部）一起显示扫描进度的详细信息。在处理过程中，窗格会由实时结果填充。

"进度"面板

进度面板显示当前阶段的扫描以及正在进行测试的 URL 和参数。

如果在扫描过程中发现了新链接（并且启用了多阶段扫描），那么会在先前的阶段完成后自动启动其他扫描阶段。新阶段可能会大大短于先前的阶段，因为仅会扫描新链接。在进度面板上还可能会显示警报，如"服务器关闭"。

状态栏

屏幕底部的状态栏显示以下扫描信息：

- **已访问页面数：**已访问的页面数量/要访问的页面总数

  随着发现某些页面，然后因为不需要扫描这些页面而拒绝此类页面，第二个数字可能会在扫描期间增加，然后减少。扫描结束时，两个数字应该相等。
- **已测试元素数量：**已测试袁术数量/要测试的元素总数

  随着发现要测试的元素，第二个数字会在"探索"阶段增加。测试阶段，第一个数字将增加。扫描结束时，两个数字应该相等。
- **发送的 HTTP 请求数**

  该数字代表所有已发送的请求，包括会话中检测请求、服务器关闭检测请求、登录请求、多步骤操作和测试请求。因此在扫描期间，这是 AppScan 正在工作的指示符，但无论是在扫描期间还是在扫描之后，实际数字没有任何特殊重要意义。
- **安全问题数**

  发现的安全问题的总数，后跟在每个类别中的编号：高、中、低和参考。

调度扫描

您可以调度扫描以自动启动一次或定期自动启动。

过程

1. 单击**工具 > 扫描调度程序**，然后单击**新建**。
2. 为调度输入名称，然后填写您所需的选项：
   - 选择**当前扫描**或**已保存的**扫描（如果选择"已保存的"，那么请浏览到必需的 .scan 文件）
   - 选择**每日**、**每周**、**每月**或**仅一次**。
   - 为扫描选择**日期**和**时间**
   - 输入**域名**和**密码**
3. 单击**确定**。

此时会在**扫描调度程序**对话框中显示调度名称。

第 5 章 处理结果

结果视图

可以三种视图来显示结果："安全问题"、"补救任务"和"应用程序数据"。可通过单击视图选择器中的按钮来选择视图。由于选定的视图不同，在三个窗格中显示的数据也会有所不同。

	**"数据"视图**	显示来自"探索"阶段的脚本参数、交互式 URL、已访问的 URL、中断链接、已过滤的 URL、注释、JavaScript 和 cookie。 **应用程序树：**完成应用程序树。 **结果列表：**从"结果列表"顶部的弹出列表中选择过滤器，以确定要显示哪些信息。 **详细信息窗格：**在"结果列表"中选定的项的详细信息 与其他两种视图不同，即使 AppScan 仅完成了"探索"步骤，"应用程序数据"视图也可用。使用"结果列表"顶部的弹出列表来过滤数据。
	**"问题"视图**	显示发现的实际问题，从概述级别一直到个别请求/响应级别。这是缺省视图。 **应用程序树：**完成应用程序树。每个项旁的计数器会显示为项找到的问题数量。 **结果列表：**列出应用程序树中所选定的节点的问题，以及每个问题的严重性。 **详细信息窗格：**显示在"结果列表"中选定问题的咨询、修订建议和请求/响应（包括所使用的所有变体）
	**任务视图**	提供特定修复任务的任务列表，以修订扫描所找到的问题。 **应用程序树：**完成应用程序树。每个项旁的计数器会显示该项的修订建议数量。 **结果列表：**列出应用程序树中所选定的节点的修订任务，以及每项任务的优先级。 **详细信息窗格：**显示在"结果列表"中所选定的修复任务的详细信息，以及该修复将解决的所有问题。

严重性级别

"结果列表"显示应用程序树中选定的任何项的问题。这些可以是以下几种级别：

- 根级别：显示所有站点问题
- 页面级别：页面的所有问题
- 参数级别：针对特定页面的特定请求的所有问题

会为每个问题分配其中一种安全级别（共四种）：

	高安全问题

	中等安全问题
	低安全问题
	参考安全问题 **注意：**此类别仅适用于"问题视图"。在"补救视图"中，所有低于"中等"的问题都分类为"低"。

注：分配给任何问题的严重性级别都可以通过右键单击节点来进行手动更改。

"安全问题"选项卡

在"安全问题"视图中，会在以下四个选项卡的"详细信息"窗格中显示选定问题的漏洞详细信息：

问题信息	其他"详细信息"窗格选项卡上提供了信息摘要以及其他信息，包括针对问题的 CVSS 度量值评分和相关屏幕快照，这些可以与结果一起保存并包含在报告中。
咨询	选定问题的技术详细信息，以及更多信息的链接。必须修订的内容和原因。
修订建议	为保障 Web 应用程序不会出现选定的特定问题而应完成的具体任务。
请求/响应	显示发送到应用程序及其响应的特定测试（可以 HTML 格式或在 Web 浏览器中查看）。 **变体：**如果存在变体（发送到同一 URL 的不同参数），那么可通过单击选项卡顶部的 **<** 和 **>** 按钮来对其进行查看。 该选项卡右边的两个选项卡使您能够查看**变体详细信息**，并添加将与结果一同保存的**快照**。

导出结果

关于此任务

您可以将完整的扫描结果导出为 XML 文件，或导出为关系数据库。（数据库选项会将结果导出到 Firebird 数据库结构。这是开放式源代码，且遵循 ODBC 和 JDBC 标准。）

过程

1. 单击**文件 > 导出**，然后选择 **XML** 或 **DB**。
2. 浏览至想要的位置，然后为文件输入名称。
3. 单击**保存**。

第 6 章 报告

AppScan 评估了您站点的漏洞后，可以生成针对组织中各种人员而配置的定制报告。

您可以在 AppScan 内打开并查看报告，并将其保存为可由第三方应用程序（如 Acrobat Reader）打开的文件。

图标	名称	简短描述
	**安全报告**	扫描期间找到的安全问题的报告。安全信息可能非常广泛，并可根据您的需要进行过滤。包括六个标准模板，但根据需要，每个模板都可轻易调整，以包括或排除信息类别。
	**行业标准报告**	应用程序针对选定的行业委员会或您自己的定制标准核对表的一致性（或非一致性）报告。
	**合规一致性报告**	应用程序针对规范或法律标准的大量选项或您自己的定制"合规一致性"模板的一致性（或非一致性）报告。
	**增量分析报告**	"增量分析"报告比较了两组扫描结果，并显示了发现的 URL 和/或安全问题中的差异。
	**基于模板的报告**	包含用户定义的数据和用户定义的文档格式化的定制报告（格式为 Microsoft Word .doc）。

注："行业标准"和"合规一致性"报告在 AppScan Developer Edition 中不可用。

第 7 章 主工具栏

工具栏上的图标对常用功能提供快速访问（也可从菜单中访问）。

图标	名称	单击以：
	扫描 >	（仅当已装入并配置扫描后才可用。）打开简短的"扫描"菜单，会显示以下选项：  全面扫描：启动全面扫描（探索和测试阶段）或继续已暂停的扫描。  仅探索：仅运行探索阶段（或继续已暂停的探索），之后不需要进行测试阶段。  仅测试：仅运行测试阶段（或继续已暂停的测试），不需要首先运行探索阶段。仅当已存在一些探索结果时，该按钮才是活动的。
	暂停扫描	（仅当扫描正在运行时，该按钮才是活动的。）暂停当前扫描（不管是"全面扫描"、"仅探索"还是"仅测试"）。 稍后您可以恢复该扫描。您也可保存已暂停的扫描，以便下次可以继续。
	手动探索	打开浏览器以进入应用程序的 URL 并手动浏览该站点，在浏览过程中填写必填的参数。然后，AppScan 在为站点创建测试时，会将该探索数据添加到其本身自动收集的探索数据。
	配置	打开"扫描配置"对话框，以配置扫描。
	报告	使用当前扫描数据来创建报告。
	查找	查找问题。（仅当已选定"问题"视图时才启用。）
	扫描日志	显示扫描期间或扫描之后的"扫描日志"。（列出扫描期间发生的并由 AppScan 所执行的所有操作。）
	PowerTool	打开随 AppScan 提供的某个 PowerTool 应用程序，以帮助您完成各种任务。

视图选择器

工具栏右侧的三个图标在三个视图间切换：应用程序数据、安全性问题和修补任务。

图标	名称	单击以显示：
	数据视图	"应用程序数据"视图。

图标	名称	单击以显示：
	问题视图	"安全性问题"视图。
	"任务"视图	"修补任务"视图。

IBM Security AppScan Standard V9.0.3.4 文档声明

编程接口：指定的编程接口使客户能够编写程序以获取 IBM Security AppScan Standard Edition 的服务。

本信息是为在美国提供的产品和服务编写的。

IBM 可能在其他国家或地区不提供本文档中讨论的产品、服务或功能特性。有关您当前所在区域的产品和服务的信息，请向您当地的 IBM 代表咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或暗示只能使用 IBM 的产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务的操作，由用户自行负责。

IBM 可能已拥有或正在申请与本文档内容有关的各项专利。提供本文档并未授予用户使用这些专利的任何许可。您可以用书面形式将许可查询寄往：

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

有关双字节 (DBCS) 信息的许可查询，请与您所在国家或地区的 IBM 知识产权部门联系，或用书面方式将查询寄往：

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

以下段落对于英国和与当地法律有不同规定的其他国家或地区均不适用： INTERNATIONAL BUSINESS MACHINES CORPORATION"按现状"提供本出版物，不附有任何种类的（无论是明示的还是默示的）保证，包括但不限于默示的有关非侵权、适销和适用于某特定用途的保证。某些国家或地区在某些交易中不允许免除明示或默示的保证。因此本条款可能不适用于您。

本信息可能包含技术方面不够准确的地方或印刷错误。本信息将定期更改；这些更改将编入本信息的新版本中。IBM 可以随时对本出版物中描述的产品和/或程序进行改进和/或更改，而不另行通知。

本资料中对非 IBM Web 站点的任何引用都只是为了方便起见才提供的，不以任何方式充当对那些 Web 站点的保证。那些 Web 站点中的资料不是此 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

IBM 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。

本程序的被许可方如果要了解有关本程序的信息以达到如下目的：(i) 支持在独立创建的程序与其他程序（包括本程序）之间进行信息交换，以及 (ii) 支持对已经交换的信息进行相互使用，那么应该与下列地址联系：

Intellectual Property Dept. for Security Software
IBM Corporation
5 Technology Park Drive
Westford, MA 01886
U.S.A.

只要遵守适当的条件和条款，包括某些情形下的一定数量的付费，都可获得这方面的信息。

本文档中描述的许可程序及其所有可用的许可资料均由 IBM 依据 IBM 客户协议、IBM 国际程序许可协议或任何同等协议中的条款提供。

此处所包含的任何性能数据都是在受控环境中测得的。因此，在其他操作环境中获得的结果可能会有明显的不同。有些测量可能是在开发级的系统上进行的，因此不保证与一般可用系统上进行的测量结果相同。此外，有些测量是通过推算而估计的。实际结果可能会有差异。本文档的用户应当验证其特定环境的适用数据。

涉及非 IBM 产品的信息可从这些产品的供应商、其出版说明或其他可公开获得的资料中获取。IBM 没有对这些产品进行测试，也无法确认其性能的精确性、兼容性或任何其他关于非 IBM 产品的声明。有关非 IBM 产品性能的问题应当向这些产品的供应商提出。

所有关于 IBM 未来方向或意向的声明都可随时更改或收回，而不另行通知，它们仅仅表示了目标和意愿而已。

本信息包含在日常业务操作中使用的数据和报告的示例。为了尽可能完整地说明这些示例，示例中可能会包括个人、公司、品牌和产品的名称。所有这些名字都是虚构的，若现实生活中实际业务企业使用的名字和地址与此相似，纯属巧合。

版权许可

本信息包括源语言形式的样本应用程序，这些样本说明不同操作平台上的编程方法。如果是为按照在编写样本程序的操作平台上的应用程序编程接口（API）进行应用程序的开发、使用、经销或分发为目的，您可以任何形式对这些样本程序进行复制、修改、分发，而无须向 IBM 付费。这些示例并未在所有条件下作全面测试。因此，IBM 不能担保或暗示这些程序的可靠性、可维护性或功能。样本程序"按现状"提供，不附有任何种类的保证。对于因使用样本程序而引起的任何损害，IBM 不承担任何责任。

凡这些实例程序的每份拷贝或其任何部分或任何衍生产品，都必须包括如下版权声明：

© (贵公司的名称) (年)。此部分代码是根据 IBM 公司的样本程序衍生出来的。© Copyright IBM Corp. 2000, 2015.

如果您正在查看本信息的软拷贝，图片和彩色图例可能无法显示。

商标声明

IBM、IBM 徽标和 ibm.com® 是 International Business Machines Corp. 在全球多个管辖区域内注册的商标和注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。IBM 商标的最新列表可在 Web 页面 www.ibm.com/legal/copytrade.shtml 上获取。

Adobe 是 Adobe 系统在美国和/或其他国家或地区设立的注册商标或商标。

Intel 和 Pentium 是 Intel Corporation 或其子公司在美国和其他国家或地区的商标或注册商标。

Microsoft、Windows 和 Windows NT是 Microsoft Corporation 在美国和/或其他国家或地区的商标。

UNIX 是 The Open Group 在美国和其他国家或地区的注册商标。

Java 和 JavaScript 是 Sun Microsystems, Inc. 在美国和/或其他国家或地区的商标。

其他产品和服务名称可能是 IBM 或其他公司的商标。

程序号：

SC43-3707-00