Rational®

IBM

AppScan Standard Edition 入门

目录

第 1 章 安装 AppScan

系统需求

硬件

硬件	最低需求
处理器	Pentium® P4, 2.4 GHz
内存	1 GB RAM
磁盘空间	10 GB
网络	1 NIC 100 Mbps（具有已配置的 TCP/IP 的网络通信）

操作系统和软件

软件	详细信息
操作系统	Windows® XP: Professional Edition, SP2 和 SP3 Windows 2003: Standard 和 Enterprise Edition, SP1 和 SP2 Windows Vista: Business、Ultimate 和 Enterprise Edition, SP1 支持 32 位和 64 位版本 **注**: Vista 不支持创建定制报告时使用的 Rational AppScan Smart 标记。
浏览器	Microsoft® Internet Explorer V6 或更高版本
其他	Microsoft .NET Framework V2.0 或更高版本（某些可选的其他功能需要 V3.0 或更高版本） （可选）在某些咨询中用于查看培训演示的 Adobe® Flash Player 9.0.124.0 或更高版本。 （可选）使用 AppScan® Smart 标记来插入定制报告模板字段的 Word 2003 或 2007。如果是 Word 2003，那么还须安装以下更新: Update for Office 2003 (KB907417): http://www.microsoft.com/downloads/details.aspx?FamilyId=1B0BFB35-C252-43CC-8A2A-6A64D6AC4670&displaylang=en （可选）关于扫描 Web Service，安装了 Rational AppScan 的通用服务客户机（GSC）可支持各种解密算法。但是，如果您的服务器需要某些高安全性加密模式，没有其他安全库（.jar 文件）的话，GSC 可能无法运行。 “BouncyCastle”（http://www.bouncycastle.org）是可能包含此类模式的安全库的提供者。

要点: 在 Rational AppScan 可以阻塞通信时，某个个人防火墙正在运行，导致不精确查找，从而降低性能。为了获得最佳结果，请不要在运行 Rational AppScan 的计算机上运行个人防火墙。

安装过程

1. 请关闭已打开的任何 Microsoft Office 应用程序。

   注: 如果已安装 Microsoft Word 2003 或更高版本，那么在安装期间，会将 Rational AppScan Smart 标记添加到它的 Smart 标记选项。创建定制报告模板时，可以将这些标记插入字段代码中。为了进行该操作，在安装期间，必须关闭 Microsoft Word 和其他任何使用标记的 Microsoft Office 程序（如 Microsoft Outlook）。

2. 启动 Rational AppScan 安装并遵循在线指示信息。“安装向导”会指导您快速简单地完成安装。

   注: 根据您的操作系统，可能需要 .NET Framework V2.0 或 V3.0，以运行 Rational AppScan。如果您有较早的版本，或尚未安装，那么会询问您是否想要安装必需版本。（如果选择**否**，那么安装会停止，因为如果没有正确版本的 .NET Framework，Rational AppScan 便无法正确运行。）

3. 将询问您是否要安装/下载 GSC（通用服务客户机）。如果要探索 Web Service 以配置 Web Service 扫描，那么 GSC 是必要的，但如果仅扫描 Web 应用程序，就不是必要的。
   - 如果 GSC 安装文件在本地可用，那么会询问您是否要安装 GSC。如果单击**是**，会安装 GSC，并完成 Rational AppScan 安装。
   - 如果 GSC 安装文件在本地不可用，那么会询问您是否要下载 GSC 并会完成 Rational AppScan 安装。要下载 GSC 安装文件，请单击**是**并将文件保存到计算机。下载完成后，双击该文件以安装 GSC，以便在扫描 Web Service 的过程中与 Rational AppScan 一起使用。

静默安装

您可以使用命令行和以下参数“静默地”安装 Rational AppScan:

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

注: 如果您的操作系统需要，静默安装将自动安装或更新 .NET Framework V2.0 或 V3.0。

要点: 如果在安装 Rational AppScan 时想要同时安装“通用服务客户机”（扫描 Web Service 所必需的，而非仅扫描 Web 应用程序所必需），您必须从包含两个安装（.exe）文件的文件夹中运行命令行。

参数	功能
/z	安装、修复或卸载 Rational AppScan 和（可选）GSC（通用服务客户机，扫描 Web Service 所必需的，而非仅扫描 Web 应用程序所必需）。 选项有: GSC（用于安装 GSC 和 Rational AppScan）、REPAIR（用于修复现有安装）和 REMOVE（用于卸载）。 如果不包括任何 /z 参数，那么仅安装 Rational AppScan（不带 GSC）。
/l	语言代码。选项有: 1033 用于安装 Rational AppScan 的英文版本（和 GSC），1041 用于安装日文版本，1042 用于安装韩文版本。
/s	激活“静默方式”（否则将启动常规安装）。不需要任何内容。
/v	设置安装 Rational AppScan 的路径。（修复或卸载不需要设置路径。） 路径必须位于 INSTALLDIR=\ 之后，并且用引号括起。路径可能包括空格。 示例: /v″INSTALLDIR=\″D:\Program Files\AppScan\″″ 如果您未定义此参数，那么安装将使用缺省路径: C:\Program Files\IBM\Rational AppScan\

示例。

- 要将 Rational AppScan 的英文版本安装在缺省目录中，请输入:

  ```
  AppScan_Setup.exe /l"1033" /s
  ```

- 要将 Rational AppScan 的日文版本和 GSC 安装在缺省目录中，请输入:

  ```
  AppScan_Setup.exe /z"GSC" /l"1041" /s
  ```

  注: 要将 GSC 包括在安装中，那么必须从包含 Rational AppScan 和 GSC 安装（.exe）文件的文件夹中运行此命令。

- 要将 Rational AppScan 的韩文版本安装在 D:\Program Files\AppScan\ 中，请输入:

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

- 要卸载:

  ```
  AppScan_Setup.exe /z"REMOVE" /s
  ```

许可证

Rational AppScan V7.9 安装包括允许扫描 IBM 定制设计的 AppScan 测试 Web 站点（但无其他站点）的缺省许可证。为了扫描您自己的站点，您必须安装 IBM® 提供的有效许可证。完成这一步后，Rational AppScan 将会装入并保存扫描和扫描模板，但不会在您的站点上运行新的扫描。

IBM Rational 许可证

从版本 7.8 开始，Rational AppScan 许可证的格式便为 FlexLM（*.upd），并且是从“Rational 许可证密钥中心”下载。IBM Rational 许可证的类型有两种，具体取决于您拥有的是 AppScan Standard Edition 还是 AppScan Express Edition:

Standard Edition 使用“浮动型”许可证
这些许可证安装在“IBM Rational 许可证服务器”上（该服务器可以是运行 AppScan 的机器）。使用 Rational AppScan 的任何服务器都必须使许可证服务器与网络连接。用户每次打开 AppScan 时都会检出许可证，而当关闭 AppScan 时又会将其检入。

Express Edition 使用“节点锁定型”许可证
这些许可证安装在运行 Rational AppScan 的机器上。会为每个许可证分配一个单独的机器。

原有许可证

如果您从 7.8 以前的产品版本进行升级，那么现有的许可证格式将不会是 FlexLM，而是 *.lic。只要有效，该许可证将继续用于新版本的 AppScan。

如果您想要将原有的许可证升级至 IBM Rational 许可证，那么可以通过单击**帮助 > 许可证 > 装入 IBM Rational 许可证**（这时会打开“许可证密钥管理员”）**> 许可证密钥 > 获取、返回或移动密钥**（这时会打开“许可支持”）**> 许可证密钥中心**，来执行这一操作。升级将使您能够使用“Rational 许可证密钥中心”来管理许可证。

要查看许可证状态:

1. 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 FlexLM 许可证（不管是在您的计算机上还是在其他网络服务器上），那么请单击此处以打开“Rational AppScan 许可证密钥管理员”，打开后便可以装入和管理许可证。
装入旧格式（.lic）的许可证	如果您拥有有效的旧格式 Watchfire 原有许可证（来自 7.8 版本以前的产品），那么请单击此处以将其装入。

查看许可协议	单击此处以查看许可协议。

2. 如果您装入了新的许可证，那么请单击  以刷新对话框中显示的许可证信息

测试运行

如果您拥有 Rational AppScan 的评估副本（例如，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。

第 2 章 基本原则

扫描步骤和扫描阶段

“Rational AppScan 全面扫描”包括两个步骤: “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”步骤**: 在第一个步骤中，会探索站点并构造应用程序树。这就是“探索”步骤。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”步骤**: 在“测试”步骤，AppScan 会发送其在“探索”步骤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”步骤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。）

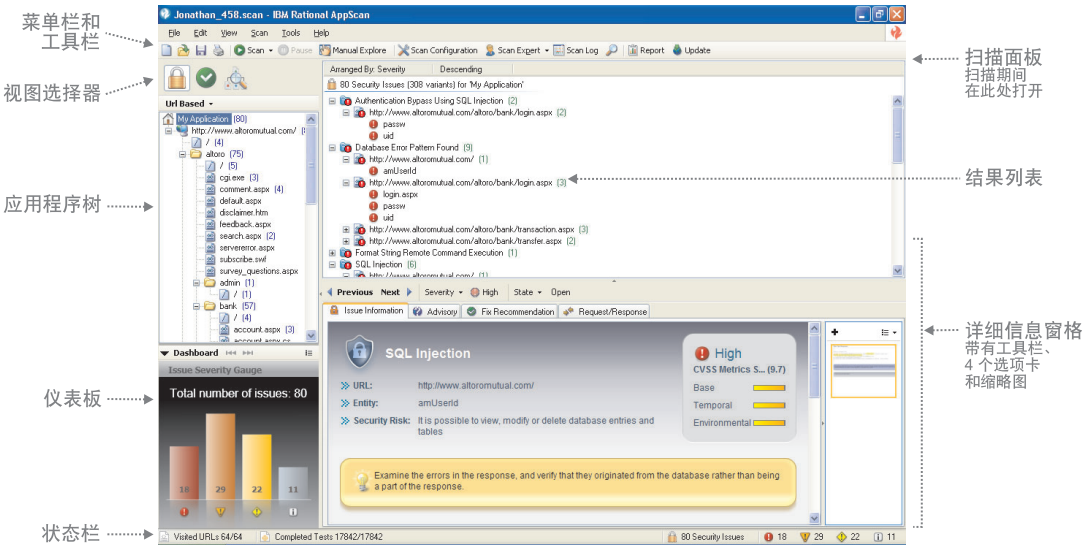
Web 应用程序与 Web Service

AppScan 既可以扫描 Web 应用程序，又可以扫描 Web Service。

- **Web 应用程序**: 如果是一般应用程序（不包含 Web Service），那么为 AppScan 提供起始 URL 和登录认证凭证可能足以使其能够测试站点。如有必要，您还可以手动搜寻站点，以使 AppScan 能够访问仅通过特定用户输入才能到达的区域。
- **Web Service**: 如果是 Web Service，那么集成的“通用服务客户机（GSC）”使用服务的 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”并用于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。
仪表板	以可连续“播放”的面板形式显示有关当前结果的信息。

工作流程

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 **Web 应用程序扫描**或 **Web Service 扫描**。
3. 使用该向导来设置扫描：

要扫描应用程序:

a. 输入起始 URL。

b. （推荐）手动执行登录过程。

c. （可选）复审“测试策略”。

要扫描 Web Service:

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，Rational 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**扫描专家**:
   a. 运行“扫描专家”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“扫描专家”以*自动*执行其分析并应用部分建议。
5. 启动自动扫描。
6. （可选）运行**结果专家**以处理扫描结果，并向“问题信息”选项卡（“详细信息”窗格）添加信息。
7. （可选）运行**恶意软件测试**以分析站点上页面和链接中的恶意或不必要的内容。

   注: “恶意软件测试”使用的数据是在常规扫描的“探索”步骤收集的数据，因此，您必须提供部分“探索”结果以便其能够运行。
8. “复审结果”用于评估站点的安全状态（“结果专家”可帮助您执行此操作），以及
   - 手动探索其他链接
   - 打印报告
   - 复审补救任务

第 3 章 扫描配置

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。

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**缺省值**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”（例如，哪一类别会用于扫描）。

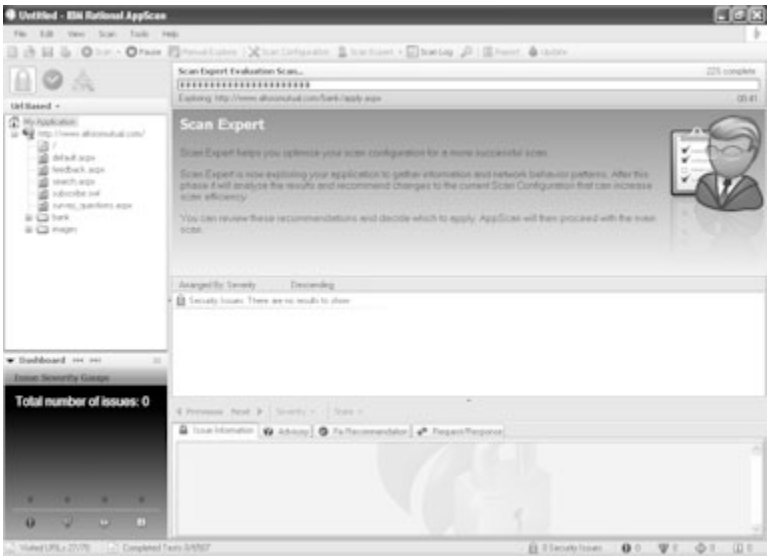
    注：缺省情况下，会使用所有除侵入式测试以外的测试。

    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“扫描专家”复选框，以便在完成向导时运行“扫描专家”。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。

扫描专家

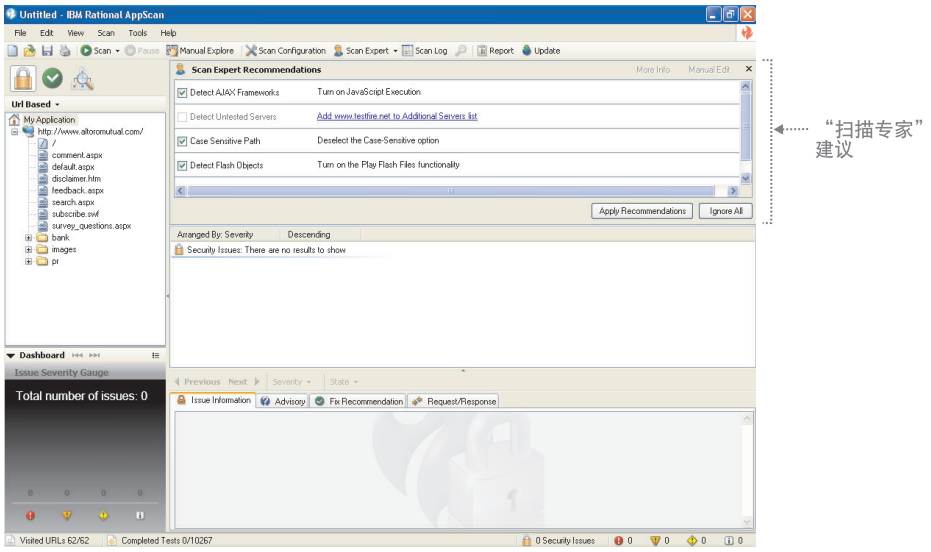
“扫描配置向导”中的其中一个选项适用于“扫描专家”，可指导其运行简短扫描，以评估特定站点的新配置的效率。

运行“扫描专家”时，会在屏幕的顶部打开“扫描专家”面板，并且由于“扫描专家”会探索站点，会开始在左边的窗格中显示应用程序树。



在简短评估结束时，“扫描专家”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：部分更改仅可由“扫描专家”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。



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。

1. 单击**扫描 > 手动探索**

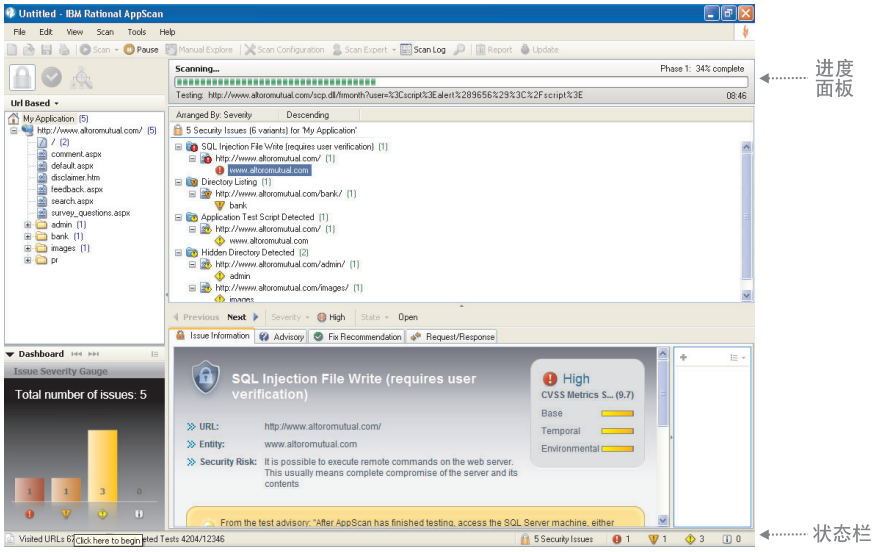
   这时会打开嵌入式浏览器。
2. 浏览站点，然后单击链接并按要求填写字段。
3. 完成后关闭浏览器。

   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**。

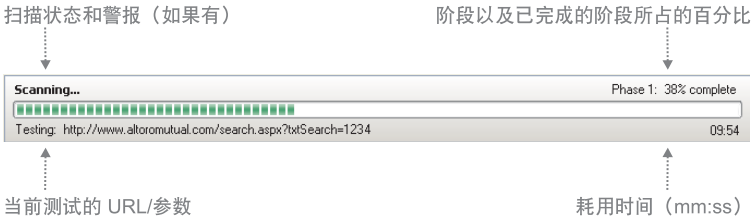
第 4 章 扫描

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

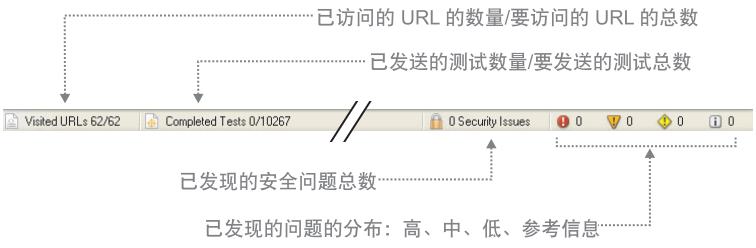
进度面板显示当前阶段的扫描以及正在进行测试的 URL 和参数。



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:



注: 在扫描过程中，要发送的测试总数或要访问的 URL 总数都可能会增加，因为会发现新链接。

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。

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。

	**“安全问题”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）
	**“补救任务”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。
	**“应用程序数据”视图**	显示来自“探索”步骤的脚本参数、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。

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。

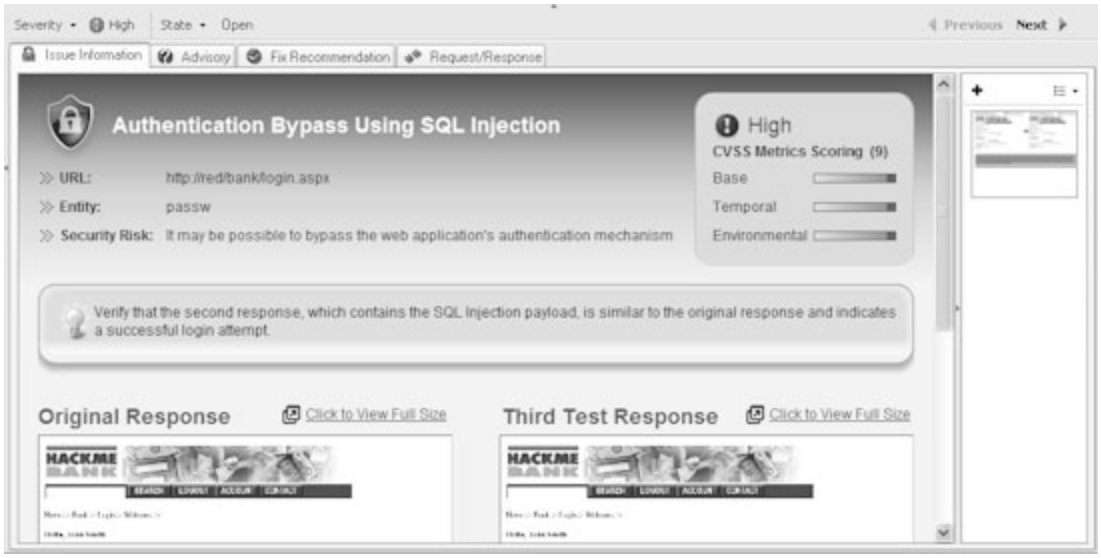
“安全问题”选项卡

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	在其他“详细信息”窗格选项卡上可用的信息摘要。其主要目的在于显示由“结果专家”添加的其他信息。此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**。

结果专家

“结果专家”由用于处理扫描结果的各种模块组成。处理的结果将添加到“详细信息”窗格的“问题信息”选项卡，以使显示的信息更加综合和详细，包括在相关处拍摄的屏幕快照。



“结果专家”通常在全面扫描之后自动运行，但是它也可在全面或部分扫描结果上随时手动运行。

若时间有限制，并且结果的数量很大，那么您可能要决定不运行“结果专家”，或者禁用它的一个或多个模块。

要更新所发现的所有问题的“问题信息”选项卡，请单击**工具 > 运行扫描专家**。

恶意软件测试

*恶意软件测试*功能会测试您应用程序中的恶意软件并链接到恶意的外部域。该功能通过分析从常规扫描的“探索”步骤获得的结果来执行此操作。在常规扫描或至少是常规扫描的“探索”步骤完成后，它会作为单独的一组测试运行。仅在存在现有“探索”结果时，*恶意软件测试*图标才处于活动状态。

该功能包含两个模块:

检查应用程序内容中的恶意软件

分析应用程序内容以及来自通向其他域的链接的可用内容中的恶意软件模式，如恶意的可执行代码。此模块可检查以下内容中的恶意模式:

- 所访问 URL 的内容
- 从外部链接检索到的内容
- 从常规扫描排除的文件类型

检查恶意的外部 Web 站点的链接

检查您的站点中通向其他域的所有链接（每个链接都会返回各自的 ISS 类别）。要执行此操作，需要因特网连接，以连接 ISS 数据库。

缺省情况下，会同时选择两个模块，但是您可以从“扫描配置”对话框对此进行调整。

要进行恶意软件测试:

1. 验证您是否拥有要测试的整个站点或部分站点的“探索”步骤结果。这些结果可以来自完整的常规扫描、“仅探索”或“手动探索”。
2. 要对配置进行任何更改，请单击**扫描 > 扫描配置 > 恶意软件**选项卡。
3. 单击工具栏上的  图标，或单击**扫描 > 恶意软件测试**。

这时会显示恶意软件进度对话框，当恶意软件测试完成时，会关闭该对话框。状态消息指示测试过程成功完成。

会将结果在“结果列表”中以其他“问题类型”的形式添加到常规扫描结果，并会将完整的详细信息添加到“详细信息窗格”。

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。）

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

Rational 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 Rational 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）进行报告。
	**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 工具栏摘要

工具栏上的按钮会提供对经常使用的功能的快速访问（也可从菜单中访问）。

按钮	名称	单击以:
	新建	选择模板，然后创建新的扫描。（可选择启动“扫描配置向导”。）
	打开	装入已保存的扫描或扫描模板。
	保存	保存当前扫描。
	打印	打印当前“视图”（安全问题、修复任务或应用程序数据）的“应用程序树”和“详细信息窗格”。节点会根据其在屏幕上的当前显示情况，呈现为展开或折叠状态。
	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”步骤）或继续已暂停的扫描。  仅探索: 仅运行“探索”步骤（或继续已暂停的“探索”），之后不需要进行“测试”步骤。  仅测试: 仅运行“测试”步骤（或继续已暂停的“测试”），不需要首先运行“探索”步骤。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，手动浏览该站点，按照要求填充必需的参数。然后，在为站点创建测试时，AppScan 将会把此“探索”数据添加到其自身自动收集的“探索”数据中。
	恶意软件测试	使用“扫描配置”对话框的“恶意软件”选项卡中配置的设置，来测试恶意软件和恶意的外部链接。此选项仅在有可以测试的部分“探索”结果时可用。
	扫描配置	打开“扫描配置”对话框，以配置扫描。
	扫描专家 >	运行“扫描专家”，以评估当前配置并提供更改建议。选择: 扫描专家评估 扫描专家仅分析（仅当已存在一些可供分析的“探索”结果时，该选项才可用。）
	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 Rational AppScan 所执行的所有操作。）

按钮	名称	单击以:
	查找	查找问题。（仅当已选定“问题”视图时才启用。）
	创建报告	使用当前扫描数据来创建报告。
	更新	检查并下载任何可用的 Rational AppScan 安全更新。