如果在扫描后未运行结果专家，“问题信息”选项卡将显示其他三个选项卡上的信息摘要，但是不含附加信息。不过，您可以随时更新选项卡:

- 要更新所发现的所有问题的“问题信息”选项卡，请依次单击**工具 > 运行扫描专家**。
- 要更新单个问题的“问题信息”选项卡，请打开该问题的**请求/响应选项卡**，然后选择**创建问题信息**。

区域	描述
标题	问题标题，包括 URL、实体和安全风险。
CVSS 度量值评分	三个 CVSS 度量值组的图形说明：基本、临时和环境。
提示（黄色框）	此信息指的是内容区域（下方）并说明在此处出现的图像或 HTML 中要注意的内容。
内容（屏幕快照或 HTML 代码）	根据问题，此区域可能包括一个屏幕快照、两个供比较的屏幕快照、一个含模拟弹出窗口的屏幕快照或 HTML 代码。（此内容还在选项卡旁通过缩略图表示。）如果是 HTML，您可以通过单击内容区域右上角的图标，将文本换行切换打开和关闭。
推理（蓝色框）	说明 Rational AppScan 已执行的操作及其将此视为问题的原因。
技术摘要（灰色框）	Rational AppScan 为测试此问题已执行的操作及其如何验证响应的技术详细信息。

“问题信息”工具栏

“详细信息”窗格上方的工具栏会显示所选问题的当前严重性及其状态，并使您能够在问题之间进行切换。

- **严重性**：选择四种标准严重性设置之一，或者手动调整此问题的 CVSS 设置。
- **状态**：选项包括“公开”或“干扰”。缺省为“公开”。对于不重要的问题，选择“干扰”。缺省情况下，指定为“干扰”的结果在结果列表中显示时带有删除线。要将其完全从显示中移除，请取消选择**工具 > 显示标记为干扰的问题**。

问题信息缩略图

“问题信息”选项卡右侧的缩略图图像表示包含在“问题信息”选项卡中，将与扫描结果一起保存并可以包含在 Word 报告中的相关屏幕快照或其他图像。

- 您可以通过单击  图标并浏览到要添加的图像来添加一幅图像。
- 您可以向任何图像添加注释和在 Word 报告中包含/排除图像，方法是单击图像的缩略图以打开“图像信息”对话框，然后选中/取消选择**在报告中包含图像**复选框。
- 您可以使用右键单击菜单从扫描结果中删除当前所选的缩略图。

CVSS 设置

您可以手动微调基于 CVSS 度量值的特定问题的严重性设置。这可通过从“问题信息”工具栏单击**严重性 > CVSS 设置**来实现。

从 CVSS 窗口单击三个部分其中之一的名称，打开该部分以进行配置。您可以恢复缺省设置

基本度量值

这些是漏洞的固定度量值，不随时间和用户环境的变化而变化。

度量值	说明	选项
访问向量	漏洞是仅可从本地利用，也可从相邻网络利用，还是可从任何网络连接利用（“可远程利用”）。	本地、相邻网络、网络
访问复杂度	利用该漏洞所涉及的困难。	高、中、低
认证	为了利用漏洞，攻击者必须认证的次数。	无、一次、多次
机密性影响	成功利用该漏洞对机密性的影响。	无、部分、完整
完整性影响	成功利用该漏洞后损害系统完整性（由应用程序提供的信息准确性）的程度。	无、部分、完整
可用性影响	成功利用该漏洞对信息资源可用性的影响。	无、部分、完整

时间度量值

这些是可能会随时间而更改的漏洞度量值。

度量值	说明	选项
可利用性	利用该漏洞的开发技术的当前状态。	未核准、概念证明、功能、高、未定义
补救级别	对漏洞进行防护的可用补救级别。	官方修订、临时修订、变通方法、不可用、未定义
报告置信度	漏洞的存在和技术详细信息的置信度等级。	未确定、未证实、已确定、未定义

环境度量值

这些度量值反映应用程序环境，并应使用“配置”对话框 > “环境度量值”选项卡全局设置。仅当该漏洞特定于应用程序环境中具有不同特性的某部分时，才在此处对其进行更改。

度量值	说明	选项
潜在间接损害	如果应用程序有漏洞，可能会被损坏或被盗。	无、低、低中、中、中高、高、未定义
目标分布	属于潜在目标的环境中系统的比例。	无、低、中、高、未定义
可用性需求	（信息的）可用性的相对重要性。	无、低、中、高、未定义
机密性需求	（用户信息的）机密性的相对重要性。	无、低、中、高、未定义
完整性需求	信息完整性（精确性）的相对重要性。	无、低、中、高、未定义

恢复缺省严重性设置

如果已（通过选择其他严重性或调整 CVSS 设置）手动更改特定问题的严重性设置，您可以恢复先前设置。

- 要使用基于该问题的当前 CVSS 设置的设置来替换手动设置（高/中/低/参考信息），请执行以下操作：在“问题信息”工具栏上，单击**严重性 > 使用 CVSS 来计算严重性**。
- 要恢复*缺省* CVSS 设置，请执行以下操作：在“问题信息”工具栏上，单击**严重性 > CVSS 设置**，然后在打开的 CVSS 设置窗口中单击 

“咨询”选项卡

“咨询”选项卡上的信息会提供有关所选问题的技术详细信息，以及更多信息的引用链接。当需要说明必须修订的内容和原因时，此信息至关重要。

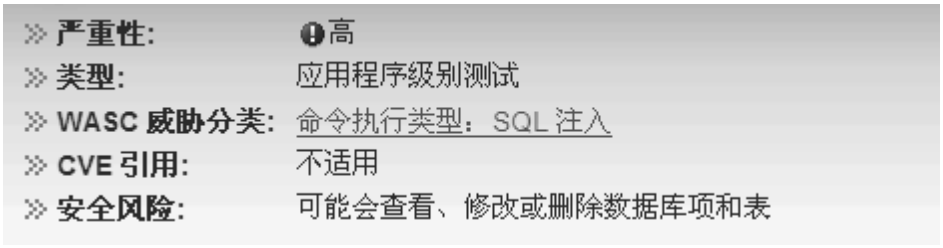
咨询选项卡可能会包含下列任一部分:

- **测试名称** – 出现在**结果列表**中。此信息可以帮助您稍后查找同一咨询。
- **测试描述** – 测试的类型。如果此描述没有显示侵入式，那么测试为非侵入式；它还会显示测试是应用程序级别还是基础结构级别。
- **WASC 威胁分类** – 指向描述此类威胁的 Web 应用程序安全联盟页面的互联网链接。
- **CVE 引用** –（如果适用）针对此类型测试的行业标准号。（有关 AppScan 如何支持 CVE 的详细信息，请参阅 『CVE 支持』。）
- **安全风险** – 作为应用程序安全风险的问题的说明。
- **培训模块** – 解释并说明问题的 Adobe Flash 演示。
- **可能原因** – 暗示问题在应用程序中的成因。
- **技术描述** – 问题的特定技术性描述。
- **受影响产品** – 可能会受到问题影响的第三方产品。
- **引用和相关链接** – 指向更多信息的链接。

CVE 支持

CVE（公共漏洞和暴露）是一个行业标准列表，可提供众所周知信息安全漏洞和暴露的公共名称。这为独立数据库和工具间的数据共享提供了便利。（有关更多详细信息，请访问 CVE Web 站点: http://cve.mitre.org/）

AppScan 咨询被指定了 CVE 引用（通常是基础结构测试）的漏洞，包括 CVE 引用。（以字母 CVE 开头的 CVE 引用是指已接受的漏洞，以 CAN 开头是指候选值。）



您可以执行以下操作:

- 通过在“测试策略管理器”中搜索 CVE 或 CAN 字符串来列出带有 CVE 引用的所有测试（请参阅第 83 页的『测试: 测试策略』）
- 通过在“测试策略管理器”中搜索其引用号来搜索特定 CVE（请参阅第 83 页的『测试: 测试策略』）
- 查看测试的咨询中测试结果的 CVE 引用
- 将 CVE 引用（作为咨询的一部分）包括在生成的报告中

“修订建议”选项卡

“修订建议”选项卡上的信息是指为保障 Web 应用程序不会出现所选的特定问题而应完成的具体任务。

修订建议选项卡会显示修订所选问题所对应的已知建议。这些解决方案可能是非常复杂的逐步指示信息。

修订建议分为以下几类:

- **一般** - 总是选取
- **.Net** - Microsoft© .NET
- **J2EE** - Sun© Java™ 2 Platform, Enterprise Edition

注: 您可以设置 Rational AppScan, 以隐藏不相关的修订建议。如需了解详细信息, 请参阅第 206 页的『“首选项”选项卡』。

请求/响应选项卡

请求/响应选项卡提供了关于测试及其特定变体的信息, 这些信息被发送到您的 Web 应用程序, 以发现应用程序的弱点。一个测试可能有多个变体。变体与 Rational AppScan 发送到 Web 应用程序服务器的原始测试请求稍有不同。（Rational AppScan 首先发送一个合法并遵循应用程序业务逻辑的请求。然后会再发送相同请求,

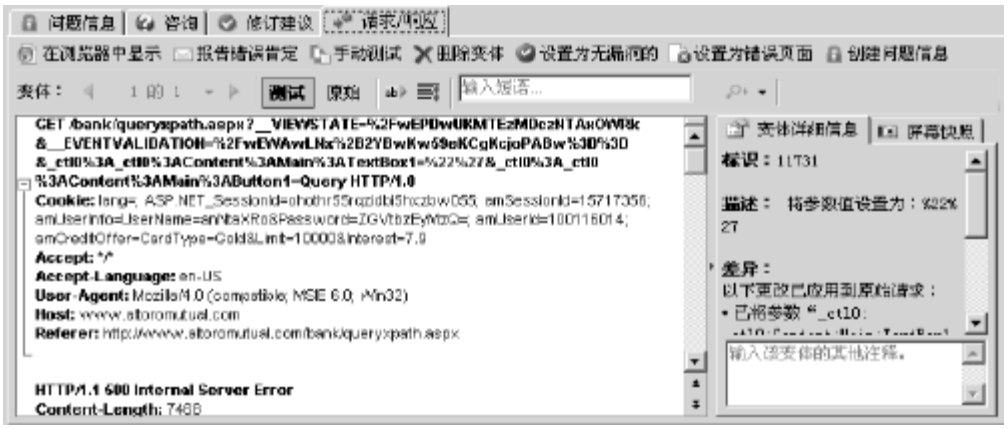
但是经过修改以发现应用程序如何处理非法或错误的请求。每个测试请求可能有多个变体；变体的数量需要足够覆盖扩展 Rational AppScan 数据库中的所有安全规则。）

例如，发送一个测试以确保您已对特定参数实施了用户输入规则。一个变体确保撇号是无效输入；另一个变体确保不允许使用引号。

变体本身以红色文本显示，验证（表示安全问题存在的响应部分）以黄色突出显示。

除了大量的解释信息，**请求/响应**选项卡还提供高级功能，以理解并使用扫描结果。

请求/响应选项卡在顶部有其自己的工具栏，在右侧还有两个选项卡（可通过切换选项卡右上角的**属性**按钮来显示/隐藏。）工具栏和选项卡如下所示，并在下表中进行概括。



工具	功能
在浏览器中显示	打开内置浏览器以显示当前页面。
报告错误肯定	用于将当前变体用电子邮件发送到 IBM Rational AppScan 技术支持，或您企业内部。（请参阅第 138 页的『报告错误肯定测试结果』。）
Manual Test	修改测试并将其保存为 Manual Test。（请参阅第 139 页的『Manual Test』。）
删除变体	从测试结果中永久删除所选变体（不可恢复）。这也可通过右键单击“结果”窗格中的变体来完成。
设置为无漏洞	将所选变体的定义更改为“无漏洞”。 由用户更改为无漏洞的肯定响应将从扫描结果中除去，将不再出现在报告中，但仍可通过“无漏洞的变体”列表查看（和恢复）。（请参阅第 142 页的『无漏洞变体列表』。）
设置为错误页面	将当前页面添加到错误页面列表中（“扫描配置”对话框 > “错误页面”），并更新结果以反映此响应是错误页面的事实。
创建问题信息	在当前问题上运行“结果复审”，并将所有可用新信息添加到“问题信息”选项卡。
变体 < >	表示当前测试的变体数。 单击 **<** 和 **>** 图标，以相应切换到上一个和下一个变体。
测试/原始	在“原始”和“测试”信息之间切换。
下一突出显示	（突出显示验证文本时可用）。将光标移动到下一突出显示的文本。
查找	输入文本以搜索特定字符串。（请参阅第 129 页的『搜索结果列表中的安全问题』。）

工具	功能
“变体详细信息”选项卡	可提供测试的**标识**、测试变体与原始请求之间的**差异**，以及 AppScan 认为该结果表示存在安全问题的**原因**。 可在选项卡底部的**注释**区域输入关于当前变体的注释，该注释将和“扫描”一同保存并包括在报告中。
屏幕快照选项卡	包含“照相机”按钮。 单击“照相机”按钮以打开浏览器，并保存当前页面的屏幕快照，该屏幕快照将和“扫描”一同保存并包括在报告中。（请参阅第 138 页的『变体的屏幕快照』。）

另请参阅:

『原始请求/响应』

『查看变体』

『变体详细信息』

第 138 页的『向变体添加注释』

第 138 页的『变体的屏幕快照』

第 138 页的『报告错误肯定测试结果』

原始请求/响应

要查看 Rational AppScan 在“探索”阶段发送到您的 Web 应用程序的原始 HTTP 请求，以及您的服务器发回的响应，请单击**原始**。

查看变体

关于此任务

每个测试可以拥有多个相关变体；每个变体会稍微更改请求，以针对众多的攻击技术来检查应用程序安全性。

1. 单击**测试**。
2. 单击左右方向按钮来查看变体请求。

   对于发送的每个变体测试，请求已修改的部分都已用红色突出显示。要获取变体的更多描述性解释，请参阅“**变体详细信息**”选项卡。

变体详细信息

详细信息窗格的**请求/响应**选项卡内的**变体详细信息**选项卡会描述变体并说明其用途。

- 变体标识，用于启用高效搜索和管理功能。
- 参数、cookie 或方法的值已更改为不同于原始请求所使用的值。
- 路径（文件夹/[文件夹]/URL）已更改。
- 参数已删除。
- HTTP 头已删除或添加。
- 已从主体中移除或向其添加了参数。

另请参阅: 第 138 页的『向变体添加注释』

向变体添加注释

您可在“变体详细信息”侧边选项卡底部的**注释**部分，输入对于当前变体的注释。这些注释和扫描一起保存，并包括在报告中。

变体的屏幕快照

关于此任务

可以为特定变体的某个状态截取 Web 应用程序屏幕快照。当生成报告时，您为变体截取的屏幕快照会包含在报告中，确切而言即报告中用于解释该特定变体的部分中。

1. 站点扫描。
2. 选择**问题**视图。
3. 在**结果列表**中选择项。
4. 在“**详细信息窗格 > 请求/响应**”选项卡中，打开**屏幕快照**侧边选项卡。（如果侧边选项卡不可见，请单击“请求/响应”选项卡右上方的**属性**按钮来显示侧边选项卡。）

5. 单击**单击以添加屏幕快照**  链接。

   此时会显示嵌入的浏览器，打开所选定变体的响应的 Web 页面。

6. 单击浏览器工具栏中的**捕获该页面**  图标，然后关闭浏览器。

   此时会将屏幕快照和变体保存在一起，并将其包含在报告中。

报告错误肯定测试结果

您可将测试信息用电子邮件发送到“AppScan 支持”，以便:

- 报告 Rational AppScan 分类为肯定，但您认为是否定的结果
- 询问“AppScan 支持”，为何将结果分类为肯定

您还可以使用方便压缩的功能，将结果用电子邮件发送给您组织内的开发者和审计员。

注: 缺省情况下，AppScan 将数据保存为加密格式，仅“支持”人员可访问。如果您在组织内部发送文件，那么您必须配置 AppScan 以将信息保存为 .zip 文件。在**“工具 | 选项 | 一般”选项卡**中，取消选中**加密附件**复选框。

报告单个错误肯定变体:

1. 在**结果列表**中选择项。
2. 在**"详细信息窗格 > 请求/响应"选项卡**中，浏览所选定问题的变体。
3. 当显示出想要发送的变体时，请单击"详细信息窗格"工具栏上的报告错误肯定。

   此时会打开"报告错误肯定"对话框。
4. 单击"保存文件"将文件保存到磁盘。

   根据您的加密设置（请参阅以下内容），文件会保存为加密格式或 .zip 格式。
5. 要将文件发送到 AppScan 技术支持，请单击**浏览至支持供应商**链接，然后登录并上载该文件。

报告错误肯定变体集:

关于此任务

使用"结果列表"中的右键单击菜单，可以报告某个附件中任何问题、URL 或子项的所有变体信息。

1. 在**结果列表**中，右键单击下列任一选项，然后选择 报告错误肯定:
   - 问题,
   - URL
   - 参数

   此时会打开"报告错误肯定"对话框。
2. 单击"保存文件"将文件保存到磁盘。

   根据您的加密设置（请参阅以下内容），文件会保存为加密格式或 .zip 格式。
3. 要将文件发送到 AppScan 技术支持，请单击**浏览至支持供应商**链接，然后登录并上载该文件。

错误肯定报告加密:

关于此任务

缺省情况下，**报告错误肯定**功能会以加密格式来保存数据，只有 AppScan 技术支持人员可以打开。

如果要在您自己的组织中发送附件，接收方将不能解密该附件，因此您需要禁用加密功能。

1. 打开**工具**菜单 > **选项** > **常规** > **报告错误肯定**.
2. 按照需要选中/取消选中**加密附件**复选框。

Manual Test

关于此任务

Manual Test 功能允许您发送自己的测试，并将它们保存为安全问题，并可包含在您的报告中。

只有在 Rational AppScan 已生成当前扫描的测试后，您才可以创建 Manual Test。仅为当前扫描保存 Manual Test。

注: 对于 AppScan Developer Edition，该功能不可用。

您可以让 Manual Test 基于现有测试，或您可以从头开始创建新的测试。

1. 要基于现有变体创建 Manual Test，请执行以下操作:
   - 在**结果列表**上，单击测试变体，或
   - 在**结果列表**上，单击测试，然后在**详细信息窗格**中使用工具栏浏览至必需的变体。

   另外，要从头开始创建新的变体，只需要打开 **Manual Test** 对话框（下一步骤），而不需要选择现有变体。
2. 打开 **Manual Test** 对话框:
   - 在**工具**菜单上，单击 **Manual Test**，或
   - 右键单击在**应用程序树**或**结果列表**中选定的变体，然后从弹出窗口中选择 **Manual Test**，或
   - 单击**详细信息窗格**中的 **Manual Test** 按钮，以获取选定的变体。

   此时会显示 **Manual Test** 对话框，将显示已选定的测试变体的属性。

3. 在**主机名/IP 地址**字段中，输入测试将要发送到的服务器。
4. 在**端口**字段中，输入 Rational AppScan 用来连接到服务器的端口。

   缺省端口是 **80**；如果选择 SSL，那么缺省端口为 **443**。
5. 如果需要，您可以编辑**请求**本身。
6. 在**选项**列表中，单击您想打开的选项。

选项	单击以
SSL	通过 SSL 发送请求。
发送请求前登录	先将登录请求发送到应用程序，然后再发送 Manual Test。

选项	单击以
自动内容长度	自动将请求中的**内容长度 HTTP** 头更新为与您所编辑的请求的请求内容相同的值。 如果选择该选项，那么用户将无法编辑内容长度的值。 如果请求头没有**内容长度**参数，那么该选项没有任何作用。

7. 单击**发送**。

   此时会发送请求，响应会显示在**响应**文本区域内（下部窗格）。
8. 要查看嵌入式浏览器中的响应，请单击**在浏览器中显示**。
9. 要将该 Manual Test 添加到当前扫描，请单击**保存**。

   此时会显示**选择问题类型**对话框，缺省情况下会选择**用户定义的测试**单选按钮。

10. 要将测试保存在现有测试类型下（而不是缺省的用户定义的测试类型），请选择第二个单选按钮，然后单击列表中的测试类型。
11. 单击**确定**。

    此时会关闭对话框。新的测试会添加到结果，当您继续或重新运行当前扫描时（**扫描 > 继续/重新扫描 > 测试**），将包含该测试。

无漏洞的变体

扫描期间，AppScan 会向它正在测试的站点发送上千的测试变体。很多对于这些变体的响应都指示不会引起任何类型的安全威胁，缺省情况下，AppScan 将废弃所有这些“无漏洞”结果。

- 如果需要，您可以配置 AppScan 以保存所有无漏洞的变体
- 您也可以将单个结果的状态更改为“无漏洞”

『保存所有的无漏洞的变体』

『将变体定义为无漏洞』

『无漏洞变体列表』

第 143 页的『删除变体』

保存所有的无漏洞的变体

关于此任务

如果想要复审“无漏洞”的测试变体，您可以配置 AppScan 来保存所有“无漏洞”变体。

注意:
保存无漏洞的测试变体信息可能会降低 AppScan 性能，并显著增加必需的磁盘空间。

在*扫描配置*对话框的*测试设置视图*中，选中**保存无漏洞的测试变体信息**复选框。

将变体定义为无漏洞

关于此任务

将测试变体定义为*无漏洞*时，该测试变体不会显示在扫描结果中或包含在报告中，但您可以（通过『无漏洞变体列表』）查看其详细信息，也可以根据需要在稍后将其恢复。

执行以下操作之一:

- 在“结果列表”上，右键单击并选择**设置为无漏洞**
- 在“结果列表”中选择变体，在“请求/响应”工具栏上，单击**设置为无漏洞**。

此时变体会从扫描结果显示中除去，且不会包含在报告中。

无漏洞变体列表

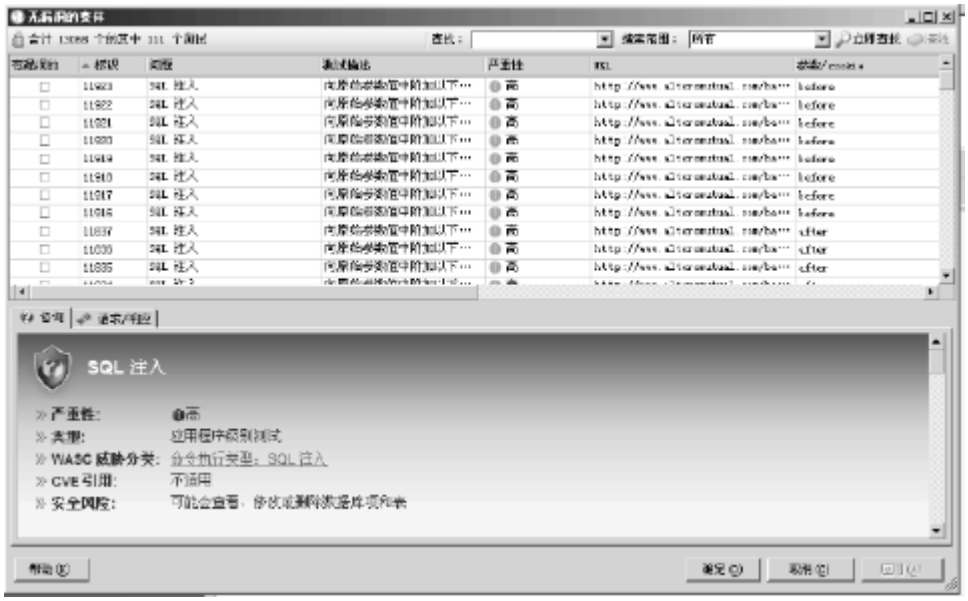
“无漏洞变体列表”可以让您查看已连同扫描结果保存起来的无漏洞变体的详细信息，如果需要，还可加以恢复。

有两种方法可以将变体添加到该列表:

- AppScan 已配置为保存无漏洞测试变体信息（请参阅第 89 页的『测试: 测试选项』）
- 您可手动将 AppScan 分类为“有漏洞”的结果更改为“无漏洞”（如前一部分所述）

查看无漏洞的变体

在**查看**菜单上，单击**无漏洞的变体**。



将无漏洞变体恢复为有漏洞的

1. 在无漏洞“变体”列表中选中一个或多个要恢复为有漏洞的变体的复选框。
2. 在对话框底部，单击**应用**。
3. 单击**确定**来确认。

删除变体

关于此任务

当删除变体（而非将其定义为无漏洞）时，这些变体会从扫描结果中全部删除，且稍后无法恢复。（要再次访问这些变体，您需要运行新的扫描。）

执行以下操作之一:

- 在“结果列表”中，右键单击并选择**删除**。
- 在“结果列表”中选择变体，在“请求/响应”工具栏上，单击**删除变体**。

此时变体会从扫描结果中除去，且不会包含在报告中。

第 7 章 结果: 修复任务

Rational AppScan 提供了查看和处理扫描结果的三种方法: “安全问题”、“修复任务”和“应用程序数据”。

本部分是讨论“修复任务”视图。

“修复任务”概述

“修复任务”视图提供为解决扫描中发现的问题而设计的解决方案。一个修复任务通常会处理多个安全问题。

在**视图选择器**上单击**修复**。

修复任务: 应用程序树

应用程序树显示已扫描的应用程序的文件夹和文件。树中每个节点都有一个计数器，显示节点中有多少项修复任务。每个节点的计数将会等于或少于**问题**视图的计数，这是由于一项修复任务可能会解决多个问题。

应用程序树显示以下级别的修复任务:

- **任务名称**
- **URL**
- **参数**或 **cookie**

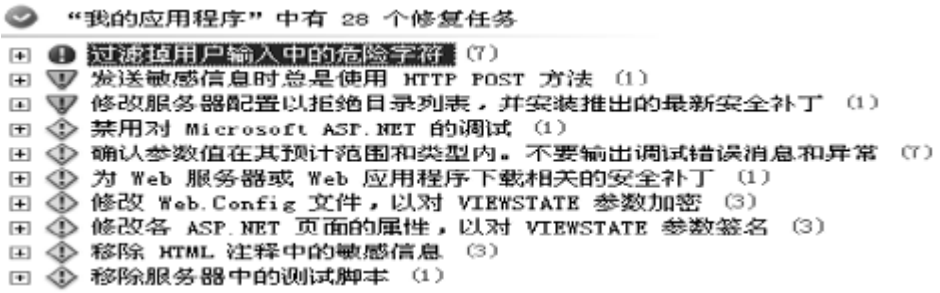
针对若干 URL 上找到的问题而设计的单个任务以及其下的 URL 将列出一次。

在**应用程序树**中选择一个节点，以过滤**结果列表**，这样将仅显示所选节点的结果。

修复任务: 结果列表

结果列表显示与**应用程序树**中所选节点相关的“修复”任务。如果您选择**我的应用程序**节点，那么**结果列表**将显示与您的应用程序相关的所有修复任务。

修复任务按处理问题可以执行的修复方法类型进行合并。每个修复项都有一个图标，指示要执行任务的优先级；还有一个计数器，指示此修复将影响多少文件、参数或 cookie。



每个任务可能托管 URL，URL 可能托管文件、参数和 cookie。 您可以更改修复排序的方式，也可以控制其优先级值。

搜索结果列表中的修复任务

关于此任务

您可以过滤**结果列表**以获取修复任务的类型，或可以搜索特定的修复。

1. 在**编辑**菜单上，单击**查找**（或按 **Ctrl + F**）。

   此时会在**结果列表**上的主窗口中显示**查找**栏。

2. 在**应用程序树**上，选择一个节点。
   - 如果选择**我的应用程序**节点，那么“查找”会搜索所有结果。
   - 如果选择树中的节点，那么“查找”会搜索选定的节点及其子节点。
3. 在**查找**栏的**查找**文本框中，输入字符串或部分字符串。
4. 在**搜索目标**列表中，选择想要搜索的部分修复:

搜索目标	要查找的字符串位置
修复	在“结果列表”中显示的修复名称
URL	与修复结果相关的 URL 的路径名
详细信息	修复任务详细信息
全部	全部上述选项

5. 单击**立即查找**或按 **Enter**。

   此时会在**结果列表**中显示结果，将覆盖先前显示的列表。如果输入另一个**查找**字符串，并再次单击**立即查找**，那么会在**应用程序数**中选定的节点上进行搜索，而不是在先前搜索的显示结果上进行搜索。

表 11. 查找示例

要查找	查找...	搜索...
与虚拟目录有关的修复任务:	“virtual direc”	修复
登录页面的修复任务:	“login”	URL

为修复任务排序

关于此任务

您可以在**结果列表**中重新安排修复任务。缺省情况下，会根据优先级来为任务排序。

1. 单击**安排方式**列标题。

   此时会显示菜单。

2. 单击菜单上的命令来为补救排序:
   - **优先级** – 根据优先级顺序列出任务名称: 首先是“高优先级”，往下一直到“低”.
   - **计数** – 受影响的 URL、参数或 cookie 的数量。首先列出解决最多问题的任务。
   - **名称** – 根据任务名称的字母顺序来排序。

   此时会在**结果列表**中为修复任务重新排序。

   要颠倒排序顺序（升序或降序），请单击**结果列表**的第二列。再次单击第二列可还原到先前的顺序。

控制优先级

关于此任务

修复任务图标会表明它们的优先级。下表会说明这些图标。

图标	表示
	高优先级任务
	中优先级任务
	低优先级任务

基于问题严重性来分配修复任务的优先级。如果严重性为“高”，那么优先级便为“高”；“中等”严重性便为“中”优先级；“低”和“参考信息”严重性便为“低”优先级。

可以查看缺省优先级设置作为在起始点。您可以更改已分配到修复任务的优先级。新的优先级设置会影响具有相同“任务”名称的所有补救。

在**结果列表**上，右键单击修复任务，然后选择**优先级 > 高/中/低**。
此时修复任务图标会更改，以匹配新的优先级。

从“结果列表”中删除“修复任务”

关于此任务

可以从**结果列表**删除任务，该操作将删除已选定的节点和包含在该节点中的所有对象。

1. 在**结果列表**上，右键单击节点。
2. 在出现的菜单中，单击**删除**。

   此时会显示消息，要求您确认删除并提醒您测试数据将永久删除。

3. 单击**是**。

此时会删除修复任务，但这不会影响问题；仍然可从“问题”视图中使用问题。

修复任务: 详细信息窗格

“修复”视图的**详细信息窗格**包含一个选项卡。它会显示在**结果列表**中当前所选的修复任务。

详细信息窗格中的信息包括:

- **任务名称**
- **问题** – 此任务所处理的扫描结果的列表
- **详细信息** – 一个或多个可能的解决方案

第 8 章 结果: 应用程序数据

Rational AppScan 提供了查看和处理扫描结果的三种方法: “安全问题”、“修复任务”和“应用程序数据”。

本部分描述“应用程序数据视图”。

应用程序数据概述

在“探索”阶段结束时，“应用程序数据视图”将显示结果。

如果您仅运行“探索”阶段，甚至只执行其中的一部分，您便可以查看“探索”结果。全面扫描（“探索”和“测试”）后，“应用程序数据”视图的结果将会更新。

这是从“探索”而非“测试”阶段所获结果的唯一视图。

在**视图选择器**上单击**应用程序数据**。

请注意，本视图仅显示从“探索”阶段所获结果，与“测试”阶段无关。

应用程序数据: 应用程序树

应用程序树显示已探索的文件夹、URL 和文件。

“探索”阶段结束后，您可以复审**应用程序树**，以简单地查看应用程序，并确保已探索所有内容。

您在**应用程序树**操作中选择的节点可作为**结果列表**中所列数据的过滤器。如果没有特定类型数据的结果，那么请选择树中的更高节点。如果您选择了**我的应用程序**，那么将列出应用程序中所能找到的特定类型的所有数据。

应用程序数据: 结果列表和详细信息窗格

结果列表会列出在“探索”阶段已发现的 URL、参数和脚本。表 12 列出了数据的类别。

表 12. 探索结果数据类型

数据类型	描述
『已访问的 URL』	Rational AppScan 已访问的 URL。
第 151 页的『交互式 URL』	需要 Rational AppScan 无法自动提供的用户输入的 URL。要了解如何定义表单参数输入，请参阅第 50 页的『探索: 登录管理』。
第 152 页的『已过滤的 URL』	由于缺省 Rational AppScan 设置或者由于所定义的探索过滤器，因此未探索的 URL（请参阅第 58 页的『探索: 排除路径和文件』）。
第 152 页的『中断链接』	未响应请求的链接。
第 153 页的『脚本参数』	Rational AppScan 已发现的脚本及其关联参数。
第 153 页的『注释』	可供用户访问的 Web 页面上的注释。
第 153 页的『JavaScript』	Rational AppScan 已发现的 JavaScript。
第 153 页的『cookie』	Rational AppScan 已发现的 cookie。

在**显示**列表中，会给出数据类型，并且各数据类型将显示在**应用程序树**中所选的节点中的项数。如果在树中选择了**我的应用程序**，那么**显示**列表计数是针对整个应用程序。

在**显示**列表中选择一种数据类型。在“探索”阶段期间所发现的项列表会在**结果列表**中显示。**结果列表**的各列以及列中所提供的信息会针对各数据类型进行更改。

例如，如果选择**中断链接**，相应的列为: **错误原因**（链接不成功而收到的响应）和 **URL**（链接所在位置）。如果选择 **Cookie**，相应的列为: **名称**、**值**和**响应 URL**。

选择**结果列表**中的一项，以在**详细信息窗格**中查看更多信息。所显示的**详细信息窗格**的选项卡和其中所显示的信息类型取决于所选的项的类型。针对各数据类型的结果列表和详细信息窗格会在下列章节主题中进行描述。

另请参阅: 第 154 页的『搜索“结果列表”中的“应用程序数据”』

已访问的 URL

已访问的 URL 是指 AppScan 收到有效响应所对应的请求。基于这些响应，AppScan 会生成用于暴露站点漏洞的测试，在“测试”阶段期间将发送这些测试。

如果请求或响应主体包含 XML（包括 XHTML 或 SOAP），那么“已访问的 URL”图标会替换为 XML 图标:

结果列表中的已访问 URL

结果列表会显示 Rational AppScan 已访问的各页面的 URL。

- 您可以通过右键单击一个**已访问的 URL** 项并单击**在浏览器中显示**，或者通过选择此 URL 并单击**详细信息窗格**中的**在浏览器中显示**链接，查看已访问的 URL。
- 您可以通过右键单击**已访问的 URL** 项并单击 **Manual Test**，或者通过选择 URL 并单击**详细信息窗格**中的 **Manual Test** 链接，创建 Manual Test。（请参阅第 139 页的『Manual Test』以了解更多信息；但是请注意，此功能不适用于 AppScan Developer Edition。）

详细信息窗格中的已访问 URL

详细信息窗格包含指向**在浏览器中显示**和 **Manual Test** 的链接，这两个链接按照与**结果列表**中右键单击命令相同的方式进行操作。

系统会显示**请求/响应**选项卡，其中又会显示在**结果列表**中所选的 URL 的请求和立即响应。

交互式 URL

交互式的 URL 是尚未发送的请求，因为它们需要从用户输入，Rational AppScan 不会提供该输入。您可配置 Rational AppScan 以提供输入；请参阅第 71 页的『探索: 自动表单填充』。如果缺少某些应用程序参数，或如果选择不使用自动表单填写程序，那么 Rational AppScan 将会提供交互式 URL 列表供您复审。

结果列表中的交互式 URL

您可以检查交互式的 URL 列表。如果您想要扫描这些页面，那么要提供“手动探索”中要求的用户信息（请参阅『手动探索交互式 URL』）。

建议您仔细检查交互式 URL 的列表，填写所需数据，然后发送这些请求。 AppScan 之后将在“测试”阶段包括这些 URL。

如果 Rational AppScan 能够发送这些请求，那么这些请求将打开站点的一个全新部分，之前 AppScan 无法访问该部分。因此，您访问交互式 URL 后，应该重新探索您的应用程序（**扫描**菜单 > **重新扫描** > **探索**）。

详细信息窗格中的交互式 URL

详细信息窗格提供一个链接，以手动探索 URL: **在浏览器中显示**。此操作等同于在**结果列表**中右键单击 > **在浏览器中显示**。

请求/响应选项卡显示发送到 URL 的请求。

『手动探索交互式 URL』

手动探索交互式 URL

关于此任务

交互式 URL 是尚未发送的请求，因为它们需要用户提供输入，而 Rational AppScan 不会提供该输入。如果缺少某些应用程序参数，或如果选择不使自动表单填充器，那么在扫描结束时，Rational AppScan 将有交互式 URL 列表。

1. 在**结果列表**的**显示**列表上，单击**交互式 URL**。

   此时在**结果列表**中会显示带有交互式输入的 URL 列表。

   单个 URL 可能不止显示一次，每个实例来自不同的表单。
2. 右键单击列表中的 URL，然后单击**手动探索该 URL**。

   此时会显示带有**手动探索**按钮的浏览器，打开该 URL。完成手动探索，请参阅第 112 页的『记录手动探索』。

   完成手动探索后，Rational AppScan 会分析新的“探索”。

   如果找到新的 URL，此时会显示消息，会建议您继续“探索”（**扫描**菜单 > **继续扫描** > **探索**）。

- 如果未找到新的 URL，但已创建新测试，此时会显示消息，会建议您继续“测试”阶段（**扫描 > 继续扫描 > 测试**）。
- 如果找到新的 URL 且已创建新测试，此时会显示消息，会建议您继续“探索”和“测试”（**扫描 > 继续扫描 > 全面测试**）。

已过滤的 URL

已过滤的 URL 是 Rational AppScan 未访问的页面，因为它们被过滤出“探索”：或者被标准过滤器过滤，或者被您配置扫描时所定义的过滤器过滤（请参阅第 58 页的『探索：排除路径和文件』）。

结果列表中已过滤的 URL

结果列表显示未探索的 URL 并提供“过滤器类型”（此页面被滤除的原因）。

您可以通过右键单击“已过滤的 URL”，然后单击**在浏览器中显示**来查看已过滤的 URL。

详细信息窗格中已过滤的 URL

详细信息窗格提供一个链接，以在浏览器中显示 URL：**在浏览器中显示**。 此操作等同于在**结果列表**中右键单击 > **在浏览器中显示**。

请求/响应选项卡显示若未被滤除便可能发送到 URL 的请求。

中断链接

*中断链接*是指向其发送请求而并无有效响应返回的链接。这通常会在站点宕机或存在其他通信问题时发生；或者请求返回错误响应状态而非请求的页面时发生。

结果列表中的中断链接

您可以重新将请求发送到中断链接，而不需重复整个扫描。“探索”阶段完成后，如果应用程序已被更改或修订，那么请执行以下过程，以重新探索中断链接。

注：如果您的应用程序需要登录，建议您在进行以下过程前手动登录 Rational AppScan （请参阅第 50 页的『探索：登录管理』）；否则将在典型使用模式之外探索中断链接。

您可以通过从“结果”窗格的**显示**下拉列表中选择**“中断链接”**来查看所有中断链接。在最右边将出现新的链接：**“重试所有中断链接”**。

如果您单击**“重试所有中断链接”**，那么这些链接将从“中断链接”列表中除去，并添加到“未访问的链接”列表。Rational AppScan 然后将继续“探索”阶段，可能时将访问“未访问的链接”列表中的链接。探索完所有“未访问的链接”后，“探索”阶段将结束。

注：如果扫描期间，Rational AppScan 和服务器之间存在通信问题，那么某些链接将会标记为“中断链接”。Rational AppScan 存在通信问题时，它将在 90 秒内，持续尝试重新发送其请求。如果在此时间内仍未建立连接，那么扫描将停止。主窗口上的“**扫描通知**面板”将通知您有关问题并显示超时倒计时。如果您看到了此通知，那么您应当在尝试对链接进行故障诊断之前修订 Rational AppScan 和应用程序之间的连接。

详细信息窗格中的中断链接

详细信息窗格可使您通过单击**“在浏览器中显示”**按钮来查看特定中断链接的响应页面。

脚本参数

*脚本参数*是包括一个或多个参数的请求。

结果列表显示“探索”阶段找到的所有参数。此列表中的 URL 最有可能受到恶意攻击。此列表在评估扫描是否生成有用测试请求集时很关键。

对于“脚本参数”列表中的每个参数，Rational AppScan 将显示参数的名称、类型、值和 URL（“结果”窗格）和值（“详细信息”窗格）。如果一个参数名称出现在不同 URL 上，或者它在相同 URL 上有不同值，那么可能多次列出。

注释

*注释*是 Rational AppScan 在“探索”阶段找到的 HTML 注释。 HTML 页面中隐藏的注释可能包含对黑客有用的信息：有时，开发者有意或偶然地将注释留在最后页面中，供自己或其他开发者使用。黑客能够从这些注释中获得很有用的内部信息，如调试密码。

结果列表中的注释

注释列表显示注释的第一行和它所在的第一个 URL。如果 Rational AppScan 多次找到相同注释，那么仅列出第一个实例。

详细信息窗格中的注释

详细信息窗格显示了**结果列表**中所选项的整个注释。在此处复审注释，以确定应该从最终应用程序中除去的注释。

JavaScript

JavaScript 列出了 Rational AppScan 在“探索”阶段找到的 JavaScript 代码。

“结果列表”中的 JavaScript

列表显示了 JavaScript 的第一行及从中找到它的第一个 URL。如果在多个 URL 上找到相同脚本，那么将只列出第一个实例。

“详细信息窗格”中的 JavaScript

详细信息窗格显示了**结果列表**中所选项的整个脚本。请复审此处的代码，以找出应从最终应用程序中除去的注释。

cookie

cookie 列出 Rational AppScan 在扫描期间找到的所有 cookie，无论是由响应设置，由 Javascript 生成，还是扫描前已存在于主机上。

结果列表中的 cookie

“结果列表”显示在“探索”阶段找到的所有 cookie。列表中的每个 cookie 都具有一个 cookie 名称、值和“响应 URL”。所列出的 URL 是可设置 cookie 的响应的 URL（即使存在其他包括“设置 cookie”命令的 URL）。如

果 cookie 不是由响应设置（例如，由 Javascript 生成，或已存在于主机上），那么在“响应 URL”字段将显示“不适用”。

详细信息窗格中的 cookie

详细信息窗格显示:

路径 在您的应用程序中，此 cookie 所发送到的特定文件夹或子文件夹。路径属性用于指定域中能使 cookie 有效的 URL 子集。如果 cookie 已经通过了域匹配（下一项），那么 URL 的路径名组件将与路径属性比较，如果仍匹配，那么认为此 cookie 有效并与 URL 请求一同发送。

域 此 cookie 将发送到的域或子域。（如果未设置域，那么 cookie 将发送到发出“设置 cookie”命令的那个域以及所有子域。

到期 cookie 到期并从用户机器中除去的日期和时间。

安全 是（安全的）或否。如果 cookie 标记为**安全**，只有在带有主机的通信信道安全的情况下才可以对其进行传输（当前仅用于 HTTPS 服务器）。如果未指定**安全**，那么 cookie 通过所有信道发送都视为安全的。

请求 URL
AppScan 所发送的带有 cookie 的第一个请求。

搜索“结果列表”中的“应用程序数据”

关于此任务

您可以过滤**结果列表**以获取特定数据。

1. 在**编辑**菜单上，单击**查找**（或按 **Ctrl + F**）。

   此时会在**结果列表**上的主窗口中显示**查找**栏。

2. 在**应用程序树**上，选择一个节点。
   - 如果选择**我的应用程序**节点，那么“查找”会搜索所有结果。
   - 如果选择树中的节点，那么“查找”会搜索选定的节点及其子节点。
3. 在**查找**栏的**查找**文本框中，输入字符串或部分字符串。
4. 在**显示**列表中，单击数据类型。
5. 单击**立即查找**或按 **Enter**。

   此时会在**结果列表**中显示结果，将覆盖先前显示的列表，计数器会更新以显示每个类别中新的项数。

   如果输入另一个**查找**字符串，并再次单击**立即查找**，那么会在**应用程序树**中选定的节点上进行新的搜索，而不是在先前搜索的显示结果上进行搜索。

   注: 要还原到完整的、未过滤的“结果列表”，请单击**清除**。

第 9 章 报告

如何从扫描结果生成专业报告。

报告概述

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

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

图标	名称	简短描述
	**安全报告**	扫描期间找到的安全问题的报告。安全信息可能非常广泛，并可根据您的需要进行过滤。包括六个标准模板，但根据需要，每个模板都可轻易调整，以包括或排除信息类别。请参阅第 156 页的『安全报告』
	**行业标准报告**	应用程序针对所选行业委员会或您自己的定制标准核对表的一致性（或非一致性）报告。请参阅第 158 页的『行业标准报告』
	**法规相符性报告**	应用程序针对规范或法律标准的大量选项或您自己的定制“法规相符性”模板的一致性（或非一致性）报告。请参阅第 159 页的『合规一致性报告』
	**增量分析报告**	“增量分析”报告比较了两组扫描结果，并显示了发现的 URL 和/或安全问题中的差异。请参阅第 161 页的『增量分析报告』
	**基于模板的报告**	包含用户定义的数据和用户定义的文档格式化的定制报告（格式为 Microsoft Word .doc）。请参阅第 168 页的『基于模板的报告』

注: “行业标准”和“法规相符性”报告在 AppScan Developer Edition 中不可用。

安全报告

关于此任务

“安全报告”会提供在扫描期间发现的关于安全问题的信息。

“安全”报告有各种不同的模板。每个模板都是一组与组织中不同受众相关的内容主题。主题包含来自每个视图（安全问题、修复任务、应用程序数据）的扫描结果，其格式便于打印，可读性高，有助于快速理解这些结果所代表的涵义，它们相关的原因及其修订方法。

选定任何模板作为基础后，您可以通过选择/取消选择要包含的信息的字段来定制个别报告的结构。

1. 在**工具**菜单上，单击**报告**，然后选择**安全报告**。
2. 选择相关**模板**:
   - **管理综合报告**: 高级别的综合报告，突出显示在 Web 应用程序中找到的安全风险以及扫描结果统计信息，其格式为表和图表。
   - **详细报告**: 详细报告包含“管理综合报告”、“安全问题”（受影响的 URL、威胁类、严重性、发送后导致肯定测试的变体请求）、注释、咨询、修订建议、修复、应用程序数据和 URL。
   - **修复任务**: 修复任务: 为处理扫描中所发现的问题而设计的操作。
   - **开发者**: 安全问题、变体、咨询和修订建议，不需要“管理综合报告”或“修复任务”部分。
   - **QA**: 安全问题、咨询和修订建议、应用程序数据，不需要详细变体信息、“管理综合报告”或“修复任务”部分。
   - **站点目录**: 仅应用程序数据。

   注: 该对话框的主窗格会显示哪些部分将包含到您所选的报告中。您可以按照需要选中或取消选中任何复选框，从而进一步定制报告。
3. 从**测试类型**列表，选择想要将其测试结果包含在报告中的测试类型:
   - **全部**: “应用程序”测试和“基础结构”测试两者所发现的问题。
   - **应用程序**: 测试所发现的针对 Web 应用程序的特定问题，这些问题是由配置不当或为有效使用而对安全规则进行的实施不充分所致。
   - **基础结构**: 测试发现的问题，这些问题由第三方商业产品或因特网系统中的已知安全弱点所预决定。

   注: 当配置扫描的“测试策略”时，可以排除“应用程序”或“基础结构”测试（请参阅第 84 页的『编辑“测试策略”』）。如果正在生成该报告的扫描已排除这些类型中的一种，那么请确保您会选择已包含的测试类型；否则报告将为空。

   例如，如果“测试策略”已排除“应用程序”测试，且您选择**应用程序**作为**测试类型**，那么报告中将没有结果。
4. 从**最低严重性**列表中，选择要包含在报告中的问题最低严重性级别。

   例如，如果想要报告仅包含“高”严重性问题，请选择**高**；如果想要报告包含所有问题，请选择**参考信息**（最低严重性级别）。
5. 您可以通过限制每个问题所列出的变体数量来缩短报告的长度。选中**限制**复选框，然后在**变体最大数量**复选框中输入每个问题所允许的变体的最大数量。

6. 要让报告显得更为清晰，您可能要选中**将页面中断添加到每个“问题 URL”后**复选框。
7. 在**报告内容**窗格中，选中想包含在报告中的主题的复选框，并清除不想包含在报告中的主题的复选框。

   完整的“详细”报告可能长达数百页，因此请确保仅包含与受众相关的部分（请参阅『“安全报告”内容』）。
8. 如果您想控制报告的外观，请打开**布局**选项卡（请参阅第 162 页的『配置报告布局』）。
9. 单击**预览**，以在 Rational AppScan 中生成并查看报告；或单击**保存报告**，以生成报告，并将其保存到文件。

“安全报告”内容

下表概括了各种“安全报告”的标准内容。任何情况下，都可根据需要，通过选中/清除“报告内容”窗格中的复选框来更改实际内容。

报告部分	描述	
管理综合报告	扫描结果和应用程序 URL 的统计信息（请参阅下表）。	
安全性问题	在您的应用程序中发现的问题:	
	变体: 发现问题的精确测试。选择要添加的变体信息:	
		请求/响应 HTTP 测试请求
		用户注释在“详细信息窗格”中输入的注释
		显示响应的认证用粗体突出显示响应的一部分，此部分导致 AppScan 将此响应认作是“安全问题”。
		屏幕快照 从“详细信息窗格”获取的屏幕快照；请参阅第 138 页的『变体的屏幕快照』
	咨询和修订建议: 说明风险和解决方案的技术信息 选择 **.NET / J2EE / PHP** 以包含在特定于这些环境的报告修订建议中（若这些环境与您的应用程序相关）。	
修复任务	修复建议和说明	
应用程序数据	Rational AppScan 在 Web 应用程序中发现的数据的列表: 应用程序 URL、脚本参数、中断链接、注释、JavaScript、Cookie	

“管理综合报告”部分

部分标题	表示的信息
已扫描的主机	已扫描的主机列表。
测试策略	应用于扫描的“测试策略”名称
安全风险	突出显示易使应用程序受到攻击的“安全风险”。
有漏洞的 URL	发现有漏洞的 URL 的百分比。
已扫描的 URL	已扫描的 URL 的数量，和已发现但未被扫描的 URL 的数量。
安全性问题可能原因	有关已发现的最常见安全问题的可能原因的解释。
安全问题最多的 URL	已扫描且问题最多的 URL 的列表。
每台主机的安全性问题	对于每台已扫描的主机，其问题统计数据都按照严重性级别显示。
每个威胁类的安全问题分布	按照 WASC 威胁类进行的的问题划分: 强制浏览、第三方错误配置，等等。
安全问题原因分布	按照“应用程序相关”和“基础结构相关”原因对问题进行划分。

行业标准报告

关于此任务

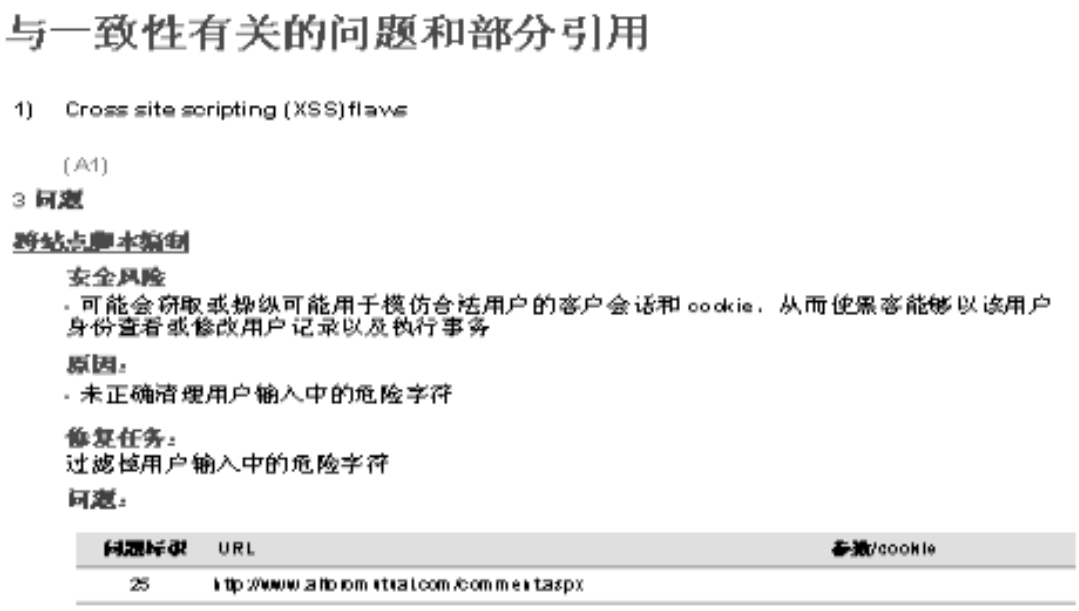
”行业标准“报告让您知道您的应用程序是否与所选定的行业委员会标准一致。当为不同行业创建新标准时，IBM 会更新可从中选择模板的模板列表，您的 Rational AppScan 会定期自动更新。

如果在列表中找不到您需要的行业标准，您可以创建自己的“行业标准”报告模板（请参阅第 164 页的『创建用户定义的报告模板』）。

“行业标准”报告包含以下部分:

部分标题	表示的信息
描述	标准的说明。
一致性摘要	非一致性问题的列表和计数。 注意: 单个问题可能表示不止一个部分的非一致性，因此对于所有部分来说，平均每个部分的问题数量可能会多于唯一问题的数量。
唯一一致性问题	非一致性 URL、相关参数或 cookie 和测试名称的列表。 每个问题仅显示一次。
按照部分分类一致性问题	详细说明您的应用程序为何不一致，并提供修复以处理问题。

下图会显示部分“行业标准报告”的样本。


与一致性有关的问题和部分引用

1) Cross site scripting (XSS) flaws

(A1)

3 问题

跨站点脚本编制

安全风险

- 可能会窃取或操纵可能用于模仿合法用户的客户会话和 cookie，从而使黑客能够以该用户身份查看或修改用户记录以及执行事务

原因：

- 未正确清理用户输入中的危险字符

修复任务：

过滤掉用户输入中的危险字符

问题：

问题标识	URL	参数/cookie
25	http://www.altoromutual.com/comment.aspx	

1. 在**工具**菜单上，单击**报告**，然后选择**行业标准**。
2. 执行以下操作之一:
   - 从列出的**行业标准报告模板**中选择其中之一。
   - 选择**用户定义的**单选按钮，并输入或浏览至定制的“行业标准”模板文件（***.asreg**）。如需了解详细信息，请参阅第 164 页的『创建用户定义的报告模板』。
3. 如果您想控制报告的外观，请打开**布局**选项卡（请参阅第 162 页的『配置报告布局』）。
4. 单击**预览**，以在 Rational AppScan 中生成并查看报告；或单击**保存报告**，以生成报告，并将其保存到文件。

合规一致性报告

关于此任务

“合规一致性”报告会让您知道您的应用程序是否与规定或法律标准一致。此处有一个来自不同国家或地区的模板的长列表，可以从列表中选择模板，每个模板会提供不同规定的一致性报告。

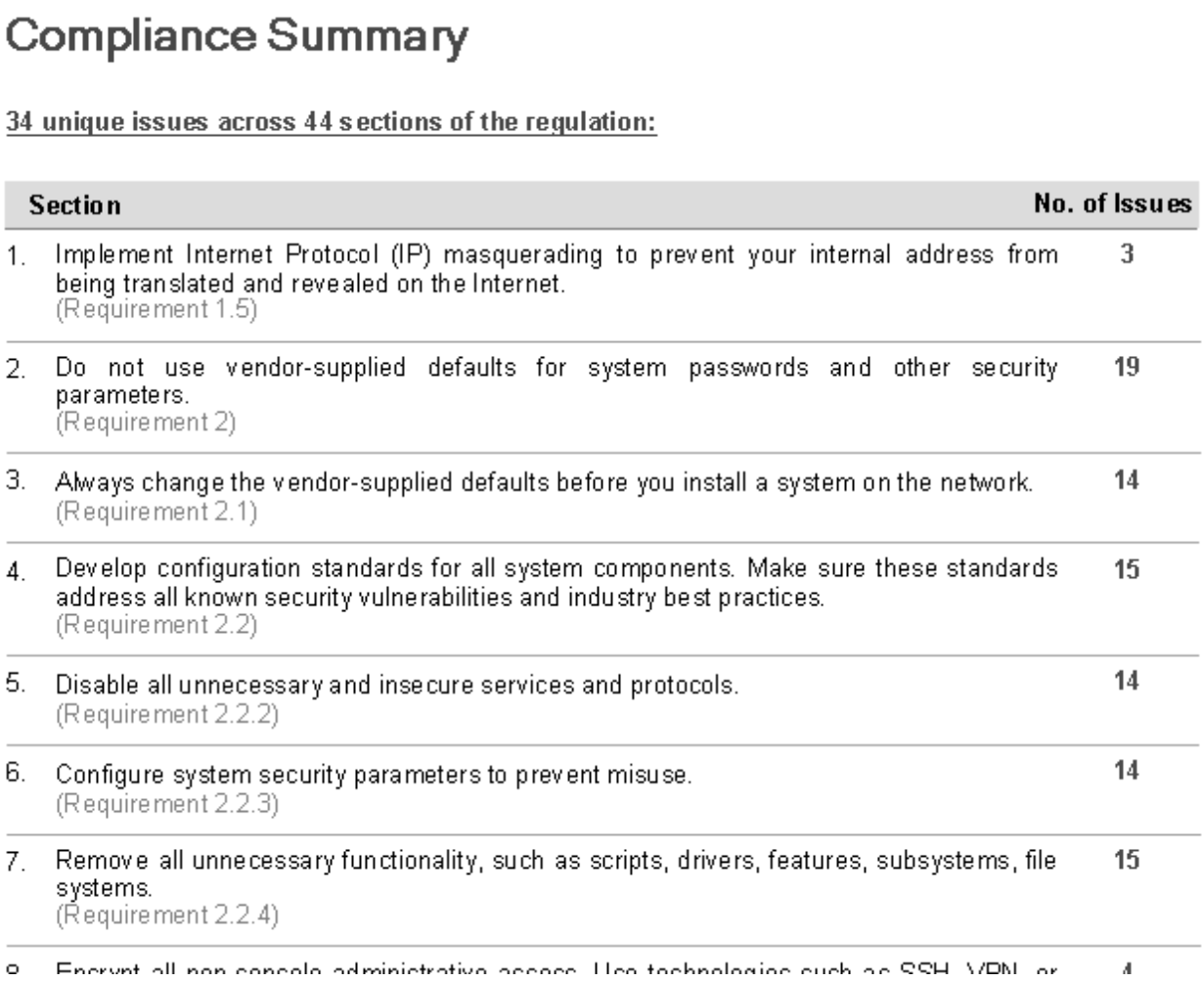
如果在列表中找不到您需要的规定，您可以创建自己的“合规一致性报告”模板（如需了解详细信息，请参阅第 164 页的『创建用户定义的报告模板』）。

“合规一致性”报告包含以下部分:

部分标题	表示的信息
描述	规定的说明。

部分标题	表示的信息
一致性摘要	非一致性问题的列表和计数。 注意：单个问题可能表示不止一个部分的非一致性，因此对于所有部分来说，平均每个部分的问题数量可能会多于唯一问题的数量。
唯一一致性问题	非一致性 URL、相关参数或 cookie 和测试名称的列表。 每个问题仅显示一次。
按照部分分类一致性问题	详细说明您的应用程序为何不一致，并提供修复以处理问题。

下图显示“合规一致性报告”中的样本。



Compliance Summary

34 unique issues across 44 sections of the regulation:

Section	No. of Issues
1. Implement Internet Protocol (IP) masquerading to prevent your internal address from being translated and revealed on the Internet. (Requirement 1.5)	3
2. Do not use vendor-supplied defaults for system passwords and other security parameters. (Requirement 2)	19
3. Always change the vendor-supplied defaults before you install a system on the network. (Requirement 2.1)	14
4. Develop configuration standards for all system components. Make sure these standards address all known security vulnerabilities and industry best practices. (Requirement 2.2)	15
5. Disable all unnecessary and insecure services and protocols. (Requirement 2.2.2)	14
6. Configure system security parameters to prevent misuse. (Requirement 2.2.3)	14
7. Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems. (Requirement 2.2.4)	15
8. Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or	4

1. 在**工具**菜单上，单击**报告**，然后选择**合规一致性**。
2. 执行以下操作之一：
   - 从列出的**合规一致性报告模板**中选择其中之一：
   - 选择**用户定义的**单选按钮，并输入或浏览至定制的“合规一致性”模板文件（***.asreg**）。如需了解详细信息，请参阅第 164 页的『创建用户定义的报告模板』。
3. 如果您想控制报告的外观，请打开**布局**选项卡（请参阅第 162 页的『配置报告布局』）。

4. 单击**预览**，以在 Rational AppScan 中生成并查看报告；或单击**保存报告**，以生成报告，并将其保存到文件。

增量分析报告

关于此任务

“增量分析”报告会比较两组扫描结果，并会显示在这两组结果中发现的 URL 和/或安全问题差异。选择“基本”和“目标”扫描，AppScan 会比较两组的结果，以允许您复审在两个扫描时间内，安全状态是如何改进或恶化的。

您可以比较当前装入的扫描和已保存的扫描，也可以比较两个已保存的扫描。

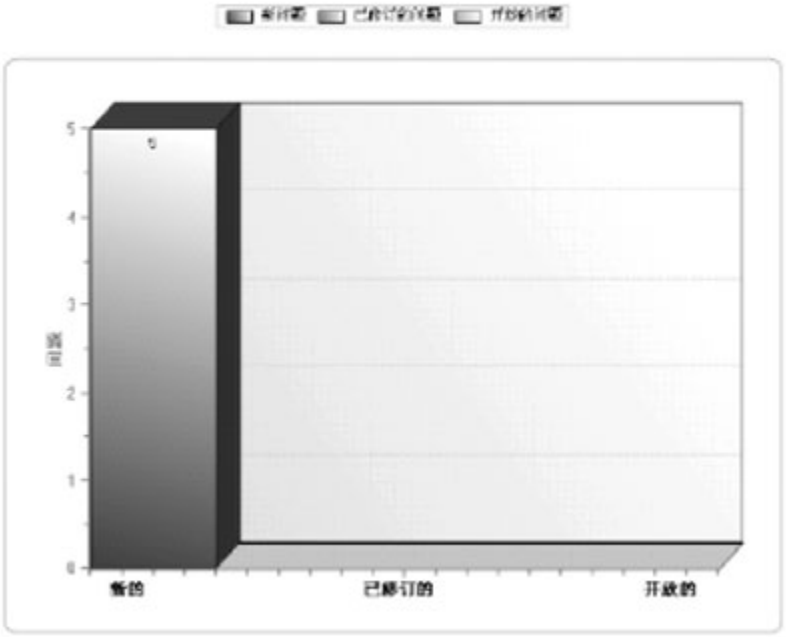
比较扫描时，通常会将较早的扫描作为“基本”扫描。然后，“增量分析”报告将指出“目标”扫描结果与“基本”扫描结果之间存在的差异。

“增量分析”报告包含以下部分:

部分标题	表示的信息
一般信息	列出“基本”扫描和“目标”扫描的名称和位置
描述	包含在扫描中的信息的描述
问题/主机	表 – 显示每次扫描中所找到的严重性“高”、“中”、“低”和“参考信息”所对应的问题数以及“全部”问题数。
应用程序 URL	（如果包含）条形图 – 显示新的/已除去的/其余的 URL 的数量，后面跟着每个类型的完整列表。
安全问题	（如果包含）“新的/固定的/其余的安全问题”的条形图，后面跟着显示两个扫描中的“严重性”分布的条形图（高/中/低/参考信息），后面跟着所有“新的/固定的/其余的”问题的完整列表。

下图会显示“增量分析报告”的样本。

安全性问题



1. 在**工具**菜单上，单击**报告**，然后选择**增量分析**。
2. 选择“基本”扫描（通常是比较的两个扫描中较早的一个）。在“基本扫描”区域，请执行以下操作:
   - 单击**当前扫描**单选按钮
   - 单击**已保存的扫描**单选按钮，然后浏览至已保存的扫描文件的位置。
3. 选择“目标”扫描（通常是比较的两个扫描中较晚的一个）。在“目标扫描”区域，请执行以下操作:
   - 单击**当前扫描**单选按钮
   - 单击**已保存的扫描**单选按钮，然后浏览至已保存的扫描文件的位置。
4. 在“报告内容”区域，请选中想要报告比较的一个或两个信息类型复选框:
   - **应用程序 URL**，和/或
   - **安全问题**
5. 如果您想控制报告的外观，请打开**布局**选项卡（请参阅『配置报告布局』）。
6. 单击**预览**，以在 Rational AppScan 中生成并查看报告；或单击**保存报告**，以生成报告，并将其保存到文件。

配置报告布局

关于此任务

“创建报告”对话框的布局选项卡允许您定制报告的外观。（该功能为可选，因为使用缺省布局即可生成报告。）

1. 在**创建报告**对话框中，单击**布局**选项卡。
2. 选择想要的布局选项，并输入合适的值:

布局选项	描述
包括封面	将封面添加到报告中。如果选择该选项，会启用封面选项。

布局选项	描述
公司徽标	将公司徽标放在封面的左上方。（单击“公司徽标”区域中的  图标，然后浏览至您计数机上的徽标文件，）
其他徽标	将其他徽标放在封面的右上方。（单击“公司徽标”区域中的  图标，然后浏览至您计数机上的徽标文件，）
报告类型	将“报告类型”（不可编辑的文本）放在封面的下半部分。
报告标题	将缺省标题或您所输入的标题作为主标题放在封面的上半部分。
描述	将缺省描述或您所输入的描述作为描述放在封面上。
报告日期	将日期放在封面上。
页眉/页脚	为每个页面添加页眉和/或页脚。输入您想要显示的文本，不超过 50 个字符。
另存为“缺省布局”	关闭对话框后，保持该对话框中的选择项。

查看和保存报告

在生成报告时，您可以在 Rational AppScan 内选择立即对其进行查看，或者将其保存为文件。

『查看“报告查看器”中的报告』

『保存报告』

查看“报告查看器”中的报告

关于此任务

“报告查看器”对话框会提供标准的查看器选项，例如：打印、缩放、布局、查找和文本选择。

在**创建报告**对话框中，单击**预览**。
此时 Rational AppScan 会生成报告，并会在**报告查看器**对话框中显示该报告。

保存报告

关于此任务

可以将报告保存为第三方应用程序（例如 Acrobat Reader）可以打开的文件。

1. 按照需要配置该报告的类型、模板和过滤器。
2. 单击**保存**。

   此时会显示**另存为**对话框。
3. 在**另存为**对话框中，为报告输入名称。
4. 从**格式**列表中，选择 **PDF**（Adobe Acrobat Reader）、**HTML**（Web 浏览器）、**RTF**（Microsoft Word）或 **TXT**（文本编辑器）。

下一步做什么

注: 如果先前已将报告保存为某种格式，现在希望将它保存为另一种格式，那么您必须将该报告保存为其他文件名。例如: 如果先前已将报告名称保存为 Report458.pdf，现在希望将它保存为 RTF 格式，那么您无法将该报告保存为 Report458.rtf，但可以将其保存为 Report_458.rtf

---

创建用户定义的报告模板

关于此任务

您可以为“行业标准”报告或“合规一致性”报告创建用户定义的模板。AppScan 报告模板具有 **.asreg** 文件扩展名。提供的模板存储在 AppScan 安装目录的 \Regulations 文件夹中；您创建的模板应该存储在“AppScan 用户文件”文件夹中。

可以从头开始创建新的模板并使用 **.asreg**扩展名将其保存，或复制现有文件并按照需要做出更改。(以下过程会描述基于现有模板创建模板的情况。)

1. 打开 **\AppScan\Regulations** 文件夹，然后复制现有 **.asreg** 文件。

   注: 除非在安装期间指定了其他的位置，否则，缺省情况下，AppScan 目录会位于 **C:\Program Files\IBM\Rational AppScan**。
2. 将该文件粘贴到“AppScan 用户文件”文件夹，并为该文件提供一个新名称。

   注: 除非在**“工具 > 选项 > 首选项”选项卡 > 文件位置 > 用户文件文件夹**中指定了其他位置，否则，缺省情况下，“AppScan 用户文件”文件夹会位于 **\My Documents\AppScan**。
3. 根标记是 Regulation，带有 format_version 的属性:

   ```
   <Regulation format_version="2.0">
   ```
4. 下一个标记应该是模板的标题:

   ```
   <Title>Our Organization's Web Application Requirement Compliance Report

   </Title>
   ```
5. 使用 Description 标记输入规则或标准的描述:

   ```
   <Description>
    <Subtitle>Sub Section</Subtitle>

    <p>This regulation addresses ...</p>

    <p>It is important because...</p>

    <Subtitle>Sub Section 2</Subtitle>

    <p>This section of the regulation addresses ...</p>

   </Description>
   ```
6. 缺省情况下，有一个 <Disclaimer> 标记，它可确保您对报告的内容不承担法律责任。
7. 为规则模板创建需求部分（<Section> 标记），并使用 <Cause> 和 <Risk> 标记来定义哪些 Rational AppScan 问题会与每个部分相关。
   - 这些部分是您自己的定义，决定您的需求内容。Section 标记的 name 属性会定义部分。
   - 每个部分中的原因摘自第 165 页的『原因列表』。每个原因会描述不完整或不正确的配置、缺少的验证或类似的状态。
   - 每个部分中的风险摘自第 166 页的『风险列表』。每个风险都是一个“最差案例方案”。