IBM Security AppScan Source for Analysis
V 9.0.3.7

用户指南

IBM Security AppScan Source for Analysis
V 9.0.3.7

用户指南

IBM

(C) Copyright IBM Corp. and its licensors 2003, 2017. All Rights Reserved.

IBM、IBM 徽标、ibm.com Rational、AppScan、Rational Team Concert、WebSphere 和 ClearQuest 是 International Business Machines Corp. 在全球多个管辖区域内的商标或注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。"版权和商标信息"Web 站点上提供了 IBM 商标的最新列表，网址为：http://www.ibm.com/legal/copytrade.shtml。 Linux 是 Linus Torvalds 在美国和/或其他国家或地区的注册商标。Microsoft、Windows、Windows NT 和 Windows 徽标是 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 和所有基于 Java 的商标和徽标是 Oracle 和/或其子公司的商标或注册商标。

本程序包括：Jacorb 2.3.0（Copyright 1997-2006 JacORB 项目）以及 XOM1.0d22 (Copyright 2003 Elliotte Rusty Harold)，上述各项均依据 Gnu Library General Public License (LGPL) 提供，该许可证的副本在本程序随附的"声明"文件中提供。

目录

© Copyright IBM Corp. 2003, 2017

第 1 章 AppScan Source for Analysis 介绍

本部分描述 AppScan® Source for Analysis 如何适应总体 AppScan Source 解决方案并提供用于了解软件保证工作流程的基础知识。

IBM Security AppScan Source 介绍

IBM® Security AppScan Source 向贵组织中每个对软件安全性产生影响的用户都提供最大的价值。无论您是安全分析人员、质量保证专员、开发人员还是执行人员，AppScan Source 产品都直接在桌面上提供您所需的功能、灵活性和能力。

产品集包括：

- **AppScan Source for Analysis**：用于配置应用程序和项目，扫描代码，对优先级漏洞进行分析、分类和操作的工作台。
- **AppScan Source for Automation**：使您能够在软件开发生命周期内将 AppScan Source 工作流的关键方面自动化并将安全性与构建环境相集成。
- **AppScan Source for Development**：Developer 插件将许多 AppScan Source for Analysis 功能都集成到 Microsoft Visual Studio、Eclipse 工作台和 Rational® Application Developer for WebSphere® Software (RAD) 中。这使软件开发者能在开发过程期间发现漏洞并对漏洞执行操作。Eclipse 插件使您能够可以扫描源代码以查找安全漏洞，并且您可以通过 Eclipse 插件来扫描 IBM MobileFirst Platform 项目。

为提高 AppScan Source 在贵组织中的价值，这些产品包含了以下组件：

- **AppScan Source 安全知识库**：关于各漏洞的上下文情报，提供关于根本原因、风险严重性和可行补救建议的准确描述。
- **AppScan Enterprise Server**：大多数 AppScan Source 产品和组件都必须与 AppScan Enterprise Server 通信。如果没有此服务器，那么可以在本地方式下使用 AppScan Source for Development - 但诸如定制规则、共享扫描配置和共享过滤器的功能将不可用。

  该服务器提供集中的用户管理功能，以及一种通过 AppScan Source 数据库共享评估的机制。该服务器包含可选的 Enterprise Console 组件。如果管理员安装该组件，那么您可从 AppScan Source for Analysis、AppScan Source for Automation 和 AppScan Source 命令行界面 (CLI) 向其发布评估。 Enterprise Console 提供各种用于处理评估的工具，例如报告功能、问题管理、趋势分析和仪表板。

  要点：对于 AppScan Source 和 AppScan Enterprise 的某些版本，两个产品的版本和发行版级别必须匹配才能从 AppScan Source 连接到 AppScan Enterprise Server。请参阅http://www.ibm.com/support/docview.wss?uid=swg21975211以了解 AppScan Source 和 AppScan Enterprise 的哪些版本是兼容的。

  注：

  – macOS 上不支持 AppScan Enterprise Server。

© Copyright IBM Corp. 2003, 2017

– 如果您拥有基本服务器许可证，那么只允许来自 AppScan 产品的最多十 (10) 个并发连接来访问该服务器。如果拥有特殊服务器许可证，那么将没有连接次数限制。

要点：扫描时，AppScan Enterprise Server 和 AppScan Source 客户机（AppScan Source for Development 除外）都需要直接连接到 AppScan Source 数据库（solidDB 或 Oracle）。

该软件产品不使用 cookie 或其他技术来和搜集个人可标识信息。

已翻译的本地语言

AppScan Source 用户界面提供以下语言版本：

- 英语
- 巴西葡萄牙语
- 简体中文
- 繁体中文
- 德语
- 西班牙语
- 法语
- 意大利语
- 日语
- 韩语
- 俄语

美国政府法规遵从性

遵从美国政府的安全和信息技术法规有助于消除销售障碍和壁垒。这还向全球潜在客户提供了一个证明点以表明 IBM 正在努力使其产品在行业中具有最高安全性。本主题列出了 AppScan Source 支持的标准和准则。

- 『因特网协议 V6 (IPV6)』
- 『联邦信息处理标准 (FIPS)』
- 第 3 页的『美国国家标准技术学会 (NIST) 特殊规范 (SP) 800-131a』
- 第 3 页的『配置为使用美国政府配置基线 (USGCB) 的 Windows 7 机器』

因特网协议 V6 (IPV6)

AppScan Source 支持 IPV6，但以下情况例外：

- 不支持输入 IPv6 数字地址，必须输入主机名。支持输入 IPv4 数字地址。
- 连接到 Rational Team Concert™ 时不支持 IPv6。

联邦信息处理标准 (FIPS)

在 AppScan Source 支持的 Windows 和 Linux 平台上，AppScan Source 通过使用经 FIPS 140-2 验证的加密模块和批准的算法来支持 FIPS 规范 140-2。在 AppScan Source 所支持的 macOS 平台上，需要执行几个手动步骤才能以 FIPS 140-2 方式运行。

要了解关于 AppScan Source FIPS 合规性的背景信息以及了解如何启动和禁用 AppScan Source FIPS 140-2 方式，请参阅以下技术说明：

- Operating AppScan Source version 8.7 or later in FIPS 140-2 mode on macOS
- How to enable/disable/verify FIPS 140-2 mode in AppScan Source (Linux and Windows)
- Background information about AppScan Source version 8.7 or later FIPS 140-2 support

美国国家标准技术学会 (NIST) 特殊规范 (SP) 800-131a

NIST SP 800-131A 准则提供加密密钥管理指导。这些准则包括：

- 密钥管理过程。
- 如何使用密码算法。
- 要使用的算法及其最小强度。
- 安全通信的密钥长度。

政府部门和金融机构使用 NIST SP 800-131A 准则来确保产品满足特定安全需求。

仅当 AppScan Source 在以 FIPS 140-2 方式运行时，才支持 NIST SP 800-131A。要了解如何启用和禁用 AppScan Source FIPS 140-2 方式，请参阅第 2 页的『联邦信息处理标准 (FIPS)』。

要点：如果您将要连接到的 AppScan Enterprise Server 支持 NIST 800-131a 合规性，那么必须将 AppScan Source 设置为强制使用传输层安全性 V1.2。如果未强制使用传输层安全性 V1.2，那么与服务器的连接将失败。

- 如果**未**安装 AppScan Source 数据库（例如，如果仅安装了客户机组件），那么可以通过修改 `<data_dir>\config\ounce.ozsettings`（其中 `<data_dir>` 是 AppScan Source 程序数据的位置，如第 275 页的『安装和用户数据文件位置』中所述） 来强制使用传输层安全性 V1.2。在此文件中，找到以下设置：

  ```
  <Setting
        name="tls_protocol_version"
        read_only="false"
        default_value="0"
        value="0"
        description="Minor Version of the TLS Connection Protocol"
        type="text"
        display_name="TLS Protocol Version"
        display_name_id=""
        available_values="0:1:2"
        hidden="false"
        force_upgrade="false"
   />
  ```

  在此设置中，将 `value="0"` 更改为 `value="2"`，然后保存文件。

- 如果您安装了 AppScan Source 数据库，请在安装 AppScan Source 以及 Enterprise Server 之后，在 IBM Security AppScan Enterprise Server 数据库配置工具中强制使用传输层安全性 V1.2。

配置为使用美国政府配置基线 (USGCB) 的 Windows 7 机器

AppScan Source 支持在使用 USGCB 规范来配置的 Windows 7 机器上扫描应用程序。

注：在使用 USGCB 规范来配置的机器上，AppScan Source 不支持将缺陷跟踪系统与 HP Quality Center 或 Rational ClearQuest® 集成。

AppScan Source 新增内容

探索已添加到 AppScan Source 的以下新功能，并请注意该发行版中已不推荐使用的任何功能部件和功能。

AppScan Source V9.0.3.7 中的新增内容

增强的和新的扫描支持

- 支持 Red Hat Enterprise Linux (RHEL) V7.3 操作系统。
- 支持将 AppScan Source for Development Visual Studio 插件 应用于 Visual Studio 2015。

AppScan Source V9.0.3.7 中不再支持的功能和特性

从 AppScan Source V9.0.3.7 开始：

- 不再支持 OS X V10.10 操作系统。
- 不再支持 Xcode V6.3。不再支持通过该版本 Xcode 扫描 Objective-C 项目。
- 不再支持 Tomcat V5 和 V6。

AppScan Source V9.0.3.6 中的新增内容

增强的和新的扫描支持

- 用于 Objective-C 的 Xcode 8.1 和 8.2（仅用于 iOS 应用程序）现在是 macOS 上受支持的编译器。对这些 Xcode 版本的支持可追溯到 AppScan Source V9.0.3.5。

AppScan Source V9.0.3.6 中不再支持的功能和特性

从 AppScan Source V9.0.3.6 开始：

- 不再支持 Red Hat Enterprise Linux V5 操作系统。
- Oracle WebLogic Server V8、V9 和 V10 不再是受支持的编译器。

AppScan Source V9.0.3.5 中的新增内容

- 『增强的和新的扫描支持』
- 『Java 源和字节码的增量扫描支持实现了更高的效率和更快的重新扫描。』

增强的和新的扫描支持

- macOS V10.12 现在是受支持的操作系统。对 macOS V10.12 的支持现在可追溯到 AppScan Source V9.0.3.4。
- 用于 Objective-C 的 Xcode 8.0、8.1 和 8.2（仅用于 iOS 应用程序）现在是 macOS 上受支持的编译器。

Java 源和字节码的增量扫描支持实现了更高的效率和更快的重新扫描。

从 V9.0.3.5 开始，可在 Windows 和 Linux 上启用 Java 增量扫描支持。启用增量分析时，AppScan Source 将对分析数据进行高速缓存。重新扫描项目或应用程序时，AppScan Source 使用该数据来确定代码更改，并将再次分析受更改影响的代码部分。最终的结果是代码的完整分析，但只是一小部分时间中的结果。

使用 IBM Security AppScan Source for Analysis、AppScan Source for Development Eclipse 插件、IBM Security AppScan Source for Automation 或 IBM Security AppScan Source 命令行界面 (CLI) 时，支持该功能。

AppScan Source V9.0.3.4 中的新增内容

- 『增强的和新的扫描支持』
- 『当通过常用访问卡 (CAC) 进行认证时现在支持将评估发布到 AppScan Enterprise Console』
- 第 6 页的『支付卡行业数据安全标准 (PCI DSS) V3.2 报告』
- 第 6 页的『AppScan Source for Analysis 产品文档』
- 第 7 页的『能够使用 AppScan Source for Analysis 中的扫描配置来除去任何 排除过滤器的结果』
- 第 7 页的『在 AppScan Source for Automation 和 AppScan Source 命令行界面 (CLI) 中扫描 WAR 和 EAR 文件时改进了库的处理』
- 第 7 页的『将 AppScan Source 评估提交到云以进行分析』
- 第 7 页的『AppScan Source V9.0.3.4 中不再支持的功能和特性』

增强的和新的扫描支持

PHP V7.0 现在可在 Windows 和 Linux 上的 IBM Security AppScan Source for Analysis、IBM Security AppScan Source for Automation 和 IBM Security AppScan Source 命令行界面 (CLI) 中被扫描。

当通过常用访问卡 (CAC) 进行认证时现在支持将评估发布到 AppScan Enterprise Console

如果要使用 CAC 认证连接到 AppScan Enterprise Server，现在可将评估从 AppScan Source 用户界面、AppScan Source 命令行界面 (CLI)和 AppScan Source for Automation 发布到 AppScan Enterprise Console。

支付卡行业数据安全标准 (PCI DSS) V3.2 报告

AppScan Source 现在支持支付卡行业数据安全标准 (PCI DSS) V3.2 报告。

AppScan Source for Analysis 产品文档

从 V9.0.3.4 开始，当您使用 AppScan Source for Analysis 中的**帮助** > **帮助内容**菜单项时，AppScan Source at IBM Knowledge Center 的联机帮助将打开（对于 V9.0.3.4，帮助将打开到 IBM Security AppScan Source V9.0.3.4 文档）。类似地，当您从 AppScan Source for Analysis"欢迎"视图访问链接时，它们将在 IBM Knowledge Center 上打开。

AppScan Source for Analysis 还提供了许多视图、首选项页面和对话框的上下文相关帮助。上下文相关帮助的键盘快捷键在 Windows 上为 F1，在 Linux 上为 Shift+F1，在 macOS 上为 command+F1。从 V9.0.3.4 开始，该上下文相关帮助还将打开到 IBM Knowledge Center 上的 AppScan Source。

如果要在没有因特网连接的情况下使用产品，帮助可在本地使用，方法如下：

- IBM Security AppScan Source"自述和发行说明"在位于 AppScan Source 安装目录中的 `readme.html` 文件中。
- 这些 PDF 用户指南安装在 AppScan Source 安装目录的 `doc/<lang>` 或 `doc\<lang>` 目录中（其中 `<lang>` 是 AppScan Source 安装的本地语言）：
  - 仅 Windows 和 Linux：*IBM Security AppScan Source for Analysis* 用户指南 (`Security_AppScan_Source_Analysis.pdf`)
  - 仅 Windows 和 Linux：*IBM Security AppScan Source Utilities* 用户指南 (`Security_AppScan_Source_Utilities.pdf`)
  - 仅 macOS：*IBM Security AppScan Source for Analysis* 用户指南 *macOS* 版 (`Security_AppScan_Source_Analysis_OSX.pdf`)
  - 仅 macOS：*IBM Security AppScan Source Utilities* 用户指南 *macOS* 版 (`Security_AppScan_Source_Utilities_OSX.pdf`)
  - *IBM Security AppScan Source* 安装和管理指南 (`Security_AppScan_Source_Installation_and_Administration.pdf`)

  您必须具有 Adobe Acrobat Reader 才能阅读这些文件。如果您没有 Acrobat Reader 副本，那么可以从 http://www.adobe.com/ 进行下载。
- 某些 AppScan Source for Analysis 功能的 Javadoc 位于 AppScan Source 安装目录的 `doc/Javadoc` 或 `doc\Javadoc` 目录中。从 V9.0.3.4 开始，这些功能的 Javadoc 可用：
  - 应用程序服务器导入框架 API 类和方法的 Javadoc 在 `doc/Javadoc/appserverimporter` 或 `doc\Javadoc\appserverimporter` 中提供。
  - 框架 API 类和方法的框架的 Javadoc 在 `doc/Javadoc/frameworks` 或 `doc\Javadoc\frameworks` 中提供。

  在这些文件夹中，打开 `index.html` 文件。

能够使用 AppScan Source for Analysis 中的扫描配置来除去任何 排除过滤器的结果

排除过滤器包含了用于从结果中移除漏洞类型、应用程序编程接口 (API)、文件、目录、项目或跟踪规则的规则。如果在扫描配置中包含多个排除过滤器，那么有可能它们彼此冲突并影响结果。例如，假定有以下两个过滤器：

- 过滤器 1 除去漏洞类型 Validation.EncodingRequired 的所有结果。它不是反向的，因此将从评估排除这些结果。
- 过滤器 2 除去漏洞类型 Validation.Required 的所有结果。它不是反向的，因此将从评估排除这些结果。

如果使用扫描配置时应用了这两个过滤器，那么缺省情况下它们会将彼此排除掉。过滤器 1 将排除 Validation.EncodingRequired 结果，但它将包含 Validation.Required 结果。过滤器 2 将排除 Validation.Required 结果，但它将包含 Validation.EncodingRequired 结果。最终的结果是将包含所有 Validation.EncodingRequired 和 Validation.Required 结果。

从 V9.0.3.4 开始，可移除通过在创建扫描配置时选择**与任何非反转排除过滤器匹配**指定的任务*any*排除过滤器的结果。该复选框位于"扫描配置"视图**常规**选项卡的**过滤器信息**部分中。在上述的示例中，如果选择了该复选框，那么将从评估排除所有 Validation.EncodingRequired 和 Validation.Required 结果。

在 AppScan Source for Automation 和 AppScan Source 命令行界面 (CLI) 中扫描 WAR 和 EAR 文件时改进了库的处理

扫描 WAR 文件时，提供了以下设置：

- -include_all_lib_jars：使用该设置可在扫描期间在 WAR 文件中包含所有库。
- -include_lib_jars：使用该设置可在 WAR 文件中指定扫描期间想要包含的库。

导入 EAR 文件时，将自动创建用于存储共享库的项目。如果没有共享库，那么将创建项目，但项目将为空。-no_ear_project 设置现在可用，使用该设置后，将不会为 EAR 文件创建项目。

将 AppScan Source 评估提交到云以进行分析

如果预订了 IBM Cloud Marketplace 上的 IBM Application Security on Cloud 或预订了 Application Security on Cloud for Bluemix，可在此处提交 AppScan Source 评估以进行分析。支持 AppScan Source V9.0 或更高版本的评估，可提交的扫描数取决于 Application Security on Cloud 预订。请参阅http://www.ibm.com/support/knowledgecenter/SSYJJF_1.0.0/ApplicationSecurityonCloud/src_managing_assessments_cloud.html以了解更多信息。

AppScan Source V9.0.3.4 中不再支持的功能和特性

从 AppScan Source V9.0.3.4 开始：

- 不再支持 OS X V10.9 操作系统。
- 不再支持 Xcode V5.x、6.0 和 6.2。不再支持扫描具有这些版本 Xcode 的 Objective-C 项目。
- 对扫描 PHP V5.3 和 5.4 的支持已不推荐使用。

AppScan Source V9.0.3.3 中的新增内容

新平台和集成解决方案支持

从 AppScan Source V9.0.3.3 开始：

- Microsoft Windows 10 现在是受支持的操作系统。这包括 Windows 10 Education、Enterprise 和 Pro 版本。

  注：

  – 在 Windows 10，AppScan Source 安装程序 (AppScanSrc_Installer.exe file) 必须在 Windows 7 兼容性方式下运行。在 Windows 10 上，还必须将 AppScan_Uninstaller.exe 文件上设置为在 Windows 7 兼容性方式下运行，然后才能卸载 AppScan Source。该文件位于 <install_dir>\Uninstall_AppScan\AppScan_Uninstaller.exe（其中 <install_dir> 是 AppScan Source 安装位置，如第 275 页的『安装和用户数据文件位置』中所述） 中。请参阅 http://www.ibm.com/support/docview.wss?uid=swg21696098以获取更多信息。

  – Windows 10 支持受 http://www.ibm.com/support/docview.wss?uid=swg21689814中描述的问题影响。

- 如果要连接到 AppScan Enterprise Server V9.0.3.1 或更高版本，IBM Security AppScan Source 数据库 可安装到 Oracle 12c 数据库。

  要点：如果具有使用 Oracle 11g 数据库的 AppScan Source 的现有安装，而且想要升级到 Oracle 12c，必须首先升级 AppScan Source，然后才能升级 Oracle 数据库。

- **Tomcat 8** 包含在 AppScan Source 的安装中。
- Visual Studio 2015 解决方案和项目文件现在可在 AppScan Source for Analysis, AppScan Source for Automation 以及 AppScan Source 命令行界面 中进行扫描。如果您具有已在 Visual Studio 2015 中创建的 .sln 或 .vcproj 文件，那么在 Windows 上使用 AppScan Source for Analysis、AppScan Source for Automation或 AppScan Source 命令行界面 时可导入和扫描这些文件。

  要点：

  – 不支持将 AppScan Source for Development Visual Studio 插件 应用于 Visual Studio 2015。

  – 受管 C++ 项目受支持。如果不受管 C++ 项目是通过 Visual Studio 2013 或较低版本中的 Platform Toolset（Platform Toolset V120 或更低版本）构建的，那么支持这些不受管 C++ 项目。

- Xcode 7.3 for Objective-C（仅针对 iOS 应用程序）现在是 macOS 上受支持的编译器（Xcode 7.3 的支持也对于 AppScan Source V9.0.3.2 有效）。

增强的和新的扫描支持

- PHP V5.5 和 5.6 现在可在 Windows 和 Linux 上的 IBM Security AppScan Source for Analysis、IBM Security AppScan Source for Automation 和 IBM Security AppScan Source 命令行界面 (CLI) 中被扫描。
- 使用 AppScan Source 来扫描 Java™ 时，`@ValidatorMethod`、`@CallbackMethod` 和 `@SuppressSecurityTrace` 方法级别注释现在也受支持。

Windows 的新安装文件名

在 Windows 上，安装文件名称已从 `setup.exe` 更改为 `AppScanSrc_Installer.exe`。

Windows 的通用访问卡 (CAC) 支持

通用访问卡 (http://www.cac.mil) 是美国的现役军人、后备役、DoD 平民雇员和有资格的承包商人员的统一标识。持卡人可以进入大楼和受控空间，并可访问 DoD 计算机网络和系统。CAC 可以用于访问配备了各种智能卡读卡器的计算机和网络。将 CAC 插入读卡器时，设备将要求用户输入 PIN。

如果要在 Windows 上运行 AppScan Source 并连接到启用了通用卡 (CAC) 认证的 AppScan Enterprise Server Ve9.0.3.1 iFix-001 或更高版本，AppScan Source 现在支持 CAC 认证。

DISA 应用程序安全和开发 STIG V3R10 报告支持

AppScan Source 现在支持 Defense Information Systems Agency (DISA) 应用程序安全和开发 Security Technical Implementation Guide (STIG) V3R10 报告。

AppScan Source V9.0.3.2 中的新增内容

AppScan Source 和 AppScan Enterprise 版本兼容性

当连接到 AppScan Enterprise Server 或发布到 AppScan Enterprise Console 时，AppScan Source 的某些版本不再需要 AppScan Source 和 AppScan Enterprise 版本和发行版级别匹配。请参阅http://www.ibm.com/support/docview.wss?uid=swg21975211以了解 AppScan Source 和 AppScan Enterprise 的哪些版本是兼容的。

这些更改可追溯到 AppScan Source 的某些先前版本，如http://www.ibm.com/support/docview.wss?uid=swg21975211中所述。

AppScan Source V9.0.3.1 中的新增内容

- 『新集成解决方案支持』
- 第 10 页的『在 AppScan Source for Automation 和 AppScan Source 命令行界面 (CLI) 中扫描 WAR 和 EAR 文件』

新集成解决方案支持

从 AppScan Source V9.0.3.1 开始：

- 现在支持 Tomcat 8 来编译 Java 和 JSP。

  注：操作系统支持取决于个别编译器支持的操作系统。

- 用于 Objective-C 的 Xcode 7.0、7.1 和 7.2（仅用于 iOS 应用程序）现在是 macOS 上受支持的编译器。

在 AppScan Source for Automation 和 AppScan Source 命令行界面 (CLI) 中扫描 WAR 和 EAR 文件

CLI 中的 openapplication (oa) 命令现在可用于打开 WAR 和 EAR 文件。此外，可在 AppScan Source for Automation 中使用 ScanApplication 命令来扫描这些文件。

AppScan Source V9.0.3 中的新增内容

新平台和集成解决方案支持

从 AppScan Source V9.0.3 开始，支持以下操作系统：

- Red Hat Enterprise Linux V6 Updates 6 和 7
- OS X V10.11。对 OS X V10.11 的支持可追溯到 AppScan Source V9.0.2，并在 http://www.ibm.com/support/docview.wss?uid=swg21968948中描述了相关限制（该限制仅影响 AppScan Source V9.0.2）。

此外：

- Objective-C 的 Xcode 6.3 和 6.4（仅针对 iOS 应用程序）现在是 OS X 平台上受支持的编译器（对 Xcode 6.3 和 6.4 的支持也对于 AppScan Source V9.0.2 有效）。请注意：对于 Xcode 6.3 和 6.4 支持，也存在某些限制。请参阅http://www.ibm.com/support/docview.wss?uid=swg21962208以获取详细信息。这些限制不适用于 AppScan Source V9.0.3.1 和更高版本。
- AppScan Source for Development Eclipse 插件 现在与 IBM MobileFirst Platform Foundation V7.1 集成。现在可扫描 AppScan Source 产品中的 IBM MobileFirst Platform V7.1 项目、应用程序、环境和 HTML 文件。
- 可扫描 Rational Application Developer for WebSphere Software (RAD) V9.1.1 项目文件和工作空间，而且 AppScan Source for Development（Eclipse 插件） 可应用于 RAD V9.1.1。
- 可扫描 Eclipse V4.5 项目文件和工作空间（仅 Java 和 IBM MobileFirst Platform），AppScan Source for Development（Eclipse 插件） 可适用于 Eclipse V4.5。
- 现在支持 IBM WebSphere Application Server V8.5.5 来编译 Java 和 JSP。

  注：操作系统支持取决于个别编译器支持的操作系统。

扫描配置增强功能

"扫描配置"视图已重新设计，现在可提供以下功能：

- 指定过滤器的功能。
- 设置扫描过程中执行的分析类型。这包含污染流分析和基于模式的分析。

AppScan Source 现在包含内置扫描配置：Web 预览扫描、Web 快速扫描、Web 平衡扫描和 Web 深度扫描。

新规则属性使您能够更准确地识别号严重性明确安全结果。

AppScan Source 的该发行版引入了 `Attribute.Likelihood.High` 和 `Attribute.Likelihood.Low` 属性。这些属性已添加到内置规则，而还可在创建定制规则时使用。

在 AppScan Source 中，*likelihood* 代表安全结果可被利用的可能性和机会。AppScan Source 采用 https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology#Step_2:_Factors_for_Estimating_Likelihood上提供的发生可能性的定义，并通过基于跟踪属性确定发生可能性来对其进行优化。通过提供一组跟踪属性（例如源 API 名称、源 API 类型、源技术或源机制），AppScan Source 确定将来可能或将要通过使用特定脆弱性来利用跟踪的可能性。

发生可能性与跟踪的源元素联系紧密。源是对程序的输入，如文件、servlet 请求、控制台输入或套接字。对于大多数输入源，返回的数据在内容和长度方面没有限制。当输入未检查时，将被认为是污染源。

发生可能性的示例包括：

- 如果提供了 HTTP 源的跟踪（例如 `Request.getQueryString`）和跨站点脚本编制接收器（例如 `Response.write`），那么将确定较高的可能性，因此提高结果的置信度。
- 如果提供了系统属性源的跟踪（例如 `getProperty`）和跨站点脚本编制接收器（例如 `Response.write`），那么将确定较低的可能性，因此降低结果的置信度。

发生可能性用于识别必须立即进行操作或修订的高优先级可操作结果。它与高度可利用的污染源关系紧密，并为您提供了为结果分类的细粒度更高的方法。发生可能性在 AppScan Source 脆弱性数据库中存储为与污染源关系紧密的属性。该功能是现成可用的。

我们已进行了大量的搜索来确定源的发生可能性因子。通过使用"定制规则向导"，可将发生可能性信息添加到您添加到规则库的新污染源。这将改进从扫描生成的结果的分类，并因此提高整体类选工作流程的效率。

在"定制规则向导"中，可为**发生可能性**属性设置两个值（**高**和**低**）。值**高**意味着源非常容易被污染。换句话讲，污点进入系统的障碍非常低，使攻击者能够非常容易地手动或自动地提交恶意数据。值**低**意味着通过该源输入恶意数据的障碍非常高。这可意味着要向源引入污点， 攻击者必须更深入的了解系统，而且必须具有能在受害者网络上进行操作的许可权。

注：由于这些规则属性，如果已在 AppScan Source 的先前版本中生成了评估，那么在 V9.0.3 中进行扫描时可能发现某些源的结果分类已更改。有关更多信息，并且要了解如何禁用这些规则属性，请参阅与这些更改相关的迁移注意事项。

自动丢失的接收器解决保证了更好的扫描结果

AppScan Source 现在通过自动推断丢失的接收器方法（例如 getter、setter 和返回布尔值的其他方法）来尝试解析跟踪中的丢失的接收器。这允许对代码进行更完整的分析，并提高了丢失的接收器解决。

注：由于这些功能部件，如果已在 AppScan Source 的先前版本中生成了评估，那么可能注意到未解析的丢失的接收器的结果中的更改。有关更多信息，并且要了解如何禁用自动标记生成，请参阅与这些更改相关的迁移注意事项。

增强的和新的扫描支持

- PHP V5.4 现在可在 Windows 和 Linux 上的 IBM Security AppScan Source for Analysis、IBM Security AppScan Source for Automation 和 IBM Security AppScan Source 命令行界面 (CLI) 中被扫描。
- AppScan Source 现在包含 Spring MVC 4 框架的内置支持。
- **Java 扫描优化：**
  - 扫描 JavaServer Pages 时，现在可选择扫描预先编译的类文件而不是在扫描之间编译这些文件。要在 AppScan Source for Development Eclipse 插件 中扫描预先编译的类文件，配置安全性扫描的项目（选择**安全性分析** > **配置扫描** > **配置安全性项目**）并选择**预编译类**复选框。要在 IBM Security AppScan Source for Analysis 中扫描预编译类文件，选择以下某个位置中的**预编译类**复选框。
    - 项目属性中的"项目依赖关系"选项卡。
    - 创建新项目或应用程序时的"Java 项目依赖关系"。
  - 扫描 Java 时，AppScan Source 现在将扫描缺少依赖关系的 Java 文件和 Java 字节代码，或扫描编译错误。如果缺少依赖关系或存在编译错误，关于这些错误的信息将写入到日志文件。通过该信息，然后可向项目属性添加依赖关系，重新扫描，并实现扫描结果的完全覆盖。
- 从 AppScan Source V9.0.3 开始，将在导入和扫描 Xcode 项目时更准确地确定标题位置和配置选项。该更改引入了 `xcodebuild -dry-run` 的使用来获取每个文件的构建配置，因此当 AppScan Source 在继续之前确定文件配置时扫描开头可能会出现暂停。

AppScan Source V9.0.3 中不再支持的功能和特性

在 AppScan Source V9.0.3 中：

- 不再支持 OS X V10.8 操作系统。
- 不再支持 Xcode V4.6。不再支持通过该版本 Xcode 扫描 Objective-C 项目。
- 不在支持 Eclipse V3.6 和 V3.7 项目文件和工作空间，AppScan Source for Development（Eclipse 插件） 可不再适用于 Eclipse V3.6 和 V3.7。
- 不再支持 Rational Application Developer for WebSphere Software (RAD) V8.0.x 项目文件和工作空间，IBM Security AppScan Source for Development plug-in for IBM Rational Application Developer for WebSphere Software (RAD) 可不再适用于 RAD V8.0.x。
- IBM Rational Team Concert V3.0 和 V3.0.1 不再是受支持的缺陷跟踪系统。
- WebSphere Application Server V6.1 不再是受支持的应用程序服务器。
- 对扫描 PHP V4.x 到 5.2 的支持已不推荐使用。

迁移到 AppScan Source 的当前版本

本主题包含了已对 AppScan Source 的此版本所做更改的迁移信息。如果您是从 AppScan Source 的较低版本进行升级，请确保留意所升级 AppScan Source 版本以及引向此当前版本的所有版本的更改。

- 『从 V9.0.2 迁移』
- 第 14 页的『从 V9.0 迁移』
- 第 14 页的『从 V8.7 迁移』

从 V9.0.2 迁移

- 『新规则属性可能导致现有扫描中的结果分类更改。』
- 『自动丢失的接收器生成』

新规则属性可能导致现有扫描中的结果分类更改。

在 V9.0.2 之后，引入了 Attribute.Likelihood.High 和 Attribute.Likelihood.Low 规则属性。使用这些属性时，AppScan Source 可更准确地确定结果是确定的和/或可疑的。因此，如果扫描 AppScan Source V9.0.2 中的源代码，可能发现在 V9.0.2 之后的产品版本中扫描相同源代码时某些结果分类将更改。对于与可高度利用的 web 源或者对于不太可利用的属性或环境源，这一点是最突出的。

缺省情况下，将使用这些规则属性。可禁用这些规则属性，如下所示：

1. 在文本编辑器中打开 <data_dir>\config\ipva.ozsettings（其中 <data_dir> 是 AppScan Source 程序数据的位置，如第 275 页的『安装和用户数据文件位置』中所述）。找到文件中的 allow_likelihood 设置。此设置将与以下类似：

   ```
   <Setting
     name="allow_likelihood"
     value="true"
     default_value="true"
     description="Allow the processing of the Likelihood
       attributes to help determine trace confidence based
       on the source API"
     display_name="Allow Likelihood"
     type="bool"
   />
   ```

   在该设置中，修改 value 属性。如果属性设置为 true，该设置将打开。如果设置为 false，那么 AppScan Source 将不会在扫描期间使用这些规则属性。
2. 在修改该设置后保存文件，并启动或重新启动 AppScan Source。

自动丢失的接收器生成

在 V9.0.2 之后，针对在 getters/setters 和返回布尔值的方法中结束的跟踪引入了自动丢失的接收器解决。这通过自动推断这些应用程序编程接口 (API) 的标记来完成。因此，如果扫描 AppScan Source V9.0.2 中的源代码，可能注意到在 V9.0.2 之后的产品版本中扫描相同源代码时包含未解析的丢失的接收器的结果中的更改。

缺省情况下，自动标记生成已打开。如果想要使用其他方式的丢失的接收器解决（例如定制规则），可禁用该选项，如下所示：

1. 在文本编辑器中打开 <data_dir>\config\ipva.ozsettings（其中 <data_dir> 是 AppScan Source 程序数据的位置，如第 275 页的『安装和用户数据文件位置』中所述）。找到文件中的 automatic_lost_sink_resolution 设置。此设置将与以下类似：

```
<name="automatic_lost_sink_resolution"
  value="true"
  default_value="true"
  description="This setting tries to perform automatic
    lost sink resolution by assuming taint propagation
    for getters, setters and APIs which return boolean
    with no arguments."
  display_name="Auto Lost Sink Resolution"
  type="bool"
/>
```

   在该设置中，修改 value 属性。如果属性设置为 true，该设置将打开。如果设置为 false，那么 AppScan Source 将不会自动生成这些方法的标记。

2. 在修改该设置后保存文件，并启动或重新启动 AppScan Source。

从 V9.0 迁移

AppScan Enterprise Server 认证：关于将 IBM Rational Jazz™ 用户认证组件替换为 IBM WebSphere Liberty 的迁移注意事项

- **从仅具有本地 Jazz 用户的 Enterprise Server 迁移**：在此升级方案中，先前的 Jazz 用户将作为 AppScan Enterprise Server 用户出现在 AppScan Source 数据库中，但他们将无效。可以从数据库中移除这些用户，或者也可以将其转换为 AppScan Source 用户（如果按照 http://www.ibm.com/support/docview.wss?uid=swg21686347 中关于如何启用该转换的指示信息进行操作）。
- **从已配置 LDAP 的 Enterprise Server 迁移**：在 Enterprise Server 升级期间，可以选择再次为 Enterprise Server 配置 LDAP。如果执行此操作，那么现有用户在 AppScan Source 中仍将有效。
- **从已配置 Windows 认证的 Enterprise Server 迁移**：如果 Enterprise Server 已配置 Windows 认证，那么现有用户在 AppScan Source 中将有效，前提是新 Enterprise Server Liberty 配置为使用 Windows 认证。

从 V8.7 迁移

- 『结果分类的更改』
- 第 15 页的『将改进扫描覆盖范围的缺省设置更改』
- 第 16 页的『复原先前版本的 AppScan Source 预定义过滤器』

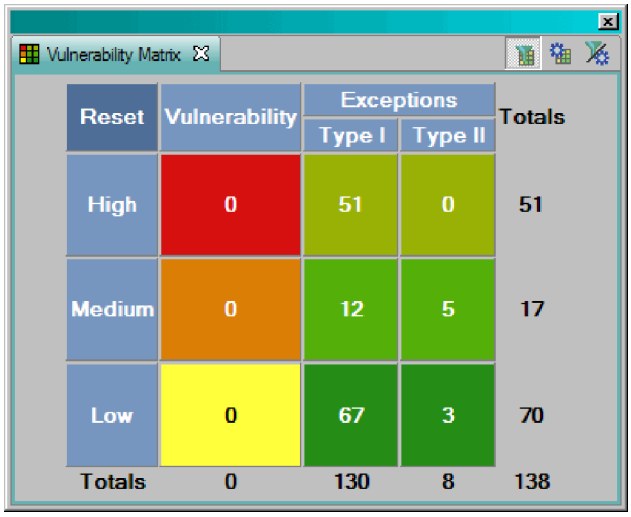
结果分类的更改

在 V8.7 之后，结果分类已更改。下表列出了旧分类与新分类的映射关系：

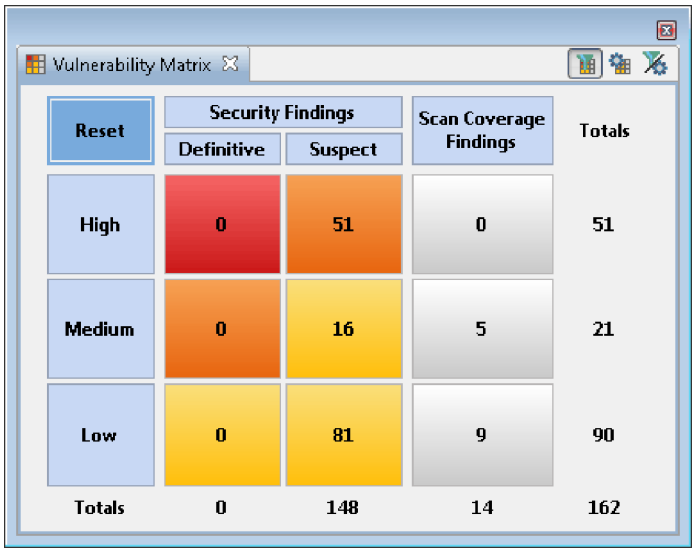
表 *1.* 结果分类更改

AppScan Source V8.8 之前的结果分类	AppScan Source V8.8 以来的分类
漏洞	明确安全性结果
I 类异常	可疑安全性结果
II 类异常	扫描覆盖范围结果

在"漏洞矩阵"视图中可以看到这些更改的示例。



在 V8.8 中，该视图看起来如下所示：



将改进扫描覆盖范围的缺省设置更改

在 AppScan Source V8.8 中：

- `scan.ozsettings` 中 `show_informational_findings` 的缺省值已从 `true` 更改为 `false`。
- `ipva.ozsettings` 中 `wafl_globals_tracking` 的缺省值已从 `false` 更改为 `true`。此设置使 AppScan Source 能够查找基于框架的应用程序的不同组件之间的数据流（例如，从控制器到视图的数据流）。

缺省情况下，对 `show_informational_findings` 的更改将致使评估不包含严重性级别为**参考**的结果。

注：如果您的在 V8.8 之前已创建的扫描配置未显式设置上述设置的值，那么这些扫描配置现在将使用其新缺省值。

复原先前版本的 AppScan Source 预定义过滤器

在 AppScan Source V8.8 中，预定义过滤器已改进，从而提供更好的扫描结果。如果您需要继续使用较低版本的 AppScan Source 的预定义过滤器（已归档过滤器在 第 130 页的『AppScan Source 预定义过滤器（V8.7.x 和更低版本）』中列出），请按照第 132 页的『复原已归档的预定义过滤器』中的指示信息操作。

AppScan Source for Analysis 概述

AppScan Source for Analysis 是一种用于分析代码并提供关于关键系统中源代码漏洞的特定信息的工具。通过 AppScan Source for Analysis，您可以集中管理跨多个应用程序甚至整个产品服务组合的软件风险。您可以扫描源代码，筛选并消除漏洞，以防止贵组织因这些漏洞而承担责任。

AppScan Source for Analysis 向审计和质量保证团队提供用于扫描源代码，对结果分类以及向缺陷跟踪系统提交缺陷的工具。

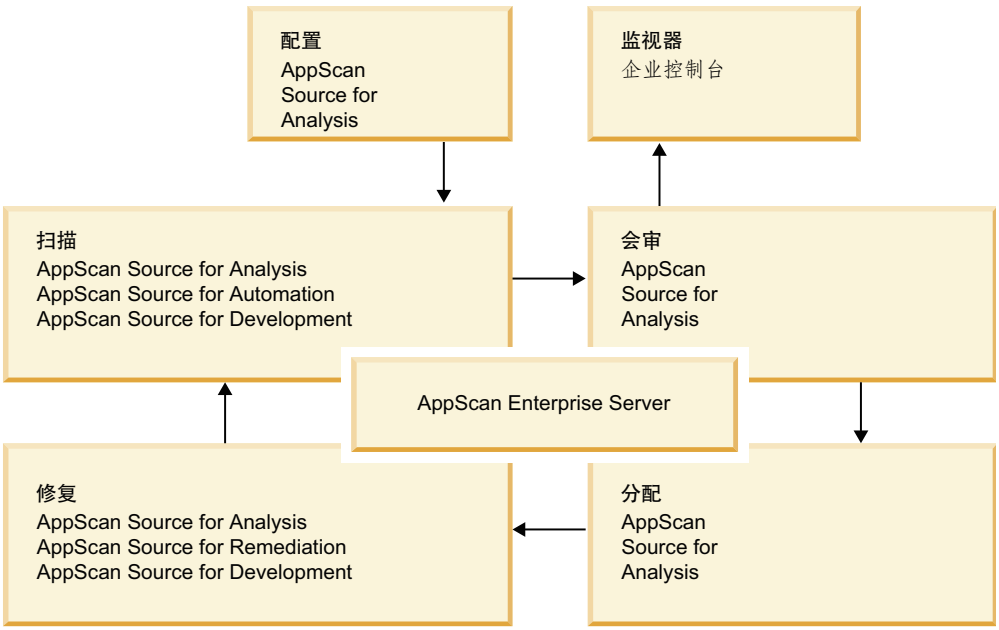
利用 AppScan Source 安全知识库提供的上下文中情报，分析员、审计员、管理员和开发者可以：

- 随需应变扫描所选源代码以找到关键漏洞
- 收到精确的补救建议并直接从分析调用其首选的开发环境和代码编辑器
- 通过从输入到输出的精确交互调用图跟踪感染的数据
- 实施编码策略，从而通过 AppScan Source 跟踪来检验已核准的输入验证和编码例程
- 在软件开发期间了解并实施安全编程最佳实践

工作流程

执行了安装、部署和用户管理后，AppScan Source 工作流程由以下基本步骤组成。

1. **设置安全需求**：经理和安全专家定义漏洞以及如何判断重要程度。
2. **配置应用程序**：组织应用程序和项目。
3. **扫描**：针对目标应用程序运行分析以识别漏洞。
4. **筛选和分析结果**：有安全意识的员工研究结果以对补救工作流程进行优先级排序，并将真实漏洞与潜在漏洞分开，从而支持立即开始对关键问题执行筛选。隔离需要首先修复的问题。
5. **定制知识库**：定制 AppScan Source 安全知识库以处理内部策略。
6. **发布扫描结果**：将扫描结果添加到 AppScan Source 数据库或将其发布到 AppScan Enterprise Console。
7. **分配补救任务**：将缺陷分配给开发团队以解决漏洞。
8. **解决问题**：通过重写代码、除去缺陷或添加安全功能来消除漏洞。
9. **验证修复**：再次扫描代码以确保消除了漏洞。



重要概念

您在开始使用或管理 AppScan Source 之前，应该让自己熟悉主要 AppScan Source 概念。本部分定义基本 AppScan Source 术语和概念。后续章节会重复这些定义以帮助您了解它们在 AppScan Source for Analysis 中的上下文。

AppScan Source for Analysis 扫描源代码以查找漏洞并生成结果。结果是在扫描期间确认的漏洞，而扫描的结果是评估。束是单独结果的命名集合并且与应用程序存储在一起。

应用程序、其属性以及项目在 AppScan Source for Analysis 中进行创建和组织：

- **应用程序**：应用程序包含一个或多个项目及其相关属性。
- **项目**：项目包含一组文件（包括源代码）及其相关信息（如配置数据）。项目始终是应用程序的一部分。
- **属性**：属性是应用程序的特征，有助于将扫描结果组织为有意义的分组（如按部门或项目主管）。您在 AppScan Source for Analysis 中定义属性。

AppScan Source for Analysis 的主要活动是扫描源代码并分析漏洞。评估提供对源代码的漏洞分析，包括：

- **严重性**：高、中或低，指示风险级别
- **漏洞类型**：漏洞类别，如 SQL 注入或缓冲区溢出
- **文件**：其中存在结果的代码文件
- **API/源**：易于受到攻击的调用，显示 API 以及传递到此 API 的参数
- **方法**：发出易受攻击调用的函数或方法
- **位置**：代码文件中包含易受攻击的 API 的行和列号
- **分类**：安全性结果或扫描覆盖范围结果。有关更多信息，请参阅第 18 页的『分类』。

分类

结果由 AppScan Source 分类以指示它们是安全性结果还是扫描覆盖范围结果。安全性结果表示实际或可能的安全漏洞 - 而扫描覆盖范围结果表示可改进配置以提供更好的扫描覆盖范围的区域。

每个结果都属于以下分类之一：

- **明确**安全性结果：一种结果，其中包含明确的设计、实施或策略违例，此违例为攻击者提供机会来使应用程序以一种非意愿方式运行。

  该攻击会导致对数据、系统或资源的未授权访问、偷窃或损坏。每个明确安全性结果都得到完整而清楚的表达，并且漏洞情况的特定底层模式已知并予以描述。
- **可疑**安全性结果：一种结果，指示可疑且可能存在漏洞的情况，该情况需要更多的信息或调查。不正确使用时可能会产生漏洞的代码元素或结构。

  可疑结果不同于明确结果，因为存在某种未知的情况妨碍对漏洞进行最终确定。此不确定性的示例可以是使用动态元素或者使用源代码不可用于的库函数。因此，需要多一级别的调查才能对可疑结果是否为明确结果进行确认或否定。
- **扫描覆盖范围**结果：表示可改进配置以提供更佳扫描覆盖范围的区域的结果（例如，丢失接收器结果）。

注：某些情况下，**无**分类可用于表示某个分类既不是安全性结果也不是扫描覆盖范围结果。

从 AppScan Source 产品登录 AppScan Enterprise Server

大多数 AppScan Source 产品和组件都需要与 AppScan Enterprise Server 连接。该服务器提供集中的用户管理功能，以及一种通过 AppScan Source 数据库共享评估的机制。

启动 AppScan Source for Analysis 时，将提示您认证到 AppScan Enterprise Server。如果您是在服务器方式下运行 AppScan Source for Development，那么在首次启动需要访问服务器的操作（例如启动扫描，或查看扫描配置）时将提示您认证到AppScan Enterprise Server。

- 『通过 AppScan Enterprise Server 用户标识和密码从 AppScan Source for Analysis 和 AppScan Source for Development 登录』
- 第 19 页的『使用通用访问卡 (CAC) 认证从 AppScan Source for Analysis 和 AppScan Source for Development 登录』
- 第 20 页的『从 AppScan Source for Automation 和 AppScan Source 命令行界面 (CLI) 登录』
- 第 20 页的『AppScan Enterprise Server SSL 证书』
- 第 20 页的『解决 AppScan Enterprise Server 证书错误』

通过 AppScan Enterprise Server 用户标识和密码从 AppScan Source for Analysis 和 AppScan Source for Development 登录

在 AppScan Source for Analysis 中，登录时将提示您指定：

- **用户标识**：指定您的用户标识（根据您的帐户的设置方式，这可以是在 AppScan Enterprise Server 上和 AppScan Source 数据库中均存在的用户标识，或者是仅在 AppScan Source 数据库中存在的用户标识）。
  - 如果 AppScan Enterprise Server 配置为使用 Windows 认证，请输入用于连接到 Enterprise Console 的域和用户名（以 \ 分隔域和用户名，例如 my_domain\my_username）。
  - 如果 AppScan Enterprise Server 已配置 LDAP，请输入用于连接到 Enterprise Console 的用户名。
- **密码**：指定用户标识的密码。
- **AppScan Enterprise Server**：指定 AppScan Enterprise Server 实例的 URL。该 URL 的格式为 http(s)://<hostname>:<port>/ase，其中 <hostname> 是已安装了 AppScan Enterprise Server 的机器的名称，<port> 是服务器运行所在的端口。该 URL 的示例为 https://myhost.mydomain.ibm.com:9443/ase。

在 AppScan Source for Development 中，登录时将提示您指定：

- **服务器 URL**：指定 AppScan Enterprise Server 实例的 URL。该 URL 的格式为 http(s)://<hostname>:<port>/ase，其中 <hostname> 是已安装了 AppScan Enterprise Server 的机器的名称，<port> 是服务器运行所在的端口。该 URL 的示例为 https://myhost.mydomain.ibm.com:9443/ase。
- **用户标识**：指定您的用户标识（根据您的帐户的设置方式，这可以是在 AppScan Enterprise Server 上和 AppScan Source 数据库中均存在的用户标识，或者是仅在 AppScan Source 数据库中存在的用户标识）。
  - 如果 AppScan Enterprise Server 配置为使用 Windows 认证，请输入用于连接到 Enterprise Console 的域和用户名（以 \ 分隔域和用户名，例如 my_domain\my_username）。
  - 如果 AppScan Enterprise Server 已配置 LDAP，请输入用于连接到 Enterprise Console 的用户名。
- **密码**：指定用户标识的密码。

使用通用访问卡 (CAC) 认证从 AppScan Source for Analysis 和 AppScan Source for Development 登录

在 Windows 上，可使用 CAC 认证连接到 AppScan Enterprise Server (http://www.cac.mil)。在执行该操作之前，必须设置 AppScan Enterprise Server 和 AppScan Source 以能够进行通用访问卡 (CAC) 认证。如果 Enterprise Server 已设置为进行 CAC 认证，那么不能使用 Enterprise Server 用户标识和密码来登录。

在 AppScan Source for Analysis 中，登录时将提示您指定：

- **用户**：从列表选择 CAC 常用名。
- **AppScan Enterprise Server**: 指定 AppScan Enterprise Server 实例的 URL。该 URL 的格式为 http(s)://<hostname>:<port>/ase，其中 <hostname> 是已安装了 AppScan Enterprise Server 的机器的名称，<port> 是服务器运行所在的端口。该 URL 的示例为 https://myhost.mydomain.ibm.com:9443/ase。

在 AppScan Source for Development 中，登录时将提示您指定：

- **服务器 URL**：指定 AppScan Enterprise Server 实例的 URL。该 URL 的格式为 http(s)://<hostname>:<port>/ase，其中 <hostname> 是已安装了 AppScan Enter-

prise Server 的机器的名称，<port> 是服务器运行所在的端口。该 URL 的示例为 https://myhost.mydomain.ibm.com:9443/ase。

- **用户**：从列表选择 CAC 常用名。

单击**确定**之后，将通过 Windows 安全对话框来提示您输入 CAC 卡密码。

提示：

- 如果登录失败，确保 AppScan Enterprise Server 已正确设置而且证书有效。检查以查看您是否可通过浏览器访问 AppScan Enterprise Server。如果可访问，那么您应该能够选择证书并登录。
- 如果登录对话框**用户**文件未列出可用证书，请确保您已修改了 JRE 中的 java.security 文件，如『启用通用访问卡 (CAC) 认证』中所述。
- 如果 Windows"安全"对话框未提示您输入 CAC 卡密码，请确保 Microsoft Smart Card Resource Manager 服务正在运行。请注意，对于某些远程桌面连接类型，该服务可能未运行。

从 AppScan Source for Automation 和 AppScan Source 命令行界面 (CLI) 登录

运行 AppScan Source for Automation 或 AppScan Source 命令行界面 (CLI) 时，也需要执行登录操作。请参阅《*IBM Security AppScan Source Utilities* 用户指南》以获取更多信息。

AppScan Enterprise Server SSL 证书

要了解关于 AppScan Enterprise Server SSL 证书的信息，请参阅第 22 页的『AppScan Enterprise Server SSL 证书』。

解决 AppScan Enterprise Server 证书错误

如果通过未知认证中心登录到 Enterprise Server，那么可能在登录时接收到证书异常或错误。AppScan Source 包含可帮助您更正该错误的小实用程序。工具为 <install_dir>\bin\certificatetool.bat（其中 <install_dir> 是 AppScan Source 安装位置） - 或 <install_dir>/bin/certificatetool.sh（在 Linux 和 macOS 上）。

启用通用访问卡 (CAC) 认证

该主题帮助您将 AppScan Source 设置为允许支持 AppScan Enterprise Server 的连接进行通用卡 (CAC) 认证。

开始之前

CAC 认证仅在 Windows 上受支持，而仅用于连接到 AppScan Enterprise Server V9.0.3.1 iFix-001 和更高版本。

过程

1. 确保 AppScan Enterprise Server 尚未设置为进行 CAC 认证。
2. 以 AppScan Source 管理员身份登录 AppScan Source for Analysis 或 AppScan Source 命令行界面 (CLI)。

3. 遵循 *IBM Security AppScan Source* 安装和管理指南 中的指示信息将所有 AppScan Enterprise Server 用户设置具有所有许可权。这会将 AppScan Enterprise Server 用户的初始缺省许可权设置为完整管理访问权，但在 CAC 设置完成后，您将能够更改缺省许可权以符合组织的需求。
4. 退出或关闭所有 AppScan Source 客户机应用程序。
5. 设置 AppScan Enterprise Server 以允许 CAC 认证
6. 遵循 *IBM Security AppScan Source* 安装和管理指南 中的指示信息将 AppScan Source 数据库 注册到支持通用访问卡 (CAC) 认证的 AppScan Enterprise Server。
7. 打开 <data_dir>\config\ounce.ozsettings（其中 <data_dir> 是 AppScan Source 程序数据的位置，如第 275 页的『安装和用户数据文件位置』中所述）。在此文件中，找到以下设置：

```
<Setting
   name="client_cert_auth"
   value="false"
   default_value="false"
   description="Uses client certificate authentication"
   display_name="Uses client certificate authentication"
   type="boolean"
   read_only="true"
   hidden="true"
 />
```

8. 在此设置中，将 value="false" 更改为 value="true"，然后保存文件。
9. 如果要从 AppScan Source for Analysis 或 AppScan Source for Development Eclipse 插件 登录 AppScan Enterprise Server：
   a. 在 Java 安装目录中，找到 jre/lib/security/java.security。对于 AppScan Source for Analysis，jre 文件夹位于 AppScan Source 安装目录中。创建该文件的备份副本。
   b. 编辑 java.security。
   c. 在提供程序及其优先顺序的列表中，添加 com.ibm.security.capi.IBMCAC 作为第一个安全提供程序。例如，如果要编辑 java.security 以用于 AppScan Source for Analysis，将以下内容：

```
security.provider.1=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.2=com.ibm.jsse2.IBMJSSEProvider2
security.provider.3=com.ibm.crypto.provider.IBMJCE
security.provider.4=com.ibm.security.cert.IBMCertPath
security.provider.5=sun.security.provider.Sun
```

   更改为以下内容：

```
security.provider.1=com.ibm.security.capi.IBMCAC
security.provider.2=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.3=com.ibm.jsse2.IBMJSSEProvider2
security.provider.4=com.ibm.crypto.provider.IBMJCE
security.provider.5=com.ibm.security.cert.IBMCertPath
security.provider.6=sun.security.provider.Sun
```

   d. 保存并关闭 java.security 文件。
10. 以 AppScan Source 管理员身份登录到 AppScan Source for Analysis 或使用的 CAC 认证的 AppScan Source 命令行界面 (CLI)。
11. 更改 AppScan Enterprise Server 用户的缺省许可权以满足组织的需求。

下一步做什么

如果想要强制实施联邦信息处理标准 (FIPS) 方式，那么您的证书不能是 SHA-1。可通过使用 SHA-2 证书并按*IBM Security AppScan Source* 安装和管理指南中的描述运行 `appscanserverdbmgr_cac_fips.bat` 工具来强制实施 FIPS 方式。在本指南中，找到将 AppScan Source 数据库 注册到支持通用访问卡 (CAC) 认证的 AppScan Enterprise Server 的帮助。

要确定您具有的证书：

1. 打开 Windows Certificate Manager：在 Windows 开始菜单中，在搜索框中输入 `certmgr.msc`，然后按 Enter。如果提示您输入管理员密码或对密码进行确认，请输入密码或进行确认。
2. 通过双击用户界面上的**打开**操作来打开证书。
3. 选择证书中的"详细信息"选项卡。
4. 找到**签名散列算法**字段。该字段的值指示证书的类型。

更改 AppScan Source 用户密码

为了能够更改 AppScan Source 用户密码，您必须拥有**管理用户**许可权并且必须在 AppScan Source for Analysis 中做出更改。如果您没有此许可权，请按照本主题中的指示信息来让管理员为您更改密码。如果 AppScan Enterprise Server 已配置为使用 LDAP 认证或 Windows 认证，那么本主题不适用。

过程

1. 在 AppScan Source for Analysis 中，从主工作台菜单选择**管理** > **管理用户**。
2. "管理用户"对话框列出现有 AppScan Source 用户。要更改这些用户之一的密码，请通过完成以下任务之一来编辑用户信息：
   - 双击此用户。
   - 右键单击此用户，然后选择**编辑用户**。
   - 选择此用户，然后单击**编辑用户**按钮。

   注：您无法从 AppScan Source 更改 AppScan Enterprise Server 用户的密码。
3. 在"编辑用户"对话框中，输入新密码，然后在**确认密码**字段中再次输入该密码。
4. 单击**确定**以更改密码。

AppScan Enterprise Server SSL 证书

安装 AppScan Enterprise Server 时，应对其进行配置以使用有效 SSL 证书。如果未完成该操作，那么在 Windows 和 Linux 上通过 AppScan Source for Analysis、AppScan Source 命令行界面 (CLI) 或 AppScan Source for Development 登录到服务器时将接收不可信的连接消息。

SSL 证书存储位置

已被永久接受的证书存储在 `<data_dir>\config\cacertspersonal` 和 `<data_dir>\config\cacertspersonal.pem`（其中 `<data_dir>` 是 AppScan Source 程序数据的位置，如第 275 页的『安装和用户数据文件位置』中所述） 中。如果不需要永久地存储证书，请除去这两个文件。

AppScan Source for Automation 和 SSL 证书验证

缺省情况下，使用 AppScan Source for Automation 时将自动接受证书。此行为由 自动化服务器 配置文件 (<data_dir>\config\ounceautod.ozsettings（其中 <data_dir> 是 AppScan Source 程序数据的位置，如第 275 页的『安装和用户数据文件位置』中所述）) 中的 ounceautod_accept_ssl 设置来确定。如果编辑了该设置以至于 value="true" 设置为 value="false"，那么将尝试 SSL 验证，而且当遇到无效证书时到 AppScan Enterprise Console 的登录或发布将失败，并会出现错误。

AppScan Source 命令行界面 (CLI) 和 SSL 证书验证

缺省情况下，当使用 CLI login 命令时，将尝试 SSL 验证，而如果遇到无效证书，那么登录到 AppScan Enterprise Console 或向其进行发布的操作将失败并出错（如果在通过其他 AppScan Source 产品登录时，您尚未永久接受证书）。可以通过在发出 login 命令时使用选项 -acceptssl 参数来修改此行为。使用此参数后，将自动接受 SSL 证书。

AppScan Source 和辅助功能选项

辅助功能选项将影响残障用户，如行动不便或视力受限的用户。辅助功能选项问题可能会阻碍功能成功使用软件产品。本主题概述了已知的 AppScan Source 辅助功能选项问题及其背景。

将 JAWS 读屏软件与 AppScan Source 安装程序配合使用

要在运要在运行 AppScan Source 安装程序时使用 Freedom Scientific JAWS (http://www.freedomscientific.com/products/fs/jaws-product-page.asp)，您必须在 AppScan Source JVM 中安装 Java Access Bridge。这可使 JAWS 正确的表示安装程序面板中的标签和控件。

- 关于 Java Access Bridge 的信息（包括下载链接和安装指示信息）可在 http://www.oracle.com/technetwork/java/javase/tech/index-jsp-136191.html 上找到。
- 关于安装 Java Access Bridge 的 InstallAnywhere 需求的信息可在 http://kb.flexerasoftware.com/selfservice/documentLink.do?externalID=Q200311 上找到。

在用户界面面板中对描述性文本使用 JAWS Screen Reading Software

AppScan Source 用户界面的许多部分都包含描述性文本。在大多数情况下，必须使用 JAWS Insert+B 击键才能读取该描述性文本。

声明

本信息是为在美国国内供应的产品和服务而编写的。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。有关您所在区域的当前可用产品和服务的信息，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 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，则由用户自行负责。

IBM 可能已拥有或正在申请与本文档中描述的内容有关的各项专利。提供本文档并不意味着授予用户使用这些专利的任何许可。您可以用书面方式将许可查询寄往：

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

有关双字节字符集 (DBCS) 信息的许可证查询，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.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

本条款不适用于英国或任何这样的条款与当地法律不一致的国家或地区：

INTERNATIONAL BUSINESS MACHINES CORPORATION"按现状"提供此出版物，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、适销或适用于某种特定用途的保证或条件。

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。

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

本信息中对任何非 IBM Web 站点的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 可以按照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程序的信息以达到如下目的：(i) 允许在独立创建的程序和其他程序（包括本程序）之间进行信息交换，以及 (ii) 允许相互使用已交换的信息，请与下列地址联系：

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 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 国际软件许可协议或任何同等协议中的条款提供。

此处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数据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，它们仅表示了目标和意愿而已。

显示的所有 IBM 价格皆为 IBM 建议的最新零售价格，且可随时更改，而不另行通知。经销价格可能会有差异。

本信息仅限规划目的使用。在提供所述的产品之前，此处的信息得随时更改。

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。所有这些名称都是虚构的，如与实际商业企业所使用的名称和地址有任何雷同，纯属巧合。

版权许可证：

本信息包含源语言形式的样本应用程序，用以阐明在不同操作平台上的编程技术。如果是为了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，那么您可以任何形式对这些样本程序进行复制、修改和分发，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。如果是以按照 IBM 的应用程序编程接口进行应用程序的开发、使用、经销或分发为目的，您可以通过任何形式对这些样本程序进行复制、修改和分发，而无须向 IBM 付费。

这些样本程序的每份拷贝/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) (年份)。此代码的某些部分是根据 IBM 公司的样本程序衍生出来的。
© Copyright IBM Corp. _输入年份_. All rights reserved.

如果您正在查看本信息的软拷贝形式，图片和彩色图例可能无法显示。

商标

IBM、IBM 徽标和 ibm.com® 是 International Business Machines Corp. 在全球许多管辖区域内注册的商标或注册商标。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 上的 "Copyright and trademark information"中获取。

Adobe、Acrobat、PostScript 以及所有基于 Adobe 的商标都是 Adobe Systems Incorporated 在美国和/或其他国家或地区的注册商标或商标。

IT Infrastructure Library 是英国中央计算机和远程通信局（现在是英国政府商务部的一部分）的注册商标。

Intel、Intel 徽标、Intel Inside、Intel Inside 徽标、Intel Centrino、Intel Centrino 徽标、Celeron、Intel Xeon、Intel SpeedStep、Itanium 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。

Linux 是 Linus Torvalds 在美国和/或其他国家或地区的商标。

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

ITIL 是英国政府商务部的注册商标和欧盟注册商标，并且已在美国专利和商标局注册。

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

Java 和所有基于 Java 的商标和徽标是 Oracle 和/或其子公司的商标或注册商标。

Cell Broadband Engine 是 Sony Computer Entertainment, Inc. 在美国和/或其他国家或地区的商标，并根据当地的许可证使用。

Linear Tape-Open、LTO、LTO 徽标、Ultrium 和 Ultrium 徽标是 HP、IBM Corp. 和 Quantum 在美国和其他国家或地区的商标。

版权

(C) Copyright IBM Corp. and its licensors 2003, 2017. All Rights Reserved.

IBM、IBM 徽标、ibm.com Rational、AppScan、Rational Team Concert、WebSphere 和 ClearQuest 是 International Business Machines Corp. 在全球多个管辖区域内的商标或注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。版权和商标信息 Web 站点上提供了 IBM 商标的当前列表，网址为：http://www.ibm.com/legal/copytrade.shtml。Linux 是 Linus Torvalds 在美国和/或其他国家或地区的注册商标。Microsoft、Windows、Windows NT 和 Windows 徽标是 Microsoft Corporation 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 和所有基于 Java 的商标和徽标是 Oracle 和/或其子公司的商标或注册商标。

本程序包括：Jacorb 2.3.0（Copyright 1997-2006 JacORB 项目）以及 XOM1.0d22 (Copyright 2003 Elliotte Rusty Harold)，上述各项均依据 Gnu Library General Public License (LGPL) 提供，该许可证的副本在本程序随附的"声明"文件中提供。

第 2 章 配置应用程序和项目

您必须先配置应用程序和项目，然后才能进行扫描。此部分说明 Application Discovery Assistant、"新建应用程序向导"和"新建项目向导"。您将了解如何配置 AppScan Source for Analysis 的属性。此外，本部分还会教您如何添加现有应用程序和项目以供扫描 - 以及如何向项目添加文件。

AppScan Source for Analysis 配置包括应用程序创建、源代码配置和属性配置。配置和扫描后，请继续进行筛选。您可以在"属性"视图中或通过"新建项目向导"来配置源代码。本章将引导您完成向导。请参阅第 242 页的『"属性"视图』以获取应用程序和项目属性的概述。

AppScan Source for Analysis 使用应用程序/项目模型，该模型直接导入先前通过 AppScan Source 实用程序创建的 Microsoft Visual Studio、Eclipse、Rational Application Developer for WebSphere Software (RAD) 或 AppScan Source 项目（请参阅《*IBM Security AppScan Source Utilities* 用户指南》以获取进一步的详细信息）。

可以添加和配置各种类型的以及含有各种语言的项目 - 指定从目标代码库及其构建过程中收集的设置。在配置期间，可以指定要从扫描中排除的目录和文件。

您必须先配置应用程序和项目，然后才能进行扫描。应用程序是项目的容器；项目是要扫描的一组文件和所使用的设置（配置）。

AppScan Source 应用程序和项目文件

AppScan Source 应用程序和项目具有对应的文件，这些文件用来维护扫描以及筛选定制所需的配置信息。建议将这些文件与源代码放置在同一目录中，因为构建项目所需的配置信息（依赖性、编译器选项等）与 AppScan Source 成功扫描这些项目所需的配置信息非常相似。最佳实践包括以源代码控制系统管理这些文件。

AppScan Source for Analysis 中创建的应用程序和项目分别具有 `.paf` 和 `.ppf` 扩展名。当您在 AppScan Source for Analysis、AppScan Source for Automation 和 AppScan Source 命令行界面 中手动创建和配置应用程序或项目时，将生成这些文件。

在 Windows 上，在您将 Visual Studio 解决方案和项目导入到 AppScan Source for Analysis、AppScan Source for Automation和 AppScan Source 命令行界面 中时，将为它们创建扩展名为 `.sln.gaf` 和 `.vcproj.gpf` 的文件。

在 macOS 上，导入 Xcode 目录和项目时，将为其创建具有 `.xcodeproj.gaf` 和 `.xcodeproj.gpf` 扩展名的文件。同样，导入 Xcode 工作空间时，将创建具有 `.xcworkspace.gaf` 扩展名的文件。

注：当 Eclipse 导入器在 Eclipse 或 Rational Application Developer for WebSphere Software (RAD) 工作空间中运行时，AppScan Source 将创建具有 `.ewf` 和 `.epf` 扩展名的中间文件。以 AppScan Source for Analysis 为目标的初始导入以及将来的扫描都需要这些文件。

© Copyright IBM Corp. 2003, 2017

要点：如果您所处理的是在开发环境中具有依赖性的 AppScan Source 项目（例如 IBM MobileFirst Platform 项目），请确保在导入该项目之前在开发环境中对其进行构建。导入该项目后，如果您修改其中的文件，请确保在 AppScan Source 中进行扫描之前在开发环境中重新构建该项目（如果不执行此操作，那么 AppScan Source 将忽略对文件做出的修改）。

表 *2. AppScan Source* 文件

AppScan Source 文件扩展名	描述
ppf	• AppScan Source 项目文件 • 在使用 AppScan Source for Analysis 或受支持的 AppScan Source 实用程序创建项目时生成 • 用户命名
paf	• AppScan Source 应用程序文件 • 在使用 AppScan Source for Analysis 或受支持的 AppScan Source 实用程序创建应用程序时生成 • 用户命名

sln.gaf	• 导入 Visual Studio 解决方案时生成的 AppScan Source 应用程序文件
	• 用来保留定制应用程序信息（例如排除项和捆绑软件）
	• 采用导入的工作空间或解决方案的名称。例如：
	`d:\my_apps\myapp.sln`
	`d:\my_apps\myapp.sln.gaf`

vcproj.gpf	• 导入 Visual Studio 项目时生成的 AppScan Source 项目文件
	• 用来保留定制项目信息（例如模式和排除项）
	• 采用所导入的项目的名称。例如：
	`d:\my_projects\myproject.vcproj`
	`d:\my_projects\myproject.vcproj.gpf`

xcodeproj.gaf	• 导入 Xcode 目录时生成的 AppScan Source 应用程序文件
	• 用来保留定制应用程序信息（例如排除项和捆绑软件）
	• 采用导入的工作空间或解决方案的名称。例如：
	`/Users/myUser/myProject.xcodeproj`
	`/Users/myUser/myProject.xcodeproj.gaf`

表 2. *AppScan Source* 文件 (续)

AppScan Source 文件扩展名	**描述**
xcodeproj.gpf	• 导入 Xcode 项目时生成的 AppScan Source 项目文件 • 用来保留定制项目信息（例如模式和排除项） • 采用导入的项目的名称：例如： /Users/myUser/myProject.xcodeproj /Users/myUser/myProject.xcodeproj.gpf
xcworkspace.gaf	• 导入 Xcode 工作空间时生成的 AppScan Source 应用程序文件 • 用来保留定制应用程序信息（例如排除项和捆绑软件） • 采用所导入的工作空间的名称。例如： /Users/myUser/myProj.xcworkspace.gaf
ewf	• Eclipse 工作空间文件 • 将 Eclipse 工作空间导入 AppScan Source 时生成 • Eclipse 导出器基于 Eclipse 工作空间内的信息创建此文件，然后 AppScan Source 导入此文件
epf	• Eclipse 项目文件 • 将 Eclipse 项目导入 AppScan Source 时生成 • Eclipse 导出器基于 Eclipse 项目内的信息创建此文件，然后 AppScan Source 导入此文件

提示：使用受支持的构建集成工具（例如，buildOunce/Ant 或 Ounce/Maven）来生成 AppScan Source 应用程序和项目文件时，建议您在源代码控制中更新这些文件（作为构建自动化的一部分）以利于在整个开发团队中将其共享。当开发者在源代码控制中更新这些文件的局部视图时，AppScan Source 应用程序和项目文件也会更新。这确保整个团队所用文件集的一致性。

注：要了解 AppScan Source for Analysis、AppScan Source for Automation 和 AppScan Source 命令行界面 支持哪些版本的导入文件，请参阅http://www.ibm.com/support/docview.wss?uid=swg27027486。在此页面中，选择您在使用的 AppScan Source 版本所对应的选项卡，然后选择您在使用的 AppScan Source 组件。如果 AppScan Source 支持从其他开发环境打开和扫描文件，该支持将在**受支持软件**选项卡的**编译器和语言**部分中列出。

配置应用程序

可以使用"新建应用程序向导"或 Application Discovery Assistant 来创建应用程序。Application Discovery Assistant 将自动为您设置应用程序，而"新建应用程序向导"允许您添加应用程序，并指导您完成配置过程。此向导将帮助您手动创建项目，或将现有项目添加到应用程序。此部分描述了用于添加应用程序和基本配置任务的以下两种方法：

注：Application Discovery Assistant 快速为 Java 源代码和 Microsoft Visual Studio 解决方案或包含了 Java 项目的 Eclipse/IBM Rational Application Developer for WebSphere Software (RAD) 工作空间创建和配置应用程序和项目。要为其他任何受支持的语言创建应用程序，请使用"新建应用程序向导"，或者将受支持的应用程序导入到 AppScan Source for Analysis。

添加项目之前，必须创建新应用程序（请参阅第 31 页的『通过"新建应用程序向导"创建新的应用程序』或第 31 页的『使用 Application Discovery Assistant 创建应用程序和项目』）或者添加现有应用程序（请参阅第 34 页的『添加现有应用程序』）。如果使用 Microsoft Visual Studio，那么您已对项目中的源文件进行了排列。通过 AppScan Source for Analysis，可以导入解决方案并将其视为 AppScan Source 应用程序。

下表列出了可通过 AppScan Source for Analysis 打开和扫描的应用程序文件类型。

表 *3.* 支持的应用程序文件类型

应用程序	文件类型
Microsoft Visual Studio **注：**要了解 AppScan Source for Analysis、AppScan Source for Automation 和 AppScan Source 命令行界面 支持哪些版本的导入文件，请参阅http://www.ibm.com/support/docview.wss?uid=swg27027486。在此页面中，选择您在使用的 AppScan Source 版本所对应的选项卡，然后选择您在使用的 AppScan Source 组件。如果 AppScan Source 支持从其他开发环境打开和扫描文件，该支持将在**受支持软件**选项卡的**编译器和语言**部分中列出。	`.sln`（解决方案）
• Eclipse 工作空间（仅 Java） • RAD 工作空间（仅 Java） 请参阅 AppScan Source 系统需求以了解对于工作空间扫描支持哪些版本的 Eclipse 和 RAD。	`<workspace directory>` 或 `.ewf` 工作空间目录包含附加目录 `.metadata`。
AppScan Source 应用程序文件	`.paf`

提示： "资源管理器"视图中将显示一个图标以指示已导入的应用程序（请参阅第 75 页的『应用程序和项目指示符』）。

注：使用"新建应用程序"向导和"新建项目"向导创建应用程序和项目时，将根据在向导中输入的**名称**来自动分配其文件名（例如，如果正在创建项目并且在**名称**字段中输入了 **MyProject**，那么项目文件名将为 `MyProject.ppf`）。可以使用"属性"视图来为应用程序和项目重命名。

通过"新建应用程序向导"创建新的应用程序

过程

1. 完成以下其中一个操作：
   - 从主菜单栏中选择**文件** > **添加应用程序** > **创建新应用程序**。
   - 在"资源管理器"视图工具栏中，单击**添加应用程序菜单**向下箭头按钮，然后从菜单中选择**创建新应用程序**。
   - 在"资源管理器"视图中，右键单击**所有应用程序**，然后从菜单中选择**添加应用程序** > **创建新应用程序**。
2. 为应用程序输入**名称**。
3. 浏览至将保存应用程序的**工作目录**。新的应用程序文件扩展名将为 `.paf`。
4. 单击**下一步**以配置构成应用程序的项目，或者单击**完成**以添加应用程序而不配置任何项目。此部分后面提供了有关配置和添加项目的帮助。

使用 Application Discovery Assistant 创建应用程序和项目

AppScan Source 包含功能强大的 Application Discovery Assistant，它使您能够为 Java 源代码和 Microsoft Visual Studio 解决方案快速创建并配置应用程序和项目。 Application Discovery Assistant 还使您能够找到包含了 Java 项目的 Eclipse 或 Rational Application Developer for WebSphere Software (RAD) 工作空间。 Application Discovery Assistant 使您能够指向源、解决方案或工作空间目录，然后 AppScan Source 将处理余下的工作。

关于此任务

您可以使用 Application Discovery Assistant 来搜索包含 Java 源代码、Microsoft Visual Studio 解决方案和/或 Eclipse 工作空间的组合的位置。通过 Application Discovery Assistant 的最后一个面板，您可以指定仅针对 Java 的应用程序/项目结构首选项。此面板与 Microsoft Visual Studio 解决方案或Eclipse 工作空间的应用程序和项目文件的放置没有任何关系：应用程序文件自动放置在解决方案或工作空间的根目录中，而项目文件自动放置在各个解决方案或工作空间项目的根目录中。

过程

1. 完成以下操作之一以启动 Application Discovery Assistant：
   - 从主菜单栏中选择**文件** > **添加应用程序** > **发现应用程序**。
   - 在"资源管理器"视图的**快速启动**部分中，选择**发现应用程序**。
   - 在"资源管理器"视图工具栏中，单击**添加应用程序菜单**向下箭头按钮，然后从菜单中选择**发现应用程序**。
   - 在"资源管理器"视图中，右键单击**所有应用程序**，然后从菜单中选择**添加应用程序** > **发现应用程序**。
2. 在"搜索位置"面板中，指定包含要扫描的源代码、解决方案或工作空间的位置。此外，还可将扫描设置为在完成应用程序发现后立即开始。

在此处，可以单击**下一步**以设置其他 Application Discovery Assistant 选项（如外部依赖关系指定、排除规则和 Java 应用程序/项目结构首选项），或者也可以单击**启动**以开始应用程序发现。如果单击**启动**：

- 将不设置任何外部依赖关系位置。如果应用程序具有外部依赖关系，但未指定这些依赖关系，那么扫描结果将受到不利影响。
- 将使用预设排除规则（请参阅第 34 页的『缺省 Application Discovery Assistant 排除规则』以查看缺省规则的列表）。
- 如果要查找 Java 源代码，那么将创建一个项目和一个应用程序（此单个项目将包含找到的所有源代码根目录）。

如果单击**下一步**，那么继续执行下一步。

3. 在"外部依赖关系"面板中，为应用程序具有的每个外部依赖关系都设置一条路径（例如，JDK 或 Web 服务器的路径）。要完成此面板，请按照以下指示信息操作：
   a. 要添加外部依赖关系，请在表内单击或单击**添加**，然后输入或通过浏览来找到外部依赖关系路径。要接受您通过键盘输入的路径，请按键盘 Enter 键。

      提示：在编辑依赖关系路径字段时在其中进行输入，将列出可选择的目录。必须至少输入盘符。对于指定的路径，将列出其包含的所有文件夹。
   b. 要除去外部依赖关系路径，请选择该路径并单击**删除**。
   c. 要修改外部依赖关系路径，请在该路径内单击，然后输入或通过浏览来找到外部依赖关系路径。

   在此处，可以单击**下一步**以设置其他 Application Discovery Assistant 选项，或者也可以单击**启动**以开始应用程序发现。如果单击**启动**：

   - 将使用预设排除规则（请参阅第 34 页的『缺省 Application Discovery Assistant 排除规则』以查看缺省规则的列表）。
   - 如果要查找 Java 源代码，那么将创建一个项目和一个应用程序（此单个项目将包含找到的所有源代码根目录）。

   如果单击**下一步**，那么继续执行下一步。
4. 在"排除规则"面板中，指定用于滤除文件和目录的规则。规则通过 PERL、Grep、EGrep 或完全匹配正则表达式来设置。例如，如果要从 Application Discovery 搜索中排除名为 `temp` 的目录，那么可以添加 PERL `.*[\\/]temp` 排除规则。

   缺省情况下，提供了一组 PERL 正则表达式来排除一些常用目录（请参阅第 34 页的『缺省 Application Discovery Assistant 排除规则』以查看完整列表）。要修改此列表或创建新规则，请按照以下指示信息操作：
   a. 要修改现有排除规则，请在该规则内单击以激活规则编辑器。完成了对规则的编辑之后，请单击它以外的区域，或按键盘 **Enter** 键。

      要修改现有规则的正则表达式类型，请在该规则的**正则表达式类型**单元格内单击，然后从菜单中选择正则表达式类型。
   b. 要添加一项排除规则，请单击**添加**。这会向表中添加新规则，您可以按照以上关于修改规则的指示信息来修改该规则。

c. 要除去排除规则，请选择该规则并单击**删除**（或者单击**全部删除**以除去面板中当前列出的所有排除规则）。

要点：在表中，有效排除规则通过复选标记来表示，而无效规则通过红色 X 来表示。您在所有规则都有效之前将无法启动 Application Discovery 或在 Application Discovery Assistant 中继续操作。

在此处：

- 如果仅要搜索 Java 源代码，那么可以单击**下一步**以设置 Application Discovery Assistant 应用程序/项目结构首选项，或者也可以单击**启动**以运行此助手程序。
- 如果仅要搜索 Microsoft Visual Studio 解决方案或Eclipse 工作空间，请单击**启动**以运行此助手程序。单击**下一步**将致使此助手程序进入仅适用于 Java 源代码发现的面板。

如果单击**下一步**，那么继续执行下一步。

5. "应用程序和项目创建"面板仅适用于 Java 源代码发现。在该面板中，指定将创建的应用程序和项目的结构：
   a. 要为找到的所有源代码根目录创建单个项目，请在**项目**菜单中选择**创建单个项目**。通过此选择，您将只能选择创建单个应用程序。
   b. 要为找到的每个源代码根目录都创建一个单独的项目，请在**项目**菜单中选择**为找到的每个源代码根目录创建项目**。通过此选择，您可以选择创建一个或多个应用程序。要创建包含已创建的所有项目的单个应用程序，请在**应用程序**菜单中选择**创建单个应用程序**。要为已创建的每个项目都创建应用程序，请在**应用程序**菜单中选择**为每个项目创建应用程序**。

   此外，选择用于存储应用程序和项目定义文件的位置。

   如果选择**为我组织文件**：
   - 如果要创建单个项目，那么将在搜索位置创建项目和应用程序文件。
   - 如果要在单个应用程序中为每个源代码根目录都创建项目，那么每个源代码根目录的项目文件都将创建在该源代码根目录的上一级目录中，而应用程序文件将创建在搜索位置。
   - 如果要为每个源代码根目录都创建项目并为每个项目都创建应用程序，那么每个源代码根目录的项目和应用程序文件都将创建在该源代码根目录的上一级目录中。

   如果指定目录，那么将在该目录中创建所有应用程序和项目文件。
6. 如果要更改已在先前面板中作出的任何设置，请单击**上一步**。当您对 Application Discovery 设置满意时，请单击**开始**对搜索位置进行扫描以查找源代码根目录。

结果

当 Application Discovery 操作完成时，因 Application Discovery 操作而创建的新应用程序和项目会显示在"资源管理器"视图中，并且已准备好进行扫描（如果已将扫描设置为在完成应用程序发现后立即开始，那么扫描将开始）。

如果在发现期间遇到了问题，那么 Application Discovery Assistant 在完成操作时会提供一个发现报告。例如，如果应用程序具有未在"外部依赖关系"面板中指定的外部依赖关系，那么该报告将包含指示无法解析外部依赖关系的警告。在该发现报告中：

- 单击**完成**以创建应用程序和项目。如果选择了**忽略警告并仍进行扫描**，那么将立即扫描应用程序和项目。
- 单击**上一步**以修改 Application Discovery Assistant 设置或再次运行 Application Discovery。
- 单击**取消**以关闭此发现报告而不创建应用程序或项目。

缺省 Application Discovery Assistant 排除规则

使用 Application Discovery Assistant 时，如果未修改"排除规则"面板，或者如果在指定搜索目录后启动 Application Discovery，那么将使用缺省排除规则。本主题中列出了缺省 Application Discovery 排除规则。

表 4. 缺省 *Application Discovery* 排除规则

排除规则	正则表达式类型
.*[\\/]example	PERL
.*[\\/]test	PERL
.*[\\/]demo	PERL
.*[\\/]sample	PERL

添加现有应用程序

通过将要扫描的现有应用程序拖放到"资源管理器"视图中，可对其进行添加，也可以使用**添加应用程序**操作进行添加。此外，还可通过将 WAR 和 EAR 文件拖放到"资源管理器"视图来添加这些文件。

要了解如何添加现有应用程序，请参阅以下主题：

- 『通过用户界面操作添加现有应用程序』
- 第 35 页的『通过拖放操作来添加现有应用程序』

通过用户界面操作添加现有应用程序

过程

1. 完成以下其中一个操作：
   - 从主工作台菜单中选择**文件** > **添加应用程序** > **打开现有应用程序**。
   - 在"资源管理器"视图工具栏中，单击**添加应用程序菜单**向下箭头按钮，然后从菜单中选择**打开现有应用程序**。
   - 在"资源管理器"视图中，右键单击**所有应用程序**，然后从菜单中选择**添加应用程序** > **打开现有应用程序**。
2. 选择包含已保存应用程序文件（.paf、.sln、.dsw 或 .ewf）的目录。

   注：要了解 AppScan Source for Analysis、AppScan Source for Automation 和 AppScan Source 命令行界面 支持哪些版本的导入文件，请参阅http://www.ibm.com/support/docview.wss?uid=swg27027486。在此页面中，选择您在使用的 AppScan Source 版本所对应的选项卡，然后选择您在使用的 AppScan

Source 组件。如果 AppScan Source 支持从其他开发环境打开和扫描文件，该支持将在**受支持软件**选项卡的**编译器和语言**部分中列出。

3. 打开应用程序文件。

通过拖放操作来添加现有应用程序

过程

1. 在工作站上，查找要添加以进行扫描的应用程序（.paf、.war、.ear、.sln、.dsw 或 .ewf）。还可以添加包含 .war 或 .ear 文件的目录（在某些应用程序服务器中，这些目录称为混入文件夹）。

   注：您不能拖放 Eclipse 工作空间目录。

   注：如果要添加 .war 或 .ear 文件，或添加包含 .war 或 .ear 文件的目录，那么文件必须位于本地文件系统上或位于映射驱动器中。

   注：要了解 AppScan Source for Analysis、AppScan Source for Automation 和 AppScan Source 命令行界面 支持哪些版本的导入文件，请参阅http://www.ibm.com/support/docview.wss?uid=swg27027486。在此页面中，选择您在使用的 AppScan Source 版本所对应的选项卡，然后选择您在使用的 AppScan Source 组件。如果 AppScan Source 支持从其他开发环境打开和扫描文件，该支持将在**受支持软件**选项卡的**编译器和语言**部分中列出。
2. 选择应用程序，然后将其拖动至"资源管理器"视图。
3. 将所选项放置在**所有应用程序**节点上或其下方。
4. 如果要添加 .war 或 .ear 文件，或添加包含 .war 或 .ear 文件的目录，那么将打开对话框以允许您在其中指定要将文件部署到的应用程序服务器。完成该对话框之后单击**确定**。

添加多个应用程序

首次使用 AppScan Source for Analysis 时，您可能希望导入多个应用程序，而不是一次只添加一个应用程序。 "选择应用程序"对话框允许您选择从中搜索 AppScan Source 应用程序 (.paf) 或 Visual Studio 解决方案文件 (.sln) 的根目录。也可以通过将多个应用程序拖放到"资源管理器"视图中来添加这些应用程序用于扫描。

要了解如何添加多个应用程序，请参阅以下主题：

- 『通过用户界面操作添加多个应用程序』
- 第 36 页的『通过拖放操作来添加多个应用程序』

注：要添加多个 WAR 和 EAR 文件，可通过拖放包含文件的目录来添加这些文件。有关更多信息，请参阅『通过拖放操作来添加现有应用程序』。

通过用户界面操作添加多个应用程序

过程

1. 从主工作台菜单中依次选择**文件** > **添加应用程序** > **多个应用程序**。
2. 在"选择应用程序"对话框中，浏览至包含要导入的应用程序的根目录。选中**递归至子目录中**复选框以在子目录中搜索。
3. 完成以下其中一个操作：

- 单击**完成**以导入应用程序并将其添加到"资源管理器"视图。
- 单击**下一步**以查看搜索结果并选择要导入的应用程序。然后单击**完成**。

注：要了解 AppScan Source for Analysis、AppScan Source for Automation 和 AppScan Source 命令行界面 支持哪些版本的导入文件，请参阅http://www.ibm.com/support/docview.wss?uid=swg27027486。在此页面中，选择您在使用的 AppScan Source 版本所对应的选项卡，然后选择您在使用的 AppScan Source 组件。如果 AppScan Source 支持从其他开发环境打开和扫描文件，该支持将在**受支持软件**选项卡的**编译器和语言**部分中列出。

通过拖放操作来添加多个应用程序

过程

1. 在工作站上，找到要添加以进行扫描的应用程序（.paf、.sln、.dsw 或 .ewf 文件）。

   注：您不能拖放 Eclipse 工作空间目录。

   注：要了解 AppScan Source for Analysis、AppScan Source for Automation 和 AppScan Source 命令行界面 支持哪些版本的导入文件，请参阅http://www.ibm.com/support/docview.wss?uid=swg27027486。在此页面中，选择您在使用的 AppScan Source 版本所对应的选项卡，然后选择您在使用的 AppScan Source 组件。如果 AppScan Source 支持从其他开发环境打开和扫描文件，该支持将在**受支持软件**选项卡的**编译器和语言**部分中列出。
2. 选择一个或多个应用程序，然后将其拖动至"资源管理器"视图中。
3. 将所选项放置在**所有应用程序**节点上或其下方。

从 Apache Tomcat 和 WebSphere Application Server Liberty 概要文件应用程序服务器导入现有 Java 应用程序

如果您拥有已部署到受支持应用程序服务器的现有 Java 应用程序，那么可以自动将其导入到 AppScan Source。

开始之前

要了解 Apache Tomcat 和 WebSphere Application Server Liberty 概要文件的哪些版本受支持，请参阅 AppScan Source 系统需求。在此页面中，选择您在使用的 AppScan Source 版本所对应的选项卡，然后选择相应 AppScan Source for Analysis 组件。可以在**受支持的软件**部分中找到受支持的应用程序服务器。

过程

1. 完成以下其中一个操作：
   - 从主工作台菜单中选择**文件** > **添加应用程序** > **从应用程序服务器导入**。
   - 在"资源管理器"视图工具栏中，单击**"添加应用程序"菜单**向下箭头按钮，然后从菜单中选择**从应用程序服务器导入**。
   - 在"资源管理器"视图中，右键单击**所有应用程序**，然后从菜单中选择**添加应用程序** > **从应用程序服务器导入**。
2. 在"从应用程序服务器导入"对话框中，单击**浏览**以查找并选择应用程序服务器的安装位置，或者在相应字段中输入服务器路径和目录，然后单击**搜索**以在所输入位置

搜索应用程序。如果将该位置识别为受支持的应用程序服务器，那么将在此对话框的**要导入的应用程序**部分中列出可用的应用程序。在此部分中，选择要导入的应用程序，然后单击**确定**。

3. 将为从应用程序服务器导入的每个应用程序都创建一个 AppScan Source 应用程序。

结果

如果您是从 WebSphere Application Server Liberty 概要文件服务器（WebSphere Application Server V8.5 和更高版本）进行导入，那么可能会收到一条消息，指示需要进行手动 JSP 预编译。发生此情况是因为 Liberty 概要文件服务器不包含独立的 JSP 编译器。如果收到此消息，请删除已由于导入而创建的任何应用程序，然后按照『为 WebSphere Application Server Liberty 概要文件生成预编译的 JavaServer Pages』中的指示信息进行操作并再次从应用程序服务器进行导入。

缺省情况下，在导入应用程序时，AppScan Source仅扫描其 JSP 文件和 `web-inf/classes` 的内容。不扫描 `web-inf/lib` 的内容。如果想要扫描其他文件，可使用项目属性来设置要扫描的其他文件扩展名（请参阅第 216 页的『文件扩展名』）。例如，如果想要扫描 `.jar` 文件（包括 `web-inf/lib` 中的文件），请遵循第 69 页的『修改应用程序和项目属性』中关于修改项目属性的指示信息。在项目的"属性"视图中，选择 第 216 页的『文件扩展名』 选项卡。在视图的"其他扩展名"部分中，单击**添加扩展名**。在"新建扩展名"对话框中，在**扩展名**字段中输入 `jar`，然后选择**扫描具有此扩展名的文件**，并单击**确定**。单击视图右上角的**保存**（或从主菜单选择**文件** > **保存**），然后再次扫描项目。如果有不想要扫描的文件，可使用"项目"视图第 217 页的『源』选项卡除去这些文件。

如果服务器上的应用程序发生更改，并且您要使用已更改的内容来刷新 AppScan Source 应用程序，那么必须再次完成上述步骤（无需首先删除初始创建的应用程序，AppScan Source 将在进行重新导入时自动删除这些应用程序）。

注：如果从一个服务器导入一个 `.war` 文件然后从另一个服务器导入另一个名称相同的 `.war` 文件，那么第二个 `.war` 文件将覆盖第一个文件。要防止出现该情况，在导入第二个 `.war` 文件之前对其重命名。

为 WebSphere Application Server Liberty 概要文件生成预编译的 JavaServer Pages

如果您是从 WebSphere Application Server Liberty 概要文件（WebSphere Application Server V8.5 和更高版本）导入应用程序，那么需要进行手动 JSP 预编译（Liberty 概要文件不包含独立的 JSP 编译器）。本主题描述了设置手动 JSP 预编译所需的步骤。

过程

1. 按照 WebSphere Application Server Network Deployment 知识中心内关于如何创建 Liberty 概要文件服务器的指示信息进行操作。对于 WebSphere Application Server V8.5.5，请参阅 Creating a Liberty profile server by using developer tools 主题。
2. 在 Liberty 概要文件 `server.xml` 文件中，将以下内容添加到 `server description` 部分：

```
<jspEngine prepareJSPs="0"/>
<webContainer deferServletLoad="false"/>
```

例如：

```
<server description="new server">

    <!-- Enable features -->
    <featureManager>
        <feature>jsp-2.2</feature>
        <feature>localConnector-1.0</feature>
       <feature>appSecurity-2.0</feature>
        <feature>restConnector-1.0</feature>
    </featureManager>

    <!-- To access this server from a remote client
         add a host attribute to the following element,
         e.g. host="*" -->
    <httpEndpoint httpPort="9080" httpsPort="9443" id="defaultHttpEndpoint"/>

...
    <jspEngine prepareJSPs="0"/>
    <webContainer deferServletLoad="false"/>
...
</server>
```

server.xml 文件在 WebSphere Application Server 中心内进行了描述。对于 WebSphere Application Server V8.5.5，请参阅 Liberty profile: Configuration elements in the server.xml file 主题。

3. 使用以下方法之一来以调试方式启动服务器：
   - 添加 -Dwas.debug.mode=true JVM 参数，如 Setting generic JVM arguments in the WebSphere Application Server V8.5 Liberty profile 中所述。
   - 按照 WebSphere Application Server Network Deployment 知识中心内关于如何启动和停止服务器的指示信息进行操作。对于 WebSphere Application Server V8.5.5，请参阅 Starting and stopping a server by using developer tools 主题。

结果

完成这些步骤后，按照第 36 页的『从 Apache Tomcat 和 WebSphere Application Server Liberty 概要文件应用程序服务器导入现有 Java 应用程序』中的步骤从 WebSphere Application Server Liberty 概要文件导入 Java 应用程序。

添加 Eclipse 或基于 Eclipse 的产品工作空间

如果您拥有包含了 Java 和/或 IBM MobileFirst Platform 项目的 Eclipse 或 Rational Application Developer for WebSphere Software (RAD) 工作空间，那么可以将其导入到 AppScan Source for Analysis。

开始之前

添加工作空间之前，请确保您已安装并更新开发环境，如第 39 页的『配置 Eclipse 和 Rational Application Developer for WebSphere Software (RAD) 项目的开发环境』中所述。

过程

1. 完成以下其中一个操作：
   - 从主工作台菜单中选择**文件** > **添加应用程序** > **导入现有基于 Eclipse 的工作空间**。

- 在"资源管理器"视图工具栏中，单击**"添加应用程序"菜单**向下箭头按钮，然后从菜单中选择**导入现有基于 Eclipse 的工作空间**。
- 在"资源管理器"视图中，右键单击**所有应用程序**，然后从菜单中选择**添加应用程序 > 导入现有基于 Eclipse 的工作空间**。

2. 选择**工作空间类型**。
3. 浏览到工作空间，选择目录，然后单击**确定**以添加工作空间。

配置 Eclipse 和 Rational Application Developer for WebSphere Software (RAD) 项目的开发环境

在导入 Eclipse 或 Rational Application Developer for WebSphere Software (RAD) 项目之前，必须正确配置开发环境。尽管 Eclipse 是每种项目类型的基础，但不同版本的 AppScan Source 之间也有所不同。

要了解 AppScan Source 支持哪个版本的 Eclipse 和 Rational Application Developer for WebSphere Software (RAD)，请参阅http://www.ibm.com/support/docview.wss?uid=swg27027486。

要更多地了解如何为此来配置开发环境，请参阅以下帮助主题：

- 『Eclipse 或 Application Developer 更新』
- 第 40 页的『Eclipse 工作空间导入器：Eclipse 或 Rational Application Developer for WebSphere Software (RAD) 首选项配置』

Eclipse 或 Application Developer 更新

对于 AppScan Source 外部的 Eclipse 或 Application Developer 环境，必须确保已安装适当的软件更新。这些指示信息解释了如何获取并安装这些更新。此过程可能因版本而异。

开始之前

要点： AppScan Source for Development 需要 V1.5 或更高版本的 Java 运行时环境 (JRE)。如果环境指向不符合该需求的 JRE，请编辑 Eclipse 安装目录中的 `eclipse.ini` 文件，以使其指向符合该需求的 JRE。关于对 `eclipse.ini` 文件进行此更改的信息，请参阅 http://wiki.eclipse.org/Eclipse.ini 的指定 *JVM* 部分。

过程

1. 在 Eclipse **帮助**菜单中，选择用于安装新软件的选项（根据您所用的 Eclipse 版本，菜单标签不尽相同）。
2. 选择用于添加"本地更新站点"的选项。
3. 当提示您提供站点位置时，请浏览至 AppScan Source 安装目录。
4. 添加此更新站点，然后遵循显示的步骤，直到提示重新启动 Eclipse。
5. 安装完成后，会出现 AppScan Source 菜单。

Eclipse 工作空间导入器：Eclipse 或 Rational Application Developer for WebSphere Software (RAD) 首选项配置

AppScan Source for Analysis 安装会提供缺省 Eclipse 导入器。此导入器确定 Eclipse 和 JRE 的位置。如果缺省 Eclipse 导入器无法导入工作空间，那么可能需要创建新的 Eclipse 导入器。

开始之前

每个导入器配置均代表一个 Eclipse 或 Rational Application Developer for WebSphere Software (RAD) 安装。要使用这些配置将现有工作空间和项目导入到 AppScan Source for Analysis，可能还需要在 Eclipse 环境中安装 AppScan Source for Development 插件。

在添加 RAD 工作空间之前，您必须创建针对工作空间类型的配置。

过程

1. 在 AppScan Source for Analysis 中，从主工作台菜单中选择**编辑** > **首选项**。
2. 选择 **Eclipse 工作空间导入器**。
3. 单击**创建新配置**，然后完成"新建导入配置"对话框以创建新配置：
   - **产品**：选择相应产品

     注：如果无法选择先前用于创建工作空间的产品，请确保在尝试创建工作空间导入器之前已完成 第 39 页的『Eclipse 或 Application Developer 更新』中概括的配置步骤。
   - **名称**：导入器名称
   - **位置**：Eclipse 安装基本目录的路径
   - **JRE 位置**：Java Runtime Environment (JRE) 的根目录。使用 `<install_dir>\JDKS`（其中 `<install_dir>` 是 AppScan Source 安装位置） 中的 JDK 或任何其他首选 JDK。
4. 单击**确定**。
5. 要将导入器确定为缺省值，请选择导入器并单击**将所选配置设为缺省值**。这将使一个图标显示在导入器的**缺省值**列中。

为应用程序创建新项目

添加了应用程序之后，向应用程序添加项目。可以扫描的项目类型包括：Java/JSP、ASP、C/C++、COBOL、ColdFusion、.NET Assembly、Pattern Based、Perl、PHP、PL/SQL、T-SQL、Visual Basic 和 JavaScript。

关于此任务

如果使用 `make` 来编译项目，建议您使用 Ounce/Make 实用程序来创建项目文件，然后再添加项目文件。如果使用 `ant` 来编译项目，请使用 Ounce/Ant 来创建项目文件，然后添加项目文件。请参阅《*IBM Rational AppScan Source Edition Utilities* 用户指南》以了解有关 Ounce/Make 和Ounce/Ant 的详细信息。

注：AppScan Source 项目的缺省文件编码为 **ISO-8859-1**。此缺省文件编码可在"常规"首选项页面中进行更改。

注：使用"新建应用程序"向导和"新建项目"向导创建应用程序和项目时，将根据在向导中输入的**名称**来自动分配其文件名（例如，如果正在创建项目并且在**名称**字段中输入了 **MyProject**，那么项目文件名将为 MyProject.ppf）。可以使用"属性"视图来为应用程序和项目重命名。

过程

1. 在"资源管理器"视图中，选择要向其添加项目的应用程序（如果您尚未添加应用程序，请参阅第 30 页的『配置应用程序』）。
2. 完成以下某个操作以打开"新建项目向导"：
   a. 从主工作台菜单中依次选择**文件** > **添加项目** > **新项目**。
   b. 右键单击选定的应用程序，然后从上下文菜单选择**添加项目** > **新项目**。
3. 完成"新建项目向导"。

添加现有项目

您可以将先前通过 AppScan Source for Analysis 创建的 AppScan Source 项目（.ppf 文件）添加到 AppScan Source 应用程序。还可以添加 Eclipse 项目文件 (.epf)，由任何受支持构建集成工具（例如，Ounce/Maven 或 Ounce/Ant）创建的项目，或者通过 Microsoft Visual C/C++（.vcproj 或 .dsp）、VB.NET (.vbproj) 或 C# (.csproj) 创建的项目文件。

此表列出了可通过 AppScan Source for Analysis 打开和扫描的项目文件类型：

表 5. 要打开的项目文件类型

项目文件类型	文件扩展名
Microsoft Visual Studio (V6)	.dsp
Microsoft Visual Studio C/C++	.vcproj
Microsoft Visual Studio C#	.csproj
Microsoft Visual Studio Visual Basic	.vbproj
AppScan Source 项目文件	.ppf
Eclipse 项目文件	.epf

要了解如何添加现有项目，请参阅以下主题：

- 第 42 页的『通过用户界面操作添加现有项目』
- 第 42 页的『通过拖放来添加现有项目』

要点：如果您所处理的是在开发环境中具有依赖性的 AppScan Source 项目（例如 IBM MobileFirst Platform 项目），请确保在导入该项目之前在开发环境中对其进行构建。导入该项目后，如果您修改其中的文件，请确保在 AppScan Source 中进行扫描之前在开发环境中重新构建该项目（如果不执行此操作，那么 AppScan Source 将忽略对文件做出的修改）。

注：导入现有 .NET 项目时，您可以指定要扫描的其他组合件。在项目的"属性"视图的"其他组合件"选项卡中添加以下组合件。添加其他组合件时，您可以将要进行构建的 .NET 项目与不进行构建的组合件（包括第三方组合件）组合在单个扫描中。

注：还可通过将 WAR 和 EAR 文件拖放到"资源管理器"视图来添加这些文件，但这些文件将添加为应用程序而不是项目。有关更多信息，请参阅第 35 页的『通过拖放操作来添加现有应用程序』。

通过用户界面操作添加现有项目

过程

1. 在"资源管理器"视图中，选择要向其添加项目的应用程序（如果您尚未添加应用程序，请参阅第 30 页的『配置应用程序』）。
2. 完成以下其中一个操作：
   - 从主工作台菜单中依次选择**文件** > **添加项目** > **现有项目**。
   - 右键单击选定的应用程序，然后从上下文菜单中选择**添加项目** > **现有项目**。
3. 浏览至项目文件以将其添加到应用程序。

   要点：如果您所处理的是在开发环境中具有依赖性的 AppScan Source 项目（例如 IBM MobileFirst Platform 项目），请确保在导入该项目之前在开发环境中对其进行构建。导入该项目后，如果您修改其中的文件，请确保在 AppScan Source 中进行扫描之前在开发环境中重新构建该项目（如果不执行此操作，那么 AppScan Source 将忽略对文件做出的修改）。

通过拖放来添加现有项目

过程

1. 在工作站上，查找您要添加以进行扫描的项目（.ppf、.vcproj、.dsp、.vbproj 或 .csproj）。

   注：无法拖放由任何受支持构建集成工具（例如，Ounce/Maven 或 Ounce/Ant）创建的文件。
2. 选择项目，然后将其拖至 AppScan Source for Analysis"资源管理器"视图。
3. 完成以下步骤之一：
   a. 将所选项放置在现有应用程序中。
   b. 将所选项放置在**所有应用程序**节点上或其下方。因为应用程序必须包含项目但此操作不会将项目添加到现有应用程序，所以"新建应用程序向导"将提示您为项目创建新应用程序。为应用程序输入**名称**，然后浏览至在其中保存应用程序的**工作目录**。单击**完成**以创建新应用程序（在"资源管理器"视图中，添加的项目将包含在该应用程序中）。

   要点：如果您所处理的是在开发环境中具有依赖性的 AppScan Source 项目（例如 IBM MobileFirst Platform 项目），请确保在导入该项目之前在开发环境中对其进行构建。导入该项目后，如果您修改其中的文件，请确保在 AppScan Source 中进行扫描之前在开发环境中重新构建该项目（如果不执行此操作，那么 AppScan Source 将忽略对文件做出的修改）。

添加多个项目

向应用程序添加多个项目时，您可以将这些项目拖放到"资源管理器"视图中，也可以浏览项目的目录并将部分或所有项目导入到当前应用程序。

要了解如何添加多个项目，请参阅以下主题：

- 『通过用户界面操作添加多个项目』
- 『通过拖放添加多个项目』

要点：如果您所处理的是在开发环境中具有依赖性的 AppScan Source 项目（例如 IBM MobileFirst Platform 项目），请确保在导入该项目之前在开发环境中对其进行构建。导入该项目后，如果您修改其中的文件，请确保在 AppScan Source 中进行扫描之前在开发环境中重新构建该项目（如果不执行此操作，那么 AppScan Source 将忽略对文件做出的修改）。

通过用户界面操作添加多个项目

可将多个项目从目录（包括子目录）、Eclipse/Rational Application Developer for WebSphere Software (RAD) 工作空间或 Microsoft 解决方案文件添加到应用程序。

过程

1. 在"资源管理器"视图中，选择要向其添加项目的应用程序（如果您尚未添加应用程序，请参阅第 30 页的『配置应用程序』）。
2. 完成以下其中一个操作：
   - 从主工作台菜单中依次选择**文件** > **添加项目** > **多个项目**。
   - 右键单击选定的应用程序，然后从上下文菜单中选择**添加项目** > **多个项目**。
3. 在"添加多个项目"对话框中，完成以下某个操作：
   - 选择**从目录导入**，然后浏览至包含要添加的项目的根目录。选中**递归至子目录中**复选框以在子目录中搜索。
   - 选择**从基于 Eclipse 的工作空间导入**。选择**工作空间类型**，然后浏览至工作空间。选择工作空间目录，然后单击**确定**。
   - 选择**从 Microsoft 解决方案文件导入**。浏览至该文件并将其选中，然后单击**确定**。
4. 完成以下其中一个操作：
   - 单击**完成**以将项目添加到应用程序。
   - 单击**下一步**以查看搜索结果，并选择要添加的项目。然后单击**完成**。

   要点：如果您所处理的是在开发环境中具有依赖性的 AppScan Source 项目（例如 IBM MobileFirst Platform 项目），请确保在导入该项目之前在开发环境中对其进行构建。导入该项目后，如果您修改其中的文件，请确保在 AppScan Source 中进行扫描之前在开发环境中重新构建该项目（如果不执行此操作，那么 AppScan Source 将忽略对文件做出的修改）。

通过拖放添加多个项目

过程

1. 在工作站上，查找您要添加以进行扫描的项目（`.ppf`、`.vcproj`、`.dsp`、`.vbproj` 或 `.csproj`）。

   注：无法拖放由任何受支持构建集成工具（例如，Ounce/Maven 或 Ounce/Ant）创建的文件。
2. 对项目进行单选或多选，然后将其拖至"资源管理器"视图中。
3. 将所选项放置在现有应用程序中。

注：您也可以将所选项放到**所有应用程序**节点上或其下方，但是不建议这样做。相反，建议将多个项目放入现有应用程序；或者，如果需要新应用程序，建议逐个放入项目。

因为应用程序必须包含项目，但将项目放到**所有应用程序**节点上或之下的操作不会将项目添加到现有应用程序，所以"新建应用程序向导"将提示您为要添加到视图中的每个项目创建新应用程序。

要将多个项目添加到尚不存在的新应用程序中，请首先创建应用程序，然后再将选定项目拖放到应用程序中。

要点：如果您所处理的是在开发环境中具有依赖性的 AppScan Source 项目（例如 IBM MobileFirst Platform 项目），请确保在导入该项目之前在开发环境中对其进行构建。导入该项目后，如果您修改其中的文件，请确保在 AppScan Source 中进行扫描之前在开发环境中重新构建该项目（如果不执行此操作，那么 AppScan Source 将忽略对文件做出的修改）。

添加新 Arxan 项目

"项目配置向导"将帮助您手动创建 Arxan 项目并将其添加到应用程序。

关于此任务

本主题中的步骤将指导您完成"新建项目向导"（如果要在其中创建应用程序，那么为"新建应用程序向导"）中的所有页面。在选定项目的"属性"视图中创建项目后，可以修改向导中进行的设置。

过程

1. 在"资源管理器"视图中，选择要向其添加项目的应用程序（如果您尚未添加应用程序，请参阅第 30 页的『配置应用程序』）。
2. 完成以下某个操作以打开"新建项目向导"：
   a. 从主工作台菜单中依次选择**文件** > **添加项目** > **新项目**。
   b. 右键单击选定的应用程序，然后从上下文菜单选择**添加项目** > **新项目**。
3. 在该向导的"选择项目类型"页面中，选择 **Arxan Android** 或 **Arxan iOS** 来作为项目类型，然后单击**下一步**以前进到下一个向导页面。
4. 在"项目源"向导页面中：
   a. 确定项目源。项目源包括在其中找到项目文件以及要包含在项目中的其他任何个别文件的目录。

      对项目命名并指定工作目录。**工作目录**是 AppScan Source 项目文件 (.ppf) 所在的位置。它也是所有相对路径的基础。
   b. 单击**添加源根目录**以指定源代码根目录以及要在扫描中包含或排除的目录或文件。 添加源根目录之后，可以从该源根目录中排除特定目录或文件。要执行此操作，请选择源根目录中的目录或文件（或者对这些项进行多选），右键单击所选内容，然后从菜单中选择**排除**。如果包含或排除文件，文件名左侧的图标将更改。
5. 单击**完成**。

添加新 ASP 项目

"项目配置向导"帮助您手动创建 ASP 项目并将其添加到应用程序。

关于此任务

注：该项目类型仅在 Windows 上受支持。

本主题中的步骤将指导您完成"新建项目向导"（如果要在其中创建应用程序，那么为"新建应用程序向导"）中的所有页面。但是，向导中的某些页面是可选的（激活**完成**按钮时所需设置已完成）。在选定项目的"属性"视图中创建项目后，可以修改向导中进行的设置。如果在不完成可选页面的情况下完成了"新建项目向导"，那么以后可在"属性"视图中更改这些页面的设置。

注：对于 PHP、VB6 和 Classic ASP，仅 ISO-8859-1 (Western Europe)、UTF-8 和 UTF-16 字符集受支持。

过程

1. 在"资源管理器"视图中，选择要向其添加项目的应用程序（如果您尚未添加应用程序，请参阅第 30 页的『配置应用程序』）。
2. 完成以下某个操作以打开"新建项目向导"：
   a. 从主工作台菜单中依次选择**文件** > **添加项目** > **新项目**。
   b. 右键单击选定的应用程序，然后从上下文菜单选择**添加项目** > **新项目**。
3. 在向导的"选择项目类型"页面中，选择 **ASP** 作为项目类型，然后单击**下一步**以前进到下一向导页面。
4. 在"项目源"向导页面中：
   a. 确定项目源。项目源包括在其中找到项目文件以及要包含在项目中的其他任何个别文件的目录。

      对项目命名并指定工作目录。**工作目录**是 AppScan Source 项目文件 (`.ppf`) 所在的位置。它也是所有相对路径的基础。
   b. 单击**添加源根目录**以指定源代码根目录以及要在扫描中包含或排除的目录或文件。 添加源根目录之后，可以从该源根目录中排除特定目录或文件。要执行此操作，请选择源根目录中的目录或文件（或者对这些项进行多选），右键单击所选内容，然后从菜单中选择**排除**。如果包含或排除文件，文件名左侧的图标将更改。
5. 单击**下一步**以前进到下一向导页面。
6. 在"ASP 项目配置"页面中：
   a. 通过确定 ASP 内容根目录和缺省语言来配置 ASP 项目：

      ASP 内容根目录：与主 Web 或域 URL 对应的目录

      缺省语言：VB 脚本（缺省）或 JavaScript
   b. 添加、删除或移动 ASP 项目进行编译所依赖于的类型库（`dll`、`exe`、`ocx` 或 `tlb`）。
7. 单击**完成**。

添加新 C/C++ 项目

关于此任务

向应用程序添加新 C/C++ 项目时，请指定要扫描的源文件集合：

- include 路径
- 预处理器定义
- 选项

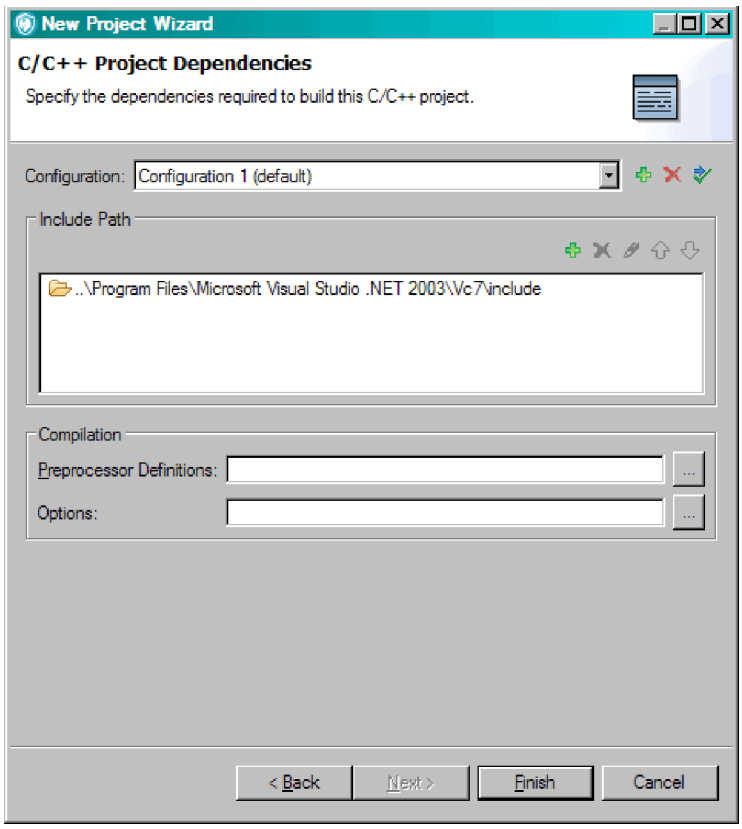
本主题中的步骤将指导您完成"新建项目向导"（如果要在其中创建应用程序，那么为"新建应用程序向导"）中的所有页面。但是，向导中的某些页面是可选的（激活**完成**按钮时所需设置已完成）。在选定项目的"属性"视图中创建项目后，可以修改向导中进行的设置。如果在不完成可选页面的情况下完成了"新建项目向导"，那么以后可在"属性"视图中更改这些页面的设置。

要点：为了扫描 C++ 项目，项目必须进行编译并且链接时不会出错。

过程

1. 在"资源管理器"视图中，选择要向其添加项目的应用程序（如果您尚未添加应用程序，请参阅第 30 页的『配置应用程序』）。
2. 完成以下某个操作以打开"新建项目向导"：
   a. 从主工作台菜单中依次选择**文件** > **添加项目** > **新项目**。
   b. 右键单击选定的应用程序，然后从上下文菜单选择**添加项目** > **新项目**。
3. 在向导的"选择项目类型"页面中，选择 **C/C++** 作为项目类型，然后单击**下一步**以前进到下一向导页面。
4. 在"项目源"向导页面中：
   a. 确定项目源。项目源包括在其中找到项目文件以及要包含在项目中的其他任何个别文件的目录。

      对项目命名并指定工作目录。**工作目录**是 AppScan Source 项目文件 (.ppf) 所在的位置。它也是所有相对路径的基础。
   b. 单击**添加源根目录**以指定源代码根目录以及要在扫描中包含或排除的目录或文件。 添加源根目录之后，可以从该源根目录中排除特定目录或文件。要执行此操作，请选择源根目录中的目录或文件（或者对这些项进行多选），右键单击所选内容，然后从菜单中选择**排除**。如果包含或排除文件，文件名左侧的图标将更改。
5. 单击**下一步**以前进到下一向导页面。
6. 在"C/C++ 项目依赖关系"页面中，通过指定项目配置和 include 路径来添加项目依赖关系。



- **配置**：项目的所有可用配置的列表。添加新配置或删除现有配置。为每个配置定义所有剩余设置。

  您可以为 C/C++ 项目定义多个配置，如 Debug 和 Release。Configuration 1 是缺省项目配置名称。
- **Include 路径**：使用此部分可向包含项目所需 #include 文件的目录添加标准路径名。
- **预处理器定义**：使用此字段可添加为项目定义的预处理符号。预处理器定义特定于 C/C++ 代码。指定预处理器定义时，不要包含编译器的 -D 选项（例如，指定 a=definition1 而不是 -Da=definition1）。指定多个定义时，请使用分号分隔的列表。
- **选项**：项目配置所需的其他编译器参数。

7. 单击**完成**。

添加新 COBOL 项目

项目配置向导帮助您手动创建 COBOL 项目并帮助您将其添加到应用程序中。

关于此任务

本主题中的步骤将指导您完成"新建项目向导"（如果要在其中创建应用程序，那么为"新建应用程序向导"）中的所有页面。在选定项目的"属性"视图中创建项目后，可以修改向导中进行的设置。

过程

1. 在"资源管理器"视图中，选择要向其添加项目的应用程序（如果您尚未添加应用程序，请参阅第 30 页的『配置应用程序』）。
2. 完成以下某个操作以打开"新建项目向导"：
   a. 从主工作台菜单中依次选择**文件** > **添加项目** > **新项目**。
   b. 右键单击选定的应用程序，然后从上下文菜单选择**添加项目** > **新项目**。
3. 在向导的"选择项目类型"页面中，选择 **COBOL** 作为项目类型，然后单击**下一步**以前进到下一向导页面。
4. 在"项目源"向导页面中：
   a. 确定项目源。项目源包括在其中找到项目文件以及要包含在项目中的其他任何个别文件的目录。

      对项目命名并指定工作目录。**工作目录**是 AppScan Source 项目文件 (.ppf) 所在的位置。它也是所有相对路径的基础。
   b. 单击**添加源根目录**以指定源代码根目录以及要在扫描中包含或排除的目录或文件。 添加源根目录之后，可以从该源根目录中排除特定目录或文件。要执行此操作，请选择源根目录中的目录或文件（或者对这些项进行多选），右键单击所选内容，然后从菜单中选择**排除**。如果包含或排除文件，文件名左侧的图标将更改。
5. 单击**完成**。

添加新 ColdFusion 项目

"项目配置向导"帮助您手动创建 ColdFusion 项目并将其添加到应用程序。

关于此任务

本主题中的步骤将指导您完成"新建项目向导"（如果要在其中创建应用程序，那么为"新建应用程序向导"）中的所有页面。在选定项目的"属性"视图中创建项目后，可以修改向导中进行的设置。

过程

1. 在"资源管理器"视图中，选择要向其添加项目的应用程序（如果您尚未添加应用程序，请参阅第 30 页的『配置应用程序』）。
2. 完成以下某个操作以打开"新建项目向导"：
   a. 从主工作台菜单中依次选择**文件** > **添加项目** > **新项目**。
   b. 右键单击选定的应用程序，然后从上下文菜单选择**添加项目** > **新项目**。
3. 在向导的"选择项目类型"页面中，选择 **ColdFusion** 作为项目类型，然后单击**下一步**以前进到下一向导页面。
4. 在"项目源"向导页面中：
   a. 确定项目源。项目源包括在其中找到项目文件以及要包含在项目中的其他任何个别文件的目录。

      对项目命名并指定工作目录。**工作目录**是 AppScan Source 项目文件 (.ppf) 所在的位置。它也是所有相对路径的基础。

b. 单击**添加源根目录**以指定源代码根目录以及要在扫描中包含或排除的目录或文件。 添加源根目录之后，可以从该源根目录中排除特定目录或文件。要执行此操作，请选择源根目录中的目录或文件（或者对这些项进行多选），右键单击所选内容，然后从菜单中选择**排除**。如果包含或排除文件，文件名左侧的图标将更改。

5. 单击**完成**。

添加新 Java 或 JavaServer Page (JSP) 项目

向应用程序添加新 Java 项目时，请指定项目名称，浏览至工作目录，然后指定源根目录和项目依赖性。

关于此任务

本主题中的步骤将指导您完成"新建项目向导"（如果要在其中创建应用程序，那么为"新建应用程序向导"）中的所有页面。但是，向导中的某些页面是可选的（激活**完成**按钮时所需设置已完成）。在选定项目的"属性"视图中创建项目后，可以修改向导中进行的设置。如果在不完成可选页面的情况下完成了"新建项目向导"，那么以后可在"属性"视图中更改这些页面的设置。

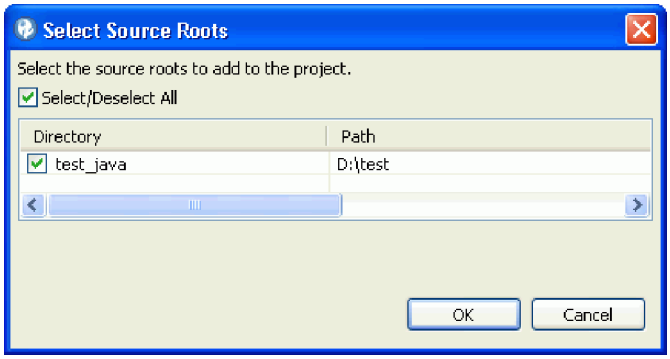
过程

1. 在"资源管理器"视图中，选择要向其添加项目的应用程序（如果您尚未添加应用程序，请参阅第 30 页的『配置应用程序』）。
2. 完成以下某个操作以打开"新建项目向导"：
   a. 从主工作台菜单中依次选择**文件** > **添加项目** > **新项目**。
   b. 右键单击选定的应用程序，然后从上下文菜单选择**添加项目** > **新项目**。
3. 在向导的"选择项目类型"页面中，选择 **Java/JSP** 作为项目类型，然后单击**下一步**以前进到下一向导页面。
4. 在"项目源"向导页面中：
   a. 确定项目源，它们包括在其中找到项目文件以及要包含在项目中的其他任何个别文件的目录。

      对项目命名并指定工作目录。**工作目录**是 AppScan Source 项目文件 (`.ppf`) 的位置和所有相对路径的基础。
   b. 手动添加源代码根目录或允许 AppScan Source for Analysis 自动查找所有有效的源代码根目录。

      要点：

      - 要分析 Java 类文件，必须使用 `-g` 选项通过 `javac` 对这些文件进行编译。AppScan Source 分析依赖于由此选项生成的调试信息。
      - 如果项目包括含有特定语言字符的 Java 源文件且您要在非本机语言环境（例如，UTF-8）中运行，那么扫描将失败，并且在控制台中将返回错误和/或警告。
      - 要自动查找源根目录，请执行以下操作：
        1) 单击**查找源根目录**，然后浏览至源代码的根目录。
        2) 从找到的所有源根目录的列表中，选择要添加到项目的源根目录。

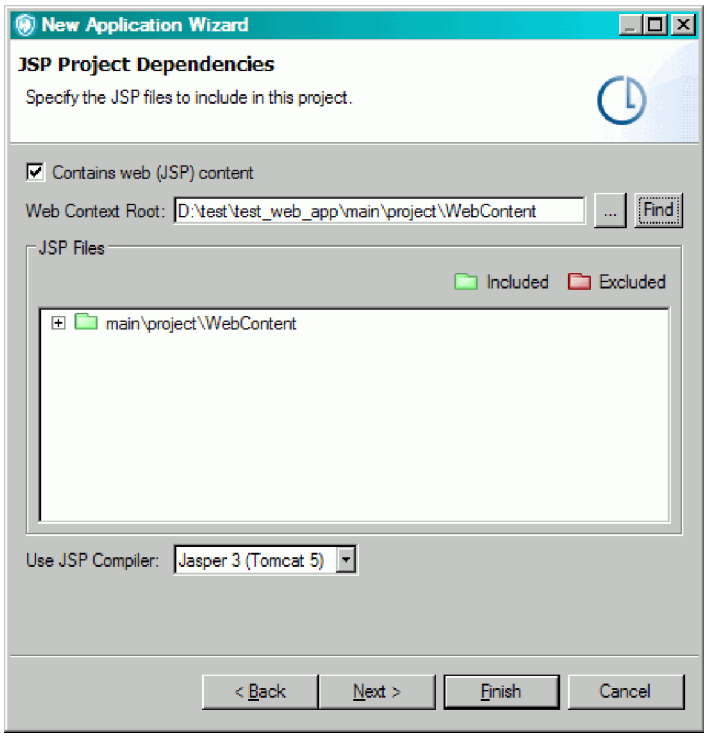


3) 单击**确定**。要包含在报告中的源将显示在**项目源**对话框中。

- 要手动查找源根目录，请执行以下操作：
  1) 单击**添加源根目录**。
  2) 选择源代码根目录或文件。
  3) 单击**确定**。添加源根目录之后，可以从该源根目录中排除特定目录或文件。要执行此操作，请选择目录或文件（或者对这些项进行多选），右键单击所选内容，然后从菜单中选择**排除**。如果包含或排除文件，文件名左侧的图标将更改。

单击**完成**以在不设置项目依赖性的情况下添加项目 - 或单击**下一步**以确定项目依赖性。

5. 在"JSP 项目依赖性"页面中：
   a. 确定 JavaServer Page (JSP) 项目依赖性：对于包含 JavaServer Page 的 Java 项目，确定 JSP 项目依赖性。如果项目是含有 JavaServer Page 的 Web 应用程序，那么请选中**包含 Web (JSP) 内容**复选框。



b. 手动选择 **Web 上下文根**，或者单击**查找**进行查找。**Web 上下文根**是 WAR 文件或包含 WEB-INF 目录的某个目录。Web 上下文根必须是有效 Web 应用程序的根目录。

c. 为项目选择 **JSP 编译器**。现成可用的 Tomcat 7 是缺省 JSP 编译器设置（缺省 JSP 编译器可以在 Java 和 JSP 首选项页面中进行更改）。要了解 AppScan Source 支持的编译器的相关信息，请参阅http://www.ibm.com/support/docview.wss?uid=swg27027486。

Apache Tomcat V7 和 V8 包含在 AppScan Source 的安装中。如果未配置 **Tomcat 7** 和 **Tomcat 8** 首选项页面，那么 AppScan Source 将使用当前提供且标记为缺省选项的 Tomcat JSP 编译器来编译 JSP 文件。如果您想要运用外部受支持 Tomcat 编译器，请使用 Tomcat 首选项页面来指向本地 Tomcat 安装版。

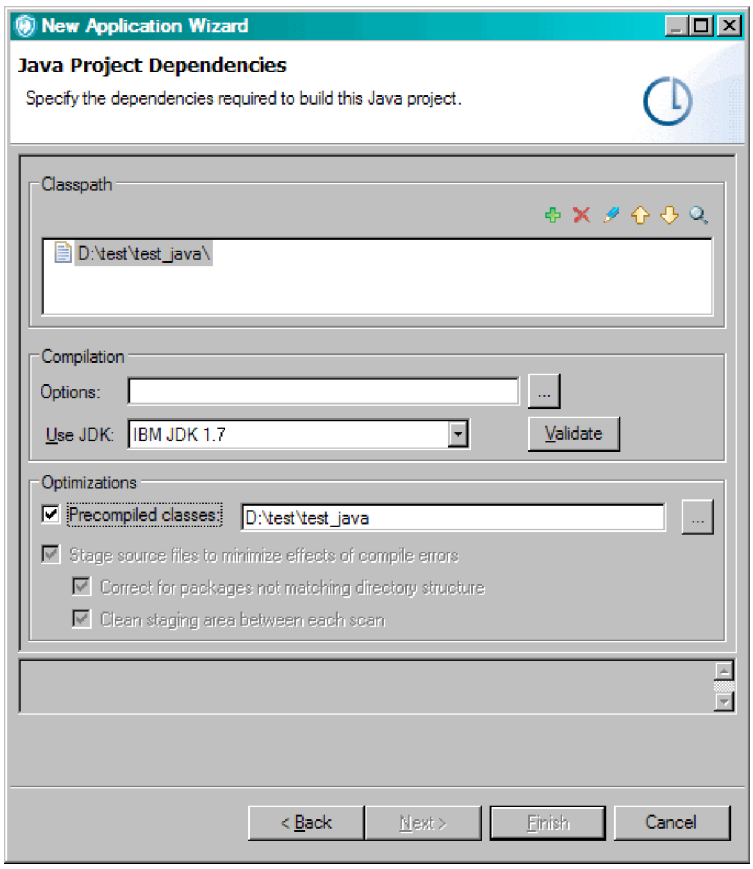
如果使用的是 Oracle WebLogic Server 或 WebSphere Application Server，那么必须将适用的首选项页面配置为指向应用程序服务器的本地安装版，以便其可在分析期间用于 JSP 编译。如果尚未完成该配置，那么选择 JSP 编译器时将显示一条消息以提示您完成配置。如果单击消息中的**是**，那么您将被转至相应的首选项页面。如果单击**否**，那么 JSP 编译器选择旁边将显示一条警告链接（访问该链接将打开首选项页面）。

单击**完成**以添加带有 JSP 项目依赖性的项目 - 或单击**下一步**以确定 Java 项目依赖性。

6. 在"Java 项目依赖性"页面中，确定构建此 Java 项目所需的依赖关系：

a. 手动添加 JAR 文件，或者单击**查找**以让 AppScan Source for Analysis 搜索包含依赖的 JAR 和类文件的目录。

类路径列表显示了该项目的相对路径。类路径必须指定所需的 JAR 文件和含有项目所需的类文件的目录。



- **添加**、**除去**、**上移**和**下移**：在类路径中添加或除去文件，或者按顺序将其上移或下移。
- **查找**：根据项目中的源文件查找 JAR 和类路径条目。

要点：如果 Java 项目包含 JavaServer Page，那么还必须添加 JSP 项目依赖性。

- 要手动查找项目依赖性，请执行以下操作：
  1) 单击"类路径"部分工具栏中的**添加**，然后选择编译 Java 项目所需的 JAR 和类文件目录。
  2) 单击**确定**。JAR 文件和目录将显示在类路径中。如有必要，请更改顺序。
- 要自动查找依赖关系，请执行以下操作：
  1) 单击"类路径"部分工具栏中的**查找**。
  2) 指定要在其中查找编译 Java 项目所需的 JAR 和类文件的目录。
  3) 如果要让 AppScan Source for Analysis 基于源并通过使用提供的搜索路径来查找必需的项目依赖性，请选中**在源和 JAR 文件中查找**复选框。
  4) 单击**下一步**以查找项目依赖性并识别冲突。
- 要解决冲突，请执行以下操作：
  1) 如果存在冲突，请在"解决冲突"对话框中选择要解决的条目，然后单击**解决**（或单击**下一步**以自动解决冲突）。当 AppScan Source for Analysis 在某个目录中找到满足依赖关系的多个 JAR 或类时，便会发生冲突。

在未解决的冲突左侧将出现一个红色图标。一旦解决了冲突，红色图标将更改为绿色图标且项目为**已解析**。您也可以**除去**冲突。

2) 解决或除去冲突后，您可能希望验证、重新排序或除去类路径条目。记录找不到的导入的列表。任何未解析的导入都会在 AppScan Source for Analysis 扫描时导致编译错误。

b. **选项**：指定项目所需的其他任何编译器参数。

编译选项是传递到编译器以便源文件可进行编译的选项。例如，`-source 1.5` 指定项目的源级别。

c. **使用 JDK**：指定扫描此代码时要使用的 Java Development Kit (JDK)。缺省情况下，将使用 **IBM JDK 1.8**。AppScan Source 还提供了 **IBM JDK 1.7** 以供选择。要定义其他 JDK，或选择其他缺省 JDK，使用 **Java 和 JSP 首选项**。

注：JSP 项目的缺省编译器是 Tomcat 7，后者需要 Java V1.6 或更高版本。如果 **Tomcat 7** 保留为缺省值，那么使用更低版本的 JDK 将导致扫描期间出现编译错误。

d. **验证**操作可确保正确配置项目依赖性。它将检查 Java 项目中源和类路径之间的配置冲突，也会检查编译错误。如果类路径中的类在源根目录中重复，那么将存在冲突。

如果冲突存在，那么验证文本区域将显示在类路径上定义类的 JAR 或位置，以及源中是否存在重复。从类路径除去冲突，然后重新运行检查。

检查完冲突后，**验证**将确定项目是否编译和报告了任何编译错误。

e. **预编译的类**：此字段允许您使用预编译的 Java 或 JSP 类文件而不是在扫描期间进行编译。

f. **登台源文件以最大限度减少编译错误所产生的影响**：如果您的源代码正确进行了编译且在目录中进行了正确安排（匹配软件包），那么请清除此复选框。

g. **更正与目录结构不匹配的软件包**：如果软件包与目录结构不匹配，那么请选中此复选框。

h. **清理各扫描之间的登台区域**：优化选项。

7. 单击**完成**。

结果

提示：如果要扫描 Java 而且 Java 项目中缺少依赖关系，那么 AppScan Source 将通过合成依赖关系会提供的片段来创建跟踪。该合成可能不会准确地反映 `.jar` 文件中的信息。要限制合成并因此提高结果的准确性，可指定缺少的依赖关系，如下所示：

1. 扫描之后，打开 `<data_dir>\logs\scanner_exceptions.log`（其中 `<data_dir>` 是 AppScan Source 程序数据的位置，如第 275 页的『安装和用户数据文件位置』中所述） 以查看 AppScan Source 是否报告了缺少的依赖关系。
2. 修改项目属性以包含依赖关系。为此，遵循第 69 页的『修改应用程序和项目属性』中的指示信息，然后在 **JSP 项目依赖关系**或**项目依赖关系**选项卡中指定和保存依赖关系。
3. 重新扫描项目。

注：缺少情况下，AppScan Source 将扫描缺少依赖关系的 Java 文件和 Java 字节代码，或扫描编译错误。可如下所示更改这些设置：

1. 在文本编辑器中打开 <data_dir>\config\scan.ozsettings。
2. 要更改编译错误设置，找到文件中的 compile_java_sources_with_errors。此设置将与以下类似：

```
<Setting
  name="compile_java_sources_with_errors"
  value="true"
  default_value="true"
  type="bool"
  hidden="true"
  display_name="compile_java_sources_with_errors"
  description="Attempt to scan java code with compilation errors."
/>
```

3. 要更改缺少的依赖关系设置，找到文件中的 scan_java_bytecode_without_dependencies。此设置将与以下类似：

```
<Setting
  name="scan_java_bytecode_without_dependencies"
  value="true"
  default_value="true"
  type="bool"
  hidden="true"
  display_name="scan_java_bytecode_without_dependencies"
  description="Scans Java bytecode even when some of
    the dependencies are missing by artificially
    synthesizing the unresolved symbols."
/>
```

4. 在设置中，修改 value 属性。如果属性设置为 true，该设置将打开。如果编译错误设置设置为 false，那么 AppScan Source 将在扫描期间跳过有编译错误的 Java 代码。如果缺少的依赖关系设置设置为 false，那么缺少依赖关系时 AppScan Source 将不会扫描 Java 字节码。
5. 在修改该设置后保存文件，并启动或重新启动 AppScan Source。

向 JSP 项目添加内容

JavaServer Page (JSP) 项目包含基于 JavaServer Pages 技术构建的 Web 应用程序。

关于此任务

要成功扫描 JSP 项目，JavaServer Page 必须处于有效的 Web 应用程序结构中。在配置 JSP 项目之前，您应该先熟悉 Web 应用程序结构。在配置 JSP 项目之前，您应该先熟悉 Web 应用程序结构。

部署到 Web 应用程序服务器（如 Tomcat）中的 Web 应用程序需要标准的目录结构。部署的应用程序可以是在目录结构中安排的一组文件或者是 WAR 文件。就 WAR 文件而言，目录结构包含在 ZIP 文件中，同时，web context root 作为目录结构的根。

在 Web 上下文根下，可找到以下标准目录：

表 *6. Web* 上下文根目录

<web-context-root>\	
WEB-INF\	
classes\	在目录（软件包）中安排的 Java 类文件

表 *6. Web* 上下文根目录 *(续)*

lib\	添加到类路径的 Jar 文件
web.xml	web.xml 描述应用程序可用的资源

其他目录包含可能也存在的必要文件。例如，您经常会看到包含内容（JSP 和 HTML 文件）以及标记库的目录：

表 *7.* 其他目录

<web-context-root>\	
jsp\	包含应用程序中的 JavaServer Page
WEB-INF\	
tld\	包含应用程序中所使用的标记库

除了这些标准 Web 应用程序目录之外，Web 应用程序服务器还可以具有特殊目录，在这些目录中预期能够找到由所有已部署的 Web 应用程序共享的类文件和 JAR 文件。例如，Tomcat 7 将这些 JAR 文件放置在 common\lib 或 common\endorsed 目录中。这些非标准目录的位置是特定于每个应用程序服务器的。

要点：扫描 JavaServer Page 之前，请确认 Web 上下文根中存在所有必要的文件。AppScan Source for Analysis 仅扫描 Web 上下文根中的 JavaServer Pages。

过程

1. 将文件复制到 Web 上下文根下的相应位置（如果有必要）。
2. 将 Web 上下文根指定为目录或包含所有 JavaServer Page 的 WAR 文件。
3. 确保类路径包括 JAR 或类文件目录。
4. 配置项目属性。

结果

AppScan Source for Analysis 将 WEB-INF\classes 目录以及 WEB-INF\lib 中的所有 JAR 文件添加到类路径（仅针对 JSP）。可以添加未包含在 Web-INF 路径中但编译 JSP 时需要的项。这些 JAR 文件类似于 weblogic.jar 或放置在应用程序服务器常见目录中的供应商 JAR 文件。

JSP 源是您要扫描的 Web 上下文根下的 JavaServer Page。源文件是相对于 Web 上下文根而言的。指定 JSP 源时，您只能指定 Web 上下文根中的文件集。

JSP 项目源包括在其中找到项目文件以及要包含在项目中的任何其他个别文件的目录。

- 指定 Web 上下文根中的 JavaServer Pages 的子集。如果未完成此操作，那么将扫描所有文件。
- 如果 JavaServer Page 取决于 Java 代码，那么必须指定这些源。
- JSP 文件包括 jsp 和 jspx 文件。

添加新的 JavaScript 项目

"项目配置向导"帮助您手动创建 JavaScript 项目并将其添加到应用程序。

关于此任务

本主题中的步骤将指导您完成"新建项目向导"（如果要在其中创建应用程序，那么为"新建应用程序向导"）中的所有页面。在选定项目的"属性"视图中创建项目后，可以修改向导中进行的设置。

过程

1. 在"资源管理器"视图中，选择要向其添加项目的应用程序（如果您尚未添加应用程序，请参阅第 30 页的『配置应用程序』）。
2. 完成以下某个操作以打开"新建项目向导"：
   a. 从主工作台菜单中依次选择**文件** > **添加项目** > **新项目**。
   b. 右键单击选定的应用程序，然后从上下文菜单选择**添加项目** > **新项目**。
3. 在向导的"选择项目类型"页面中，选择 **JavaScript** 作为项目类型，然后单击**下一步**以前进到下一向导页面。
4. 在"项目源"向导页面中：
   a. 确定项目源。项目源包括在其中找到项目文件以及要包含在项目中的其他任何个别文件的目录。

      对项目命名并指定工作目录。**工作目录**是 AppScan Source 项目文件 (`.ppf`) 所在的位置。它也是所有相对路径的基础。
   b. 单击**添加源根目录**以指定源代码根目录以及要在扫描中包含或排除的目录或文件。 添加源根目录之后，可以从该源根目录中排除特定目录或文件。要执行此操作，请选择源根目录中的目录或文件（或者对这些项进行多选），右键单击所选内容，然后从菜单中选择**排除**。如果包含或排除文件，文件名左侧的图标将更改。
5. 单击**完成**。

添加新的 .NET 组合件项目

"新建项目向导"会帮助您创建 .NET 组合件项目。当源文件可能不可用或不可构建时，.NET 组合件项目可以用来扫描已编译的 .NET 组合件文件。 .NET 组合件项目包含工作目录和源列表，它可能是目录或个别组合件文件。

关于此任务

注：该项目类型仅在 Windows 上受支持。

本主题中的步骤将指导您完成"新建项目向导"（如果要在其中创建应用程序，那么为"新建应用程序向导"）中的所有页面。在选定项目的"属性"视图中创建项目后，可以修改向导中进行的设置。

过程

1. 在"资源管理器"视图中，选择要向其添加项目的应用程序（如果您尚未添加应用程序，请参阅第 30 页的『配置应用程序』）。
2. 完成以下某个操作以打开"新建项目向导"：
   a. 从主工作台菜单中依次选择**文件** > **添加项目** > **新项目**。
   b. 右键单击选定的应用程序，然后从上下文菜单选择**添加项目** > **新项目**。

3. 在向导的"选择项目类型"页面中，选择 **.NET 组合件**作为项目类型，然后单击**下一步**以前进到下一向导页面。
4. 在"项目源"向导页面中：
   a. 确定项目源。项目源包括在其中找到项目文件以及要包含在项目中的其他任何个别文件的目录。

      对项目命名并指定工作目录。**工作目录**是 AppScan Source 项目文件 (.ppf) 所在的位置。它也是所有相对路径的基础。
   b. 单击**添加源根目录**以指定源代码根目录以及要在扫描中包含或排除的目录或文件。 添加源根目录之后，可以从该源根目录中排除特定目录或文件。要执行此操作，请选择源根目录中的目录或文件（或者对这些项进行多选），右键单击所选内容，然后从菜单中选择**排除**。如果包含或排除文件，文件名左侧的图标将更改。
5. 单击**完成**。

添加新的基于模式的项目

关于此任务

"新建项目向导"帮助您手动创建 Pattern Based 项目并将其添加到应用程序。Pattern Based 项目包括用于基于模式的分析和扫描的任何与语言无关的文件的集合。

例如，您可能希望对 .xml 和 .config 文件进行逻辑分组并在其中搜索某些基于模式的表达式。AppScan Source for Analysis 扫描文件并搜索表达式（请参阅第 205 页的『以基于模式的规则进行定制』以获取详细信息）。

本主题中的步骤将指导您完成"新建项目向导"（如果要在其中创建应用程序，那么为"新建应用程序向导"）中的所有页面。在选定项目的"属性"视图中创建项目后，可以修改向导中进行的设置。

过程

1. 在"资源管理器"视图中，选择要向其添加项目的应用程序（如果您尚未添加应用程序，请参阅第 30 页的『配置应用程序』）。
2. 完成以下某个操作以打开"新建项目向导"：
   a. 从主工作台菜单中依次选择**文件** > **添加项目** > **新项目**。
   b. 右键单击选定的应用程序，然后从上下文菜单选择**添加项目** > **新项目**。
3. 在向导的"选择项目类型"页面中，选择 **Pattern Based** 作为项目类型，然后单击**下一步**以前进到下一向导页面。
4. 在"项目源"向导页面中：
   a. 确定项目源。项目源包括在其中找到项目文件以及要包含在项目中的其他任何个别文件的目录。

      对项目命名并指定工作目录。**工作目录**是 AppScan Source 项目文件 (.ppf) 所在的位置。它也是所有相对路径的基础。
   b. 单击**添加源根目录**以指定源代码根目录以及要在扫描中包含或排除的目录或文件。 添加源根目录之后，可以从该源根目录中排除特定目录或文件。要执行此

操作，请选择源根目录中的目录或文件（或者对这些项进行多选），右键单击所选内容，然后从菜单中选择**排除**。如果包含或排除文件，文件名左侧的图标将更改。

5. 单击**完成**。

添加新 Perl 项目

"新建项目向导"帮助您手动创建 Perl 项目并将其添加到应用程序。

过程

1. 在"资源管理器"视图中，选择要向其添加项目的应用程序（如果您尚未添加应用程序，请参阅第 30 页的『配置应用程序』）。
2. 完成以下某个操作以打开"新建项目向导"：
   a. 从主工作台菜单中依次选择**文件** > **添加项目** > **新项目**。
   b. 右键单击选定的应用程序，然后从上下文菜单选择**添加项目** > **新项目**。
3. 在向导的"选择项目类型"页面中，选择 **Perl** 作为项目类型，然后单击**下一步**以前进到下一向导页面。
4. 在"项目源"向导页面中：
   a. 确定项目源。项目源包括在其中找到项目文件以及要包含在项目中的其他任何个别文件的目录。

      对项目命名并指定工作目录。**工作目录**是 AppScan Source 项目文件 (`.ppf`) 所在的位置。它也是所有相对路径的基础。
   b. 单击**添加源根目录**以指定源代码根目录以及要在扫描中包含或排除的目录或文件。 添加源根目录之后，可以从该源根目录中排除特定目录或文件。要执行此操作，请选择源根目录中的目录或文件（或者对这些项进行多选），右键单击所选内容，然后从菜单中选择**排除**。如果包含或排除文件，文件名左侧的图标将更改。
5. 单击**完成**。

PHP 项目配置

向应用程序添加新的 PHP（超文本预处理器项目）时，请指定项目名称，浏览至工作目录，然后指定源根目录和项目依赖关系。创建项目之后，也可以在项目属性的"项目依赖关系"选项卡中设置项目依赖关系。

关于此任务

本主题中的步骤将指导您完成"新建项目向导"（如果要在其中创建应用程序，那么为"新建应用程序向导"）中的所有页面。但是，向导中的某些页面是可选的（激活**完成**按钮时所需设置已完成）。在选定项目的"属性"视图中创建项目后，可以修改向导中进行的设置。如果在不完成可选页面的情况下完成了"新建项目向导"，那么以后可在"属性"视图中更改这些页面的设置。

注：对于 PHP、VB6 和 Classic ASP，仅 ISO-8859-1 (Western Europe)、UTF-8 和 UTF-16 字符集受支持。

过程

1. 在"资源管理器"视图中，选择要向其添加项目的应用程序（如果您尚未添加应用程序，请参阅第 30 页的『配置应用程序』）。
2. 完成以下某个操作以打开"新建项目向导"：
   a. 从主工作台菜单中依次选择**文件** > **添加项目** > **新项目**。
   b. 右键单击选定的应用程序，然后从上下文菜单选择**添加项目** > **新项目**。
3. 在向导的"选择项目类型"页面中，选择 **PHP** 作为项目类型，然后单击**下一步**以前进到下一向导页面。
4. 在"项目源"向导页面中：
   a. 确定项目源。项目源包括在其中找到项目文件以及要包含在项目中的其他任何个别文件的目录。

      对项目命名并指定工作目录。**工作目录**是 AppScan Source 项目文件 (`.ppf`) 所在的位置。它也是所有相对路径的基础。
   b. 单击**添加源根目录**以指定源代码根目录以及要在扫描中包含或排除的目录或文件。 添加源根目录之后，可以从该源根目录中排除特定目录或文件。要执行此操作，请选择源根目录中的目录或文件（或者对这些项进行多选），右键单击所选内容，然后从菜单中选择**排除**。如果包含或排除文件，文件名左侧的图标将更改。
5. **PHP 项目配置**：在 **PHP 文档根目录**字段中，输入或浏览至表示 PHP 应用程序根目录的目录。这是映射到站点基本 URL 的文件系统目录。如果未指定 PHP 文档根目录，那么将使用在"项目源"页面中指定的源根目录。
6. 可选： 设置 **Include 路径**。 Include 路径目录用于解析在 PHP `include` 语句（例如，`include`、`include_once`、`require`、`require_once`）中所使用文件的相对路径。
7. 可选： 设置**类 Include 路径**。类 include 路径目录用于查找包含 PHP 类定义的文件。
8. 单击**完成**。
9. 可选： **配置未解析的依赖关系**：在项目属性中，转至"项目依赖关系"页面并遵循第 60 页的『配置未解析的 PHP `include` 表达式』和第 63 页的『配置未解析的 PHP 类引用』的步骤。

示例：创建新 PHP 项目

关于此任务

此示例显示如何使用"新建应用程序向导"来创建 PHP 项目。

过程

1. 完成以下其中一个操作：
   - 从主菜单栏中选择**文件** > **添加应用程序** > **创建新应用程序**。
   - 在"资源管理器"视图工具栏中，单击**添加应用程序菜单**向下箭头按钮，然后从菜单中选择**创建新应用程序**。
   - 在"资源管理器"视图中，右键单击**所有应用程序**，然后从菜单中选择**添加应用程序** > **创建新应用程序**。
2. 为应用程序输入**名称**。

3. 浏览至将保存应用程序的**工作目录**。新的应用程序文件扩展名将为 .paf。
4. 单击**下一步**以配置项目。
5. 在向导的"选择项目类型"页面中，选择 **PHP** 作为项目类型，然后单击**下一步**以前进到下一向导页面。
6. 在"项目源"页面中：
   a. 在**名称**字段中，为项目输入名称 - 例如 MyProject。
   b. 在**工作目录**字段中，浏览至用于存储将创建的项目文件的位置 - 例如，C:\Apps\MyProject。
   c. 单击**添加源根目录**以添加含有应扫描的 PHP 文件的所有目录。例如，在"选择文件或目录"对话框中，浏览至 C:\Apps\MyProject\root，然后单击**确定**以关闭对话框。

   单击**下一步**。
7. 在"PHP 项目配置"页面中：
   a. 在 **PHP 文档根目录**字段中，输入或浏览以查找表示 PHP 应用程序根目录的目录。这是映射到站点基本 URL 的文件系统目录。缺省情况下，此字段将预填充在"项目源"页面中指定的源根目录。
   b. 可选： 添加 Include 路径目录。这些目录用于解析在 PHP Include 语句（例如，include、include_once、require、require_once）中所使用文件的相对路径。
   c. 可选： 添加类路径目录。这些目录用于查找含有 PHP 类定义的文件。
8. 单击**完成**。现在，您便拥有一个已准备好进行扫描的 PHP 项目。

配置未解析的 PHP include 表达式

开始之前

在项目属性中，转至"项目依赖性"页面。

过程

1. 单击**配置未解析的 Include 表达式**以打开"配置未解析的 Include 表达式"对话框。
2. 该对话框的上半部分列出了未解析的 include 表达式（所有未解析或需要额外处理才能解析的 include 表达式）。提供的有关表达式的信息包括：

选项	描述
包含的文本/更新的文本	此列显示源代码中存在的表达式文本。单击 **+** 可展开此列，以显示上次扫描期间使用的更新文本。如果上次扫描期间没有可用的已更新文本，那么将显示 <empty>。展开时可能显示多行已更新文本，源代码中每个使用此表达式的位置都对应一行。
状态	此列包含 X（用于未解析的表达式）或勾选标记（用于已成功解析的表达式）。

选项	描述
解析方式	此列指示已更新文本的生成方式。值包括： • AutoResolver：应用程序使用内部探索来查找文件。 • SearchReplace：已向包含的文本应用了一个或多个搜索和替换规则，以生成已更新文本。 • SearchReplace+AutoResolver：已向包含的文本应用了一个或多个搜索和替换规则以生成已更新文本，然后应用了内部探索方法来查找文件。 • SearchReplace+IncludePath：已向包含的文本应用了一个或多个搜索和替换规则以生成已更新文本，然后与 include 路径上的目录进行了合并以查找文件。 • SearchReplace+RelativeDir：已向包含的文本应用了一个或多个搜索和替换规则以生成已更新文本，然后被发现与包含 include 表达式的文件的源目录相关。
源文件、行、列	这些列显示源代码中使用表达式的位置。您可能希望在编辑器中查看这些位置，以查看应该如何对其进行解析。

注：某些列可能是空白的。因为展开的包含文本中可能具有多行已更新文本。这些列将包含针对上述每一行的相应文本。

3. 在对话框的下半部分，"Include 路径"选项卡包含在"PHP 项目依赖性"页面中输入的 include 路径信息。可以在此对话框中更新此信息（在查看未解析的 include 表达式时）。
4. 在此对话框的下半部分，"搜索和替换"选项卡用于添加将 include 表达式中的动态文本替换为静态文本（include 文件的完整或部分文件路径）的规则。"搜索和替换"表中有三列：

选项	描述
命令	此列中的值确定**搜索文本**和**替换文本**列的使用方式。选项有： • **替换文本**：此命令用于简单文本搜索和替换。**搜索文本**将按原样使用，如果在包含的文本中的任何位置找到该文本，那么会将其替换为**替换文本**。 • **替换函数**：此命令在替换函数调用时使用。**搜索文本**应该是不带有括号的函数名称。将增强搜索文本，以查找具有指定名称（后跟括号）的函数调用，且搜索文本将匹配括号内的所有内容。 • **替换正则表达式**：这是高级功能，允许为搜索文本指定正则表达式。

选项	描述
搜索文本	这是要在 include 表达式中搜索的文本。可在 include 表达式中选择文本并将其复制到剪贴板，然后粘贴到此处。有关指定搜索文本的不同变化，请参阅以上**命令**列的描述。
替换文本	这是用于替换搜索文本的文本。此静态文本是 include 文件的完整或部分路径。此外，还存在一些可以放在替换文本中的变量。可以将它们直接输入到**替换文本**单元格或从表上方的**替换文本变量**菜单中进行选择（这会将选定变量复制到剪贴板）。可从**替换文本变量**菜单列表中选择的变量有： • %ROOT_DIR%：此变量将替换为针对项目指定的 PHP 文档根目录。 • %SRC_DIR%：此变量将替换为包含 include 表达式的文件目录。 • %ARG_N%：此变量仅在命令为**替换函数**时适用。变量中的 N 应替换为整数（例如 %ARG_1% 或 %ARG_2%）。此变量继而将替换为传递到函数调用的第 N 个参数的文本。

将按顺序应用规则。每次成功进行搜索和替换操作后，都将检查新文本以查看是否可找到文件。如果找不到文件，那么将针对已更新的文本尝试下一条规则。

每个 PHP 项目都以三个搜索和替换规则开头，这些规则尝试替换 include 表达式中常用的某些标准 PHP 常量和函数。

示例：配置未解析的 *include* 表达式：
开始之前

未解析的 include 表达式在项目属性的"项目依赖性"选项卡式页面中进行配置。在该页面中时，单击**配置未解析的 Include 表达式**以打开"配置未解析的 Include 表达式"对话框。

此示例假定您已将 include 路径添加到项目（此操作可在创建项目时或在"项目依赖性"页面中完成）且已运行扫描。扫描完成后，打开"配置未解析的 Include 表达式"对话框以查看**未解析的 Include 表达式**列表。在此示例中，MYPROJECT_ROOT_PATH.'/a/b/filename.php'、MYPROJECT_ROOT_PATH.'/language/'.$configInfo['language'].'/mypage.php' 和 configGet('database_inc','./includes/database.inc') 是该列表中的表达式。

过程

1. 通过执行以下步骤将前导 PHP 常量或变量替换为目录：
   a. 选择 MYPROJECT_ROOT_PATH.'/a/b/filename.php' - 这将选定表达式中的文本。然后，可使用鼠标或光标键来选择表达式的一部分。选择 MYPROJECT_ROOT_PATH，然后右键单击并选择**复制**。
   b. 选择"搜索和替换"选项卡。

c. 单击**为选定的未解析项添加规则**按钮（用绿色**加号**表示）。此操作将向列表中添加新的搜索和替换规则。

d. 在新规则中，选择 NewSearchText，然后右键单击并从菜单中选择**粘贴**。这会将 NewSearchText 替换为 MYPROJECT_ROOT_PATH。

e. 从**替换文本变量**菜单中选择 %ROOT_DIR%。这会将 %ROOT_DIR% 文本字符串复制到剪贴板。

f. 在此规则中选择 NewReplacementText，然后右键单击并从菜单中选择**粘贴**。这会将 NewReplacementText 替换为 %ROOT_DIR%。

您现在便拥有一个新的规则，该规则会将常量替换为 PHP 文档根目录的路径。PHP 并置运算符 (.) 及其后面跟随的文本字符串将与替换文本合并以生成单个路径表达式。下次扫描项目时，使用此常量的 include 表达式应该可成功完成。

2. 要将动态表达式替换为单个值，请执行以下操作：

a. 选择 MYPROJECT_ROOT_PATH.'/language/'.$configInfo['language'].'/mypage.php' - 这将选定表达式中的文本。然后，可使用鼠标或光标键来选择表达式的一部分。选择 $configInfo['language']，然后右键单击并选择**复制**。

b. 选择"搜索和替换"选项卡。

c. 单击**为选定的未解析项添加规则**按钮（用绿色**加号**表示）。此操作将向列表中添加新的搜索和替换规则。

d. 在新规则中，选择 NewSearchText，然后右键单击并从菜单中选择**粘贴**。这会将 NewSearchText 替换为 $configInfo['language']。

e. 在规则中选择 NewReplacementText，输入 english 将其替换为新文本。

您现在便拥有一个新的规则，该规则会将表达式替换为指定值。 PHP 并置运算符 (.) 将应用，以生成单个路径表达式。下次扫描项目时，使用此表达式的 include 表达式应该可成功完成。

3. 要将 PHP 函数调用替换为其参数之一，请执行以下操作：

a. 选择 configGet('database_inc','./includes/database.inc') - 这将选定表达式中的文本。然后，可使用鼠标或光标键来选择表达式的一部分。选择 configGet，然后右键单击并选择**复制**。

b. 选择"搜索和替换"选项卡。

c. 在新规则中，从第一列中选择 Replace Text，然后从菜单中选择 Replace Function。

d. 在规则中选择 NewSearchText，然后右键单击并从菜单中选择**粘贴**。这会将 NewSearchText 替换为 configGet。

e. 从**替换文本变量**菜单中，选择 %ARG_1%。这会将变量复制到剪贴板中。

f. 在此规则中选择 NewReplacementText，然后右键单击并从菜单中选择**粘贴**。将粘贴的文本编辑为 %ARG_2%（取代 %ARG_1%）。

您现在便拥有一个新的规则，该规则会将函数调用替换为其第二个参数的值。下次扫描项目时，使用此函数调用的 include 表达式应该可成功完成。

配置未解析的 PHP 类引用

开始之前

在项目属性中，转至"项目依赖性"页面。

过程

1. 单击**配置未解析的类引用**以打开"配置未解析的类引用"对话框。
2. 对话框的上部会列出未解析的类引用（上次扫描期间未解析的所有类引用）。提供的关于类引用的信息包括：

选项	描述
类名/生成的文件名	此列显示在源代码中引用的类名。通过单击 **+** 可以展开此列，然后，它将显示在上次扫描期间使用的所生成文件名（用来尝试查找类）。将其展开时可能有多个文件名 - 在源代码中使用此类的每个位置都有一个文件名。
状态	此列将包含 X（用于未解析的类）或勾选标记（用于已成功解析的类）。
解析方式	此列指示创建生成的文件名的方式。值包括： • AutoResolver：应用程序使用内部探索来查找文件。 • SearchReplace：已将一个或多个搜索和替换规则应用于类名以创建生成的文件名。
源文件、行、列	这些列显示在源代码中使用此类的位置。您可能希望在编辑器中查看这些位置，以查看应该如何对其进行解析。

注：某些列可能是空白的。这是因为在展开时，类名可以拥有多个生成的文件名行。这些列将拥有针对这些生成的每个文件名行的相应文本。

3. 在对话框的下半部分，"类 Include 路径"选项卡包含在"PHP 项目依赖关系"页面中输入的类 include 路径信息。（查看未解析的类引用时）可以在此对话框中更新此信息。
4. 在此对话框的下半部分，"搜索和替换"选项卡用于添加规则以将未解析的类名修改为包含该类的定义的完整或部分文件路径。"搜索和替换"表中有三列：

选项	描述
命令	此列中的值确定**搜索文本**和**替换文本**列的使用方式。选项有： • **匹配文本**：此命令用于文本搜索和替换。* 字符允许在搜索文本中使用，且匹配 0 或多个字符。匹配文本的结果将不会影响任何其他搜索和替换规则。这通常用来尝试将扩展名添加到类名，或在生成文件名时从类名中过滤出前缀和后缀。 • **替换文本**：此命令用于简单文本搜索和替换。**搜索文本**将按原样使用，如果在类名中的任何位置找到它，那么会使用**替换文本**对其进行替换。这用来修改在以下规则中使用的类名。 • **替换正则表达式**：这是高级功能，允许为搜索文本指定正则表达式。

选项	描述
搜索文本	这是要在类引用中搜索的文本。可以在类名中选择文本并将其复制到剪贴板，然后粘贴到此处。有关指定搜索文本的不同变化，请参阅以上**命令**列的描述。
替换文本	这是用于替换搜索文本的文本。此静态文本是包含类定义的文件的完整或部分路径。此外，还存在一些可以放在替换文本中的变量。可以将它们直接输入到**替换文本**单元格或从表上方的**替换文本变量**菜单中进行选择（这会将选定变量复制到剪贴板）。可从**替换文本变量**菜单列表中选择的变量有： • %ROOT_DIR%：此变量将替换为针对项目指定的 PHP 文档根目录。 • %SRC_DIR%：此变量将由含有类引用的文件目录替换。 • %MATCH_N%：仅当命令为**匹配文本**时此变量才适用。变量中的 N 应使用整数来替换（例如，%MATCH_1% 或 %MATCH_2%）。然后，此变量将替换为与搜索文本中第 N 个 * 匹配的文本。

将按顺序应用规则。每次成功进行搜索和替换操作后，都将检查新文本以查看是否可找到文件。如果找不到文件，那么将针对已更新的文本尝试下一条规则（命令为**匹配文本**则除外）。

每个 PHP 项目都以两个简单的"搜索/替换"规则开始，这两个规则会尝试将一些常见文件扩展名添加到类名。

5. 在对话框的下半部分，"已找到的类"选项卡会列出在上次扫描期间找到的所有类。这可用来更新类 include 路径以及搜索和替换规则。可以在对话框的"未解析的类引用"部分中选择未解析的类引用，然后单击**查找声明**。如果找到了声明，那么它将在"已找到的类"选项卡列表中显示。

示例：配置未解析的类引用：
开始之前

未解析的类引用在项目属性的"项目依赖关系"选项卡式页面中进行配置。一旦进入此页面，请单击**配置未解析的类引用**以打开"配置未解析的类引用"对话框。

此示例假设您已将类 include 路径添加到项目（此操作可以在创建项目时或在"项目依赖关系"页面中执行）且您已运行了扫描。扫描完成后，请打开"配置未解析的类引用"对话框，以查看**未解析的类引用**列表。

在这些示例中，由您提供替换文本值。注意，这些示例在文本中可以拥有多个变量 - 例如，%ROOT_DIR%/modules/%MATCH_1%/classes/%MATCH_1%.class.inc。

过程

1. 要添加 include 文件所使用的其他文件扩展名，请执行以下操作：
   a. 选择"搜索和替换"选项卡。

b. 单击**为选定的未解析项添加规则**按钮（用绿色**加号**表示）。这会将新的搜索和替换规则添加到列表。

c. 在新规则中，选择**替换文本**：%MATCH_1%.php。在此字符串中，删除 .php，然后在其所在位置输入 .class.inc。**替换文本**现在应为 %MATCH_1%.class.inc。

现在，您拥有了新规则，在解析类时，该规则会尝试将后缀 .class.inc 添加到类名。

2. 要从类名除去前缀，请执行以下操作：

a. 选择"搜索和替换"选项卡。

b. 单击**为选定的未解析项添加规则**按钮（用绿色**加号**表示）。这会将新的搜索和替换规则添加到列表。

c. 在新规则中，选择**搜索文本**列中的字符串 (*)，然后在它的位置输入 Abc*。

d. 请勿改变 %MATCH_1%.php 替换文本。

现在，您拥有了新规则，该规则会将类名（如 AbcHello）映射到 Hello.php。

3. 要从类名除去后缀，请执行以下操作：

a. 选择"搜索和替换"选项卡。

b. 单击**为选定的未解析项添加规则**按钮（用绿色**加号**表示）。这会将新的搜索和替换规则添加到列表。

c. 在新规则中，选择**搜索文本**列中的字符串 (*)，然后在它的位置输入 *Xyz。

d. 请勿改变 %MATCH_1%.php 替换文本。

现在，您拥有了新规则，该规则会将类名（如 ByeByeXyz）映射到 ByeBye.php。

4. 您可能想要映射诸如 Abc_Def_Ghi_class 的类名，以便将其前缀用作文件系统的相对路径（例如 Abc/Def/Ghi/class.php）。要修改类名文本以在其他规则中使用，请执行以下操作：

a. 选择"搜索和替换"选项卡。

b. 单击**为选定的未解析项添加规则**按钮（用绿色**加号**表示）。这会将新的搜索和替换规则添加到列表。

c. 在新规则中，选择第一列中的**匹配文本**，然后从菜单中选择**替换文本**。

d. 在新规则中，选择**搜索文本**列中的字符串 (*)，然后在它的位置输入 _。

e. 选择**替换文本**列中的字符串，然后在它的位置输入 /。

f. 选择了规则后，请单击**上移**以将此规则移动到列表顶部。

现在，您拥有了新规则，该规则会将下划线 (_) 替换为斜杠 (/)，并且所有后续规则都将使用已更新的文本。此规则会将 Abc_Def_Ghi_class 更改为 Abc/Def/Ghi/class，然后，剩下的**匹配文本**规则将尝试添加扩展名（如 .php 和 .inc）。

添加新 PL/SQL 项目

"新建项目向导"帮助您手动创建 PL/SQL 项目并将其添加到应用程序。

关于此任务

本主题中的步骤将指导您完成"新建项目向导"（如果要在其中创建应用程序，那么为"新建应用程序向导"）中的所有页面。在选定项目的"属性"视图中创建项目后，可以修改向导中进行的设置。

过程

1. 在"资源管理器"视图中，选择要向其添加项目的应用程序（如果您尚未添加应用程序，请参阅第 30 页的『配置应用程序』）。
2. 完成以下某个操作以打开"新建项目向导"：
   a. 从主工作台菜单中依次选择**文件** > **添加项目** > **新项目**。
   b. 右键单击选定的应用程序，然后从上下文菜单选择**添加项目** > **新项目**。
3. 在向导的"选择项目类型"页面中，选择 **PL/SQL** 作为项目类型，然后单击**下一步**以前进到下一向导页面。
4. 在"项目源"向导页面中：
   a. 确定项目源。项目源包括在其中找到项目文件以及要包含在项目中的其他任何个别文件的目录。

      对项目命名并指定工作目录。**工作目录**是 AppScan Source 项目文件 (.ppf) 所在的位置。它也是所有相对路径的基础。
   b. 单击**添加源根目录**以指定源代码根目录以及要在扫描中包含或排除的目录或文件。 添加源根目录之后，可以从该源根目录中排除特定目录或文件。要执行此操作，请选择源根目录中的目录或文件（或者对这些项进行多选），右键单击所选内容，然后从菜单中选择**排除**。如果包含或排除文件，文件名左侧的图标将更改。
5. 单击**完成**。

添加新 T-SQL 项目

"新建项目向导"帮助您手动创建 T-SQL 项目并将其添加到应用程序。

关于此任务

本主题中的步骤将指导您完成"新建项目向导"（如果要在其中创建应用程序，那么为"新建应用程序向导"）中的所有页面。在选定项目的"属性"视图中创建项目后，可以修改向导中进行的设置。

过程

1. 在"资源管理器"视图中，选择要向其添加项目的应用程序（如果您尚未添加应用程序，请参阅第 30 页的『配置应用程序』）。
2. 完成以下某个操作以打开"新建项目向导"：
   a. 从主工作台菜单中依次选择**文件** > **添加项目** > **新项目**。
   b. 右键单击选定的应用程序，然后从上下文菜单选择**添加项目** > **新项目**。
3. 在向导的"选择项目类型"页面中，选择 **T-SQL** 作为项目类型，然后单击**下一步**以前进到下一向导页面。
4. 在"项目源"向导页面中：
   a. 确定项目源。项目源包括在其中找到项目文件以及要包含在项目中的其他任何个别文件的目录。

      对项目命名并指定工作目录。**工作目录**是 AppScan Source 项目文件 (.ppf) 所在的位置。它也是所有相对路径的基础。

b. 单击**添加源根目录**以指定源代码根目录以及要在扫描中包含或排除的目录或文件。 添加源根目录之后，可以从该源根目录中排除特定目录或文件。要执行此操作，请选择源根目录中的目录或文件（或者对这些项进行多选），右键单击所选内容，然后从菜单中选择**排除**。如果包含或排除文件，文件名左侧的图标将更改。

5. 单击**完成**。

添加新 Visual Basic 项目

关于此任务

注：该项目类型仅在 Windows 上受支持。

本主题中的步骤将指导您完成"新建项目向导"（如果要在其中创建应用程序，那么为"新建应用程序向导"）中的所有页面。在选定项目的"属性"视图中创建项目后，可以修改向导中进行的设置。

注：对于 PHP、VB6 和 Classic ASP，仅 ISO-8859-1 (Western Europe)、UTF-8 和 UTF-16 字符集受支持。

过程

1. 在"资源管理器"视图中，选择要向其添加项目的应用程序（如果您尚未添加应用程序，请参阅第 30 页的『配置应用程序』）。
2. 完成以下某个操作以打开"新建项目向导"：
   a. 从主工作台菜单中依次选择**文件** > **添加项目** > **新项目**。
   b. 右键单击选定的应用程序，然后从上下文菜单选择**添加项目** > **新项目**。
3. 在向导的"选择项目类型"页面中，选择 **Visual Basic** 作为项目类型，然后单击**下一步**以前进到下一向导页面。
4. 在"项目源"向导页面中：
   a. 确定项目源。项目源包括在其中找到项目文件以及要包含在项目中的其他任何个别文件的目录。

      对项目命名并指定工作目录。**工作目录**是 AppScan Source 项目文件 (.ppf) 所在的位置。它也是所有相对路径的基础。
   b. 单击**添加源根目录**以指定源代码根目录以及要在扫描中包含或排除的目录或文件。 添加源根目录之后，可以从该源根目录中排除特定目录或文件。要执行此操作，请选择源根目录中的目录或文件（或者对这些项进行多选），右键单击所选内容，然后从菜单中选择**排除**。如果包含或排除文件，文件名左侧的图标将更改。
5. 单击**完成**。

复制项目

通过 AppScan Source for Analysis，可以复制除 .NET 项目外的所有类型的项目。对项目的修改不会影响重复的项目；复制项目后，原始项目和复制的项目之间没有任何联系。复制已导入的项目时，将使用所有配置信息创建 AppScan Source 项目文件 (.ppf)。

过程

1. 在"资源管理器"视图中，右键单击要复制的项目，然后在菜单中选择**复制项目**。
2. 在"复制项目"对话框中：
   a. 对新项目命名。
   b. 确定已复制的项目的目标应用程序（目标应用程序必须是手动创建的 AppScan Source 应用程序或使用 Application Discovery Assistant 创建的应用程序）。
   c. 确定目标目录（新项目的工作目录）。

修改应用程序和项目属性

在"资源管理器"视图中选择应用程序或项目时，当前属性在"属性"视图中显示，您可在该视图中进行修改。

关于此任务

第 213 页的『属性视图：选定应用程序』和第 214 页的『属性视图：选定项目』提供了有关在选择应用程序或项目时可在"属性"视图中修改的设置的详细信息。

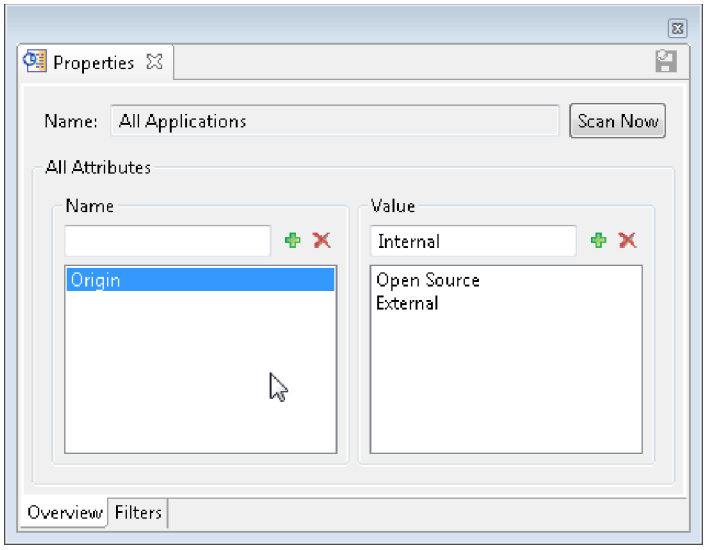
过程

1. 使用以下某种方法打开应用程序或项目的"属性"视图：
   a. 在"资源管理器"视图中选择应用程序或项目，然后打开"属性"视图以显示其属性。
   b. 在"资源管理器"视图中右键单击应用程序或项目，并选择**属性**。
2. 在"属性"视图中复审属性。
3. 在相应选项卡页面上进行更改。可用属性页面根据语言有所不同。
4. 单击**保存**。

全局属性

必须首先定义全局属性，然后才能将其与个别应用程序关联。全局属性是通过在"资源管理器"视图中选择**所有应用程序**以在"属性"视图中定义的。

关于此任务



要删除属性或其值，请选择其名称或值，并单击**删除属性** ( )。删除属性不会影响历史结果。

要创建属性并使其可用于任何应用程序：

过程

1. 在"资源管理器"视图中选择**所有应用程序**。
2. 打开"属性"视图中的**概述**选项卡。
3. 输入属性的名称并单击**添加属性** ( )，或单击**添加属性**而不首先指定名称（随后对话框将提示您输入属性的名称）。
4. 输入属性的**值**并单击**添加属性值**，或单击**添加属性值**而不首先指定值（随后对话框将提示您添加值）。
5. 重复这些步骤以添加多个属性值。

应用程序属性

应用程序属性应用于当前选定的应用程序，并依赖于先前创建的全局属性。

过程

1. 在"资源管理器"视图中选择应用程序。
2. 打开"属性"视图中的**概述**选项卡。
3. 单击**添加属性**。此时将出现**全局属性**对话框，其中包含先前创建的属性的列表（创建全局属性的指示信息可在第 69 页的『全局属性』中找到）。
4. 双击要添加的属性，或选择该属性并单击**确定**。该属性将添加到"属性"视图的"应用程序属性"部分。
5. 单击**值**列并从列表选择此应用程序的值（如果使用多个值创建了全局属性，那么有多个值可用）。您可以将多个属性关联到应用程序。

移除应用程序和项目

如果应用程序和项目尚未注册，那么您可以从 AppScan Source for Analysis 中将其移除。

过程

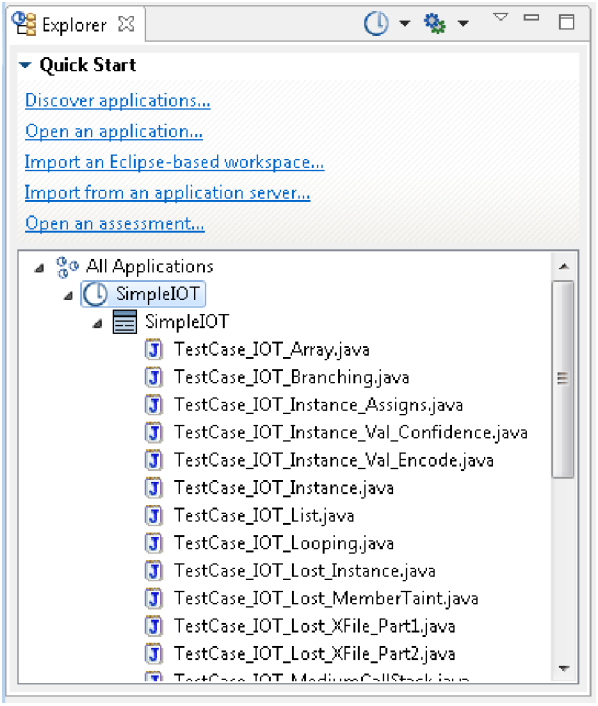
1. 选择要移除的应用程序或项目。可以选择多个应用程序和多个项目来进行移除，但不能混合选择应用程序和项目来进行移除。
2. 完成以下其中一个操作：
   - 右键单击所选项，然后从菜单中选择**移除应用程序**或**移除项目**。
   - 按键盘 Delete 键。
   - 从主工作台菜单选择**编辑** > **移除**。

"资源管理器"视图

"资源管理器"视图在顶部包含**快速启动**部分，在底部包含资源管理器部分，该部分包含一个节点：**所有应用程序**。**快速启动**部分包含若干个启动常用操作的有用链接。资源管理器部分包含一个树形窗格，该窗格提供了资源（应用程序、项目、目录和项目文件）的分层视图，并以**所有应用程序**作为其根。浏览这些资源的方式与在文件浏览器中类似。在视图中浏览时，树的选择状态确定了"属性"视图中可用的选项卡。

- 第 72 页的『常规信息』
- 第 72 页的『"快速启动"部分』
- 第 73 页的『工具栏按钮』
- 第 73 页的『右键单击菜单选项』
- 第 75 页的『应用程序和项目指示符』

常规信息



在"资源管理器"视图中，可使用工具栏按钮、**快速启动**部分中的链接或者资源管理器部分中的右键单击菜单命令来添加应用程序和项目并扫描代码。一旦添加了应用程序，资源管理器部分便会提供应用程序和项目的可视指示符以及每个所添加项的状态。

提示：在"资源管理器"视图中，悬浮式帮助可用于指示应用程序、项目和文件的文件名和路径。悬浮式帮助还指示应用程序或项目是否已注册。

"快速启动"部分

快速启动部分提供以下用于启动常用任务的链接：

- **发现应用程序**：这会启动 Application Discovery Assistant，它使您能够为 Java 和 Microsoft Visual Studio 源代码快速创建并配置应用程序和项目。
- **打开应用程序**：这会启动"打开"对话框，您可以通过此对话框来浏览到现有应用程序并将其添加到应用程序集。可以添加的文件或目录类型包括 `.paf`、`.sln`、`.dsw` 和 `.ewf`。
- **导入基于 Eclipse 的工作空间**：这会启动"添加工作空间"对话框，您可以通过此对话框来添加包含了 Java 项目的现有 Eclipse 或 IBM Rational Application Developer for WebSphere Software (RAD) 工作空间。导入了此工作空间后，您将能够扫描其包含的任何 Java 项目。

  注：导入工作空间之前，请确定您已按照第 39 页的『配置 Eclipse 和 Rational Application Developer for WebSphere Software (RAD) 项目的开发环境』中所述安装并更新了开发环境。
- **从应用程序服务器导入**：从 Apache Tomcat 或 WebSphere Application Server Liberty 应用程序服务器导入现有 Java 应用程序。

- **打开评估**：这会启动"打开"对话框，您可以通过此对话框来浏览到 AppScan Source 评估文件。可打开的文件的类型包括 `.ozasmt` 和 `.xml`。

工具栏按钮

表 *8.* 工具栏按钮

操作	图标	描述
添加应用程序菜单		通过单击**添加应用程序菜单**按钮上的向下箭头，可以选择用于创建新应用程序，打开现有应用程序，导入工作空间或启动 Application Discovery Assistant 的操作。
扫描所选项		通过**扫描所选项**按钮，可以扫描在资源管理器部分中选择的对象。缺省扫描配置将用于扫描。要选择其他扫描配置来用于扫描，请单击**扫描所选项**按钮上的向下箭头。选择要使用的扫描配置，或选择**编辑配置**操作以将其他扫描配置设为缺省值（在"扫描配置"视图中，选择要设为缺省值的配置，然后单击**选为缺省值**）。
视图菜单		**视图菜单**按钮可打开用于刷新资源管理器部分和隐藏已注册项的菜单。

右键单击菜单选项

右键菜单选项的可用性由资源管理器部分中所选的项决定。

- 如果在资源管理器部分中选择了**所有应用程序**，那么以下右键单击菜单选项可用：
  - **扫描所有应用程序**：扫描所有应用程序。扫描将使用缺省扫描配置来运行。
  - **扫描所有应用程序时使用**：选择要使用的扫描配置，或选择**编辑配置**操作以将其他扫描配置设为缺省值（在"扫描配置"视图中，选择要设为缺省值的配置，然后单击**选为缺省值**）。
  - **添加应用程序**
    - **创建新应用程序**：将新应用程序添加到应用程序集。此操作会启动"新建应用程序"向导。
    - **打开现有应用程序**：这会启动"打开"对话框，您可以通过此对话框来浏览到现有应用程序并将其添加到应用程序集。可以添加的文件或目录类型包括 `.paf`、`.sln`、`.dsw` 和 `.ewf`。
    - **导入现有基于 Eclipse 的工作空间**：这会启动"添加工作空间"对话框，您可以通过此对话框来添加包含了 Java 项目的现有 Eclipse 或 IBM Rational Application Developer for WebSphere Software (RAD) 工作空间。导入了此工作空间后，您将能够扫描其包含的任何 Java 项目。

注：导入工作空间之前，请确定您已按照第 39 页的『配置 Eclipse 和 Rational Application Developer for WebSphere Software (RAD) 项目的开发环境』中所述安装并更新了开发环境。

- **发现应用程序**：这会启动 Application Discovery Assistant，它使您能够为 Java 和 Microsoft Visual Studio 源代码快速创建并配置应用程序和项目。

– **全部展开**

– **全部折叠**

– **属性**：选择此选项会打开所选项的"属性"视图。

• 如果在资源管理器部分中选择了一个应用程序，那么以下右键单击菜单选项可用：

– **扫描应用程序**：扫描所选应用程序、项目或文件。扫描将使用缺省扫描配置来运行。

– **扫描应用程序时使用**：选择要使用的扫描配置，或选择**编辑配置**操作以将其他扫描配置设为缺省值（在"扫描配置"视图中，选择要设为缺省值的配置，然后单击**选为缺省值**）。

– **添加项目**

- **新项目**：如果在"资源管理器"视图中选择了某个应用程序，那么此操作可用，而选择此操作将使您能够向此应用程序添加新项目。此操作会启动"新建项目"向导。

- **现有项目**：如果在"资源管理器"视图中选择了某个应用程序，那么此操作可用，而选择此操作将使您能够向此应用程序添加现有项目。此操作会启动一个对话框，您可以通过此对话框来浏览到要打开的 .ppf、.vcproj、.vcxproj、.csproj、.vbproj、.dsp 或 .epf 文件。

- **多个项目**：将多个项目添加到在"资源管理器"视图中选择的应用程序。此操作会启动一个对话框，您可以通过此对话框来完成以下任务之一：

  • 指定要在其中搜索项目的目录。

  • 指定要在其中搜索项目的工作空间。

  • 指定要在其中搜索项目的 Microsoft 解决方案文件。

  在搜索结果中，您可以选择一个或多个要添加的项目。

– **移除应用程序**：如果在"资源管理器"视图中选择了某个应用程序，那么此操作可用，而选择此操作会移除所选应用程序。

– **添加定制结果**：此操作会启动"创建定制结果"对话框，使您能够为所选应用程序创建定制结果。

– **刷新**：刷新所选应用程序、项目或视图的内容。

– 注册/注销：

- **注册应用程序**：向 AppScan Source 注册所选的应用程序或项目。您必须先注册应用程序和项目，然后才能将其发布到 AppScan Source 数据库。

- **将应用程序注册为...**：选择此选项可使用新名称来注册应用程序。

- **注销应用程序**：注销所选的应用程序或项目。

- **定位**：选择此选项可将本地应用程序或项目与已由其他 AppScan Source 用户注册的应用程序或项目相关联。

– **全部展开**

– **全部折叠**

- **属性**：选择此选项会打开所选项的"属性"视图。

- 如果在资源管理器部分中选择了一个项目，那么以下右键单击菜单选项可用：
  - **扫描项目**：扫描所选应用程序、项目或文件。扫描将使用缺省扫描配置来运行。
  - **扫描项目时使用**：选择要使用的扫描配置，或选择**编辑配置**操作以将其他扫描配置设为缺省值（在"扫描配置"视图中，选择要设为缺省值的配置，然后单击**选为缺省值**）。
  - **复制项目**：如果在"资源管理器"视图中选择了某个项目，那么此操作可用，而选择此操作将打开一个对话框，您可以通过此对话框将此项目复制到另一个应用程序，或在当前包含此项目的应用程序中创建此项目的副本。
  - **移除项目**：移除所选对象。
  - 注册/注销：
    - **注册项目**：向 AppScan Source 注册所选的应用程序或项目。您必须先注册应用程序和项目，然后才能将其发布到 AppScan Source 数据库。
    - **注销项目**：注销所选的应用程序或项目。
    - **定位**：选择此选项可将本地应用程序或项目与已由其他 AppScan Source 用户注册的应用程序或项目相关联。
  - **全部展开**
  - **全部折叠**
  - **属性**：选择此选项会打开所选项的"属性"视图。
- 如果在资源管理器部分中选择了一个文件，那么以下右键单击菜单选项可用：
  - **扫描文件**：扫描所选应用程序、项目或文件。扫描将使用缺省扫描配置来运行。
  - **扫描文件时使用**：选择要使用的扫描配置，或选择**编辑配置**操作以将其他扫描配置设为缺省值（在"扫描配置"视图中，选择要设为缺省值的配置，然后单击**选为缺省值**）。
  - **从扫描中排除**：从扫描中移除所选文件。
  - **在内部编辑器中打开**：在 AppScan Source 编辑器（在"分析"透视图中）中打开所选文件。
  - **在外部编辑器中打开**：选择要在其中打开所选文件的外部编辑器。
  - **属性**：选择此选项会打开所选项的"属性"视图。

应用程序和项目指示符

下表标识了"资源管理器"视图中的应用程序和项目图标。

表 *9.* 应用程序和项目图标

应用程序或项目类型	未注册	已注册	缺失/找不到
已导入的应用程序			
手动创建或使用 Application Discovery Assistant 创建的应用程序			
已导入的项目			

表 9. 应用程序和项目图标 (续)

应用程序或项目类型	未注册	已注册	缺失/找不到
手动创建或使用 Application Discovery Assistant 创建的项目			

"资源管理器"视图显示本地应用程序和项目，以及已在服务器上注册的应用程序和项目（已在服务器上注册但未在本地保存的应用程序和项目，例如，由其他用户注册的应用程序和项目，以灰色显示）。如果单击工具栏**视图菜单**按钮并将**隐藏服务器上已注册项**菜单项切换为未选择状态，那么可以查看现有服务器应用程序和项目。如果项目以灰色显示，那么可以右键单击并选择菜单中的**查找**。

第 3 章 首选项

首选项是关于 AppScan Source for Analysis 的外观和操作的个人选项。

要打开首选项页面，请从主工作台菜单中选择**编辑** > **首选项**。您可以通过浏览左窗格中的所有标题来浏览首选项，或使用左窗格顶部的过滤器字段来搜索一小部分标题。 过滤器返回的结果与首选项页面标题和关键字（如 JSP 或电子邮件）都匹配。

使用右窗格右上方的箭头控件，您可以浏览先前查看过的页面。查看若干页面后要返回某个页面，请单击向下箭头以显示最近查看过的首选项页面的列表。

常规首选项

通过常规首选项，可以定制部分 AppScan Source for Analysis 缺省设置以符合您的个人偏好。

选择语言

AppScan Source for Analysis 用户界面可使用不同的本地语言进行显示。要更改显示的本地语言，请从**选择语言**列表中进行选择，然后单击首选项对话框中的**确定**。必须手动重新启动工作台才能使更改生效。

注：要利用此功能，在安装过程中至少必须安装一个语言包。如果英语是安装的唯一语言，那么使用此首选项并重新启动工作台后，产品将以英语显示。在这种情况下，如果您要显示英语以外的语言，那么请再次运行安装向导并通过添加一个或多个语言包来选择修复安装。

文件编码

必须对项目中文件的字符编码进行相应设置，以便 AppScan Source 可以正确读取这些文件（并且例如，在源视图中正确显示这些文件）。在此部分选择缺省字符编码。

记录级别

更改日志记录级别以提供要在错误日志中包含的信息级别。从**跟踪**、**调试**、**参考**、**警告**、**错误**和**致命**中进行选择，其中**跟踪**提供繁杂程度最高的日志记录，**致命**仅记录关键事件，而其余设置则提供级别依次提高的日志记录。

在退出时保存所有过滤器

如果选择该选项，那么将禁用在退出 AppScan Source 时询问您是否自动保存所有新创建或编辑的过滤器的提示。

出错时取消扫描

如果选中，那么在出现错误时，将通过取消扫描来避免不完全的扫描。

© Copyright IBM Corp. 2003, 2017

为每个结果创建标记

选择时，如果具有打开的评估，编辑器中打开的扫描的源将包含存在结果的位置处的标记。

缺省情况下，启用了标记创建。

创建标记可能会减慢扫描速度。如果您的项目包含许多源文件（或者大型源文件），那么关闭标记创建可能会改善性能。

扫描完成后

缺省设置是接收提示，询问您在扫描结束时是否要评估自动打开。如果您不希望看到该提示，请选择**始终打开新评估**或**从不打开**。

扫描完成后，相同目标尚有未保存的扫描

缺省情况下，将提示您保存或放弃现有的未保存扫描。您可以修改此首选项，以便始终自动删除或者从不自动删除重复扫描。设置此首选项时，请注意，在删除重复扫描的情况下，内存使用率将减少。

使用绝对路径发布或导出评估时

缺省情况下，将在发布时提示您定义绝对路径变量。此部分中的设置允许您禁用此缺省提示，或自动打开对话框以允许您在绝对路径存在时定义变量。

在初始发布时自动注册应用程序

缺省情况下，在您发布未注册应用程序或项目的评估时，会提示您注册这些应用程序或项目。您可以选择在发布应用程序和项目时始终予以注册，也可选择从不注册。

要点：您必须拥有**注册**许可权才能注册应用程序和项目。

应用程序名称出现冲突时

AppScan Source for Analysis 中可以存在同名的应用程序，但是，无法对这些应用程序的使用进行管理。缺省情况下，如果尝试向某个应用程序提供与现有应用程序相同的名称（或导入与现有应用程序同名的应用程序），将向您提示警告。警告消息允许您为应用程序生成唯一的名称，保留冲突的名称，或取消。

如果要让 AppScan Source for Analysis 在冲突发生时自动生成唯一的应用程序名称，请在首选项页面中选择**生成唯一名称**。如果要自动接受冲突的应用程序名称，请选择**保留现有名称**。

注：应用程序将以文件名 `<application_name>.paf` 进行存储。如果选择**保留现有名称**，那么不能将工作目录设置为与同名现有应用程序相同的工作目录。在此情况下，将提示您覆盖现有文件名，但是覆盖将失败，因为现有应用程序已在 AppScan Source for Analysis 中打开。

项目名称出现冲突时

仅当您尝试创建或导入与同一应用程序中存在的项目同名的项目时，此设置才适用。在此情况下，项目名称不能冲突。如果尝试此操作，那么缺省情况下，将提示您生成

唯一的名称，或取消该操作。如果要让 AppScan Source for Analysis 在冲突发生时自动生成唯一的项目名称，请在首选项页面中选择**生成唯一名称**。

启动时在已发布的评估和我的评估中显示的评估数

设置要在"已发布的评估"视图或"我的评估"视图中查看的评估的最大数量。

"欢迎"视图中显示的 RSS 订阅源

缺省情况下，"欢迎"视图显示 X-Force® RSS 订阅源内容。要显示其他内容，在**"欢迎"视图中显示的 RSS 订阅源**字段中输入需要的 URL。

针对高网络延迟进行优化

选中此复选框可在客户机上高速缓存更多信息以最大限度减少服务器调用。

重新装入系统配置

装入最新的系统设置。如果您在产品运行时在产品外部更改了设置（例如，通过修改 `<data_dir>\config` （其中 `<data_dir>` 是 AppScan Source 程序数据的位置，如第 275 页的『安装和用户数据文件位置』中所述） 中的 `.ozsettings` 文件），那么选择此按钮可刷新产品中的设置。

AppScan Enterprise Console 首选项

如果 AppScan Enterprise Server 已与 AppScan Enterprise Console 选件一起安装，那么您可以向其发布评估。Enterprise Console 提供各种用于处理评估的工具，例如报告功能、问题管理、趋势分析和仪表板。

要启用此功能部件，请填写 AppScan Enterprise Console 首选项页面。在启用 Enterprise Console 发布功能之前，必须使用有效输入内容来填写此页面中的所有字段：

- **用户标识**字段：输入 AppScan Enterprise Server 用户标识（已创建用于代表您的 AppScan Source 用户进行发布的用户标识）。
  - 如果 AppScan Enterprise Server 配置为使用 Windows 认证，请输入用于连接到 Enterprise Console 的域和用户名（以 \ 分隔域和用户名，例如 `my_domain\my_username`）。
  - 如果 AppScan Enterprise Server 已配置 LDAP，请输入用于连接到 Enterprise Console 的用户名。
  - 在 Windows 上，如果支持 AppScan Enterprise Server 进行通用访问卡 (CAC) 认证，从列表选择 CAC 通用名。

  至少您必须是 QuickScan 用户。如果您连接到版本低于 V9.0.3 的 AppScan Enterprise Server，必须在 Enterprise Server 有您自己的用户文件夹。
- **密码**字段：仅当 AppScan Enterprise Server 认证方法为用户标识和密码时，该字段才可用。输入用于登录到Enterprise Console的密码（已输入的用户名的密码）。
- **Enterprise Console URL** 字段：输入用于访问 Enterprise Console Web 应用程序的 URL。

  此 URL 的格式为：

  `http(s)://<hostname>:<port>/ase`

其中 <hostname> 是安装 Enterprise Console的机器的名称，<port> 是运行此控制台的端口（缺省值 <port> 为 9443）。该 URL 的示例为 https://myhost.mydomain.ibm.com:9443/ase。

注：

- 如果已设置 **Enterprise Console URL**，那么无需修改此字段。
- 您必须通过**管理 AppScan Enterprise 设置**许可权登录到 AppScan Source 才能设置 **Enterprise Console URL** 字段。关于用户帐户和许可权的信息，请参阅产品信息中心的管理部分，或《*IBM Security AppScan Source* 安装和管理指南》的"管理 *AppScan Source*"一节。
- **用户标识**和**密码**存储在运行 AppScan Source 客户机（例如 AppScan Source for Analysis）的机器上，而 **Enterprise Console URL** 则存储在 Enterprise Server（可能位于远程机器上）中。您无法从远程机器访问用户名和密码信息（例如，通过从远程机器发出 getaseinfo 命令）。
- AppScan Source 不支持向已配置为使用代理设置的 AppScan Enterprise Console实例进行发布。尝试向使用代理设置的实例进行发布将导致错误。

完成设置后，强烈建议您通过单击**测试连接**来确保与 Enterprise Console 服务器的连接有效。

提示：如果连接测试失败，请检查 Enterprise Console 服务器是否在运行，以及您是否能够在浏览器中访问其控制中心 URL（使用以上已指定的同一 **Enterprise Console URL**）。

用于 JavaServer Page 编译的应用程序服务器首选项

如果您扫描的是包含 JavaServer Pages (JSP) 的应用程序，那么 AppScan Source 分析引擎必须能够编译 JSP 代码才可以对该应用程序进行分析。创建 JSP 项目时，必须指定 AppScan Source 应该使用的 JSP 编译器（或者接受缺省编译器，这可在 Java 和 JSP 首选项页面中进行设置）。如果 AppScan Source 无法编译 JSP 文件，请使用应用程序服务器首选项页面来配置应用程序所使用的 JSP 编译器。

Apache Tomcat V7 和 V8 包含在 AppScan Source 的安装中。如果未配置 **Tomcat 7** 和 **Tomcat 8** 首选项页面，那么 AppScan Source 将使用当前提供且标记为缺省选项的 Tomcat JSP 编译器来编译 JSP 文件。如果您想要运用外部受支持 Tomcat 编译器，请使用 Tomcat 首选项页面来指向本地 Tomcat 安装版。

如果使用的是 Oracle WebLogic Server 或 WebSphere Application Server，那么必须将适用的首选项页面配置为指向应用程序服务器的本地安装版，以便其可在分析期间用于 JSP 编译（如果您创建 JSP 项目而不首先配置应用程序服务器，那么系统将提示您此时配置应用程序服务器）。

Tomcat

本主题描述了需要设置哪些首选项，才能将 AppScan Source 配置为引用 AppScan Source 所随附 Apache Tomcat 应用程序服务器以外的 Apache Tomcat 应用程序服务器。

Apache Tomcat V7 和 V8 包含在 AppScan Source 的安装中。如果未配置 **Tomcat 7** 和 **Tomcat 8** 首选项页面，那么 AppScan Source 将使用当前提供且标记为缺省选

项的 Tomcat JSP 编译器来编译 JSP 文件。如果您想要运用外部受支持 Tomcat 编译器，请使用 Tomcat 首选项页面来指向本地 Tomcat 安装版。

如果使用的是外部的受支持 Tomcat 编译器，请转至相应首选项页面并设置应用程序服务器安装目录。指定此安装目录将使 AppScan Source 能够在配置项目时自动找到所有应用程序服务器从属项。

WebLogic 11 和 12

本主题描述为了将 AppScan Source 配置为引用 Oracle WebLogic Server 应用程序服务器而需要设置的首选项。

在 Weblogic 首选项页面中，请指定服务器安装目录，并且可设置高级配置选项。指定此安装目录将使 AppScan Source 能够在配置项目时自动找到所有应用程序服务器依赖关系。

将 AppScan Source 配置为引用 WebLogic 安装目录、WebLogic JAR 文件和 JavaServer Page (JSP) 编译器选项。

如果需要更改缺省 WebLogic JSP 编译器选项或查找 weblogic.jar 文件，那么仅选择**启用高级配置选项**复选框。缺省 WebLogic JSP 编译器包括：

```
%JSP_JVM_OPTIONS%
 -Dcom.sun.xml.namespace.QName.useCompatibleSerialVersionUID=1.0
 -classpath
%JSP_COMPILER_CLASSPATH% weblogic.jspc
%JSP_OPTIONS% -verboseJspc -package
%PACKAGE_NAME% -linenumbers -g -debug -keepgenerated -compiler
%JAVAC_PATH% -webapp
%WEB_CONTEXT_ROOT_PATH% -d
%OUTPUT_PATH%
```

WebSphere Application Server

本主题描述了需要设置哪些首选项，才能将 AppScan Source 配置为引用 WebSphere Application Server 以进行 JSP 编译。

要了解 AppScan Source 支持哪个版本的 WebSphere Application Server，请参阅 http://www.ibm.com/support/docview.wss?uid=swg27027486。

在 WebSphere Application Server 首选项页面中，请指定服务器安装目录，并且可设置高级配置选项。指定此安装目录将使 AppScan Source 能够找到并使用 WebSphere Application Server JSP 编译器。

将 AppScan Source 配置为引用 WebSphere Application Server 安装目录。此外，高级配置选项使您能够设置 WebSphere Application Server JSP 编译器命令行和类路径。

请仅在要定制 WebSphere Application Server JSP 命令行或指定缺省 WebSphere Application Server 类路径（如果想要在所有 WebSphere Application Server 应用程序所使用的类路径中包含其他 jar，请更改此设置）以外的类路径的情况下选中**启用高级配置选项**复选框。

缺省 WebSphere Application Server JSP 编译器命令行选项为：

```
%CMD_EXE% %CMD_ARGS%
'%FILE(%%JSP_COMPILER_INSTALL_DIR%/bin/JspBatchCompiler%BAT%%)%'
-response.file
'%TMP_FILE(%-keepgenerated=true -recurse=true -useFullPackageNames=true
-verbose=false -createDebugClassfiles=true -jsp.file.extensions=%WEB_EXTS%
-javaEncoding=%ENCODING%
%JSP_OPTIONS% %QUOTE%-war.path=%WEB_CONTEXT_ROOT_PATH%%QUOTE%
%QUOTE%-filename=%RELATIVE_FILENAME_NO_QUOTE% %QUOTE%  %)%'
```

定义变量

保存评估或束，或者发布评估时，AppScan Source for Analysis 可能建议您创建变量来替换绝对路径（如果没有变量，AppScan Source for Analysis 会将绝对路径写入评估文件以引用诸如源文件之类的项）。为绝对路径配置变量时，可便于在多台计算机上共享评估。建议在共享评估时使用变量。

关于此任务

可以在发出保存或发布操作之前遵循本主题中的指示信息创建变量，也可以在发出保存或发布操作之后遵循第 117 页的『发布和保存时定义变量』中的步骤创建变量。

要通过示例了解变量如何帮助共享评估，请参阅第 118 页的『示例：定义变量』。

过程

1. 从主菜单中选择**编辑** > **首选项**。在"首选项"对话框中，选择**更改变量**。
2. 单击"更改变量"首选项页面上的**添加变量**按钮。
3. 输入变量的名称并浏览至将由变量替换的文件位置（创建变量后，AppScan Source for Analysis 将在两端插入百分比符号 (%)）。
4. 对评估中的任何其他引用项重复上述步骤（例如，如果评估引用了多个位置中的源，请为每个位置添加一个变量）。
5. 使用首选项页面上的**修改变量**和**删除变量**按钮来编辑和除去变量。
6. 完成对变量的定义后，单击**确定**。

通过首选项启用缺陷跟踪

"缺陷跟踪系统"首选项允许您支持将发现结果提交到缺陷跟踪系统，并确定提交缺陷的方式。

"缺陷跟踪系统"首选项页面中的"常规"选项卡用于在 AppScan Source 中启用或禁用缺陷跟踪系统集成功能。如果选中**启用缺陷跟踪系统集成**对话框，那么**提交缺陷**上下文菜单操作将可用于评估结果。 "常规"选项卡还提供对提交缺陷时哪些缺陷跟踪系统可用的离散控制。

要了解可以为受支持的缺陷跟踪系统设置的首选项，请参阅以下帮助主题：

- 第 83 页的『Rational ClearQuest 首选项』
- 第 83 页的『Quality Center 首选项』
- 第 85 页的『Rational Team Concert 首选项』
- 第 86 页的『Team Foundation Server 首选项』

Rational ClearQuest 首选项

要能够完成 Rational ClearQuest 首选项，Rational ClearQuest 管理员必须向您提供所需的 Rational ClearQuest 设置。这些设置特定于您的 Rational ClearQuest 环境。

注：与 Rational ClearQuest V8.0 集成时，Rational ClearQuest 模式必须包含 **DefectTracking** 预定义模式中可用的字段。

数据库集合

一个或多个缺陷数据库的集合。

Linux 缺省值为连接名称，Windows 缺省值为数据库集合

数据库名称

缺陷要提交到的数据库的名称。

数据库用户名

缺省 Rational ClearQuest 数据库用户名。

CQPerl 可执行文件的位置

本地计算机上 Rational ClearQuest CQPerl 可执行文件的位置。所提供的缺省位置映射到缺省 Rational ClearQuest 安装位置。

缺陷记录的实体

Rational ClearQuest 安装所配置的用于缺陷对象的实体（数据库对象）。

缺省实体为**缺陷**。

记录的描述字段

缺省描述是**描述**。

记录的标题字段

缺省标题为**标题**。

每个结果按缺陷

将一组结果作为单个缺陷或作为多个缺陷来提交。创建缺陷时，您可以更改提交方法。

Quality Center 首选项

必须首先启用 HP Quality Center 作为"常规缺陷跟踪系统"首选项，然后在 Quality Center 选项卡上设置个别首选项。

服务器 URL

Quality Center 服务器 URL - 例如 `http://<hostname>:<port>/qcbin/` 或 `https://<hostname>:<port>/qcbin/`。

用户名（可选）

用于登录 Quality Center 的用户名

密码（可选）

如果输入了用户名，请为其输入密码。

域

要连接到的 Quality Center 域。

项目

要连接到的 Quality Center 项目

自动登录

如果为 true，那么在提交结果时 AppScan Source 不提示输入登录信息，并会使用"首选项"中指定的缺省凭证进行登录。如果为 false，那么每次您向 Quality Center 提交结果时都必须登录。

自动提交

如果为 true，那么提交结果时不会出现用于提交新缺陷的对话框。AppScan Source for Analysis 使用"首选项"中指定的**缺省缺陷属性**。如果为 false，那么提交结果时将出现提示，请求您输入缺陷信息（严重性、优先级、缺陷类型以及状态等）。

重新提交之前提交的结果

已提交到 Quality Center 的结果将使用 Quality Center 缺陷信息（缺陷标识、提交用户和提交日期）进行标记。缺省情况下，AppScan Source 不会多次重新提交同一结果。这允许您将多个结果分派到 Quality Center，只需在 Quality Center 数据库中输入新结果。选中 (true) 时，可以向 Quality Center 重新提交先前提交的结果。

将每个结果作为单个错误提交

在单次操作中提交多个结果时，可以将所有结果作为单个 Quality Center 缺陷或者作为各单独 AppScan Source 结果的不同 Quality Center 缺陷进行提交。选中该复选框会将标志设置为 true，这将为各个结果创建单独的 Quality Center 缺陷。将标志设置为 false 将为已提交的所有结果创建一个 Quality Center 缺陷，作为批量提交过程的一部分。

自动生成错误摘要

如果为 true，那么 AppScan Source 会在 Quality Center 中自动生成用于提交的缺陷摘要。摘要指示缺陷中包含的结果数以及包含的结果类型，如 `Validation.Required`。

如果为 false，那么在创建新缺陷时打开的对话框中提交缺陷时，将向您显示要填写的"摘要"字段。

自动装入错误字段

缺省设置为 true。如果选中该复选框，那么 AppScan Source 会根据 Quality Center 中的当前用户和组设置来自动装入 Quality Center 数据库中的缺陷字段定义。如果设置为 false，那么在您创建新缺陷时，AppScan Source 不会在打开的对话框中显示 Quality Center 中的缺陷字段。

缺省缺陷属性

要为不同 Quality Center 缺陷属性设置缺省值，请单击"Quality Center 首选项"选项卡上的**缺省缺陷属性**。缺省值将在提交时预填充**新缺陷**对话框，或者，如果选择**自动提交**首选项，那么缺省值会静默发送到 Quality Center。

注：如果选择**自动装入错误字段**，那么在每次出现**缺陷属性**对话框时，将从 Quality Center 动态抽取缺陷属性及其可用值。因此，添加到 Quality Center 数据库的任何新字段和值都会自动显示在 AppScan Source for Analysis 中。要打开**缺省属性**对话框并使用 Quality Center 信息对其进行填充，必须具有有效的服务器、登录和连接信息。

定制 Quality Center 缺陷字段

通过配置文件，可以在"新缺陷"对话框中定制字段以及这些字段之间的交互。您可以在 `<data_dir>\config\qc.dts`（其中 `<data_dir>` 是 AppScan Source 程序数据的位置，如第 275 页的『安装和用户数据文件位置』中所述） 中找到一个示例配置文件，该文件包含样本定制和其他文档。这些定制允许您在"新缺陷"对话框中直接对 Quality Center 工作流程脚本逻辑进行建模。

可用的定制包括：

- 显示定制字段和/或缺失字段
- 强制字段一直显示（覆盖 Quality Center 设置）
- 根据其他字段的选择来更新字段的必填状态。
- 根据其他字段中的列表框选择来动态更新字段的列表框选项

Rational Team Concert 首选项

通过"Rational Team Concert 首选项"选项卡，您可以配置与 Rational Team Concert 服务器的连接，以及配置工作项属性的值。

一旦输入了您的连接信息并成功登录，那么您便可以选择连接到一个或多个项目区域。每个项目区域都可以拥有其自己的属性预置值配置。

注：连接到 Rational Team Concert 时（通过配置首选项或者提交缺陷），可能会提示您接受 SSL 证书。请参阅第 86 页的『Rational Team Concert SSL 证书』以了解更多信息。

要为给定项目区域配置属性值，请选择项目区域，然后选择**配置**。在配置对话框中，您可以将属性值设置为硬编码值或（在某些情况下）设置为将引用所选结果的变量。例如，在提交期间，在属性值中使用的 `{Finding.fileName}` 将被替换为结果的实际源代码文件名。为支持这些变量的属性值提供了内容辅助 (`<Ctrl>+<Space>`)。鼓励团队使用 Rational Team Concert 首选项主页上提供的**导入**和**导出**按钮来共享这些配置。

Rational Team Concert SSL 证书

安装 Rational Team Concert 服务器时，应对其进行配置以使用有效 SSL 证书。如果未完成该操作，那么在登录到该服务器时将接收到不可信连接消息（在配置首选项或提交缺陷时）。本主题概述了 Rational Team Concert SSL 证书注意事项。

SSL 证书存储位置

已被永久接受的证书存储在 <user_home>/.jazzcerts（其中 <user_home> 是您的操作系统主目录（例如，在 Windows 上，此目录可能是 C:\Documents and Settings\Administrator\））中。移除 <user_home>/.jazzcerts 会删除 AppScan Source 和 Rational Team Concert 客户机的所有已存储证书。

与 Rational Team Concert 客户机共享 SSL 证书

AppScan Source 将其证书库与 Rational Team Concert 客户机共享。如果您使用 Rational Team Concert 客户机永久接受某个证书，那么此证书将被 AppScan Source 复用（您不会在 AppScan Source 中收到关于接受证书的提示）。类似地，如果您在 AppScan Source 中永久接受某个证书，那么此证书将被 Rational Team Concert 客户机复用。

从 AppScan Source for Analysis 进行缺陷跟踪时的 Rational Team Concert 服务器重命名注意事项

如果已在 AppScan Source for Analysis 中启用了 Rational Team Concert 缺陷跟踪，而且 Rational Team Concert 服务器已重命名，那么该服务器上项目区域的任何现有配置在 AppScan Source for Analysis 中都将不再可用。您将需要通过该服务器的新存储库 URI 连接到服务器，并在"缺陷跟踪系统"首选项中重新创建配置。

Team Foundation Server 首选项

使用"Team Foundation Server 首选项"选项卡，您可以配置至 Microsoft Team Foundation Server 的连接以及配置工作项字段的值。

一旦输入了您的连接信息并成功登录，那么您便可以选择连接到一个或多个项目。

注：将登录名配置为 Team Foundation Server 2010 时，服务器 URL 必须包含您要连接到的 Team Project Collection。例如，http://myserver:8080/tfs/*DefaultCollection*。

每个项目都可以拥有其自己的字段预置值配置。

要为给定项目配置字段值，请选择项目，然后选择**配置**。在配置对话框中，您可以将字段值设置为硬编码值或（在某些情况下）设置为将引用所选结果的变量。例如，在提交期间，在字段值中使用的 {Finding.fileName} 将被替换为结果的实际源代码文件名。为支持这些变量的字段提供了内容辅助 (<Ctrl>+<Space>)。

鼓励团队使用**导入**和**导出**按钮（在主 Team Foundation Server 首选项页面上提供）来共享这些配置。

Eclipse 工作空间导入器：Eclipse 或 Rational Application Developer for WebSphere Software (RAD) 首选项配置

AppScan Source for Analysis 安装会提供缺省 Eclipse 导入器。此导入器确定 Eclipse 和 JRE 的位置。如果缺省 Eclipse 导入器无法导入工作空间，那么可能需要创建新的 Eclipse 导入器。

开始之前

每个导入器配置均代表一个 Eclipse 或 Rational Application Developer for WebSphere Software (RAD) 安装。要使用这些配置将现有工作空间和项目导入到 AppScan Source for Analysis，可能还需要在 Eclipse 环境中安装 AppScan Source for Development 插件。

在添加 RAD 工作空间之前，您必须创建针对工作空间类型的配置。

过程

1. 在 AppScan Source for Analysis 中，从主工作台菜单中选择**编辑** > **首选项**。
2. 选择 **Eclipse 工作空间导入器**。
3. 单击**创建新配置**，然后完成"新建导入配置"对话框以创建新配置：
   - **产品**：选择相应产品

     注：如果无法选择先前用于创建工作空间的产品，请确保在尝试创建工作空间导入器之前已完成 第 39 页的『Eclipse 或 Application Developer 更新』中概括的配置步骤。
   - **名称**：导入器名称
   - **位置**：Eclipse 安装基本目录的路径
   - **JRE 位置**：Java Runtime Environment (JRE) 的根目录。使用 `<install_dir>\JDKS`（其中 `<install_dir>` 是 AppScan Source 安装位置） 中的 JDK 或任何其他首选 JDK。
4. 单击**确定**。
5. 要将导入器确定为缺省值，请选择导入器并单击**将所选配置设为缺省值**。这将使一个图标显示在导入器的**缺省值**列中。

电子邮件

配置用来发送视为缺陷的结果的电子邮件设置。

- **收件人地址**：接收方的电子邮件地址。缺省情况下，"通过电子邮件发送结果"对话框中的**收件人**字段将使用此电子邮件地址进行填充，但可以在准备电子邮件时轻松对该字段进行更改。
- **发件人地址**：发件方的电子邮件地址。

  注：将建议有效的电子邮件地址，以避免接收方邮件客户端将该电子邮件视为垃圾邮件。
- **邮件服务器**：配置为 `mail.myexample.com` 的 SMTP 邮件服务器。

  要点：请与系统管理员进行核对，以确保您采用了正确的邮件服务器信息。

Java 和 JavaServer Pages

使用该首选项页面可添加、修改或删除用于扫描的 Java Development Kit (JDK)（并设置缺省 JDK）。此外，使用该页面还可设置缺省 JavaServer Page (JSP) 编译器。

缺省值

确认用于扫描的 JDK 的位置。当项目未指定显式的 JDK 时，扫描将使用缺省 JDK 路径。要将 JDK 设置为缺省值，请右键单击所确认的 JDK 名称，然后单击**设置缺省 JDK**。缺省值图标将显示在表中，确认当前的缺省 JDK。

注：JSP 项目的缺省编译器是 Tomcat 7，后者需要 Java V1.6 或更高版本。如果 **Tomcat 7** 保留为缺省值，那么使用更低版本的 JDK 将导致扫描期间出现编译错误。

JDK 名称和路径

确认 JDK 的名称和位置。

JSP 项目的缺省编译器

现成可用的 Tomcat 7 是缺省 JSP 编译器设置。要了解 AppScan Source for Analysis 支持的编译器的相关信息，请参阅http://www.ibm.com/support/docview.wss?uid=swg27027486。

知识库文章

使用"知识库文章"首选项页面来设置包含 AppScan Source 安全知识库文章的位置。

该页面列出了包含文章的目录。要添加目录，请单击**添加内容目录**，并浏览至文章位置。要除去目录，请将其选中，然后单击**除去**。

项目文件扩展名

为每个项目类型配置或添加有效的全局文件扩展名，更改要在扫描中包含的扩展名，从扫描中排除扩展名，以及将扩展名指定为 Web 文件。

将为每种可用的语言或项目类型显示一个选项卡页面：
Java、JavaScript、ASP、Perl、PHP、ColdFusion、PBSA（用于基于模式的项目类型）、COBOL、PL/SQL、T-SQL、VB.NET、.Net Assembly、VB、C/C++、ASP .NET 1.x、ASP .NET 2.x、WSDL 和 C#。添加新扩展名时，确定具有新扩展名的文件是否可以进行扫描，是否视为 Web 文件，或者是否可以排除。

该页面中的设置是全局的。要为单个项目设置文件扩展名，使用所选项目的"属性"视图的 第 216 页的『文件扩展名』 选项卡。

文件扩展名设置

表 *10.* 文件扩展名设置

设置	描述	用法示例
扫描或**评估**	包含带有在完整分析中指示的扩展名的文件。	• 如果已为 Java 项目创建 .xxx 扩展名并将此扩展名标记为**扫描**或**评估**，那么将编译并扫描具有该扩展名的文件。 • 如果不应编译和扫描某个文件（例如 C++ 中的头文件），那么该文件是项目的一部分但不被标记为**扫描**或**评估**。这些文件应包含在项目中，而且应在基于模式的分析过程中进行搜索。.
Web 文件	用针对 JSP 编译的指定扩展名标记文件。该设置使 AppScan Source 能够将 web 源与非 web 源分开。	如果已为 Java 项目创建 .yyy 扩展名并将此扩展名标记为 **Web 文件**，那么具有该扩展名的文件将被安排为项目中的 Web 源。当 AppScan Source 为分析做准备时，这些文件将被预编译为类以进行分析。
排除	请勿在项目中为带有指定扩展名的文件创建源文件。将不会扫描带有该扩展名的文件。	为项目需要进行编译的文件创建 .zzz 扩展名，但无需包含在分析中。

第 4 章 扫描源代码和管理评估

本部分说明如何扫描源代码和管理评估。

一旦配置了应用程序和项目，或者使用 Application Discovery Assistant 为您创建了应用程序和项目，您即已准备好扫描源代码。可以保存或发布扫描的结果，即评估。已保存的评估是本地保存的扫描结果文件，可以将其发布，以后打开以另行分类，或者在 AppScan Source for Development 中打开。已发布的评估包含了保存到 AppScan Enterprise Server 的扫描结果。

您在两个视图中管理评估：

- 我的评估
- 已发布的评估

注：保存、发布或打开评估时，在状态栏中显示进度。

扫描源代码

此任务描述用于启动扫描的各种方法。

关于此任务

您可以在各级别（所有应用程序、一个或多个应用程序、一个或多个项目或者一个或多个文件）进行扫描。如果您已完成扫描，那么可以再次扫描，前提是其评估已打开。

- 『扫描所有应用程序』
- 第 92 页的『扫描一个或多个应用程序』
- 第 92 页的『扫描一个或多个项目』
- 第 92 页的『扫描一个或多个文件』
- 第 93 页的『重新扫描代码』

请参阅第 93 页的『扫描注意事项』以了解关于特定于操作系统的注意事项、特定于语言的注意事项和可能影响扫描的其他限制的信息。

扫描时，会一直使用扫描配置。如果设置缺省扫描配置然后将其删除，那么扫描时将以静默方式使用**普通扫描**内置扫描配置。要了解关于扫描配置的更多信息，请参阅第 94 页的『管理扫描配置』和以下扫描选项描述。

扫描所有应用程序

过程

完成以下其中一个操作：

1. 在主工作台菜单中选择**扫描** > **扫描全部**。扫描将使用缺省扫描配置来运行。
2. 在"资源管理器"视图中：

© Copyright IBM Corp. 2003, 2017

- 右键单击**所有应用程序**，然后从菜单中选择**扫描所有应用程序**。扫描将使用缺省扫描配置来运行。
- 要将其他扫描配置用于扫描，请右键单击**所有应用程序**，然后从菜单中选择**扫描所有应用程序时使用**。选择要使用的扫描配置；或者，如要设置其他缺省扫描配置，请选择**编辑配置**操作（在"扫描配置"视图中，选择要设为缺省的配置，然后单击**选为缺省**）。

扫描一个或多个应用程序

过程

1. 在"资源管理器"视图中，选择一个或多个应用程序。
2. 完成以下其中一个操作：
   a. 在主工作台菜单中选择**扫描** > **扫描所选项**。扫描将使用缺省扫描配置来运行。
   b. 在"资源管理器"视图中：
      - 右键单击所选项，然后从菜单中选择**扫描应用程序**。扫描将使用缺省扫描配置来运行。
      - 要将其他扫描配置用于扫描，请右键单击所选项，然后从菜单中选择**扫描应用程序时使用**。选择要使用的扫描配置；或者，如要设置其他缺省扫描配置，请选择**编辑配置**操作（在"扫描配置"视图中，选择要设为缺省的配置，然后单击**选为缺省**）。

扫描一个或多个项目

过程

1. 在"资源管理器"视图中，选择一个或多个项目。
2. 完成以下其中一个操作：
   a. 从主工作台菜单中选择**扫描** > **扫描所选项**。扫描将使用缺省扫描配置来运行。
   b. 在"资源管理器"视图中：
      - 右键单击所选项，然后从菜单中选择**扫描项目**。扫描将使用缺省扫描配置来运行。
      - 要将其他扫描配置用于扫描，请右键单击所选项，然后从菜单中选择**扫描项目时使用**。选择要使用的扫描配置；或者，如要设置其他缺省扫描配置，请选择**编辑配置**操作（在"扫描配置"视图中，选择要设为缺省的配置，然后单击**选为缺省**）。

扫描一个或多个文件

过程

1. 在"资源管理器"视图中，选择一个或多个文件。
2. 完成以下其中一个操作：
   a. 从主工作台菜单中选择**扫描** > **扫描所选项**。扫描将使用缺省扫描配置来运行。
   b. 在"资源管理器"视图中：
      - 右键单击所选项，然后从菜单中选择**扫描文件**。扫描将使用缺省扫描配置来运行。

- 要将其他扫描配置用于扫描，请右键单击所选项，然后从菜单中选择**扫描文件时使用**。选择要使用的扫描配置；或者，如要设置其他缺省扫描配置，请选择**编辑配置**操作（在"扫描配置"视图中，选择要设为缺省的配置，然后单击**选为缺省**）。

重新扫描代码

过程

要重新扫描当前目标，请从主菜单中选择**扫描** > **重新扫描**。最近用来扫描此项（或多个所选项）的扫描配置将再次用于扫描：

- 如果上次扫描使用了缺省扫描配置，并且已设置了新的缺省扫描，那么将使用新缺省扫描配置来进行扫描。
- 如果上次扫描使用了非缺省扫描配置，那么将使用该扫描配置进行扫描。如果该扫描配置自上次扫描以来已修改并保存，那么将使用修改后的扫描配置。

扫描注意事项

该主题描述了可能影响您的扫描的限制和注意事项。

- 『常规』
- 『Windows』
- 『Linux』
- 第 94 页的『Java』

常规

限制：当扫描多个应用程序或项目时，将在"我的评估"视图中创建一个父节点（其中包含每个已扫描项的评估）。在此情况下，无法管理单独子评估（例如，无法单个地移除或发布子评估）。当同时扫描多个应用程序或项目时，您只能将评估作为组（父节点）来管理。

要点：如果您所处理的是在开发环境中具有依赖性的 AppScan Source 项目（例如 IBM MobileFirst Platform 项目），请确保在导入该项目之前在开发环境中对其进行构建。导入该项目后，如果您修改其中的文件，请确保在 AppScan Source 中进行扫描之前在开发环境中重新构建该项目（如果不执行此操作，那么 AppScan Source 将忽略对文件做出的修改）。

Windows

对于 Microsoft .NET 文件（例如 `.cs` 和 `.vbnet`）而言，扫描一个或多个选定文件的功能不可用。

Linux

AppScan Source for Analysis 客户机基于 Eclipse 构建。在 Linux 上，Eclipse 要求安装第三方组件才能呈现基于浏览器的内容。如果没有此组件，那么 AppScan Source for Analysis 可能会显现诸如登录后挂起或在产品使用期间发生故障之类的症状。请参阅第 104 页的『在 Linux 上使 AppScan Source for Analysis 支持基于浏览器的内容』以了解更多信息。

Java

提示：如果要扫描 Java 而且 Java 项目中缺少依赖关系，那么 AppScan Source 将通过合成依赖关系会提供的片段来创建跟踪。该合成可能不会准确地反映 .jar 文件中的信息。要限制合成并因此提高结果的准确性，可指定缺少的依赖关系，如下所示：

1. 扫描之后，打开 <data_dir>\logs\scanner_exceptions.log（其中 <data_dir> 是 AppScan Source 程序数据的位置，如第 275 页的『安装和用户数据文件位置』中所述） 以查看 AppScan Source 是否报告了缺少的依赖关系。
2. 修改项目属性以包含依赖关系。为此，遵循第 69 页的『修改应用程序和项目属性』中的指示信息，然后在 **JSP 项目依赖关系**或**项目依赖关系**选项卡中指定和保存依赖关系。
3. 重新扫描项目。

注：缺少情况下，AppScan Source 将扫描缺少依赖关系的 Java 文件和 Java 字节代码，或扫描编译错误。可如下所示更改这些设置：

1. 在文本编辑器中打开 <data_dir>\config\scan.ozsettings。
2. 要更改编译错误设置，找到文件中的 compile_java_sources_with_errors。此设置将与以下类似：

```
<Setting
  name="compile_java_sources_with_errors"
  value="true"
  default_value="true"
  type="bool"
  hidden="true"
  display_name="compile_java_sources_with_errors"
  description="Attempt to scan java code with compilation errors."
/>
```

3. 要更改缺少的依赖关系设置，找到文件中的 scan_java_bytecode_without_dependencies。此设置将与以下类似：

```
<Setting
  name="scan_java_bytecode_without_dependencies"
  value="true"
  default_value="true"
  type="bool"
  hidden="true"
  display_name="scan_java_bytecode_without_dependencies"
  description="Scans Java bytecode even when some of
    the dependencies are missing by artificially
    synthesizing the unresolved symbols."
/>
```

4. 在设置中，修改 value 属性。如果属性设置为 true，该设置将打开。如果编译错误设置设置为 false，那么 AppScan Source 将在扫描期间跳过有编译错误的 Java 代码。如果缺少的依赖关系设置设置为 false，那么缺少依赖关系时 AppScan Source 将不会扫描 Java 字节码。
5. 在修改该设置后保存文件，并启动或重新启动 AppScan Source。

管理扫描配置

当启动扫描时，会使用扫描配置。在扫描配置中，您可以指定要在扫描期间使用的源规则。在扫描配置中进行的设置通常可以产生更佳的扫描结果，而能够保存这些设置，就可以使扫描更为轻松和省时。

关于此任务

此任务对管理扫描配置所涉及的步骤进行描述。

- 『创建扫描配置』
- 第 97 页的『修改扫描配置』
- 第 98 页的『除去扫描配置』
- 第 98 页的『共享扫描配置和使用共享配置』
- 第 98 页的『将扫描配置设置为缺省配置』
- 第 99 页的『内置扫描配置』

扫描配置在第 99 页的『"扫描配置"视图』中进行管理。可以通过从主菜单栏中选择**视图 > 扫描配置**，或者通过选择"资源管理器"视图中的**编辑配置**操作来打开此视图。

一旦扫描配置已就位，在 AppScan Source for Analysis 中启动扫描时即可使用这些配置（请参阅第 91 页的『扫描源代码』以获取更多信息）。在 AppScan Source for Automation、AppScan Source for Development 和 AppScan Source 命令行界面 (CLI) 中启动扫描时也可使用扫描配置。

创建扫描配置

过程

1. 完成以下其中一个操作：
   a. 单击"扫描配置"视图中的**新建**按钮。
   b. 从列表中选择现有配置，然后单击**复制**。这将导致系统根据原始扫描配置的设置来创建扫描配置，您可以修改该配置并将其另存为新配置。
2. 在**常规**选项卡 - **基本信息**部分中：
   a. 在**名称**字段中输入配置的唯一名称。请注意，在扫描配置中，指定唯一名称是唯一的必需设置，所有其他设置都是可选的。
   b. 可选： 输入此扫描配置的描述。
3. 可选： 使用**常规**选项卡 - **过滤器信息**部分来设置扫描的过滤器。要了解关于过滤器的信息，请参阅第 124 页的『通过过滤器筛选』。 在该部分中，可选择每当使用配置时就会应用于扫描的一个或多个过滤器。选择过滤器时，可选择 AppScan Source预定义过滤器或共享过滤器或您已创建的过滤器。在该部分中：
   a. 单击**添加**，然后在"选择过滤器"对话框中，选择想要添加的过滤器。选择过滤器后，其特征将在对话框的右边显示为只读。单击**确定**以将过滤器添加到扫描配置。

      注：

      - 要将过滤器的反面应用于扫描配置，首先选择**反转过滤器**对话框，然后单击**确定**。
      - 当您处于"选择过滤器"对话框中时，可选择多个要添加的过滤器。如果执行该操作时选中了**反转过滤器**复选框，所有选的过滤器的反面都将添加到扫描配置。

      退出"选择过滤器"对话框之后，过滤器将出现在列表中，而且**已反转**列将指示过滤器是否已反转。
   b. 要除去已添加的过滤器，选择或多选过滤器，然后单击**除去**。

c. 排除过滤器包含了用于从结果中移除漏洞类型、应用程序编程接口 (API)、文件、目录、项目或跟踪规则的规则。如果在扫描配置中包含多个排除过滤器，那么有可能它们彼此冲突并影响结果。例如，假定有以下两个过滤器：

   - 过滤器 1 除去漏洞类型 Validation.EncodingRequired 的所有结果。它不是反向的，因此将从评估排除这些结果。
   - 过滤器 2 除去漏洞类型 Validation.Required 的所有结果。它不是反向的，因此将从评估排除这些结果。

   如果使用扫描配置时应用了这两个过滤器，那么缺省情况下它们会将彼此排除掉。过滤器 1 将排除 Validation.EncodingRequired 结果，但它将包含 Validation.Required 结果。过滤器 2 将排除 Validation.Required 结果，但它将包含 Validation.EncodingRequired 结果。最终的结果是将包含所有 Validation.EncodingRequired 和 Validation.Required 结果。

   要已指定的任何排除过滤器的结果，选择**与任何非反转排除过滤器匹配**。在上述的示例中，如果选择了该复选框，那么将从评估排除所有 Validation.EncodingRequired 和 Validation.Required 结果。

4. 可选： 使用**污染流分析**选项卡 - **污染流分析**部分来启用污染流分析。缺省情况下选择了**污染流分析**，它是 AppScan Source 执行的主要分析类型。启动扫描后，污染流分析将生成使您能够更好地确定漏洞的数据流。可设置分析的**范围**，如下所示：
   - **应用程序**范围：将在应用程序中的项目以及项目中的文件之间执行污染流分析。
   - **项目**范围：将项目中的文件之间执行污染流分析。
   - **文件**范围：将单独地为每个文件执行污染流分析。

   注：扫描 JavaScript、ColdFusion、Perl、Cobol、PL/SQL 或 T-SQL 时，**污染流分析**选项卡中的设置不适用。

5. 可选： **污染流分析**选项卡 - **扫描规则**部分使您能指定将对扫描生效的源规则（请参阅第 100 页的『"污染流分析"选项卡』以获取更多信息）。在此部分中，可以选择使用所选源规则集来进行扫描，也可以选择将单独规则属性用于扫描：
   a. 缺省情况下，此部分允许您选择要应用的规则集。选中一个或多个可用规则集复选框。
   b. 要选择个别规则属性而不是规则集，请单击**放弃所选规则集并让我选择个别规则属性**。这会打开"选择规则属性"对话框，以允许您选择个别规则属性。如果完成此对话框，将放弃已选择的任何规则集。具有选定规则属性的扫描规则将用于扫描。

   如果选择了个别规则属性用于扫描，但要改为选择规则集，请单击**放弃所选规则属性并让我按规则集进行选择**。这将放弃已在"选择规则属性"对话框中选择的任何规则属性，并允许您改为选择规则集。

   注：
   - 选择单个规则属性时，选定项适用于源（而不是接收器）的属性。这意味着您会将攻击表面限制为只是具有选定属性的那些源。您可能会看到在结果中漏洞与选定属性不匹配，因为漏洞类型基于接收器而不基于源。
   - 扫描 JavaScript、ColdFusion、Perl、Cobol、PL/SQL 或 T-SQL 时，**污染流分析**选项卡中的设置不适用。

6. 可选： **污染流分析**选项卡 - **高级设置**部分仅供高级用户使用。它包含可改进扫描结果的各种设置。悬浮式文本描述此部分中的各设置。

   注：扫描 JavaScript、ColdFusion、Perl、Cobol、PL/SQL 或 T-SQL 时，**污染流分析**选项卡中的设置不适用。

7. 可选： **模式分析**选项卡中的设置使您能够启用和设置基于模式的扫描的规则。基于模式的扫描是根据定制的搜索条件来对源代码进行的分析。请参阅第 205 页的『以基于模式的规则进行定制』以了解更多信息。 要启用基于模式的扫描，选择**模式分析**复选框。执行该操作时，**模式规则集**和**模式规则**部分将变为已启用：

   a. 要添加规则集，单击**模式规则集**部分中的**添加**。这会打开"添加模式规则集"对话框，以允许您选择一个或多个规则集。选择规则集时，它所包含的规则将显示在对话框的右边，规则集适用的项目类型在**项目类型**字段中列出。单击**确定**以添加选定规则集。

   b. 要添加规则，单击**模式规则**部分中的**添加**。这会打开"添加模式规则"对话框，以允许您选择一个或多个规则。还可单击**新建规则**以创建新规则（请参阅第 208 页的『创建模式规则』）。如果创建新规则，那么该规则将添加到列表并被选中。选择或创建规则后，单击**确定**以将它们添加到扫描配置。

      提示：在"添加模式规则"对话框中，工具提示帮助指示用于每个规则的表达式。

      注：

      - 添加规则集时，该规则集中的规则将从"添加模式规则"对话框中过滤掉。
      - 如果添加规则然后添加还包含规则的规则集，"模式规则"部分将列出规则，并指示规则包含在规则集中。因为该规则已包含在规则集中，如果尝试除去单个规则，将仅从"模式规则"部分将其除去，而不会从扫描配置中将其除去。要从扫描配置除去规则，除去规则集或对规则集进行修改以便它不包含规则。

   c. 您添加的任何规则集或规则都可使用**除去**按钮或通过右键单击并选择**除去**来除去。还可以使用该操作选择多个规则和规则集。

      注：如果扫描配置包含在后面将从脆弱性数据库中除去的规则或规则集，那么下次打开扫描配置时，将显示规则或规则集以及指示它们不存在的消息。**除去**操作将不可用于这些规则或规则集，但下次保存扫描配置时，它们将被自动除去。

8. 一旦在扫描配置中作出了所有设置，单击**保存**。

修改扫描配置

过程

1. 在"扫描配置"视图中，选择要修改的扫描配置。

   注：要共享扫描配置，或者修改或删除已共享的扫描配置，您必须拥有**管理共享配置**许可权。要了解关于设置许可权的信息，请参阅《*IBM Security AppScan Source* 安装和管理指南》。

   注：您无法修改 第 99 页的『内置扫描配置』。

2. 修改此扫描配置后，单击**保存**。

除去扫描配置

过程

1. 在"扫描配置"视图中，选择要除去的扫描配置。

   注：您无法除去 第 99 页的『内置扫描配置』。

2. 单击**删除**。

共享扫描配置和使用共享配置

关于此任务

可以将扫描配置保存到 AppScan Source 数据库 以将其与他人共享。要将扫描配置与他人共享，请单击**共享**。

注：要共享扫描配置，或者修改或删除已共享的扫描配置，您必须拥有**管理共享配置**许可权。要了解关于设置许可权的信息，请参阅《*IBM Security AppScan Source* 安装和管理指南》。

已由他人共享的扫描配置会在扫描配置列表中显示。

注：

- 扫描配置一经共享，就无法除去共享。您可以完成以下其中一个任务：
  - 删除共享扫描配置。这将在服务器上将其删除。
  - 复制共享扫描配置，然后将其删除。复制扫描配置将会创建该配置的相同的本地副本。
- 如果要共享包含已共享过滤器的扫描配置，共享操作将在没有提示的情况下完成。但如果要共享包含已在本地创建的过滤器的扫描配置，提示将告诉您还将共享过滤器。如果不想共享本地过滤器，您将能够取消扫描配置共享操作。
- 您无法通过添加本地过滤器来修改和保存共享扫描配置。要将这些过滤器添加到共享扫描配置，请共享过滤器，然后将它们添加到共享扫描配置。
- 如果您具有**管理共享配置**许可权，但没有**管理共享过滤器**许可权，那么无法共享包含本地过滤器的扫描配置。

将扫描配置设置为缺省配置

关于此任务

您可以将任何扫描配置设置为缺省配置 - 无论它是本地、内置还是共享的配置。如果将共享扫描配置设置为缺省配置，那么该设置将仅在本地进行，而不会影响其他用户。扫描时，会一直使用扫描配置。如果设置缺省扫描配置然后将其删除，那么扫描时将以静默方式使用**普通扫描**内置扫描配置。

要了解如何使用缺省扫描配置，请参阅第 91 页的『扫描源代码』。

过程

1. 在"扫描配置"视图中，选择要设置为缺省配置的扫描配置。
2. 单击**选择为缺省配置**。

内置扫描配置

关于此任务

AppScan Source 提供内置扫描配置。不能修改或除去这些配置。在列表中选择这些配置后，您就能够复制它们或查看其设置。

"扫描配置"视图

通过"扫描配置"视图，您可以创建能够在启动扫描时使用的配置。还可以使用视图来设置缺省扫描配置。在扫描配置中，可以指定要在扫描期间使用的源规则，并且可以包含许多扫描设置。在扫描配置中进行的设置通常可以产生更佳的扫描结果，而能够保存这些设置，就可以使扫描更为轻松和省时。

"扫描配置"视图有以下主要部分：

- 『扫描配置管理』
- 『"一般"选项卡』
- 第 100 页的『"污染流分析"选项卡』
- 第 101 页的『"模式分析"选项卡』

扫描配置管理

使用此部分可选择、添加、除去、保存和共享扫描配置，以及将扫描配置设置为缺省配置。

- 要创建新扫描配置，请单击**新建**。完成扫描配置设置后，单击**保存**以保存更改。要将该扫描配置设置为缺省配置，请在将其保存后单击**选为缺省**。要了解如何使用缺省扫描配置，请参阅第 91 页的『扫描源代码』。
- 要处理现有扫描配置，请从列表中选择该配置：
  - 如果修改扫描配置设置，请单击**保存**以保存更改（通过切换到其他扫描配置，然后单击**放弃**，可以放弃不需要的更改）。
  - 要除去所选扫描配置，请单击**删除**。
  - 要复制此扫描配置，请单击**复制**。这样，将基于原始扫描配置的设置来创建新扫描配置。
  - 要将此扫描配置设置为缺省配置，请单击**选为缺省**。要了解如何使用缺省扫描配置，请参阅第 91 页的『扫描源代码』。
  - 要将此扫描配置与他人共享，请单击**共享**。这会将此扫描配置保存到 AppScan Source 数据库。

    注：要共享扫描配置，或者修改或删除已共享的扫描配置，您必须拥有**管理共享配置**许可权。要了解关于设置许可权的信息，请参阅《*IBM Security AppScan Source* 安装和管理指南》。

  注：AppScan Source 提供内置扫描配置。不能修改或除去这些配置。在列表中选择这些配置后，您就能够复制它们或查看其设置。

"一般"选项卡

基本信息

通过此部分，您可以对扫描配置命名并为其提供描述。

过滤器

在该部分中，可选择每当使用配置时就会应用于扫描的一个或多个过滤器。选择过滤器时，可选择 AppScan Source预定义过滤器或共享过滤器或您已创建的过滤器。请参阅第 94 页的『管理扫描配置』以了解更多详细信息。

"污染流分析"选项卡

污染流分析

启用和设置污染流分析的范围。

扫描规则

使用此部分可确定哪些源规则将对扫描生效。

源是对程序的输入，如文件、servlet 请求、控制台输入或套接字。通过排除某些源规则，可加速扫描并避免检测您并不感兴趣的输入产生的漏洞。

规则通过规则属性进行了标记，以指示它们与特定漏洞、机制、属性或技术相关。这些属性分组为规则集，而规则集对应于一组常用的相关规则。可通过指定规则集或各个规则属性来限制扫描中包含的源规则。

- 选择要包含在扫描中的一个或多个漏洞类型（在规则集中按类型进行组织）：
  - **所有内容**：如果选择该项，将检测从所有受支持输入源产生的漏洞。
  - **用户输入**：如果选择该项，将检测最终用户的输入产生的漏洞。
  - **Web 应用程序**：如果选择该项，将检测 Web 应用程序风险产生的漏洞。
  - **错误处理和记录**：如果选择该项，那么将检测错误处理和日志记录机制产生的漏洞。
  - **环境**：如果选择该项，那么将检测配置文件、系统环境文件和属性文件产生的漏洞。
  - **外部系统**：如果选择该项，将检测外部实体产生的漏洞。
  - **数据存储**：如果选择该项，那么将检测数据存储（例如数据库和高速缓存）产生的漏洞。
  - **异常内容**：如果选择该项，那么将检测通常不属于生产应用程序的例程产生的漏洞。
  - **文件系统**：如果选择该项，将检测文件系统产生的漏洞。
  - **敏感数据**：如果选择该项，将检测敏感数据产生的漏洞。

  悬浮式文本描述此部分中的各规则集。
- 选择要包含在扫描中的各条扫描规则属性：单击**放弃所选规则集并让我选择个别规则属性**。这会打开"选择规则属性"对话框，以允许您选择个别规则属性。如果完成此对话框，将放弃已选择的任何规则集。具有选定规则属性的扫描规则将用于扫描。

高级设置

此部分旨在仅供高级用户使用。它包含可改进扫描结果的各种设置。悬浮式文本描述此部分中的各设置。

"模式分析"选项卡

模式分析

使用扫描配置时使用该部分来启用基于模式的扫描。基于模式的扫描是根据定制的搜索条件来对源代码进行的分析。

模式规则集和模式规则

使用这些部分可添加要在模式分析期间使用的规则和规则集。请参阅第 205 页的『以基于模式的规则进行定制』和第 94 页的『管理扫描配置』，以获取更多信息。

Java 的递增分析

启用递增分析时，AppScan Source 将对分析数据进行高速缓存。然后，当您重新扫描项目或应用程序时，AppScan Source 使用该值来确定代码更改，并将仅再次分析受更改影响的代码部分。最终结果是代码的完整分析，但是一小部分时间内的完整分析。

关于此任务

在 Windows 和 Linux 上支持递增分析。启用后，将对 AppScan Source 项目或应用程序或者对 Eclispe 项目或工作空间执行递增分析。启用递增分析之后，对项目、应用程序或工作空间运行的第一个扫描将始终是完整扫描（完整扫描期间才会更新漏洞分析高速缓存）。这使 AppScan Source 能够对后续扫描的数据进行高速缓存。因此，只要漏洞分析高速缓存未被清除而且只要已更改文件的数量不超过您可以确定的阈值设置，那么项目、应用程序或工作空间的扫描是递增扫描。

要启用和使用递增分析，请执行以下步骤：

过程

1. 在文本编辑器（其中 <data_dir> 是 AppScan Source 程序数据的位置，如第 275 页的『安装和用户数据文件位置』中所述）中打开 <data_dir>\config\scan.ozsettings。在文件中查找 incremental_analysis 设置。此设置将与以下类似：

   ```
   <Setting
     name="incremental_analysis"
        read_only="false"
     default_value="false"
     description="Attempt to scan only changed files,
       instead of re-scanning everything."
     type="bool"
     value="false"
     display_name="Incremental Analysis"
     hidden="true"
   />
   ```

   在该设置中，修改 value 属性。如果属性设置为 true，该设置将打开。如果属性设置为 false，那么 AppScan Source 在扫描时将不会执行递增分析。

2. 在 <data_dir>\config\scan.ozsettings 中，找到 percentage_of_files_changed 设置：

   ```
   <Setting
     name="percentage_of_files_changed"
        read_only="false"
     default_value="50"
     description="In incremental scanning, if percentage of files
   ```

```
  being changed since last scan exceeds the threshold, full
  scan will be initiated. The percentage ranges from 0 to 100.
  Default threshold is 50, which represents 50%."
  type="int"
  value="50"
  display_name="Percentage of files being changed"
  hidden="true"
/>
```

该设置使您能够指定开始完整扫描之前需要更改的文件的百分百。缺省情况下，该阈值百分比为 50%，这意味着如果在项目、应用程序或工作空间中有 50% 或更多文件发生更改后重新扫描，那么将启动完整扫描而不是递增分析扫描。在该设置中，根据需要将 value 属性更改为您期望的阈值百分比。

3. 在修改所有相关设置之后保存 <data_dir>\config\scan.ozsettings，然后启动或重新启动支持递增分析的 AppScan Source 产品。例如，重新启动 AppScan Source for Analysis、AppScan Source for Development Eclipse 插件 或 AppScan Source 命令行界面 (CLI)，或者重新启动 AppScan Source for Automation 服务。
4. 现在，当您通过相同扫描配置重新扫描 Java 应用程序或项目时，如果已更改文件的数量未超过阈值而且如果漏洞分析高速缓存尚未清除，那么将执行递增分析。
5. **清除漏洞分析高速缓存：**如果递增扫描有问题，或者想要在启用递增分析时执行完整分析扫描，请在再次扫描之前清除漏洞高速缓存：
   - AppScan Source for Analysis:
     a. 打开 AppScan Source 项目的"属性"视图。如果要扫描应用程序，打开任何子项目的属性视图（删除项目的高速缓存也将删除其应用程序的高速缓存）。
     b. 在"概述"选项卡中，单击**清除高速缓存**。
   - AppScan Source for Development Eclipse 插件：删除 <data_dir>\temp\<workspace>\<project>，其中：
     – <data_dir> 是 AppScan Source 程序数据的位置，如第 275 页的『安装和用户数据文件位置』中所述.
     – <workspace> 是在其中进行扫描的 Eclipse 工作空间的名称。要删除整个工作空间的高速缓存，请删除整个 <data_dir>\temp\<workspace> 目录。
     – <project> 是要扫描的 Eclipse 项目的名称。要删除项目的高速缓存，请删除 <data_dir>\temp\<workspace>\<project> 目录。
   - AppScan Source 命令行界面 (CLI)：使用 clearcache 命令，如*IBM Security AppScan Source Utilities* 用户指南中所述。
   - AppScan Source for Automation：使用 ScanApplication命令 -clearcache 参数，如*IBM Security AppScan Source Utilities* 用户指南中所述。

结果

在 AppScan Source for Analysis 中进行扫描之后，可使用**评估差异**功能在代码更改之前和之后比较评估。

提示：

- 要强制实施完整分析扫描，禁用递增分析或清除漏洞分析高速缓存。
- 执行递增分析时，应在进行以下任何更改之后运行完整分析扫描：
  – 安全性规则更改或适用于项目或应用程序的定制规则更改。

- 扫描配置更改。
- 影响扫描的 .ozsettings 文件更改。
- 应用程序或项目属性的更改。例如，在所有应用程序或选定应用程序或项目的 AppScan Source for Analysis"属性"视图中进行的任何更改。
- 将新项目添加到应用程序或删除现有项目。
- 从扫描排除文件。例如，在 AppScan Source for Analysis 中，可通过在"资源管理器"视图中右键单击文件并选择**从扫描排除**来选择排除该文件。

• 有关递增分析的最新信息可在http://www.ibm.com/support/docview.wss?uid=swg21994390中找到。

注：

- 递增扫描之后，编辑器中的结果标记可能不再出现在正确的位置。
- 没有跟踪的已修复结果可能会出现在递增扫描结果中。
- 在递增分析期间不能同时具有多个 AppScan Source 产品或组件。此外，当您在扫描时，另一个用户无法同时在相同机器上扫描相同应用程序或项目。

从扫描中排除文件

开始之前

注：如果您的应用程序为 Eclipse 工作空间，那么无法从扫描排除文件。

过程

1. 在"资源管理器"视图中，选择要从扫描中消除的文件。
2. 右键单击所选内容，然后从菜单中选择**从扫描中排除**。

结果

打开包含了文件的项目的"属性"视图后，视图的**源**选项卡将列出项目中的文件，包括排除的文件。

项目文件在**源根目录**图标下列出。从扫描排除的文件具有红色文件图标（如果右键单击了排除的文件，那么其菜单中的**排除**被禁用，**包含**被启用。）要排除包含的文件，右键单击该文件并选择菜单中的**排除**。要包含排除的文件，右键单击该文件并选择菜单中的**包含**。

取消或停止扫描

虽然您可以取消进行中的扫描，但是取消扫描会导致丢失该扫描的所有数据。另外，可以停止扫描，并生成一个评估（其中包含到目前为止发现的结果）。

在 AppScan Source for Analysis 中取消或停止扫描

要取消当前正在进行的扫描，请从主菜单选择**扫描** > **取消扫描**或**扫描** > **停止扫描**。

取消扫描将终止扫描且不会生成任何结果。**停止扫描**将停止扫描并生成其中包含到目前为止发现的结果的评估。

在 AppScan Source for Development（Eclipse 插件）中停止扫描

但扫描正在进行时：

- 要取消扫描，请从主菜单选择**安全性分析** > **扫描** > **取消扫描**。扫描将终止且不会生成任何结果 - 取消诊断消息将出现在 Eclipse 中。
- 要停止扫描，请从主菜单选择**安全性分析** > **扫描** > **停止扫描**。扫描将终止，并会生成在发出停止操作以前收集到的结果的评估。

注：仅 Windows 和 Linux 上支持 AppScan Source for Development（Eclipse 插件）。

在 AppScan Source for Development（Microsoft Visual Studio 插件）中取消扫描

当扫描在运行时，从主菜单中选择 **IBM Security AppScan Source** > **扫描** > **取消扫描**。扫描将终止且不会生成任何结果。

注：仅 Windows 上支持 AppScan Source for Development Microsoft Visual Studio 插件。

Linux 上的 AppScan Source for Analysis 和 AppScan Source for Development（Eclipse 插件）必备组件

在 Linux 上，Eclipse 要求安装第三方组件才能呈现基于浏览器的内容。如果没有此组件，那么 AppScan Source for Analysis 和 AppScan Source for Development Eclipse 插件可能会显现诸如登录后挂起或在产品使用期间发生故障之类的症状。

关于此必备组件的信息可在 http://www.eclipse.org/swt/faq.php#browserwebkitgtk 获取。

- 『在 Linux 上使 AppScan Source for Analysis 支持基于浏览器的内容』
- 第 105 页的『在 Linux 上使安装到 Eclipse V3.7 或更高版本的 AppScan Source for Development 支持基于浏览器的内容』

在 Linux 上使 AppScan Source for Analysis 支持基于浏览器的内容

AppScan Source for Analysis 在 Eclipse 的基础上构建，因此受此问题的影响。

对此问题进行纠正的建议方法是确保安装 32 位或 i686 版本的 WebKitGTK 1.2.0 或更高。您应咨询系统管理员以了解安装软件包的正确方法，但在某些系统上，这可能只需简单地发出 `yum install webkitgtk.i686` 命令。

如果您无法安装 WebKitGTK，那么可以选择安装 32 位版本的 Mozilla XULRunner 1.8。对于此选项，您可能还需要对环境变量进行以下更新：

- 将 `MOZILLA_FIVE_HOME` 设置为 XULRunner 安装位置。
- 更新 `LD_LIBRARY_PATH` 以追加（或前置）`$MOZILLA_FIVE_HOME`。

在 Linux 上使安装到 Eclipse V3.7 或更高版本的 AppScan Source for Development 支持基于浏览器的内容

对此问题进行纠正的建议方法是确保安装 32 位或 i686 版本的 WebKitGTK 1.2.0 或更高。您应咨询系统管理员以了解安装软件包的正确方法，但在某些系统上，这可能只需简单地发出 `yum install webkitgtk.i686` 命令。

如果您无法安装 WebKitGTK，那么可以选择安装 32 位版本的 Mozilla XULRunner 1.8。对于此选项，您可能还需要对环境变量进行以下更新：

- 将 `MOZILLA_FIVE_HOME` 设置为 XULRunner 安装位置。
- 更新 `LD_LIBRARY_PATH` 以追加（或前置）`$MOZILLA_FIVE_HOME`。

管理"我的评估"

"我的评估"视图包含评估（当前打开的评估以及您已保存的任何评估）的列表。在此视图中，您可以打开、删除、保存、重命名或比较评估。扫描完整或您打开已保存的评估时，评估显示在"我的评估"视图中。"我的评估"显示打开或保存的评估的表，并标识已发布或修改的评估。从此视图除去评估（不进行保存或发布）将永久删除该评估。

有关"我的评估"视图的更多信息，请参阅第 256 页的『"我的评估"视图』。

限制：当扫描多个应用程序或项目时，将在"我的评估"视图中创建一个父节点（其中包含每个已扫描项的评估）。在此情况下，无法管理单独子评估（例如，无法单个地移除或发布子评估）。当同时扫描多个应用程序或项目时，您只能将评估作为组（父节点）来管理。

提示：您一次只能打开属于一个应用程序的扫描结果。要查看多应用程序或多项目扫描的结果，您必须展开"我的评估"视图中的树，然后双击要打开的评估。

将 AppScan Source 评估提交到云以进行分析

如果预订了 IBM Cloud Marketplace 上的 IBM Application Security on Cloud 或预订了 Application Security on Cloud for Bluemix，可在此处提交 AppScan Source 评估以进行分析。支持 AppScan Source V9.0 或更高版本的评估，可提交的扫描数取决于 Application Security on Cloud 预订。

关于此任务

当您使用 Application Security on Cloud 服务的 静态分析功能时，可生成使用 Intelligent Finding Analytics (IFA) 的安全分析报告。IFA 是一种功能强大的机器学习技术，通过过滤出假正并对可由一个代码点中的修订补救的结果分组来执行大多数分类工作。要了解关于 IFFA 的更多信息，请参阅此文章。

如果使用 AppScan Source V9.0 或更高版本而且具有 Application Security on Cloud 预订，那么可通过将 AppScan Source 评估上载到 Application Security on Cloud 来利用该技术。作为回报，您将接收到已通过该技术自动进行分类的新评估。该评估可以是 HTML 报告的形式，或者评估可在 AppScan Source 产品中打开。

如果具有 Application Security on Cloud 预订，那么每月可能具有有限的扫描次数。请参阅http://www.ibm.com/support/knowledgecenter/SSYJJF_1.0.0/ApplicationSecurityonCloud/src_managing_assessments_cloud.html以获取关于扫描和并发扫描权利的更多信息。

注：如果通过 Application Security on Cloud 的免费试用版本扫描 AppScan Source 评估，那么除了已通过 IFA 分类的 AppScan Source 评估文件之外，可下载完整 HTML 报告。对于所有其他扫描类型，仅可在具有免费试用时下载摘要报告。

过程

1. **如果已在使用 Application Security on Cloud for 静态分析，请跳过该步骤：**
   a. 如果没有 Application Security on Cloud 预订，可通过以下方法获取预订：
      - **IBM Cloud Marketplace：**转至 https://appscan.ibmcloud.com/serviceui/home 并通过 IBM 标识登录。如果没有 IBM 标识，那么使用链接来创建一个标识。然后，使用服务中提供的链接来注册免费使用版本或收费预订。
      - **IBM Bluemix®：**转至 https://console.ng.bluemix.net/ 并使用**注册**按钮并完成在 Bluemix 上注册的表单。然后创建 Application Security on Cloud for Bluemix 服务实例。
   b. **仅 IBM Cloud Marketplace：**在 Application Security on Cloud 服务中，创建应用程序（请参阅http://www.ibm.com/support/knowledgecenter/SSYJJF_1.0.0/ApplicationSecurityonCloud/ent_create_application.html），然后单击**创建扫描**。
   c. 在**您今天要扫描什么类型的应用程序？**屏幕中，选择**桌面**或 **Web** > **静态**。
   d. 如果先前未下载和设置 Static Analyzer Client Utility，请现在进行这些操作。请参阅http://www.ibm.com/support/knowledgecenter/SSYJJF_1.0.0/ApplicationSecurityonCloud/src_utility_install.html以了解更多信息。
2. 在 AppScan Source 产品或所选择的工具中生成评估（.ozasmt 文件）。支持 V9.0 或更高版本。
3. 使用 Client Utility 命令行界面 (CLI) 可生成 中间表示 (IRX 或 .irx) 文件来进行评估（.ozasmt 文件）：
   a. 将 Client Utility 解压缩到本地磁盘后，将 \bin 目录的位置添加到 PATH 环境变量。如果不执行操作，那么每次发出命令时，将使用 \bin 目录来限定所有 Client Utility CLI 命令。请参阅http://www.ibm.com/support/knowledgecenter/SSYJJF_1.0.0/ApplicationSecurityonCloud/src_irx_gen_cli.html以了解更多信息。
   b. 在 Windows 上发出以下命令：

      ```
      appscan package -d <save_path> -f <assessment_file> -n <file_name>
      ```

      或者在 Linux 上发出以下命令：

      ```
      appscan.sh package -d <save_path> -f <assessment_file> -n <file_name>
      ```

      命令参数是可选的：
      - -d：指定 -d <save_path>，其中 <save_path> 是用于保存 IRX 文件的目录。

- `-f`：指定 `-f <assessment_file>`，其中 `<assessment_file>` 是您希望打包以进行扫描的 `.ozasmt` 文件。如果 `<assessment_file>` 文件不在当前目录中，请使用此选项指定评估文件路径和文件名。

  注：仅当以下一个或两个语句都满足时，才需要该选项：

  – 您是从包含多个评估文件的目录发出的命令。如果该目录仅包含一个评估文件，那么未使用 `-f` 选项时将对该文件打包。

  – 您是从不包含评估文件的目录发出的命令。在此情况下，必须使用 `-f` 选项来指定要打包的评估文件的路径和文件名。

- `-n`：指定 `-n <file_name>`，其中 `<file_name>` 为 IRX 文件名。您可以指定带有或不带有 `.irx` 文件扩展名的文件名。如果指定不带有扩展名的文件名，生成文件时将自动添加扩展名。

关于 `package` 命令的其他信息（包括用法示例）可在 配置命令 (Windows) 或 配置命令 (Linux) 上找到。

4. 使用 CLI `queue_analysis` 命令来上载 IRX 文件

   a. 从 CLI 登录服务。执行该操作的方法在 IBM Cloud Marketplace 和 IBM Bluemix 上不同。有关在 CLI 中认证服务的详细信息可在认证命令 (Windows) 或认证命令 (Linux) 中找到。

   - **IBM Cloud Marketplace:**

     在 Windows 上发出以下命令：

     ```
     appscan scx_login -P <password> -u <user_name> -persist
     ```

     或者在 Linux 上发出以下命令：

     ```
     appscan.sh scx_login -P <password> -u <user_name> -persist
     ```

     需要以下参数：

     – `-P`：指定 `-P <password>`，其中 `<password>` 是注册 Application Security on Cloud 服务时指定的密码。

     – `-u`：指定 `-u <user_name>`，其中 `<user_name>` 是注册 Application Security on Cloud 服务时指定的电子邮件地址。

     该参数是可选的：

     – `-persist`：在登录令牌文件过期后自动尝试重新向服务认证。

   - **IBM Bluemix:**

     在 Windows 上发出以下命令：

     ```
     appscan login -P <password> -u <user_name> -persist
     ```

     或者在 Linux 上发出以下命令：

     ```
     appscan.sh login -P <password> -u <user_name> -persist
     ```

     需要以下参数：

     – `-P`：指定 `-P <password>`，其中 `<password>` 是服务凭证中指定的密码。

     – `-u`：指定 `-u <user_name>`，其中 `<user_name>` 是服务凭证中指定的绑定标识。

要确定 Bluemix 服务凭证，在服务仪表板左边导航窗格中选择**服务凭证**。请参阅启用外部应用程序以使用 Bluemix 服务。

该参数是可选的：

– `-persist`：在登录令牌文件过期后自动尝试重新向服务认证。

b. 使用 `queue_analysis` 命令上载 IRX 文件：

• 在 Windows 上发出以下命令：

```
appscan queue_analysis -a <app_id> -f <irx_file> -n <scan_name>
```

或者在 Linux 上发出以下命令：

```
appscan.sh queue_analysis -a <app_id> -f <irx_file> -n <scan_name>
```

需要以下参数：

– `-f`：指定 `-f <irx_file>`，其中 `<irx_file>` 是您希望提交以进行扫描的 IRX 文件。如果 IRX 文件不在当前目录中，请使用此选项指定 IRX 文件路径和文件名。

注：仅当以下一个或两个语句都满足时，才需要该选项：

- 您是从包含多个 IRX 文件的目录发出的命令。如果目录仅包含一个 IRX 文件，那么在未使用 `-f` 选项的情况下将提交此文件。
- 您是从不包含 IRX 文件的目录发出的命令。在此情况下，必须使用 `-f` 选项指定要提交的 IRX 文件的路径和文件名。

– `-n`：指定 `-n <scan_name>`，其中 `<scan_name>` 是云上将发生的扫描的名称。

– `-a`（**仅 IBM Cloud Marketplace：**）如果您已连接至位于 IBM Cloud Marketplace 的 Application Security on Cloud 服务，那么您提交到云的 IRX 文件必须与现有 Application Security on Cloud 应用程序关联。使用此选项，指定 `-a <app_id>`，其中 `<app_id>` 是要关联的应用程序的标识。要确定标识，请使用 `list_apps` 命令。

• 当 `queue_analysis` 命令完成时，将显示分析作业的标识。如果想要使用 CLI 来接收 Application Security on Cloud 分析报告，将需要在 `get_result` 命令中包含该作业标识，并记下该标识。如果使用 CLI 来接收分析报告，将可选择接收其中包含 `.ozasmt` 文件的归档 (`.zip`) 文件，以便分析报告可在 AppScan Source 中打开。如果只是对看到 HTML 报告感兴趣，可使用 CLI 或 Application Security on Cloud web 客户机来下载报告。

关于使用 `queue_analysis` 命令的报告可在分析命令 (Windows) 或分析命令 (Linux) 中找到。

5. 分析完成后，如果使用 CLI 上载了 IRX 或者如果在 Application Security on Cloud web 客户机中选择了**扫描完成后向我发送电子邮件**复选框，将接收到电子邮件。
6. 选择用于检索分析报告的方法。可使用 CLI `get_result` 命令，或者可使用 Application Security on Cloud web 客户机。如果使用 CLI 来接收分析报告，将可选择接收其中包含 `.ozasmt` 文件的归档 (`.zip`) 文件，以便分析报告可在 AppScan Source 中打开。如果只是对看到 HTML 报告感兴趣，可使用 CLI 或 Application Security on Cloud web 客户机来下载报告。
7. **如果想要使用 CLI `get_result` 命令来检索分析报告，完成该步骤：**

a. 确保您已从 CLI 登录到服务。

b. 在 Windows 上发出以下命令：

```
appscan get_result -d <file_path> -i <job_id> -t <type>
```

或者在 Linux 上发出以下命令：

```
appscan.sh get_result -d <file_path> -i <job_id> -t <type>
```

该参数是必需的：

- `-i`：指定 `-i <job_id>`，其中 `<job_id>` 是分析作业的标识。

注：如果在发出 `queue_analysis` 命令时未记下标识，可使用 `appscan list` 或 `appscan.sh list` 命令来查看所有分析作业的列表。请参阅分析命令 (Windows) 或分析命令 (Linux) 以获取更多信息。

以下参数是可选的：

- `-d`：指定 `-d <file_path>`，其中 `<file_path>` 是目标文件的标准路径和/或目标文件的文件名。如果未指定文件名，那么文件名将基于扫描作业名。如果未指定路径，那么文件将保存到当前目录。如果未包含该选项，那么文件将以基于扫描作业名的文件名保存到当前目录。
- `-t`：指定 `-t <type>`，其中 `<type>` 是 `html` 或 `zip`。结果将另存为 HTML 文件或包含 HTML 结果的 `.zip` 文件。如果未包含该选项，结果将另存为 HTML 文件。

  如果扫描结果是针对 `package` 命令所生成的 IRX 文件，那么指定 `-t zip` 会保存包含新 `.ozasmt` 文件的结果，该文件可以装入到 AppScan Source V9.0 或更高产品版本中。

关于使用 `get_result` 命令的报告可在结果命令 (Windows) 或结果命令 (Linux) 中找到。

8. **如果想要使用 web 客户机来检索分析报告，完成该步骤：**如果只是对看到 HTML 报告感兴趣，可使用 Application Security on Cloud web 客户机来下载报告。

   登录服务之后，应自动看到扫描的列表（如果已导航至服务的另一个部分，单击右上角的 **X** 图标以返回到扫描的列表）。在扫描列表中，找到扫描并选择**下载**图标，然后选择 XML 或 HTML 格式。

   要了解关于 IBM Cloud Marketplace 上的扫描结果的 Application Security on Cloud 更多信息，请参阅http://www.ibm.com/support/knowledgecenter/en/SSYJJF_1.0.0/ApplicationSecurityonCloud/appseccloud_results_dashboard_cm.html。在 IBM Bluemix 上，查看https://console.ng.bluemix.net/docs/services/ApplicationSecurityonCloud/appseccloud_results.html#results。

发布评估

AppScan Source 提供两种可选发布方式。您可以将评估发布到 AppScan Source 数据库以存储和共享评估。或者，如果您的 AppScan Enterprise Server 已与 Enterprise Console 选件一起安装，那么可以向该选件发布评估。AppScan Enterprise Console 提供各种用于处理评估的工具，例如报告功能、问题管理、趋势分析和仪表板。

要了解关于 AppScan Source 发布功能的更多信息，请参阅『将评估发布到 AppScan Source』 和第 112 页的『将评估发布到 AppScan Enterprise Console』。

注：对于 AppScan Source 和 AppScan Enterprise 的某些版本，两个产品的版本和发行版级别必须匹配才能从 AppScan Source 发布到 AppScan Enterprise Console。请参阅http://www.ibm.com/support/docview.wss?uid=swg21975211以了解 AppScan Source 和 AppScan Enterprise 的哪些版本在发布评估时是兼容的。

注册应用程序和项目以发布到 AppScan Source

您必须先注册为了创建评估而扫描的应用程序或项目，然后才能向 AppScan Source 数据库发布该评估。缺省情况下，如果您尝试发布未注册应用程序或项目的评估，那么将提示您在此时注册这些应用程序或项目。如果**常规**首选项**初始发布时自动注册应用程序**设置为**总是注册**，那么 AppScan Source for Analysis 会为您自动注册。

要点：您必须拥有**注册**许可权才能注册应用程序和项目。

要在扫描之前注册应用程序和项目，请在"资源管理器"视图中选择应用程序或项目，然后从主工作台菜单中选择**文件** > **注册**。如果右键单击"资源管理器"视图中的选定项目，**注册应用程序**和**注册项目**操作也可用。

如果应用程序已注册，那么您可以使用新名称再次对其进行注册。要执行此操作，请选择并右键单击应用程序，然后从菜单选择**将应用程序注册为**。在"重命名"对话框中，为已注册的应用程序或项目输入新名称。

要注销应用程序和项目，请在"资源管理器"视图中选择应用程序或项目，然后从主工作台菜单中选择**文件** > **注销**。在右键单击"资源管理器"视图中的选定项时，**注销应用程序**和**注销项目**操作也可用。

注：对项进行注销不会从 AppScan Source 数据库中除去任何已发布的数据。

将评估发布到 AppScan Source

您可以将评估发布到 AppScan Source 数据库以便存储和共享评估。

关于此任务

必须先向 AppScan Source 注册应用程序和项目，然后才能发布这些应用程序和项目的评估。请参阅『注册应用程序和项目以发布到 AppScan Source』以了解更多信息。缺省情况下，如果您尝试发布未注册应用程序或项目的评估，那么将提示您在此时注册这些应用程序或项目（这需要**注册**许可权）。

注：不能发布因扫描单独文件而创建的评估。

限制：当扫描多个应用程序或项目时，将在"我的评估"视图中创建一个父节点（其中包含每个已扫描项的评估）。在此情况下，无法管理单独子评估（例如，无法单个地移除或发布子评估）。当同时扫描多个应用程序或项目时，您只能将评估作为组（父节点）来管理。

过程

1. 要发布"分类"透视图中当前已打开的评估，请在主工作台菜单中选择**文件** > **将评估发布到AppScan Source**。

2. 要在"我的评估"视图中发布评估，请选择该评估，然后单击该视图的**将评估发布到 AppScan Source**按钮，或者右键单击该评估并选择**将评估发布到AppScan Source**。

结果

保存评估时，AppScan Source for Analysis 会将绝对路径写入评估文件以引用诸如源文件的项。这些绝对路径可能导致难以共享具有不同目录结构的另一台计算机上的文件。为了能够创建可移植评估文件，应创建一个变量（请参阅第 82 页的『定义变量』或第 117 页的『发布和保存时定义变量』）。

发布后，"我的评估"视图中列出的该评估在**已发布**列中立即生成一个图标。此外，该评估还将显示在"已发布的评估"视图中，该视图是发布到 AppScan Source 数据库的评估的过滤器驱动视图。可将此视图设置为仅显示匹配过滤条件的评估。例如，如果发布了 1,000 个评估，而您只希望查看您所发布的评估，那么可以创建将**按发布者**作为条件并将**当前用户**或您的用户名作为值的过滤器。

在"已发布的评估"视图中设置过滤器

过滤器可用于限制"已发布的评估"视图中显示的评估数量。

过程

1. 在"已发布的评估"视图中，单击工具栏上的**设置过滤器**按钮。
2. 选中所需过滤条件的一个或多个复选框：
   - **按应用程序**：选择要显示其评估的应用程序。如果指定的应用程序是评估的一部分，那么将显示为多个应用程序生成的评估。
   - **按发布程序**：设置要显示当前用户（或者指定要显示其已发布评估的用户）已发布评估的视图。
   - **按日期接近性**：按小时、天、周、月或年指定相对于当前日期的日期范围。可以选择**按日期接近性**或**按日期范围**，但不能同时选择这两个选项。
   - **按日期范围**：指定要在视图中显示评估日期的范围。可以选择**按日期接近性**或**按日期范围**，但不能同时选择这两个选项。
3. 单击**确定**以设置过滤器。

结果

应用过滤条件后，单击**刷新过滤器**以刷新自上次应用过滤器以来添加或除去评估的视图。单击**清除过滤器**以除去现有过滤器并显示所有评估。

从 AppScan Source 中删除已发布的评估

如果您已将某个评估发布到 AppScan Source，那么可使用"已发布的评估"视图中的操作将其移除。

过程

1. 在"已发布的评估"视图中，选择要删除的评估。还可以使用键盘 Ctrl 或 Shift 键来选择多个评估。
2. 在该视图的工具栏中选择**删除评估**按钮，或者右键单击所选项并从菜单中选择**删除评估**。

将评估发布到 AppScan Enterprise Console

如果您的 AppScan Enterprise Server 已与 Enterprise Console 选件一起安装，那么可以向该选件发布评估。Enterprise Console 提供各种用于处理评估的工具，例如报告功能、问题管理、趋势分析和仪表板。

关于此任务

您必须先在 AppScan Enterprise Console首选项页面中配置服务器设置，然后才能将评估发布到 Enterprise Console。有关设置首选项的信息，请参阅 第 79 页的『AppScan Enterprise Console 首选项』。

注：对于 AppScan Source 和 AppScan Enterprise 的某些版本，两个产品的版本和发行版级别必须匹配才能从 AppScan Source 发布到 AppScan Enterprise Console。请参阅http://www.ibm.com/support/docview.wss?uid=swg21975211以了解 AppScan Source 和 AppScan Enterprise 的哪些版本在发布评估时是兼容的。

限制：当扫描多个应用程序或项目时，将在"我的评估"视图中创建一个父节点（其中包含每个已扫描项的评估）。在此情况下，无法管理单独子评估（例如，无法单个地移除或发布子评估）。当同时扫描多个应用程序或项目时，您只能将评估作为组（父节点）来管理。

过程

1. 使用以下某种方法将一个或多个评估发布到 Enterprise Console：
   a. 在"我的评估"视图中选择一个或多个评估，然后单击**将评估发布到 AppScan Enterprise Console**。
   b. 在"我的评估"视图中右键单击该评估（或选择的一组评估），然后选择**将评估发布到 AppScan Enterprise Console**菜单项。
   c. 评估打开时，从主菜单中选择**文件** > **将评估发布到 AppScan Enterprise Console**。
2. 在"发布到 AppScan Enterprise Console"对话框中：
   a. 指定要与评估关联的 AppScan Enterprise Console 应用程序。当连接到 AppScan Enterprise Server V9.0.3 和更高版本时，这是必需的（除非禁用需求，如此处>所示）。当连接到 AppScan Enterprise Server 的较低版本时，关联应用程序是可选的。缺省情况下，如果连接到 AppScan Enterprise Server 的较低版本，应用程序将设置为指定用于发布的上一个应用程序。如果先前在发布时未指定任何应用程序，那么缺省情况下将不使用任何应用程序。要指定应用程序：
      1) 单击**应用程序**字段**选择**按钮。
      2) 将打开"选择应用程序"对话框，其中显示已存在于 AppScan Enterprise Console 中的所有应用程序。要在 AppScan Enterprise Console 中查看应用程序的属性，请单击该应用程序旁边的**查看概要信息**。
      3) 选择要与扫描关联的应用程序，或者通过单击**新建应用程序**来为此目的创建新应用程序。单击此链接将打开 AppScan Enterprise Console 并允许您创建新应用程序。一旦保存了新应用程序的属性，"选择应用程序"对话框便将自动刷新以包含该应用程序供选择（如果它未自动包含新应用程序，请单击**刷新**）。

提示：在"选择应用程序"对话框中，可以使用过滤器字段来缩短应用程序的列表。当您输入时，过滤器会自动应用于应用程序的列表。星号 (*) 和问号 (?) 字符可用作通配符。星号与任意一组的零个或更多字符匹配，而问号与任意单个字符匹配。

4) 选择了应用程序后，单击**确定**。

b. 必需： 在**名称**字段中，指定评估将在 AppScan Enterprise Console 中另存为的名称。

c. 可选： **当连接到 V9.0.3 之前的 AppScan Enterprise Server 版本时：**使用**文件夹**字段来设置要发布到的位置。缺省情况下，该位置设置为上次用于发布的位置。如果先前未发布任何评估，那么将选择缺省AppScan Enterprise Console文件夹（注意：这是在 AppScan Enterprise Console首选项页面中指定的用户标识的缺省文件夹）。要选择发布到其他文件夹，请单击**文件夹**字段**选择**按钮，然后选择所需的文件夹（仅您有权向其发布内容的文件夹才可用）。如果要向其发布内容的文件夹不可用，请单击**刷新**以使用已在服务器上做出的任何更改来更新文件夹树。

3. 单击**发布**。

结果

保存评估时，AppScan Source for Analysis 会将绝对路径写入评估文件以引用诸如源文件的项。这些绝对路径可能导致难以共享具有不同目录结构的另一台计算机上的文件。为了能够创建可移植评估文件，应创建一个变量（请参阅第 82 页的『定义变量』或第 117 页的『发布和保存时定义变量』）。

发布此评估后，将在参考消息中提供指向 AppScan Enterprise (Enterprise Console) 的链接。单击该链接将在缺省外部 Web 浏览器中打开门户网站页面。

提示：如果发布失败，请检查 Enterprise Console 服务器是否在运行，以及您是否能够在浏览器中访问其控制中心 URL（使用您已在 AppScan Enterprise Console 首选项页面中指定的同一 **Enterprise Console URL**）。

注：

- 大型评估可能需要更长时间才能显示在门户网站中。如果发布后收到错误消息，而门户网站上没有出现报告，那么请与管理员核实。
- 任何发布与当前正在由 Enterprise Console 所处理评估同名的评估的尝试都将失败。此外，如果在处理了第一个评估后发布与该评估同名的评估，那么第二个评估将覆盖第一个评估（如果已提前将 Enterprise Console 配置为提供同名报告的趋势分析，那么它便能够执行此操作）。要确定对评估的处理是否已完成，请在浏览器中访问 Enterprise Console 控制中心，然后浏览至相应的用户文件夹并检查报告的状态。
- AppScan Source 不支持向已配置为使用代理设置的 Enterprise Console 实例进行发布。尝试向使用代理设置的实例进行发布将导致错误。

要点：

升级到 AppScan Source V9.0.3.4 时，将注意到以下更改：

- 在将评估发布到 AppScan Enterprise Console 时，现在必须将评估与 AppScan Enterprise 中的应用程序关联（如果您正在运行 AppScan Enterprise Server V9.0.3 和更高版本）。因此，如果自动化脚本不包含应用程序关联，那么它们可能失败。

在 AppScan Enterprise Server 中，如果想要利用 AppScan Enterprise Server 应用程序安全性风险管理功能，那么需要应用程序关联。请参阅http://www.ibm.com/support/knowledgecenter/SSW2NF_9.0.3/com.ibm.ase.help.doc/topics/c_overview.html。

- 此外，必须从 AppScan Enterprise URL 除去端口。
  1. 在 AppScan Source for Analysis 中，单击**编辑** > **首选项**。
  2. 在 AppScan Enterprise Console 设置中，从 **Enterprise Console URL** 字段除去端口。
- 发布评估之后，它仅可在 AppScan Enterprise"监视器"视图中可用（在先前发行版中，评估可在 AppScan Enterprise"扫描"视图中可用）。http://www.ibm.com/support/knowledgecenter/SSW2NF_9.0.3/com.ibm.ase.help.doc/topics/t_workflow_for_applications.html中描述了如何迁移到该视图。

这是使用通用访问卡 (CAC) 认证时 AppScan Source 与发布到 AppScan Enterprise Server 所需的 AppScan Enterprise Server 之间的已更改通信协议的结果。

如果不想在启用了 CAC 认证时将评估发布到 AppScan Enterprise Server，或者如果不想利用 Enterprise Server 应用程序安全性风险管理功能，可还原至先前的通信协议，如下所示：

1. 打开 <data_dir>\config\ounce.ozsettings（其中 <data_dir> 是 AppScan Source 程序数据的位置，如第 275 页的『安装和用户数据文件位置』中所述）。
2. 在此文件中，找到以下设置：

```
<Setting
  name="force_ase902_assessment_publish"
  value="false"
  default_value="false"
  description="Use ASE 9.0.2-style assessment publish"
  display_name="Use ASE 9.0.2-style assessment publish"
  type="boolean"
  read_only="true"
  hidden="true"
/>
```

3. 在此设置中，将 value="false" 更改为 value="true"，然后保存文件。
4. 重新启动将从其中发布评估的 AppScan Source 产品。

当该设置设置为 value="true" 时：

- 如果在发布时将评估与 AppScan Enterprise 中的应用程序关联，那么评估将在"监视器"和"扫描"视图中可用。
- 如果在发布时不将评估与应用程序关联，评估将在"扫描"视图中可用。
- 启用 CAC 认证后您将无法将评估发布到 AppScan Enterprise Server。

有关更多信息，请参阅http://www.ibm.com/support/docview.wss?uid=swg21993010。

AppScan Enterprise Console 首选项

如果 AppScan Enterprise Server 已与 AppScan Enterprise Console 选件一起安装，那么您可以向其发布评估。Enterprise Console 提供各种用于处理评估的工具，例如报告功能、问题管理、趋势分析和仪表板。

要启用此功能部件，请填写 AppScan Enterprise Console 首选项页面。在启用 Enterprise Console 发布功能之前，必须使用有效输入内容来填写此页面中的所有字段：

- **用户标识**字段：输入 AppScan Enterprise Server 用户标识（已创建用于代表您的 AppScan Source 用户进行发布的用户标识）。
  - 如果 AppScan Enterprise Server 配置为使用 Windows 认证，请输入用于连接到 Enterprise Console 的域和用户名（以 \ 分隔域和用户名，例如 my_domain\my_username）。
  - 如果 AppScan Enterprise Server 已配置 LDAP，请输入用于连接到 Enterprise Console 的用户名。
  - 在 Windows 上，如果支持 AppScan Enterprise Server 进行通用访问卡 (CAC) 认证，从列表选择 CAC 通用名。

  至少您必须是 QuickScan 用户。如果您连接到版本低于 V9.0.3 的 AppScan Enterprise Server，必须在 Enterprise Server 有您自己的用户文件夹。
- **密码**字段：仅当 AppScan Enterprise Server 认证方法为用户标识和密码时，该字段才可用。输入用于登录到Enterprise Console的密码（已输入的用户名的密码）。
- **Enterprise Console URL** 字段：输入用于访问 Enterprise Console Web 应用程序的 URL。

  此 URL 的格式为：

  ```
  http(s)://<hostname>:<port>/ase
  ```

  其中 <hostname> 是安装 Enterprise Console的机器的名称，<port> 是运行此控制台的端口（缺省值 <port> 为 9443）。该 URL 的示例为 https://myhost.mydomain.ibm.com:9443/ase。

  注：
  - 如果已设置 **Enterprise Console URL**，那么无需修改此字段。
  - 您必须通过**管理 AppScan Enterprise 设置**许可权登录到 AppScan Source 才能设置 **Enterprise Console URL** 字段。关于用户帐户和许可权的信息，请参阅产品信息中心的管理部分，或《*IBM Security AppScan Source* 安装和管理指南》的"管理 *AppScan Source*"一节。
  - **用户标识**和**密码**存储在运行 AppScan Source 客户机（例如 AppScan Source for Analysis）的机器上，而 **Enterprise Console URL** 则存储在 Enterprise Server（可能位于远程机器上）中。您无法从远程机器访问用户名和密码信息（例如，通过从远程机器发出 getaseinfo 命令）。
  - AppScan Source 不支持向已配置为使用代理设置的 AppScan Enterprise Console实例进行发布。尝试向使用代理设置的实例进行发布将导致错误。

完成设置后，强烈建议您通过单击**测试连接**来确保与 Enterprise Console 服务器的连接有效。

提示：如果连接测试失败，请检查 Enterprise Console 服务器是否在运行，以及您是否能够在浏览器中访问其控制中心 URL（使用以上已指定的同一 **Enterprise Console URL**）。

保存评估

开始之前

要点：要保存评估，您必须拥有**保存评估**许可权。要了解关于设置许可权的信息，请参阅《*IBM Security AppScan Source* 安装和管理指南》。

关于此任务

评估可以保存在本地，然后随时再次打开。缺省情况下，评估将以 .ozasmt 文件扩展名保存到操作系统主目录（例如，在 Windows 上，该目录可能是 C:\Documents and Settings\Administrator\）。

过程

1. 要保存"分类"透视图中当前打开的评估，请选择主工作台菜单中的**文件** > **保存评估**或**文件** > **将评估另存为**。选择**将评估另存为**操作允许您指定所保存的评估的位置和文件名。
2. 要保存"我的评估"视图中的评估，请选择该评估并单击该视图的**保存评估**或**将评估另存为**按钮，或者右键单击该评估并选择**保存评估**或**将评估另存为**。

结果

保存评估时，AppScan Source for Analysis 会将绝对路径写入评估文件以引用诸如源文件的项。这些绝对路径可能导致难以共享具有不同目录结构的另一台计算机上的文件。为了能够创建可移植评估文件，应创建一个变量（请参阅第 82 页的『定义变量』或第 117 页的『发布和保存时定义变量』）。

自动保存评估

缺省情况下，扫描会自动保存到 <data_dir>\scans（其中 <data_dir> 是 AppScan Source 程序数据的位置，如第 275 页的『安装和用户数据文件位置』中所述） 中三天时间。此行为由 <data_dir>\config\scanner.ozsettings 中的 assessment_auto_save、assessment_auto_save_location 和 assessment_auto_save_stale_period 设置来确定。

- 如果 assessment_auto_save 设置设为 true，那么评估在完成时会自动保存（您必须拥有**保存评估**许可权）。
- assessment_auto_save_location 设置用来确定将评估存储到的位置。缺省情况下，评估会存储到 <data_dir>\scans。要更改此位置，请将 value 属性设置为您所选的目录。例如，要将此位置设置为 C:\myFolder，请将该属性设置为 value="C:\myFolder"。
- assessment_auto_save_stale_period 设置用来确定评估将在 assessment_auto_save_location 中保存的天数。您可以通过 value 属性来更改此设置。例如，如果该属性设置为 value="10"，那么将在 10 天后从 assessment_auto_save_location 中移除已保存的评估。

从"我的评估"中移除评估

从"我的评估"视图中移除评估时，不会从本地文件系统中移除这些评估。如果从该视图中移除了某个评估，还可以通过**打开评估**操作来重新添加此评估。

关于此任务

限制：当扫描多个应用程序或项目时，将在"我的评估"视图中创建一个父节点（其中包含每个已扫描项的评估）。在此情况下，无法管理单独子评估（例如，无法单个地移除或发布子评估）。当同时扫描多个应用程序或项目时，您只能将评估作为组（父节点）来管理。

过程

1. 在"我的评估"视图中，选择要移除的评估。还可以使用键盘 Ctrl 或 Shift 键来选择多个评估。
2. 在该视图的工具栏中选择**从我的评估中移除**按钮，或者右键单击所选项并从菜单中选择**从我的评估中移除**。

定义变量

保存评估或束，或者发布评估时，AppScan Source for Analysis 可能建议您创建变量来替换绝对路径（如果没有变量，AppScan Source for Analysis 会将绝对路径写入评估文件以引用诸如源文件之类的项）。为绝对路径配置变量时，可便于在多台计算机上共享评估。建议在共享评估时使用变量。

关于此任务

可以在发出保存或发布操作之前遵循本主题中的指示信息创建变量，也可以在发出保存或发布操作之后遵循『发布和保存时定义变量』中的步骤创建变量。

要通过示例了解变量如何帮助共享评估，请参阅第 118 页的『示例：定义变量』。

过程

1. 从主菜单中选择**编辑** > **首选项**。在"首选项"对话框中，选择**更改变量**。
2. 单击"更改变量"首选项页面上的**添加变量**按钮。
3. 输入变量的名称并浏览至将由变量替换的文件位置（创建变量后，AppScan Source for Analysis 将在两端插入百分比符号 (%)）。
4. 对评估中的任何其他引用项重复上述步骤（例如，如果评估引用了多个位置中的源，请为每个位置添加一个变量）。
5. 使用首选项页面上的**修改变量**和**删除变量**按钮来编辑和除去变量。
6. 完成对变量的定义后，单击**确定**。

发布和保存时定义变量

尝试保存或发布评估时，AppScan Source for Analysis 将检测该评估中的任何绝对路径。如果还没有为绝对路径创建对应变量，将提示您创建这些变量。

关于此任务

可以在发出保存或发布操作之前遵循第 82 页的『定义变量』中的指示信息创建变量，也可以在发出保存或发布操作之后遵循本主题中的步骤创建变量。

要通过示例了解变量如何帮助共享评估，请参阅第 118 页的『示例：定义变量』。

过程

1. 发出保存或发布操作之后，在"检测到绝对路径"消息中单击**是**。
2. 在"定义变量"对话框中，AppScan Source for Analysis 建议包含该数据的一组路径。
3. 选择一个目录，然后单击**添加变量**。
4. 对评估中的任何其他引用项重复上述步骤（例如，如果评估引用了多个位置中的源，请为每个位置添加一个变量）。
5. "定义变量"对话框也可用于通过使用**修改变量**和**删除变量**按钮来编辑和除去变量。
6. 单击**确定**以完成保存或发布操作。

示例：定义变量

要共享评估数据，您必须定义相应变量。本主题中的示例说明对变量的需求。

用户 Joe 在计算机 A 上扫描，其中所有源代码存在于目录 C:\dev\my_code 下。Joe 希望将其扫描结果保存到文件并将其与 Bill 共享。Bill 使用计算机 B 且在目录 C:\code\bills_code 下具有 Joe 扫描的相同代码。无需变量，评估文件将引用具有以 C:\dev\my_code 开头的绝对路径的所有源文件。如果 Bill 在计算机 B 上打开此评估文件，那么 AppScan Source for Analysis 无法找到源文件，因为它们存在于计算机 B 上的 C:\code\bills_code 下。

解决方案

Joe 和 Bill 应该创建指向源代码根的变量。Joe 在 AppScan Source for Analysis 中创建一个名为 SRC_ROOT 的变量，并向其赋值 C:\dev\my_code。此变量对于 Joe 的 AppScan Source for Analysis 安装版为本地变量。然后，Joe 告知 Bill 变量名称 (SRC_ROOT) 及其指向的位置。Bill 随后在其 AppScan Source for Analysis 中创建名为 SRC_ROOT 且值为 C:\code\bills_code 的变量。 Joe 保存其扫描时，变量 SRC_ROOT 替换路径 C:\dev\my_code。Bill 打开从 Joe 处收到的评估文件时，C:\code\bills_code 替换 SRC_ROOT 变量。

第 5 章 筛选和分析

通过对相似发现结果进行分组，安全分析人员或 IT 审计员可以对源代码问题进行分段和分类。此部分说明如何将 AppScan Source 评估分类和对结果进行分析。

扫描代码时，将出现扫描结果或结果。筛选是评估结果并确定如何解决其问题的过程。但是，达到此目标所需的步骤取决于多个因素，包括发现结果的总数、特定安全注意事项、应用程序风险评估等。除了决定某个发现结果是否代表有效的安全问题之外，筛选还涉及在适当情况下修改发现结果的属性（严重性、类型和分类）。

分类策略对于确保您按照所需顺序并在所需时间段内完成目标非常重要。分类在迭代方式下完成效果最好，在此方式下，您对发现结果的子集进行评估，并确定每个子集在每个迭代中的处理。确定如何定义筛选迭代的有效方法很多。一种方法是根据总体严重性创建高风险发现结果的子集。您可以首先解决潜在风险最大的发现结果，然后逐渐处理到可能风险最低的发现结果。另一种方法是根据安全问题来定义子集，如"SQL 注入"或"需要验证"。

一般来说，由安全分析员或 IT 审计员执行筛选。分析人员或审计员可将需要代码更改的发现结果提交至缺陷跟踪系统，然后提交给开发者进行补救。在其他情况下，开发人员可能执行筛选并解决问题。

在筛选阶段，您可以：

- 复审特别重要漏洞类型的结果
- 查看特定类别中的 API
- 比较不同评估中的结果
- 过滤或排除特定结果
- 更改结果的严重性或漏洞类型
- 将可疑和扫描覆盖范围结果升级为明确结果
- 对结果进行注释
- 将缺陷提交至缺陷跟踪系统，或将结果用电子邮件发送给其他人。

AppScan Source 提供了通过使用各种分类策略来分析结果时所需的所有工具。通过过滤的方法，可以仅查看特定筛选迭代中将处理的结果。如果您的迭代策略是以严重性和分类为依据，那么可从"漏洞矩阵"视图中过滤发现结果。如果您的迭代策略是以漏洞类型为依据，那么可从"评估摘要"视图进行过滤。 AppScan Source for Analysis 还提供过滤器编辑器来支持复杂迭代方法。

一旦选择了分类方法，AppScan Source for Analysis 便支持对结果进行处理。

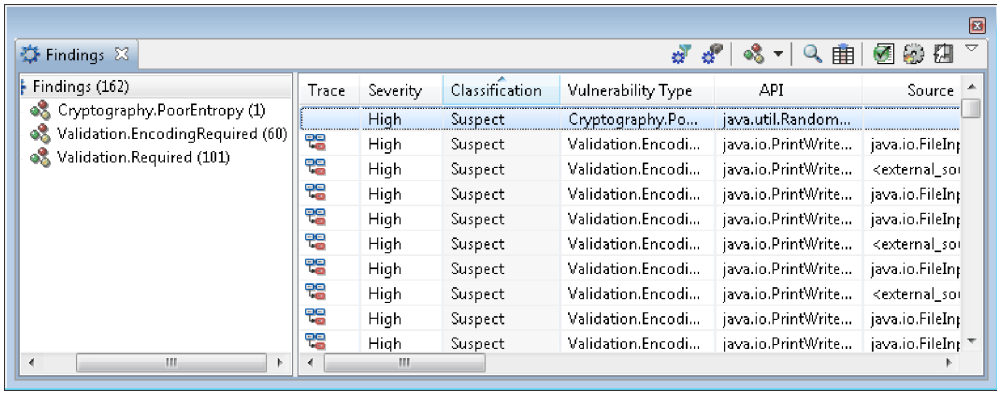
- 排除个别结果或结果集合
- 修改结果详细信息（类型、严重性和分类）
- 创建束（针对结果的分组机制）
- 通过"评估差异"视图对评估进行比较

© Copyright IBM Corp. 2003, 2017

显示结果

"发现结果"视图或包含发现结果的任何视图都将针对每个扫描显示一个发现结果树（评估条件的分层分组）和一个结果表。发现结果树中选择的项确定了表中将出现的发现结果。

选择树的根会导致所有发现结果都显示在表中，而选择分组类型会导致仅显示这些类型的发现结果。



AppScan Source for Analysis 按不同分组显示结果，这些分组包括：

- **漏洞类型**
- **分类**
- **文件**
- **源**
- **接收器**
- **API**
- **束**
- **CWE**
- **表**

注：缺省情况下，以降序对分类和严重性进行排序。所有其他列都以升序进行排序。

以下列将出现在结果表中。

表 *11.* 结果表

列标题	描述
跟踪	此列中的图标指示丢失或已知的接收器存在跟踪。

表 *11.* 结果表 *(续)*

列标题	描述
严重性	• 高：对数据的机密性、完整性或可用性和/或处理资源的完整性或可用性具有风险。高严重性情况应该优先予以立即修复。 • 中：对数据安全性和资源完整性具有风险，但是此情况较不容易受到攻击的影响。中严重性情况应该予以复审，并在可能之处予以修复。 • 低：对数据安全性或资源完整性具有极低的风险。 • 参考：结果本身不易受到威胁的影响。更确切而言，它描述代码中使用的技术、体系结构特征或安全性机制。
分类	结果的类型：**明确**或**可疑**安全性结果，或者**扫描覆盖范围**结果。 **注：**某些情况下，**无**分类可用于表示某个分类既不是安全性结果也不是扫描覆盖范围结果。
漏洞类型	漏洞类别，如 `Validation.Required` 或 `Injection.SQL`。
API	易受攻击的调用，显示 API 及向其传递的参数。
源	源是对程序的输入，如文件、servlet 请求、控制台输入或套接字。对于大多数输入源，返回的数据在内容和长度方面没有限制。在未检查某个输入的情况下，会将其视为已感染。
接收器	接收器可以是可将数据写出到的任何外部格式。接收器示例包括数据库、文件、控制台输出和套接字。数据未经检查就写入接收器可能预示着严重的安全漏洞。
目录	已扫描文件的完整路径。
文件	其中出现安全性结果或扫描覆盖范围结果的代码文件的名称。结果中的文件路径与已扫描的项目工作目录相关。
调用方法	从中进行易受攻击调用的函数（或方法）。
行	代码文件中的包含易受攻击 API 的行号。
束	包含此结果的束。
CWE	由社区编写的常见软件弱点字典的标识和主题（Common Weakness Enumeration (CWE) 主题）。

注：如果选择了 AppScan Source 无法找到其源的结果，将通过对话框提示您在无法找到源文件时是否希望收到提示。如果选择**是**，那么每次选择无法找到其源的结果时都将收到提示。如果选择**否**，将不会收到提示。只要当前评估处于打开状态，该设置就将持续存在。每次重新打开评估时或者您退出 AppScan Source 都将重新设置该设置。

AppScan Source 分类过程

分类过程包括通过束、过滤器和排除来处理发现结果，以及对评估结果进行比较。

过滤器

过滤器是定义具有某些特征的结果的一组规则。使用过滤器，可呈现发现内容的动态视图，并可对相似结果进行筛选。

过滤器为共享过滤器或本地过滤器：

- 共享过滤器驻留在 AppScan 服务器上。连接到该服务器的任何用户都可使用该过滤器。
- 本地过滤器位于本地计算机上。

束

束是通过应用程序进行存储的各个发现结果的命名集合。要创建束，只需选择发现结果并将其添加到新束或现有束。

通过将相似结果分组到束，安全分析员可以对源代码问题进行筛选。可将束提交到缺陷跟踪系统，或通过电子邮件将发现结果发送给开发者以在分类和分析过程中进行复审。

排除内容

排除可从扫描中除去结果。 AppScan Source 具有内置的**已排除的束**，其中包含您所排除的任何发现结果（例如，因为它们不需要解决）。

注：从评估结果中排除的发现结果不参与应用程序或项目度量的计算。

已修改的结果

已修改的结果是其漏洞类型、严重性或分类发生更改的结果。如果向结果添加说明，那么结果也被视作已修改。

比较评估

评估是在 AppScan Source for Analysis 中使用**差异评估**操作进行比较的。比较两个评估时，两者之间的差异将显示在"评估差异"视图中（这类似于"我的评估"视图和"发现结果"视图的组合）。

注：比较评估时，将忽略过滤器和束。

样本筛选

此示例描述了安全分析人员所使用的 AppScan Source 分类工作流程。筛选工作流程可能因您的业务需求而有所不同。

Jones 先生是公司的安全分析人员，他希望对自己的扫描结果进行分类。他希望对相似发现结果进行分组并划分优先级，然后将其提交至相应开发者以加以解决。

首先，Jones 先生扫描自己的应用程序的源代码，然后在"分类"透视图中打开评估。扫描产生约 2,000 条结果，均可在"结果"视图中复审。然而，Jones 先生希望首先大致浏览结果，然后打开"漏洞矩阵"视图，其中按严重性和发现项类型（安全性或扫描覆盖范围）显示划分图。扫描覆盖范围发现项和可疑安全性发现项需要进一步调查以确认其风险。

在"脆弱性矩阵"中，Jones 先生看到八个高严重性的明确安全性发现项。他单击指示八个明确发现项的矩阵框，从而自动创建一个过滤器，并且导致"发现项"视图也刷新以仅显示这八个关键问题。Jones 先生决定将这些问题视作错误。他选择了这八项，提交到缺陷跟踪系统。他随后从"漏洞矩阵"复位了其过滤器。

Jones 先生然后关注"评估摘要"视图。他注意到，这 2,000 个发现结果包含六个以上的脆弱性类型。他决定重点关注验证问题，并从"评估摘要"视图创建了另一个过滤器。他在图形上单击 Validation.EncodingRequired 和 Validation.Required，将"结果"视图中的结果数减少到约 500 个。

五百个结果仍然很难进行筛选。Jones 先生决定进一步过滤结果。在"过滤器编辑器"视图中，他通过对高严重性的需求增强了从"评估摘要"中创建的过滤器。发现结果表现在显示 150 个条目。

按文件名进行排序时，他发现有些发现结果位于第三方库中的代码。Jones 先生知道此库的使用是孤立的，因此不打算处理其安全问题。他排除了这些发现结果，从而使"发现结果"视图和度量立即更新。将来的扫描将检测到这些结果，但这些项目已隔离，将不再计入度量。

Jones 先生发现类型为 Validation.Required 的几个高严重性可疑安全性发现项。他知道该数据在未经验证的情况下便被使用。因此他决定将这些结果从可疑提升为明确。进行此修改时，他决定添加说明以解释自己的更改，然后将这些发现结果通过电子邮件发送给自己，以提醒自己优先对其进行补救或在"已修改的发现结果"视图中对其进行复审。

接下来，Jones 先生再次按文件名进行排序，并注意到有些发现结果位于后端服务器中，而有些位于用户界面中。他选择了所有后端发现结果，并创建一个标签为 Backend Server - Validation Required 的新束。他随后选择余下的结果并置于标签为 UI - Validation Required 的束中。继续筛选，重点集中于具有高严重性的 Validation.EncodingRequired 类型。

一天下来，Jones 先生创建了十二个束。这一天中，他使用了图形、过滤器和脆弱性矩阵来将这些发现结果减少到视图中一次可管理的数量。有时他将这些个别结果放在束中。有时排除不重要的结果。他还不时针对特定发现结果创建新束；有时他向现有束添加发现结果。

现在 Jones 先生复审这十二个束。他决定应该将 Backend Server - Validation Required 和 UI - Validation Required 束提交到自己的缺陷跟踪系统，以通知开发者这些需要关注的区域。

Jones 转至"束"视图，打开了 Backend Server - Validation Required 束。此时将打开名为 **Backend Server - Validation Required** 的新视图，其中包含他放置在该束中的发现结果的列表。然后，他将此束提交到缺陷跟踪系统。当晚稍后，当开发者登录到 Rational ClearQuest 并看到分配给自己的错误时，便可在 AppScan Source for Development 中打开结果。

Jones 复审其他束。他将某些束提交到缺陷跟踪系统，并通过电子邮件将其他束发送给他的同事。不过，有些束包含进一步复审后对他来说不太重要的结果。他将这些不太重要的结果移动到两个新的束：By Design 和 Irrelevant。Jones 先生确定这些发现结果是可接受的，因而不打算更改其代码。除 By Design 和 Irrelevant 结果外，Jones 先生还发现所有 Cryptography.PoorEntropy 结果对其也不重要。他知道这些密码术调用的平均信息量可能不足，并且尽管速度比较快的计算机可以在不到一周的时间内破解密钥，但这对于应用程序来说并不重要，因为其中数据在加密数小时后便不再有用。因此，Jones 先生希望也将其除去。

然后，他将 By Design 和 Irrelevant 束添加到"属性"视图的**已排除的束**列表中。他还打开了"过滤器编辑器"，通过脆弱性类型 Cryptography.PoorEntropy 创建了另一个过滤器，保存了名为 Crypto 的过滤器，并将 Crypto 过滤器的行为设置为**反向**（在"选择过滤器"对话框中，他选择了**反向过滤器**）。之后，他启动扫描并来到主页。只有在下次扫描之后，度量才会反映这些排除。

通过过滤器筛选

AppScan Source for Analysis 针对所有潜在安全性漏洞进行报告，并可能为中到大型代码库生成成千上万个结果。扫描时，您可能觉得结果列表中包含对您不重要的项。要从"结果"视图除去某些结果，可以选择预定义的过滤器，或者创建您自己的过滤器。过滤器可指定用于决定要从视图中除去哪些结果的条件。

- 『过滤器概述』
- 第 125 页的『过滤规则』
- 第 127 页的『过滤器示例』

过滤器概述

过滤器除去或限制满足过滤规则确定的条件的项，并有助于您在类选或报告期间管理扫描结果。过滤器可帮助您引导工作流程，并将安全分析员重点分配到结果子集的最关键区域。例如，在代码检测期间，分析员可以创建过滤器以避免查看低严重性结果。此外，分析人员还可能首选排除系统库 include 文件中的漏洞。过滤器可从视图中除去这些项，也可排除个别文件或先前调查过的文件。

可在扫描之前或之后应用过滤器：

- 要在扫描之前应用过滤器，在项目或应用程序属性中设置全局过滤器，或通过包含过滤器的扫描配置进行扫描。在扫描之前应用过滤器时，无法显示未过滤的结果或在不再次进行扫描的情况下除去过滤器。
- 各种视图（特别是"过滤器编辑器"视图）使您能在扫描之后应用过滤器。当这些视图用于过滤时，所有已过滤项都保留在扫描结果中，但仅会在选择了**显示已过滤的结果**（ ）切换按钮后出现在"结果"视图中。

AppScan Source 包含多个可选择用于过滤扫描结果的预定义过滤器。

选择过滤器后，可对属性进行设置以将过滤器设置为排除。排除将影响扫描，除去与过滤器匹配的所有结果，或者不与过滤器匹配的所有结果。

过滤规则

每个过滤器都包含用于定义要在结果表的结果中限制（包含）或除去（排除）哪些发现结果的规则（对于跟踪规则，您可以根据跟踪属性对其加以限制或除去）。

- **限制为**规则（包含规则）将排除不包含指定条件的发现结果，并从结果表的可视结果中除去这些发现结果。
- **除去**规则（排除规则）除去扫描结果中包含条件的结果。除去规则将除去包含指定条件的所有结果，并从可视结果中将其除去。

过滤规则可能包括以下特征：

- **严重性**：标识个别结果的潜在影响或风险。严重性规则仅为限制。
  - 高：对数据的机密性、完整性或可用性和/或处理资源的完整性或可用性具有风险。高严重性情况应该优先予以立即修复。
  - 中：对数据安全性和资源完整性具有风险，但是此情况较不容易受到攻击的影响。中严重性情况应该予以复审，并在可能之处予以修复。
  - 低：对数据安全性或资源完整性具有极低的风险。
  - 参考：结果本身不易受到威胁的影响。更确切而言，它描述代码中使用的技术、体系结构特征或安全性机制。
- **分类**：根据本主题中描述的分类过滤结果。分类规则仅为限制。
- **漏洞类型**：按特定漏洞类别（如 BufferOverflow）进行过滤。当添加漏洞类型时，可以从所有可能的漏洞类型中进行选择，或者可以仅从已在当前评估中找到的那些类型中进行选择。要从已在当前评估中找到的漏洞类型中进行选择，请在"选择值"对话框中选择**仅显示已打开评估中的值**。

  在为将来的扫描创建过滤器时，从所有可能的漏洞类型中进行选择很有用。要显示所有漏洞类型，请取消选中**仅显示已打开评估中的值**（如果没有任何已打开的评估，那么缺省情况下会显示所有漏洞类型，并且**仅显示已打开评估中的值**复选框不可用）。
- **API**：对特定 API 的所有漏洞进行过滤。
- **文件**：对特定文件中的所有漏洞进行过滤。
- **目录**：对特定目录中的所有漏洞进行过滤。
- **项目**：对特定项目中的所有漏洞进行过滤。
- **跟踪**：允许您基于跟踪属性来过滤结果（请参阅第 161 页的『源和接收器』以了解有关跟踪属性的更多信息）。过滤器可包含根据跟踪属性同时进行限制和除去操作的跟踪规则。在任一部分（限制或除去）中单击**添加**时，将打开"跟踪规则条目"对话框。在该对话框中，可指定：
  - **源**：在"源"部分的 **API 正则表达式**字段中，指定跟踪源或涵盖多个源的正则表达式（缺省条目是 .* - 此正则表达式或通配符将返回全部内容）。如果要使用正则表达式，请在**正则表达式类型**字段菜单中选择类型（缺省正则表达式类型是 **PERL**）。如果不使用正则表达式，请在**正则表达式类型**字段菜单中选择**完全匹配**。

    如果 **API 正则表达式**条目是有效的表达式，那么字段旁将显示一个绿色勾选图标。如果该条目不是有效的表达式，那么字段旁将显示红色的 X 图标，且将禁用对话框的**确定**按钮。将光标悬停在这两个图标的任意一个上均会看到有关验证结果的更多信息。如果已创建的条目不是有效的表达式，但仍希望继续使用

它，请选中对话框底部的**忽略以上验证错误**复选框。此操作将启用对话框的**确定**按钮（只要表达式不为空），并且无效表达式旁的图标将更改为带有**验证已禁用**悬浮文本的绿色勾选符号。

您还可以通过使用"源属性"部分中的**添加 VMAT 属性**按钮来按机制或技术优化过滤器（关于 VMAT 属性的更多信息在下面提供），但是，使用此功能来按漏洞进行限制不会有所需的效果，因为漏洞类型由接收器而不是源来决定。

– **接收器**：在"接收器"部分，可将接收器添加为过滤器（与指定源的方法相同）。

  您可以通过将过滤器限制为特定漏洞类型（将跟踪规则条目的影响限制为仅特定类型的漏洞、机制或技术）来优化过滤器。要完成此任务，请单击"接收器属性"部分中的**添加 VMAT 属性**按钮，然后在"选择属性"对话框中选择属性。使用**过滤器**字段可对属性列表进行过滤。

  VMAT 是对 AppScan Source 应用于应用程序编程接口 (API) 的四种主要类型属性的分类。VMAT 属性类别包括：

  - **漏洞**：可导致安全违例的利用或攻击媒介类型
  - **机制**：用于阻止漏洞的安全性控制
  - **属性**：这些属性当前在"选择属性"对话框中不可用
  - **技术**：对于 API 所提供功能类型的一般描述

  过滤器示例：要对来自 HTTP（最高风险源）的所有 SQL 注入和 XSS 进行过滤，请在"源属性"部分中创建包含了 `Technology.Communications.HTTP` 过滤器的**限制为**跟踪规则，并在"接收器属性"部分中创建 `Vulnerability.Injection.SQL` 和 `Vulnerability.CrossSiteScripting` 规则。

– **必需调用**：在"必需调用"部分，将路径上必须存在的特定 API 调用从源添加到接收器。必须调用将结果限制为具有经由指定必需调用的跟踪。单击**添加中间调用**时，将打开"配置 API"对话框。在此对话框中，以指定源和接收器的方式来指定调用。

– **禁止调用**：在"禁止调用"部分中，将路径上不可存在的特定 API 调用从源添加到接收器。禁止调用将结果限制为具有未经由指定已禁止调用的跟踪。以添加必需调用的方法添加禁用调用。

提示：

– 当按**漏洞类型**、**API**、**文件**、**目录**或**项目**进行过滤时，可以通过在"选择值"对话框顶部的过滤器字段中输入模式来对该对话框中显示的列表进行过滤。

– 在任何结果表中，查看**源**和**接收器**列以了解要进行过滤的源和接收器。

– 要了解希望过滤的源、接收器和调用属性，请查看任何结果表中的**漏洞类型**列。

– 要查看可能要过滤的调用，请查看任何结果表中的 **API** 列中的条目。

过滤器示例

表 *12.* 过滤器示例

结果表中的过滤器行为	"过滤器编辑器"视图中的过滤器设置
结果表仅包含高严重性可疑安全性结果。	• 在"严重性"部分，选中**高**复选框，清除所有其他复选框。 • 在"分类"部分，选中**可疑**复选框，并清除所有其他复选框。
结果表包含名为 ProjectA 的项目中的所有结果，但参考漏洞类型除外。	• 在"漏洞类型"部分，选中**除去**单选按钮并单击**添加**。在"选择值"对话框中，选择**Vulnerability.Info**。 • 在"项目"部分，选中**限制为**单选按钮并单击**添加**。在"选择值"对话框中，选择 ProjectA。
仅显示包含跟踪的结果。	在"跟踪"部分中，单击**限制为**部分中的**添加**。接受"跟踪规则条目"对话框中的缺省条目，然后单击**确定**。对话框中的缺省值是： • 源 **API 正则表达式**字段是 **.***，正则表达式类型是 **PERL**。这样，AppScan Source 将过滤带有源的任何发现结果（使用 Perl 正则表达式语法）。 • 接收器 **API 正则表达式**字段是 **.***，正则表达式类型是 **PERL**。这样，AppScan Source 将过滤带有接收器的任何发现结果（使用 Perl 正则表达式语法）。
此结果表显示未经由 java.lang.Integer.parseInt 的从 HTTP 相关源到 SQL 注入相关接收器的跟踪。	在"跟踪"部分中，单击**限制为**部分中的**添加**。在"跟踪规则条目"对话框中，完成以下步骤： • 在"源"部分，单击**添加 VMAT 属性**。在"选择属性"对话框中，选择 Technology.Communications.HTTP。单击**确定**以添加 VMAT 属性，并返回到"跟踪规则条目"对话框。 • 在"接收器"部分，单击**添加 VMAT 属性**。在"选择属性"对话框中，选择 Vulnerability.Injection.SQL。单击**确定**以添加 VMAT 属性，并返回到"跟踪规则条目"对话框。 • 在"禁止调用"部分，单击**添加中间调用**。在"配置 API"对话框中的 **API 正则表达式**字段中输入 java.lang.Integer.parseInt.*。单击**确定**以添加中间调用，并返回到"跟踪规则条目"对话框，然后单击**确定**以添加跟踪规则条目。

使用 AppScan Source 预定义过滤器

AppScan Source 包含一组可选择用于过滤扫描结果的预定义过滤器。此帮助主题描述了这些预设过滤器。

注：在 AppScan Source V8.8 中，预定义过滤器已改进，从而提供更好的扫描结果。如果您需要继续使用较低版本的 AppScan Source 的预定义过滤器（已归档过滤器在 第 130 页的『AppScan Source 预定义过滤器（V8.7.x 和更低版本）』中列出），请按照第 132 页的『复原已归档的预定义过滤器』中的指示信息操作。

注：在 AppScan Source for Development（Visual Studio 插件）中，该视图是"编辑过滤器"窗口的一部分。

- 『! - AppScan 关键的少数』
- 『! - 高风险源』
- 『! - 重要类型』
- 第 129 页的『CWE SANS 2010 年的前 25 个漏洞』
- 第 129 页的『外部通信』
- 第 129 页的『低严重性和参考』
- 第 129 页的『干扰 - 质量』
- 第 129 页的『OWASP 移动设备前 10 个漏洞』
- 第 130 页的『OWASP 2010 年前 10 个漏洞』
- 第 130 页的『OWASP 2013 年前 10 个漏洞』
- 第 130 页的『支付卡行业数据安全标准漏洞』
- 第 130 页的『目标漏洞 - HTTP 源的 EncodingRequired』
- 第 130 页的『目标漏洞 - C/C++ 接收器的 Validation.Required』
- 第 130 页的『可信源』
- 第 130 页的『没有跟踪的漏洞』

! - AppScan 关键的少数

此过滤器与一些最危险漏洞类别中的结果匹配。这些结果被限制为"高"和"中"严重性漏洞。将从这些结果中移除具有特定源的结果。此过滤器中包含的特定漏洞类别为：

```
Vulnerability.CrossSiteScripting
Vulnerability.CrossSiteScripting.Reflected
Vulnerability.CrossSiteScripting.Stored
Vulnerability.Injection.OS
Vulnerability.Injection.LDAP
Vulnerability.Injection.SQL
Vulnerability.Injection.Mail
```

! - 高风险源

此过滤器将结果限制为具有以下属性之一的特定漏洞类型和源：

```
Technology.Communications.HTTP
Technology.Communications.IP
Technology.Communications.RCP
Technology.Communications.TCP
Technology.Communications.UDP
Technology.Communications.WebService
```

! - 重要类型

此过滤器包含更广范围的重要漏洞类别中的结果。这些结果被限制为属于"明确"或"可疑"分类的"高"和"中"严重性。此过滤器中包含的特定类别为：

```
Vulnerability.AppDOS
Vulnerability.Authentication.Credentials.Unprotected
Vulnerability.BufferOverflow
Vulnerability.BufferOverflow.FormatString
Vulnerability.BufferOverflow.ArrayIndexOutOfBounds
Vulnerability.BufferOverflow.BufferSizeOutOfBounds
Vulnerability.BufferOverflow.IntegerOverflow
Vulnerability.BufferOverflow.Internal
Vulnerability.CrossSiteRequestForgery
Vulnerability.CrossSiteScripting
Vulnerability.CrossSiteScripting.Reflected
Vulnerability.CrossSiteScripting.Stored
Vulnerability.FileUpload
Vulnerability.Injection
Vulnerability.Injection.LDAP
Vulnerability.Injection.OS
Vulnerability.Injection.SQL
Vulnerability.Injection.XML
Vulnerability.Injection.XPath
Vulnerability.Malicious.EasterEgg
Vulnerability.Malicious.Trigger
Vulnerability.Malicious.Trojan
Vulnerability.PathTraversal
Vulnerability.Validation.EncodingRequired
Vulnerability.Validation.EncodingRequired.Struts
```

CWE SANS 2010 年的前 25 个漏洞

此过滤器主要关注与 2010 年"CWE/SANS TOP 25 Most Dangerous Software Errors"相关的漏洞类型。

要了解 *2011 CWE/SANS Top 25 Most Dangerous Software Errors*，请参阅 http://cwe.mitre.org/top25/。

外部通信

此过滤器与从应用程序外部和整个网络产生的结果匹配。此过滤器与在任何 `Technology.Communications` 源产生的结果匹配。

低严重性和参考

此过滤器包含严重性为"低"和"参考"的结果。包含所有分类（明确、可疑和扫描覆盖范围）。

干扰 - 质量

该过滤器导致结果仅包含与质量编码实践相关的漏洞类型。

OWASP 移动设备前 10 个漏洞

此过滤器主要关注与"Open Web Application Security Project (OWASP) Mobile Top 10 Release Candidate V1.0"列表相关的漏洞类型。

要了解关于 OWASP 的信息，请参阅https://www.owasp.org/index.php/Main_Page。 https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project 处提供了各种 OWASP 文档和安全风险的链接。

OWASP 2010 年前 10 个漏洞

此过滤器主要关注与 2010 年"Open Web Application Security Project (OWASP) Top 10"列表相关的漏洞类型。

要了解关于 OWASP 的信息，请参阅https://www.owasp.org/index.php/Main_Page。 https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project 处提供了各种 OWASP 文档和安全风险的链接。

OWASP 2013 年前 10 个漏洞

此过滤器主要关注与 2013 年"Open Web Application Security Project (OWASP) Top 10"列表相关的漏洞类型。

要了解关于 OWASP 的信息，请参阅https://www.owasp.org/index.php/Main_Page。 https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project 处提供了各种 OWASP 文档和安全风险的链接。

支付卡行业数据安全标准漏洞

此过滤器主要关注与支付卡行业数据安全标准 (PCI DSS) V3.2 标准相关的漏洞类型。

要获取有关信息，请参阅https://www.pcisecuritystandards.org/security_standards/index.php。

扫描覆盖范围结果

该过滤器导致结果仅包含"扫描覆盖范围结果"（请参阅第 18 页的『分类』以获取更多信息）。

目标漏洞 - HTTP 源的 EncodingRequired

此过滤器主要关注 Validation.EncodingRequired 和 Validation.EncodingRequired.Struts 漏洞类别中的结果。仅包含从 Technology.Communications.HTTP 源产生的结果。这些发现项被限制为属于"明确"或"可疑"分类的"高"和"中"严重性。

目标漏洞 - C/C++ 接收器的 Validation.Required

此过滤器主要关注一组已知 C 和 C++ 接收器的 Validation.Required 漏洞。这些发现项被限制为属于"明确"或"可疑"分类的"高"和"中"严重性。

可信源

此过滤器假定来自于特定源（如会话对象或请求属性）的数据是安全的。

没有跟踪的漏洞

该过滤器列出不包含跟踪的漏洞。

AppScan Source 预定义过滤器（V8.7.x 和更低版本）

本主题列出了 AppScan Source V8.7.x 和更低版本中包含的预定义过滤器。

如果您需要访问这些过滤器，请按照第 132 页的『复原已归档的预定义过滤器』中的指示信息进行操作。

! - 关键的少数

此过滤器与一些最危险漏洞类别中的结果匹配。仅包含在外部网络通信源中产生的结果。此过滤器提供高风险结果的高度聚焦起点。此过滤器中包含的特定类别为：

```
Vulnerability.BufferOverflow
Vulnerability.BufferOverflow.FormatString
Vulnerability.PathTraversal
Vulnerability.CrossSiteScripting
Vulnerability.CrossSiteScripting.Reflected
Vulnerability.CrossSiteScripting.Stored
Vulnerability.Injection
Vulnerability.Injection.LDAP
Vulnerability.Injection.SQL
Vulnerability.Injection.OS
Vulnerability.Injection.XML
Vulnerability.Injection.XPath
```

高优先级 - 外部通信

此过滤器与从应用程序外部和整个网络产生的结果匹配。此过滤器与在任何 Technology.Communications 源产生的结果匹配。

高优先级 - 重要类型

此过滤器包含一些最危险漏洞类别（如 CrossSiteScripting 和 Injection.SQL）中的结果。此过滤器中包含的特定类别为：

```
Vulnerability.AppDOS
Vulnerability.Authentication.Credentials.Unprotected
Vulnerability.Authentication.Entity
Vulnerability.BufferOverflow
Vulnerability.BufferOverflow.FormatString
Vulnerability.CrossSiteScripting
Vulnerability.CrossSiteScripting.Reflected
Vulnerability.CrossSiteScripting.Stored
Vulnerability.Injection
Vulnerability.Injection.LDAP
Vulnerability.Injection.OS
Vulnerability.Injection.SQL
Vulnerability.Injection.XML
Vulnerability.Injection.XPath
Vulnerability.PathTraversal
```

低优先级 - 测试代码

此过滤器包含测试代码中的结果。此过滤器中的特定类型包括：

```
Vulnerability.Quality.TestCode
```

干扰 - 类似复制操作

此过滤器包含与类似复制操作相关的结果。从可能可信也可能不可信的源中获取数据时会发生类似复制操作，但是对此数据执行的操作可信。

将查找以下模式：

```
Technology.Database --> Vulnerability.Injection.SQL
Mechanism.SessionManagement --> Mechanism.SessionManagement
Technology.XML, Technology.XML.DOM, Technology.XML.Schema,
Technology.XML.XPath --> Vulnerability.AppDOS.XML,
Vulnerability.Injection.XML
```

干扰 - 日志记录问题

此过滤器包含与错误处理相关的结果。找到的结果来自于指向日志记录机制的错误处理例程。将与以下模式匹配：

```
Mechanism.ErrorHandling -->
Vulnerability.Logging, Vulnerability.Logging.Forge, Vulnerability.Logging.Required
```

干扰 - 低严重性

此过滤器包含严重性为"低"的结果。包含所有分类。

干扰 - 可信源

此过滤器包含来自于可信源的结果。只有以 `java.lang.System.getProperty.*` 作为其源的结果才包含在此过滤器中。

复原已归档的预定义过滤器

通过执行本任务中的步骤，可将 V8.8 之前的 AppScan Source 中已提供的预定义过滤器添加回本产品。在单台机器上复原后，便可以按照与所创建的过滤器相同的方式来管理上述过滤器（例如，上述过滤器可共享到多个客户机）。

关于此任务

已归档的预定义过滤器位于 `<data_dir>\archive\filters`（其中 `<data_dir>` 是 AppScan Source 程序数据的位置，如第 275 页的『安装和用户数据文件位置』中所述）中。

过程

1. 在 `<data_dir>\archive\filters` 中，找到想要复原的一个或多个过滤器（AppScan Source 过滤器具有 `.off` 文件扩展名）。
2. 将这一个或多个过滤器复制到 `<data_dir>\scanner_filters`。
3. 重新启动 AppScan Source。

下一步做什么

要了解如何管理过滤器（包括您已复原的已归档过滤器），请参阅第 133 页的『在"过滤器编辑器"视图中创建和管理过滤器』。

创建和管理过滤器

AppScan Source 提供多种方法来创建和使用过滤器。用于创建过滤器的主视图（"过滤器编辑器"视图）提供强大的规则集，可以手动设置这些规则，然后保存到过滤器。"过滤器编辑器"视图还提供一种机制来管理您已创建的过滤器，使您能够轻松地对其进行修改或移除。此外，您还可以使用提供了结果的图形表示法的视图来对结果表进行过滤，然后将这些过滤器保存在"过滤器编辑器"视图中。创建过滤器时，其他视图将更新以反映过滤器属性。

- 『在"过滤器编辑器"视图中创建、管理和应用过滤器』
- 『从"评估摘要"和"漏洞矩阵"视图中进行过滤』
- 『在"源和接收器"视图中创建过滤器』

在"过滤器编辑器"视图中创建、管理和应用过滤器

"过滤器编辑器"视图使您能够通过指定过滤规则来创建过滤器。可以保存、修改和移除在"过滤器编辑器"视图中创建的过滤器。在该视图中创建过滤器后，便可以通过视图中的下拉菜单来对其进行应用。请参阅『在"过滤器编辑器"视图中创建和管理过滤器』。

在 AppScan Source for Analysis 中，您可将已创建的过滤器共享到 AppScan Enterprise Server，并访问他人已共享的过滤器。在 AppScan Source for Development 中，如果在服务器方式下运行，那么可以访问共享的过滤器。

注：在 AppScan Source for Development（Visual Studio 插件）中，该视图是"编辑过滤器"窗口的一部分。

从"评估摘要"和"漏洞矩阵"视图中进行过滤

注：

- "评估摘要"视图在 macOS 上不可用。
- 在 AppScan Source for Development（Visual Studio 插件）中，这些视图是"编辑过滤器"窗口的一部分。

"评估摘要"和"漏洞矩阵"视图提供对结果的图形表示法。在这些视图中，结果以不同方式分组。可选择这些组来对结果表进行过滤，以使该表仅显示选定的一个或多个组内的那些结果。通过此方法执行的任何过滤都会自动反映在"过滤器编辑器"视图中，然后您可以从其中保存过滤器设置。

在"源和接收器"视图中创建过滤器

注："源和接收器"视图在 AppScan Source for Development（Visual Studio 插件）中不可用。

"源和接收器"视图提供查看结果并基于输入和输出的跟踪来对其进行过滤的能力。在该视图中执行的过滤可直接保存在视图中。创建过滤器时，可以选择立即将其应用于扫描结果。

请参阅第 137 页的『在"源和接收器"视图中创建过滤器』。

在"过滤器编辑器"视图中创建和管理过滤器

在该视图中，您可以创建、编辑、保存、删除和管理过滤器。如果使用 AppScan Source for Analysis，那么可以共享过滤器并访问已由他人共享的过滤器。在 AppScan Source for Development 中，如果使用服务器方式并已登录到 AppScan Enterprise Server，那么可访问共享的过滤器。

过程

1. 在第 271 页的『"过滤器编辑器"视图』工具栏中，单击**新建**。新过滤器名称是 `Untitled<-number>`（其中第一个新的无标题过滤器是 `Untitled`，而下一个新的无标题过滤器是 `Untitled-1`，以此类推）。

注：在 AppScan Source for Development（Visual Studio 插件）中，该视图是"编辑过滤器"窗口的一部分。

2. 展开类别，然后选择要指定给过滤器的条件。
3. 单击**保存**或**另存为**。
4. 指定过滤器名称，然后单击**确定**。新过滤器名称将替换过滤器列表中的 `Untitled<-number>`。

下一步做什么

要应用过滤器，请在"过滤器编辑器"视图下拉菜单中将其选定。

注：在"漏洞矩阵"视图外应用的过滤器可能不会影响"漏洞矩阵"视图。必须选择"漏洞矩阵"视图**显示已过滤结果的计数**工具栏按钮才会在"漏洞矩阵"视图中反映过滤器。

可以在"过滤器编辑器"视图中通过选择列表中的过滤器然后予以处理来直接管理过滤器，或者也可以单击**管理过滤器**以打开"管理过滤器"对话框，其中提供已保存的过滤器的列表。

- **修改过滤器**：在"过滤器编辑器"视图中或在"管理过滤器"对话框中选择过滤器，然后修改其过滤规则并保存更改。

  注：无法修改或删除内置过滤器。
- **删除过滤器**：在"过滤器编辑器"视图中或在"管理过滤器"对话框中选择过滤器，然后单击**删除**。在"管理过滤器"对话框中，您可以选择多个过滤器，然后单击**删除**以同时将其移除。
- **从另一过滤器创建过滤器**：您可以修改某个过滤器，然后单击**另存为**以将其另存为使用新名称的过滤器。这允许您通过在现有过滤器的设置上进行构建来创建新的过滤器。您可以在"过滤器编辑器"视图和"管理过滤器"对话框中执行此操作。

  提示：可通过打开过滤器并使用**另存为**操作以新名称进行保存来完成相同操作。然后可打开新过滤器并对其进行修改。通过选择该方法，可从一个内置过滤器创建新过滤器。
- **恢复过滤器设置**：如果修改某个过滤器的属性并希望撤销这些更改，请单击**恢复**以将此过滤器返回到其上次保存的设置。可以在"过滤器编辑器"视图和"管理过滤器"对话框中执行此操作。在对话框中，如果您有多个过滤器存在未保存的更改，单击**恢复**将导致存在未保存的更改的所有选定过滤器恢复到其保存的设置。
- **共享过滤器**（仅限 AppScan Source for Analysis）：要创建共享的过滤器，请在过滤器编辑器中打开过滤器，并在"过滤器编辑器"视图工具栏上单击**共享过滤器**。

  注：要修改、删除或创建共享过滤器，您必须具有**管理共享过滤器**许可权。要了解关于设置许可权的信息，请参阅《*IBM Security AppScan Source* 安装和管理指南》。

从"评估摘要"视图过滤

扫描完成后，可在"评估摘要"视图中查看其结果（缺省情况下，该视图在"筛选"透视图中打开）。在此视图中，您可以从条形图中创建过滤器。

关于此任务

扫描完成后，第 271 页的『"评估摘要"视图』包含对这些发现的图形条形图表示。此视图可以通过优化来按漏洞类型、API、项目或文件显示发现。在"评估摘要"视图中选择分组的发现时，发现表切换为仅显示在"评估摘要"视图中选择的那些发现。

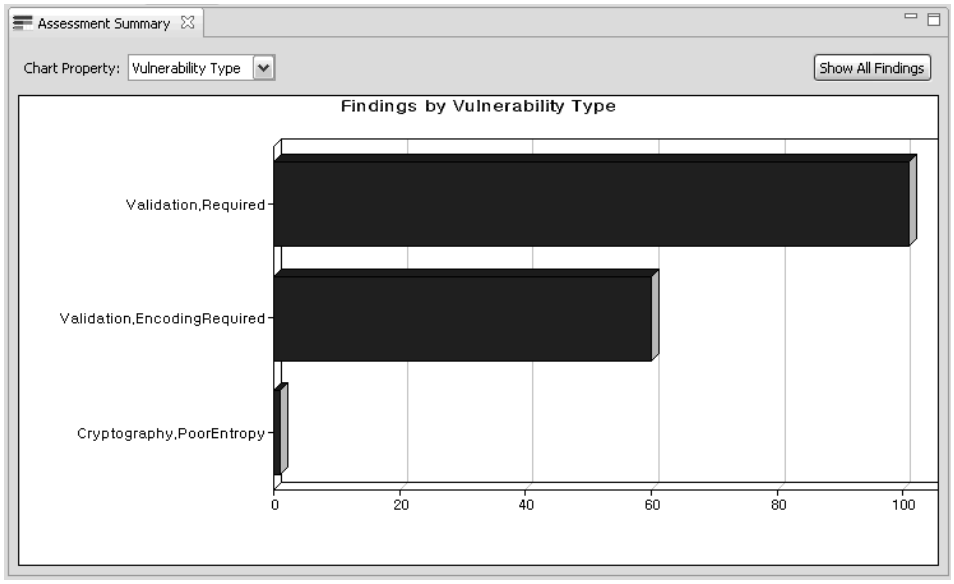
注：在"漏洞矩阵"视图外应用的过滤器可能不会影响"漏洞矩阵"视图。必须选择"漏洞矩阵"视图**显示已过滤结果的计数**工具栏按钮才会在"漏洞矩阵"视图中反映过滤器。

注：

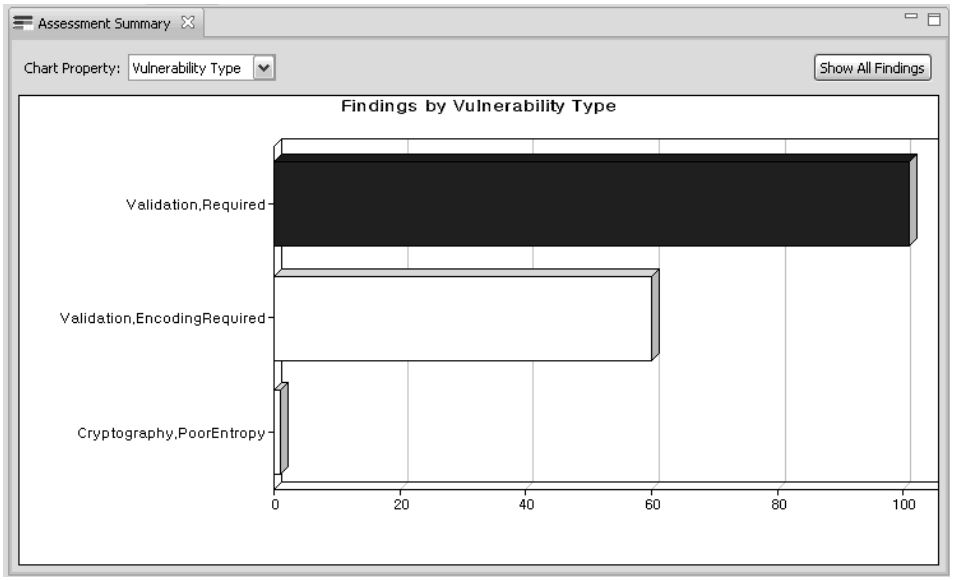
- "评估摘要"视图在 macOS 上不可用。
- 在 AppScan Source for Development（Visual Studio 插件）中，该视图是"编辑过滤器"窗口的一部分。

过程

1. 在"评估摘要"视图中，更改图形表示以适应您的需求。例如，给出一个包含 `Validation.Required`、`Validation.EncodingRequired` 和 `Cryptography.PoorEntropy` 漏洞类型的评估，将**图表属性**设置为**漏洞类型**。这将在条形图表示法中按漏洞类型显示这些发现：

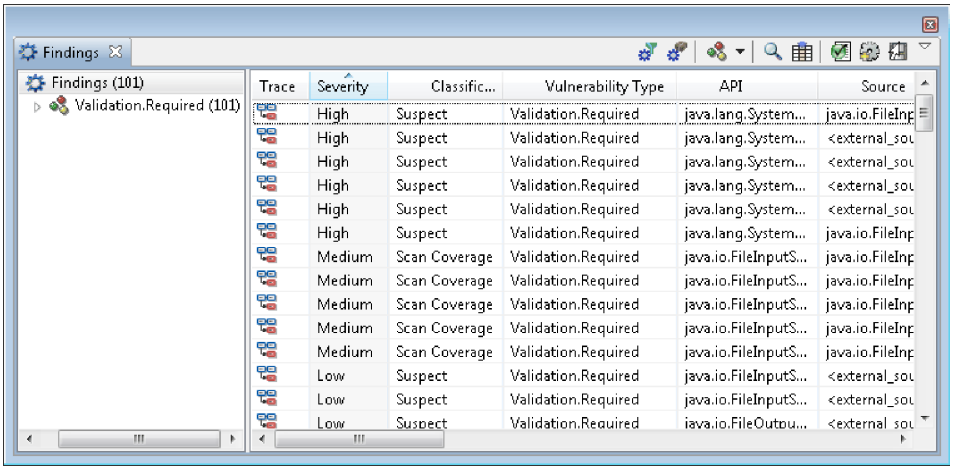


2. 要创建 `Validation.Required` 漏洞类型的过滤器，请单击图表中的 `Validation.Required` 条形图。

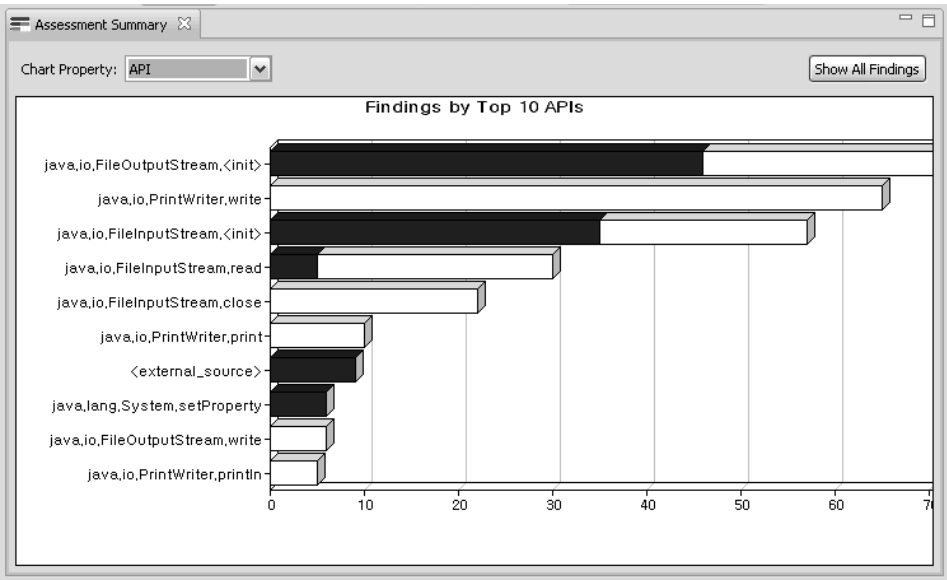


提示：在条形图上按住鼠标以查看漏洞的数量。

过滤的结果显示在发现表中：



3. 过滤操作还使"过滤器编辑器"视图用"评估摘要"视图中选择的过滤规则设置进行填充。此过滤器可以保存在"过滤器编辑器"视图中（要了解过滤规则设置以及如何保存过滤器，请参阅第 133 页的『在"过滤器编辑器"视图中创建和管理过滤器』）。
4. 要通过 API 查看同一过滤器结果，可将**图表属性**设置为 **API**：



从漏洞矩阵进行过滤

"漏洞矩阵"视图显示扫描中所包含全部应用程序的结果的合计数量。这些结果按严重性级别在矩阵中分组。您可以通过选择这些结果组来创建过滤器。

关于此任务

在第 272 页的『"漏洞矩阵"视图』中选择已分组的结果时，结果表将更改为仅显示在漏洞矩阵中已选定的那些结果。

注：在 AppScan Source for Development（Visual Studio 插件）中，该视图是"编辑过滤器"窗口的一部分。

注："漏洞矩阵"视图中不包含**质量**结果和分类为**参考**严重性级别的结果。

过程

1. 在"漏洞矩阵"视图中，选择您想要在结果表中看到的矩阵部分。例如，要在结果表中仅看到**高**严重性**可疑**安全性结果，请选择矩阵的该部分。这将使经过滤的结果显示在结果表中。
2. 过滤操作还会使"过滤器编辑器"视图用"漏洞矩阵"中所选项的过滤规则设置进行填充。此过滤器可以保存在"过滤器编辑器"视图中（要了解过滤规则设置以及如何保存过滤器，请参阅第 133 页的『在"过滤器编辑器"视图中创建和管理过滤器』）。

在"源和接收器"视图中创建过滤器

过程

1. 打开或浏览到"源和接收器"视图。
2. "源和接收器"视图包含三个部分。此视图的结果表部分显示您已选择在其他两个部分中显示的源、接收器和中间节点的结果。这在第 266 页的『"源和接收器"视图』中进行了描述。

3. 已将结果表设置为显示您感兴趣的结果后，单击**新建基于所选源、接收器和中间节点的过滤器**。
4. 在"创建过滤器"对话框中：
   - 在**名称**字段中指定过滤器的名称。
   - 选中**立即应用此过滤器**可将此过滤器应用于评估中的所有结果表。选中此复选框等同于在"过滤器编辑器"视图中选择过滤器。它设置当前主过滤器，从而影响所有视图（例如，"漏洞矩阵"和"结果"视图）。

     注：在"漏洞矩阵"视图外应用的过滤器可能不会影响"漏洞矩阵"视图。必须选择"漏洞矩阵"视图**显示已过滤结果的计数**工具栏按钮才会在"漏洞矩阵"视图中反映过滤器。
   - 如果过滤出的结果与您的当前工作无关，那么可以通过选中**创建用于排除这些结果的应用程序过滤器**复选框来从评估中将其移除。选中此复选框会将新过滤器添加为应用程序属性中的排除过滤器（在应用程序的"属性"视图中，选择"排除"选项卡可查看排除过滤器的列表）。对于应用程序的未来扫描，将在"排除结果"视图而不是在"结果"视图中报告与此过滤器匹配的结果。
5. 单击**确定**以对结果进行过滤或排除。

应用过滤器

可在扫描之前或之后应用过滤器。要在扫描之后应用过滤器，使用"过滤器编辑器"或使您能够应用过滤器的另一个视图。要在扫描之前应用过滤器，使用扫描配置设置全局过滤器。在扫描之前应用过滤器时，无法显示未过滤的结果或在不再次进行扫描的情况下除去过滤器。

在扫描之前应用过滤器

请参阅『全局应用过滤器』以了解如何设置全局过滤器，或参阅第 94 页的『管理扫描配置』以了解如何在扫描配置中设置过滤器。

在扫描之后应用过滤器

当您在"过滤器编辑器"视图中选择过滤器后，它将自动应用于结果的列表。其他视图提供过滤操作，如第 132 页的『创建和管理过滤器』中所述。

全局应用过滤器

已创建的过滤器可应用于所有应用程序、单个应用程序以及单个项目。全局过滤器应用于"属性"视图中，在该视图中可指定想要应用过滤器的方式（可直接应用过滤器，也可应用其反向过滤器）。例如，如果您想要设置应用程序的全局过滤器，请在"资源管理器"视图中选择该应用程序，然后打开其"属性"视图（使用**视图**菜单或通过右键单击应用程序并单击**属性**）。

开始之前

如果要为所有应用程序或单个项目设置过滤器，请使用"属性"视图中的"过滤器"选项卡。如果要为单个应用程序设置过滤器，请使用"属性"视图中的"排除和过滤器"选项卡。

过程

1. 在选项卡的"过滤器"部分中，单击**添加**。
2. 在"选择过滤器"对话框中，选择想要全局应用的过滤器。
3. 可选： 如果想要应用过滤器的反向过滤器（而不是直接应用过滤器），请选择**反向过滤器**。
4. 单击**确定**以关闭"选择过滤器"对话框。
5. 完成过滤器的添加后，在"属性"视图中保存更改。

确定所应用的过滤器

可在进行扫描之前全局地将过滤器应用于应用程序和项目，或者可在扫描之后将过滤器应用于评估。要使您能够快速地确定过滤器如何应用于评估中的结果，AppScan Source 在主工作台的底部提供了过滤器指示符。

如果尚未应用过滤器，那么工作台底部的过滤器指示符指示**未过滤结果**。

如果已应用了过滤器，指示符将更改为显示为**已过滤结果**的链接。选择该链接将打开一条消息，该消息使您能够确定如何应用了过滤器。

- **扫描时间过滤器**是应用于应用程序和项目的全局过滤器：
  - 如果评估是因扫描与已配置的过滤器不匹配的应用程序或项目得到的，那么该消息将指示未应用扫描时间过滤器。
  - 如果已扫描的应用程序或项目具有已配置过滤器，那么将按名称列出已配置的过滤器。
  - 在某些情况下，AppScan Source 检测到已应用扫描时间过滤器，但评估不包含关于这些过滤器的信息。例如，打开旧评估时会发生该情况。
- **当前过滤器**是在扫描后已应用于结果的过滤器。消息指示是否未应用当前过滤器，或者是否已应用过滤器。如果是后者，那么**重置**链接可用。选择该链接后，将从结果除去当前过滤器。

通过排除进行分类

扫描过后，您可确定与当前工作无关的结果，并且在对扫描结果分类时，使其在结果表中不可视。这些排除（或已排除的结果）将不再出现在"结果"视图中，而且将使用更改的结果立即更新评估度量值。添加到配置中的过滤器和束排除仅在后续扫描中生效。

排除的作用域

排除可应用于所有应用程序（全局）、个别应用程序或项目。

- **全局排除**应用于所有扫描。
- **应用程序排除**仅应用于针对特定应用程序及其对应项目运行的扫描。
- **项目排除**应用于特定项目中存在的发现结果。

注：排除将影响评估度量，包括发现结果总数（已排除的发现结果不会包含在评估度量中）。

全局排除

您可以从任何 AppScan Source for Analysis 应用程序存储或访问全局排除，并且这些排除会应用于所有扫描。只有共享过滤器才能成为全局过滤器。

应用程序和项目排除

束排除仅应用于应用程序。过滤器排除可以应用于应用程序或项目。应用于应用程序和项目的排除可以是共享排除或本地排除。

指定排除

从结果表或"属性"视图中可将发现结果标记为排除。排除可包含个别结果、过滤器或束。通常，从结果表创建的排除将立即生效。 "属性"视图中创建的排除需要再次进行扫描才能生效。

在以下过程中，排除将立即应用于应用程序：

- 选择一个或多个发现结果，右键单击所选内容，然后从菜单中选择**排除发现结果**。
- 将一个或多个发现结果添加到当前排除的束中（包括已排除的束）。
- 从先前排除的束（包括已排除的束）中删除一个或多个发现结果。
- 删除已排除的束。

在以下情况下，排除不立刻应用于应用程序：

- 将束添加为排除。
- 将过滤器添加为排除。
- 修改发现结果，以使其与已排除过滤器的条件相匹配。
- 修改发现结果，以使其不再与已排除过滤器的条件相匹配。

在结果表中将结果标记为排除

过程

1. 选择结果表中可能对您不重要或者您不希望查看的结果（或结果组）。
2. 右键单击所选内容，然后从菜单中选择**排除结果**。排除将立即应用。排除的发现不再显示在表中，且度量值立即更新。

结果

要查看已排除的结果，请打开"已排除的结果"视图。已排除的结果也显示在名为**已排除的束**的视图中。

要重新包含已排除的结果，请按照『重新包含已标记为排除项的结果』中的指示信息进行操作。

重新包含已标记为排除项的结果

已排除的结果出现在"已排除结果"视图中。从该视图中，可以重新包含已排除的结果。

过程

1. 在"已排除的结果"视图中，选择要重新包含的结果（或结果组）。
2. 右键单击所选内容，然后从菜单中选择**包含结果**。

结果

已包含的结果添加回评估中 - 并且结果表和度量值立即更新以反映已重新包含的结果。结果不再显示在"已排除的结果"视图中。

注：在 AppScan Source for Analysis 中，还可通过从束除去结果或通过将结果移至未排除的新束来从**已排除**束视图重新包含已排除的结果。

示例：指定过滤器排除

过滤器条件可确定过滤器是否排除与过滤器匹配或不匹配的结果。

这些示例描述了如何创建排除发现结果的过滤器：

- 『示例：过滤和排除目录』
- 『示例：过滤和排除 API』

示例：过滤和排除目录

在此示例中，将创建一个过滤器，其中仅显示包含 Microsoft `include` 文件的发现结果。然后，此过滤器将用于缩小结果列表（将排除与过滤器匹配的所有结果）。

过程

1. 在"过滤器编辑器"视图的**目录**部分中，添加指向 Microsoft include 文件的路径（例如 `C:\Program Files\Microsoft Visual Studio 8\VC\include`）。
2. 选择**限制为**以使其成为包含规则。
3. 在"结果"视图工具栏上，单击**显示与过滤器不匹配的结果**以仅查看 Microsoft 头文件的结果。这使您能够查看在再次全局地应用反向过滤器并进行扫描之后扫描结果呈现的状态。
4. 使用名称保存过滤器，如 **MS 包含**。
5. 返回到"配置"透视图，并在"资源管理器"视图中选择 C/C++ 应用程序或项目。
6. 如果选择了应用程序，请打开"属性"视图的"排除和过滤器"选项卡。如果选择了项目，请打开"属性"视图的"过滤器"选项卡。单击**添加**。选择 **MS 包含**，然后选择**反向过滤器**。
7. 在"属性"视图中保存更改，然后再次扫描应用程序或项目。
8. 返回到筛选。"已排除的结果"视图将显示此排除中的结果。

示例：过滤和排除 API

希望优先处理结果，且希望排除某些结果时，筛选过程早期可能发生常见筛选场景。例如，您确定三个 API 不构成威胁，并希望从后续扫描中排除这些 API。

过程

1. 在"过滤器编辑器"的 API 部分，单击**添加**并选择三个 API。
2. 选择**限制为**。
3. 对过滤器命名并保存。

4. 返回到"配置"透视图，并在"资源管理器"视图中选择项目（或应用程序）。
5. 在"属性"视图中，将过滤器的行为设置为**反向**（在"选择过滤器"对话框中，选择**反向过滤器**）。
6. 再次扫描。过滤器中的 API 将不再出现在结果中。

结果

使用同一示例，您可能只想看到过滤器中包含的结果。在此实例中，在将过滤器添加到列表时，请勿选择**反向过滤器**。再次扫描时，将仅显示过滤器中的结果。

从"属性"视图中指定束排除

束排除将消除束中的发现结果。只能从应用程序中排除束。

过程

1. 如第 143 页的『创建束』中所述创建束。
2. 在"资源管理器"视图中，选择要与束关联的应用程序。
3. 在"属性"视图中，选择**排除**选项卡。
4. 单击**添加束**，并在"选择束"对话框中选择包含要从应用程序中排除的发现结果的束。
5. 单击**确定**。
6. 再次扫描。束中的发现结果将不再出现在结果表中。

通过束进行筛选

束具有独特的特征，可能对筛选过程至关重要。

关于此任务

- 可以将束作为单个缺陷或束中每个发现结果的缺陷导出到缺陷跟踪系统。
- 束可以是报告生成的基础。
- 束连接到应用程序。

要点：一个结果一次只能存在于一个束中。如果一个结果存在于一个束中，那么将此结果移到另一个束则将从第一个束中移除此结果。

以下示例概述了通过束进行的简单筛选：

过程

1. 扫描源代码。
2. 创建名为 `Resolve ASAP` 的束。
3. 向束添加一些关键结果。
4. 向束中的结果添加说明。
5. 将束或发现结果提交至缺陷跟踪系统，或通过电子邮件将其发送给其他开发者。
6. 修复这些问题。

创建束

束的创建在"束"视图或包含结果表的视图中进行。可向现有束或新束中添加发现内容。

以下主题描述了"束"视图和"发现结果"视图中的束创建：

- 『在"束"视图中新建束』
- 『在"结果"视图中新建束』

注：要能够为评估创建束，必须在 AppScan Source for Analysis 中装入为了创建此评估而扫描过的应用程序。如果您打开未装入的应用程序的评估，那么束创建操作将不可用。

在创建了一个或多个束之后，"结果"视图**隐藏束结果**操作（ ）将允许您切换视图中对束结果的显示。此操作会隐藏已创建的所有已包含束中的结果。此设置不影响已排除束中结果的显示 - 这些结果从不在"结果"视图中显示。

在"束"视图中新建束

过程

1. 在"束"视图中，单击工具栏上的**新建束**。
2. 对束进行命名并单击**确定**。束名称将出现在"束"视图中。
3. 要将发现结果添加到束，请遵循『将结果添加到现有束』中的指示信息。

在"结果"视图中新建束

过程

1. 在"结果"视图中，选择要添加到束的结果。
2. 右键单击所选内容，从菜单中依次选择**添加到束** > **新建**。
3. 对束进行命名并单击**确定**。

将结果添加到现有束

关于此任务

可从多个视图中将发现结果添加到束：

- "结果"视图
- "已排除的结果"视图
- "已修正/修改的结果"视图
- "缺失的结果"视图
- "报告"视图
- 结果详细信息

提示：通过使用拖放操作，可将发现结果从结果表移至"束"视图。

要将结果添加到束，请执行以下操作：

过程

1. 选择要添加到束的发现结果。
2. 右键单击所选内容，并从菜单中依次选择**添加到束** > **<束名称>**（此列表包含最近创建的五个束）或者**添加到束** > **选择**。
3. 如果选择**添加到束** > **选择**，请在"选择束"对话框中选择要添加结果的束，然后单击**确定**。

在束之间移动结果

过程

1. 在"束"视图中，打开包含要移动的发现结果的束。
2. 选择您要移动的一个或多个结果，然后完成以下操作之一：
   - 单击视图工具栏上的**移动到束**或**移动到新束**。然后选择要将结果移动到的束，或为结果创建新束。
   - 右键单击所选项，然后单击**移动到束**。这样将打开一个菜单，该菜单允许您从列表或对话框选择现有束，或者创建要将所选内容移动至的新束。

结果

注：移动到或添加到已排除束的结果不会在当前评估中被排除。要将结果标记为在当前评估中被排除，请使用**排除结果**操作。

查看束中的结果

将结果添加到束时，发现内容在束中显示为一行。如果打开束，将会看到束中包含的所有结果。

关于此任务

束中来自多个项目的结果的显示方式可能不同。如果最近扫描中找不到束中的结果，那么将以绿色斜体显示。

请参考以下应用程序 X 的示例。

过程

1. 应用程序 X 包含项目 A 和 B。
2. 扫描应用程序 X。
3. 创建包含来自项目 A 和 B 的结果的束。
4. 扫描项目 B。在"束"视图中，项目 B 中的结果将出现，且项目 A 中的结果显示为绿色斜体。

结果

以绿色斜体突出显示的发现结果是已修复/缺失结果。已修复/缺失结果是束中的结果，而不是当前评估中的结果。结果标识为已修正/缺失是因为该结果已解决、除去或源文件未扫描。在"束"视图中，**已排除**列标识是否已排除该束。

将束保存到文件

您可以将束另存为文件，以在 AppScan Source for Development 中打开。束还允许您将发现结果的快照从 AppScan Source for Analysis 导入到 AppScan Source for Remediation。

过程

1. 完成以下其中一个操作：
   a. 在"束"视图中，选择束并单击工具栏中的**将束保存到文件**。
   b. 打开束并单击工具栏中的**将束保存到文件**。
2. 选择要保存束文件的目录。
3. 对束文件命名 (`<file_name>.ozbdl`)。

结果

要打开已保存的束：

- 在 AppScan Source for Development（Eclipse 插件）中，选择**安全分析** > **打开** > **打开束**。
- 在 AppScan Source for Development（Microsoft Visual Studio 插件）中，选择 **IBM Security AppScan Source** > **打开束**。
- 在 AppScan Source for Analysis 中，单击"束"视图工具栏中的**打开束**。

提示：在 Windows 系统上，双击"束"视图中的束文件，以在 AppScan Source for Analysis 或 AppScan Source for Development 中将其打开。

将束提交至缺陷跟踪及通过电子邮件发送

束中的发现结果可以提交至您的企业缺陷跟踪系统，或通过电子邮件进行发送。将结果置于束中后，可将这些结果作为错误提交给开发者进行修复。

过程

1. 打开束。
2. 单击**将束提交至缺陷跟踪**工具栏按钮向下箭头，然后选择您的缺陷跟踪系统。

   注：根据您的缺陷跟踪系统，您可能希望在提交束之前修改"缺陷跟踪系统"首选项。

   或者，在"束"工具栏上，单击**通过电子邮件发送束**以将束发送到其他人（必须提前配置电子邮件首选项）。
3. 完成打开的配置对话框。根据所选择的缺陷跟踪系统的不同，这些对话框也有所不同，在帮助的 *AppScan Source for Analysis* 和缺陷跟踪部分中描述了这些对话框。

向束添加说明

过程

1. 在"束"视图中，选择要添加注释的束。
2. 单击"束"工具栏上的**添加说明**，或右键单击所选内容并从菜单中选择**添加说明**。
3. 输入说明并单击**确定**。

修改结果

已修改的结果是已更改了漏洞类型、分类或严重性，或者具有注释的结果。"已修改的结果"视图显示当前应用程序（由于打开其评估而处于活动状态的应用程序）的这些结果。在"我的评估"视图中（仅在 AppScan Source for Analysis 中可用），**已修改**列指示结果在当前评估中是否发生了更改。

对结果的修改即时生效，同时还会更新度量值。修改随应用程序进行存储 - 并且应用于其将来的扫描。

可以在"结果详细信息"视图中或从具有发现表的任何视图修改结果。"结果详细信息"视图允许更改单个结果，此外，在结果表中还可以修改多个结果。

注：您必须拥有**保存评估**许可权才能在修改评估后保存更改。

从结果表中修改

如果将对多个文件进行相同更改，可能想要通过结果表修改结果。如果将修改单个结果，请使用结果表或"结果详细信息"视图。

- 『更改漏洞类型』
- 『提升结果分类』
- 『修改严重性』
- 第 155 页的『支持的注释和属性』

更改漏洞类型

可以对单独的结果或一组结果更改漏洞类型。

过程

1. 从结果表，选择要修改的单个或一组结果。
2. 右键单击所选项，然后从菜单中选择**设置漏洞类型**。
3. 在"选择漏洞类型"对话框中，选择需要的漏洞类型并单击**确定**。

提升结果分类

分类为可疑安全性结果或扫描覆盖范围结果的结果可提升为明确结果。

过程

1. 从结果表，选择要修改的单个或一组结果。
2. 右键单击所选项，然后从菜单中选择**提升为明确**。

修改严重性

选择新的严重性级别将更改各选定结果的严重性。例如，AppScan Source 可能会报告某个 API 为中等严重性，但是您的公司政策将其标识为更严重。可以修改严重性以满足您的需求，但请注意 AppScan Source 补救帮助不会包含此修改。

过程

1. 从结果表，选择要修改的单个或一组结果。
2. 右键单击所选项，然后从菜单中选择**设置严重性**。
3. 选择**高**、**中**、**低**或**参考**，作为新的严重性级别。

对结果进行说明

注释可用于提醒您对结果采取进一步的操作 - 或将关于结果的信息传递给其他人。您可以向单个结果或一组结果添加注释。

过程

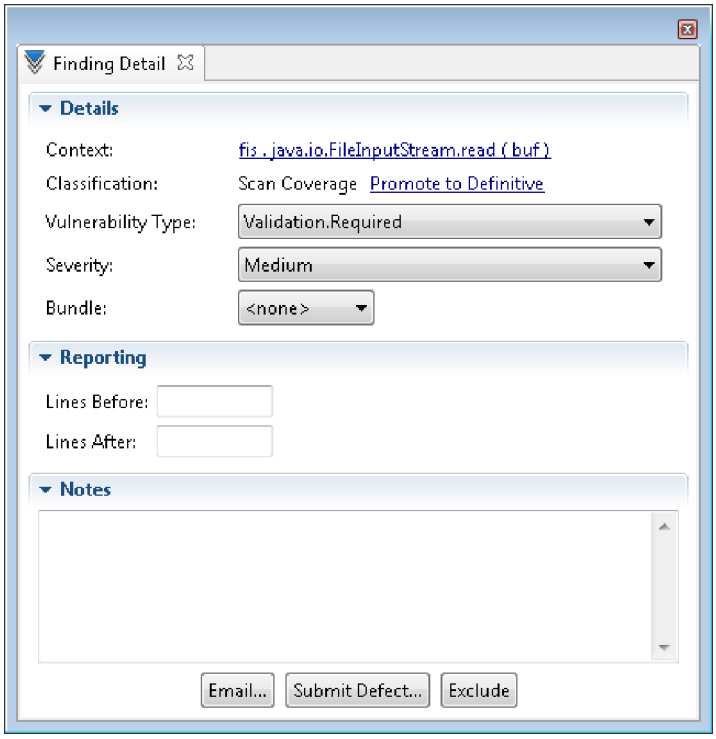
1. 从结果表，选择要修改的单个或一组结果。
2. 右键单击所选项，然后从菜单中选择**添加注释**。
3. 输入注释，然后单击**确定**。

在"结果详细信息"视图中修改结果

可在"结果详细信息"视图中修改单个结果。如果在表中选择结果，并打开"结果详细信息"视图，那么将出现选定结果及其特征。

"结果详细信息"视图

选择结果后，"结果详细信息"视图将显示并允许您修改其属性。通过该视图，您可以修改单个结果。



- 第 148 页的『"详细信息"部分』
- 第 148 页的『"报告"部分（仅在 AppScan Source for Analysis 和 AppScan Source for Development（Eclipse 插件）中可用）』
- 第 148 页的『"注释"部分』
- 第 148 页的『"结果详细信息"视图操作』
- 第 149 页的『定制结果的"结果详细信息"视图（仅在 AppScan Source for Analysis 中可用）』

"详细信息"部分

- **上下文**：漏洞周围的代码片段
- **分类**：明确或可疑安全性结果或者扫描覆盖范围结果，并且具有用于将结果提升为**明确**或还原为原始值（如果分类已更改）的链接
- **漏洞类型**
- **严重性**：高、中、低或参考
- **束**：包含结果的束的名称（在 AppScan Source for Development（Visual Studio 插件）中不可用）

"报告"部分（仅在 AppScan Source for Analysis 和 AppScan Source for Development（Eclipse 插件）中可用）

指定在报告中的结果之前和/或之后要包含的代码行的数量。

"注释"部分

对结果进行注释。

"结果详细信息"视图操作

- **排除**：单击**排除**以从结果表中排除（移除）结果。要查看已排除的结果，请打开"已排除的结果"视图。
- 仅在 AppScan Source for Analysis 中可用：
  - **发送电子邮件**：如果您已配置电子邮件首选项，那么可以通过电子邮件直接将结果束发送给开发者以告知他们扫描后所发现的潜在缺陷。该电子邮件包含束附件（其中含有结果），并且电子邮件文本描述这些结果。
    1. 要通过电子邮件发送"结果详细信息"视图中的当前结果，请单击**发送电子邮件**。
    2. 在"附件文件名"对话框中，指定将附加到电子邮件的结果束的名称。例如，在**附件文件名**字段中指定 `my_finding` 会将文件名为 `my_finding.ozbdl` 的束附加到电子邮件。
    3. 单击**确定**以打开"通过电子邮件发送结果"对话框。缺省情况下，将使用电子邮件首选项中指定的**收件人地址**来填充"通过电子邮件发送结果"对话框中的**收件人**字段，不过，可在准备电子邮件时轻松对其进行更改。在此对话框中，复审电子邮件的内容，然后单击**确定**以发送电子邮件。
  - **提交缺陷**：要将结果提交为缺陷，请单击**提交缺陷**。这将打开"选择缺陷跟踪系统"对话框。
    - 如果选择 **ClearQuest** 并单击**确定**，那么将打开"附件文件名"对话框。在该对话框中，指定将附加到缺陷的结果束的名称，然后单击**确定**。登录到 Rational ClearQuest，然后提交结果。
    - 如果选择 **Quality Center** 并单击**确定**，那么将打开"登录"对话框，使您能够登录到 Quality Center 以提交结果。
    - 如果选择任一 **Team Foundation Server** 选项，那么均将打开一个对话框，提示您登录到缺陷跟踪系统并提供其他配置详细信息。

    注：Rational Team Concert 是 macOS 上唯一受支持的缺陷跟踪系统。

定制结果的"结果详细信息"视图（仅在 AppScan Source for Analysis 中可用）

定制结果的"结果详细信息"视图提供您可以编辑的其他信息：

- 文件
- 行
- 列
- API

此外，对于某些字段，编辑第 148 页的『"详细信息"部分』所用的方法与标准结果不同（例如，定制结果的分类显示在列表中）。

移除结果修改

如果您已修改结果，那么可以使用本主题中描述的方法来移除这些修改（还原为原始值）。

关于此任务

有多种方法来移除结果修改：

- 『在"已修改的结果"视图中移除修改』：此方法要求为含有要移除的修改的应用程序打开评估。当您要还原多个已修改的结果时，此方法很有用。
- 『在包含结果的其他视图中移除修改』：此方法需要已打开的评估 - 在您对结果做出了多项修改并要还原这些更改的一部分的情况下尤其有用。例如，如果您已更改结果的严重性和分类 - 并且要在保留已修改的分类的同时还原为原始严重性 - 那么此方法最合适。
- 第 150 页的『在"属性"视图的"已修改的结果"选项卡中移除修改（仅限 AppScan Source for Analysis）』：如果您要移除对不具有已打开评估的应用程序的修改，那么此方法很有用 - 并且此方法可用来还原多个已修改的结果。

在"已修改的结果"视图中移除修改

过程

1. 在"已修改的结果"视图中，选择要还原的已修改结果。可以使用键盘 Ctrl 和 Shift 键（在 Windows 上）或 Command 和 Shift 键（在 macOS 上）来选择多个结果。
2. 单击**删除修改**，或者右键单击所选内容，然后从菜单中选择**删除修改**。

结果

此操作移除已对结果做出的所有修改。如果您对结果做出了多项修改并要还原这些更改的一部分，请使用『在包含结果的其他视图中移除修改』中描述的方法。

在包含结果的其他视图中移除修改

关于此任务

在包含结果表的任何视图中，您都可以使用**选择列并对其排序**操作来选择要显示的列。使用此功能，可以显示**严重性（原始）**、**严重性（定制）**、**分类（原始）**和**分类（定制）**列。这些列帮助您将修改还原为其原始值（通过结果表中的操作或者通过使

用"结果详细信息"视图）。例如，给定一个**严重性**或**严重性（定制）**的值为**高**，并且**严重性（原始）**值为**中**的结果，那么可以使用诸如以下的多种方法将严重性级别还原为**中**：

- 在结果表中，右键单击结果，然后在菜单中选择**设置严重性 > 中**。
- 选择结果，然后在"结果详细信息"视图中，将**严重性**字段设置为**中**。

在"属性"视图的"已修改的结果"选项卡中移除修改（仅限 AppScan Source for Analysis）

过程

1. 在"资源管理器"视图中，选择包含了要移除的修改的应用程序。
2. 在"已修改的结果"视图中，选择要还原的已修改结果。可以使用键盘 Ctrl 和 Shift 键来选择多个结果。
3. 单击**删除修改**，或者右键单击所选内容，然后从菜单中选择**删除修改**。

结果

此操作移除已对结果做出的所有修改。如果您对结果做出了多项修改并要还原这些更改的一部分，请使用第 149 页的『在包含结果的其他视图中移除修改』中描述的方法。

比较结果

评估是使用**差异评估**操作进行比较的。比较两个评估时，两者之间的差异将显示在"评估差异"视图中。此视图显示新发现结果、已修复/缺失结果以及常见发现结果。

"评估差异"视图中提供了这些控件：

- **差异评估**：显示选定的两个评估之间的差异。
- **新结果**（蓝色）：使用此工具栏按钮可切换对新结果（进行了蓝色标记的评估中的结果，而非进行了绿色标记的评估中的结果）的显示。
- **已修正/缺失结果**（绿色）：使用此工具栏按钮可切换对已修正/缺失结果（进行了绿色标记的评估中的结果，而非进行了蓝色标记的评估中的结果）的显示。
- **常见**（白色）：使用此工具栏按钮可切换两个评估之间常见的发现结果的显示。
- **下一个**：移至新发现结果或已修复/缺失结果的下一个块。
- **上一个**：移至新发现结果或已修复/缺失结果的上一个块

在"评估差异"视图中比较两个评估

过程

1. 在左侧窗格中，选择要比较的两个评估。
2. 单击**差异评估**工具栏按钮，或右键单击所选内容并从菜单中选择**差异评估**。

从主菜单栏中比较两个评估

过程

1. 在主菜单栏中选择**工具 > 差异评估**。
2. 在"差异评估"对话框中，选择两个评估。

3. 单击**确定**以在"评估差异"视图中打开两个评估的比较。

查找"我的评估"视图与"已发布的评估"视图中评估之间的差异

过程

1. 在其中一个视图中选择两个评估。
2. 单击**差异评估**工具栏按钮，或者右键单击所选内容并从菜单中选择**差异评估**。这将在"评估差异"视图中打开两个评估的比较。

定制结果

要增强分析结果，可创建定制结果。这些是用户创建的发现结果，由 AppScan Source for Analysis 将其添加到当前打开的评估或所选的应用程序。定制结果会影响评估度量，并可包含在报告中。创建后，定制发现结果将自动包含在应用程序的将来扫描中。

定制结果的行为取决于创建该项目的视图。

根据"结果"视图中创建时，定制结果：

- 应用于当前已打开的评估。
- 另存为应用程序的一部分，并出现在应用程序属性中。
- 影响同一应用程序的当前扫描和将来扫描。
- 立即影响评估度量。

如果从"属性"视图中创建或者通过为所选应用程序选择**添加定制结果**操作来创建，那么定制结果将：

- 应用于选定应用程序。
- 添加到当前评估（如果该应用程序是已扫描的应用程序）。
- 包含在该应用程序的将来扫描中。

从代码编辑器中创建时：

- 如果评估已打开，那么定制发现结果以在"发现结果"视图中创建时的方式运行。
- 如果评估未打开，那么定制结果以在"属性"视图中创建时的方式运行。

创建定制结果后，AppScan Source for Analysis 将自动保存应用程序。无法在不修改应用程序的情况下修改评估。但是，如果评估未与应用程序关联，那么将不修改任何应用程序。

如果将定制发现结果添加到应用程序，那么这些发现结果将包含在该应用程序的后续扫描中，并且不能将其排除。要除去定制发现结果，必须将其从评估或应用程序中排除。

注： 定制发现结果不能是已修复/缺失的发现结果。

定制发现结果包含以下属性：

- **漏洞类型**（必需）
- **严重性**（必需）
- **分类**（必需）

- **文件**（必需）
- **上下文**
- **行号**
- **列号**
- **API**
- **说明**
- **束**

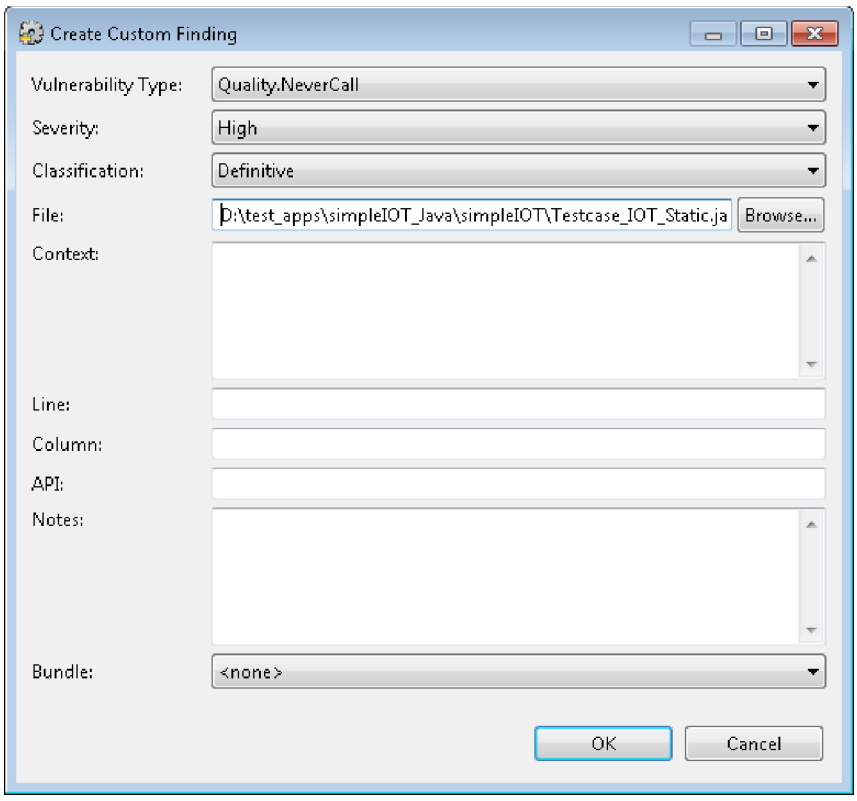
在"属性"视图中创建定制发现结果

从应用程序"属性"视图中创建或编辑定制发现结果将影响当前评估结果和将来的扫描。

过程

1. 在"资源管理器"视图中选择应用程序。
2. 在"属性"视图中，选择**定制发现结果**选项卡。
3. 单击工具栏上的**创建定制结果**。
4. 在"创建定制发现结果"对话框中，添加必需项：
   - **漏洞类型**
   - **严重性**
   - **分类**
   - **文件**

   （可选）添加上下文、行号、列、API、说明和束指定。



5. 单击**确定**将定制结果保存到应用程序。

在"属性"页面中修改或除去定制发现结果

从应用程序"属性"视图中创建或编辑定制发现结果将影响当前评估结果和将来的扫描。

过程

1. 选择发现结果。如果要除去定制发现结果，可选择一组要删除的发现结果。
2. 要修改定制发现结果，请单击工具栏上的**编辑选定发现结果**，然后修改先前定义的发现结果信息。
3. 要除去定制发现结果，请单击工具栏上的**删除选定发现结果**。

在发现结果视图中创建定制发现结果

可从多个发现结果视图（例如"发现结果"和"定制发现结果"视图）创建或管理定制发现结果。

从视图中创建定制结果的操作可将新的结果添加到当前评估，并更新评估度量。

在发现结果视图中添加定制发现结果时，单击视图的**创建定制发现结果**工具栏按钮。这将打开"创建定制发现结果"对话框，完成该对话框的方式与第 152 页的『在"属性"视图中创建定制发现结果』中描述的方式相同。

要除去定制发现结果，必须将其从评估中排除或者将其从应用程序删除，或者通过遵循『在"属性"页面中修改或除去定制发现结果』中的指示信息。这些操作在其他发现结果视图中不可用。

在源代码编辑器中创建定制发现结果

关于此任务

使用源代码编辑器添加定制发现结果时，以下条件适用：

- 如果源代码编辑器中的可视源文件属于当前打开的评估，那么定制发现结果将添加到该评估以及关联的应用程序。
- 如果定制发现结果不属于当前打开的评估，那么定制发现结果仅添加到包含该源文件的应用程序。
- 如果源文件属于多个应用程序，或者 AppScan Source for Analysis 无法确定应用程序，那么您必须选择适当的应用程序。

如果从源代码编辑器创建定制发现结果，那么"创建定制发现结果"对话框将预填充编辑器中的信息。

- **文件**：当前打开的文件的名称
- **上下文**：编辑器中的任何选定文本。如果文本未选定，那么上下文为光标当前所在行。如果选定了多行，那么所有选定行都将成为上下文。
- **行**号和**列**号：当前行号和列号

要从编辑器创建定制结果，请执行以下操作：

过程

1. 选择要添加为定制结果的代码行。

2. 右键单击所选内容，并从菜单中选择**创建定制结果**。"创建定制发现结果"对话框将填充文件、上下文、列号和行号。
3. 选择**漏洞类型**、**严重性**和**分类**。（可选）添加 API、说明或束指定。
4. 单击**确定**。

解决安全问题以及查看修复帮助

AppScan Source 针对安全错误或常见设计缺陷向您发出警报，并在解决过程中提供帮助。AppScan Source 安全知识库以及内部或外部代码编辑器可帮助执行此过程。

关于此任务

AppScan Source 安全知识库提供关于更正结果的建议。每个漏洞的此上下文中情报均提供关于根本原因、风险严重性以及可操作修复建议的准确描述。例如，它将 `strcpy()`（一种"缓冲区溢出"类型）描述为具有高严重性级别，并提供以下修复帮助：

> `strcpy` 易受目标缓冲区溢出影响，因为它不知道目标缓冲区的长度，从而无法进行检查以确保它不会覆盖此缓冲区。您应该考虑使用可采用长度参数的 `strncpy`。`strncpy` 也会带来安全风险，尽管程度较低。

要查看 AppScan Source 安全知识库，请执行以下操作：

过程

- 在 AppScan Source for Analysis 中，打开"修复帮助"视图，然后在结果表中选择一个结果。将显示该特定结果的修复帮助。或者，从主菜单栏中选择**帮助** > **安全知识库**以在浏览器中打开整个 AppScan Source 安全知识库。
- 在 AppScan Source for Development（Eclipse 插件） 中，打开"修复帮助"视图，然后在结果表中选择一个结果。将显示该特定结果的修复帮助。
- 在 AppScan Source for Development（Visual Studio 插件）中，选择结果表中的一个结果。从主菜单栏中选择**IBM Security AppScan Source** > **知识库帮助**，或者右键单击此结果并从菜单选择**知识库帮助**。这将打开所选结果的修复帮助。

在编辑器中分析源代码

通过 AppScan Source，您可以在内部编辑器中分析或修改源代码，也可以从各种外部编辑器中进行选择。

通过外部编辑器，可以在 AppScan Source for Analysis 中复审结果并在您选择的开发环境中作出代码修改。外部编辑器有：

表 *13.* 受支持的外部编辑器

编辑器	平台
Eclipse（请参阅 AppScan Source 系统需求以了解哪些版本的 Eclipse 受支持）	Windows 和 Linux
记事本	Windows
vi	Linux
系统缺省	Windows 和 Linux

注： 不可编辑 `WAR` 文件中的源文件。

要在编辑器中查看/修改源代码，请选择以下某个选项：

- 在结果表中双击发现内容。内部编辑器将在代码行处打开。
- 右键单击结果表中的结果，然后选择**在内部编辑器中打开**或**在外部编辑器中打开** > **<editor>**（其中，**<editor>** 是上表中所列的受支持的外部编辑器）。
- 选择跟踪节点，然后选择**在内部编辑器中打开**或**在外部编辑器中打开** > **<editor>** 工具栏按钮，或右键单击所选内容并从菜单中选择**在内部编辑器中打开**或**在外部编辑器中打开** > **<editor>**。

如果已在编辑器中打开某个文件，那么标记将指示该文件中代表发现结果的位置。要从这些位置追溯到结果表，请右键单击编辑器中的相应代码行，然后从菜单中选择**在发现结果视图中显示**。

支持的注释和属性

扫描期间将处理用于修饰代码的一些注释或属性。如果扫描期间在代码内找到受支持的注释或属性，那么会使用该信息将已修饰方法标记为受感染回调。标记为受感染回调的方法将被视为其所有参数都包含受感染的数据。这会使得跟踪发现更多内容。本帮助主题中列出了受支持的注释和属性。

- 『受支持的 Java 注释』
- 『受支持的 AppScan Source Java 注释』
- 第 157 页的『受支持的 Microsoft .NET 属性』

受支持的 Java 注释

表 *14.* 受支持的 *Java* 注释

注释	缩写词
javax.xml.ws.WebServiceProvider	@WebServiceProvider
javax.jws.WebService	@WebService
javax.jws.WebMethod	@WebMethod

受支持的 AppScan Source Java 注释

- 『使用 AppScan Source 注释』
- 第 156 页的『@ValidatorMethod』
- 第 156 页的『@SuppressSecurityTrace』
- 第 156 页的『@CallbackMethod』

使用 AppScan Source 来扫描 Java 时，@ValidatorMethod、@CallbackMethod 和 @SuppressSecurityTrace 方法级别注释受支持。

使用 AppScan Source 注释

可通过以下步骤来使用注释：

1. 缺省情况下，启用了注释的支持。注释 .jar 文件位于 <install_dir>\lib\SecurityAnnotations.jar（其中 <install_dir> 是 AppScan Source 安装位置）中。

2. 如果要扫描预编译类、.war 文件或 .jar 文件，那么找到包含附注释的源代码的 Java 项目。
3. 将 SecurityAnnotations.jar 添加到项目的类路径。
4. 重新构建项目。

注释可在扫描之前添加到源代码，或在扫描之后和类选期间进行添加以识别和消除假的正面值。

提供注释是为了让您能够直接以安全性注释的形式在源代码中插入您的知识。因为注释可用于声明代码安全的部分，所以使用它们时应非常小心。它们不应用于会被扫描以查找安全漏洞的代码。如果使用注释，安全分析人员可通过禁用 <data_dir>\config\scanner.ozsettings（其中 <data_dir> 是 AppScan Source 程序数据的位置，如第 275 页的『安装和用户数据文件位置』中所述） 中的功能来忽略这些注释。在此文件中，找到以下设置：

```
<Setting
name="process_security_annotations"
value="true"
default_value="true"
description="When turned on, security annotations in the
     source code will be processed by AppScan Source."
display_name="Process Security Annotations"
type="bool"
/>
```

要禁用该功能，将 value="true" 更改为 value="false"。

@ValidatorMethod

Validator 是对数据数据执行检查并通常返回代表输入是否有效的布尔值的方法。您可以将输入数据更改为可接受的格式，而不是接受或拒绝使用 validator 的输入。这些方法称为 sanitizer。

通过使用 @ValidatorMethod 注释，可识别应用程序源代码中的所有 validator 和 sanitizer 方法。在 AppScan Source 扫描期间，该信息将用于除去自数据被认为安全以来流经这些方法的数据流。

注：当前，没有任何规定来指定附注释的方法的哪些参数应被认为是已经过验证的。在 AppScan Source 扫描期间，所有输入参数都将被认为已经过验证。

@SuppressSecurityTrace

将除去流经通过该注释标记的方法的所有跟踪。当特定跟踪组标识为假阳性或者没有其他跟踪重要或有趣时，这非常有用。您可以使用该注释来过滤出这些跟踪或隐藏这些跟踪以减少混乱。

@CallbackMethod

该注释用于识别应用程序的回调或入口点。所有参数都被认为包含污点。

受支持的 Microsoft .NET 属性

表 15. 受支持的 *Microsoft .NET* 属性

属性	缩写词
System.Web.Services.WebServiceAttribute	WebService
System.Web.Services.WebMethodAttribute	WebMethod

第 6 章 AppScan Source 跟踪

利用 AppScan Source 跟踪，您可以确认符合您的软件安全性策略的输入验证和编码。可查看将产生输入/输出跟踪的结果，并可将方法标记为验证和编码例程、源/接收器、回调或感染传播器。

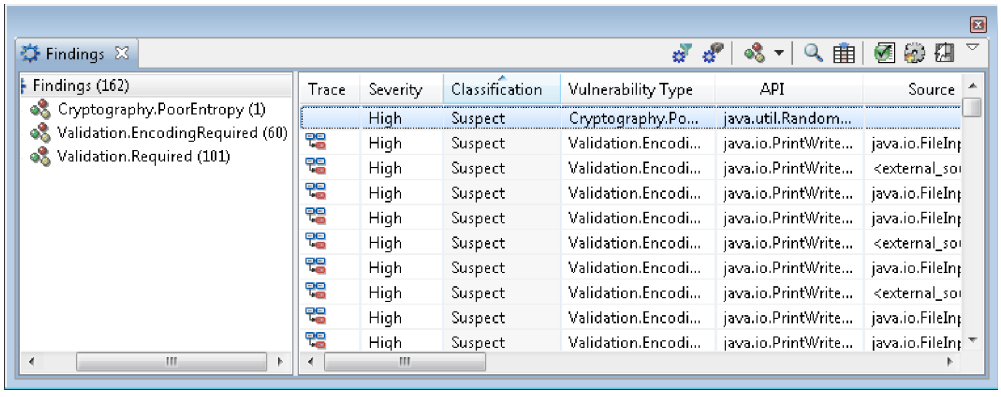
AppScan Source 在整个应用程序中跨模块和语言地跟踪数据流。它在调用图中显示可能不安全的数据的路径，并指示应用程序中可能易受漏洞影响的方面。

跟踪可标识应用程序中是否缺少已核准的输入验证和编码例程，从而帮助您击败 SQL 注入、跨站点脚本编制和其他输入验证攻击。您可交互地跟踪整个调用图，直接从"跟踪"视图中进行单击，以在所选开发环境或代码编辑器中查看源代码。通过跟踪还可实施策略，允许您识别正确输入验证和编码所需的核准例程、感染传播或接收器和源，并在未来扫描时使用。

扫描产生跟踪时，您可以为"跟踪"视图中的特定结果创建输入验证或编码例程、漏洞、接收器、源或感染传播器。例如，如果在 AppScan Source for Analysis 中将某个例程标记为验证例程，并将其添加到 AppScan Source 安全知识库，那么后续扫描便不再为调用此例程的数据路径报告 `Validation.Required` 或 `Validation.Encoding.Required` 结果。在跟踪视图中，您还可以将漏洞定义为源和/或接收器，并将某个方法标识为感染传播器、感染的回调或不易受感染。

AppScan Source 跟踪扫描结果

扫描结果可能包含由 AppScan Source 跟踪标识的跟踪。**跟踪**列中的图标指示存在调用图的跟踪。



扫描可能生成类型为 `Validation.Required` 和 `Validation.EncodingRequired` 的结果。这些结果指示源代码中从外部源读取数据或将数据保存到外部接收器的位置。扫描将标记这些情况，因为数据应该进行验证或编码以防止恶意或错误数据造成损害。

验证和编码

验证是检查输入数据以确保其格式良好的过程。`Validation.Required` 发现指示沿着从源到接收器的给定数据路径没有发生验证。验证可以很简单，就是将数据绑定到最大

© Copyright IBM Corp. 2003, 2017

长度，也可以很复杂，要检查名称和地址是否格式良好。验证还可以通过检测启用这些攻击的非法字符序列来检查攻击，例如：SQL 注入。

编码是将数据变换为格式良好的状态的过程。Validation.EncodingRequired 发现指示沿着从源到接收器的给定数据路径没有发生编码。编码可以很简单，就是转义字符，也可以很复杂，要加密数据。编码还可以通过将导致这些攻击的字符转义来阻止攻击，例如：跨站点脚本编制。

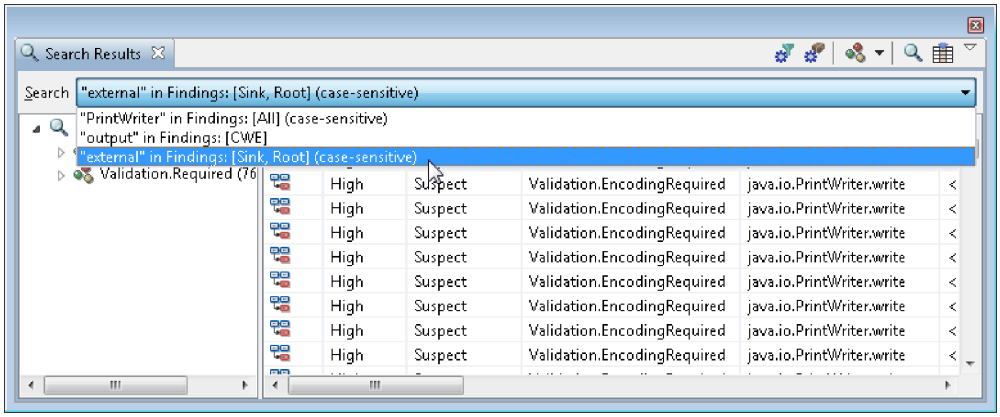
首次扫描时，AppScan Source 可能会将结果标识为可疑安全性结果。当您创建应用于特定源代码的验证或编码例程时，如果 AppScan Source for Analysis 在从此源代码接收到数据后该指定验证或编码例程未被调用，那么它会将此结果报告为明确结果（而不是可疑结果）。

评估跟踪整个项目中已知源的数据。如果可以从已知源跟踪数据到已知接收器，那么指定的验证和编码例程可以确保不会以极大的输入数据进行恶意攻击。

搜索 AppScan Source 跟踪

如果您希望将跟踪结果分组，可以搜索源或接收器。这会导致跟踪发现结果出现在"搜索结果"视图中。

在"跟踪"视图中，单击**搜索带有相同类型例程的跟踪**。然后，在"搜索发现结果"对话框中，选择源、接收器、丢失的接收器（包括虚拟丢失的接收器）、虚拟丢失的接收器或跟踪调用，以将结果隔离到包含该字符串的跟踪。在"搜索结果"视图中显示累积的搜索结果。从此视图，您可以再次搜索以优化搜索。



输入/输出跟踪

当 AppScan Source for Analysis 可以跟踪从已知源到接收器或丢失的接收器的数据时，会生成输入/输出跟踪。

输入/输出跟踪

如果代码分析可以跟踪感染的源到接收器或丢失的接收器，那么分析将生成输入/输出跟踪。跟踪的原理是从感染源获取数据并将其传递到一系列调用（最终写入不受保护的接收器）的方法。

源和接收器

- **源**：源是对程序的输入，如文件、servlet 请求、控制台输入或套接字。对于大多数输入源，返回的数据在内容和长度方面没有限制。在未检查某个输入的情况下，会将其视为已感染。源列在任一结果表的**源**列中。
- **接收器**：接收器可以是数据能够写为的任意外部格式。接收器示例包括数据库、文件、控制台输出和套接字。数据未经检查就写入接收器可能预示着严重的安全漏洞。
- **丢失的接收器**：丢失的接收器是指无法继续跟踪的 API 方法。

  注：丢失的接收器不适用于 JavaScript 结果。

使用"跟踪"视图

关于此任务

在"跟踪"视图中，可查看单个输入/输出跟踪以查找结果。此窗格划分为三个面板：

- 输入和输出堆栈
- 数据流
- 图形调用图

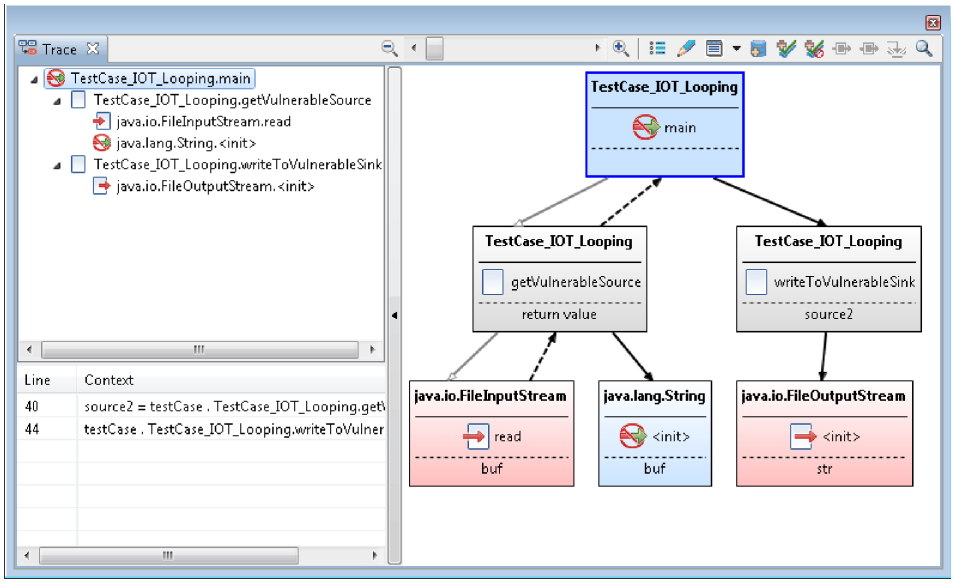
在第 162 页的『"跟踪"视图中的输入/输出堆栈』中更详细地描述了这些面板。

注：在 JavaScript 跟踪中，将显示 第 163 页的『JavaScript 语句图』 而非图形调用图。

要查看 AppScan Source 跟踪：

过程

1. 在"结果"视图中扫描和查找跟踪结果。
2. 从"视图"菜单，打开"跟踪"视图。
3. 选择结果表中显示**跟踪**图标的行。"跟踪"视图将显示跟踪详细信息。



"跟踪"视图中的输入/输出堆栈

左上方的面板显示**输入**和**输出**堆栈。堆栈是在源（输入堆栈）或接收器（输出堆栈）处终止的调用序列。

数据流

左下方的面板包含所选方法的数据流。数据可以流经方法调用或分配。"数据流"部分显示了项和上下文在源代码中出现的行号。

调用图

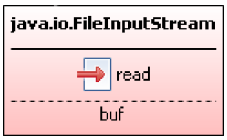
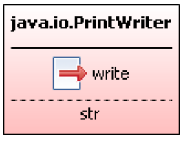
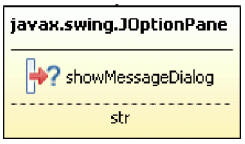
注：在 JavaScript 跟踪中，将显示 第 163 页的『JavaScript 语句图』 而非图形调用图。

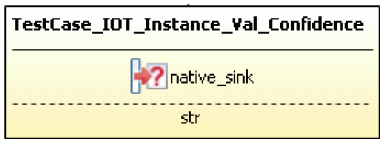
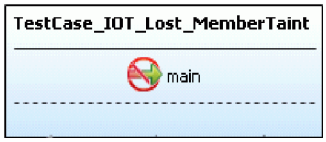
图表是调用图的图形表示法。每个方法调用都是图形内显示类名和方法名称的一个矩形：

- 红色将方法调用标识为源和/或接收器。
- 丢失的接收器是无法继续跟踪的 API 方法。虚拟丢失的接收器是丢失的接收器，同时又是虚函数（可具有多个实现的函数）。如果为黄色，指示方法调用是丢失的接收器或虚拟丢失的接收器。
- 如果为蓝色，则指示方法调用不是验证/编码例程。
- 如果为灰色，则代表所有其他跟踪节点类型。

每个方法调用都划分为三个部分：类名、方法名称和已感染参数的名称。方法调用的悬浮式文本提供了更详细的信息。

带箭头的行表示从方法到方法的调用。空心箭头指示在调用中不存在已知的感染数据，而实心箭头指示感染的数据流。虚线箭头指示 return 语句。

符号	描述
	没有已知感染数据的方法调用
	带有感染数据的方法调用
	带有感染数据的返回
	源（红色）：作为潜在不可信数据的起源的方法、函数或参数。
	接收器（红色）：对于已感染数据可能存在漏洞或在使用时可能很危险的方法或函数。
	丢失的接收器（黄色）：一种方法/函数，对于已感染数据可能存在漏洞或在使用时可能很危险。

符号	描述
	虚拟丢失的接收器（黄色）：一种丢失的接收器，解析为多个具体实现。
	非验证/编码例程（蓝色）。如果将 API 标记为非验证/编码例程，即标识此 API 不会验证任何数据。
	感染传播器：将感染传播到其一个或多个参数、其返回值或 this 指针的一种函数/方法。

提示：

- 在"跟踪"视图中，将鼠标悬停在图形中的跟踪节点上将提供关于此节点的信息。
- 该视图中的两个左面板（输入/输出堆栈面板和数据流面板）可折叠以便更容易查看图形调用图。要折叠这些面板，请选择**隐藏树视图**箭头按钮。要在这些面板被隐藏时显示它们，请选择**显示树视图**箭头按钮。
- 移动滚动条可放大并聚焦于详细信息，或者缩小以查看更多内容。将鼠标悬浮在缩放滚动条上将提供当前缩放级别。要放大到最高级别，请单击**放大到 200%**。要尽可能缩小，请单击**缩放到适合**。

JavaScript 语句图

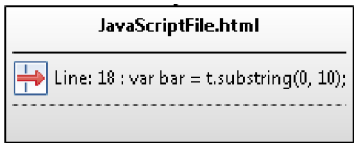
JavaScript 跟踪的语句图部分显示语句之间的数据流。

在图中，每个语句是提供以下信息的矩形：

- 受影响文件的路径和文件名。如果下一个语句位于同一文件中，那么仅列出文件名。
- 包含语句的行号。
- 如果可用，则为感兴趣的代码部分。
- 如果矩形为红色，语句为源和/或接收器。
- 如果矩形为灰色，那么语句为污点传播程序。
- 语句的悬浮式文本提供了更详细的信息。

带箭头的行表示从语句到语句的数据流。

符号	描述
	感染数据流
	源（红色）：作为潜在不可信数据的起源的语句。

符号	描述
	接收器（红色）：对于已感染数据可能存在漏洞或在使用时可能很危险的语句。
	感染传播器：将感染传播到其一个或多个参数、其返回值或 this 指针的一种语句。

提示：

- 在"跟踪"视图中，将鼠标悬停在图形中的跟踪节点上将提供关于此节点的信息。
- 该视图中的两个左面板（输入/输出堆栈面板和数据流面板）可折叠以便更容易查看图形调用图。要折叠这些面板，请选择**隐藏树视图**箭头按钮。要在这些面板被隐藏时显示它们，请选择**显示树视图**箭头按钮。
- 移动滚动条可放大并聚焦于详细信息，或者缩小以查看更多内容。将鼠标悬浮在缩放滚动条上将提供当前缩放级别。要放大到最高级别，请单击**放大到 200%**。要尽可能缩小，请单击**缩放到适合**。

在编辑器中分析源代码

通过 AppScan Source，您可以在内部编辑器中分析或修改源代码，也可以从各种外部编辑器中进行选择。

通过外部编辑器，可以在 AppScan Source for Analysis 中复审结果并在您选择的开发环境中作出代码修改。外部编辑器有：

表 *16.* 受支持的外部编辑器

编辑器	平台
Eclipse（请参阅 AppScan Source 系统需求以了解哪些版本的 Eclipse 受支持）	Windows 和 Linux
记事本	Windows
vi	Linux
系统缺省	Windows 和 Linux

注： 不可编辑 WAR 文件中的源文件。

要在编辑器中查看/修改源代码，请选择以下某个选项：

- 在结果表中双击发现内容。内部编辑器将在代码行处打开。
- 右键单击结果表中的结果，然后选择**在内部编辑器中打开**或**在外部编辑器中打开** > **<editor>**（其中，**<editor>** 是上表中所列的受支持的外部编辑器）。
- 选择跟踪节点，然后选择**在内部编辑器中打开**或**在外部编辑器中打开** > **<editor>** 工具栏按钮，或右键单击所选内容并从菜单中选择**在内部编辑器中打开**或**在外部编辑器中打开** > **<editor>**。

如果已在编辑器中打开某个文件，那么标记将指示该文件中代表发现结果的位置。要从这些位置追溯到结果表，请右键单击编辑器中的相应代码行，然后从菜单中选择**在发现结果视图中显示**。

验证和编码作用域

从"跟踪"视图，可以指定定制验证和编码例程，这些例程一旦存储在 AppScan Source 安全知识库中，就会将数据标记为已检查而不是已感染。通过"定制规则向导"，可基于这些例程的作用域对其进行定义。

请参阅第 175 页的『示例 4：深度验证』以了解用于创建验证和编码例程的过程。

验证或编码例程基于其作用域并定义为：

- 『特定于 API』
- 『特定于调用站点』

特定于 API

特定于 API 的验证和编码例程可能与单个项目或多个项目相关联。

特定于 API 的例程将清洁来自特定源 API 的所有实例的任何数据。例如，您可以指定针对 API 的任何输入的验证例程：

```
javax.servlet.ServletRequest.getParameter
(java.lang.string):java.lang.string
```

特定于 API 的例程存储在服务器上。某个项目的特定于 API 的例程存储在该项目中。

特定于调用站点

特定于调用站点的例程始终与单个项目相关联。

特定于调用站点的例程将清洁来自代码中特定位置的数据。创建特定于调用站点的验证或编码例程时，您指定该例程应用于特定输入调用站点。特定于调用站点的例程始终存储在项目中。

注："特定于调用站点"应用于对同一方法内验证例程的任何调用。

从 AppScan Source 跟踪创建定制规则

您可以从"跟踪"视图创建定制规则，这样允许您可以使用跟踪来过滤感染传播器（而不是易受感染的影响）或接收器的结果。您还可以在跟踪中将方法标记为验证/编码例程（或指出它们是非验证/编码例程的）。

关于此任务

请参阅第 170 页的『示例 2：从"跟踪"视图创建验证/编码例程』以了解源代码示例、输出以及用于创建验证和编码例程的过程。

表 17. "跟踪"视图节点的有效标记

所选方法	有效标记
中间节点	• 验证/编码例程 • 不易受感染 • 非验证/编码例程
丢失的接收器	• 感染传播器 • 不易受感染 • 接收器

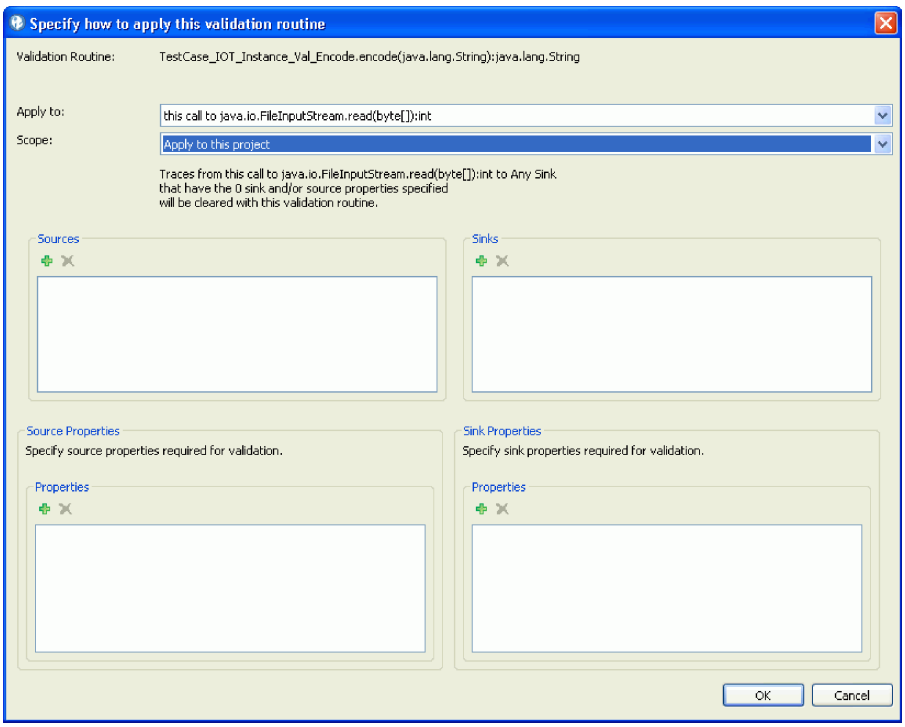
过程

1. 在"跟踪"视图中，右键单击要创建定制规则的方法或节点，然后选择要创建的定制规则 - 或者选择方法或节点，然后单击相应定制规则工具栏按钮。用于标记例程和方法的选项为：

选项	描述
标记为验证/编码例程	
标记为非验证/编码例程	
标记为感染传播器	
标记为不易受感染	
标记为接收器	

   注：如果"跟踪"视图中没有您要创建定制规则所需方法的条目，请单击**启动定制规则向导来添加跟踪视图中不存在的验证例程**。在"定制规则向导"中，前进到"选择验证/编码例程"例程。根据下一步骤中的指示信息选择验证例程，然后指定位置、作用域、任何源或接收器或任何属性。有关使用此向导创建验证例程的详细信息，请参阅第 173 页的『示例 2：从定制规则向导创建验证/编码例程』。

2. 如果您正在创建将方法标记为接收器或验证/编码例程的定制规则，您可能需要进一步设置：
   a. 如果将此方法标记为接收器，请指定接收器属性：
      - **漏洞类型**
      - **严重性**
   b. 对于验证例程，请指定验证例程应该应用的位置和作用域及任何源或接收器或他们的属性。



- **应用于**：
  - **对 <method name> 的此调用**（特定于调用站点）：仅应用于此调用的输入。
  - **任何调用 <method name>**（特定于 API）：应用于方法的任何调用的验证/编码例程。
  - **未考虑<方法名称>，下面显示了指定的所有约束**：允许所有资源均受规则影响。
- **作用域**：
  - **应用于该项目**：选中后，规则将存储在该项目中 (.ppf) 文件。
  - **应用于所有项目**：使用该设置创建的验证规则存储在数据库中。
- **源**：选择要应用于验证例程的一个或多个输入源。要添加源，请单击**添加**，然后从"选择特征符"对话框中选择源。要添加多个源，您可以在"选择特征符"对话框中选中多个源。
- **接收器**：选择验证例程要应用的一个或多个接收器。要添加接收器，请单击**添加**，然后从"选择特征符"对话框中选择接收器。要添加多个接收器，您可以在"选择特征符"对话框中选中多个接收器。
- **源属性**：如果希望规则清除在带有特定属性的源中开始的跟踪，请单击**添加 VWAT 属性**，然后从"选择属性"对话框中选择该属性。要添加多个属性，可以在"选择属性"对话框中选中多个属性。
- **接收器属性**：如果您希望规则过滤掉在带有特定属性的接收器中结束的跟踪，请单击**添加 VWAT 属性**，然后从"选择属性"对话框中选择属性。要添加多个属性，可以在"选择属性"对话框中选中多个属性。

3. 在"跟踪"视图创建定制规则后，您必须再次扫描您的代码以查看结果列表和跟踪中反映的规则。您在"跟踪"视图中创建的定制规则可在"定制规则"视图中进行查看和删除。要查看"定制规则"视图中规则的详细信息，请选择规则，然后单击**定制规则信息**。

用于跟踪的代码示例

本部分提供了代码示例，用于演示如何跟踪从源到接收器的感染数据，以及如何创建验证和编码例程。

示例 1：从源到接收器

在以下代码样本中，main 方法调用方法 getVulnerableSource，后者返回一个字符串。请注意，虽然该方法从完全未知的文件读取数据，但是它从不检查所返回数据的有效性。然后，main 方法将此感染的数据传递到 writeToVulnerableSink 中。writeToVulnerableSink 方法将数据写出到文件，从不检查其有效性。

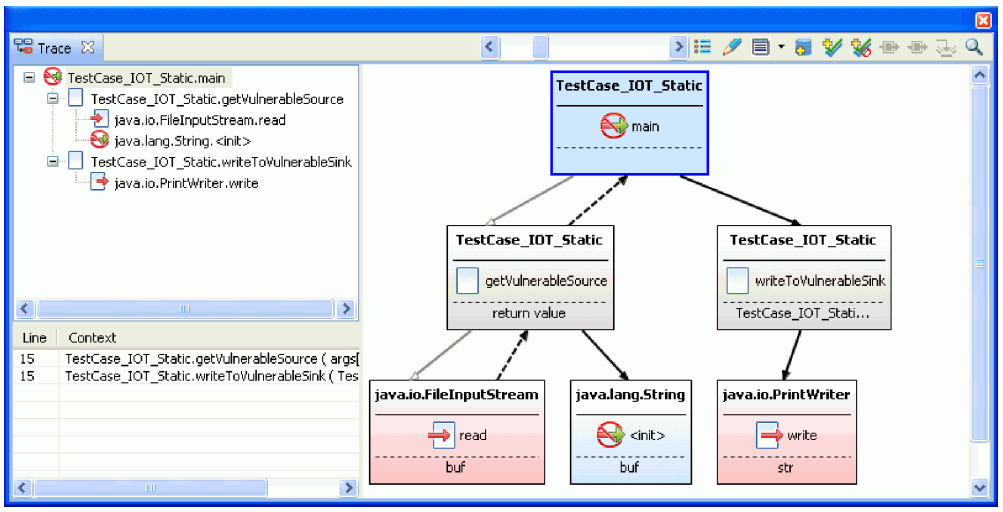
```
import java.io.*;

public class TestCase_IOT_Static {
   public static void main(String[] args) {
    try {
      writeToVulnerableSink(getVulnerableSource(args[0]));
      } catch (Exception e) {
    }
  }

   public static String getVulnerableSource(String file)
      throws java.io.IOException, java.io.FileNotFoundException {
      FileInputStream fis = new FileInputStream(file);
      byte[] buf = new byte[100];
      fis.read(buf);
      String ret = new String(buf);
      fis.close();
      return ret;
  }

  public static void writeToVulnerableSink(String str)
      throws java.io.FileNotFoundException {
      FileOutputStream fos = new FileOutputStream(str);
      PrintWriter writer = new PrintWriter(fos);
      writer.write(str);
  }
}
```

代码样本生成以下跟踪：



该窗格显示输入堆栈（其中 main 调用 getVulnerableSource，后者调用 FileInputStream.read）和输出堆栈（其中 main 调用 writeToVulnerableSink，后者调用 PrintWriter.write）。该图形显示数据如何从 read 方法流到 write 方法（通过 main 连接两个调用堆栈）。"数据流"部分显示了 main 方法的操作中传递感染的行号。在此示例中，两个方法调用存在于方法内的同一行（第 15 行）上（在上面的样本代码中，这将转换为第 7 行，因为在截屏中，文件包含 8 行注释）。

示例 2：从源到接收器的修改版

示例 2 是示例 1 代码的修改版。它通过添加名为 getVulnerableSource 的验证例程和名为 writeToVulnerableSink 的编码例程来增强示例 1。

```
import java.io.*;

public class TestCase_IOT_Instance_Val_Encode {
   public static void main(String[] args) {
    try {
      TestCase_IOT_Instance_Val_Encode testCase = new
        TestCase_IOT_Instance_Val_Encode();
         String file = args[0];
         String source = testCase.getVulnerableSource(file);
      source = testCase.validate(source);
      String encodedStr = testCase.encode(source);
      testCase.writeToVulnerableSink(file, encodedStr);
      } catch (Exception e) {
    }
  }

   public String getVulnerableSource(String file) throws Exception {
      FileInputStream fis = new FileInputStream(file);
      byte[] buf = new byte[100];
      fis.read(buf);
      fis.close();

      String ret = new String(buf);
      return ret;
  }

   public void writeToVulnerableSink(String file, String str)
         throws FileNotFoundException {
      FileOutputStream fos = new FileOutputStream(file);
      PrintWriter writer = new PrintWriter(fos);
      writer.write(str);
  }
```

```
  private String validate(String source) throws Exception {
      if (source.length() > 100) {
         throw new Exception("Length too long: " + source.length());
    }
  return source;
  }

   private String encode(String source) {
      return source.trim();
  }
}
```

第一个扫描生成的堆栈跟踪类似于示例 1 中的堆栈跟踪。

将知识库扩展为包含验证和编码例程将减少结果中的干扰，并确保为所有调用图都调用了验证和编码例程。例如，如果在先前示例中指定了来自对 java.io.FileInputStream.read(byte[]):int 的任何调用的数据，那么该扫描会从 read 中消除也调用了此验证例程的任何调用。而且，来自 read 的并未调用定制验证方法的调用将提升到明确安全性结果状态，因为在代码中不调用已知的验证方法可能会导致恶意攻击。

验证例程还可以验证 FileInputStreamread 方法的其他变量。这些可以指定为其他源。此外，您还可以了解只有特定的接收器（或带有特定属性的接收器）可通过此方法验证。例如，该例程可限制属性为 Technology.IO 的接收器，如 PrintWriter.write 接收器，用于消耗该示例数据。

示例 2：从"跟踪"视图创建验证/编码例程

关于此任务

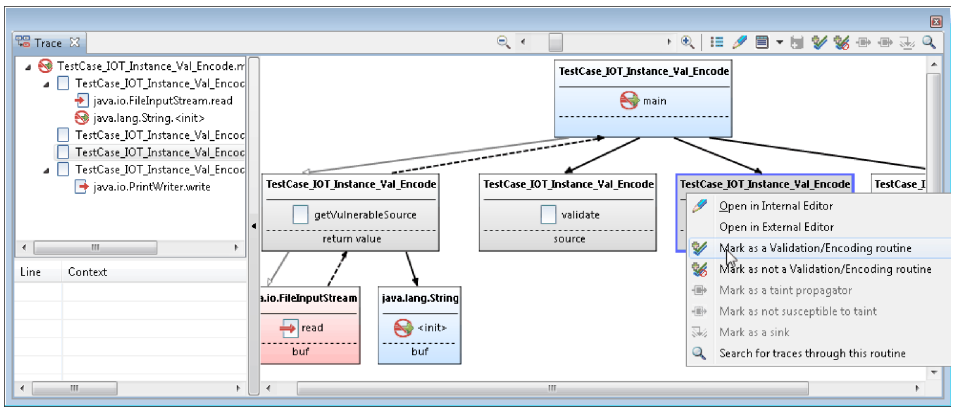
由于 AppScan Source 跟踪 将 FileInputStream.read 方法标识为生成感染数据的源，因此您应该创建验证或编码例程以从未来的扫描中消除此结果。

要为 FileInputStream.read 创建输入验证例程：

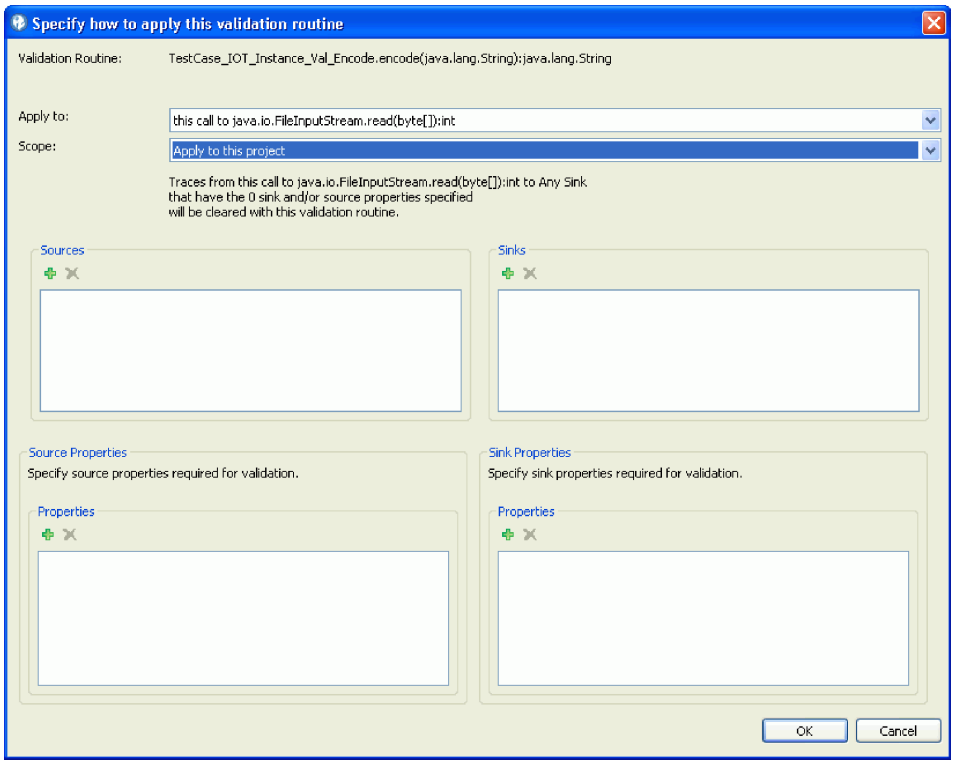
过程

1. 在"跟踪"视图调用图中，选择并右键单击 TestCase_IOT_Instance_Val_Encode.encode 方法。

   提示：如果要创建的验证/编码例程没有出现在跟踪图形中，您可以通过从"跟踪"视图启动"定制规则向导"来创建该例程。第 173 页的『示例 2：从定制规则向导创建验证/编码例程』解释了执行此操作所包含的步骤。
2. 在菜单中选择**标记为验证/编码例程**。



3. 如果 encode 例程仅应用于调用 FileInputStream.read 的此特定实例，请在"指定如何应用此验证例程"对话框中选择**对 java.io.FileInputStream.read 的此调用**。



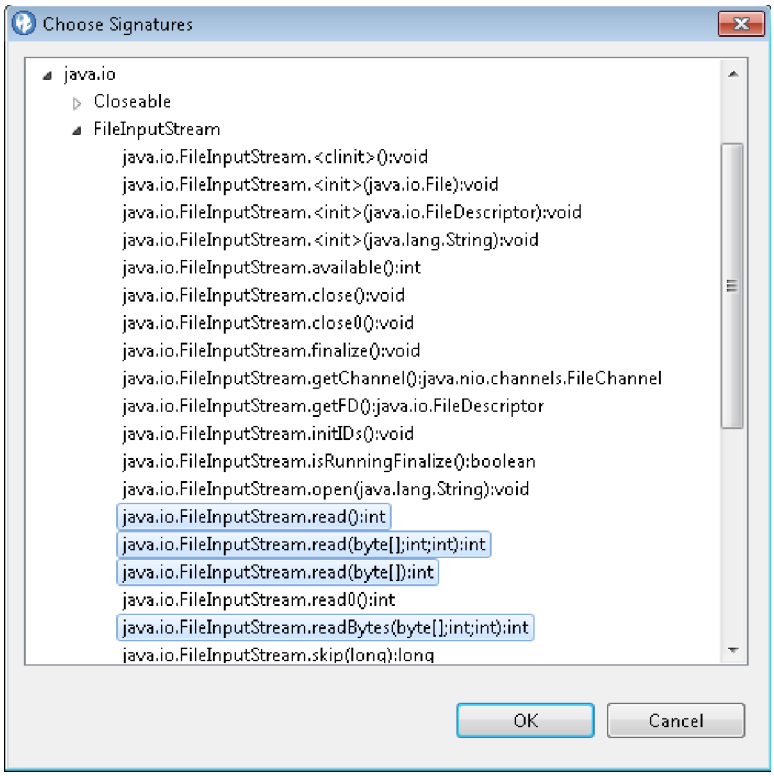
通常，您将指定**对 java.io.FileInputStream.read 的此调用**，因为 validate 方法是该类的私有方法并且与代码紧密关联。

选择**对 java.io.FileInputStream.read 的任何调用**以将验证例程应用于对 read 方法的任何调用。选择此选项时，还请选择**应用于此项目**（如果这仅对当前项目有效）或者**应用于所有项目**。

4. 将例程设置为应用于 FileInputStream 类的所有 read 方法以及带有 Technology.IO 属性的任何接收器（如 java.io.PrintWrite.write 方法）：

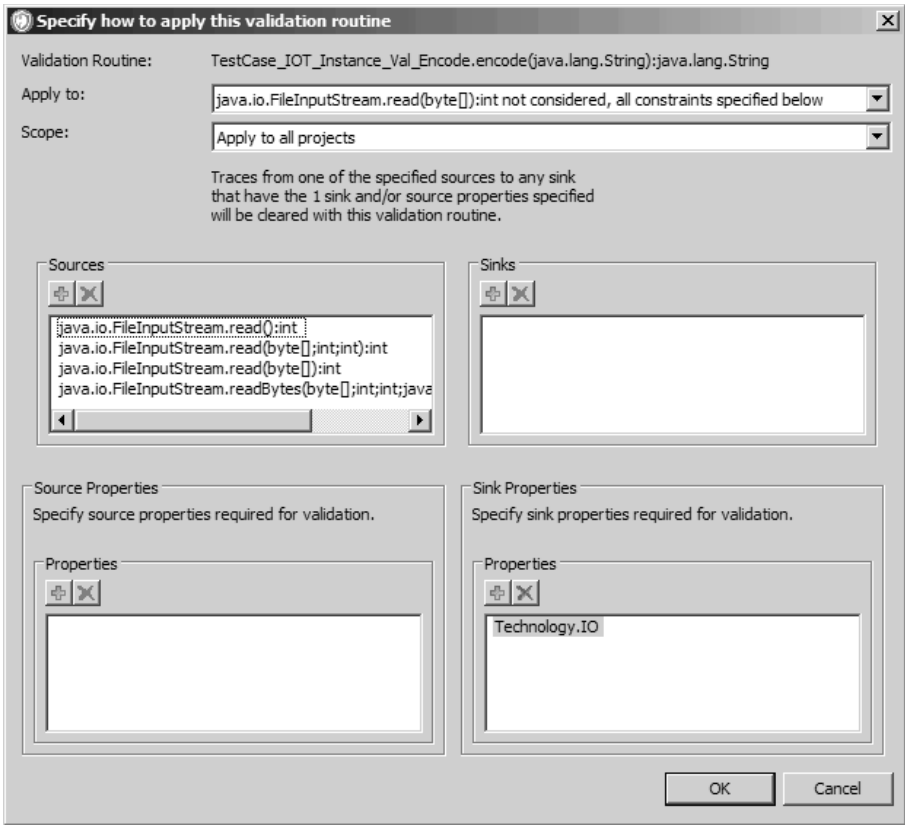
   a. **将 read 方法添加为源**：尽管您可以指定**对 java.io.FileInputStream.read (byte[]):int 的任何调用**以将 java.io.FileInputStream.read(byte[]):int 添加为源，但是我们将改为逐个添加源。在"指定如何应用此验证例程"对话框的

应用于菜单中选择**未考虑 java.io.FileInputStream.read(byte[]):int，下面指定了所有约束**。然后，单击**源**部分**添加**按钮。在"选择特征符"对话框中，展开 java.io，然后展开 FileInputStream 部分。多项选中 java.io.FileInputStream.read* 节点，然后单击**确定**。



b. **添加接收器属性**：单击**接收器属性**部分的**添加 VMAT 属性**按钮。在"选择属性"对话框中，选择 Technology.IO 属性，然后单击**确定**。

c. 完成所有设置后，对话框应类似于如下所示：



5. 单击**确定**将验证例程添加到数据库。

示例 2：从定制规则向导创建验证/编码例程

如果要创建的验证/编码例程没有出现在跟踪图形中，您可以通过从"跟踪"视图启动"定制规则向导"来创建该例程。

关于此任务

该示例将创建与第 170 页的『示例 2：从"跟踪"视图创建验证/编码例程』中创建的相同验证例程，但是，在该示例中，该例程将使用"定制规则向导"创建。

过程

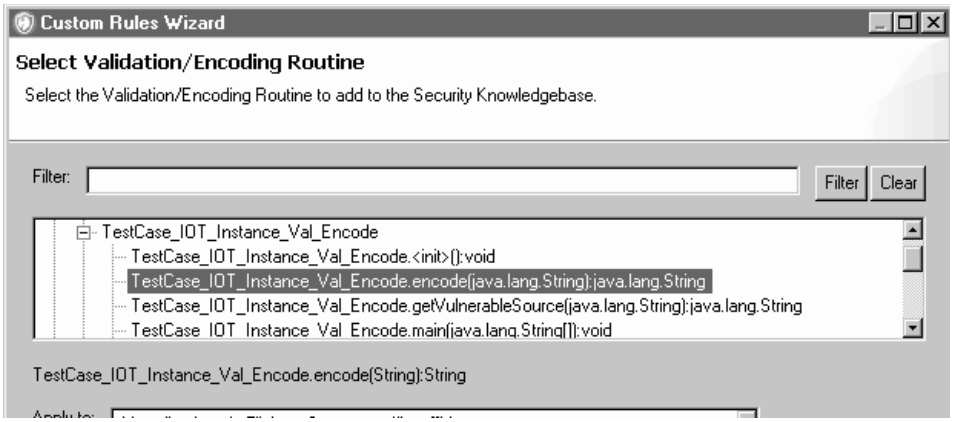
1. 在"跟踪"视图中，单击工具栏上的**启动定制规则向导来添加跟踪视图中不存在的验证例程**。

   注：如果"定制规则向导"是从"定制规则"视图启动的，那么无法从该向导创建验证例程。

2. 在向导的"选择验证/编码例程"页面中，指定验证例程的位置。

   对于本示例，选择以下例程：

   ```
   TestCase_IOT_Instance_Val_Encode.encode(java.lang.String):
   java.lang.String
   ```



3. 在第 170 页的『示例 2：从"跟踪"视图创建验证/编码例程』中，使用在**指定如何应用该验证例程**对话框中选择的相同设置完成向导页面的剩余部分。
4. 单击**完成**将验证例程添加到数据库。

示例 3：不同的源和接收器文件

以下示例说明来自接收器的其他文件中的源。

TestCase_IOT_Xfile_Part1.java：

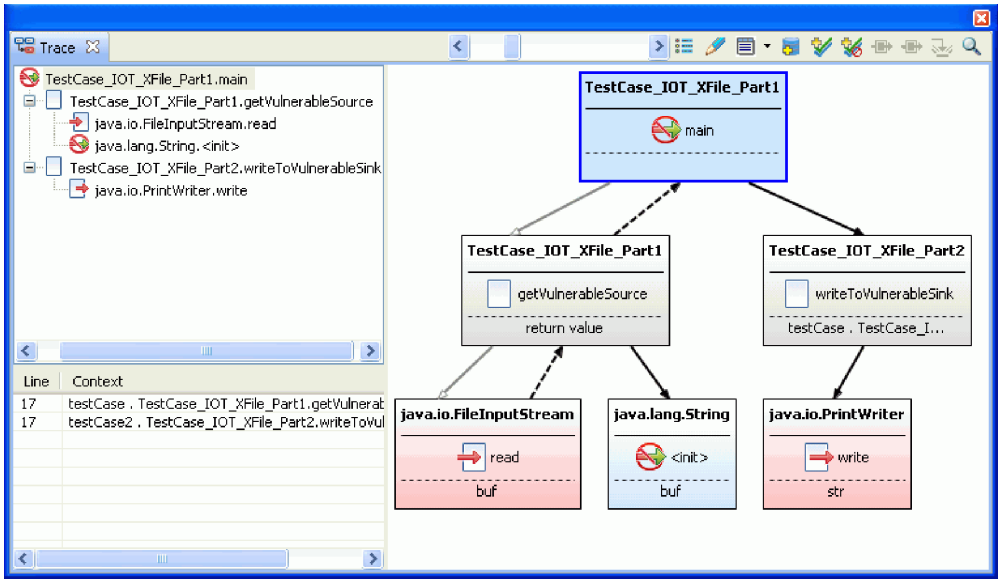
```
public class TestCase_IOT_XFile_Part1 {
  public static void main(String[] args) {
  try {
      TestCase_IOT_XFile_Part1 testCase =
        new TestCase_IOT_XFile_Part1();
      TestCase_IOT_XFile_Part2 testCase2 =
        new TestCase_IOT_XFile_Part2();
   testCase2.writeToVulnerableSink(
        testCase.getVulnerableSource(args[0]));
    } catch (Exception e) {
  }
 }

  public String getVulnerableSource(String file)
    throws IOException, FileNotFoundException {
    FileInputStream fis = new FileInputStream(file);
    byte[] buf = new byte[100];
    fis.read(buf);
    String ret = new String(buf);
    fis.close();
    return ret;
 }
}
```

TestCase_IOT_Xfile_Part2.java：

```
public class TestCase_IOT_XFile_Part2 {
  public void writeToVulnerableSink(String str)
     throws FileNotFoundException {
    FileOutputStream fos = new FileOutputStream(str);
    PrintWriter writer = new PrintWriter(fos);
    writer.write(str);
 }
}
```

从 TestCase_IOT_Xfile_Part1.java 到 TestCase_IOT_Xfile_Part2.java 跟踪数据允许在整个程序中跟踪数据流。将显示堆栈跟踪：



此示例显示数据通过 main 方法从 TestCase_IOT_XFile_Part1 流到 TestCase_IOT_XFile_Part2。

示例 4：深度验证

扫描示例 4 代码时，第一次扫描包含三个在对应跟踪例程中具有根的 AppScan Source 跟踪。假定在 trace1 中选择 FileInputStream.read 方法，且添加 validate 例程。样本源代码之后的部分描述每个作用域对验证例程的影响。

```
public class TestCase_IOT_UserValidation {
     ResultSet resultSet;
     FileInputStream fileInputStream;
     PrintWriter printWriter;
     byte[] buffer;

     public static void main(String[] args) throws Exception {
        TestCase_IOT_UserValidation testCase = new TestCase_IOT_UserValidation();
          testCase.trace1();

        TestCase_IOT_UserValidation testCase2 = new TestCase_IOT_UserValidation();
        testCase2.trace2();

        TestCase_IOT_UserValidation testCase3 = new TestCase_IOT_UserValidation();
        testCase3.trace3();
    }

     private void trace1() throws Exception {
          String source = getVulnerableSource1();
        source = validate(source);
          writeToVulnerableSink(source);
    }

     private void trace2() throws Exception {
          String source = getVulnerableSource2();
        source = validate(source);
          writeToVulnerableSink(source);
    }

     private void trace3() throws Exception {
```

```
            String source = getVulnerableSource3();
           source = validate(source);
            writeToVulnerableSink(source);
    }

     public String getVulnerableSource1() throws Exception {
            fileInputStream.read(buffer);
            return new String(buffer);
    }

     public String getVulnerableSource2() throws Exception {
            fileInputStream.read(buffer);
            return new String(buffer);
    }

     public String getVulnerableSource3() throws Exception {
            return resultSet.getString("x");
    }

     public void writeToVulnerableSink(String str) throws Exception {
            printWriter.write(str);
    }

    private String validate(String source) throws Exception {
            // validate
           return source;
    }
}
```

特定于调用站点的验证例程 - 针对 FileInputStream.read 的此调用的输入

在验证仅适合非常狭窄的上下文时，或在输入方法太宽泛而无法提供一个验证例程的情况下，创建特定于调用站点的验证例程。在 trace1 方法中**应用于对 FileInputStream.read 的此调用**时，trace1 不会在下次扫描后显示为结果，因为其调用堆栈包含对 validate 方法的调用。但是，仍会报告 trace2，尽管它调用 validate，因为验证例程的作用域与 trace1 调用站点相绑定。trace3 方法也调用 validate，但是会继续报告该方法，因为它使用 ResultSet.getString 作为源。

特定于 API 的验证例程 - 针对 FileInputStream.read 的任何调用的输入

验证仅适用于特定源时，创建特定于 API 的验证例程。**应用于对 FileInputStream.read 方法的任何调用**时，trace1 和 trace2 方法在下次扫描时都没有结果，因为它们包含对 validate 方法的调用。但是，trace3 方法继续存在，尽管它调用 validate，因为它使用 ResultSet.getString 作为源。

第 7 章 AppScan Source for Analysis 和缺陷跟踪

AppScan Source for Analysis 与缺陷跟踪系统 集成以直接向开发者桌面传递已确认的软件漏洞。提交到缺陷跟踪系统的缺陷包含对错误的文本描述和一个仅包含与缺陷一起提交的发现的文件。

您可以通过 AppScan Source for Analysis 与各种缺陷跟踪系统（包括 IBM Rational ClearQuest、IBM Rational Team Concert、HP Quality Center 和 Microsoft Team Foundation Server）的集成来跟踪软件漏洞缺陷。

在向缺陷跟踪系统提交结果或将缺陷用邮件发送到开发者之前，您可能需要配置缺陷跟踪系统首选项（请参阅第 82 页的『通过首选项启用缺陷跟踪』）。

通过首选项启用缺陷跟踪

"缺陷跟踪系统"首选项允许您支持将发现结果提交到缺陷跟踪系统，并确定提交缺陷的方式。

"缺陷跟踪系统"首选项页面中的"常规"选项卡用于在 AppScan Source 中启用或禁用缺陷跟踪系统集成功能。如果选中**启用缺陷跟踪系统集成**对话框，那么**提交缺陷**上下文菜单操作将可用于评估结果。 "常规"选项卡还提供对提交缺陷时哪些缺陷跟踪系统可用的离散控制。

要了解可以为受支持的缺陷跟踪系统设置的首选项，请参阅以下帮助主题：

- 第 83 页的『Rational ClearQuest 首选项』
- 第 83 页的『Quality Center 首选项』
- 第 85 页的『Rational Team Concert 首选项』
- 第 86 页的『Team Foundation Server 首选项』

Rational ClearQuest 首选项

要能够完成 Rational ClearQuest 首选项，Rational ClearQuest 管理员必须向您提供所需的 Rational ClearQuest 设置。这些设置特定于您的 Rational ClearQuest 环境。

注：与 Rational ClearQuest V8.0 集成时，Rational ClearQuest 模式必须包含 **DefectTracking** 预定义模式中可用的字段。

数据库集合

一个或多个缺陷数据库的集合。

Linux 缺省值为连接名称，Windows 缺省值为数据库集合

数据库名称

缺陷要提交到的数据库的名称。

© Copyright IBM Corp. 2003, 2017

数据库用户名

缺省 Rational ClearQuest 数据库用户名。

CQPerl 可执行文件的位置

本地计算机上 Rational ClearQuest CQPerl 可执行文件的位置。所提供的缺省位置映射到缺省 Rational ClearQuest 安装位置。

缺陷记录的实体

Rational ClearQuest 安装所配置的用于缺陷对象的实体（数据库对象）。

缺省实体为**缺陷**。

记录的描述字段

缺省描述是**描述**。

记录的标题字段

缺省标题为**标题**。

每个结果按缺陷

将一组结果作为单个缺陷或作为多个缺陷来提交。创建缺陷时，您可以更改提交方法。

Quality Center 首选项

必须首先启用 HP Quality Center 作为"常规缺陷跟踪系统"首选项，然后在 Quality Center 选项卡上设置个别首选项。

服务器 URL

Quality Center 服务器 URL - 例如 `http://<hostname>:<port>/qcbin/` 或 `https://<hostname>:<port>/qcbin/`。

用户名（可选）

用于登录 Quality Center 的用户名

密码（可选）

如果输入了用户名，请为其输入密码。

域

要连接到的 Quality Center 域。

项目

要连接到的 Quality Center 项目

自动登录

如果为 true，那么在提交结果时 AppScan Source 不提示输入登录信息，并会使用"首选项"中指定的缺省凭证进行登录。如果为 false，那么每次您向 Quality Center 提交结果时都必须登录。

自动提交

如果为 true，那么提交结果时不会出现用于提交新缺陷的对话框。AppScan Source for Analysis 使用"首选项"中指定的**缺省缺陷属性**。如果为 false，那么提交结果时将出现提示，请求您输入缺陷信息（严重性、优先级、缺陷类型以及状态等）。

重新提交之前提交的结果

已提交到 Quality Center 的结果将使用 Quality Center 缺陷信息（缺陷标识、提交用户和提交日期）进行标记。缺省情况下，AppScan Source 不会多次重新提交同一结果。这允许您将多个结果分派到 Quality Center，只需在 Quality Center 数据库中输入新结果。选中 (true) 时，可以向 Quality Center 重新提交先前提交的结果。

将每个结果作为单个错误提交

在单次操作中提交多个结果时，可以将所有结果作为单个 Quality Center 缺陷或者作为各单独 AppScan Source 结果的不同 Quality Center 缺陷进行提交。选中该复选框会将标志设置为 true，这将为各个结果创建单独的 Quality Center 缺陷。将标志设置为 false 将为已提交的所有结果创建一个 Quality Center 缺陷，作为批量提交过程的一部分。

自动生成错误摘要

如果为 true，那么 AppScan Source 会在 Quality Center 中自动生成用于提交的缺陷摘要。摘要指示缺陷中包含的结果数以及包含的结果类型，如 `Validation.Required`。

如果为 false，那么在创建新缺陷时打开的对话框中提交缺陷时，将向您显示要填写的"摘要"字段。

自动装入错误字段

缺省设置为 true。如果选中该复选框，那么 AppScan Source 会根据 Quality Center 中的当前用户和组设置来自动装入 Quality Center 数据库中的缺陷字段定义。如果设置为 false，那么在您创建新缺陷时，AppScan Source 不会在打开的对话框中显示 Quality Center 中的缺陷字段。

缺省缺陷属性

要为不同 Quality Center 缺陷属性设置缺省值，请单击"Quality Center 首选项"选项卡上的**缺省缺陷属性**。缺省值将在提交时预填充**新缺陷**对话框，或者，如果选择**自动提交**首选项，那么缺省值会静默发送到 Quality Center。

注：如果选择**自动装入错误字段**，那么在每次出现**缺陷属性**对话框时，将从 Quality Center 动态抽取缺陷属性及其可用值。因此，添加到 Quality Center 数据库的任何新字段和值都会自动显示在 AppScan Source for Analysis 中。要打开**缺省属性**对话框并使用 Quality Center 信息对其进行填充，必须具有有效的服务器、登录和连接信息。

定制 Quality Center 缺陷字段

通过配置文件，可以在"新缺陷"对话框中定制字段以及这些字段之间的交互。您可以在 <data_dir>\config\qc.dts（其中 <data_dir> 是 AppScan Source 程序数据的位置，如第 275 页的『安装和用户数据文件位置』中所述） 中找到一个示例配置文件，该文件包含样本定制和其他文档。这些定制允许您在"新缺陷"对话框中直接对 Quality Center 工作流程脚本逻辑进行建模。

可用的定制包括：

- 显示定制字段和/或缺失字段
- 强制字段一直显示（覆盖 Quality Center 设置）
- 根据其他字段的选择来更新字段的必填状态。
- 根据其他字段中的列表框选择来动态更新字段的列表框选项

Rational Team Concert 首选项

通过"Rational Team Concert 首选项"选项卡，您可以配置与 Rational Team Concert 服务器的连接，以及配置工作项属性的值。

一旦输入了您的连接信息并成功登录，那么您便可以选择连接到一个或多个项目区域。每个项目区域都可以拥有其自己的属性预置值配置。

注：连接到 Rational Team Concert 时（通过配置首选项或者提交缺陷），可能会提示您接受 SSL 证书。请参阅第 86 页的『Rational Team Concert SSL 证书』以了解更多信息。

要为给定项目区域配置属性值，请选择项目区域，然后选择**配置**。在配置对话框中，您可以将属性值设置为硬编码值或（在某些情况下）设置为将引用所选结果的变量。例如，在提交期间，在属性值中使用的 {Finding.fileName} 将被替换为结果的实际源代码文件名。为支持这些变量的属性值提供了内容辅助 (<Ctrl>+<Space>)。鼓励团队使用 Rational Team Concert 首选项主页上提供的**导入**和**导出**按钮来共享这些配置。

Team Foundation Server 首选项

使用"Team Foundation Server 首选项"选项卡，您可以配置至 Microsoft Team Foundation Server 的连接以及配置工作项字段的值。

一旦输入了您的连接信息并成功登录，那么您便可以选择连接到一个或多个项目。

注：将登录名配置为 Team Foundation Server 2010 时，服务器 URL 必须包含您要连接到的 Team Project Collection。例如，http://myserver:8080/tfs/*DefaultCollection*。

每个项目都可以拥有其自己的字段预置值配置。

要为给定项目配置字段值，请选择项目，然后选择**配置**。在配置对话框中，您可以将字段值设置为硬编码值或（在某些情况下）设置为将引用所选结果的变量。例如，在提交期间，在字段值中使用的 {Finding.fileName} 将被替换为结果的实际源代码文件名。为支持这些变量的字段提供了内容辅助 (<Ctrl>+<Space>)。

鼓励团队使用**导入**和**导出**按钮（在主 Team Foundation Server 首选项页面上提供）来共享这些配置。

将 HP Quality Center 与 AppScan Source for Analysis 集成

HP Quality Center 与 AppScan Source for Analysis 的集成需要在本地计算机上安装 Quality Center 客户机。您通过 Quality Center 基于浏览器的客户机接口首次登录 Quality Center 时，就在本地计算机上下载并安装了 Quality Center 客户机应用程序。

配置 Quality Center 信息

Quality Center 是在 Quality Center 选项卡上的"缺陷跟踪系统"首选项中配置的。您必须先启用 Quality Center 并设置 Quality Center 首选项，然后才能将 AppScan Source 结果作为缺陷进行提交。请参阅第 83 页的『Quality Center 首选项』以获取对每个首选项设置的描述。

注：在某些环境中（例如，运行 HP Quality Center V11 的环境），您可能需要安装 HP ALM Client MSI Generator 附加组件才能使 HP Quality Center integration 运行。

将发现提交到 Quality Center

结果可通过任何 AppScan Source for Analysis 结果视图提交到 Quality Center。

过程

1. 选择表中的发现，或者打开束。（如果打开束，请选择要提交的束发现。）
2. 右键单击所选内容，然后从菜单选择**提交缺陷** > **分派到 Quality Center**。
3. 登录到 Quality Center。

   如果您的首选项配置为自动登录，那么将不会显示"登录"对话框。AppScan Source 以缺省凭证登录。
4. 提交结果。

   如果您的首选项配置为自动提交，那么 AppScan Source 会使用**缺省缺陷属性**首选项提交结果信息。

结果

提交结果后，显示参考消息，指示成功提交的发现数量。

跟踪提交到 Quality Center 的发现

以提交信息来标记提交到 Quality Center 的发现：

- Quality Center 缺陷标识
- 提交日期
- Quality Center 用户名

提交信息显示在任何发现结果视图内的结果表中的**缺陷标识**、**缺陷日期**和**缺陷用户**列中。但是，缺省"发现表"没有包含这些列。您必须通过单击**选择和排序列**工具栏按钮并定制表来配置表以包含这些列。请参阅第 260 页的『定制发现表』以了解关于将列添加到发现视图的详细信息。

缺陷信息在不同扫描之间保留，从而允许您在分类和补救期间跟踪 AppScan Source 发现结果的状态。

Quality Center 中的 AppScan Source 结果信息

当 AppScan Source for Analysis 在 Quality Center 数据库中创建缺陷时，结果信息会设置为缺陷**描述**。此结果信息包含严重性、类型、API 和分类。

Quality Center 缺陷还可包含作为附件添加到该缺陷的 AppScan Source 束文件 (`.ozbdl`)。束文件包含关于 AppScan Source 结果的所有相关信息（包括跟踪）。然后，开发者可以在 AppScan Source for Analysis/Developer 插件中保存和打开束，并将缺陷分类。

将 Rational ClearQuest 与 AppScan Source for Analysis 集成

Rational ClearQuest 与 AppScan Source for Analysis 的集成需要在本地计算机上安装 Rational ClearQuest 客户机。此安装包括 `CQPerl` 可执行文件，并且您必须在 AppScan Source for Analysis Rational ClearQuest 首选项中配置该可执行文件的位置。

配置 Rational ClearQuest 集成首选项时，请指定关于缺陷数据库模式的信息。 Rational ClearQuest 实体是指 Rational ClearQuest 数据库对象，并且您必须指定 Rational ClearQuest 安装所用于缺陷的实体。

注：AppScan Source for Analysis 集成所需的 CQPerl 可执行文件的缺省位置为 Rational ClearQuest 缺省安装目录。

注：与 Rational ClearQuest V8.0 集成时，Rational ClearQuest 模式必须包含 **DefectTracking** 预定义模式中可用的字段。

将结果提交到 Rational ClearQuest

发现与公司缺陷跟踪系统集成以便开发者进行补救。您可以将单独结果发送到缺陷跟踪系统，也可以提交含有一个或多个结果的束。在 AppScan Source 会话期间首次将发现结果从 AppScan Source 提交到 Rational ClearQuest 时，必须使用您的用户名和密码登录。

将束提交到 Rational ClearQuest 时，错误编号与束中的特定结果而不是束本身相关联。这确保您可以进一步处理束，并在创建缺陷时保留与缺陷关联的特定发现。

一个束可以包含许多结果。您可以选择将所有发现提交为一个缺陷，或者将每个发现提交为单独的缺陷。如果您选择**每个结果单个缺陷**首选项，并且存在多个结果，那么可以编辑这些缺陷的描述。您只能编辑单个缺陷提交的描述。

注：登录到 Rational ClearQuest 之前，您必须设置"缺省跟踪系统"首选项。

注：与 Rational ClearQuest V8.0 集成时，Rational ClearQuest 模式必须包含 **DefectTracking** 预定义模式中可用的字段。

将缺陷提交到 Rational ClearQuest

过程

1. 选择表中的发现，或者打开束。（如果打开束，请选择要提交的束发现。）
2. 右键单击所选内容，然后从菜单选择**提交缺陷 > 分派到 ClearQuest**。
3. 登录到 Rational ClearQuest 并提交结果。

结果

仅包含相关文件的评估文件附加到每个缺陷。AppScan Source for Analysis 或 AppScan Source for Development 可以打开此评估文件。

注：与 Rational ClearQuest V8.0 集成时，Rational ClearQuest 模式必须包含 **DefectTracking** 预定义模式中可用的字段。

将 Rational Team Concert 与 AppScan Source for Analysis 集成

Rational Team Concert 与 AppScan Source for Analysis 的集成不需要在您的计算机上再安装一个 Rational Team Concert 客户机。

要配置与 Rational Team Concert 的连接，请转至"缺陷跟踪系统"首选项中的"Rational Team Concert"选项卡；或者您也可以提交缺陷，而此时将提示您登录并配置连接。

通过 Rational Team Concert 首选项，还可以配置将在缺陷提交期间使用的预设字段值。这使您能够设置要用于每个缺陷的值，以及修改 AppScan Source 随附的缺陷值。

注：连接到 Rational Team Concert 时（通过配置首选项或者提交缺陷），可能会提示您接受 SSL 证书。请参阅第 86 页的『Rational Team Concert SSL 证书』以了解更多信息。

将缺陷提交到 Rational Team Concert

您可以将包含一个或多个结果的束提交到 Rational Team Concert，或者也可以提交单独结果。首次将结果从 AppScan Source for Analysis 提交到 Rational Team Concert 时，必须使用您的用户名和密码登录。如果要配置将在提交期间使用的预设字段值，那么可在 Rational Team Concert 首选项中执行此操作。

关于此任务

将束提交到 Rational Team Concert 时，工作项编号与束中的特定结果而不是束本身相关联。这确保您可以进一步处理束，同时保留特定发现与工作项编号的关联。

过程

1. 选择表中的发现，或者打开束。（如果打开束，请选择要提交的束发现。）
2. 右键单击所选内容，然后从菜单选择**提交缺陷 > 分派到 Rational Team Concert**。
3. 然后，提交对话框将指导您完成此过程（如需登录，也将包括在内，并填充必填属性）。

注：连接到 Rational Team Concert 时（通过配置首选项或者提交缺陷），可能会提示您接受 SSL 证书。请参阅第 86 页的『Rational Team Concert SSL 证书』以了解更多信息。

结果

束将自动添加到已提交的工作项，而该工作项可由 AppScan Source for Analysis 或 AppScan Source for Development 的用户在以后打开。

Rational Team Concert SSL 证书

安装 Rational Team Concert 服务器时，应对其进行配置以使用有效 SSL 证书。如果未完成该操作，那么在登录到该服务器时将接收到不可信连接消息（在配置首选项或提交缺陷时）。本主题概述了 Rational Team Concert SSL 证书注意事项。

SSL 证书存储位置

已被永久接受的证书存储在 `<user_home>/.jazzcerts`（其中 `<user_home>` 是您的操作系统主目录（例如，在 Windows 上，此目录可能是 `C:\Documents and Settings\Administrator\`）） 中。移除 `<user_home>/.jazzcerts` 会删除 AppScan Source 和 Rational Team Concert 客户机的所有已存储证书。

与 Rational Team Concert 客户机共享 SSL 证书

AppScan Source 将其证书库与 Rational Team Concert 客户机共享。如果您使用 Rational Team Concert 客户机永久接受某个证书，那么此证书将被 AppScan Source 复用（您不会在 AppScan Source 中收到关于接受证书的提示）。类似地，如果您在 AppScan Source 中永久接受某个证书，那么此证书将被 Rational Team Concert 客户机复用。

将 Microsoft Team Foundation Server 与 AppScan Source for Analysis 集成

Team Foundation Server 与 AppScan Source for Analysis 的集成需要在本地计算机上安装 Microsoft Visual Studio Team Explorer 客户机。

要配置到 Team Foundation Server 的连接，请转至"缺陷跟踪系统"首选项中的 Team Foundation Server 选项卡 - 或者您可以提交缺陷且将在该点提示您登录和配置连接。

Team Foundation Server 首选项还允许您配置在缺陷提交期间将使用的预设置字段值。这使您能够设置要用于每个缺陷的值，以及修改 AppScan Source 随附的缺陷值。

将缺陷提交到 Microsoft Team Foundation Server

您可以将带有一个或多个发现的束提交到 Team Foundation Server - 或者您可以提交个别发现。首次将结果从 AppScan Source for Analysis 提交到 Team Foundation Server 时，必须使用您的用户名和密码登录。如果您希望配置在提交过程中使用的预设置字段值，您可以在 Team Foundation Server 首选项中执行此操作。

关于此任务

将束提交到 Team Foundation Server 时，工作项编号与束中的特定发现（而不是束本身）相关联。这确保您可以进一步处理束，同时保留特定发现与工作项编号的关联。

注：将登录名配置为 Team Foundation Server 2010 时，服务器 URL 必须包含您要连接到的 Team Project Collection。例如，`http://myserver:8080/tfs/DefaultCollection`。

过程

1. 选择表中的发现，或者打开束。（如果打开束，请选择要提交的束发现。）
2. 右键单击所选内容，然后从菜单选择**提交缺陷 > 分派到 Team Foundation Server**。
3. 然后，提交对话框将指导您完成此过程（如需登录，也将包括在内，并填充必填字段）。

结果

束将自动添加到已提交的工作项，而该工作项可由 AppScan Source for Analysis 或 AppScan Source for Development 的用户在以后打开。

处理已提交的缺陷

将诸多发现提交为单独缺陷时，在您继续筛选过程的同时，进程在后台运行。在提交缺陷后，将从缺陷系统收到的缺陷标识附加到相关发现并保持在该发现中。要处理已提交到缺陷跟踪系统的缺陷，请遵循此主题中的步骤。

过程

1. 打开缺陷跟踪系统并找到缺陷。
2. 将附件另存为 AppScan Source 束 (`.ozbdl`) 文件。您可以在 AppScan Source for Analysis 中打开此文件，或者在 AppScan Source for Development 中以束形式打开此文件。

将束提交至缺陷跟踪及通过电子邮件发送

束中的发现结果可以提交至您的企业缺陷跟踪系统，或通过电子邮件进行发送。将结果置于束中后，可将这些结果作为错误提交给开发者进行修复。

过程

1. 打开束。
2. 单击**将束提交至缺陷跟踪**工具栏按钮向下箭头，然后选择您的缺陷跟踪系统。

   注：根据您的缺陷跟踪系统，您可能希望在提交束之前修改"缺陷跟踪系统"首选项。

   或者，在"束"工具栏上，单击**通过电子邮件发送束**以将束发送到其他人（必须提前配置电子邮件首选项）。
3. 完成打开的配置对话框。根据所选择的缺陷跟踪系统的不同，这些对话框也有所不同，在帮助的 *AppScan Source for Analysis* 和缺陷跟踪部分中描述了这些对话框。

通过电子邮件跟踪缺陷（通过电子邮件发送结果）

关于此任务

如果您已配置了电子邮件首选项，那么可以直接将结果或束通过电子邮件发送给开发人员以告知他们扫描后所发现的潜在缺陷。电子邮件包括附件（其中包含结果）以及描述结果的文本。

注：一些简单电子邮件传输协议 (SMTP) 中继设备仅将邮件发送到特定域。在此情况下，如果您从 mydomain.com 发送，那么只有 mydomain.com 中的收件人才能通过 AppScan Source for Analysis 接收到电子邮件。

要通过电子邮件发送结果表中的发现结果：

过程

1. 选择表中的发现，或者打开束。如果打开束，请选择要通过电子邮件发送的束结果。
2. 右键单击所选内容，然后从菜单选择**用电子邮件发送发现**。
3. 电子邮件将包含束附件（其中包含结果）。在"附件文件名"对话框中，指定结果束的名称。例如，在**附件文件名**字段中指定 my_finding 会将文件名为 my_finding.ozbdl 的束附加到电子邮件。 单击**确定**以打开"通过电子邮件发送结果"对话框。
4. 缺省情况下，将使用电子邮件首选项中指定的**收件人地址**来填充"通过电子邮件发送结果"对话框中的**收件人**字段，不过，可在准备电子邮件时轻松对其进行更改。在此对话框中，复审电子邮件的内容，然后单击**确定**以发送电子邮件。

结果

示例电子邮件内容：

```
1 findings:
Name: JavaAny.test_DataInput
Type: Vulnerability.Validation.Required
Severity: Low
Classification: Suspect
File Name: C:\TestApps\java\JavaAny\src\JavaAny.java
Line / Col: 275 / 0
Context: di . java.io.DataInput.readFully ( ba )
Notes: Check into this vulnerability and report back ASAP.
```

提示：您可以用电子邮件发送来自"结果详细信息"视图的个别发现或束。还可以通过单击"束"工具栏上的**通电子邮件发送束**来通过电子邮件发送束。

第 8 章 发现结果报告和审计报告

安全分析人员和风险管理员可以访问对选定结果的报告，或一系列用于度量与软件安全最佳做法和法规要求是否一致的审计报告。本部分说明如何创建对聚集结果数据的报告。

AppScan Source for Analysis 生成两种报告类型：发现结果报告和 AppScan Source 报告。结果报告是所选结果的报告。*AppScan Source* 报告基于根据特定安全策略调整的所有发现结果的分类分组。AppScan Source 报告在 第 189 页的『AppScan Source 报告』中列出。

报告提供关于在特定扫描期间收集的结果的详细信息，并且所有 AppScan Source 报告都可包含添加到结果的任何注释和跟踪数据。报告的长度取决于报告中包含的结果数。可以生成 PDF 文件格式或超文本标记语言 (HTML) 格式的报告。HTML 报告运行方式与 Web 页面类似，在其中您可以通过单击按钮或链接跳到某个部分。然后，您可以使用 Web 浏览器中存在的浏览功能来浏览信息。

报告还列出了已应用于结果的任何扫描时间过滤器。扫描时间过滤器在第 139 页的『确定所应用的过滤器』中进行了描述。

创建发现结果报告

关于此任务

扫描之后，您可能想要生成关于已识别漏洞的报告。可生成多个结果报告：

- 结果
- 结果（按类型）
- 结果（按分类）
- 结果（按文件）
- 结果（按 API）
- 结果（按束）
- 发现结果（按 CWE，即常见弱点枚举）
- DTS 活动

注：发现结果报告按类别显示详细的发现结果，与结果表中的结果类似。结果报告的生成可以是内存密集型（与 https://xmlgraphics.apache.org/fop/1.1/running.html#memory 相关），最多可能需要 1024 MB 的额外系统内存。如果为大型应用程序的扫描生成报告并注意到内存问题，可单独地扫描应用程序的各个部分或更改扫描配置，然后再次尝试生成报告。

发现结果报告中的 CWE 标识超链接将连接至 CWE Web 站点，地址为：http://cwe.mitre.org/。

要生成结果报告，请执行以下操作：

© Copyright IBM Corp. 2003, 2017

过程

1. 在包含结果的视图中，选择要包含在报告中的结果。如果不选择任何发现结果，那么报告将包含活动视图中所有的发现结果。

   在**工具**菜单上，单击**生成结果报告**。或者，在包含发现结果的视图中，选择并右键单击一组发现结果，然后选择菜单中的**生成发现结果报告**。
2. 在**选择发现结果报告**对话框中，选择报告类型。

   单击**完成**以生成报告，或单击**下一步**以在"指定目标和样式表"页面中指定以下可选设置：

   - 可以指定报告目标和格式。可以将报告生成为 HTML 格式、包含所有 HTML 报告组件的 ZIP 文件或者 PDF（必须具有 Adobe Acrobat Reader 才能查看 PDF 报告）。如果不指定报告目标和格式（或在"选择结果报告"页面中单击**完成**），那么缺省情况下将选择 HTML，并且报告将保存到 `<data_dir>\reports`（其中 `<data_dir>` 是 AppScan Source 程序数据的位置，如第 275 页的『安装和用户数据文件位置』中所述）。

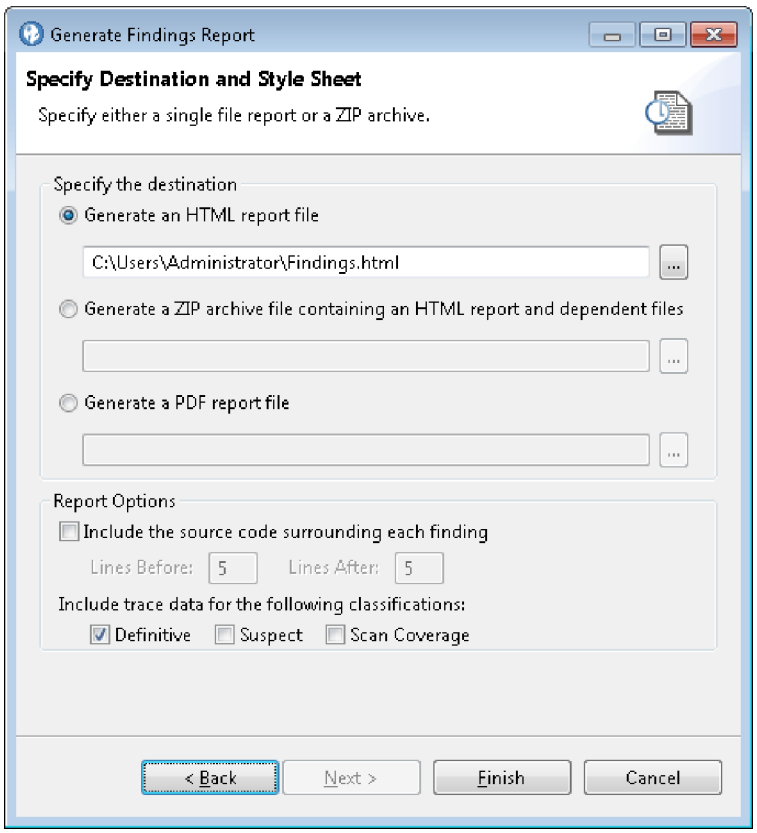
     注：如果要以 PDF 格式创建定制报告（而不是发现结果报告），可指定要在报告中包含的详细级别：

     – **摘要**：包含对每个报告组的计数
     – **详细**：包含对各漏洞属性的每个 API 的计数
     – **综合**：包含由各 API 的每个结果组成的表
     – **注释**：包含所有发现结果以及发现结果随附的任何说明、跟踪数据或代码片段
   - 要在报告中包含代码片段，请选择**包含每个发现结果周围的源代码**，并指示报告中要包含在易受攻击代码行之前和之后的行数。

     提示：在"发现结果详细信息"视图的"报告"部分中，也可以设置报告中要包含在发现结果之前和之后的代码行数。

     生成报告后，展开包含说明或代码片段的发现结果时，源代码将显示在发现结果之下的蓝色框中或黄色说明下。红色粗体文本突出显示易受攻击的代码行。
   - 要在报告中包含 AppScan Source 跟踪数据，请选择**包含以下分类的跟踪数据**下的一个或多个分类（**明确**、**可疑**或**扫描覆盖范围**）。

   单击**完成**以生成报告。



AppScan Source 报告

AppScan Source 报告帮助软件安全性分析人员、开发管理员和风险管理审计员度量与软件安全性最佳实践和法规要求的一致性。AppScan Source 报告帮助确保关键应用程序符合您设置的安全性标准。

AppScan Source 使用源代码漏洞分析结果来支持一系列报告，这些报告向安全性、开发或审计专业人员提供合规性的详细情形。

AppScan Source 报告功能部件：

- 报告卡：报告卡是对各主要类别的安全状态进行的简述。
- 详细审计复审：对不合规结果的详细审计
- 向下钻取：直接访问不合规代码，以进行进一步分析并对修复和分配进行优先级划分。

AppScan Source for Analysis 生成各种 AppScan Source 报告：

- 第 191 页的『CWE/SANS Top 25 2011 报告』
- 第 191 页的『DISA 应用程序安全和开发 STIG V3R10 报告』
- 第 192 页的『开放式 Web 应用程序安全项目 (OWASP) Mobile Top 10 报告』
- 第 191 页的『开放式 Web 应用程序安全项目 (OWASP) Top 10 2013 报告』
- 第 192 页的『支付卡行业数据安全标准 (PCI DSS) V3.2 报告』

- 第 192 页的『软件安全概要文件报告』：提供应用程序安全状态的全景（包括每个主要的漏洞类别）。

创建 AppScan Source 定制报告

过程

1. 在**工具**菜单上，单击**生成报告**。
2. 在"生成报告"对话框中，选择 AppScan Source 报告：
   - **CWE SANS Top 25 2011**
   - **DISA Application Security and Development STIG V3R10**
   - **OWASP Mobile Top 10**
   - **OWASP Top 10 2013**
   - **PCI Data Security Standard V3.2**
   - **软件安全概要文件**

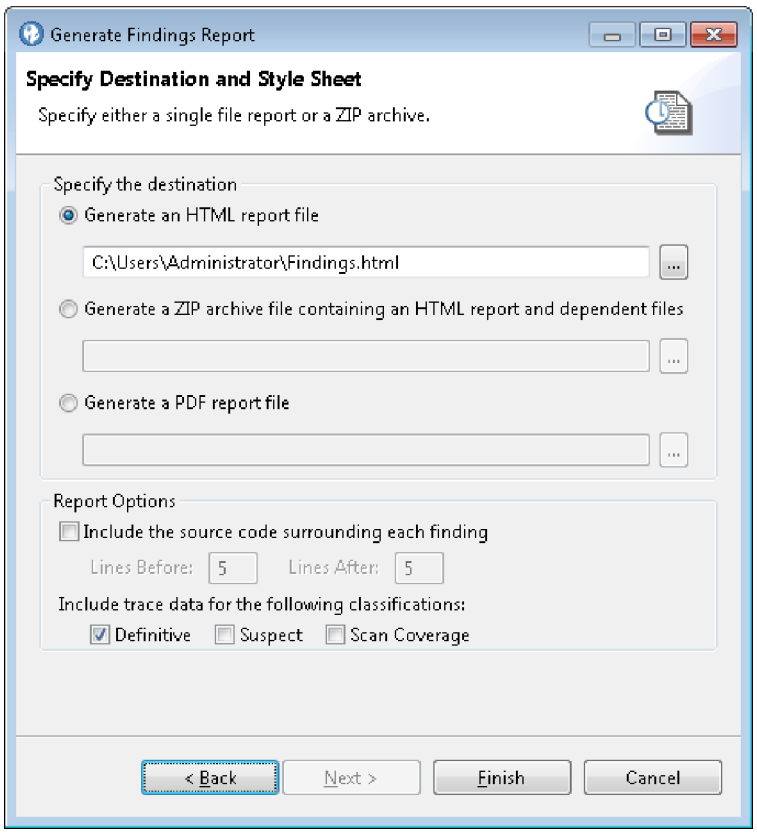
   单击**完成**以生成报告，或单击**下一步**以在"指定目标和样式表"页面中指定以下可选设置：
   - 可以指定报告目标和格式。可以将报告生成为 HTML 格式、包含所有 HTML 报告组件的 ZIP 文件或者 PDF（必须具有 Adobe Acrobat Reader 才能查看 PDF 报告）。如果不指定报告目标和格式（或在"选择结果报告"页面中单击**完成**），那么缺省情况下将选择 HTML，并且报告将保存到 `<data_dir>\reports`（其中 `<data_dir>` 是 AppScan Source 程序数据的位置，如第 275 页的『安装和用户数据文件位置』中所述）。

     注：如果要以 PDF 格式创建定制报告（而不是发现结果报告），可指定要在报告中包含的详细级别：
     - **摘要**：包含对每个报告组的计数
     - **详细**：包含对各漏洞属性的每个 API 的计数
     - **综合**：包含由各 API 的每个结果组成的表
     - **注释**：包含所有发现结果以及发现结果随附的任何说明、跟踪数据或代码片段
   - 要在报告中包含代码片段，请选择**包含每个发现结果周围的源代码**，并指示报告中要包含在易受攻击代码行之前和之后的行数。

     提示：在"发现结果详细信息"视图的"报告"部分中，也可以设置报告中要包含在发现结果之前和之后的代码行数。

     生成报告后，展开包含说明或代码片段的发现结果时，源代码将显示在发现结果之下的蓝色框中或黄色说明下。红色粗体文本突出显示易受攻击的代码行。
   - 要在报告中包含 AppScan Source 跟踪数据，请选择**包含以下分类的跟踪数据**下的一个或多个分类（**明确**、**可疑**或**扫描覆盖范围**）。

   单击**完成**以生成报告。



CWE/SANS Top 25 2011 报告

CWE/SANS Top 25 2011 报告基于 *2011 CWE/SANS Top 25 Most Dangerous Software Errors*。

要了解 *2011 CWE/SANS Top 25 Most Dangerous Software Errors*，请参阅 http://cwe.mitre.org/top25/。

要了解 AppScan Source 支持的所有常用弱点枚举 (CWE) 弱点，请参阅第 279 页的第 15 章, 『CWE 支持』。

DISA 应用程序安全和开发 STIG V3R10 报告

本主题提供了 Defense Information Systems Agency (DISA) 应用程序安全和开发 Security Technical Implementation Guide (STIG) Web 站点和指导信息文档的链接。

要了解关于 DISA 应用程序安全和开发 STIG 的更多信息，请参阅 http://iase.disa.mil/。

开放式 Web 应用程序安全项目 (OWASP) Top 10 2013 报告

该主题提供了开放式 Web 应用程序安全项目 (OWASP) Web 站点以及指导信息文档的链接。

要了解关于 OWASP 的信息，请参阅https://www.owasp.org/index.php/Main_Page。 https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project 处提供了各种 OWASP 文档和安全风险的链接。

开放式 Web 应用程序安全项目 (OWASP) Mobile Top 10 报告

该主题提供了开放式 Web 应用程序安全项目 (OWASP) Web 站点以及指导信息文档的链接。

要了解 OWASP Mobile 安全项目，请参阅 https://www.owasp.org/index.php/OWASP_Mobile_Security_Project。

支付卡行业数据安全标准 (PCI DSS) V3.2 报告

此报告提供确保与支付卡行业数据安全标准 (PCI DSS) 一致所需的相关数据。

要获取有关信息，请参阅https://www.pcisecuritystandards.org/security_standards/index.php。

软件安全概要文件报告

软件安全概要文件表示对与应用程序安全直接相关的应用程序特征的综合分析。它提供了在软件中对特定项目的关键安全功能的详细审计。此报告帮助您在证明软件可部署之前验证对需求内容（如加密、访问控制、记录和错误处理）的实施。

该复合体确定存在潜在风险的区域并提供对最大限度降低这些风险的建议。报告有助于更好地评估总体应用程序安全性，这对于合规性、策略和体系结构复审都很有用。结果基于使用包含缺陷、漏洞、行业特定标准和常规最佳实践的数据库对源代码所进行的广泛静态分析。

软件安全概要文件显示以下信息：

- 包含：指向报告详细信息和严重性指示符（对此部分进行总结）的链接报告卡。
- 概述：总结报告的用途并描述应用程序配置。
- 度量：确定项目中软件包、类、方法和所有软件包中代码行的总数。
- 详细的结果（按类别）：报告使用漏洞类别名称找到的各漏洞类别以及指示漏洞严重性级别的图标。

第 9 章 创建定制报告

在报告编辑器中，可创建用于生成定制报告的报告模板。

AppScan Source 发现结果报告或 AppScan Source 报告可能不会提供您需要的确切数据；您可能需要报告包含更多或更少的信息。通过 AppScan Source for Analysis 报告编辑器，可以创建定制报告。

通常，当您必须执行以下操作时，需要创建定制报告：

- 生成映射到唯一安全策略的报告，并针对此策略进行报告。您首先创建定制报告，然后再将此报告应用于特定评估。
- 定义并生成报告以突出显示独特的结果和特征。
- 修改现有报告或向其中添加内容。

如果将报告模板保存到 <data_dir>\reports（其中 <data_dir> 是 AppScan Source 程序数据的位置，如第 275 页的『安装和用户数据文件位置』中所述），那么报告可用于对任何应用程序的评估。如果保存到特定应用程序的目录中，那么报告可用于扫描该应用程序或该应用程序的任何项目。

开始创建或编辑 AppScan Source 报告之前，请熟悉报告类型和组成每个报告的元素。创建定制报告时，您能够以任何顺序映射报告元素。报告元素包括结果信息、代码片段、跟踪、修复内容以及文本和图形元素。

报告编辑器

通过"报告编辑器"，可以编辑定制报告或模板，或者创建新的报告。定制报告包括可用于发现结果报告的任何项，如发现结果信息、代码片段、AppScan Source 跟踪和补救内容以及漏洞矩阵。在开始设计新报告之前，建议您先通过在"报告编辑器"中修改现有报告模板来熟悉报告创建过程。

报告编辑器包含"报告布局"、"类别"和"预览"选项卡。

- **报告布局**：设计报告的外观。在布局中，您可以添加和除去 AppScan Source 报告元素并对其重新排序。
- **类别**：创建和编辑类别。类别是一组结果。类别用于确定要包含在报告中的发现结果、这些发现结果的分组方式以及分组顺序。
- **预览**：在您编辑报告时查看报告中的当前评估。

以下三个选项卡包含常用字段：

- **文件**：已保存的分组文件的路径（只读）。保存文件后，此字段中才会显示内容。保存后，该分组文件是用于定义报告的 XML 文件。
- **名称**：用户定义的报告名称。

用于保存、打开、创建、复制和生成定制报告的工具栏按钮包括：

- **创建新报告**：创建新的定制报告
- **从现有新建报告**：从现有报告模板创建新定制报告

© Copyright IBM Corp. 2003, 2017

- **打开已保存的报告**：打开要编辑的分组文件
- **保存**：将当前报告保存到指定的文件
- **另存为**：将当前报告保存到新文件
- **生成此报告的实例**：为当前打开的评估创建报告副本

提示：要查看现有报告的样本，请单击**从现有报告新建报告**，然后选择以下某个 AppScan Source 报告模板。通过在模板中探查"报告布局"和"类别"选项卡，您可以了解设计报告的方式。

"报告布局"选项卡

"报告布局"选项卡包含"选用板"和"布局"部分，以及允许您指定在每个页面上显示的页眉或页脚的部分。

页眉和页脚

页眉字段允许您指定出现在每个报告页面顶部的文本，而**页脚**字段允许您指定出现在每个页面底部的文本。

选用板

"选用板"显示用于构成 AppScan Source 标准报告的元素的列表。某些元素仅显示"类别"选项卡中已定义的类别的信息（请参阅表 19）。

表 *18.* 报告布局选用板 - 不依赖于类别的元素

报告元素	描述
文本标题	向报告布局添加粗体文本块。
图像标题	显示缩放到指定大小（以像素为单位）的图像。
AppScan Source 标题	包含 AppScan Source 标记的报告标题。
标题和日期	包含已扫描项的名称的报告标题，以及扫描日期和生成报告的日期。
文本块	任何用户定义的文本。也可以为**标签**字段中的文本块添加标题。
漏洞矩阵	评估漏洞矩阵（显示出现在"漏洞矩阵"视图中的相同图形）。
度量值	确定项目中软件包、类、方法和所有软件包中代码行的总数。
扫描历史记录	当前扫描的度量和同一目标的扫描的历史度量。

表 *19.* 报告布局选用板 - 依赖于类别的元素

报告元素	描述
报告卡	"类别"选项卡中定义的每个类别的漏洞级别的简短细分。包含指向总结该部分的报告详细信息和严重性指示符的链接。
漏洞细分	包含"类别"选项卡中定义的所有类别中漏洞数量细分情况（按严重性和分类排序）的表。

表 *19.* 报告布局选用板 - 依赖于类别的元素（续）

报告元素	描述
部分报告卡	用户指定的类别（如"类别"选项卡中所指定）的漏洞级别的细分。
类别	按"类别"选项卡中的定义列出所有已分类的发现结果数据。
类别	列出"类别"选项卡中已定义的一个或多个类别中的所有发现结果。

布局

从选用板添加项时，所添加项将出现在布局中。使用部分工具栏可在布局中除去、修改或移动项。

"类别"选项卡

通过使用"类别"选项卡，可添加类别以包含基于束和属性的发现结果或所选择的选定发现结果。然后，在将某些项添加到布局时可使用这些类别。例如，在将"漏洞细分"添加到布局时，会将包含所有类别的漏洞数量细分情况（按严重性和分类排序）的表添加到布局。"类别"选项卡包含一个带有类别树的窗格和一个可在其中编辑选定类别的属性的窗格。每个类别都包含评估中满足您所定义的某些要求的结果。

可用的类别包括：

- 束：束类别包含束名称列表。束中其名称显示在列表中的任何发现结果都将在此类别中显示。虽然您从当前评估选择束，但是您可以将束类别应用于任何评估，因为束按名称匹配。
- 个别结果：选择要添加到类别的特定结果。只会将结果的快照添加到报告中。如果将发现结果添加到报告之后再对其进行修改，那么报告不会反映该更改。
- "漏洞类型"、"机制"和"技术"属性：从 AppScan Source 安全知识库中的 API 选择属性和必需属性的集合。如果结果包含至少一个**属性**和所有**必需属性**，那么该结果将包含在报告中。

下表标识了类别窗格和构成该窗格的项。

表 *20.* "类别"选项卡属性

属性	描述	编辑方式
标签	类别的简称，如"缓冲区溢出"。标签标识类别树列表中的类别，它是定制报告中的类别标题。	在单行文本字段中输入标签。
摘要	语句的模板，用于说明在此类别中报告的发现结果数量。在报告生成期间，实际计数将替换 `%FindingCount%`。	为类别输入简短描述，然后单击 **添加计数** 以将变量 `%FindingCount%` 放置在光标位置的短语中。
文本	简短的类别描述。	输入描述类别的文本。

表 20. "类别"选项卡属性 (续)

属性	描述	编辑方式
属性（仅限"属性"类别）	将在此类别中报告具有至少其中一个属性的结果。如果结果不具有列出的所有必需属性，那么结果将不会包含在此类别中。	单击工具栏上的**添加**，然后从"添加属性"对话框中选择属性。单击**除去**以从列表中除去所选项。
必需属性（仅限"属性"类别）	具有所有必需属性并且至少具有一个属性的发现结果将显示在此类别下的报告中。	单击工具栏上的**添加**，然后从"添加属性"对话框中选择属性。单击**除去**以从列表中除去所选项。
束（仅限"束"类别）	指定要包含在此类别中的束的名称。	单击"束"部分中的**添加束**，然后从列表中选择束。
发现结果（仅限"发现结果"类别）	指定要包含在此类别中的结果。	选择任何结果表中的发现结果，然后单击表工具栏上的**添加发现结果**以添加选定发现结果。如果多个视图包含选定发现结果，那么将提示您选择包含您要添加的选定发现结果的视图。 也可将发现结果从结果表拖动到"报告编辑器"视图中的表中，或在"报告编辑器"中，或直接拖动到类别树中的现有发现结果类别。

"预览"选项卡

您可以在编辑模板时预览 AppScan Source for Analysis 报告。在"预览"窗格中，单击**预览**以查看针对打开的评估的报告。

生成定制报告

此部分的主题中的过程描述如何从现有定制报告设计和生成报告。此外，您还可以创建新报告。要编辑现有报告，请打开报告并遵循设计、修改和预览过程。

- 第 197 页的『从现有定制报告设计报告』
- 第 197 页的『在报告中包括类别』
  - 第 197 页的『向类别添加束』
  - 第 197 页的『向类别添加结果』
  - 第 198 页的『向类别添加属性』
- 第 198 页的『预览报告』
- 第 198 页的『保存报告模板』

从现有定制报告设计报告

过程

1. 在"报告编辑器"视图中，单击工具栏上的**从现有新建报告**。
2. 从现有报告列表中选择报告模板。在"布局"窗格中，预览报告模板。
3. 更改报告名称、页眉和页脚或者模板元素：
   a. 添加**页眉**或**页脚**。页眉和页脚出现在每个页面上。
   b. 向报告添加其他元素。从**选用板**中选择所需的报告元素，然后单击**插入**（必须单独插入每个元素）。
   c. 从报告删除元素。从模板选择要除去的元素并单击**除去选定报告元素**工具栏按钮。
4. 将报告元素重新排序。在预览中选择元素，然后单击工具栏上的**向上移动选定报告元素**或**向下移动选定报告元素**来向上或向下移动报告元素。
5. 在"布局"窗格中双击元素以对其进行编辑；或者选择该元素并单击工具栏上的**编辑选定报告元素**。

   在生成的对话框中，进行所需的更改。例如，要编辑文本块，通过在"编辑文本块"对话框中修改标签和描述性文本来进行更改。

   注：某些元素无法修改。

在报告中包括类别

定义了布局后，便可确定要在报告中包括的类别。

过程

1. 在"类别"窗格中，单击**创建新属性类别**、**创建新束类别**或**创建新结果类别**。
2. 通过为类别输入标签来命名该类别，该标签是类别的简短摘要，可以包含计数和描述性文本。

   使用工具栏箭头按钮对类别或子类别进行升级或降级。
3. 将束、结果或属性添加到类别。

向类别添加束

过程

1. 打开包含束的评估。如果评估尚未包含束，那么您无法向报告添加束。
2. 在"束"窗格中，单击**添加束**，然后指定要包含在该类别中的一个或多个束。

向类别添加结果

过程

1. 打开包含要添加的结果的结果视图。选择所需的结果并将其拖入结果表中或拖至报告编辑器中类别树的节点。
2. 或者，单击结果表上方工具栏上的**添加发现结果**，以将选定的发现结果包含在其他视图中。如果在多个视图中选择了结果，那么必须选择包含了添加到类别的结果的视图。

3. 从包含结果表的任何视图中选择发现结果。

向类别添加属性

过程

1. 单击**添加属性**（属性包括"漏洞"、"机制"和"技术"）。选择属性时，将显示该属性的 知识库描述（如果可用）。
2. 选择至少一个属性和任何必需属性。结果必须具有**必需属性**列表中的所有属性才能包含在类别中。

   要创建子类别，请选择类别并单击工具栏上的向左或向右箭头按钮。

预览报告

设计定制报告时，您可以先对其进行预览，然后再生成最终报告。在"预览"窗格中，单击**预览**以显示针对当前打开的评估的报告。

保存报告模板

在"报告编辑器"视图工具栏中，您可以单击**保存**以保留当前报告模板，或单击**另存为**以将当前报告模板保存到新文件。

如果将报告模板保存到与应用程序文件（.paf 或 .gaf）相同的目录中，那么该报告模板在"定制报告"向导的选项列表中可用，并且在"报告编辑器"视图中可用来对该应用程序进行后续扫描。如果将它保存到 <data_dir>\reports（其中 <data_dir> 是 AppScan Source 程序数据的位置，如第 275 页的『安装和用户数据文件位置』中所述），那么它可用于对任何应用程序进行的扫描。

第 10 章 定制漏洞数据库和模式规则

本节描述如何定制数据库以及将定制的漏洞和其他例程集成到扫描中。

扫描过程中有多个阶段：

- 使用漏洞数据库（或 AppScan Source 安全知识库）运行特定于语言的扫描。
- 使用漏洞数据库运行跟踪。
- 使用来自全局模式规则库的模式规则来运行基于模式的扫描。

您可以使用定制规则将 AppScan Source 安全知识库定制为符合您的特定安全性标准，并在整个企业内一致地应用这些标准。您还可以定制模式规则。

扩展 AppScan Source 安全知识库

本节描述如何定制数据库以及将定制的漏洞和其他例程集成到扫描中。定制规则将 AppScan Source 安全知识库（或漏洞数据库）定制为符合您的特定安全性标准，并在整个企业内一致地应用这些标准。

指定您自己的验证和编码例程或者将特定应用程序编程接口 (API) 定义为漏洞、接收器和源、感染传播器或参考项常常变得很重要。创建这些规则时，会定制和扩展 AppScan Source 漏洞数据库（AppScan Source 安全知识库不可或缺的一部分）。一旦向该数据库添加了定制规则，AppScan Source for Analysis 便会在扫描期间识别该规则。对定制 API 的调用会被显示为安全性结果或扫描覆盖范围结果，然后会报告这些结果。

例如，分析人员可能添加名为 `readBuffer( )` 的 API（类型为 `BufferOverflow`）。然后，后续扫描会在 AppScan Source for Analysis 发现符合此新 API 的规范的漏洞时引用此新 API。要获取关于漏洞类型的更多详细信息，请参阅 AppScan Source 安全知识库（在工作台主菜单中选择**帮助** > **安全知识库**）。

如果添加定制验证和编码例程，那么 AppScan Source for Analysis 不再将传入和传出这些例程的数据视为易受攻击。通过向知识库添加定制例程，AppScan Source for Analysis 确定数据是否无需验证或编码即可从已感染输入源流到输出。

注：AppScan Source 安全知识库不提供针对定制记录的联机帮助，但会显示针对漏洞类型的帮助。

要点： 您必须拥有知识库管理许可权才能对 AppScan Source 安全知识库作出更改。

创建定制规则

在"定制规则"视图中，您可以打开"定制规则向导"，该工具会指导您完成创建定制数据库记录的过程。一旦创建定制规则，就可以在"定制规则"视图中查看这些规则。该表显示签名、语言和用途。

如果规则应用于的项目存在于"资源管理器"视图中的**所有应用程序**下的某个应用程序中，那么特定于项目的验证和编码例程仅显示在"定制规则"视图中。

© Copyright IBM Corp. 2003, 2017

- **签名**：签名是标准函数名。例如，Java 签名包含参数和返回类型，如 `com.test.vulnerable.VulnClass.vulnerable(java.lang.string;int):int`。
- **语言**：C/C++、Java、Visual Basic、Classic ASP 或 .NET
- **用途**：关于给定方法的定制记录类型，如 `Validation.EncodingRequired` 例程、接收器或源。

提示：如果要通过迭代扫描和添加定制规则，然后在不更改源代码的情况下重新扫描来优化代码库的评估，那么您可以通过将项目属性设置为使用漏洞分析高速缓存来极大地减少扫描时间。要执行此操作，请在项目属性中选中**启用漏洞分析高速缓存**复选框。要了解如何设置项目属性，请参阅关于使用第 215 页的『选定项目"概述"选项卡』的指示信息。

使用"定制规则"向导

定制规则向导帮助您将方法添加到 AppScan Source 安全知识库。大部分定制规则的作用域是全局的（应用于所有项目）。定制无跟踪结果、源、接收器和感染传播器始终是全局的。定制验证/编码例程不是全局的。

注："定制规则"向导没有验证您的选择。例如，您可能定义一条定制规则，该规则将某个方法标识为感染传播器和接收器，这不是有效的方案。

定制规则向导指引您完成定义以下项并将其添加到知识库的过程：

- 源和接收器
- 感染传播器
- 不易感染的应用程序编程接口 (API)
- 漏洞
- 生成没有跟踪的结果的 API
- 不是验证/编码例程的 API
- 感染的回调
- 参考性结果

（感染）源

向程序提供输入的方法，这些输入可能格式错误或者是恶意的。

（易受感染的）接收器

一个将数据从程序（或者程序的可见部分）发出到文件、网络、数据库、其他库的 API 或者易于收到恶意输入的设备。

感染传播器

将某个方法标记为感染传播器将暗示如果从未验证的输入数据（感染的数据）派生 API 的任何参数，调用后，其他参数引用的非常量数据以及返回值也可能受到感染。此类数据必须验证或编码，然后发送到接收器。因为来自感染参数的数据复制或附加到其他参数，或者被返回，所以通常发生此情况。

不易于感染

将 API 标记为不易于感染（非感染传播器）暗示使用从未验证的输入数据（感染数据）派生的参数调用 API 不会使 API 行为不安全或有恶意行为。

如果已感染数据接触到调用，但该调用标记为不易受感染，那么 AppScan Source 会在跟踪方面忽略该调用。AppScan Source 跟踪不报告丢失的跟踪，并且不会将所传播的数据视为已感染。

注： 如果感染的数据访问验证或编码例程、接收器、感染传播器以外的方法，或不易于感染的方法，那么此方法会报告为丢失的跟踪。非常量参数和返回值不一定受到感染。AppScan Source 跟踪调用图会显示丢失的跟踪。

非跟踪结果

始终显示为结果但不生成跟踪的方法或 API。

非验证/编码例程

将 API 标记为**非验证/编码例程**将标识此 API 没有验证任何数据。

感染的回调

回调是您代码中一般由其他代码（例如，来自低级框架）调用的例程。将回调作为参数传递到其他代码，稍后以可能感染的参数来对其进行调用。如果怀疑回调可能将感染的数据传递到其参数，您可以将其标记为感染的回调。这使感染数据在例程内的分布变为可见。

对标记为感染回调的例程进行分析，就像该例程在调用图的根处一样（换言之，由某个未知的外部调用者调用），其所有输入参数被认为已感染。因此，AppScan Source 将报告具有从已感染回调参数开始的跟踪的结果。

如果您的应用程序代码在其他上下文中调用同一例程，那么在对其进行处理时，不会有对感染的任何特殊考虑。在这些上下文中，将进行通常的分析。

参考信息

虽然标识为参考性结果的代码行可能不易受到攻击，但是应该包含在安全审计中。

添加规则

本任务主题描述使用"定制规则向导"添加定制规则的过程。

关于此任务

注：添加或除去安全性结果或扫描覆盖范围结果以及更改严重性会影响项目的 V-Density。

过程

1. 通过单击**启动定制规则向导**按钮来从"定制规则"视图打开此向导。
2. 在**选择应用程序、项目和文件**页面中，选择规则将应用于的**应用程序**和**项目**。确定当前应用程序和项目与您要添加到知识库的项的源代码相关。选择**配置**（如果可用）。

3. 在**范围**部分中，设置扫描的范围。根据您要扫描的语言，提供以下范围选项：

表 *21.* 项目文件选项（按语言）

语言	项目文件选项
.NET	• **扫描整个项目以查找方法特征符** • **选择项目之外的一个或多个文件** .NET 项目包含任何有效组合件，一般为 .dll 或 .exe 文件。
Java	• **扫描整个项目以查找方法特征符** • **选择项目中的一个或多个文件** • **选择项目之外的一个或多个文件** Java 项目包含 .jar 或 .class 文件，或者类文件的目录层次结构。
C/C++	• **扫描整个项目以查找方法特征符** • **选择项目中的一个或多个文件**
Visual Basic	扫描 FRM（格式）文件、CLS（类）文件以及 BAS（基本）
Classic ASP	仅扫描 ASP 文件

- **扫描整个项目以查找方法特征符**是缺省扫描方式。此方式扫描整个项目并返回所有可用的特征符。此扫描方式可能很耗时。
- **选择项目中的一个或多个文件**选项会隔离包含可能需要定制规则的方法的特定项目文件。
- **选择项目外的一个或多个文件**选项会标识此项目外部的要包含在扫描中的文件。

4. 在**高速缓存**部分中，选中用来重新读取已修改的项目或已修改的代码的复选框。也将清除漏洞分析高速缓存（如果当前项目设置为将漏洞分析高速缓存，那么将在下一次扫描中重新创建漏洞分析高速缓存）。
5. **字符串分析**：字符串分析监控 Java 或 Microsoft .NET 项目中的字符串操控。它能够自动检测清理器和验证器例程。通过此检测，可减少错误的肯定和否定。选择**启用字符串分析以查找验证器/清理器函数**复选框以启用字符串分析。**将导入的规则应用于全局作用域**复选框确定是将发现的清理器和验证器例程应用于单个项目，还是在全局级别上应用（应用于所有项目）。

   注：字符串分析的应用会降低扫描速度。因此，建议您仅在代码更改后应用它，然后为后续扫描将其禁用。此外，应该将发现的例程作为建议查看并由审计员复审。可以在"定制规则"视图中查看这些例程。
6. 单击**下一步**以继续到向导中的下一页。
7. 在**选择方法**页面中：
   a. 选择要添加到 知识库的一个或多个方法。方法是易受攻击的 API 的名称。

      可以通过以下两种方式来对方法列表进行过滤：
      - 自动过滤：在**过滤器**字段中输入过滤器文本。在您输入时，过滤器将自动应用于方法列表。这是缺省过滤方式。

- 手动过滤：在**过滤器**字段中输入过滤器文本，然后单击**过滤**按钮（或按 Enter 键）以将过滤器应用于列表。当大量方法导致自动过滤延迟时，您可能希望使用手动过滤。

在这两种情况下，都可以使用星号 (*) 和问号 (?) 字符作为通配符。星号与任意一组的零个或更多字符匹配，而问号与任意单个字符匹配。

要更改过滤方式，请将**过滤**按钮用作切换按钮，方法是：双击该按钮，或者使用键盘导航至该按钮，然后按空格键。当手动过滤开启后，**过滤**按钮会显示为未按下，并且其悬浮式帮助会显示**应用过滤器（双击按钮或按空格键以自动过滤）**。当自动过滤开启后，该按钮显示为已按下，并且其悬浮式帮助会显示**手动过滤**。

为更好地查看方法列表，提供了展开和折叠操作。要展开或折叠整个树，请右键单击并选择**全部展开**或**全部折叠**。要展开某个软件包或类及其所有子条目，请右键单击此软件包或类，然后选择**展开子代**。

选择多个方法，请使用键盘 Ctrl 或 Shift 键。

选中**显示完整签名**复选框可显示树中方法的标准签名。例如，标准的 Java 签名包含软件包、类、方法、参数类型和返回类型，例如 `com.test.vulnerable.VulnClass.vulnerable(java.lang.string;int):int`。

b. 确定扫描是否应将方法标记为以下某项：
   - 第 200 页的『（感染）源』
   - 第 200 页的『（易受感染的）接收器』
   - 第 200 页的『感染传播器』
   - 第 201 页的『不易于感染』
   - 第 201 页的『非跟踪结果』
   - 第 201 页的『非验证/编码例程』
   - 第 201 页的『感染的回调』
   - 第 201 页的『参考信息』

8. 如果将方法添加为 第 201 页的『不易于感染』、第 201 页的『非验证/编码例程』、第 200 页的『感染传播器』 或 第 201 页的『感染的回调』，单击**完成**以将记录添加到 AppScan Source 安全知识库。
9. 如果将方法添加为 第 200 页的『（感染）源』 或 第 201 页的『参考信息』：
   a. 单击**下一步**以前进到**分配规则属性**页面。
   b. 对于已添加的每个方法：选择要分配到方法的一个或多个属性。方法的**类型**列将更新以指示定制规则将生成的结果的漏洞类型。

      提示：要将相同属性添加到多个方法，使用键盘 Ctrl 或 Shift 键来选择多个方法，然后选择想要分配到方法的属性。

   c. 单击**完成**以将记录添加到 AppScan Source 安全知识库。
10. 如果将方法添加为 第 200 页的『（易受感染的）接收器』：
    a. 单击**下一步**以前进到**分配规则属性**页面。
    b. 对于已添加的每个方法：
       - 选择漏洞影响的**严重性**级别：**高**、**中**或**低**。

- 选择要应用于方法的**漏洞类型**。

  提示：要将相同属性添加到多个方法，使用键盘 Ctrl 或 Shift 键来选择多个方法，然后选择想要分配到方法的属性。

c. 单击**完成**以将记录添加到 AppScan Source 安全知识库。

11. 如果将方法添加为 第 201 页的『非跟踪结果』：
    a. 单击**下一步**以前进到**分配规则属性**页面。
    b. 对于已添加的每个方法：
       - 选择漏洞影响的**严重性**级别：**高**、**中**或**低**。
       - 选择要分配给方法的**分类**：**明确**、**可疑**或**配置**。
       - 选择要应用于方法的**漏洞类型**。

       提示：要将相同属性添加到多个方法，使用键盘 Ctrl 或 Shift 键来选择多个方法，然后选择想要分配到方法的属性。

    c. 单击**完成**以将记录添加到 AppScan Source 安全知识库。

Likelihood 规则属性

`Attribute.Likelihood.High` 和 `Attribute.Likelihood.Low` 属性是内置规则的一部分，可在创建定制规则时使用。

在 AppScan Source 中，*likelihood* 代表安全结果可被利用的可能性和机会。AppScan Source 采用 https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology#Step_2:_Factors_for_Estimating_Likelihood上提供的发生可能性的定义，并通过基于跟踪属性确定发生可能性来对其进行优化。通过提供一组跟踪属性（例如源 API 名称、源 API 类型、源技术或源机制），AppScan Source 确定将来可能或将要通过使用特定脆弱性来利用跟踪的可能性。

发生可能性与跟踪的源元素联系紧密。源是对程序的输入，如文件、servlet 请求、控制台输入或套接字。对于大多数输入源，返回的数据在内容和长度方面没有限制。当输入未检查时，将被认为是污染源。

发生可能性的示例包括：

- 如果提供了 HTTP 源的跟踪（例如 `Request.getQueryString`）和跨站点脚本编制接收器（例如 `Response.write`），那么将确定较高的可能性，因此提高结果的置信度。
- 如果提供了系统属性源的跟踪（例如 `getProperty`）和跨站点脚本编制接收器（例如 `Response.write`），那么将确定较低的可能性，因此降低结果的置信度。

发生可能性用于识别必须立即进行操作或修订的高优先级可操作结果。它与高度可利用的污染源关系紧密，并为您提供了为结果分类的细粒度更高的方法。发生可能性在 AppScan Source 脆弱性数据库中存储为与污染源关系紧密的属性。该功能是现成可用的。

我们已进行了大量的搜索来确定源的发生可能性因子。通过使用"定制规则向导"，可将发生可能性信息添加到您添加到规则库的新污染源。这将改进从扫描生成的结果的分类，并因此提高整体类选工作流程的效率。

在"定制规则向导"中，可为**发生可能性**属性设置两个值（**高**和**低**）。值**高**意味着源非常容易被污染。换句话讲，污点进入系统的障碍非常低，使攻击者能够非常容易地手动

或自动地提交恶意数据。值**低**意味着通过该源输入恶意数据的障碍非常高。这可意味着要向源引入污点， 攻击者必须更深入的了解系统，而且必须具有能在受害者网络上进行操作的许可权。

通过 AppScan Source 跟踪来定制输入/输出跟踪

一些应用程序（尤其是 Web 应用程序）需要输入/输出跟踪来标识与 SQL 注入、命令注入和跨站点脚本编制相关的安全漏洞。通过 AppScan Source 跟踪，您可以指定用来消除对任何漏洞的报告的验证例程。如果尚未验证输入，那么其他所有输出将标记为漏洞。

用户定义的验证例程是处理输入数据的例程，并会确保到输出例程的传递过程的安全性。如果验证例程处理输入数据，然后将其传递到输出例程，那么不存在任何输入验证漏洞。开发者可指定自己的输入验证和编码例程以处理跟踪。

以基于模式的规则进行定制

AppScan Source 基于模式的扫描是根据定制搜索条件来对源代码进行的分析。基于模式的扫描类似于 grep（grep 搜索一个或多个文件以查找给定字符串或模式）。执行筛选的审计员或安全分析人员可能使用基于模式的扫描来搜索特定应用程序或项目中的特定模式。一旦将模式定义为漏洞类型，对您源代码的扫描会将该模式标识为漏洞。当 AppScan Source 找到匹配项时，该项会显示在结果表中。即开即用 AppScan Source 规则库包含预定义的规则和规则集（规则的集合）。

基于模式的扫描搜索正则表达式。正则表达式（常常称为模式）是按照特定语法规则来描述或匹配一组字符串的字符串。您可以通过创建规则来指定搜索。规则与您在"定制规则"视图中添加到 AppScan Source 安全知识库的定制规则类似。创建规则时，您将定义严重性、分类、漏洞类型和其他条件。

第 242 页的『"模式规则库"视图』 使您能够新建模式规则和规则集，并修改或除去现有规则和规则集。然后，使用选定应用程序的"属性"视图、选定项目的"属性"视图或扫描配置来应用模式规则和规则集（还可以启动使您能够从这些视图新建规则的对话框）。要了解关于应用规则和规则集的更多信息，请参阅第 210 页的『应用模式规则和规则集』。

可以创建的模式规则示例包括：

- 文件名模式匹配
- 具有多个模式的单一规则
- 缺席规则

注： 您必须具有**管理模式**许可权才可以创建模式规则或规则集 - 或修改和除去定制规则和规则集。

模式规则集

模式规则集是模式规则的集合。您可以添加新的模式规则集，也可以修改或除去现有扫描规则集。AppScan Source 提供一系列特定于语言的模式规则集，您可以选择将其应用于项目或应用程序（例如，您可能希望将 **Java** 模式规则集应用于 **Java/JSP** 项目）。

第 242 页的『"模式规则库"视图』 使您能够新建模式规则和规则集，并修改或除去现有规则和规则集。然后，使用选定应用程序的"属性"视图、选定项目的"属性"视图或扫描配置来应用模式规则和规则集（还可以启动使您能够从这些视图新建规则的对话框）。要了解关于应用规则和规则集的更多信息，请参阅第 210 页的『应用模式规则和规则集』。

AppScan Source 随附的一部分模式规则集不包含任何规则。您可以将适合贵组织的规则添加到这些规则集。这些规则集包括：

- ColdFusion
- JQuery
- 客户机端 JavaScript
- Visual Basic 6
- MooTools

提示：在"模式规则库"视图中，右键单击某个规则集并选择**属性**以打开一个对话框，该对话框显示有关规则集的信息。 "规则集属性"对话框提供信息，例如模式规则集中的规则数以及与其他规则集的父/子关系。它还使您能够修改规则集的**显示名称**和**项目类型**。

注： 您必须具有**管理模式**许可权才可以创建模式规则或规则集 - 或修改和除去定制规则和规则集。

在"模式规则库"视图中创建规则集

模式规则集是模式规则的集合。要了解如何创建规则集，请遵循该主题中的指示信息。

开始之前

注： 您必须具有**管理模式**许可权才可以创建模式规则或规则集 - 或修改和除去定制规则和规则集。

过程

1. 在"模式规则库"视图中，单击**新建规则集**。
2. 在"新建规则集"对话框中的**名称**字段中输入规则集的名称。
3. 选择规则集将应用于的项目的一个或多个类型。
4. 单击**确定**。
5. 新规则集显示在规则列表中。您可以用两种方式之一填充规则集：
   a. 在模式规则部分中选择一个规则或多个规则，并将其拖放到规则集中。
   b. 在模式规则部分中选择一个规则或多个规则，然后右键单击所选内容并选择**添加到规则集**菜单项。在"选择规则集"对话框中，选择您要将这一个或多个规则添加到的规则集。

修改和除去规则集

可以在"模式规则库"视图中修改和除去现成模式规则集和您已创建的模式规则。

注： 您必须具有**管理模式**许可权才可以创建模式规则或规则集 - 或修改和除去定制规则和规则集。

修改规则集

可以对规则集进行以下修改：

- 您可以通过遵循第 206 页的『在"模式规则库"视图中创建规则集』中关于填充新规则集的指示信息将规则添加到现有规则集。
- 要从规则集除去规则，选择一个或多个要除去的规则，然后执行以下操作之一：
  - 单击**从集内除去规则**。
  - 右键单击并选择**从集内除去规则**。
- 您可以用两种方式之一将规则集添加到另一规则集：
  - 选择规则集，然后将其拖放到另一规则集。
  - 右键单击规则集，并选择**将规则集添加为子代**，然后在"选择规则集"对话框中，选择您要添加为父规则集的规则集。
- 可修改规则集的**显示名称**和**项目类型**：右键单击规则集，并选择**属性**来打开"规则集属性"对话框。在该对话框中，可编辑**显示名称**字段，或者可单击**属性类型**字段**编辑**按钮来选择一个或多个项目类型。

除去规则集

要除去规则集，将其选中，然后执行以下操作之一：

- 单击**除去规则集**。
- 右键单击并选择**除去**。

模式规则

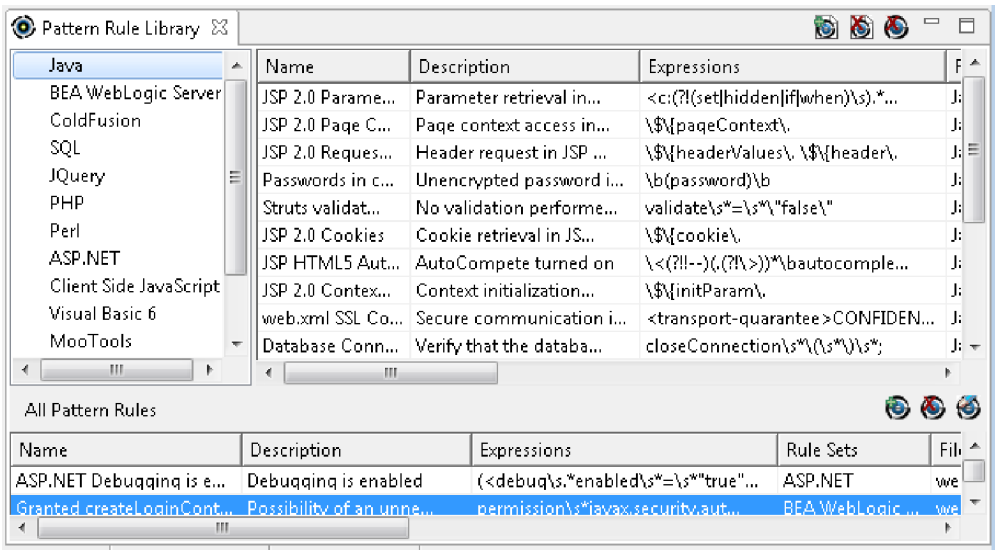
AppScan Source 文本规则可以是扩展全局正则表达式打印 (egrep)、全局正则表达式 (grep) 或 Perl 正则表达式。这些正则表达式（具有使用字母数字和特殊字符的完整集合的字符串值的表达式）匹配规则。

字符	描述
^	开头
$	结尾
\n, \t 或 \r	字面值换行、跳格、返回
[xyz]	列出的任何字符
[^abx]	任何字符（除了列出的字符）
[a-fA-F0-9]	任何十六进制字符
.	任何字符
|	任一
\	取消特殊字符含义 \$ \^ \\ \?

模式规则存储在全局模式规则库中（在 AppScan Source 数据库 中）且可以跨项目和应用程序共享。规则和规则集还可以由所有用户共享。规则是通过引用添加的，您可以通过除去关联对象中的引用来予以禁用，而不必删除底层的规则。

您在"模式规则库"视图、"资源管理器"视图的"属性"选项卡或扫描配置中创建规则。如果安装 AppScan Source，那么"模式规则库"视图会显示 AppScan Source 提供的规则。

在此视图中，您可以编辑、删除或创建规则。



要点： 您可以添加或除去搜索条件，但是每个基于模式的规则必须至少具有一个搜索条件。

搜索文本模式

在给定的源文件内，基于模式的扫描按扩展名在文件中搜索文本模式，允许在源文件、XML 配置文件和其他文本文件中执行搜索。

例如，您可能希望创建模式搜索以确保不当的电子邮件地址没有硬编码到应用程序中。在此情况下，如果您希望确保应用程序没有使用公司电子邮件地址，您可以搜索模式，例如 `.*@mycompany.com`。

示例

此模式查找	模式
电子邮件地址	`[A-Za-z]\.[A-Za-z]@[A-Za-z][A-Za-]\.com`
模式的所有实例，例如 `passWord =`	`[Pp][Aa][Ss][Ss][Ww][Oo][Rr][Dd]\W*=`
MD5 散列算法的所有实例	`getInstance[[:space:]]*\([[:space:]]*"MD5`

创建模式规则

规则可在"模式规则库"视图中、项目或应用程序的"属性"视图中或在扫描配置中创建。

开始之前

注： 您必须具有**管理模式**许可权才可以创建模式规则或规则集 - 或修改和除去定制规则和规则集。

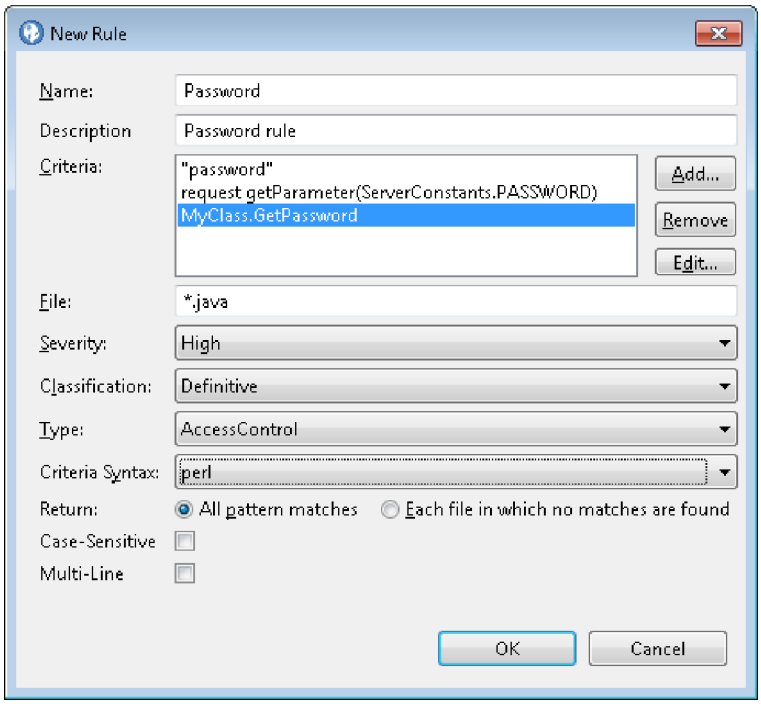
在"新建规则"对话框中创建规则：

- 要在"模式规则库"视图中打开该对话框，单击**新建规则**。
- 在扫描配置中，选择"模式分析"选项卡，然后选择**模式分析**复选框。在选项卡的"模式规则"部分中，单击**添加**以打开"添加模式规则"对话框。在该对话框中，单击**新建规则**以打开"新建规则"对话框。

- 要从选定应用程序或项目的"属性"视图打开该对话框，选择"属性"视图的**规则和规则集**选项卡，单击**添加**，或在"规则"部分中右键单击并选择**添加**。在"选择规则"对话框中单击**新建规则**。

过程

1. 在"新建规则"对话框中，**命名**扫描规则。
2. 可选： 为规则添加**描述**。
3. 添加**条件**。单击**添加**并输入每条规则的正则表达式。
4. 标识文件类型，例如 `*.java` 或 `*.xml`。您可以使用或者不使用通配符来输入任何文件类型。
5. 可选： 选择**严重性**：
   - **高**
   - **中**
   - **低**
   - **参考**
6. 可选： 选择**分类**：
   - **明确**
   - **可疑**
   - **扫描覆盖范围**
7. 可选： 选择要在扫描中搜索的漏洞类型。（有关漏洞类型的更多详细信息，请参阅 AppScan Source 安全知识库）



8. 可选： 选择条件语法：
   - **egrep**
   - **grep**
   - **perl**

9. 可选： 确定返回的结果包含**所有模式匹配**还是**其中未找到匹配项的每个文件**。未找到匹配项时，模式为缺席规则。
10. 可选： 如果模式匹配应为区分大小写，请选择**区分大小写**复选框。
11. 可选： 如果规则应与跨多行的模式匹配，请选择**多行**复选框。
12. 单击**确定**以验证规则中的正则表达式是否有效。然后，将规则添加到模式规则库。

修改和除去模式规则

可以在"模式规则库"视图中修改和除去您已创建的模式规则。

注： 您必须具有**管理模式**许可权才可以创建模式规则或规则集 - 或修改和除去定制规则和规则集。

修改规则

要编辑规则，将其选中，然后执行以下操作之一：

- 单击**编辑规则**。
- 右键单击并选择**编辑**。

该操作打开"编辑规则"对话框，它允许您修改任何设置（除了规则名称）。

除去规则

选择一个或多个规则，然后执行以下操作之一：

- 单击**除去规则**。
- 右键单击并选择**除去**。

应用模式规则和规则集

规则和规则集在"属性"视图中或在扫描配置中的应用程序或项目级别上应用。在您以应用的规则扫描应用程序或项目后，或使用包含规则的扫描配置之后，规则搜索的结果将显示在包含结果的视图中。

在扫描配置中应用规则和规则集

要启用基于模式的扫描，选择**模式分析**复选框。执行该操作时，**模式规则集**和**模式规则**部分将变为已启用：

- 要添加规则集，单击**模式规则集**部分中的**添加**。这会打开"添加模式规则集"对话框，以允许您选择一个或多个规则集。选择规则集时，它所包含的规则将显示在对话框的右边，规则集适用的项目类型在**项目类型**字段中列出。单击**确定**以添加选定规则集。
- 要添加规则，单击**模式规则**部分中的**添加**。这会打开"添加模式规则"对话框，以允许您选择一个或多个规则。还可单击**新建规则**以创建新规则（请参阅第 208 页的『创建模式规则』）。如果创建新规则，那么该规则将添加到列表并被选中。选择或创建规则后，单击**确定**以将它们添加到扫描配置。

  提示：在"添加模式规则"对话框中，工具提示帮助指示用于每个规则的表达式。

使用"属性"视图应用规则和规则集

在"资源管理器"视图中选择项目或应用程序，然后对其"属性"视图的"模式规则和规则集"选项卡进行以下所列的修改。指定要应用于应用程序或项目的规则和规则集后，保存应用程序或项目属性。然后，应用程序或项目的后续扫描将包含这些规则。

- 要添加规则集，单击**规则集**部分中的**添加**，或者在该部分中右键单击并选择**添加**。这将打开"选择规则集"对话框，这使您能够选择要添加的规则集。
- 要除去某规则集以便在应用程序或项目的扫描期间不使用该规则集，选择该规则集并单击**除去**，或右键单击规则集并选择**除去**。
- 要添加规则，单击**规则**部分中的**添加**，或者在该部分中右键单击并选择**添加**。这将打开"选择规则"对话框，这使您能够选择要添加的规则。在该对话框中，还可单击**新建规则**来创建新规则（请参阅第 208 页的『创建模式规则』）。如果创建新规则，那么该规则将添加到列表并被选中。选择或创建规则后，单击**确定**以添加规则。
- 要除去某规则以便在应用程序或项目的扫描期间不使用该规则，选择该规则集并单击**除去**，或右键单击规则并选择**除去**。还可选择多个规则并使用这些操作除去这些规则。

"扫描配置"视图

通过"扫描配置"视图，您可以创建能够在启动扫描时使用的配置。还可以使用视图来设置缺省扫描配置。在扫描配置中，可以指定要在扫描期间使用的源规则，并且可以包含许多扫描设置。在扫描配置中进行的设置通常可以产生更佳的扫描结果，而能够保存这些设置，就可以使扫描更为轻松和省时。

"扫描配置"视图有以下主要部分：

- 第 99 页的『扫描配置管理』
- 第 99 页的『"一般"选项卡』
- 第 100 页的『"污染流分析"选项卡』
- 第 101 页的『"模式分析"选项卡』

扫描配置管理

使用此部分可选择、添加、除去、保存和共享扫描配置，以及将扫描配置设置为缺省配置。

- 要创建新扫描配置，请单击**新建**。完成扫描配置设置后，单击**保存**以保存更改。要将该扫描配置设置为缺省配置，请在将其保存后单击**选为缺省**。要了解如何使用缺省扫描配置，请参阅第 91 页的『扫描源代码』。
- 要处理现有扫描配置，请从列表中选择该配置：
  - 如果修改扫描配置设置，请单击**保存**以保存更改（通过切换到其他扫描配置，然后单击**放弃**，可以放弃不需要的更改）。
  - 要除去所选扫描配置，请单击**删除**。
  - 要复制此扫描配置，请单击**复制**。这样，将基于原始扫描配置的设置来创建新扫描配置。
  - 要将此扫描配置设置为缺省配置，请单击**选为缺省**。要了解如何使用缺省扫描配置，请参阅第 91 页的『扫描源代码』。

– 要将此扫描配置与他人共享，请单击**共享**。这会将此扫描配置保存到 AppScan Source 数据库。

注：要共享扫描配置，或者修改或删除已共享的扫描配置，您必须拥有**管理共享配置**许可权。要了解关于设置许可权的信息，请参阅《*IBM Security AppScan Source* 安装和管理指南》。

注：AppScan Source 提供内置扫描配置。不能修改或除去这些配置。在列表中选择这些配置后，您就能够复制它们或查看其设置。

"一般"选项卡

基本信息

通过此部分，您可以对扫描配置命名并为其提供描述。

过滤器

在该部分中，可选择每当使用配置时就会应用于扫描的一个或多个过滤器。选择过滤器时，可选择 AppScan Source预定义过滤器或共享过滤器或您已创建的过滤器。请参阅第 94 页的『管理扫描配置』以了解更多详细信息。

"污染流分析"选项卡

污染流分析

启用和设置污染流分析的范围。

扫描规则

使用此部分可确定哪些源规则将对扫描生效。

源是对程序的输入，如文件、servlet 请求、控制台输入或套接字。通过排除某些源规则，可加速扫描并避免检测您并不感兴趣的输入产生的漏洞。

规则通过规则属性进行了标记，以指示它们与特定漏洞、机制、属性或技术相关。这些属性分组为规则集，而规则集对应于一组常用的相关规则。可通过指定规则集或各个规则属性来限制扫描中包含的源规则。

- 选择要包含在扫描中的一个或多个漏洞类型（在规则集中按类型进行组织）：
  – **所有内容**：如果选择该项，将检测从所有受支持输入源产生的漏洞。
  – **用户输入**：如果选择该项，将检测最终用户的输入产生的漏洞。
  – **Web 应用程序**：如果选择该项，将检测 Web 应用程序风险产生的漏洞。
  – **错误处理和记录**：如果选择该项，那么将检测错误处理和日志记录机制产生的漏洞。
  – **环境**：如果选择该项，那么将检测配置文件、系统环境文件和属性文件产生的漏洞。
  – **外部系统**：如果选择该项，将检测外部实体产生的漏洞。
  – **数据存储**：如果选择该项，那么将检测数据存储（例如数据库和高速缓存）产生的漏洞。

- **异常内容**：如果选择该项，那么将检测通常不属于生产应用程序的例程产生的漏洞。
- **文件系统**：如果选择该项，将检测文件系统产生的漏洞。
- **敏感数据**：如果选择该项，将检测敏感数据产生的漏洞。

悬浮式文本描述此部分中的各规则集。

- 选择要包含在扫描中的各条扫描规则属性：单击**放弃所选规则集并让我选择个别规则属性**。这会打开"选择规则属性"对话框，以允许您选择个别规则属性。如果完成此对话框，将放弃已选择的任何规则集。具有选定规则属性的扫描规则将用于扫描。

高级设置

此部分旨在仅供高级用户使用。它包含可改进扫描结果的各种设置。悬浮式文本描述此部分中的各设置。

"模式分析"选项卡

模式分析

使用扫描配置时使用该部分来启用基于模式的扫描。基于模式的扫描是根据定制的搜索条件来对源代码进行的分析。

模式规则集和模式规则

使用这些部分可添加要在模式分析期间使用的规则和规则集。请参阅第 205 页的『以基于模式的规则进行定制』和第 94 页的『管理扫描配置』，以获取更多信息。

属性视图：选定应用程序

在此视图中，可配置选定应用程序的属性。应用程序属性取决于先前创建的全局属性。

- 『 概述』
- 『排除和过滤器』
- 第 214 页的『规则和规则集』
- 第 214 页的『已修改的结果』
- 第 214 页的『定制结果』

概述

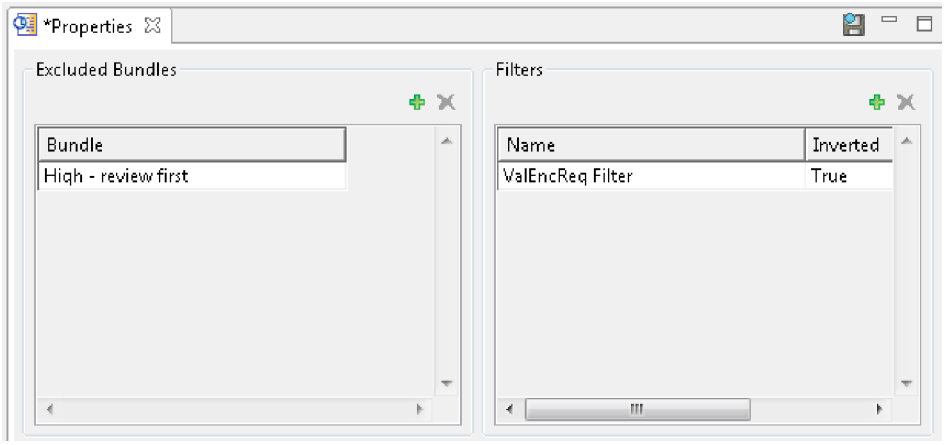
"概述"选项卡中显示：

- 应用程序名称。可以通过在该字段中输入新名称来重命名应用程序。
- 应用程序属性

排除和过滤器

该选项卡使您能够指定选定应用程序的现有过滤器，以及您想要如何应用过滤器（可直接应用过滤器，也可应用其反向过滤器）。在该选项卡中，还可以管理从扫描排除了结果的束。请参阅第 119 页的第 5 章, 『筛选和分析』以获取关于过滤器的信息，以及第 138 页的『全局应用过滤器』以获取关于全局地应用过滤器的详细信息。

已排除和已过滤的结果将不再出现于扫描结果中，也不再作为应用程序或项目度量中的因素。



规则和规则集

在"资源管理器"视图中选择应用程序时，"属性"视图中的"模式规则和规则集"选项卡允许您添加扫描应用程序时将应用的模式规则和规则集。使用基于模式的扫描来搜索希望显示为结果的文本模式。各个规则和规则集可应用于应用程序和项目。请参阅第 205 页的『以基于模式的规则进行定制』以了解有关基于模式的分析的信息，并参阅第 210 页的『应用模式规则和规则集』以了解有关如何在"属性"视图中应用规则和规则集的信息。

已修改的结果

在"已修改的结果"选项卡上，可查看、编辑或删除任何先前修改的结果，或者修改现有结果。已修改的结果是漏洞类型、严重性、分类或说明发生过更改的结果。

定制结果

在"定制结果"选项卡上，可查看、添加、编辑或删除定制结果。请参阅第 151 页的『定制结果』以了解更多详细信息。

属性视图：选定项目

在"属性"视图的此方式下，可配置选定项目的参数。项目属性取决于先前创建的全局属性。属性因选定项目而有所不同。

- 第 215 页的『选定项目"概述"选项卡』
- 第 216 页的『过滤器』
- 第 216 页的『模式规则和规则集』
- 第 216 页的『文件扩展名』
- 第 217 页的『源』
- 第 217 页的『JavaServer Page (JSP) 项目依赖性』
- 第 218 页的『项目依赖性』
- 第 218 页的『编译』
- 第 218 页的『优化』

- 第 218 页的『预编译选项卡（仅 ASP.NET）』

选定项目"概述"选项卡

"概述"选项卡中显示：

- 项目**名称**。可以通过在该字段中输入新名称来重命名项目。
- 项目**文件**名称和路径
- **项目类型**
- 配置：此部分显示目标配置。对于 .NET 和 C++ 项目，此部分显示已在"项目依赖性"选项卡中保存的目标配置。对于所有其他项目类型，此部分显示**缺省值**。
- 过滤器选项：选择**外部源中包含的过滤器结果**，以过滤出扫描项目源文件以外的文件中所发现的任何结果。如果项目以编译器生成的文件或临时文件（如 ASP.NET）来报告结果，那么该选项可降低其噪声。
- 漏洞分析高速缓存选项：如果通过迭代扫描并添加定制规则，然后在不更改源代码的情况下重新扫描，从而优化代码库的评估，那么您可通过将项目属性设置为使用漏洞分析高速缓存来大幅缩短扫描时间。要执行此操作，请在项目属性中选中**启用漏洞分析高速缓存**复选框。选中此复选框后第一次扫描项目时，将创建漏洞分析高速缓存。每次对项目进行后续扫描时，都将使用漏洞分析高速缓存，从而可缩短扫描时间。

  要清除漏洞分析高速缓存，以及启用 Java 递增分析时创建的高速缓存，单击**清除高速缓存**。下次扫描项目时，将发生完整扫描，并将创建新的漏洞分析高速缓存。在下列情况下，您可能希望清除高速缓存：

  – 上次扫描后，项目中的源代码已更改。
  – 已更改了项目配置，如添加或删除源文件。
  – 已更改代码配置选项。例如，如果要扫描 Java，且类路径已经更改，那么您可能希望清除高速缓存；或者如果要扫描 C 或 C++，且已更改了 include 路径或预处理器定义，也可能希望清除高速缓存。
  – 您已启用了 Java 递增分析并想要运行完整扫描，或者您将要遇到可能通过清除高速缓存来进行补救的问题。请参阅第 101 页的『Java 的递增分析』以了解更多信息。

  注：还可通过在"定制规则向导"中创建定制规则时选中**清除高速缓存**复选框来清除漏洞分析高速缓存。
- **字符串分析**：字符串分析监控 Java 或 Microsoft .NET 项目中的字符串操控。它能够自动检测清理器和验证器例程。通过此检测，可减少错误的肯定和否定。选择**启用字符串分析以查找验证器/清理器函数**复选框以启用字符串分析。**将导入的规则应用于全局作用域**复选框确定是将发现的清理器和验证器例程应用于单个项目，还是在全局级别上应用（应用于所有项目）。

  注：字符串分析的应用会降低扫描速度。因此，建议您仅在代码更改后应用它，然后为后续扫描将其禁用。此外，应该将发现的例程作为建议查看并由审计员复审。可以在"定制规则"视图中查看这些例程。
- **文件编码**：必须对项目中文件的字符编码进行相应设置，以便 AppScan Source 能够正确读取这些文件（并且例如，在源视图中正确显示这些文件）。

注：AppScan Source 项目的缺省文件编码为 **ISO-8859-1**。此缺省文件编码可在"常规"首选项页面中进行更改。

过滤器

该选项卡使您能够指定选定项目的现有过滤器，以及您想要如何应用过滤器（可直接应用过滤器，也可应用其反向过滤器）。请参阅第 119 页的第 5 章, 『筛选和分析』以获取关于过滤器的信息，以及第 138 页的『全局应用过滤器』以获取关于全局地应用过滤器的详细信息。

模式规则和规则集

在"资源管理器"视图中选择项目时，"属性"视图中的"模式规则和规则集"选项卡允许您添加扫描项目时将应用的模式规则和规则集。使用基于模式的扫描来搜索希望显示为结果的文本模式。各个规则和规则集可应用于应用程序和项目。参阅第 205 页的『以基于模式的规则进行定制』以了解有关基于模式的分析的信息，并参阅第 210 页的『应用模式规则和规则集』以了解有关如何在"属性"视图中应用规则和规则集的信息。

文件扩展名

使用该选项卡可为项目配置或添加有效的文件扩展名，从扫描排除文件，并将扩展名指定为 web 文件。

文件扩展名部分列出了已在当前项目类型的第 88 页的『项目文件扩展名』首选项页面中全局设置的扩展名（可使用**文件扩展名集**菜单为其他项目类型选择文件扩展名）。要从当前项目的扫描排除扩展名，在列表中选择扩展名，并单击**排除扩展名**。这会导致扩展名在选项卡的**已排除的扩展名**部分中列出。

要为项目添加其他扩展名，在**其他扩展名**部分中选择**添加扩展名**，然后输入文件扩展名，并指示是应该扫描带有该扩展名的文件，将其视为 web 文件还是将其排除。

表 22. 文件扩展名设置

设置	描述	用法示例
扫描或**评估**	包含带有在完整分析中指示的扩展名的文件。	• 如果已为 Java 项目创建 .xxx 扩展名并将此扩展名标记为**扫描**或**评估**，那么将编译并扫描具有该扩展名的文件。 • 如果不应编译和扫描某个文件（例如 C++ 中的头文件），那么该文件是项目的一部分但不被标记为**扫描**或**评估**。这些文件应包含在项目中，而且应在基于模式的分析过程中进行搜索。.

表 22. 文件扩展名设置 (续)

设置	描述	用法示例
Web 文件	用针对 JSP 编译的指定扩展名标记文件。该设置使 AppScan Source 能够将 web 源与非 web 源分开。	如果已为 Java 项目创建 .yyy 扩展名并将此扩展名标记为 **Web 文件**，那么具有该扩展名的文件将被安排为项目中的 Web 源。当 AppScan Source 为分析做准备时，这些文件将被预编译为类以进行分析。
排除	请勿在项目中为带有指定扩展名的文件创建源文件。将不会扫描带有该扩展名的文件。	为项目需要进行编译的文件创建 .zzz 扩展名，但无需包含在分析中。

源

指定扫描中将包含的源。

- 工作目录：AppScan Source 项目文件 (ppf) 的位置和所有相对路径的基础。
- **添加源根目录**和**除去源根目录**："源"选项卡显示为来自"项目配置向导"的项目或在已导入 ppf 中定义的项目建立的属性。

  仅当选择**源根目录**图标时，**除去源根目录**才可用。它用于除去源代码根目录。
- 查找源代码根目录（仅 Java 项目）：允许 AppScan Source for Analysis 自动查找所有有效的源代码根目录。
- 项目文件在**源根目录**图标下列出。从扫描排除的文件具有红色文件图标（如果右键单击了排除的文件，那么其菜单中的**排除**被禁用，**包含**被启用。）要排除包含的文件，右键单击该文件并选择菜单中的**排除**。要包含排除的文件，右键单击该文件并选择菜单中的**包含**。

JavaServer Page (JSP) 项目依赖性

"JSP 项目依赖性"选项卡显示针对特定 JSP 项目建立的属性。

- 包含 Web (JSP) 内容：确定项目是否为包含 JavaServer Page 的 Web 应用程序。
- Web 上下文根：包含 WEB-INF 目录的 WAR 文件或目录。 Web 上下文根必须是有效 Web 应用程序的根目录。
- JSP 编译器：现成可用的 Tomcat 7 是缺省 JSP 编译器设置（缺省 JSP 编译器可以在 Java 和 JSP 首选项页面中进行更改）。要了解 AppScan Source 支持的编译器的相关信息，请参阅http://www.ibm.com/support/docview.wss?uid=swg27027486。

  Apache Tomcat V7 和 V8 包含在 AppScan Source 的安装中。如果未配置 **Tomcat 7** 和 **Tomcat 8** 首选项页面，那么 AppScan Source 将使用当前提供且标记为缺省选项的 Tomcat JSP 编译器来编译 JSP 文件。如果您想要运用外部受支持 Tomcat 编译器，请使用 Tomcat 首选项页面来指向本地 Tomcat 安装版。

  如果使用的是 Oracle WebLogic Server 或 WebSphere Application Server，那么必须将适用的首选项页面配置为指向应用程序服务器的本地安装版，以便其可在分析期间用于 JSP 编译。如果尚未完成该配置，那么选择 JSP 编译器时将显示一条消

息以提示您完成配置。如果单击消息中的**是**，那么您将被转至相应的首选项页面。如果单击**否**，那么 JSP 编译器选择旁边将显示一条警告链接（访问该链接将打开首选项页面）。

项目依赖性

"项目依赖性"选项卡显示项目属性。此选项卡上的配置设置会根据语言而不同，例如：

- 使用**选项**可以选择任何其他必需的编译器参数。
- JDK 设置特定于 Java。
- 预处理器定义特定于 C/C++ 代码。指定预处理器定义时，不要包含编译器的 `-D` 选项（例如，指定 `a=definition1` 而不是 `-Da=definition1`）。指定多个定义时，请使用分号分隔的列表。
- 目标配置仅可用于 .NET 和 C++ 项目。

编译

- 选项：项目配置所需的其他编译器参数。
- 使用 JDK：确定用于项目编译的 JDK，如首选项中所配置。请参阅第 77 页的第 3 章，『首选项』。

  Java 项目可能引用本地 Java Development Kit (JDK) 位置。当项目移动到服务器时，JDK 路径可能会不再有效。要将本地项目传输到服务器，必须确定各项目中指定已命名 JDK 的缺省 JDK 路径。

  注：JSP 项目的缺省编译器是 Tomcat 7，后者需要 Java V1.6 或更高版本。如果 **Tomcat 7** 保留为缺省值，那么使用更低版本的 JDK 将导致扫描期间出现编译错误。
- 验证：**验证**可确保正确配置项目依赖性。它检查 Java 项目中源和类路径之间 的配置冲突，并检查编译错误。如果类路径中的类在源根目录中重复出现，那么**存在冲突**。（如果存在冲突，请修改类路径以除去有冲突的类。）

  检查完冲突后，**验证**将确定项目是否编译和报告了任何编译错误。

优化

- **预编译类**：使用预编译 Java 或 JSP 类文件，而不是在扫描期间编译。选择后，此选项将禁用源登台选项。
- 将源文件登台以将编译错误的影响最小化：控制 AppScan Source 是否将源复制到登台目录。

  更正与目录不匹配的软件包需要 Java 编译以打开各源文件。

  清理扫描之间的登台区域将提高扫描之间的性能。

预编译选项卡（仅 ASP.NET）

预编译通过向 Web 站点中的特定页面（缺省情况下是 `precompile.axd`）发出 HTTP 请求来实现。此页面通过 `web.config` 中指定的特定 HTTP 处理程序进行处理。此处理程序可将整个站点（包括 `client.aspx`）编译到 .NET Framework 目录中的临时 ASP.NET 文件目录（然后在这里全部进行扫描）。

要扫描 ASP.NET 1.1，必须对 Web 站点进行相应配置，使之编译和构建了调试消息。从而，Web 站点编译和构建调试信息这一事实其本身就是安全漏洞。由于扫描需要，您可以安全地忽略此漏洞。然而，请确保您部署的应用程序在 web.config 中没有编译 debug=true。

要对 ASP.NET 1.1 Web 站点进行预编译，请将以下元素作为 web.config 元素的子代添加到 <system.web> 文件中：

```
  <httpHandlers><add verb="*" path="precompile.axd"
type="System.Web.Handlers.BatchHandler"/></httpHandlers>
```

还应在编译元素中设置 debug=true。例如：

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <system.web>
  <httpHandlers><add verb="*" path="precompile.axd"
    type="System.Web.Handlers.BatchHandler"/>
    </httpHandlers>
      <compilation
        defaultLanguage="c#"
        debug="true"
   />
...
```

此元素指定 Web 站点的页面 precompile.axd 将通过特定 .Net System.Web.Handlers.BatchHandler 类进行处理。此类将 Web 站点的内容预编译到临时 ASP.NET 文件目录。

- Web 站点：预编译站点的请求目标。缺省位置是 precompile.axd。Precompile.axd 是虚拟文件，映射到 web.config 文件中指定的文件。
- 输出目录：作为预编译目标的目录。AppScan Source 在此目录中查找预编译输出。
- 预编译 ASP.NET Web 站点：AppScan Source 在扫描期间自动预编译并扫描已预编译的输出。
- 如果预编译失败，停止扫描：选择**>预编译 ASP.NET Web 站点**和**如果预编译失败，停止扫描**后，预编译失败时扫描将停止。否则，扫描将仅针对 Web 站点的主要输出继续。
- 立刻编译：扫描之前运行此测试，以查看基于当前设置的预编译是否成功。编译输出将在"预编译输出"窗格中显示。
- 其他组合件：对于任何 .NET 项目类型，请指定要扫描的其他组合件。
- 项目引用：列出了在其中搜索 .NET 组合件项目和现有 .NET 项目中所引用组合件的目录。

第 11 章 扩展应用程序服务器导入框架

AppScan Source 允许您从 Apache Tomcat 和 WebSphere Application Server Liberty 概要文件导入 Java 应用程序。您可以按照本主题中的说明，通过扩展应用程序服务器导入框架来从其他应用程序服务器导入 Java 应用程序。

关于此任务

应用程序服务器导入框架包含不通过 PDF 提供的随附 API 文档。如果您是通过 Adobe PDF 访问本帮助主题，那么只能通过以下方式来访问此 API 文档：启动 AppScan Source for Analysis 联机帮助并浏览至**扩展产品功能** > **扩展应用程序服务器导入框架** > **应用程序服务器导入扩展 API 类和方法**，或者在 http://www.ibm.com/support/knowledgecenter/SSS9LM/welcome 查找该部分帮助。

要扩展应用程序服务器导入框架，请完成以下步骤。这些步骤将让您执行以下操作：

- 配置 Eclipse 集成开发环境
- 在 Eclipse 中创建新插件
- 在新创建的插件中设置必要从属项
- 在该插件中定义应用程序服务器的扩展
- 测试该插件
- 为 AppScan Source for Analysis 启用该插件

过程

1. 为 AppScan Source 应用程序服务器导入框架所必需的从属项配置 Eclipse 集成开发环境：
   a. 在 Eclipse 中，从主菜单选择**窗口** > **首选项**。
   b. 在"首选项"对话框中，展开**插件开发**，然后选择**目标平台**。
   c. 在"目标平台"首选项页面中，单击**添加**以创建新目标定义。
   d. 在"目标定义"向导页面中，选择**无内容：从空目标定义开始**，然后按**下一步**。
   e. 在"目标内容"向导页面中的**名称**字段内输入目标的名称，然后单击**添加**以添加 AppScan Source 安装目录（请参阅第 275 页的『安装和用户数据文件位置』）。
   f. 可选： 选择**显示位置内容**以验证插件是否可用。
   g. 单击**完成**。
   h. 在"目标平台"首选项页面中，选择刚才创建的目标平台并按**应用**。然后按**确定**。
2. 在 Eclipse 中创建新插件：
   a. 从主菜单选择**文件** > **新建项目**以打开"新建项目"向导。
   b. 在"选择向导"页面中，选择**插件项目**，然后按**下一步**。
   c. 在"插件项目"页面中的**项目名称**字段内输入插件的名称（本帮助主题将使用 `com.example.appserverimporter` 来作为示例），然后按**下一步**。

© Copyright IBM Corp. 2003, 2017

d. 在"内容"页面中，取消选择**生成激活器（用于控制插件生命周期的 Java 类）**，然后按**完成**。

3. 在刚才创建的插件中，设置必要的从属项：
   a. 打开 META-INF\MANIFEST.MF，然后选择**从属项**选项卡。
   b. 在编辑器的**所需插件**部分中：
      - 单击**添加**，然后添加 com.ouncelabs.core.appserverimporter 和 org.eclipse.core.runtime。
      - 选择刚刚添加的 com.ouncelabs.core.appserverimporter 插件并单击**属性**。在插件属性中，除去**最小版本**和**最大版本**字段中的任何条目，然后单击**确定**。
      - 对 org.eclipse.core.runtime 插件重复上述步骤。
   c. 从主菜单选择**文件** > **保存**以保存已对编辑器所作的所有更改。
   d. 下一步将让您定义对应用程序服务器的扩展。对于该步骤，您将继续在 META-INF\MANIFEST.MF 编辑器中工作。
4. 按照以下步骤来为应用程序服务器定义导入器扩展：
   a. 选择**扩展**选项卡，然后单击**添加**以添加 com.ouncelabs.appserver，然后再从主菜单选择**文件** > **保存**。
   b. 选择 **plugin.xml** 选项卡。其内容应看起来类似于：

```
<?xml version="1.0" encoding="UTF-8"?>
<?eclipse version="3.4"?>
<plugin>
  <extension
    point="com.ouncelabs.appserver">
  </extension>
</plugin>
```

   通过编辑如下内容来完成扩展定义。例如：

```
<?xml version="1.0" encoding="UTF-8"?>
<?eclipse version="3.4"?>
<plugin>
  <extension
    point="com.ouncelabs.appserver">
    <importer
     class="com.example.appserverimporter.MyAppServerImporter"
     id="com.example.appserverimporter.myappserver"
     name="My App Server">
   </importer> </extension>
</plugin>
```

   c. 从主菜单选择**文件** > **保存**来保存已对 **plugin.xml** 做出的更改。
5. 创建导入器类（在本示例中为 com.example.appserverimporter.MyAppServerImporter）以定义新应用程序服务器导入器的行为。该类必须扩展 BaseAppServerImporter（框架对 AppServerImporter 接口的基本实施）。在该类中：
   a. 实施 AppServerImporter.importAppServer(String)。这供框架用来确定要导入的 Java EE 项目及其所在位置。通常情况下，仅需要每个 Java EE 项目的名称和路径。如果创建了 EAR 项目，那么在 AppScan Source 用户界面中选择项目时，所包含的 Java EE 项目将被隐藏。在此情况下，将导入整个 EAR。否则，将列出所有项目以供逐个进行选择。

      在适用情况下，高度建议使用以下方法：

- BaseAppServerImporter.processDropInsFolder(AppServerProfile, File)
- BaseAppServerImporter.processEARFile(AppServerProfile, File)

b. 实施 AppServerImporter.isValidLocation(String)。这用于在已给定安装目录的情况下检测服务器类型。

c. 可选： 覆盖 BaseAppServerImporter.getJSPCompilerType()。此方法将返回要用于 AppScan Source 项目的 JSP 编译器。如果未执行此操作，那么基本实施会返回空值，并且将使用产品缺省 JSP 编译器。

6. 可选： 作为高级选项，可以定制 JSP 编译以使用预编译的 JSP 编译器（JSP 编译将在导入之前或期间进行）：

a. 覆盖 BaseAppServerImporter.getJSPCompilerType() 以返回 JSPCompilerType.PRECOMPILED。

b. 覆盖 BaseAppServerImporter.getJSPCompilerType() 以调用 JMX、Java API 和外部脚本来编译 JSP 文件，或者只是将类文件复制到 AppScan Source 项目的登台目录。使用 Application.getStagingDirectory(Project) 以获取此登台目录。

c. 覆盖 BaseAppServerImporter.createJSPCompilerSupport() 以返回 JSPCompilerSupport 的定制扩展。这用于保持 JSP 文件与所生成类文件之间的映射，并用于在 JSP 编译后进行验证。

d. 覆盖 BaseAppServerImporter.createClasspathProvider() 以返回 AppServerClasspathProvider 的定制实施。编译对服务器库具有依赖性的任何 Java 或 JSP 文件时均需要该类。该类必须扩展 BaseAppServerClasspathProvider。请注意，调用 getClasspathEntries() 时，BaseAppServerClasspathProvider.installDirectory 将已经设置为应用程序服务器的安装目录。

7. 按以下步骤来测试插件：

a. 从主菜单选择**运行** > **运行配置**（或者如果要以调试方式进行测试，那么选择**运行** > **调试**）。

b. 创建新 **Eclipse 应用程序**配置。

- 转至此新配置的**主要**选项卡。在**要运行的程序**部分中，选择**运行产品**，然后将其设置为运行 **com.ouncelabs.osa.rcp.product**。
- 转至**参数**选项卡。在**工作目录**部分中，选择**其他**，然后在字段中输入 AppScan Source 数据目录（请参阅第 275 页的『安装和用户数据文件位置』）。
- 在**插件**选项卡中，将**启动方式**选项设置为**仅以下所选插件**。展开**工作空间**并确保选择已创建的插件，然后在**目标平台**下取消选择以下插件：
  - com.ouncelabs.plugin.base
  - com.ouncelabs.plugin.base
  - com.ouncelabs.plugin.base.nl
  - com.ouncelabs.plugin.base.nl
  - com.ouncelabs.plugin.enhanced
  - com.ouncelabs.plugin.enhanced
  - com.ouncelabs.plugin.enhanced.nl
  - com.ouncelabs.plugin.enhanced.nl

c. 单击"运行配置"对话框中的**运行**之前，请转至 AppScan Source 安装目录并运行 bin\OunceScanner.exe。

d. 返回到"运行配置"对话框并单击**运行**以启动 AppScan Source for Analysis 并测试插件。

8. 按以下步骤来为 AppScan Source for Analysis 启用插件：

a. 右键单击项目并选择**导出**。

b. 在"导出"向导的"选择"页面中，展开**插件开发**，选择**可部署的插件和片段**，然后单击**下一步**。

c. 在"可部署的插件和片段"页面中：

- 转至**目标**选项卡，并通过浏览至机器上的临时目录来设置**目录**。
- 转至**选项**选项卡，并选择**将插件打包为单独 JAR 归档**和**限定符替换**。
- 单击**完成**。

d. 找到已用作插件导出目标的临时目录，然后打开其 plugins\ 文件夹。在此文件夹中，找到已创建的 .jar 文件并将其复制到 <install_dir>\dropins（其中 <install_dir> 是 AppScan Source 安装位置）。

注：

- 如果 \dropins 目录不存在，那么您将需要手动予以创建。
- 变更 AppScan Source 安装目录可能需要管理特权。

e. 找到 <install_dir>\configuration\org.eclipse.equinox.simpleconfigurator\bundles.info。创建此文件的备份副本，然后编辑此文件并将以下内容添加到其末尾：

```
<my_plugin>,<my_plugin_version>,
dropins/<my_plugin>_<my_plugin_version>.jar,4,false
```

其中：

- <my_plugin> 是已创建的插件的名称。
- <my_plugin_version> 是已创建的插件的版本号。

注：在此条目的开头，<my_plugin>、<my_plugin_version> 和 dropins/ 位置以逗号 (,) 进行分隔。

f. 启动 AppScan Source for Analysis。

g. 从主菜单选择**帮助** > **关于 AppScan Source for Analysis**，然后单击**安装详细信息**。选择**插件**选项卡并确保其中列出了您的插件。

h. 关闭"安装详细信息"对话框并开始使用应用程序服务器导入框架。

第 12 章 AppScan Source for Analysis 样本

AppScan Source for Analysis 包含了可用于帮助您熟悉产品的样本应用程序。

安装 AppScan Source for Analysis 后，样本应用程序位于 <data_dir>\samples（其中 <data_dir> 是 AppScan Source 程序数据的位置，如第 275 页的『安装和用户数据文件位置』中所述） 中。

Java 应用程序样本：simpleIOT

simpleIOT 样本是一种小型的 Java 应用程序，其中包含了各种安全性漏洞。可将其手动导入到 AppScan Source for Analysis 工作台，或者可以导入样本随附的应用程序文件 (SimpleIOT.paf) 或项目文件 (SimpleIOT.ppf)。要了解如何添加应用程序和项目，请参阅第 27 页的第 2 章, 『配置应用程序和项目』。

在您将样本添加到 AppScan Source 后，可对其进行扫描并探索其结果。

用于了解 Framework for Frameworks 处理 API 的样本应用程序：F4FEjbExample.zip

该示例项目归档用于演示 Framework for Frameworks 处理 API。请参阅《*IBM Security AppScan Source Utilities* 用户指南》以获取更多信息。

© Copyright IBM Corp. 2003, 2017

第 13 章 AppScan Source for Analysis 工作环境

要充分利用 AppScan Source，您应该了解 AppScan Source for Analysis 工作环境背后的基本概念以及如何使用最适合于您的工作流程的选项。

AppScan Source for Analysis 工作台

AppScan Source for Analysis 工作流程在工作台中执行，后者由根据上下文而显示或隐藏的透视图、视图和编辑器组成。

透视图

产品中的三个透视图（配置、筛选和分析）都包含多个视图。虽然每个透视图打开时都带有缺省视图，但是您可以重新组织视图以定制每个透视图。帮助的第 237 页的第 14 章，『视图』部分中详细描述了这些视图。

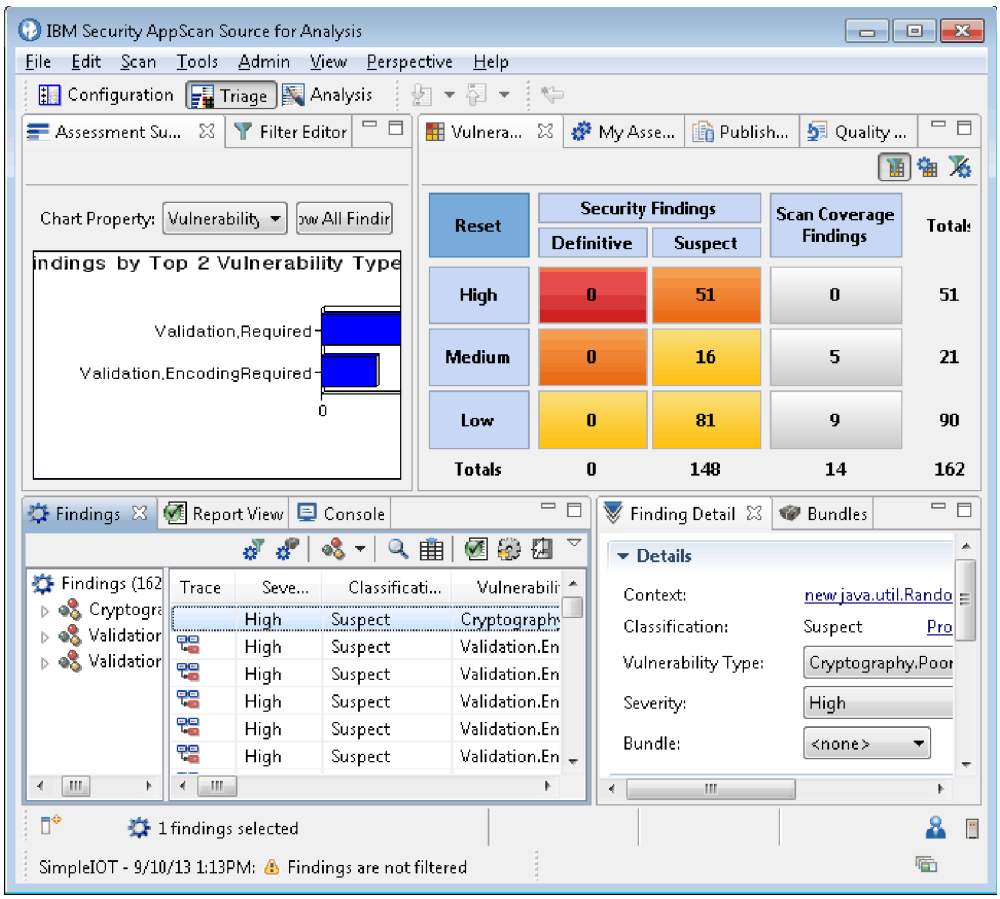
- 配置透视图：创建和管理应用程序、项目和属性。
- 筛选透视图：查看扫描结果以设置补救工作流程优先级，并从潜在漏洞中分离出真实漏洞。此透视图可用于隔离需要首先修复的问题。
- 分析透视图：向下钻取到单独结果，并复审源代码、补救建议和 AppScan Source 跟踪信息。

工作台窗口

AppScan Source for Analysis 工作台窗口由以下元素组成：

- 主菜单：用于访问 AppScan Source for Analysis 功能的菜单
- 工具栏：常用功能的图标和按钮
- 透视图：视图的集合
- 视图：用来浏览工作台中信息的表示法和方式

© Copyright IBM Corp. 2003, 2017



工作台底部的工具栏和信息

- **快速视图**工具栏：快速视图是可快速打开和关闭的隐藏视图。它们与其他视图的功能类似，区别在于它们不会占用工作台窗口中的空间。快速视图由快速视图栏上的工具栏按钮表示，快速视图栏是工作台窗口左上角的工具栏。单击快速视图的工具栏按钮时，该视图将在当前透视图中临时打开（与其重叠）。在您单击该视图之外的区域或视图失去焦点时，将再次隐藏。要将视图设置为快速视图，请单击**将视图显示为快速视图**，然后从菜单选择视图。
- 选定结果：选择结果后，工作台底部的指示符将显示选定结果的数量。
- 源文件信息：源文件打开时，关于该文件的信息将显示在工作台的底部。
  - 文件是可写的还是只读的。如果尝试编辑只读文件，AppScan Source for Analysis 中的提示将使您能够将文件设置为可写。
  - 操作系统输入方式是插入还是覆盖。
  - 文件中的当前光标位置（行和列标题）。
- 服务器连接信息：光标悬停在用户图标上将指示当前登录到 AppScan Enterprise Server 的用户，光标悬停在服务器图标上使您能够查看 AppScan Source for Analysis 所连接的 AppScan Enterprise Server。
- 评估打开时，工作台底部包含了该信息：
  - 评估的名称，以及创建评估的日期和时间。
  - 使您能够快速确定过滤器如何应用到评估中的结果的指示符。请参阅第 139 页的『确定所应用的过滤器』以了解更多信息。

- 进度指示符也会显示在工作台的底部，指示正在进行的操作。例如，扫描和评估发布期间该指示符将出现。此外，该部分还指示评估何时处于打开状态。

主菜单

主菜单栏包含了使您能够执行各种操作的菜单。您的用户特权可能会对这些菜单中可供您使用的命令进行管控。

- 『文件菜单』
- 第 232 页的『编辑菜单』
- 第 233 页的『扫描菜单』
- 第 233 页的『"工具"菜单』
- 第 234 页的『管理菜单』
- 第 234 页的『"视图"菜单』
- 第 234 页的『"透视图"菜单』
- 第 235 页的『帮助菜单』

文件菜单

文件菜单提供用于应用程序、项目和评估的选项，并且允许您编辑产品。某些**文件**菜单项是上下文相关的项，并依赖于活动视图以及该视图中当前选择的项。

表 *23.* 文件菜单

菜单项	描述	键盘快捷键
添加应用程序 > 创建新应用程序	将新应用程序添加到应用程序集。此操作会启动"新建应用程序"向导。	Ctrl+N
添加应用程序 > 打开现有应用程序	这会启动"打开"对话框，您可以通过此对话框来浏览到现有应用程序并将其添加到应用程序集。可以添加的文件或目录类型包括 .paf、.sln、.dsw 和 .ewf。	Ctrl+O
添加应用程序 > 导入现有基于 Eclipse 的工作空间	这会启动"添加工作空间"对话框，您可以通过此对话框来添加包含了 Java 项目的现有 Eclipse 或 IBM Rational Application Developer for WebSphere Software (RAD) 工作空间。导入了此工作空间后，您将能够扫描其包含的任何 Java 项目。 **注：**导入工作空间之前，请确定您已按照第 39 页的『配置 Eclipse 和 Rational Application Developer for WebSphere Software (RAD) 项目的开发环境』中所述安装并更新了开发环境。	

表 23. 文件菜单 (续)

菜单项	描述	键盘快捷键
添加应用程序 > 从应用程序服务器导入	从 Apache Tomcat 或 WebSphere Application Server Liberty 应用程序服务器导入现有 Java 应用程序。	
添加应用程序 > 多个应用程序	将多个应用程序添加到应用程序集合。此操作会启动一个对话框，您可以通过此对话框来指定要在其中搜索应用程序的目录。在搜索结果中，您可以选择一个或多个要添加的应用程序。	
添加应用程序 > 发现应用程序	这会启动 Application Discovery Assistant，它使您能够为 Java 和 Microsoft Visual Studio 源代码快速创建并配置应用程序和项目。	
除去应用程序	如果在"资源管理器"视图中选择了某个应用程序，那么此操作可用，而选择此操作会移除所选应用程序。	
添加项目 > 新建项目	如果在"资源管理器"视图中选择了某个应用程序，那么此操作可用，而选择此操作将使您能够向此应用程序添加新项目。此操作会启动"新建项目"向导。	
添加项目 > 现有项目	如果在"资源管理器"视图中选择了某个应用程序，那么此操作可用，而选择此操作将使您能够向此应用程序添加现有项目。此操作会启动一个对话框，您可以通过此对话框来浏览到要打开的 .ppf、.vcproj、.vcxproj、.csproj、.vbproj、.dsp 或 .epf 文件。	
添加项目 > 复制项目	如果在"资源管理器"视图中选择了某个项目，那么此操作可用，而选择此操作将打开一个对话框，您可以通过此对话框将此项目复制到另一个应用程序，或在当前包含此项目的应用程序中创建此项目的副本。	

表 23. 文件菜单 (续)

菜单项	描述	键盘快捷键
添加项目 > 多个项目	将多个项目添加到在"资源管理器"视图中选择的应用程序。此操作会启动一个对话框，您可以通过此对话框来完成以下任务之一： • 指定要在其中搜索项目的目录。 • 指定要在其中搜索项目的工作空间。 • 指定要在其中搜索项目的 Microsoft 解决方案文件。 在搜索结果中，您可以选择一个或多个要添加的项目。	
注册	向 AppScan Source 注册所选的应用程序或项目。您必须先注册应用程序和项目，然后才能将其发布到 AppScan Source 数据库。	
注销	注销所选的应用程序或项目。	
打开评估	这会启动"打开"对话框，您可以通过此对话框来浏览到 AppScan Source 评估文件。可打开的文件的类型包括 `.ozasmt` 和 `.xml`。	F7
关闭评估	关闭当前在"筛选"透视图中打开的评估。	
保存评估	将已打开评估保存到文件。	Ctrl+Shift+S
将评估另存为	以其他名称保存评估和/或将其保存在其他目录中。	
将评估发布到 AppScan Source	将当前评估存储在 AppScan Source 数据库中。必须先注册所扫描的应用程序（或应用程序包含的项目或文件），然后才能完成发布操作。如果您尚未注册应用程序，那么在选择发布操作时，系统将会提示您注册。	
将评估发布到 AppScan Enterprise Console	如果您的 AppScan Enterprise Server 已与 Enterprise Console 选件一起安装，那么可以向该选件发布评估。 必须先使用有效值填写 AppScan Enterprise Console 首选项页面，然后才能将评估发布到 Enterprise Console。	

表 23. 文件菜单 (续)

菜单项	描述	键盘快捷键
保存	此操作在以下情况下可用： • 应用程序的属性已在"属性"视图中被修改。 • 项目的属性已在"属性"视图中被修改。 • 内部编辑器中打开的文件已被修改。 选择此操作可保存这些更改。	Ctrl+S
退出	退出 AppScan Source for Analysis。	

注：要了解 AppScan Source for Analysis、AppScan Source for Automation 和 AppScan Source 命令行界面 支持哪些版本的导入文件，请参阅http://www.ibm.com/support/docview.wss?uid=swg27027486。在此页面中，选择您在使用的 AppScan Source 版本所对应的选项卡，然后选择您在使用的 AppScan Source 组件。如果 AppScan Source 支持从其他开发环境打开和扫描文件，该支持将在**受支持软件**选项卡的**编译器和语言**部分中列出。

编辑菜单

此菜单提供标准的修改和搜索/替换控件。此菜单还用于启动产品首选项。某些**编辑**菜单项是上下文相关的项，并依赖于活动视图以及该视图中当前选择的项。

表 24. 编辑菜单

菜单项	描述	键盘快捷键
剪切	复制并移除所选文本。对在控制台、编辑器或各种文本字段中选择的文本使用此操作。	Ctrl+X
复制	将所选文本复制到剪贴板。对在控制台、编辑器或各种文本字段中选择的文本使用此操作。	Ctrl+C
粘贴	粘贴已复制或剪切的文本。此操作通常用于创建信息的副本或者在产品的其他部分中重现信息。	Ctrl+V
重命名	重命名所选对象。可以重命名的对象包括应用程序、项目、评估和束。	F2
除去	移除所选对象。	删除
全选	选择文本的整体。对控制台、编辑器或各种文本字段中的文本使用此操作。	Ctrl+A
刷新	刷新所选应用程序、项目或视图的内容。	F5

表 *24.* 编辑菜单 *(续)*

菜单项	描述	键盘快捷键
查找	在控制台或编辑器中搜索文本，或者在结果表中搜索结果。	Ctrl+F
查找下一个	如果已使用查找操作在控制台或编辑器中搜索文本，那么使用此操作可查找此文本的下一个实例。	F3
首选项	选择此选项可打开"首选项"对话框。首选项是关于 AppScan Source for Analysis 的外观和操作的个人选项。	

扫描菜单

您从**扫描**菜单管理对所选应用程序、项目或文件的扫描。

表 *25.* 扫描菜单

菜单项	描述	键盘快捷键
全部扫描	扫描所有应用程序。扫描将使用缺省扫描配置来运行。	
扫描所选项	扫描所选应用程序、项目或文件。扫描将使用缺省扫描配置来运行。	F4
重新扫描	重新扫描评估目标。最近用来对此项（或多个所选项）进行扫描的扫描配置将再次用于扫描。	
取消扫描	终止扫描且不生成任何结果。	
停止扫描	停止扫描且生成部分结果。	
构建配置	配置定义项目构建参数，如：预处理器定义或 Include 路径。通常，将从导入的项目显示名为**发布**或**调试**的配置。 当此菜单项不适用时，会将其禁用。	

"工具"菜单

此菜单包含用于比较评估和生成报告的选项以及用于在编辑器中复审文件和结果的选项。某些**工具**菜单项是上下文相关的项，并依赖于活动视图以及该视图中当前选择的项。

表 26. "工具"菜单

菜单项	描述
差异评估	此操作会打开一个对话框，您可以通过此对话框来选择两个要比较的评估。
生成结果报告	生成所选发现或束内容的报告。在发出此操作时，必须选择了一个结果或束视图。如果该视图中未选择结果，那么报告将包含该视图中的所有结果。
生成报告	生成一个报告，它允许您查看基于特定合规性需求或准则的所有结果。
在内部编辑器中打开	在内部 AppScan Source for Analysis 编辑器中打开文件。此操作可用于所选的结果，并且将致使与该结果相关联的文件在此编辑器中打开。
在外部编辑器中打开	使用外部编辑器来打开文件。此操作可用于所选的结果，并且将致使与该结果相关联的文件在此编辑器中打开。

管理菜单

管理菜单提供使您能够管理用户及启动审计信息的操作。

表 27. 管理菜单

菜单项	描述
管理用户	此操作启动一个对话框，您可以通过此对话框来创建和编辑用户及许可权。 您必须拥有 AppScan Source 管理许可权才能管理用户。
审计	此操作启动一个视图，您可以通过此视图来查看审计信息，如认证事件。

请参阅《*IBM Security AppScan Source* 安装和管理指南》以了解关于管理任务的更多详细信息。

"视图"菜单

视图菜单控制每个视图的显示或选择打开的视图。

要获取关于 AppScan Source for Analysis 中可用视图的更多信息，请参阅 AppScan Source for Analysis 视图。

"透视图"菜单

透视图菜单控制 AppScan Source for Analysis 透视图（即，视图和选项的预配置集合）的显示。

表 28. "透视图"菜单

菜单项	描述	键盘快捷键
配置	此透视图允许您创建和管理应用程序、项目和属性。	Alt+1
筛选	此透视图允许您查看扫描结果以对补救工作流程进行优先级排序，并从潜在漏洞中分离出真实漏洞。此透视图可用于隔离需要首先修复的问题。	Alt+2
分析	此透视图允许您向下钻取到单独结果，并复审源代码、补救建议和 AppScan Source 跟踪信息。	Alt+3
重置透视图	选择此项将致使当前显示的透视图返回到其缺省视图和布局。	

帮助菜单

帮助菜单包含用来打开各种工具（有助于产品使用）的操作。这些工具包括产品欢迎、联机用户帮助以及 AppScan Source 安全知识库。

表 29. 帮助菜单

菜单项	描述
欢迎	选择此项可打开 AppScan Source for Analysis"欢迎"视图。此视图提供各种帮助资源（包括 X-Force RSS 订阅源）的快速链接。
帮助内容	选择此项可打开 AppScan Source for Analysis 产品用户帮助。
安全知识库	此操作可打开 AppScan Source 安全知识库。知识库提供了关于每个漏洞的情报：提供关于根本原因、风险严重性和可行补救建议的准确描述。
日志	选择此项可打开"日志"视图。在此视图内，您可以通过选项卡来选择要显示的日志文件。
关于 IBM Security AppScan Source for Analysis	选择此项可打开一个对话框，其中提供关于 AppScan Source for Analysis 的产品信息。

工具栏

AppScan Source for Analysis 工作台中的工具栏提供命令的图形快捷方式。要确认特定工具栏图标，请将鼠标在该图标上悬停片刻，直到悬浮式帮助出现。工具栏按钮表示常用操作（也位于**主**菜单中）。工具栏操作是依赖于上下文的。

主工具栏提供指向 AppScan Source for Analysis 透视图的快速链接。此外，大多数视图都具有工具栏，这些工具栏提供了启动与视图相关的常用操作的快捷方法。

悬浮式帮助

悬浮式帮助是一种形式的上下文相关帮助，它在鼠标指针位于界面元素上时会显示在一个小弹出窗口中。此界面元素的简述会显示在该弹出窗口中。

除了提供按钮和图标的悬浮式帮助，AppScan Source for Analysis 还在各不同位置提供悬浮式帮助，例如：

- 在"资源管理器"视图中，悬浮式帮助可用于指示应用程序、项目和文件的文件名和路径。悬浮式帮助还指示应用程序或项目是否已注册。
- 在"跟踪"视图中，将鼠标悬停在图形中的跟踪节点上会提供关于该节点的信息。
- 在"过滤器编辑器"视图**跟踪**部分中，将鼠标悬停在跟踪条目上会提供关于此条目的详细信息。
- 在"扫描配置"视图**高级设置**部分中，每个设置均有悬浮式帮助可用。
- 将鼠标悬停在"评估摘要"视图中的条形图上会提供以条形表示的精确结果数。
- 在工作台状态栏（位于工作台底沿）中，将鼠标悬停在用户图标上可启动悬浮式帮助，此帮助用于标识已登录的用户。将鼠标悬停在服务器图标上可启动悬浮式帮助，此帮助用于指示 AppScan Source for Analysis 连接到的 Enterprise Server。

状态栏

位于工作台底沿的状态栏会显示参考消息，用于标识当前操作（如扫描）。

例如，在扫描期间，此状态栏可能显示正在扫描 <项目名称>，并带有进度指示。此外，还会显示扫描的当前阶段，例如：正在准备进行漏洞分析：99%。在扫描完成后，将在此状态栏中显示耗用时间。

此状态栏还包含关于当前用户和服务器连接的信息。将鼠标悬停在用户图标上可启动悬浮式帮助，此帮助用于标识已登录的用户。将鼠标悬停在服务器图标上可启动悬浮式帮助，此帮助用于指示 AppScan Source for Analysis 连接到的 Enterprise Server。

第 14 章 视图

AppScan Source for Analysis 工作环境由多个透视图和视图组成，而这些图包含了不同的评估或扫描数据。

AppScan Source for Analysis 视图提供对结果的备选表示法（其中一些支持代码编辑），并使您能够在工作台中浏览信息。例如，"资源管理器"视图可显示应用程序、项目和其他资源。视图可能单独出现，或者在选项卡式笔记本中和其他视图一起堆栈化。您可通过打开和关闭视图并通过将其停靠在工作台窗口中的不同位置来更改透视图的布局。

以下部分中更详细地描述了视图：

- 『配置视图』
- 第 255 页的『协助扫描输出的视图』
- 第 258 页的『协助分类的视图』
- 第 267 页的『用于调查单个结果的视图』
- 第 271 页的『用于处理评估的视图』
- 第 273 页的『"束"视图』

配置视图

此部分中的视图用于配置 AppScan Source。

- 『"定制规则"视图』
- 第 71 页的『"资源管理器"视图』
- 第 242 页的『"模式规则库"视图』
- 第 242 页的『"属性"视图』
- 第 99 页的『"扫描配置"视图』
- 第 193 页的『报告编辑器』

"定制规则"视图

在"定制规则"视图中，可使用"定制规则向导"来创建定制规则。添加、查看或删除现有规则。

如需了解更多详细信息，请参阅第 199 页的『创建定制规则』。

"资源管理器"视图

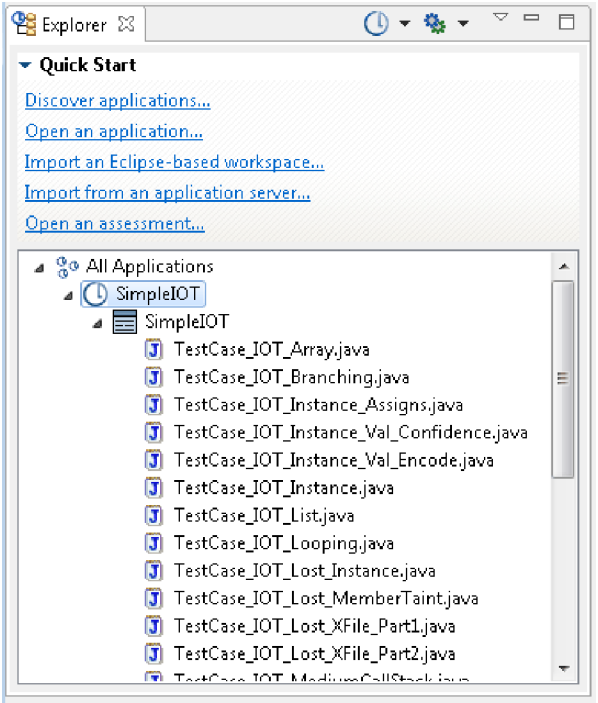
"资源管理器"视图在顶部包含**快速启动**部分，在底部包含资源管理器部分，该部分包含一个节点：**所有应用程序**。**快速启动**部分包含若干个启动常用操作的有用链接。资源管理器部分包含一个树形窗格，该窗格提供了资源（应用程序、项目、目录和项目文件）的分层视图，并以**所有应用程序**作为其根。浏览这些资源的方式与在文件浏览器中类似。在视图中浏览时，树的选择状态确定了"属性"视图中可用的选项卡。

- 第 72 页的『常规信息』

© Copyright IBM Corp. 2003, 2017

- 第 72 页的『"快速启动"部分』
- 第 73 页的『工具栏按钮』
- 第 73 页的『右键单击菜单选项』
- 第 75 页的『应用程序和项目指示符』

常规信息



在"资源管理器"视图中，可使用工具栏按钮、**快速启动**部分中的链接或者资源管理器部分中的右键单击菜单命令来添加应用程序和项目并扫描代码。一旦添加了应用程序，资源管理器部分便会提供应用程序和项目的可视指示符以及每个所添加项的状态。

提示：在"资源管理器"视图中，悬浮式帮助可用于指示应用程序、项目和文件的文件名和路径。悬浮式帮助还指示应用程序或项目是否已注册。

"快速启动"部分

快速启动部分提供以下用于启动常用任务的链接：

- **发现应用程序**：这会启动 Application Discovery Assistant，它使您能够为 Java 和 Microsoft Visual Studio 源代码快速创建并配置应用程序和项目。
- **打开应用程序**：这会启动"打开"对话框，您可以通过此对话框来浏览到现有应用程序并将其添加到应用程序集。可以添加的文件或目录类型包括 `.paf`、`.sln`、`.dsw` 和 `.ewf`。
- **导入基于 Eclipse 的工作空间**：这会启动"添加工作空间"对话框，您可以通过此对话框来添加包含了 Java 项目的现有 Eclipse 或 IBM Rational Application Developer for WebSphere Software (RAD) 工作空间。导入了此工作空间后，您将能够扫描其包含的任何 Java 项目。

注：导入工作空间之前，请确定您已按照第 39 页的『配置 Eclipse 和 Rational Application Developer for WebSphere Software (RAD) 项目的开发环境』中所述安装并更新了开发环境。

- **从应用程序服务器导入：**从 Apache Tomcat 或 WebSphere Application Server Liberty 应用程序服务器导入现有 Java 应用程序。
- **打开评估：**这会启动"打开"对话框，您可以通过此对话框来浏览到 AppScan Source 评估文件。可打开的文件的类型包括 `.ozasmt` 和 `.xml`。

工具栏按钮

表 *30.* 工具栏按钮

操作	图标	描述
添加应用程序菜单		通过单击**添加应用程序菜单**按钮上的向下箭头，可以选择用于创建新应用程序，打开现有应用程序，导入工作空间或启动 Application Discovery Assistant 的操作。
扫描所选项		通过**扫描所选项**按钮，可以扫描在资源管理器部分中选择的对象。缺省扫描配置将用于扫描。要选择其他扫描配置来用于扫描，请单击**扫描所选项**按钮上的向下箭头。选择要使用的扫描配置，或选择**编辑配置**操作以将其他扫描配置设为缺省值（在"扫描配置"视图中，选择要设为缺省值的配置，然后单击**选为缺省值**）。
视图菜单		**视图菜单**按钮可打开用于刷新资源管理器部分和隐藏已注册项的菜单。

右键单击菜单选项

右键菜单选项的可用性由资源管理器部分中所选的项决定。

- 如果在资源管理器部分中选择了**所有应用程序**，那么以下右键单击菜单选项可用：
  - **扫描所有应用程序：**扫描所有应用程序。扫描将使用缺省扫描配置来运行。
  - **扫描所有应用程序时使用：**选择要使用的扫描配置，或选择**编辑配置**操作以将其他扫描配置设为缺省值（在"扫描配置"视图中，选择要设为缺省值的配置，然后单击**选为缺省值**）。
  - **添加应用程序**
    - **创建新应用程序：**将新应用程序添加到应用程序集。此操作会启动"新建应用程序"向导。
    - **打开现有应用程序：**这会启动"打开"对话框，您可以通过此对话框来浏览到现有应用程序并将其添加到应用程序集。可以添加的文件或目录类型包括 `.paf`、`.sln`、`.dsw` 和 `.ewf`。

- **导入现有基于 Eclipse 的工作空间**：这会启动"添加工作空间"对话框，您可以通过此对话框来添加包含了 Java 项目的现有 Eclipse 或 IBM Rational Application Developer for WebSphere Software (RAD) 工作空间。导入了此工作空间后，您将能够扫描其包含的任何 Java 项目。

  注：导入工作空间之前，请确定您已按照第 39 页的『配置 Eclipse 和 Rational Application Developer for WebSphere Software (RAD) 项目的开发环境』中所述安装并更新了开发环境。
- **发现应用程序**：这会启动 Application Discovery Assistant，它使您能够为 Java 和 Microsoft Visual Studio 源代码快速创建并配置应用程序和项目。

– **全部展开**

– **全部折叠**

– **属性**：选择此选项会打开所选项的"属性"视图。

• 如果在资源管理器部分中选择了一个应用程序，那么以下右键单击菜单选项可用：

– **扫描应用程序**：扫描所选应用程序、项目或文件。扫描将使用缺省扫描配置来运行。

– **扫描应用程序时使用**：选择要使用的扫描配置，或选择**编辑配置**操作以将其他扫描配置设为缺省值（在"扫描配置"视图中，选择要设为缺省值的配置，然后单击**选为缺省值**）。

– **添加项目**

- **新项目**：如果在"资源管理器"视图中选择了某个应用程序，那么此操作可用，而选择此操作将使您能够向此应用程序添加新项目。此操作会启动"新建项目"向导。
- **现有项目**：如果在"资源管理器"视图中选择了某个应用程序，那么此操作可用，而选择此操作将使您能够向此应用程序添加现有项目。此操作会启动一个对话框，您可以通过此对话框来浏览到要打开的 .ppf、.vcproj、.vcxproj、.csproj、.vbproj、.dsp 或 .epf 文件。
- **多个项目**：将多个项目添加到在"资源管理器"视图中选择的应用程序。此操作会启动一个对话框，您可以通过此对话框来完成以下任务之一：
  - 指定要在其中搜索项目的目录。
  - 指定要在其中搜索项目的工作空间。
  - 指定要在其中搜索项目的 Microsoft 解决方案文件。

  在搜索结果中，您可以选择一个或多个要添加的项目。

– **移除应用程序**：如果在"资源管理器"视图中选择了某个应用程序，那么此操作可用，而选择此操作会移除所选应用程序。

– **添加定制结果**：此操作会启动"创建定制结果"对话框，使您能够为所选应用程序创建定制结果。

– **刷新**：刷新所选应用程序、项目或视图的内容。

– 注册/注销：

- **注册应用程序**：向 AppScan Source 注册所选的应用程序或项目。您必须先注册应用程序和项目，然后才能将其发布到 AppScan Source 数据库。
- **将应用程序注册为...**：选择此选项可使用新名称来注册应用程序。
- **注销应用程序**：注销所选的应用程序或项目。

    - **定位**：选择此选项可将本地应用程序或项目与已由其他 AppScan Source 用户注册的应用程序或项目相关联。
  - **全部展开**
  - **全部折叠**
  - **属性**：选择此选项会打开所选项的"属性"视图。
- 如果在资源管理器部分中选择了一个项目，那么以下右键单击菜单选项可用：
  - **扫描项目**：扫描所选应用程序、项目或文件。扫描将使用缺省扫描配置来运行。
  - **扫描项目时使用**：选择要使用的扫描配置，或选择**编辑配置**操作以将其他扫描配置设为缺省值（在"扫描配置"视图中，选择要设为缺省值的配置，然后单击**选为缺省值**）。
  - **复制项目**：如果在"资源管理器"视图中选择了某个项目，那么此操作可用，而选择此操作将打开一个对话框，您可以通过此对话框将此项目复制到另一个应用程序，或在当前包含此项目的应用程序中创建此项目的副本。
  - **移除项目**：移除所选对象。
  - 注册/注销：
    - **注册项目**：向 AppScan Source 注册所选的应用程序或项目。您必须先注册应用程序和项目，然后才能将其发布到 AppScan Source 数据库。
    - **注销项目**：注销所选的应用程序或项目。
    - **定位**：选择此选项可将本地应用程序或项目与已由其他 AppScan Source 用户注册的应用程序或项目相关联。
  - **全部展开**
  - **全部折叠**
  - **属性**：选择此选项会打开所选项的"属性"视图。
- 如果在资源管理器部分中选择了一个文件，那么以下右键单击菜单选项可用：
  - **扫描文件**：扫描所选应用程序、项目或文件。扫描将使用缺省扫描配置来运行。
  - **扫描文件时使用**：选择要使用的扫描配置，或选择**编辑配置**操作以将其他扫描配置设为缺省值（在"扫描配置"视图中，选择要设为缺省值的配置，然后单击**选为缺省值**）。
  - **从扫描中排除**：从扫描中移除所选文件。
  - **在内部编辑器中打开**：在 AppScan Source 编辑器（在"分析"透视图中）中打开所选文件。
  - **在外部编辑器中打开**：选择要在其中打开所选文件的外部编辑器。
  - **属性**：选择此选项会打开所选项的"属性"视图。

应用程序和项目指示符

下表标识了"资源管理器"视图中的应用程序和项目图标。

表 *31.* 应用程序和项目图标

应用程序或项目类型	未注册	已注册	缺失/找不到
已导入的应用程序			

表 31. 应用程序和项目图标 (续)

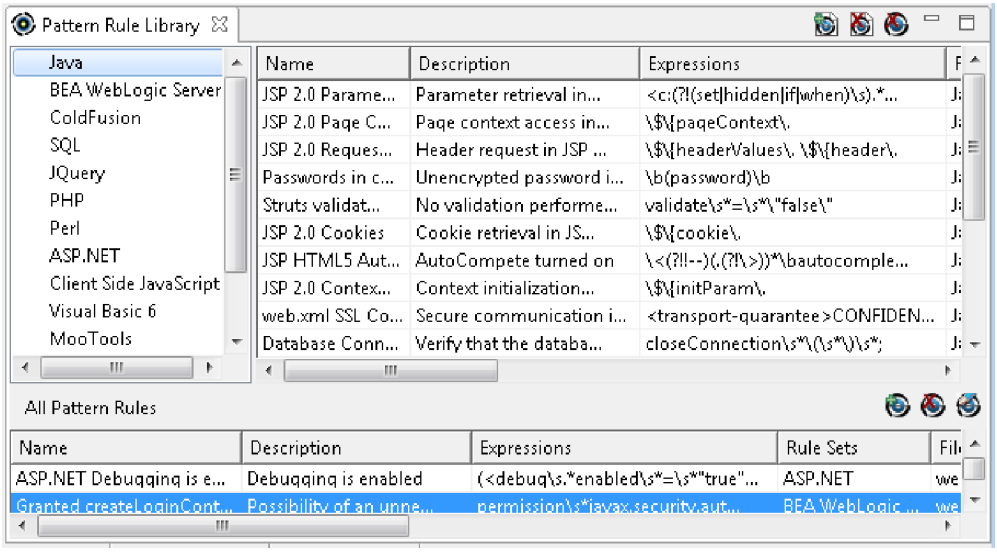
应用程序或项目类型	未注册	已注册	缺失/找不到
手动创建或使用 Application Discovery Assistant 创建的应用程序			
已导入的项目			
手动创建或使用 Application Discovery Assistant 创建的项目			

"资源管理器"视图显示本地应用程序和项目，以及已在服务器上注册的应用程序和项目（已在服务器上注册但未在本地保存的应用程序和项目，例如，由其他用户注册的应用程序和项目，以灰色显示）。如果单击工具栏**视图菜单**按钮并将**隐藏服务器上已注册项**菜单项切换为未选择状态，那么可以查看现有服务器应用程序和项目。如果项目以灰色显示，那么可以右键单击并选择菜单中的**查找**。

"模式规则库"视图

基于模式的扫描是根据定制的搜索条件来对源代码进行的分析。"模式规则库"视图允许您按照语言来查看现有基于模式的规则（包括现成可用的 AppScan Source 模式规则库）。此外，此视图还允许您为基于模式的扫描添加规则和模式。

构建规则库后，可将模式分析应用于特定应用程序或项目。请参阅第 205 页的『以基于模式的规则进行定制』以了解有关模式搜索的详细信息。



"属性"视图

"属性"视图的内容取决于在"资源管理器"视图中选择的项。属性可应用于所有应用程序、个别应用程序、项目或文件。可视的属性取决于语言或所选的项目类型。

- 第 243 页的『属性视图：所有应用程序』

- 第 213 页的『属性视图：选定应用程序』
- 第 214 页的『属性视图：选定项目』
- 第 250 页的『文件属性』

属性视图：所有应用程序

在"资源管理器"视图中选择**所有应用程序**时，"属性"视图将显示"概述"和"过滤器"选项卡。

概述

"概述"选项卡显示全局属性。属性是具有相似特征的用户定义项的已命名分组。可添加或删除属性及其值。

过滤器

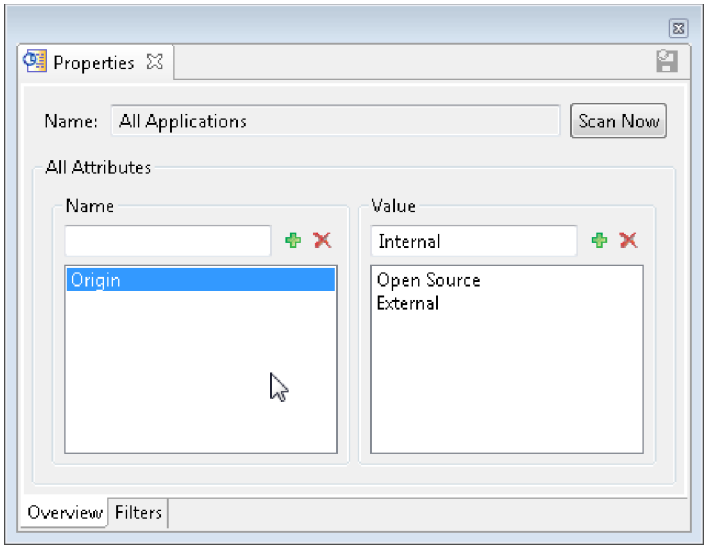
该选项卡使您能够指定所有应用程序的现有过滤器，以及您想要如何应用过滤器（可直接应用过滤器，也可应用其反向过滤器）。请参阅第 119 页的第 5 章，『筛选和分析』以获取关于过滤器的信息，以及第 138 页的『全局应用过滤器』以获取关于全局地应用过滤器的详细信息。

已过滤的结果将不再出现于扫描结果中，也不再作为应用程序或项目度量中的因素。

添加和除去全局属性：

必须定义**所有应用程序**的属性，然后才能对应用程序的属性进行分组。

关于此任务



要删除全局属性或其值，请选择属性名称或属性值，然后单击**除去属性**。该名称或值将不再显示在列表中。

注：删除属性不会影响历史结果。

要添加全局属性和其值，请遵循下面的步骤。

过程

1. 选择**所有应用程序**。
2. 在"属性"视图中的"概述"选项卡上，为属性输入名称。
3. 单击**添加属性**。属性名称将显示在"名称"列表中。
4. 选择已命名的属性。
5. 为属性输入**值**。
6. 单击**添加值**。属性值将显示在"值"列表中。

属性视图：选定应用程序

在此视图中，可配置选定应用程序的属性。应用程序属性取决于先前创建的全局属性。

- 第 213 页的『 概述』
- 第 213 页的『排除和过滤器』
- 第 214 页的『规则和规则集』
- 第 214 页的『已修改的结果』
- 第 214 页的『定制结果』

概述

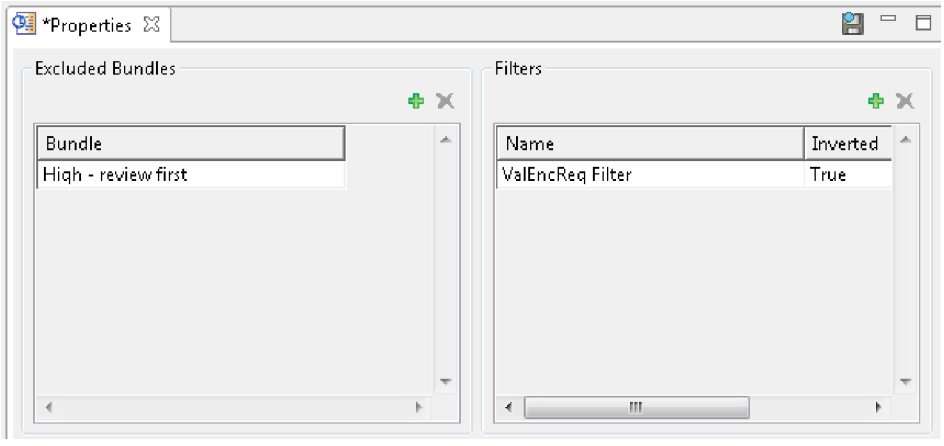
"概述"选项卡中显示：

- 应用程序名称。可以通过在该字段中输入新名称来重命名应用程序。
- 应用程序属性

排除和过滤器

该选项卡使您能够指定选定应用程序的现有过滤器，以及您想要如何应用过滤器（可直接应用过滤器，也可应用其反向过滤器）。在该选项卡中，还可以管理从扫描排除了结果的束。请参阅第 119 页的第 5 章, 『筛选和分析』以获取关于过滤器的信息，以及第 138 页的『全局应用过滤器』以获取关于全局地应用过滤器的详细信息。

已排除和已过滤的结果将不再出现于扫描结果中，也不再作为应用程序或项目度量中的因素。



规则和规则集

在"资源管理器"视图中选择应用程序时，"属性"视图中的"模式规则和规则集"选项卡允许您添加扫描应用程序时将应用的模式规则和规则集。使用基于模式的扫描来搜索希望显示为结果的文本模式。各个规则和规则集可应用于应用程序和项目。请参阅第 205 页的『以基于模式的规则进行定制』以了解有关基于模式的分析的信息，并参阅第 210 页的『应用模式规则和规则集』以了解有关如何在"属性"视图中应用规则和规则集的信息。

已修改的结果

在"已修改的结果"选项卡上，可查看、编辑或删除任何先前修改的结果，或者修改现有结果。已修改的结果是漏洞类型、严重性、分类或说明发生过更改的结果。

定制结果

在"定制结果"选项卡上，可查看、添加、编辑或删除定制结果。请参阅第 151 页的『定制结果』以了解更多详细信息。

创建应用程序属性：

过程

1. 在"概述"选项卡上，单击**添加属性**。
2. 在**全局属性**对话框中，选择将应用于应用程序的属性的名称。
3. 单击**值**列，并从列表中选择属性值。

属性视图：选定项目

在"属性"视图的此方式下，可配置选定项目的参数。项目属性取决于先前创建的全局属性。属性因选定项目而有所不同。

- 第 215 页的『选定项目"概述"选项卡』
- 第 216 页的『过滤器』
- 第 216 页的『模式规则和规则集』
- 第 216 页的『文件扩展名』
- 第 217 页的『源』
- 第 217 页的『JavaServer Page (JSP) 项目依赖性』
- 第 218 页的『项目依赖性』
- 第 218 页的『编译』
- 第 218 页的『优化』
- 第 218 页的『预编译选项卡（仅 ASP.NET）』

选定项目"概述"选项卡

"概述"选项卡中显示：

- 项目**名称**。可以通过在该字段中输入新名称来重命名项目。
- 项目**文件**名称和路径
- **项目类型**

- 配置：此部分显示目标配置。对于 .NET 和 C++ 项目，此部分显示已在"项目依赖性"选项卡中保存的目标配置。对于所有其他项目类型，此部分显示**缺省值**。
- 过滤器选项：选择**外部源中包含的过滤器结果**，以过滤出扫描项目源文件以外的文件中所发现的任何结果。如果项目以编译器生成的文件或临时文件（如 ASP.NET）来报告结果，那么该选项可降低其噪声。
- 漏洞分析高速缓存选项：如果通过迭代扫描并添加定制规则，然后在不更改源代码的情况下重新扫描，从而优化代码库的评估，那么您可通过将项目属性设置为使用漏洞分析高速缓存来大幅缩短扫描时间。要执行此操作，请在项目属性中选中**启用漏洞分析高速缓存**复选框。选中此复选框后第一次扫描项目时，将创建漏洞分析高速缓存。每次对项目进行后续扫描时，都将使用漏洞分析高速缓存，从而可缩短扫描时间。

  要清除漏洞分析高速缓存，以及启用 Java 递增分析时创建的高速缓存，单击**清除高速缓存**。下次扫描项目时，将发生完整扫描，并将创建新的漏洞分析高速缓存。在下列情况下，您可能希望清除高速缓存：
  - 上次扫描后，项目中的源代码已更改。
  - 已更改了项目配置，如添加或删除源文件。
  - 已更改代码配置选项。例如，如果要扫描 Java，且类路径已经更改，那么您可能希望清除高速缓存；或者如果要扫描 C 或 C++，且已更改了 include 路径或预处理器定义，也可能希望清除高速缓存。
  - 您已启用了 Java 递增分析并想要运行完整扫描，或者您将要遇到可能通过清除高速缓存来进行补救的问题。请参阅第 101 页的『Java 的递增分析』以了解更多信息。

  注：还可通过在"定制规则向导"中创建定制规则时选中**清除高速缓存**复选框来清除漏洞分析高速缓存。
- **字符串分析**：字符串分析监控 Java 或 Microsoft .NET 项目中的字符串操控。它能够自动检测清理器和验证器例程。通过此检测，可减少错误的肯定和否定。选择**启用字符串分析以查找验证器/清理器函数**复选框以启用字符串分析。**将导入的规则应用于全局作用域**复选框确定是将发现的清理器和验证器例程应用于单个项目，还是在全局级别上应用（应用于所有项目）。

  注：字符串分析的应用会降低扫描速度。因此，建议您仅在代码更改后应用它，然后为后续扫描将其禁用。此外，应该将发现的例程作为建议查看并由审计员复审。可以在"定制规则"视图中查看这些例程。
- **文件编码**：必须对项目中文件的字符编码进行相应设置，以便 AppScan Source 能够正确读取这些文件（并且例如，在源视图中正确显示这些文件）。

  注：AppScan Source 项目的缺省文件编码为 **ISO-8859-1**。此缺省文件编码可在"常规"首选项页面中进行更改。

过滤器

该选项卡使您能够指定选定项目的现有过滤器，以及您想要如何应用过滤器（可直接应用过滤器，也可应用其反向过滤器）。请参阅第 119 页的第 5 章, 『筛选和分析』以获取关于过滤器的信息，以及第 138 页的『全局应用过滤器』以获取关于全局地应用过滤器的详细信息。

模式规则和规则集

在"资源管理器"视图中选择项目时，"属性"视图中的"模式规则和规则集"选项卡允许您添加扫描项目时将应用的模式规则和规则集。使用基于模式的扫描来搜索希望显示为结果的文本模式。各个规则和规则集可应用于应用程序和项目。参阅第 205 页的『以基于模式的规则进行定制』以了解有关基于模式的分析的信息，并参阅第 210 页的『应用模式规则和规则集』以了解有关如何在"属性"视图中应用规则和规则集的信息。

文件扩展名

使用该选项卡可为项目配置或添加有效的文件扩展名，从扫描排除文件，并将扩展名指定为 web 文件。

文件扩展名部分列出了已在当前项目类型的第 88 页的『项目文件扩展名』首选项页面中全局设置的扩展名（可使用**文件扩展名集**菜单为其他项目类型选择文件扩展名）。要从当前项目的扫描排除扩展名，在列表中选择扩展名，并单击**排除扩展名**。这会导致扩展名在选项卡的**已排除的扩展名**部分中列出。

要为项目添加其他扩展名，在**其他扩展名**部分中选择**添加扩展名**，然后输入文件扩展名，并指示是应该扫描带有该扩展名的文件，将其视为 web 文件还是将其排除。

表 *32.* 文件扩展名设置

设置	描述	用法示例
扫描或**评估**	包含带有在完整分析中指示的扩展名的文件。	• 如果已为 Java 项目创建 .xxx 扩展名并将此扩展名标记为**扫描**或**评估**，那么将编译并扫描具有该扩展名的文件。 • 如果不应编译和扫描某个文件（例如 C++ 中的头文件），那么该文件是项目的一部分但不被标记为**扫描**或**评估**。这些文件应包含在项目中，而且应在基于模式的分析过程中进行搜索。.
Web 文件	用针对 JSP 编译的指定扩展名标记文件。该设置使 AppScan Source 能够将 web 源与非 web 源分开。	如果已为 Java 项目创建 .yyy 扩展名并将此扩展名标记为**Web 文件**，那么具有该扩展名的文件将被安排为项目中的 Web 源。当 AppScan Source 为分析做准备时，这些文件将被预编译为类以进行分析。
排除	请勿在项目中为带有指定扩展名的文件创建源文件。将不会扫描带有该扩展名的文件。	为项目需要进行编译的文件创建 .zzz 扩展名，但无需包含在分析中。

源

指定扫描中将包含的源。

- 工作目录：AppScan Source 项目文件 (ppf) 的位置和所有相对路径的基础。

- **添加源根目录**和**除去源根目录**："源"选项卡显示为来自"项目配置向导"的项目或在已导入 ppf 中定义的项目建立的属性。

  仅当选择**源根目录**图标时，**除去源根目录**才可用。它用于除去源代码根目录。
- 查找源代码根目录（仅 Java 项目）：允许 AppScan Source for Analysis 自动查找所有有效的源代码根目录。
- 项目文件在**源根目录**图标下列出。从扫描排除的文件具有红色文件图标（如果右键单击了排除的文件，那么其菜单中的**排除**被禁用，**包含**被启用。）要排除包含的文件，右键单击该文件并选择菜单中的**排除**。要包含排除的文件，右键单击该文件并选择菜单中的**包含**。

JavaServer Page (JSP) 项目依赖性

"JSP 项目依赖性"选项卡显示针对特定 JSP 项目建立的属性。

- 包含 Web (JSP) 内容：确定项目是否为包含 JavaServer Page 的 Web 应用程序。
- Web 上下文根：包含 WEB-INF 目录的 WAR 文件或目录。 Web 上下文根必须是有效 Web 应用程序的根目录。
- JSP 编译器：现成可用的 Tomcat 7 是缺省 JSP 编译器设置（缺省 JSP 编译器可以在 Java 和 JSP 首选项页面中进行更改）。要了解 AppScan Source 支持的编译器的相关信息，请参阅http://www.ibm.com/support/docview.wss?uid=swg27027486。

  Apache Tomcat V7 和 V8 包含在 AppScan Source 的安装中。如果未配置 **Tomcat 7** 和 **Tomcat 8** 首选项页面，那么 AppScan Source 将使用当前提供且标记为缺省选项的 Tomcat JSP 编译器来编译 JSP 文件。如果您想要运用外部受支持 Tomcat 编译器，请使用 Tomcat 首选项页面来指向本地 Tomcat 安装版。

  如果使用的是 Oracle WebLogic Server 或 WebSphere Application Server，那么必须将适用的首选项页面配置为指向应用程序服务器的本地安装版，以便其可在分析期间用于 JSP 编译。如果尚未完成该配置，那么选择 JSP 编译器时将显示一条消息以提示您完成配置。如果单击消息中的**是**，那么您将被转至相应的首选项页面。如果单击**否**，那么 JSP 编译器选择旁边将显示一条警告链接（访问该链接将打开首选项页面）。

项目依赖性

"项目依赖性"选项卡显示项目属性。此选项卡上的配置设置会根据语言而不同，例如：

- 使用**选项**可以选择任何其他必需的编译器参数。
- JDK 设置特定于 Java。
- 预处理器定义特定于 C/C++ 代码。指定预处理器定义时，不要包含编译器的 -D 选项（例如，指定 a=definition1 而不是 -Da=definition1）。指定多个定义时，请使用分号分隔的列表。
- 目标配置仅可用于 .NET 和 C++ 项目。

编译

- 选项：项目配置所需的其他编译器参数。
- 使用 JDK：确定用于项目编译的 JDK，如首选项中所配置。请参阅第 77 页的第 3 章，『首选项』。

Java 项目可能引用本地 Java Development Kit (JDK) 位置。当项目移动到服务器时，JDK 路径可能会不再有效。要将本地项目传输到服务器，必须确定各项目中指定已命名 JDK 的缺省 JDK 路径。

注：JSP 项目的缺省编译器是 Tomcat 7，后者需要 Java V1.6 或更高版本。如果 **Tomcat 7** 保留为缺省值，那么使用更低版本的 JDK 将导致扫描期间出现编译错误。

- 验证：**验证**可确保正确配置项目依赖性。它检查 Java 项目中源和类路径之间 的配置冲突，并检查编译错误。如果类路径中的类在源根目录中重复出现，那么**存在冲突**。（如果存在冲突，请修改类路径以除去有冲突的类。）

  检查完冲突后，**验证**将确定项目是否编译和报告了任何编译错误。

优化

- **预编译类**：使用预编译 Java 或 JSP 类文件，而不是在扫描期间编译。选择后，此选项将禁用源登台选项。
- 将源文件登台以将编译错误的影响最小化：控制 AppScan Source 是否将源复制到登台目录。

  更正与目录不匹配的软件包需要 Java 编译以打开各源文件。

  清理扫描之间的登台区域将提高扫描之间的性能。

预编译选项卡（仅 ASP.NET）

预编译通过向 Web 站点中的特定页面（缺省情况下是 precompile.axd）发出 HTTP 请求来实现。此页面通过 web.config 中指定的特定 HTTP 处理程序进行处理。此处理程序可将整个站点（包括 client.aspx）编译到 .NET Framework 目录中的临时 ASP.NET 文件目录（然后在这里全部进行扫描）。

要扫描 ASP.NET 1.1，必须对 Web 站点进行相应配置，使之编译和构建了调试消息。从而，Web 站点编译和构建调试信息这一事实其本身就是安全漏洞。由于扫描需要，您可以安全地忽略此漏洞。然而，请确保您部署的应用程序在 web.config 中没有编译 debug=true。

要对 ASP.NET 1.1 Web 站点进行预编译，请将以下元素作为 web.config 元素的子代添加到 <system.web> 文件中：

```
  <httpHandlers><add verb="*" path="precompile.axd"
type="System.Web.Handlers.BatchHandler"/></httpHandlers>
```

还应在编译元素中设置 debug=true。例如：

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <system.web>
  <httpHandlers><add verb="*" path="precompile.axd"
    type="System.Web.Handlers.BatchHandler"/>
    </httpHandlers>
      <compilation
        defaultLanguage="c#"
        debug="true"
   />
...
```

此元素指定 Web 站点的页面 precompile.axd 将通过特定 .Net System.Web.Handlers.BatchHandler 类进行处理。此类将 Web 站点的内容预编译到临时 ASP.NET 文件目录。

- Web 站点：预编译站点的请求目标。缺省位置是 precompile.axd。Precompile.axd 是虚拟文件，映射到 web.config 文件中指定的文件。
- 输出目录：作为预编译目标的目录。AppScan Source 在此目录中查找预编译输出。
- 预编译 ASP.NET Web 站点：AppScan Source 在扫描期间自动预编译并扫描已预编译的输出。
- 如果预编译失败，停止扫描：选择**>预编译 ASP.NET Web 站点**和**如果预编译失败，停止扫描**后，预编译失败时扫描将停止。否则，扫描将仅针对 Web 站点的主要输出继续。
- 立刻编译：扫描之前运行此测试，以查看基于当前设置的预编译是否成功。编译输出将在"预编译输出"窗格中显示。
- 其他组合件：对于任何 .NET 项目类型，请指定要扫描的其他组合件。
- 项目引用：列出了在其中搜索 .NET 组合件项目和现有 .NET 项目中所引用组合件的目录。

文件属性

文件属性与项目依赖性类似，一般都针对 C/C++ 应用程序进行配置。

包含项目中的配置数据：包含文件配置中的项目配置数据。如此，文件配置即包含累积的项目配置和文件配置。文件配置将取代项目配置。

"扫描配置"视图

通过"扫描配置"视图，您可以创建能够在启动扫描时使用的配置。还可以使用视图来设置缺省扫描配置。在扫描配置中，可以指定要在扫描期间使用的源规则，并且可以包含许多扫描设置。在扫描配置中进行的设置通常可以产生更佳的扫描结果，而能够保存这些设置，就可以使扫描更为轻松和省时。

"扫描配置"视图有以下主要部分：

- 第 99 页的『扫描配置管理』
- 第 99 页的『"一般"选项卡』
- 第 100 页的『"污染流分析"选项卡』
- 第 101 页的『"模式分析"选项卡』

扫描配置管理

使用此部分可选择、添加、除去、保存和共享扫描配置，以及将扫描配置设置为缺省配置。

- 要创建新扫描配置，请单击**新建**。完成扫描配置设置后，单击**保存**以保存更改。要将该扫描配置设置为缺省配置，请在将其保存后单击**选为缺省**。要了解如何使用缺省扫描配置，请参阅第 91 页的『扫描源代码』。
- 要处理现有扫描配置，请从列表中选择该配置：
  - 如果修改扫描配置设置，请单击**保存**以保存更改（通过切换到其他扫描配置，然后单击**放弃**，可以放弃不需要的更改）。
  - 要除去所选扫描配置，请单击**删除**。

- 要复制此扫描配置，请单击**复制**。这样，将基于原始扫描配置的设置来创建新扫描配置。
- 要将此扫描配置设置为缺省配置，请单击**选为缺省**。要了解如何使用缺省扫描配置，请参阅第 91 页的『扫描源代码』。
- 要将此扫描配置与他人共享，请单击**共享**。这会将此扫描配置保存到 AppScan Source 数据库。

  注：要共享扫描配置，或者修改或删除已共享的扫描配置，您必须拥有**管理共享配置**许可权。要了解关于设置许可权的信息，请参阅《*IBM Security AppScan Source* 安装和管理指南》。

注：AppScan Source 提供内置扫描配置。不能修改或除去这些配置。在列表中选择这些配置后，您就能够复制它们或查看其设置。

"一般"选项卡

基本信息

通过此部分，您可以对扫描配置命名并为其提供描述。

过滤器

在该部分中，可选择每当使用配置时就会应用于扫描的一个或多个过滤器。选择过滤器时，可选择 AppScan Source预定义过滤器或共享过滤器或您已创建的过滤器。请参阅第 94 页的『管理扫描配置』以了解更多详细信息。

"污染流分析"选项卡

污染流分析

启用和设置污染流分析的范围。

扫描规则

使用此部分可确定哪些源规则将对扫描生效。

源是对程序的输入，如文件、servlet 请求、控制台输入或套接字。通过排除某些源规则，可加速扫描并避免检测您并不感兴趣的输入产生的漏洞。

规则通过规则属性进行了标记，以指示它们与特定漏洞、机制、属性或技术相关。这些属性分组为规则集，而规则集对应于一组常用的相关规则。可通过指定规则集或各个规则属性来限制扫描中包含的源规则。

- 选择要包含在扫描中的一个或多个漏洞类型（在规则集中按类型进行组织）：
  - **所有内容**：如果选择该项，将检测从所有受支持输入源产生的漏洞。
  - **用户输入**：如果选择该项，将检测最终用户的输入产生的漏洞。
  - **Web 应用程序**：如果选择该项，将检测 Web 应用程序风险产生的漏洞。
  - **错误处理和记录**：如果选择该项，那么将检测错误处理和日志记录机制产生的漏洞。
  - **环境**：如果选择该项，那么将检测配置文件、系统环境文件和属性文件产生的漏洞。

- **外部系统**：如果选择该项，将检测外部实体产生的漏洞。
- **数据存储**：如果选择该项，那么将检测数据存储（例如数据库和高速缓存）产生的漏洞。
- **异常内容**：如果选择该项，那么将检测通常不属于生产应用程序的例程产生的漏洞。
- **文件系统**：如果选择该项，将检测文件系统产生的漏洞。
- **敏感数据**：如果选择该项，将检测敏感数据产生的漏洞。

悬浮式文本描述此部分中的各规则集。

- 选择要包含在扫描中的各条扫描规则属性：单击**放弃所选规则集并让我选择个别规则属性**。这会打开"选择规则属性"对话框，以允许您选择个别规则属性。如果完成此对话框，将放弃已选择的任何规则集。具有选定规则属性的扫描规则将用于扫描。

高级设置

此部分旨在仅供高级用户使用。它包含可改进扫描结果的各种设置。悬浮式文本描述此部分中的各设置。

"模式分析"选项卡

模式分析

使用扫描配置时使用该部分来启用基于模式的扫描。基于模式的扫描是根据定制的搜索条件来对源代码进行的分析。

模式规则集和模式规则

使用这些部分可添加要在模式分析期间使用的规则和规则集。请参阅第 205 页的『以基于模式的规则进行定制』和第 94 页的『管理扫描配置』，以获取更多信息。

报告编辑器

通过"报告编辑器"，可以编辑定制报告或模板，或者创建新的报告。定制报告包括可用于发现结果报告的任何项，如发现结果信息、代码片段、AppScan Source 跟踪和补救内容以及漏洞矩阵。在开始设计新报告之前，建议您先通过在"报告编辑器"中修改现有报告模板来熟悉报告创建过程。

报告编辑器包含"报告布局"、"类别"和"预览"选项卡。

- **报告布局**：设计报告的外观。在布局中，您可以添加和除去 AppScan Source 报告元素并对其重新排序。
- **类别**：创建和编辑类别。类别是一组结果。类别用于确定要包含在报告中的发现结果、这些发现结果的分组方式以及分组顺序。
- **预览**：在您编辑报告时查看报告中的当前评估。

以下三个选项卡包含常用字段：

- **文件**：已保存的分组文件的路径（只读）。保存文件后，此字段中才会显示内容。保存后，该分组文件是用于定义报告的 XML 文件。
- **名称**：用户定义的报告名称。

用于保存、打开、创建、复制和生成定制报告的工具栏按钮包括：

- **创建新报告**：创建新的定制报告
- **从现有新建报告**：从现有报告模板创建新定制报告
- **打开已保存的报告**：打开要编辑的分组文件
- **保存**：将当前报告保存到指定的文件
- **另存为**：将当前报告保存到新文件
- **生成此报告的实例**：为当前打开的评估创建报告副本

提示：要查看现有报告的样本，请单击**从现有报告新建报告**，然后选择以下某个 AppScan Source 报告模板。通过在模板中探查"报告布局"和"类别"选项卡，您可以了解设计报告的方式。

"报告布局"选项卡

"报告布局"选项卡包含"选用板"和"布局"部分，以及允许您指定在每个页面上显示的页眉或页脚的部分。

页眉和页脚

页眉字段允许您指定出现在每个报告页面顶部的文本，而**页脚**字段允许您指定出现在每个页面底部的文本。

选用板

"选用板"显示用于构成 AppScan Source 标准报告的元素的列表。某些元素仅显示"类别"选项卡中已定义的类别的信息（请参阅第 194 页的表 19）。

表 *33.* 报告布局选用板 - 不依赖于类别的元素

报告元素	描述
文本标题	向报告布局添加粗体文本块。
图像标题	显示缩放到指定大小（以像素为单位）的图像。
AppScan Source 标题	包含 AppScan Source 标记的报告标题。
标题和日期	包含已扫描项的名称的报告标题，以及扫描日期和生成报告的日期。
文本块	任何用户定义的文本。也可以为**标签**字段中的文本块添加标题。
漏洞矩阵	评估漏洞矩阵（显示出现在"漏洞矩阵"视图中的相同图形）。
度量值	确定项目中软件包、类、方法和所有软件包中代码行的总数。
扫描历史记录	当前扫描的度量和同一目标的扫描的历史度量。

表 34. 报告布局选用板 - 依赖于类别的元素

报告元素	描述
报告卡	"类别"选项卡中定义的每个类别的漏洞级别的简短细分。包含指向总结该部分的报告详细信息和严重性指示符的链接。
漏洞细分	包含"类别"选项卡中定义的所有类别中漏洞数量细分情况（按严重性和分类排序）的表。
部分报告卡	用户指定的类别（如"类别"选项卡中所指定）的漏洞级别的细分。
类别	按"类别"选项卡中的定义列出所有已分类的发现结果数据。
类别	列出"类别"选项卡中已定义的一个或多个类别中的所有发现结果。

布局

从选用板添加项时，所添加项将出现在布局中。使用部分工具栏可在布局中除去、修改或移动项。

"类别"选项卡

通过使用"类别"选项卡，可添加类别以包含基于束和属性的发现结果或所选择的选定发现结果。然后，在将某些项添加到布局时可使用这些类别。例如，在将"漏洞细分"添加到布局时，会将包含所有类别的漏洞数量细分情况（按严重性和分类排序）的表添加到布局。"类别"选项卡包含一个带有类别树的窗格和一个可在其中编辑选定类别的属性的窗格。每个类别都包含评估中满足您所定义的某些要求的结果。

可用的类别包括：

- 束：束类别包含束名称列表。束中其名称显示在列表中的任何发现结果都将在此类别中显示。虽然您从当前评估选择束，但是您可以将束类别应用于任何评估，因为束按名称匹配。
- 个别结果：选择要添加到类别的特定结果。只会将结果的快照添加到报告中。如果将发现结果添加到报告之后再对其进行修改，那么报告不会反映该更改。
- "漏洞类型"、"机制"和"技术"属性：从 AppScan Source 安全知识库中的 API 选择属性和必需属性的集合。如果结果包含至少一个**属性**和所有**必需属性**，那么该结果将包含在报告中。

下表标识了类别窗格和构成该窗格的项。

表 35. "类别"选项卡属性

属性	描述	编辑方式
标签	类别的简称，如"缓冲区溢出"。标签标识类别树列表中的类别，它是定制报告中的类别标题。	在单行文本字段中输入标签。

表 35. "类别"选项卡属性 (续)

属性	描述	编辑方式
摘要	语句的模板，用于说明在此类别中报告的发现结果数量。在报告生成期间，实际计数将替换 %FindingCount%。	为类别输入简短描述，然后单击 **添加计数** 以将变量 %FindingCount% 放置在光标位置的短语中。
文本	简短的类别描述。	输入描述类别的文本。
属性（仅限"属性"类别）	将在此类别中报告具有至少其中一个属性的结果。如果结果不具有列出的所有必需属性，那么结果将不会包含在此类别中。	单击工具栏上的**添加**，然后从"添加属性"对话框中选择属性。单击**除去**以从列表中除去所选项。
必需属性（仅限"属性"类别）	具有所有必需属性并且至少具有一个属性的发现结果将显示在此类别下的报告中。	单击工具栏上的**添加**，然后从"添加属性"对话框中选择属性。单击**除去**以从列表中除去所选项。
束（仅限"束"类别）	指定要包含在此类别中的束的名称。	单击"束"部分中的**添加束**，然后从列表中选择束。
发现结果（仅限"发现结果"类别）	指定要包含在此类别中的结果。	选择任何结果表中的发现结果，然后单击表工具栏上的**添加发现结果**以添加选定发现结果。如果多个视图包含选定发现结果，那么将提示您选择包含您要添加的选定发现结果的视图。 也可将发现结果从结果表拖动到"报告编辑器"视图中的表中，或在"报告编辑器"中，或直接拖动到类别树中的现有发现结果类别。

"预览"选项卡

您可以在编辑模板时预览 AppScan Source for Analysis 报告。在"预览"窗格中，单击**预览**以查看针对打开的评估的报告。

协助扫描输出的视图

此部分中的视图用于查看和管理扫描输出。

- 『"控制台"视图』
- 第 256 页的『"度量值"视图』
- 第 256 页的『"我的评估"视图』
- 第 257 页的『"已发布的评估"视图』

"控制台"视图

"控制台"视图显示当前扫描的输出，包括状态信息、输出文本和错误消息。此视图可显示两个控制台，一个针对当前运行的扫描，另一个针对已完成的扫描。

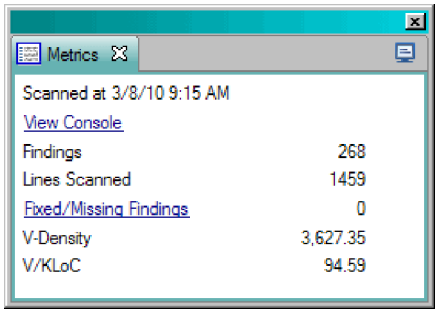
输出控制台显示完整的扫描输出，包括已扫描的文件、扫描的文件总数、发现的漏洞总数、扫描时间和漏洞密度。

可使用工具栏按钮来处理控制台输出。

错误控制台显示输出错误消息以及扫描中的错误数。错误值将在扫描期间进行更新。

"度量值"视图

"度量值"视图逐个评估地提供统计信息，并且包含已扫描的代码行数、结果的总数、V-Density 以及 V/KLoC。



视图控制台

用于打开"控制台"视图以查看当前扫描的输出的超链接。

结果

扫描所识别的结果的数量。

已扫描的行数

已扫描的代码行数。

已修复/缺失结果

包含在应用程序束中但在此扫描中未找到的项的数量。

V-Density

支持以一致方式来评估应用程序漏洞的数字表达式。V-Density 通过将结果的数量和重要程度与所分析的应用程序或项目的大小相关联来予以计算。

V/KLoC

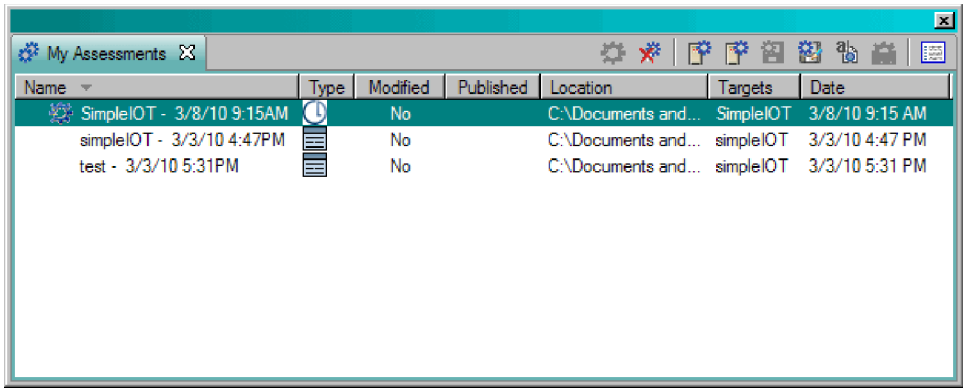
每千行代码中找到的漏洞数。

"我的评估"视图

"我的评估"视图包含评估（当前打开的评估以及您已保存的任何评估）的列表。如果修改了当前的评估工作集（例如，如果您添加新评估或修改评估），那么视图标题旁边的星号表明此工作集中有未保存的更改。

- **名称**：评估名称。

- **类型**：表明在扫描范围内的应用程序（ ）、项目（ ）或文件（ ）的图标。评估名称旁边的星形指示评估当前已打开。
- **扫描配置**：用于扫描的扫描配置。
- **已修改**：**是**或**否**，表明评估的修改状态。
- **已发布**：指示评估已发布到 AppScan Source 数据库。
- **位置**：评估文件的路径 (<file_name>.ozasmt)。
- **目标**：扫描的应用程序、项目或文件。
- **日期**：扫描完成日期。



扫描完成后，将自动出现在"我的评估"视图中。该视图中可视的评估包括从此计算机进行的扫描或您添加的扫描。

在此视图中，可针对评估进行打开、添加、除去、发布、保存、重命名或比较操作。如果在未保存或未发布的情况下，除去此视图中的评估，那么该评估将永久删除。请注意，每个已保存的评估都包含所有结果、输出和错误日志。请参阅第 116 页的『保存评估』以了解有关保存和发布评估的详细信息。

请参阅第 150 页的『在"评估差异"视图中比较两个评估』以了解有关比较评估的详细信息。

提示：常规首选项设置在"已发布的评估"视图中显示的最大评估数。

"已发布的评估"视图

"已发布的评估"视图列出已发布到 AppScan Source 数据库的评估。

- **名称**：评估名称。
- **类型**：表明在扫描范围内的应用程序（ ）、项目（ ）或文件（ ）的图标。评估名称旁边的星形指示评估当前已打开。
- **扫描配置**：用于扫描的扫描配置。
- **发布者**：发布评估的人的用户名
- **目标**：扫描的应用程序、项目或文件。
- **日期**：扫描完成日期。

在"已发布的评估"视图中，您可以：

- 向"我的评估"视图添加评估
- 过滤评估

- 打开和删除评估
- 关闭评估
- 比较评估
- 保存评估
- 将评估重命名
- 查看度量

提示：常规首选项设置在"已发布的评估"视图中显示的最大评估数。

协助分类的视图

此部分中的视图用于细致的扫描输出查看和管理。

- 『"评估差异"视图』
- 第 259 页的『"定制结果"视图』
- 第 263 页的『"已排除的结果"视图』
- 第 261 页的『"结果"视图』
- 第 263 页的『"已修复/缺失结果"视图』
- 第 263 页的『"已修改的结果"视图』
- 第 263 页的『"搜索结果"视图』
- 第 264 页的『"报告"视图』
- 第 266 页的『"源和接收器"视图』

"评估差异"视图

"评估差异"视图表示"我的评估"视图和"结果"视图的组合。选择两个评估以进行比较时，将显示两个评估之间的差异。

在此视图中，您可看到新建、已修复/缺失和常见结果的总数。

- 常见结果在两个评估中均可出现
- 新建结果仅出现在两个评估中的最新一个中（蓝色突出显示）
- 已修复/缺失结果仅出现在较早的一个评估中（绿色斜体突出显示）

右侧窗格显示结果。在表中右键单击结果可：

- 生成结果报告
- 将结果提交为缺陷
- 在外部编辑器中打开
- 在内部编辑器中打开

左侧窗格列出了要比较的评估。

注："评估差异"视图将忽略过滤器。

"定制结果"视图

"定制结果"视图显示当前打开的评估中存在的用户定义的或定制结果。在此视图中，您可以创建、删除和修改当前评估的定制结果。在"定制结果"视图中创建定制结果时，会将新的结果添加到当前评估，并且会更新评估度量值。

过滤器和束不会影响"定制结果"视图中的结果。在此视图中，您无法查看定制报告结果或保存选定的结果。

包含结果的视图

许多 AppScan Source for Analysis 视图都包含结果：

- "结果"视图
- "已修改的结果"视图
- "定制结果"视图
- "已排除的结果"视图
- "束"视图
- "已修复/缺失结果"视图
- "报告"视图
- "搜索结果"视图
- "评估差异"视图

结果表

下表描述了在发现表中可用的列。如果列不可用，那么可能会在表中予以隐藏。要选择列以进行查看（或者在表中执行其他任何定制任务），请按照第 260 页的『定制发现表』中的指示信息进行操作。

表 *36.* 结果表

列标题	描述
跟踪	此列中的图标指示丢失或已知的接收器存在跟踪。
严重性	• 高：对数据的机密性、完整性或可用性和/或处理资源的完整性或可用性具有风险。高严重性情况应该优先予以立即修复。 • 中：对数据安全性和资源完整性具有风险，但是此情况较不容易受到攻击的影响。中严重性情况应该予以复审，并在可能之处予以修复。 • 低：对数据安全性或资源完整性具有极低的风险。 • 参考：结果本身不易受到威胁的影响。更确切而言，它描述代码中使用的技术、体系结构特征或安全性机制。

表 *36.* 结果表 *(续)*

列标题	描述
分类	结果的类型：**明确**或**可疑**安全性结果，或者**扫描覆盖范围**结果。 **注：**某些情况下，**无**分类可用于表示某个分类既不是安全性结果也不是扫描覆盖范围结果。
漏洞类型	漏洞类别，如 `Validation.Required` 或 `Injection.SQL`。
API	易受攻击的调用，显示 API 及向其传递的参数。
源	源是对程序的输入，如文件、servlet 请求、控制台输入或套接字。对于大多数输入源，返回的数据在内容和长度方面没有限制。在未检查某个输入的情况下，会将其视为已感染。
接收器	接收器可以是可将数据写出到的任何外部格式。接收器示例包括数据库、文件、控制台输出和套接字。数据未经检查就写入接收器可能预示着严重的安全漏洞。
目录	已扫描文件的完整路径。
文件	其中出现安全性结果或扫描覆盖范围结果的代码文件的名称。结果中的文件路径与已扫描的项目工作目录相关。
调用方法	从中进行易受攻击调用的函数（或方法）。
行	代码文件中的包含易受攻击 API 的行号。
束	包含此结果的束。
CWE	由社区编写的常见软件弱点字典的标识和主题（Common Weakness Enumeration (CWE) 主题）。

定制发现表：

在包含结果的所有视图（AppScan Source for Analysis 中的"评估差异"视图除外）中，您都可以通过仅确认您希望看到的列以及列顺序来定制结果表。每个视图可能具有不同的设置，或者您可以将选项应用于所有视图。要定制列顺序，请遵循此任务主题中的步骤。

关于此任务

要了解关于发现表中列的信息，请参阅第 259 页的『结果表』。

过程

1. 单击**选择和排序列**工具栏按钮。

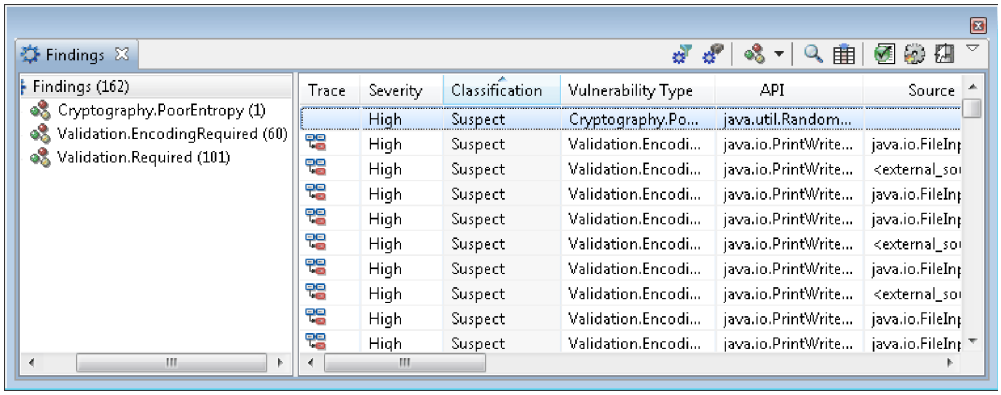
   注：在 AppScan Source for Development（Visual Studio 插件）中，单击**对表列进行选择和排序**工具栏按钮。
2. 在**选择和排序列**对话框中，选择列名称，然后单击**向上**箭头或**向下**箭头以移动列位置。
3. 单击**添加列**按钮将列添加到视图。或者，单击**删除列**按钮从视图除去列。

注：在 AppScan Source for Development（Visual Studio 插件）中，这些按钮的标签分别为**插入**和**移除**。

4. 单击**复原缺省值**以重置缺省列和列顺序。
5. 单击**确定**以保存设置。

"结果"视图

"结果"视图包含评估中结果的数据。这些结果可按本主题中列出的参数进行分组。



切记：在 AppScan Source for Development（Eclipse 插件） 和 AppScan Source for Analysis 中，这些被称为用户界面中的视图。在 AppScan Source for Development（Visual Studio 插件）中，它们被称为用户界面中的窗口。在此文档中，术语视图一般用于表示视图和窗口。

"结果"表参数分组

在"结果"视图中，选择**选择树层次结构**工具栏按钮向下箭头，然后选择对结果进行分组所依照的参数。

表 37. "结果"表参数分组

方式	分组
漏洞类型	类型、严重性、分类
分类	分类、严重性、类型
文件	项目、目录、文件、方法
API	API、类型
束	束、类型、API
CWE	CWE
表	无分组

工具栏按钮

表 38. 工具栏按钮

操作	图标	描述
显示不匹配过滤器的结果		通过此按钮，可以切换"结果"视图中已过滤结果的显示。

表 38. 工具栏按钮 (续)

操作	图标	描述
显示束结果		通过此按钮，可以切换"结果"视图中束结果的显示。此操作会隐藏已创建的所有已包含束中的结果。此设置不影响已排除束中结果的显示 - 这些结果从不在"结果"视图中显示。
选择树层次结构	因所选的分组而异。	请参阅 第 261 页的『"结果"表参数分组』。
搜索		此按钮会打开一个对话框，通过该对话框可搜索结果。该对话框中提供多种搜索选项。执行了搜索后，将在"搜索结果"视图中显示结果。
选择列并对其排序		此按钮会打开"选择列并对其排序"对话框，通过该对话框可添加或移除列，或者修改现有列。
报告视图		此按钮会打开"报告"视图，该视图根据度量了与软件安全最佳实践和法规要求的一致性的综合审计报告来显示结果。
创建定制已结果		此按钮仅在 AppScan Source for Analysis 中可用。选择此按钮会打开"创建定制结果"对话框，通过该对话框可在当前评估中添加定制结果。
保存所选结果		如果选择了一个或多个结果，那么此按钮会打开"保存所选结果"对话框，通过该对话框可将所选结果保存到新评估文件。
视图菜单		此菜单提供对所有工具栏按钮操作的快速访问途径。

在"发现"视图中，您可以：

- 在代码编辑器中打开发现
- 创建排除项
- 修改结果
- 以不同的分组查看结果
- 搜索发现以查找特定项项目

在 AppScan Source for Analysis 中使用该视图时，您还可以：

- 将结果移到束
- 将缺陷提交到缺陷跟踪系统
- 创建定制结果

- 生成结果报告
- 用电子邮件发送结果或束

"已排除的结果"视图

"已排除的结果"视图仅包含已排除的结果。已排除的结果是您从扫描中省略的结果。在此视图中，您可以搜索特定结果。此视图中的列与"结果"视图中的列相同。

要重新包含已排除的结果，请按照第 140 页的『重新包含已标记为排除项的结果』中的指示信息进行操作。

"已修改的结果"视图

"已修改的结果"视图包含当前应用程序的所有已更改的结果。已修改的结果是漏洞类型、严重性、分类或说明发生过更改的结果。丢失的结果（未在当前打开的评估中的结果）以绿色斜体字显示且无法对其进行修改。

在此视图中，您可以：

- 搜索特定结果。
- 进行其他修改

在 AppScan Source for Analysis 中，您还可以在该视图中执行以下操作：

- 将结果添加到束
- 将缺陷提交到缺陷跟踪系统
- 通过电子邮件发送结果（缺陷）
- 生成结果报告

"已修复/缺失结果"视图

"已修复/缺失结果"视图标识包含在束中但未包含在当前评估中的结果。结果标识为已修复/缺失的原因是已解决、已除去此结果或源文件未扫描。

"搜索结果"视图

搜索结果时，将在"搜索结果"视图中显示结果。

在该视图中，您可以

- 对结果排序
- 在内部或外部编辑器中编辑代码
- 设置漏洞类型
- 将可疑和扫描覆盖范围结果升级为明确结果
- 设置严重性级别
- 对结果进行注释
- 排除特定结果
- 执行后续搜索

在 AppScan Source for Analysis 中使用该视图时，您还可以：

- 将结果添加到束
- 将缺陷提交到缺陷跟踪系统或者通过电子邮件发送结果
- 生成结果报告

"搜索结果"视图仅包含与搜索条件匹配的项，并且最多保留五个搜索结果。例如，如果在"搜索结果"视图中搜索"缓冲区溢出"这一漏洞类型，然后搜索"明确"这一分类，那么搜索结果是这两个搜索的交集。

搜索条件在"搜索"字段中显示，用于表示搜索，其格式为 "<keyword>" in <originating_view>: <fields searched>，例如 "shutdown" in Findings [Context, API, Method]。如果关闭当前评估，那么将放弃所有搜索结果，并且所显示的"搜索"字段包含文本：No Current Search。

"报告"视图

通过"报告"视图，您可以根据度量了与软件安全最佳实践和法规要求的一致性的各种审计报告来组织扫描结果。

该视图根据以下报告显示结果：

- 第 191 页的『CWE/SANS Top 25 2011 报告』
- 第 191 页的『DISA 应用程序安全和开发 STIG V3R10 报告』
- 第 192 页的『开放式 Web 应用程序安全项目 (OWASP) Mobile Top 10 报告』
- 第 191 页的『开放式 Web 应用程序安全项目 (OWASP) Top 10 2013 报告』
- 第 192 页的『支付卡行业数据安全标准 (PCI DSS) V3.2 报告』
- 第 192 页的『软件安全概要文件报告』

如果您使用 AppScan Source for Analysis 来创建会保存到 <data_dir>\reports\profile（其中 <data_dir> 是 AppScan Source 程序数据的位置，如第 275 页的『安装和用户数据文件位置』中所述） 的定制报告，那么还可使用"报告"视图来通过此定制报告显示结果。

"报告"视图中的列与第 261 页的『"结果"视图』中的列相同。

搜索结果

在包含结果的多个视图中，您可以搜索特定结果。搜索条件包括束、代码、文件、项目或漏洞类型。搜索结果在"搜索结果"视图中显示。

搜索代码时，可以针对多个项目或所有项目进行搜索，包括：

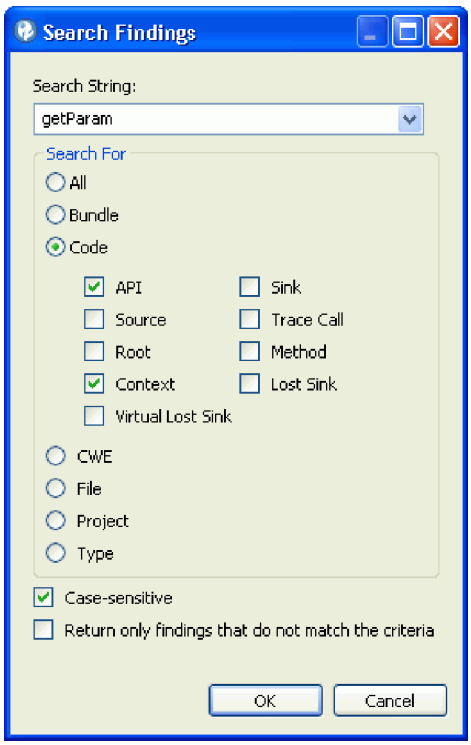
- API
- 上下文
- 方法
- 源
- 接收器
- 丢失的接收器
- 根
- 跟踪调用

在所有结果中搜索某个项的每次出现：

过程

1. 选择要在其中进行搜索的视图。

2. 从主菜单中选择**编辑** > **查找**（在 AppScan Source for Development（Eclipse 插件） 中，选择**编辑** > **查找/替换**，或在 AppScan Source for Development（Visual Studio 插件）中，在具有结果的视图上单击**搜索**按钮）。



3. 在**搜索结果**对话框中输入搜索字符串。
4. 在**束**、**代码**、**CWE**、**文件**、**项目**、**类型**或**全部**中搜索字符串。匹配的结果将在"搜索结果"视图中显示。

   选择**区分大小写**以搜索区分大小写文本。

   如果使用的是 AppScan Source for Analysis 或 AppScan Source for Development（Eclipse 插件），请选择**仅返回不满足条件的结果**以返回那些不满足搜索条件的结果。

在结果表中搜索结果：

过程

1. 单击工具栏上的**搜索**。
2. 识别搜索特性，然后单击**确定**。

在结果树中进行搜索：

过程

1. 单击工具栏上的**搜索**。
2. 识别搜索特性，然后单击**确定**。

结果

在结果视图中，您还可以在可视结果的子集内进行搜索。例如，您可能希望搜索在特定子集（如"漏洞类型"）中搜索结果。

"源和接收器"视图

"源和接收器"视图提供基于对输入和输出的跟踪来查看结果的能力

"源和接收器"视图分为三个部分：

- **源和接收器**：在左侧面板中，有三个顶级节点：
  - **源**：源是对程序的输入，如文件、servlet 请求、控制台输入或套接字。对于大多数输入源，返回的数据在内容和长度方面没有限制。在未检查某个输入的情况下，会将其视为已感染。源列在任一结果表的**源**列中。
  - **接收器**：接收器可以是数据能够写为的任意外部格式。接收器示例包括数据库、文件、控制台输出和套接字。数据未经检查就写入接收器可能预示着严重的安全漏洞。
  - **丢失的接收器**：丢失的接收器是指无法继续跟踪的 API 方法。

  可以对每个节点进行扩展以显示受影响的软件包。软件包进而可进一步扩展以显示受影响的类以及方法。然后可以对这些方法进行扩展以在跟踪的另一端显示软件包、类以及方法。例如，如果您关注某个特定的接收器，那么您可以向下钻取到**接收器**根目录下的方法。一旦到达此处，该方法下的树将显示返回（指向该接收器的）所有源的路径：

```
- Sources
 - packageA
  - classA
   - methodA
    - packageB
     - classB
            - methodB（跟踪的相反一端）
- Sinks
 - packageB
  - classB
   - methodB
    - packageA
     - classA
      - methodA
- Lost Sinks
```

  在此树视图中所作的选择将确定在视图的其他两个部分中显示的内容。

- **中间节点**：视图的此部分显示应用于"源和接收器"部分中所选项的跟踪的所有中间节点的集合。它允许您对结果表中显示的内容进行优化。

  此部分在缺省情况下会隐藏。通过单击**显示/隐藏中间调用表**可对其进行显示（或再次隐藏）。

  要仅显示软件包、类或方法的结果，请选中其**必需**列中的复选框。要过滤出软件包、类或方法的结果，请选中其**除去**列中的复选框。在此部分中所作的过滤器设置可以用来创建新过滤器。

  用法示例：给定"源和接收器"部分中的以下树节点：

```
- Sources
 - java.util
  - Properties
   - getProperty
```

当选择 getProperty 时，结果表仅显示包含将 getProperty 作为源的跟踪的那些结果。此时，中间节点部分将显示源为 getProperty 的所有跟踪的所有中间节点（跟踪内除了源和接收器之外的所有节点）。然而，您可能不关心跟踪是否通过了特定 API。例如，您可能具有用于确保来自 getProperty 中的数据有效性的验证例程，因此，您不想查看通过此验证例程的跟踪。中间节点部分将包含此验证例程，因为它是跟踪的中间节点。您可以浏览到中间节点部分中的此验证例程，然后单击其**除去**复选框。这将从具有通过了此中间节点的跟踪的结果表中除去所有结果。

- **结果**：此部分与第 261 页的『"结果"视图』以及具有结果的其他视图都具有相同的第 259 页的『结果表』（以及关联操作）。它显示您已选择以在视图的其他两个部分中显示的源、接收器和中间节点的结果。

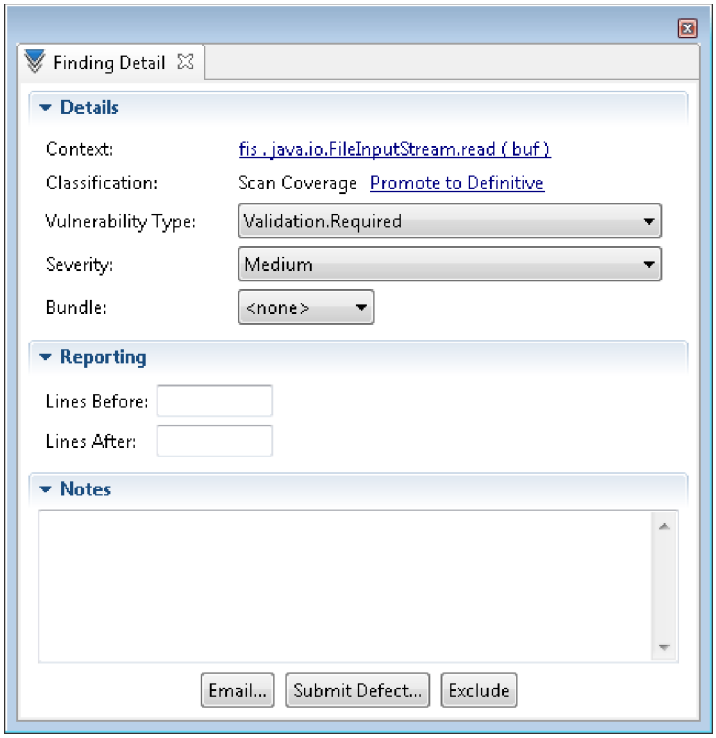
用于调查单个结果的视图

此部分中的视图用于调查单独的结果。

- 第 147 页的『"结果详细信息"视图』
- 第 269 页的『"修复帮助"视图』
- 第 269 页的『"跟踪"视图』

"结果详细信息"视图

选择结果后，"结果详细信息"视图将显示并允许您修改其属性。通过该视图，您可以修改单个结果。



- 第 148 页的『"详细信息"部分』
- 第 148 页的『"报告"部分（仅在 AppScan Source for Analysis 和 AppScan Source for Development（Eclipse 插件）中可用）』
- 第 148 页的『"注释"部分』
- 第 148 页的『"结果详细信息"视图操作』
- 第 149 页的『定制结果的"结果详细信息"视图（仅在 AppScan Source for Analysis 中可用）』

"详细信息"部分

- **上下文**：漏洞周围的代码片段
- **分类**：明确或可疑安全性结果或者扫描覆盖范围结果，并且具有用于将结果提升为**明确**或还原为原始值（如果分类已更改）的链接
- **漏洞类型**
- **严重性**：高、中、低或参考
- **束**：包含结果的束的名称（在 AppScan Source for Development（Visual Studio 插件）中不可用）

"报告"部分（仅在 AppScan Source for Analysis 和 AppScan Source for Development（Eclipse 插件）中可用）

指定在报告中的结果之前和/或之后要包含的代码行的数量。

"注释"部分

对结果进行注释。

"结果详细信息"视图操作

- **排除**：单击**排除**以从结果表中排除（移除）结果。要查看已排除的结果，请打开"已排除的结果"视图。
- 仅在 AppScan Source for Analysis 中可用：
  - **发送电子邮件**：如果您已配置电子邮件首选项，那么可以通过电子邮件直接将结果束发送给开发者以告知他们扫描后所发现的潜在缺陷。该电子邮件包含束附件（其中含有结果），并且电子邮件文本描述这些结果。
    1. 要通过电子邮件发送"结果详细信息"视图中的当前结果，请单击**发送电子邮件**。
    2. 在"附件文件名"对话框中，指定将附加到电子邮件的结果束的名称。例如，在**附件文件名**字段中指定 `my_finding` 会将文件名为 `my_finding.ozbdl` 的束附加到电子邮件。
    3. 单击**确定**以打开"通过电子邮件发送结果"对话框。缺省情况下，将使用电子邮件首选项中指定的**收件人地址**来填充"通过电子邮件发送结果"对话框中的**收件人**字段，不过，可在准备电子邮件时轻松对其进行更改。在此对话框中，复审电子邮件的内容，然后单击**确定**以发送电子邮件。
  - **提交缺陷**：要将结果提交为缺陷，请单击**提交缺陷**。这将打开"选择缺陷跟踪系统"对话框。

- 如果选择 **ClearQuest** 并单击**确定**，那么将打开"附件文件名"对话框。在该对话框中，指定将附加到缺陷的结果束的名称，然后单击**确定**。登录到 Rational ClearQuest，然后提交结果。
- 如果选择 **Quality Center** 并单击**确定**，那么将打开"登录"对话框，使您能够登录到 Quality Center 以提交结果。
- 如果选择任一 **Team Foundation Server** 选项，那么均将打开一个对话框，提示您登录到缺陷跟踪系统并提供其他配置详细信息。

注：Rational Team Concert 是 macOS 上唯一受支持的缺陷跟踪系统。

定制结果的"结果详细信息"视图（仅在 AppScan Source for Analysis 中可用）

定制结果的"结果详细信息"视图提供您可以编辑的其他信息：

- 文件
- 行
- 列
- API

此外，对于某些字段，编辑第 148 页的『"详细信息"部分』所用的方法与标准结果不同（例如，定制结果的分类显示在列表中）。

"修复帮助"视图

AppScan Source 安全知识库提供各漏洞的特定于上下文的情报。知识库告诉您漏洞是什么，它为什么不安全，如何对其进行修复，以及如何在将来予以避免。一旦扫描了源代码，知识库便会提供从任务关键应用程序中消除风险所需的特定信息。知识库补救建议会在"补救帮助"视图中显示。一旦进行了扫描，知识库便会提供从任务关键应用程序中消除风险所需的特定信息。

查看知识库并获取补救建议

- 选择结果表中的一个结果，然后打开 知识库"帮助"或"修复帮助"视图。
- 在 AppScan Source for Analysis 中，您还可以从菜单中选择**帮助** > **安全性知识库**以查看整个知识库。

数据库中的特定 API 会列出严重性级别和严重性类型。例如，API `strcpy()`（缓冲区溢出类型）具有"高"严重性级别。该描述说明 `strcpy()` 易受目标缓冲区溢出攻击，因为它不知道目标缓冲区的长度，因此无法进行检查以确保它不会覆盖目标缓冲区。使用带有长度参数的 `strncpy ()` 来修复此问题。

如果结果具有关联的公共弱点枚举 (CWE) 标识，那么在"修复帮助"视图中，将出现指向 CWE 主题 (`CWE: <id>`) 的超链接：`http://cwe.mitre.org/data/definitions/<CWE_ID>.html`。

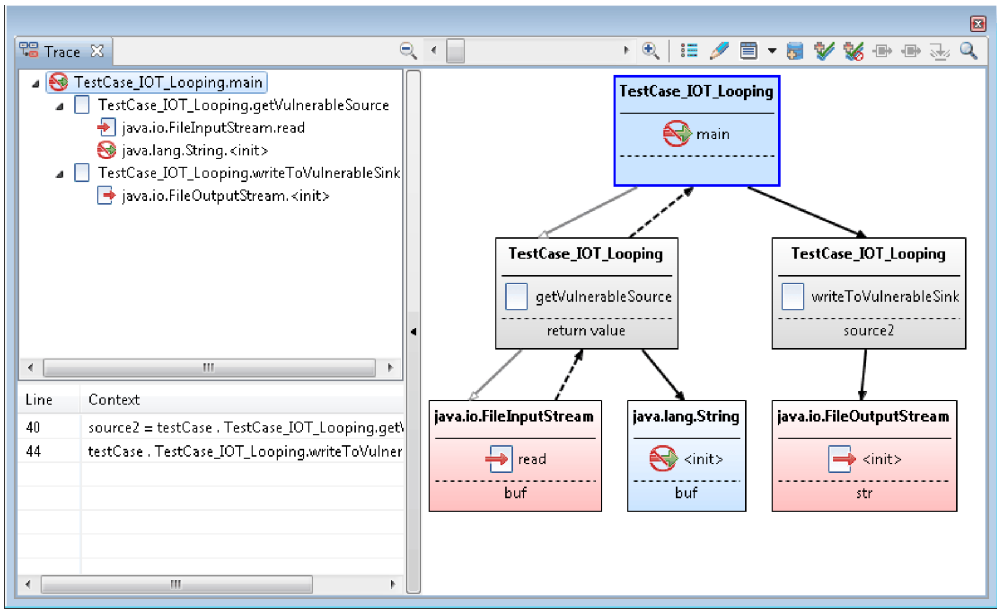
"跟踪"视图

AppScan Source 执行输入/输出分析并且识别和显示这些漏洞。结果列表中会出现一个图标以标识包含了 AppScan Source 跟踪图形的行。

在"跟踪"视图中，您将看到根节点，输入和输出堆栈汇接于此根节点。输入堆栈是导向已知提供已感染数据的源的一系列调用。输出堆栈是导向接收器的一系列调用。如果所分析的代码可以跟踪对未受保护接收器使用未受保护源的情况，那么将生成 AppScan Source 跟踪。

- **源**：源是对程序的输入，如文件、servlet 请求、控制台输入或套接字。对于大多数输入源，返回的数据在内容和长度方面没有限制。在未检查某个输入的情况下，会将其视为已感染。源列在任一结果表的**源**列中。
- **接收器**：接收器可以是数据能够写为的任意外部格式。接收器示例包括数据库、文件、控制台输出和套接字。数据未经检查就写入接收器可能预示着严重的安全漏洞。
- **丢失的接收器**：丢失的接收器是指无法继续跟踪的 API 方法。

该图说明了从根经过输入堆栈和输出堆栈的调用序列。



在该图中：

- 空心箭头显示不具有已知的受感染数据流的调用。
- 实心箭头表示具有可能受感染的数据。虚线显示返回路径。
- 实线表示方法调用。

提示：

- 在"跟踪"视图中，将鼠标悬停在图形中的跟踪节点上将提供关于此节点的信息。
- 该视图中的两个左面板（输入/输出堆栈面板和数据流面板）可折叠以便更容易查看图形调用图。要折叠这些面板，请选择**隐藏树视图**箭头按钮。要在这些面板被隐藏时显示它们，请选择**显示树视图**箭头按钮。
- 移动滚动条可放大并聚焦于详细信息，或者缩小以查看更多内容。将鼠标悬浮在缩放滚动条上将提供当前缩放级别。要放大到最高级别，请单击**放大到 200%**。要尽可能缩小，请单击**缩放到适合**。

用于处理评估的视图

此部分中的视图用于在高级别处理评估。

- 『"评估摘要"视图』
- 『"过滤器编辑器"视图』
- 第 272 页的『"漏洞矩阵"视图』

"评估摘要"视图

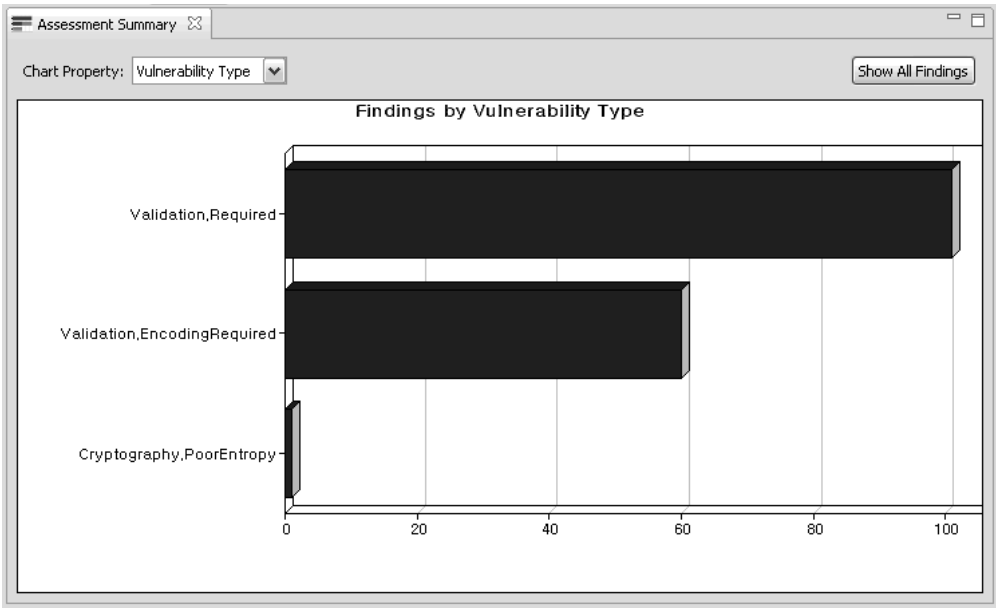
"评估摘要"视图是一种打开的评估条形图图形视图，显示所选结果的信息。

注：

- "评估摘要"视图在 macOS 上不可用。
- 在 AppScan Source for Development（Visual Studio 插件）中，该视图是"编辑过滤器"窗口的一部分。

可以按图表属性查看：

- **漏洞类型**：漏洞分类，如 `Validation.Encoding` 或者 `Injection.SQL`
- **API**：其中出现漏洞的 API 名称
- **项目**：按项目排列的结果（如果存在多个项目）
- **文件**：其中出现漏洞的单个文件



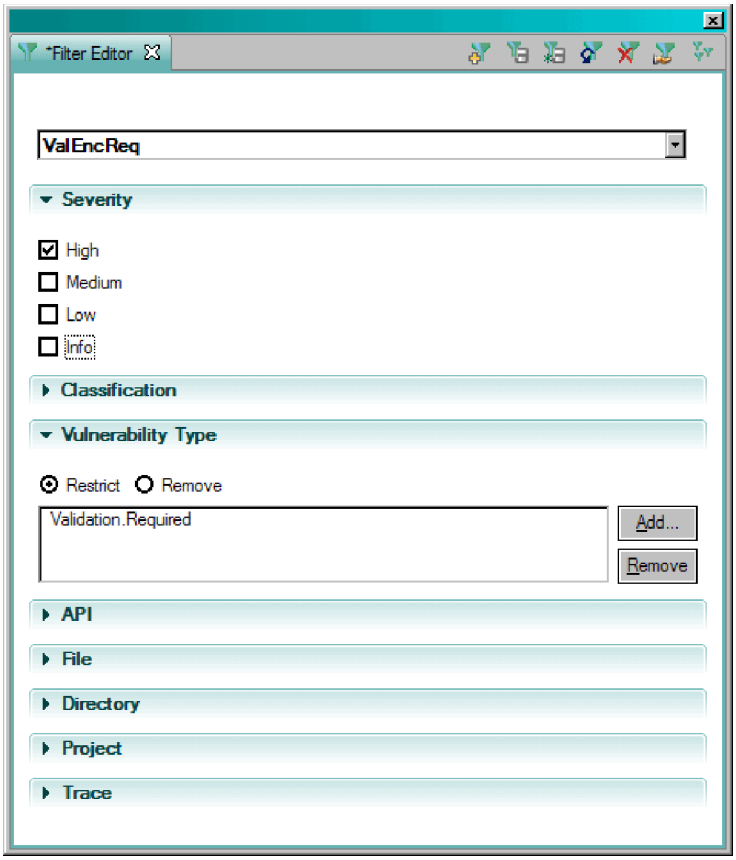
单击图表以向下钻取到结果的详细信息并开始筛选。

提示：将鼠标悬停在"评估摘要"视图中的条形图上会提供以条形表示的精确结果数。

"过滤器编辑器"视图

"过滤器编辑器"视图提供比 AppScan Source 视图更详细的对当前所选过滤器的处理。该视图包含您可以依据其过滤的所有条件。

注：在 AppScan Source for Development（Visual Studio 插件）中，该视图是"编辑过滤器"窗口的一部分。

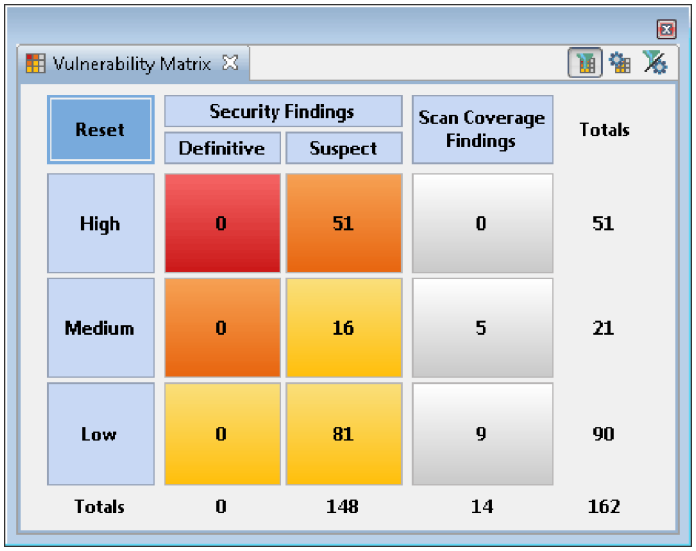


提示：在"过滤器编辑器"视图的**跟踪**部分中，将鼠标悬停在跟踪条目上会提供关于该条目的详细信息。

"漏洞矩阵"视图

"漏洞矩阵"视图显示扫描中所包含全部应用程序的结果的合计数量。对结果的修改将更新此矩阵。

注：在 AppScan Source for Development（Visual Studio 插件）中，该视图是"编辑过滤器"窗口的一部分。



安全性结果和扫描覆盖范围结果在有颜色的方框内显示，这些方框指示了调查或处理结果时应采取的优先顺序：

1. 高严重性明确结果的颜色为红色，标记为最高优先级。
2. 中严重性明确结果和高严重性可疑安全性结果的颜色为橙色，应该在上述项之后进行处理。
3. 以下矩阵条目的颜色为黄色，应该在上述项之后予以考虑：
   - 低严重性明确安全性结果
   - 中低严重性可疑安全性结果
4. 扫描覆盖范围结果位于灰色正方形中，并且可以被授予最低优先级。

单击**漏洞矩阵**中的单元格、行标题或列标题时，该视图将更新当前过滤器以仅包含该单元格、行或列中的结果。单击**重置**可返回到所有结果的视图。

在"漏洞矩阵"视图中，工具栏按钮用于控制有颜色的方框内的数字。您可以查看：

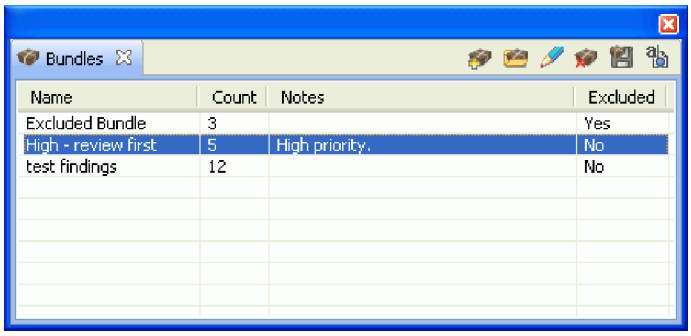
- 仅进行了过滤的结果的计数和总数
- 结果的计数和总数

  注："漏洞矩阵"视图中不包含**质量**结果和分类为**参考**严重性级别的结果。
- 进行了过滤的结果以及所有结果的计数和总数

注：在"漏洞矩阵"视图外应用的过滤器可能不会影响"漏洞矩阵"视图。必须选择"漏洞矩阵"视图**显示已过滤结果的计数**工具栏按钮才会在"漏洞矩阵"视图中反映过滤器。

"束"视图

在"束"视图中，可新建束，向束中添加结果，查看束和说明，对束进行重命名或删除束。此视图列出了束名称、附加到束的任何说明、束中的结果数，以及束是否已排除。打开束查以看其内容时，可将结果移至其他束，修改结果，编辑代码，或者将束提交到缺陷跟踪系统。



更多相关信息，请参阅第 142 页的『通过束进行筛选』。

"束"视图

"束"视图显示束中的结果。束是在 AppScan Source for Analysis 中创建的结果的集合。

要查看束中的结果，请双击"束"视图中的束名称。束名称在"束"视图中显示为标题。您也可以导入束，然后在"束"视图中查看其内容。您无法修改或删除束中的结果。

类似于结果表的"束"视图包含以下详细信息：

表 39. "束"视图列

列	描述
跟踪	此列中的图标指示丢失或已知的接收器存在跟踪。
文件	其中出现安全性结果或扫描覆盖范围结果的代码文件的名称。结果中的文件路径与已扫描的项目工作目录相关。
分类	结果的类型：**明确**或**可疑**安全性结果，或者**扫描覆盖范围**结果。 **注：**某些情况下，**无**分类可用于表示某个分类既不是安全性结果也不是扫描覆盖范围结果。
严重性	• 高：对数据的机密性、完整性或可用性和/或处理资源的完整性或可用性具有风险。高严重性情况应该优先予以立即修复。 • 中：对数据安全性和资源完整性具有风险，但是此情况较不容易受到攻击的影响。中严重性情况应该予以复审，并在可能之处予以修复。 • 低：对数据安全性或资源完整性具有极低的风险。 • 参考：结果本身不易受到威胁的影响。更确切而言，它描述代码中使用的技术、体系结构特征或安全性机制。
漏洞类型	漏洞类别，如 `Validation.Required` 或 `Injection.SQL`。
上下文	漏洞周围的代码片段。
调用方法	从中进行易受攻击调用的函数（或方法）。

表 39. "束"视图列 (续)

列	描述
CWE	由社区编写的常见软件弱点字典的标识和主题（Common Weakness Enumeration (CWE) 主题）。
行	代码文件中的包含易受攻击 API 的行号。
说明	添加到此结果中的任何说明。
缺陷标识	缺陷跟踪系统中的缺陷标识。

安装和用户数据文件位置

安装 AppScan Source 时，用户数据和配置文件存储在安装目录外。

- 『缺省安装位置』
- 『缺省 AppScan Source 数据目录』
- 第 276 页的『AppScan Source 临时文件位置』

缺省安装位置

安装了 AppScan Source 后，该软件位于以下缺省位置之一：

- Microsoft Windows 32 位版本：

  `<SYSTEMDRIVE>:\Program Files\IBM\AppScanSource`
- Microsoft Windows 64 位版本：

  `<SYSTEMDRIVE>:\Program Files (x86)\IBM\AppScanSource`
- Linux：如果您是 root 用户，那么安装向导会将软件安装在 `/opt/ibm/appscansource` 中。如果您不是 root 用户，那么可以安装 AppScan Source for Development Eclipse 插件，它在缺省情况下安装到 `<home_directory>/AppScan_Source`。
- macOS：`/Applications/AppScanSource.app`

要点：

- 安装目录名只能包含英语字符。不允许文件夹名包含非英语字符。
- 如果您是在 Windows 上进行安装，那么必须拥有管理员特权才能安装 AppScan Source 组件。
- 如果您是在 Linux 上进行安装，那么必须拥有 root 用户特权才能安装 AppScan Source 服务器组件。

缺省 AppScan Source 数据目录

AppScan Source 数据由诸如配置、样本和目录文件的项组成。安装了 AppScan Source 后，数据文件在缺省情况下位于以下位置：

- Microsoft Windows：`<SYSTEMDRIVE>:\ProgramData\IBM\AppScanSource`

  注：`ProgramData\` 是隐藏的文件夹，要查看该文件夹，必须在**资源管理器**中修改您的查看首选项以显示隐藏的文件和文件夹。
- Linux：`/var/opt/ibm/appscansource`

- macOS：/Users/Shared/AppScanSource

要了解如何更改 AppScan Source 数据目录的位置，请参阅『更改 AppScan Source 数据目录』。

AppScan Source 临时文件位置

某些 AppScan Source 操作会导致创建临时文件，这些临时文件缺省情况下存储在以下位置：

- Microsoft Windows：<SYSTEMDRIVE>:\ProgramData\IBM\AppScanSource\temp

  注：ProgramData\ 是隐藏的文件夹，要查看该文件夹，必须在**资源管理器**中修改您的查看首选项以显示隐藏的文件和文件夹。
- Linux：/var/opt/ibm/appscansource/temp
- macOS：/Users/Shared/AppScanSource/temp

临时文件位置始终在 AppScan Source 数据目录内的 temp 目录中。您可以通过更改数据目录来更改临时文件位置，如『更改 AppScan Source 数据目录』中所述。这将使 temp 位于您已选的数据目录中。

更改 AppScan Source 数据目录

您可能想要更改 AppScan Source 数据目录的位置，以管理硬盘空间。您可以按照本主题中的步骤来在 AppScan Source 安装后更改此位置。

开始之前

完成此任务之前，请确保所有 AppScan Source 客户机应用程序都已退出或关闭。AppScan Source 客户机应用程序包括：

- AppScan Source for Analysis
- AppScan Source for Development（Eclipse 或 Visual Studio 插件）（仅在 Windows 和 Linux 上受支持）
- AppScan Source 命令行界面 (CLI)
- AppScan Source for Automation

此外，如果您已安装 AppScan Source for Automation，请确保 自动化服务器 已关闭：

- 在 Windows 上，请停止 **IBM Security AppScan Source Automation** 服务。
- 在 Linux 上，发出以下命令：/etc/init.d/ounceautod stop
- 在 macOS 上，发出以下命令：launchctl stop com.ibm.appscan.autod

过程

1. 定义 APPSCAN_SOURCE_SHARED_DATA=<data_dir> 环境变量，其中 <data_dir> 是要将 AppScan Source 数据存储在的位置。

   注：

   - <data_dir> 位置必须是 AppScan Source 所安装在的机器上已存在的完整绝对路径。
   - <data_dir> 目录名称只能包含英语字符。不允许文件夹名包含非英语字符。

2. 找到安装 AppScan Source 时创建的缺省数据目录（请参阅第 275 页的『缺省 AppScan Source 数据目录』以了解缺省数据目录位置）。
3. 将缺省数据目录的内容复制或移动到上述环境变量中所指定的 <data_dir> 位置。
4. **仅适用于 Linux 上安装的 AppScan Source for Automation**：
   a. 编辑 /etc/init.d/ounceautod 文件。
   b. 找到以下行：

```
su - ounce -c
'export LD_LIBRARY_PATH="/opt/IBM/AppScan_Source/bin":$LD_LIBRARY_PATH &&
cd "/opt/IBM/AppScan_Source/bin" &&
"/opt/IBM/AppScan_Source/bin/ounceautod" -s' >>
"/var/opt/ibm/appscansource/logs/ounceautod_output.log" 2>&1 &
```

   并将其替换为以下内容：

```
su - ounce -c
'export APPSCAN_SOURCE_SHARED_DATA=<new data directory path here> &&
export LD_LIBRARY_PATH="/opt/IBM/AppScan_Source/bin":$LD_LIBRARY_PATH &&
cd "/opt/IBM/AppScan_Source/bin" &&
"/opt/IBM/AppScan_Source/bin/ounceautod" -s' >>
"<new data directory path here>/logs/ounceautod_output.log" 2>&1 &
```

   注：以上命令为一行。
   c. 保存 /etc/init.d/ounceautod 文件。

下一步做什么

如果您已安装 AppScan Source for Automation，请启动 自动化服务器：

- 在 Windows 上，请启动 **IBM Security AppScan Source Automation** 服务。
- 在 Linux 上，发出以下命令：/etc/init.d/ounceautod start
- 在 macOS 上，发出以下命令：launchctl start com.ibm.appscan.autod

第 15 章 CWE 支持

常用弱点枚举 (CWE) 是一种行业标准列表，它提供了公众熟知的软件弱点的常见名称。该主题列出了 AppScan Source 的当前版本中受支持的 CWE 标识。

扫描期间，AppScan Source 查找以下 CWE 列表标识，以及它们的父标识或子标识。

表 *40. CWE* 支持

15、16、20、73、74、77、79、88、89、90、91、95、98
105、109、112、113、116、117、120、129、130、131、134、185、190
201，209，242，250，257，264，266，267，285，287，288，295
310，311，312，319，327，331，335，345，352，359，367，382，388，390，398
400，404，407，425，434，447，470，472，477，489，497
506，507，511，517，520，521，522，523，524，525，532，538，543，544，546，547，565，569，586
601，613，615，624，643，645

© Copyright IBM Corp. 2003, 2017

术语表

本术语表包含 AppScan Source 的术语和定义。

本术语表中使用下列交叉引用：

- 参见将您从某个术语指引到首选同义词，或从从缩略词或缩写词指引到已定义的完整格式。
- 另请参见将您指引到相关或相反的术语。

要查看其他 IBM 产品的术语表，请转至 www.ibm.com/software/globalization/terminology。

B

编码 (encode)
在计算机安全性中，使用代码系统将明文转换为无法了解的格式。

D

调用图 (call graph)
使用线的一幅图，表示程序中子例程之间的数据流。

丢失的接收器 (lost sink)
无法继续跟踪的 API 方法。

堆栈 (stack)
内存中的某个区域，通常用于存储诸如临时注册信息、参数值以及子例程的返回地址等信息，且基于后进先出 (LIFO) 的原则。

F

发现项目 (finding)
发现代码中安全性暴露的实例。AppScan 将发现分为两类：漏洞和异常。

G

感染 (taint)
允许在代码中分布的不安全数据。

工作台 (workbench)
Eclipse 和基于 Eclipse 的工具（例如 IBM Rational Application Developer）中的用户界面和集成开发环境 (IDE)。

攻击 (attack)
未授权的个人想要破坏软件程序或网络系统的操作而进行的所有尝试。

过滤器 (filter)
以某些特征定义发现的一组规则。

© Copyright IBM Corporation 2005, 2013 © IBM 2003, 2017

H

回调 (callback)
一个线程用于通知另一应用程序线程发生了事件的方式。

会审 (triage)
评估发现以及确定如何予以解决的过程。

J

接收器 (sink)
数据可以写入到的任何外部格式。接收器示例包括数据库、文件、控制台输出和套接字。

K

跨站点脚本编制 (cross-site scripting)
强制 Web 站点回传客户机提供的数据（在用户的 Web 浏览器中执行）的一种攻击技术。

L

漏洞分析高速缓存 (vulnerability analysis cache)
在源代码的扫描期间发现的漏洞的高速缓存，可以用于后续扫描以减少扫描时间。

P

排除 (exclusion)
用户可以标记并忽略的发现。

评估 (assessment)
通过扫描代码生成的发现项目的集合，用户可以对其进行处理、保存并与其他人共享。

Q

缺陷 (defect)
一个变更请求类型，标识工作产品中的反常或缺陷。

S

扫描 (scan)
AppScan 探索和测试应用程序并提供结果的过程。

扫描规则 (scan rule)
在扫描期间搜索的模式或正则表达式。

属性 (attribute)
应用程序的特征，帮助将扫描结果组织为有意义的分组，例如：部门或项目主管。

束 (bundle)
用户创建的一组发现。可以导出并在人员与应用程序之间共享束。

T

套接字 (socket)
TCP/IP 使用的通信句柄。

透视图 (perspective)
一组视图，显示工作台中资源的各个方面。

V

V-Density
允许以一致方式评估应用程序漏洞的数字表达式。V-Density 通过将漏洞和异常的数量及关键性与进行分析的应用程序或项目的大小相关联来计算。

X

XSS 请参阅跨站脚本编制 (cross-site scripting)。

修复 (remediation)
有关如何修订问题的建议。

Y

异常 (exception)
指示需要其他信息或调查的可疑且可能易受攻击的情况。

应用程序 (application)
一个或多个计算机程序或软件组件，用于在特定业务流程或过程的直接支持中提供功能。

Z

组合件 (assembly)
构成 .NET Framework 应用程序中部署、版本控制、复用、激活作用域限定和安全许可权的单元的类型和资源的集合。

声明

本信息是为在美国国内供应的产品和服务而编写的。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。有关您所在区域当前可获得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，则由用户自行负责。

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

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

有关双字节字符集 (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.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

本条款不适用于英国或任何这样的条款与当地法律不一致的国家或地区：

INTERNATIONAL BUSINESS MACHINES CORPORATION"按现状"提供此出版物，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、适销或适用于某种特定用途的保证或条件。

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。

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

本信息中对任何非 IBM Web 站点的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 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。

© Copyright IBM Corp. 2003, 2017

本程序的被许可方如果要了解有关程序的信息以达到如下目的：(i) 允许在独立创建的程序和其他程序（包括本程序）之间进行信息交换，以及 (ii) 允许相互使用已交换的信息，请与下列地址联系：

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 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数据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，它们仅仅表示目标和意愿。

显示的所有 IBM 价格皆为 IBM 建议的最新零售价格，且可随时更改，而不另行通知。经销价格可能会有差异。

本信息仅限规划目的使用。在提供所述的产品之前，此处的信息得随时更改。

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。所有这些名称都是虚构的，如与实际商业企业所使用的名称和地址有任何雷同，纯属巧合。

版权许可证：

本信息包含源语言形式的样本应用程序，用以阐明在不同操作平台上的编程技术。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。如果是为按照 IBM 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。

这些样本程序的每份拷贝/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) (年份)。此代码的某些部分是根据 IBM 公司的样本程序衍生出来的。
© Copyright IBM Corp. _输入年份_. All rights reserved.

如果您正在查看本信息的软拷贝形式，图片和彩色图例可能无法显示。

商标

IBM、IBM 徽标和 ibm.com 是 International Business Machines Corp. 在全球许多管辖区域内的商标或注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。IBM 商标的当前列表可从 Web 站点 www.ibm.com/legal/copytrade.shtml 处获取。

Adobe、Acrobat、PostScript 以及所有基于 Adobe 的徽标是Adobe Systems Incorporated 在美国和/或其他国家或地区的注册商标或商标。

IT Infrastructure Library 是 Central Computer and Telecommunications Agency 的注册商标，该企业现已成为 Office of Government Commerce 的一部分。

Intel、Intel 徽标、Intel Inside、Intel Inside 徽标、Intel Centrino、Intel Centrino 徽标、Celeron、Intel Xeon、Intel SpeedStep、Itanium 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。

Linux 是 Linus Torvalds 在美国和/或其他国家或地区的商标。

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

ITIL 是英国政府商务部的注册商标和欧盟注册商标，且已在美国专利和商标局注册。

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

Java 和所有基于 Java 的商标和徽标是 Oracle 和/或其子公司的商标或注册商标。

Cell Broadband Engine 是 Sony Computer Entertainment, Inc. 在美国和/或其他国家或地区的商标。

Tape-Open、LTO、LTO徽标、Ultrium 和 Ultrium 徽标是 HP、IBM Corp. 及 Quantum在美国和/或其他国家或地区的商标。

索引

[A]

[B]

[C]

[D]

[F]

[G]

© Copyright IBM Corp. 2003, 2017

[J]

[K]

[L]

[M]

[N]

[P]

[Q]

[R]

[S]

[T]

[W]

[X]

[Y]

[Z]

A

C

D

E

F

G

H

I

Printed in China