



IBM Security AppScan

移动应用安全扫描平台方案建议书





目 录

摘要	1
第 1 章 我们对您的目标的理解	3
1.1 WEB 应用的基础概念	3
1.2 WEB 应用安全全景	4
第 2 章 APPSCAN 移动应用安全扫描平台介绍	6
2.1 概览	6
2.2 APPSCAN 企业版方案	7
2.2.1 AppScan 企业版方案简介	7
2.2.2 主要功能特点	7
2.2.3 系统部署	9
2.3 APPSCAN 标准版方案	9
2.3.1 AppScan 标准版方案简介	9
2.3.2 产品的主要特点	10
2.4 APPSCAN 源码版方案	13
2.4.1 AppScan 源码版方案简介	13
2.4.2 IBM Security Web 应用静态白盒安全检测解决方案	14
2.4.3 AppScan Source Edition 产品主要特点	23
第 3 章 IBM 方案优势	31
第 4 章 为什么选择 IBM	33



摘要

我们对您的目标的理解

今天的大多数组织依赖 Web 应用（包括移动应用）软件来运行业务流程、管理交易和提供客户服务。不幸的是，许多企业不能充分执行必要的安全性测试，常常要花费很多时间来确保应用程序符合行业和监管标准。结果导致许多企业可能会不知不觉地将数据暴露给恶意攻击这些漏洞的网络罪犯，将企业置于风险之中。因此，企业迫切需要一个可以将安全测试整合到整个软件开发生命周期里的解决方案作为起点，确保 Web 应用（包括移动应用）软件的安全。

IBM 解决方案

IBM Security AppScan（先前称作 IBM Rational AppScan）为 Web 应用和移动应用交付了应用漏洞测试和管理解决方案，包括静态和动态的应用安全测试。产品版本主要有：

AppScan Enterprise（企业版）

为应用安全测试和风险管理提供了企业级的解决方案。

AppScan Source（源码版）

除了提供 AppScan Enterprise 的功能外，还提供了源代码分析功能。

AppScan Standard Edition（标准版）

为 IT 安全人员、审计员和专业测试人员（penetration testers）提供了自动化的 Web 应用安全测试功能。

IBM 方案优势

- 真正的企业级架构应用安全平台
- 最有效率的检测系统
- 最为全面的规则库
- 不仅仅发现问题，更注重解决问题
- 强大的报告分析能力



- 最可靠的安全平台
- 在线漏洞攻击培训，提升安全防范水平

为什么选择IBM

IBM Security AppScan 在市场占有率、产品发展、技术支持方面都占有很大优势，并有三方评测结果得以验证。

- IDC报告：2007~2011年市场第一名是AppScan
- IDC信息安全产品研究总监评论： AppScan在十年间一直是市场领导产品
- Information week web2.0安全调研报告：强烈推荐web2.0时代关注安全的公司采用 AppScan

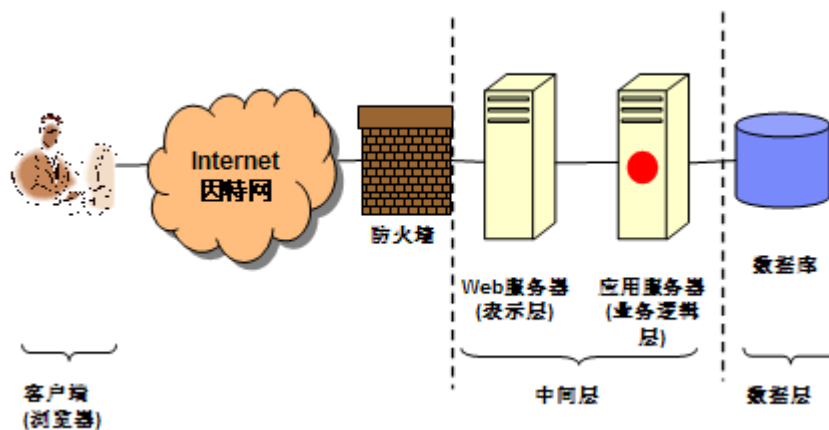


第1章 我们对您的目标的理解

当今世界，Internet（因特网）已经成为一个非常重要的基础平台，很多企业都将应用架设在该平台上，为客户提供更为方便、快捷的服务支持。这些应用在功能和性能上，都在不断的完善和提高，然而在非常重要的安全性上，却没有得到足够的重视。由于网络技术日趋成熟，黑客们也将注意力从以往对网络服务器的攻击逐步转移到了对 Web 应用的攻击上。根据 Gartner 的最新调查，信息安全攻击有 75% 都是发生在 Web 应用而非网络层面上。同时，数据也显示，三分之二的 Web 站点都相当脆弱，易受攻击。然而现实却是，绝大多数企业将大量的投资花费在网络和服务器的安全上，没有从真正意义上保证 Web 应用本身的安全，给黑客以可乘之机。

1.1 Web 应用的基础概念

Web 应用是由动态脚本、编译过的代码等组合而成。它通常架设在 Web 服务器上，用户在 Web 浏览器上发送请求，这些请求使用 HTTP 协议，经过因特网和企业的 Web 应用交互，由 Web 应用和企业后台的数据库及其他动态内容通信。尽管不同的企业会有不同的 Web 环境搭建方式，一个典型的 Web 应用通常是标准的三层架构模型，如图所示。



典型 Web 应用的三层架构模型

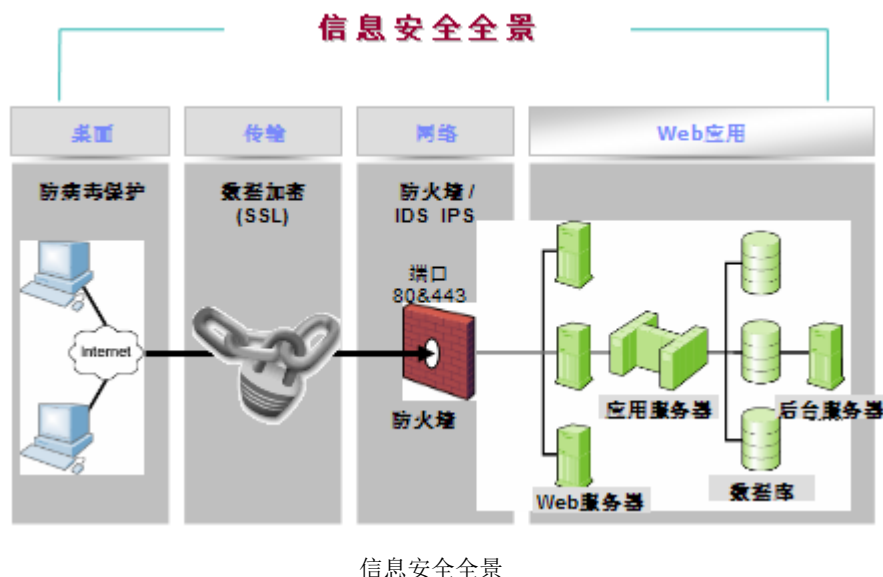
在这种最常见的模型中，客户端是第一层；使用动态 Web 内容技术的部分属于中间层；数据库是第三层。用户通过 Web 浏览器发送请求（request）给中间层，由中间层将用户的请求转换为对后台数据的查询或是更新，并将最终的结果在浏览器上展示给用户。



1.2 Web 应用安全全景

当讨论起 Web 应用安全，我们经常会听到这样的回答：

“我们使用了防火墙”、“我们使用了网络脆弱扫描工具”、“我们使用了 SSL 技术”、“我们每个季度都会进行渗透测试”…… 所以，“我们的应用是安全的”。现实真是如此吗？让我们一起来看一下 Web 应用安全的全景图。



在企业 Web 应用的各个层面，都会使用不同的技术来确保安全性。为了保护客户端机器的安全，用户会安装防病毒软件；为了保证用户数据传输到企业 Web 服务器的传输安全，通信层通常会使用 SSL（安全套接层）技术加密数据；企业会使用防火墙和 IDS（入侵诊断系统）/IPS（入侵防御系统）来保证仅允许特定的访问，不必要暴露的端口和非法的访问，在这里都会被阻止；即使有防火墙，企业依然会使用身份认证机制授权用户访问 Web 应用。

但是，即便有防病毒保护、防火墙和 IDS/IPS，企业仍然不得不允许一部分的通讯经过防火墙，毕竟 Web 应用的目的是为用户提供服务，保护措施可以关闭不必要暴露的端口，但是 Web 应用必须的 80 和 443 端口，是一定要开放的。可以顺利通过的这部分通讯，可能是善意的，也可能是恶意的，很难辨别。这里需要注意的是，Web 应用是由软件构成的，那么，它一定会包含缺陷（bugs），这些 bug 就可以被恶意的用户利用，他们通过执行各种恶意的操作，或者偷窃、或者操控、或者破坏 Web 应用中的重要信息。

因此可以看出，企业的回答，并不能真正保证企业的应用安全：



- 网络脆弱性扫描工具，由于它仅仅用来分析网络层面的漏洞，不了解应用本身，所以不能彻底提高 Web 应用安全性；
- 防火墙可以阻止对重要端口的访问，但是 80 和 443 端口始终要开放，我们无法判断这两个端口中通讯数据是善意的访问还是恶意的攻击；
- SSL 可以加密数据，但是它仅仅保护了在传输过程中数据的安全性，并没有保护 Web 应用本身；
- 每个季度的渗透测试，无法满足处于不断变更之中的应用。

只要访问可以顺利通过企业的防火墙，Web 应用就毫无保留的呈现在用户面前。因此，**只有加强 Web 应用自身的安全，才是真正的 Web 应用安全解决之道。**

您需要一套行业领先的 Web 应用程序安全解决方案，能够为组织提供必要的可见性和控制能力以解决以上关键问题。同时，提供扫描、报告和修复建议等功能，适合于各种用户各种类型的安全测试，包括应用程序开发人员、QA 团队、入侵测试人员、安全审核人员和高级管理员。



第2章 AppScan 移动应用安全扫描平台介绍

2.1 概览

IBM Security AppScan（先前称作 IBM Rational AppScan）为 Web 应用和移动应用交付了应用漏洞测试和管理解决方案，包括静态和动态的应用安全测试。产品版本主要有：AppScan 企业版、AppScan 标准版、AppScan 源码版。

■ AppScan Enterprise（企业版）

IBM Security AppScan 为应用安全测试和风险管理提供了企业级的解决方案。IBM Security AppScan 是一个 Web 应用程序漏洞测试和报告解决方案，它将安全性测试扩展到了整个企业。它促进了信息安全性、开发和管理之间的沟通和协作。Rational AppScan Enterprise Edition 有助于防止未经测试的 Web 应用程序和合规性问题给企业带来风险。Rational AppScan Enterprise Edition 可交付：

- 战略性 Web 应用程序安全——针对 Web 应用程序安全采取战略性方法。
- 全面扫描功能——同时扫描和测试成百上千个应用程序并且频繁对其进行重新测试。
- 企业级报告——使用 Web 界面和企业报告能够轻松沟通安全性状态和特定问题。
- 补救——依靠发布公告以有效的补救措施来帮助指导开发者。

■ AppScan Source（源码版）

除了提供 AppScan Enterprise 的功能外，还提供了源代码分析功能。

■ AppScan Standard Edition（标准版）

为 IT 安全人员、审计员和专业测试人员（penetration testers）提供了自动化的 Web 应用安全测试功能。

AppScan Standard Edition 可自动执行漏洞测试，帮助抵御网络攻击威胁。该解决方案将动态分析与静态 JavaScript 分析相结合，用于在生产之前和之后测试和审计 Web 应用程序。AppScan Standard Edition 支持：

- 全面的覆盖范围 - 针对广泛的应用程序漏洞提供扫描和测试功能。



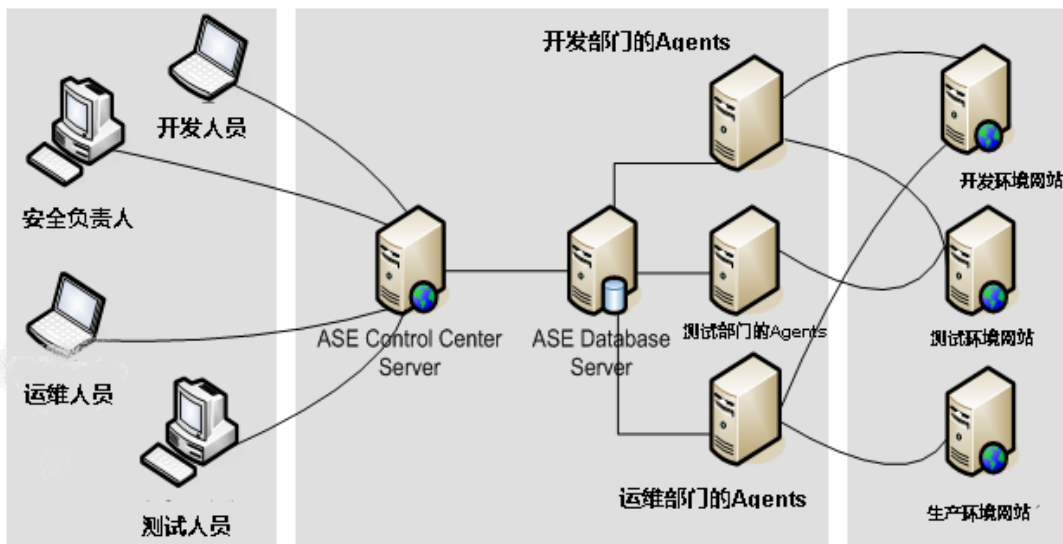
- 准确扫描和高级测试 - 交付高级别的扫描准确性和先进的测试实用程序。
- 快速纠正 - 通过排列优先次序的结果和修复建议快速纠正问题。
- 增强的洞察力和合规性 - 帮助管理合规性并获得对主要问题的洞察。

2.2 AppScan 企业版方案

2.2.1 AppScan 企业版方案简介

Security AppScan Enterprise 是企业提供的一款 Web 应用程序漏洞扫描和报告解决方案。对于那些想要集中进行 Web 应用程序安全测试的企业来说，AppScan Enterprise 提供了高级应用程序扫描、修复功能、管理安全指标以及指示板和关键法规遵从性报告，并且提供了与桌面 AppScan 版本的无缝集成。通过加速安全测试并为那些真正需要报告的人员提供报告，AppScan Enterprise 解决方案能够提高安全团队的生产力。除了在开发生命周期的早期阶段发现安全问题之外，AppScan Enterprise 还通过访问权限、高级报告和趋势指标提供了集中的控制，使项目有更高的可见性。它能够监视已部署到网站上的应用程序，从而针对新的威胁来保护网站。

AppScan 部署如下：



2.2.2 主要功能特点

- 全面的漏洞规则库



在漏洞检测能力方面，ASE 能够覆盖 WASC 和 OWASP 两大 web 安全标准组织定义的、目前主流的各种攻击技术和手段，包括但不限于 Brute Force、Insufficient Authentication、Credential/Session Prediction、Insufficient Authorization、Insufficient Session Expiration、Session Fixation、Content Spoofing、Cross-site Scripting、Buffer Overflow、Format String Attack、LDAP Injection、OS Commanding、SQL Injection、SSI Injection、XPath Injection、Directory Indexing、Information Leakage、Path Traversal、Predictable Resource Location、Abuse of Functionality、Denial of Service、Insufficient Process Validation 等攻击技术和方法。其中，对于 Cross Site Scripting，AppScan 能够检测至少 20 种变种；而对 SQL Injection 至少有 40 种不同的变种。

同时，漏洞规则库支持方便的管理和升级。ASE 支持漏洞规则库的灵活管理，包括在线/手动升级、规则导入/导出、规则自定义等功能，能够确保及时使用最新的、最全面的、最准确的漏洞攻击技术和方法来抵御各种攻击。

➤ 漏洞扫描的全面性和准确性

AppScan 支持当前采用的 Web 应用的技术，如 JavaScript、HTTPS 以及认证等，以便确保发现 URL 的完整性。

➤ 报表功能和漏洞管理

漏洞报告和管理功能是本次测试的重要部分。针对客户应用众多、页面多、分布比较广泛等实际情况，需要该平台能够提供强大、灵活的报表展示功能、漏洞报告和管理功能，以便于客户不同层面的人员，如高层管理人员，部门管理人员，技术人员（开发、测试、运维等）等，能够查看不同层面和粒度的数据和报表，从而简化日常的管理和维护。同时，ASE 提供的强大的报表展现和定制功能，能够为客户不同角色的人员定制其关注的报表；同时，借助 ASE 全生命周期的漏洞管理理念，实现了漏洞的灵活管理。

➤ 管理的便利性

产品的系统管理的便利性、灵活性以及安全性，是系统日常运维过程中的一个重要指标。这里，我们重点说明 ASE 的权限管理、规则管理、系统配置等方面的内容。

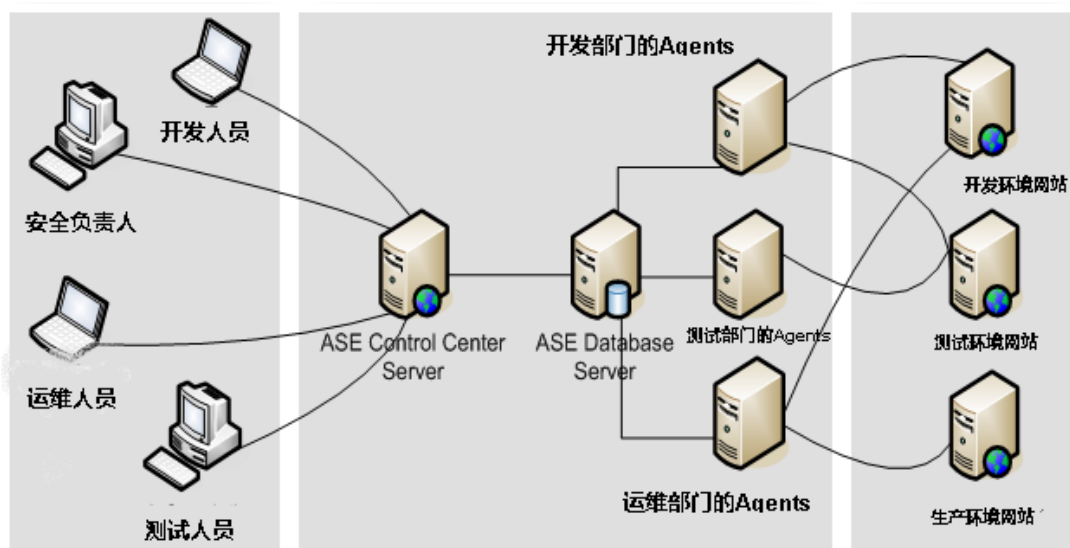
- 1) ASE能够支持任意增加扫描Agent的个数，提供扫描效率
- 2) 可以为用户指定不同的角色，即user type，从而让用户具有不同的权限类型。
- 3) 内置用户和组的管理，包括创建、删除、修改以及权限设置等功能
- 4) ASE同时支持与LDAP server集成的方式，实现用户的统一管理



- 5) ASE通过配置可以扫描的服务器ip地址、域名以及ip地址段，从而可以限制用户可以扫描的对象
- 6) 通过编辑用户的属性，可以指定该用户可以扫描的服务器、ip地址段等内容，从而使得漏洞扫描工具更加安全
- 7) 针对ASE中的每个对象，可以设置其对应的访问权限，如目录、扫描任务、报表、修改权限任务等。通过多种权限设置，可以限定特定的人员访问特定的信息，确保漏洞管理平台的安全性，避免漏洞信息的泄漏
- 8) 可以定制符合客户规定的漏洞等级

2.2.3 系统部署

为了测试实现“集中管理，分布式部署”的要求，让 ASE 可以通过部署不同的 Agent，让 Agent 分布式地测试不同网络、不同环境下的不同应用，以便测试是否满足客户的部署要求，如下图所示。



2.3 AppScan 标准版方案

2.3.1 AppScan 标准版方案简介

IBM Security AppScan，是对 Web 应用和 Web Services 进行自动化安全扫描的黑盒工具，它不但可以简化企业发现和修复 Web 应用安全隐患的过程，还可以根据发现的安全隐患，提出针对性的修复建议，并能形成多种符合法规、行业标准的报告，方便相关人员全面了解企业应用的安全状况。



企业仅需要指明 Web 应用的入口链接，AppScan 就会利用网络爬行（Crawling）技术，遍历应用中所有需要测试的链接，并对每个链接发送多种测试参数，诊断其有无漏洞可被利用。最后将结果呈现在用户面前。

IBM Security AppScan 不仅可以对 Web 应用进行自动化的扫描、指出安全漏洞的修复意见，还可以将诊断结果，使用不同的行业标准、法规，形成针对性的报告，让相关人员对应用安全状况和法规遵从等有了全面的认识。比如 AppScan 可以自动生成的行业标准报告，同时满足近 40 种的法规遵从报告，如赛班斯法规遵从等。

2.3.2 产品的主要特点

➤ 最强悍的Web应用安全检测工具，全面提高您的安全级别

防火墙、入侵检测系统并不意味着您的 Web 是安全的，通过 Web 应用本身的漏洞黑客就可以轻松的进入系统，防火墙、入侵检测系统则如同虚设。这种针对 Web 应用的攻击是网络安全产品无法防范的。完整的 Web 安全解决方案不仅仅需要网络安全产品，如防火墙/入侵检测系统，也需要针对应用安全的产品。

AppScan 是业界最为强悍的安全检测工具，使用 AppScan 将会全面提高您的安全级别。AppScan 核心技术是利用内置的漏洞规则库模拟黑客对 Web 进行扫描，从而发现漏洞，帮助用户改进漏洞。用一句形象的比喻来说明：防火墙/入侵检测系统如同金钟罩、铁布衫等外功，防止明枪；AppScan 如同太极等内功，弥补了自身的漏洞，躲避暗箭；内外兼修才能确保企业 Web 应用信息安全。

➤ 易用性极强，轻松上手

面对越来越复杂的应用，AppScan 的使用却是非常简单。不需要关注 Web 应用是如何开发的，不需要对编程有深入的了解，AppScan 让即便不了解软件的使用者都能立刻上手，快速地检测应用安全漏洞。

实际上 AppScan 是一个黑盒测试工具，内置的漏洞规则库针对 Web 应用模拟外部攻击，通过收集反馈判断安全漏洞所在的位置。AppScan 不仅可以自动化地帮助客户全面检测整个 Web 应用，或者用户所关注的某部分；也可以录制客户的操作，模拟客户真正关心的操作场景，进而发现这个场景中的安全隐患。AppScan 的易用性能让业务人员、质量管理人员都参与到 Web 应用开发、运维过程中来，最准确的保证了业务安全性。

➤ 最全面的漏洞规则库，最快的规则库更新



拿大家常用的杀毒工具作个比喻：杀毒工具核心部分是病毒特征库，特征库中病毒种类越多，杀毒工具查杀的病毒越多；杀毒工具常常自动更新特征库，更新的越频繁，新病毒也就越快的能被查杀。查杀病毒的种类多、更新快的杀毒工具是客户的首选。

同理，AppScan 核心是漏洞攻击规则，也是业界最为强悍的规则库，保证了 AppScan 是最强悍的应用安全检测工具。同时，AppScan 每周将会更新 2~3 次规则库，一旦有新的攻击方式出现，它也会被最快的更新到规则库中，用户可以迅速检测出该漏洞。在线更新保障客户拥有业界最新最完整的漏洞规则库，轻松应对更多的安全挑战。

➤ 提供了最完整的针对漏洞的解决方法

AppScan 不仅仅能够发现漏洞，更提供了解决该漏洞的方法。例如，针对平台的安全漏洞 AppScan 告诉系统管理员应该去打相应的补丁包；针对程序安全漏洞，AppScan 告诉开发人员如何修改程序去避免这样的漏洞，并且提供了各种程序语言的例子加以说明。

➤ 基于国际标准，提高企业的遵从性

在 Web 应用安全方面有两个组织：WASC 和 OWASP，它们在呼吁企业加强应用安全意识和指导企业开发安全的 Web 应用方面，起到了重要的作用。

Web Application Security Consortium (WASC)，是一个由安全专家、行业顾问和诸多组织的代表组成的国际团体。他们负责为 WWW 制定被广为接受的应用安全标准。WASC 组织的关键项目之一是“Web 安全威胁分类”，也就是将 Web 应用所受到的威胁、攻击进行说明并归纳成具有共同特征的分类。该项目的目的是针对 Web 应用的安全隐患，制定和推广行业标准术语。WASC 将 Web 应用安全威胁分为如下六类：

➤ **Authentication (验证)**

用来确认某用户、服务或是应用身份的攻击手段。

➤ **Authorization (授权)**

用来决定是否某用户、服务或是应用具有执行请求动作必要权限的攻击手段。

➤ **Client-Side Attacks (客户侧攻击)**

用来扰乱或是探测 Web 站点用户的攻击手段。

➤ **Command Execution (命令执行)**

在 Web 站点上执行远程命令的攻击手段。



➤ **Information Disclosure (信息暴露)**

用来获取 Web 站点具体系统信息的攻击手段。

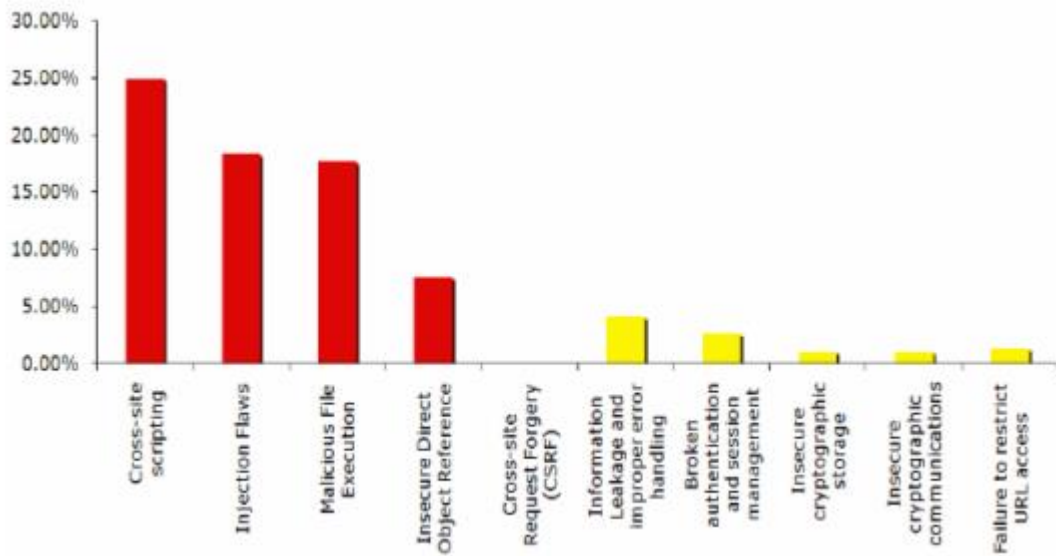
➤ **Logical Attacks (逻辑性攻击)**

用来扰乱或是探测 Web 应用逻辑流程的攻击手段。

可以通过如下的网址访问该组织网站，获得更多详细信息：www.webappsec.org。也可以通过如下链接，具体了解“Web 安全威胁分类”项目：

http://www.webappsec.org/projects/threat/v1/WASC-TC-v1_0.pdf

Open Web Application Security Project (OWASP)，该组织致力于发现和解决不安全 Web 应用的根本原因。它们最重要的项目之一是“Web 应用的十大安全隐患”，总结了目前 Web 应用最常受到的十种攻击手段，并且按照攻击发生的概率进行了排序。这个项目的目的是统一业界最关键的 Web 应用安全隐患，并且加强企业对 Web 应用安全的意识。



Web 应用十大安全隐患

可以通过如下的网址访问该组织，了解更为详细的信息：www.owasp.org。也可以通过如下链接，具体了解“Web 应用十大安全隐患”项目。

http://www.owasp.org/index.php/OWASP_Top_Ten_Project。

IBM Security 是上述两个组织的成员，AppScan 完全支持以上两个组织的成果和标准。



2.4 AppScan 源码版方案

2.4.1 AppScan 源码版方案简介

IBM Security AppScan 系列产品提供了一组帮助企业实现“安全设计”的理念。这一理念将安全测试集成到整个软件开发生命周期——从代码到成品——提供开发安全代码所需的工具。AppScan 源码版除了提供 AppScan 企业版的功能外，还提供了源代码分析功能。

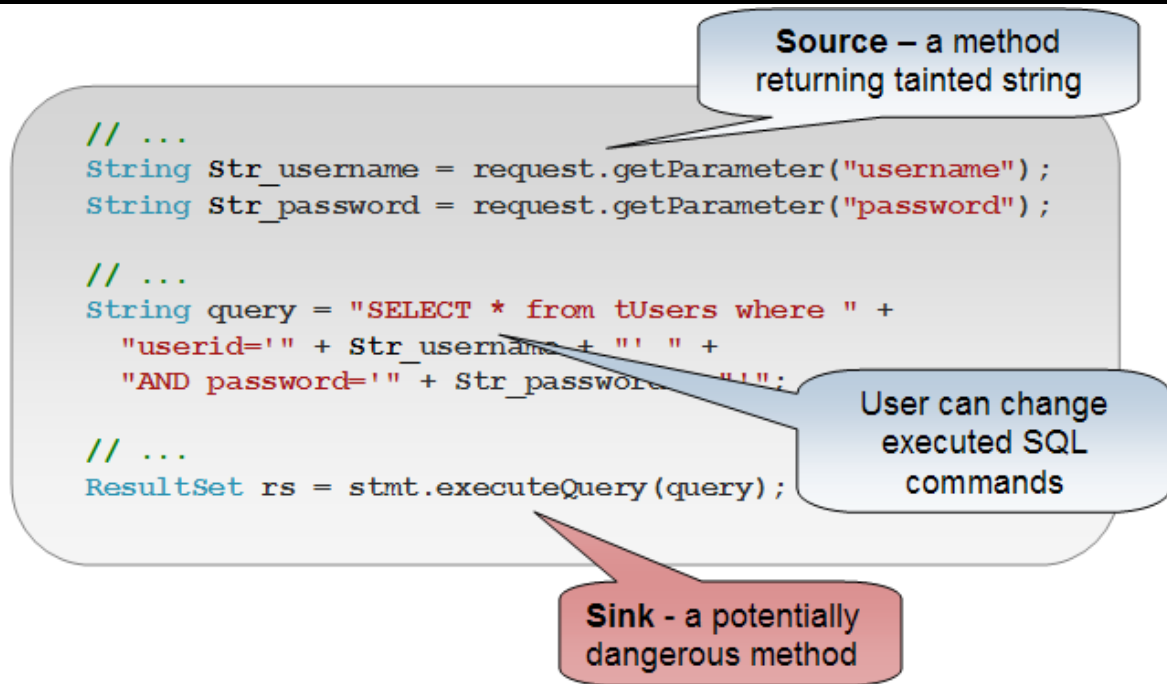
白盒技术，也叫静态分析技术。它是通过手工或者工具检验应用程序的源代码，利用大量的代码安全规则，来分析源代码中的违反规则部分，进而确定可能存在的安全隐患。

今天使用较为普遍的静态分析方法叫做 Taint Flow Analysis。这种技术的主要思路是在应用源码中，监控一个不被信任的可疑点（tainted data）的传递过程。它首先标记可疑点的来源方法（通常被称为“Source”），比如说传递一个 HTTP 参数的方法，然后跟踪这个参数是否在应用源代码中被复制或者被传给其它的参数，追寻这条线索一直到这个可疑数据被某种操作执行（通常被称为“Sink”）。如果在这一整条路径中，可疑点都没有经过某种方式清洗，就可以被标识成为潜在的安全隐患。

同样使用 SQL 注入攻击举例，我们来看一下白盒技术的工作原理。

如图 3 所示，在 Web 应用页面上需要用户输入的两个字符串“username”和“password”，通过 request.getParameter()方法被直接赋值给字符串 Str_username 和 Str_password，该方法就是 Source。继续跟踪这两个字符串，它们又被直接用来构建 SQL 查询语句。由于查询语句字符串中包含可疑点，因此整个查询字符串都被认为是可疑的。最后，通过跟踪，发现查询语句作为字符串被直接赋给一个执行查询语句的方法 stmt.executeQuery()，该方法就是 Sink。在这个跟踪过程中，我们没有看到任何对这些变量的过滤或者清洗操作，于是，当可疑点到达 Sink 时，也就意味着黑客有可能注入自己的恶意代码到该方法中，我们就标识这是一个潜在的漏洞。

图 3 白盒防技术工作原理：



白盒防御技术的优势：

- 在软件开发早期就可以发现安全隐患，解决问题的成本较低；
- 完整代码扫描，保证了发现漏洞的全面性及高代码覆盖率；
- 通过架构分析，还可以发现设计漏洞及其它应用“后门”。

2.4.2 IBM Security Web 应用静态白盒安全检测解决方案

Security AppScan Source 白盒代码扫描工具支持多种语言，包括 Java、JSP、C、C++、C#、VB.NET、ASP.NET、Classic ASP、VB6 PHP。这款产品的性能非常不错，使用 C/C++ 语言构建了内存管理模块，使用基于 Eclipse 的前端展现构建其主要界面，在设计之初就兼顾了扫描性能和易用性，同时结合拥有专利的核心扫描引擎，可以达到每小时扫描百万行代码的速度。

Security AppScan Source 产品包含了一系列功能模块，用来全方位的管理从应用代码诊断分析、漏洞展现到漏洞修复的整个过程。这些模块包括：

- **AppScan Enterprise Server，核心服务器端组件。**它主要包含了安全测试规则和扫描结果。当使用扫描组件进行扫描时，系统将会从Core中拿到测试规则，当企业对扫描规则进行自定义之后，这些结果也是存储在Core组件中的。通常，Core组件包括如下信息：
 1. 企业部署环境中的用户认证信息；
 2. 企业部署环境中的用户授权信息；



3. 应用安全规则库信息;
 4. 用户定义的安全规则信息;
 5. 所有企业中“已发布”状态的应用扫描结果信息（没有发布的私有应用，可以以HTML或者PDF或者专有格式输出）；
- **AppScan Source for Security**，核心客户端组件。是扫描组件之一。它主要由安全小组或者是具有高级用户权限的成员使用，可以根据企业环境定制扫描规则、发起扫描、对扫描结果进行分析和挑选、将结果创建报告给到管理层，或者将扫描结果直接发给开发人员让其修复。它也是主要的管理接口，比如用户管理、创建报告模板等等工作也是由该组件实现。
 - **AppScan Source for Developer**，开发人员插件，扫描组件之一。可以无缝集成到Eclipse、Security Application Developer、Visual Studio等主流开发工具中。当安全人员将查询出来的漏洞发送给开发人员时，他们可以使用该组件打开并直接定位到代码上，同时可以参考工具提供的修复意见进行修改，如果允许连接到Core组件上，还可以进行再次扫描以验证修改是否成功。
 - **AppScan Source for Automation**，服务器端可选组件，扫描组件之一。它可以在企业代码构建阶段，将代码扫描的能力结合进来。目前它可以和Ant、Maven、Make等构建系统集成。也可以和Cruise Control、Hudson等持续集成系统集成。
 - **AppScan Source for Remediation**，可选客户端组件。它类似于功能受限版的开发人员插件，只能看到安全人员发出的漏洞，并根据建议修复，不具备再次扫描的功能。

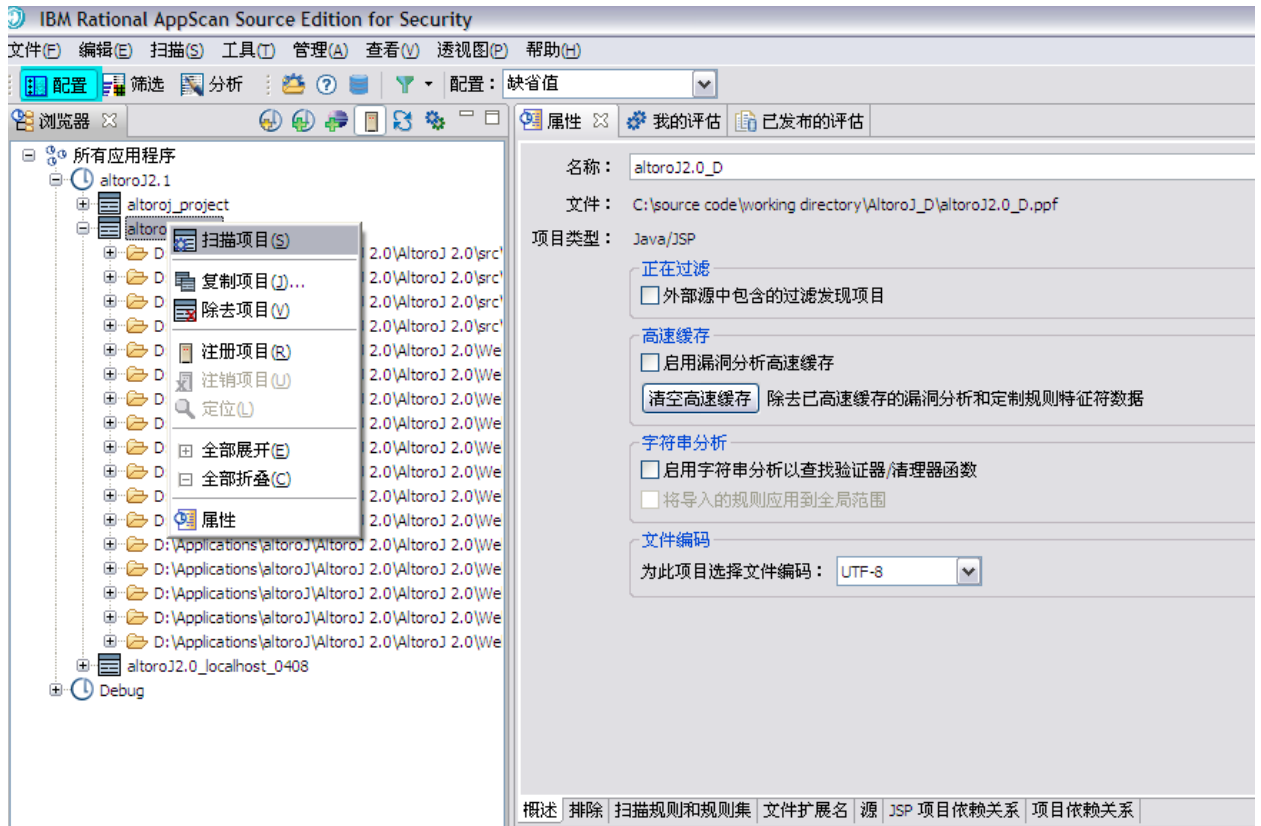
AppScan Source 可以提供各种报告和报表，可以使用 PDF、HTML 等格式导出，也可以通过和企业版、AppScan Reporting Console 等产品结合，进行展现。

上述组件的配合和流程如图 4 所示。

图 4 AppScan Source 各组件功能及其 workflow:



图 5 AppScan Source for Security 的配置界面：



图表 1 配置扫描项目

2、筛选 (Triage)：扫描结果的展现视图，内容非常丰富。如图 10 所示，左上方是对扫描结果的简单总结，可以用多种方式分类：如漏洞类型、项目、文件等，还可以选择用柱状条、圆饼或是表格展示。从图上可以看出，用“发现的最重要的 9 类漏洞”来分类，该企业的跨站脚本攻击和 SQL 注入漏洞非常严重，可以点击某一个柱状条，在左下方看到细节分析。图 6 的右上方是 AppScan Source for Security 中非常有特色的名为“漏洞矩阵 (Vulnerability Matrix)”的视图。通常，我们了解漏洞的严重等级，仅仅会分成高/中/低、严重/一般等，而在 AppScan Source for Security 中，我们可以从多维的、带有一定“可信度”的角度，理解扫描出来的漏洞。也就是说，我们不仅发现所有的漏洞，还根据某种规则，将结果分为真正的漏洞（高可信度的漏洞，图中 Vulnerability 列）、Type I 和 Type II 的例外（低可信度的漏洞，图中 Exceptions 列），在每一种漏洞上，又分为高/中/低严重程度。利用多维角度，可以帮助企业的安全分析人员快速定位哪些漏洞值得优先关注、立刻解决，哪些漏洞需要再仔细分析。一般情况下，企业需要高度重视第一列 (Vulnerability)，对于二、三列 (Exceptions)，在有时间和人力时候再进一步调研。图中的每个行列的内容块都可以点击，进行快速过滤，并在透视图下方展示细节信息。



对于确定的漏洞，我们这里不多强调。那么，Type I 和 Type II 的例外，工具是怎么解释的呢？Type I 代表了有可能的漏洞，当 AppScan Source for Security 跟踪一个被污染（tainted）的 Source 到 Sink 的过程中，会有一或多个中间节点。如果这些中间节点工具无法进行判断（没有在工具规则库中做过标识），就会报出一个 Type I 的漏洞。这表示安全分析人员需要进一步确认，没有标识的中间节点，如果它们都确实拥有一定的“清洗”方法，就可以被忽略，否则就很有可能被利用。对于 Type II 型的例外，工具在扫描应用的时候，会将所有 Sink 都标记为 Type II，无论是否有被污染的数据传给它，因此，这种类型通常只用作参考，比如可以利用它建立编写安全代码的最佳实践。

由于 Triage 是安全分析人员的重要工作，他们需要从发现的大量结果（Findings）中，通过过滤和优选，快速找到最重要、最需要先解决的那部分给到研发人员，因此，工具的过滤、搜索、分发的功能相当重要。

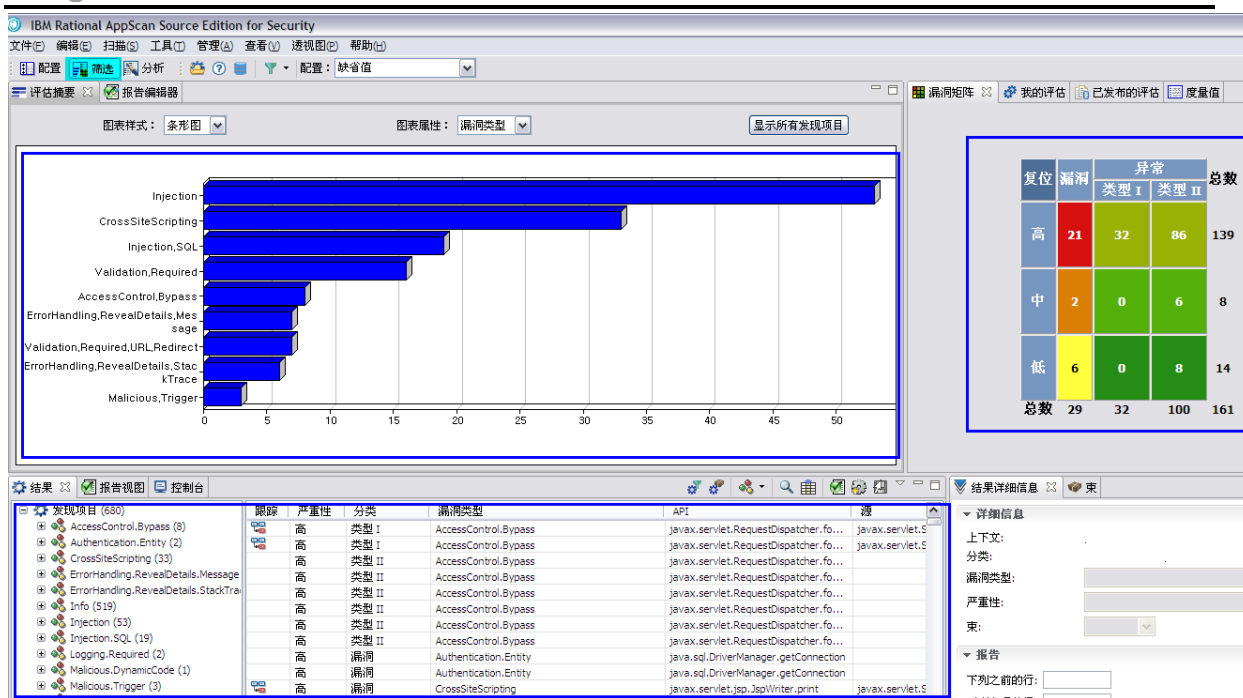
过滤：在 AppScan Source for Security 中，有强大的过滤编辑器，可以按照漏洞的 API、文件、类别等多种方式过滤。安全分析人员可以将不同的过滤器保存起来，用来针对不同部门、不同应用。同时，还可以将这些过滤器共享，在整个企业范围内提高效率。

搜索：对于搜索功能，只要在有 Findings 的视图里，都可以对扫描的结果进一步的搜索，包括在文件、API、Sink、项目中搜索。

分发：当安全分析人员优选了部分需要立刻解决的漏洞后，他可以选择打包（在工具中，称为 Bundle），也就是将这些漏洞进行分组，如按照漏洞类型分组、按照应用模块分组等。分组后，可以通过两种方式给到相应开发人员：导出后通过邮件发送、或者直接提交到已经集成好的缺陷管理系统中，如 ClearQuest、Quality Center 等。

优选（Triage）过程的另外一个重要活动是，深入分析安全漏洞。这个工作可以由安全分析人员实现，也可以交给开发人员，这和企业的应用安全管理模式相关。关于管理模式，我们在下一节讨论。通过图 10 中的“Findings”视图（图 10 的正下方），我们可以进一步分析每一个安全漏洞。点击结果中“Injection.SQL”类型，可以看到一共有 24 个此类型的漏洞，其中有 22 个 Vulnerability 和 2 个 Type II 例外。再点击 Vulnerability，工具展示了这 22 个漏洞，并且标识出了包含漏洞的方法、源代码的具体位置等，比如图中的 IsValidUser 方法，在源文件的第 112 行。如果还需要深入到代码中去分析，只要双击这行，工具自动进入分析页面。

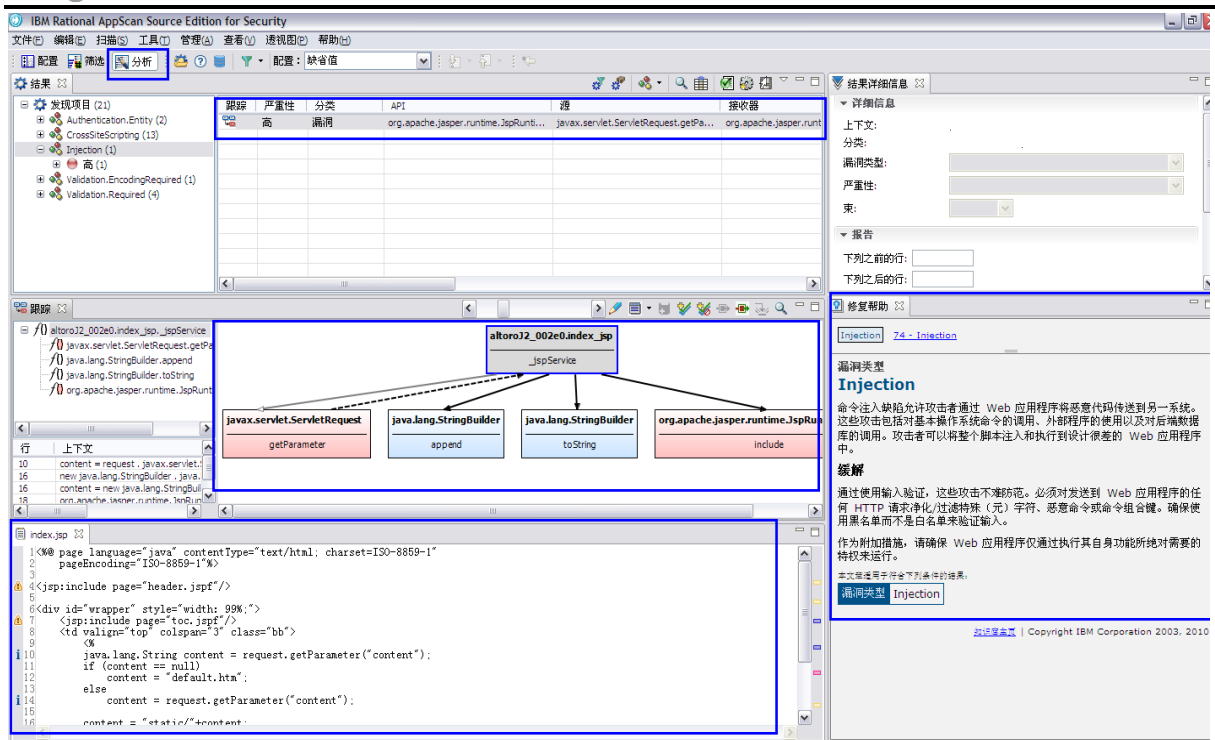
图 6 AppScan Source for Security 的 Triage 界面：



3、分析 (Analysis)： 对扫描结果进行深入探究的视图。内容丰富且包含了多种具有产品特色和专利技术的功能。如图 11 所示。在分析透视图的右下方，是名为修复助手的视图。这是一个庞大的漏洞信息知识库，对每一个漏洞的详细解释、“好”代码和“坏”代码片段示例、到行业标准信息如 CWE 的链接等。这些信息可以帮助安全分析人员快速理解问题，也有利于开发人员修复问题。图的左方是具有产品特色的 Smart Trace（智能追踪）视图。

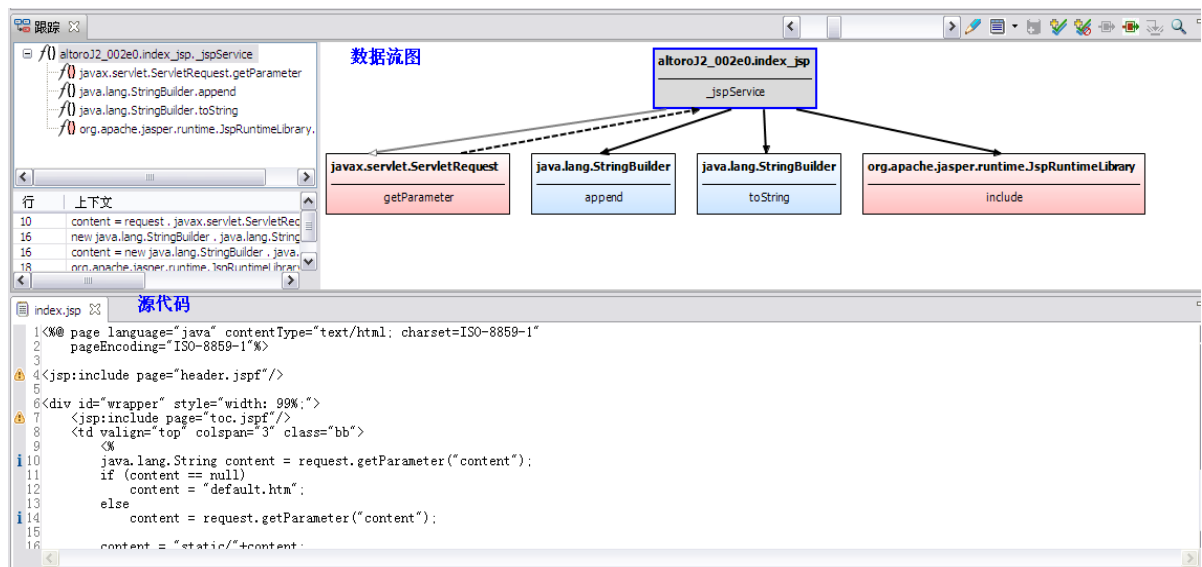
Smart Trace 使用调用图的方式显示危险数据的传递流程。它通过标识应用缺乏一定的验证和编码手段，帮助用户分析输入类安全攻击，如跨站脚本攻击、SQL 注入等。调用图是交互式的，可以通过点击，直接进入图中的源、或者 Sink，如图 7 中左下方就是通过调用图进入的真实代码位置。

图 7 AppScan Source for Security 的分析界面：



Smart Trace 视图中包含了大量信息。左上方是输入/输出方法调用序列，如图 7 所示，_main.asp._Page 类中的方法_WebServices，调用了 ASPTTypeLibrary.IRequest 类中的 ServerVariables 方法，同时还调用了 ASPTTypeLibrary.IResponse 类中的 Write 方法。每点击一个方法，下面都会附上该方法使用到的数据流和在代码中出现的行号，用行号表示。





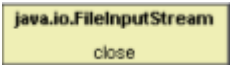

图 8 Smart Trace 视图：



右上方是调用图，由矩形方法框和箭头组成。箭头的方向代表了方法调用的方向。图 8 解释了这些箭头和矩形框代表的意义。



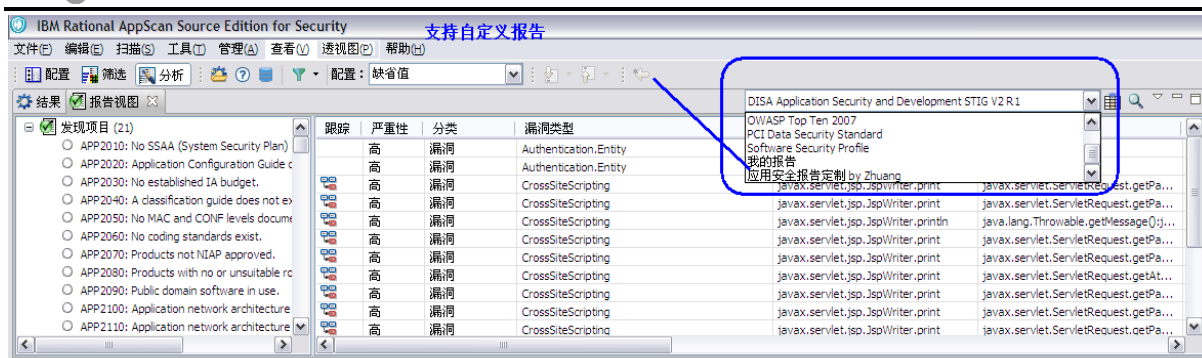
图 8 Smart Trace 调用图中符号的解释说明：

符号	解释
	灰色空箭头表示该方法调用没有传递被污染的数据
	黑色实箭头表示该方法传递了被污染的数据
	虚线箭头表示方法的返回值包含被污染的数据
	红色方框表示该方法是Source或Sink
	黄色方框表示通过该方法的污染数据无法继续跟踪下去，也就是Lost Sink
	浅蓝色方框表示该方法没有对经过的数据进行任何验证

以图 7 为例，ServerVariables 方法是一个 Source，通过它，引入了可能有污染的变量 SERVER_NAME，而该方法的返回值 servename 同样也被“传递”了污染性（源代码第 99 行）；由于在整个跟踪过程中，变量 servename 都没有经过任何清洗，而且在调用 Write 方法时使用了，因此传递给 Write 方法一个有污染的数据，那么这个 Write 方法就变成了一个 Sink（源代码第 107 行）。

除了上述介绍的三个步骤外，安全分析人员的日常工作，还有能够灵活的将结果生成报告。AppScan Source for Security 中的 SmartAudit，可以按照不同的行业标准对扫描结果进行分类，方便审计人员了解发现的漏洞违反了哪些、怎样违反行业标准。如图 14 所示，工具可以支持的行业标准有 DISA ASD、OWASP、OWASP 2007、PCI 以及基本的软件安全分类。审计人员可以方便的在工具中选择不同的模板来组织数据，也可以直接将结果用这些行业模板导出。同时，SmartAudit 还提供自定义报告，通过 SmartAudit Editor，可以完全定制符合企业需要的报告模板，如报表布局、报表包括的数据等。

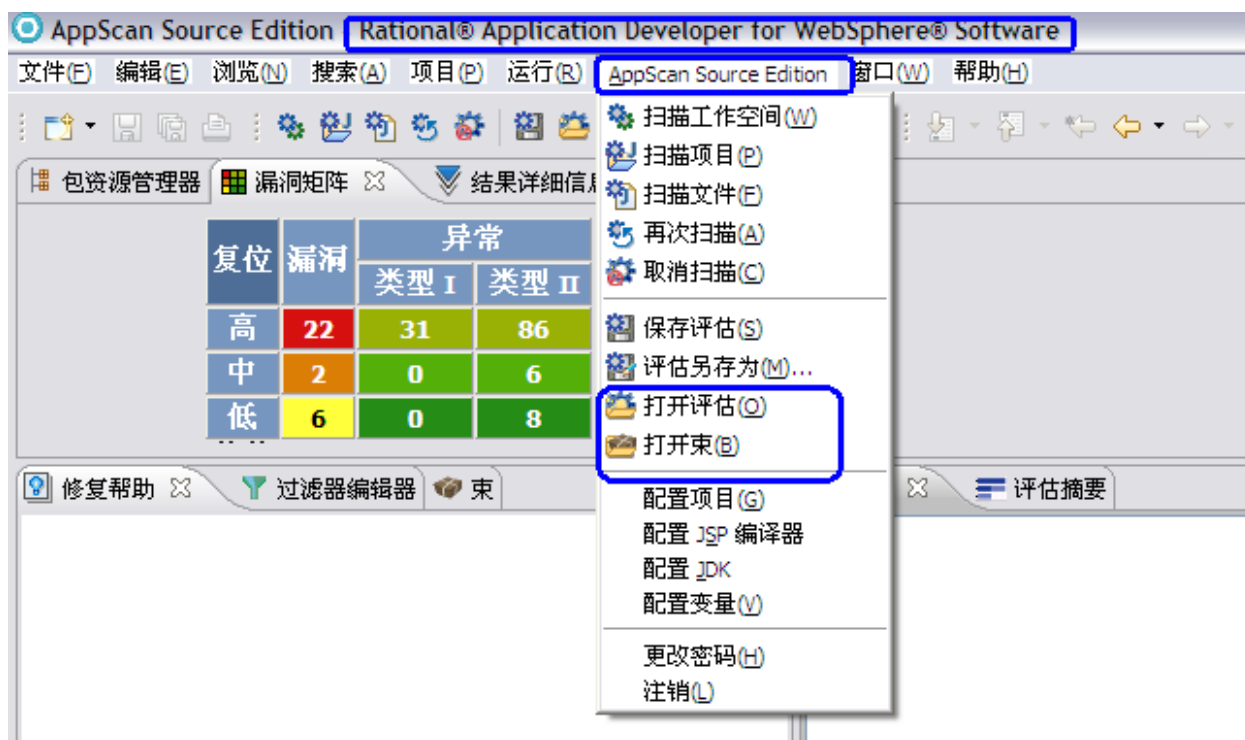
图 9 报告支持的行业标准：



2.4.2.2 开发人员和 AppScan Source

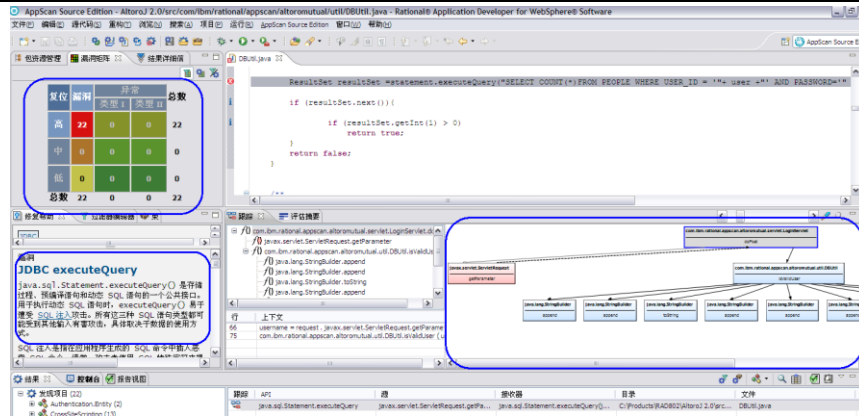
AppScan Source 可以和 Eclipse、Security Application Developer、Visual Studio 等主流开发工具集成，因此方便开发人员在日常开发中顾及应用安全。如 3.3.1 节所述，安全分析人员将扫描发现的安全隐患进行某种归类，创建出不同的 Bundle，将这些 Bundle 给到开发人员。开发人员在集成好 AppScan Source for Developer 或 AppScan Source for Remediation 的开发环境中，可以直接打开该 Bundle。如图 15 所示为将 AppScan Source for Developer 和 Security Application Developer 集成。

图 10 开发人员在 Eclipse 中打开扫描结果：



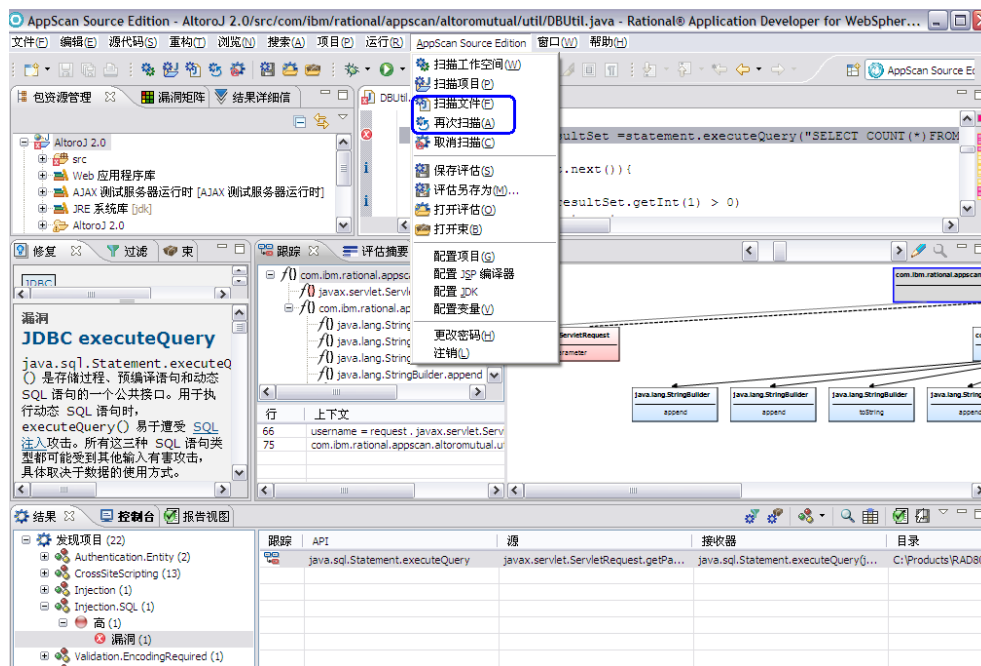
在 Eclipse 中选择 AppScan Source Edition 菜单中的“Open Bundle”选项，开发人员就可以直接在 Eclipse 中看到类似于 AppScan Source for Security 工具中的界面，包括修复助手、漏洞矩阵、Smart Trace、过滤器、详细信息等视图。如图 11 所示。

图11 开发人员在Eclipse中可以直接看到漏洞的详细信息，根据建议进行代码修改：



开发人员可以从每个安全隐含的 Smart Trace 中直接进入源代码修改。修改完成后，还可以直接在 IDE 中重新测试，以确定该漏洞是否被正确修复（能否重新测试，取决于该用户是否有权限以及使用的是哪种客户端版本）。如图 12 所示。

图 12 开发人员修改完代码之后可以直接在 RAD 中进行测试：



2.4.3 AppScan Source Edition 产品主要特点

Security AppScan Source 白盒代码扫描工具支持多种语言，包括 Java、JSP、C、C++、C#、VB.NET、ASP.NET、Classic ASP、VB6 PHP。这款产品的性能非常不错，使用 C/C++语言构建了内存管理模块，使用基于 Eclipse 的前端展现构建其主要界面，在设计之初就兼顾了扫描性能和易用性，同时结合拥有专利的核心扫描引擎，可以达到每小时扫描百万行代码的速度。



2.4.3.1 支持众多类型的应用

AppScan source Edition 支持扫描的应用类型包括：ASP、C/C++、客户端 JavaScript（包括 JQuery）、ColdFusion、Java/JSP、.NET 组合件、模式分析、Perl、PLSQL,T-SQL,PHP 和 Visual Basic。

2.4.3.2 内置代码规范性检查模块

AppScan source Edition 内置丰富的 Java 代码审查规则，覆盖代码审查、架构发现和深度分析，能够在代码复审中从 J2EE 最佳实践、J2SE 最佳实践、JUnit 单元测试、安全性、命名规范与全球化、设计原则等多种方面进行深度分析。

2.4.3.3 向导式的流程化使用模式

AppScan Source Edition 的主要客户端的 Security 模块的使用模式支持流程化，主要分为“配置”，“筛选”，“分析”三个步骤，方便用户快速上手，展开使用。

2.4.3.4 安全的用户和角色管理功能

作为一个安全工具，AppScan source edition 本身的安全管理也很严格，用户使用工具时候首先需要用户名和密码，还可以用户对应的角色，不同角色对应不同的许可权，通过“用户—角色-许可权”的三层模式，共同管理权限。

许可权标识了允许该用户执行的 AppScan® Source 任务。AppScan source Edition 提供的许可权模块如下，每个角色都可以对应一个或者多个许可权。

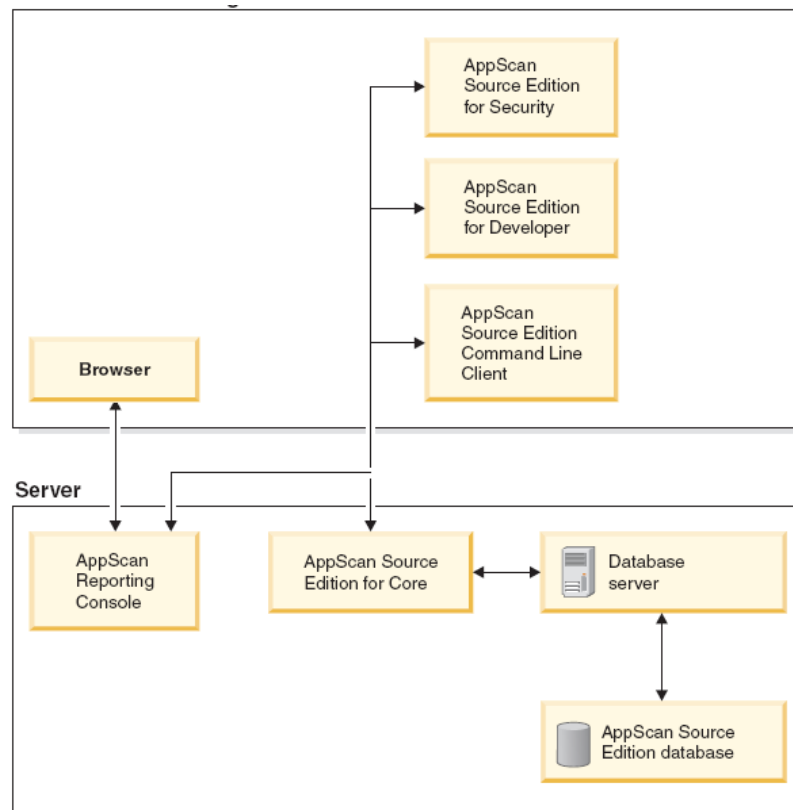
许可权组	许可权
应用程序和项目管理	注册（注册和注销应用程序与项目）
	应用属性
	管理属性
	扫描
	查看已注册的内容
评估管理	删除已发布的评估
	发布评估
	保存评估
	查看已发布的评估



许可权组	许可权
知识库管理	管理定制规则
	管理扫描规则
管理	管理 LDAP 设置
	管理用户

2.4.3.5 分布式的架构，便于沟通和共享

AppScan Source 产品支持分布式部署，包含了一系列功能模块，用来全方位的管理从应用代码诊断分析、漏洞展现到漏洞修复的整个过程。其中 AppScan Enterprise Server 是服务器核心模块，众多的客户端需要可以连接到 AppScan Enterprise Server； 在一个客户端完成扫描以后，可以发布到服务器上，然后其他客户端的用户登录以后，根据权限分配，就可以访问到这些项目，从而很方便地实现资源的共享和使用。



图表 2 AppScan Source edition 部署模式之一

AppScan Source Edition 的主要模块包括：



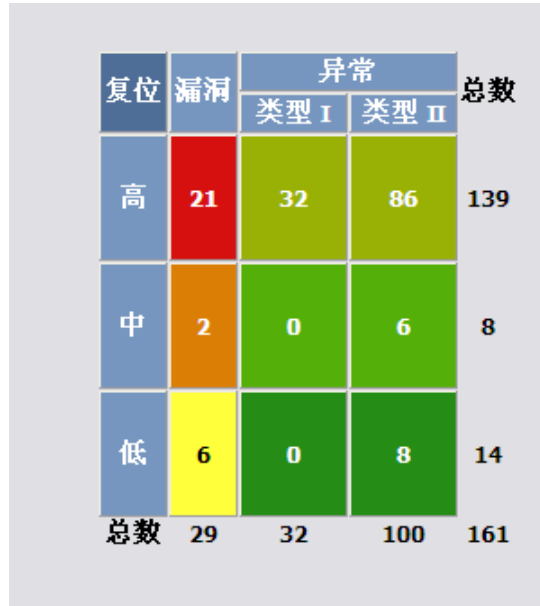
- **AppScan Enterprise Server**，核心服务器端组件。它主要包含了安全测试规则和扫描结果。当使用扫描组件进行扫描时，系统将会从Core中拿到测试规则，当企业对扫描规则进行自定义之后，这些结果也是存储在Core组件中的。通常，Core组件包括如下信息：
 1. 企业部署环境中的用户认证信息；
 2. 企业部署环境中的用户授权信息；
 3. 应用安全规则库信息；
 4. 用户定义的安全规则信息；
 5. 所有企业中“已发布”状态的应用扫描结果信息（没有发布的私有应用，可以以HTML或者PDF或者专有格式输出）；
- **AppScan Source for Security**，核心客户端组件。是扫描组件之一。它主要由安全小组或者是具有高级用户权限的成员使用，可以根据企业环境定制扫描规则、发起扫描、对扫描结果进行分析和挑选、将结果创建报告给到管理层，或者将扫描结果直接发给开发人员让其修复。它也是主要的管理接口，比如用户管理、创建报告模板等工作也是由该组件实现。
- **AppScan Source for Developer**，开发人员插件，扫描组件之一。可以无缝集成到Eclipse、Security Application Developer、Visual Studio等主流开发工具中。当安全人员将查询出来的漏洞发送给开发人员时，他们可以使用该组件打开并直接定位到代码上，同时可以参考工具提供的修复意见进行修改，如果允许连接到Core组件上，还可以进行再次扫描以验证修改是否成功。

2.4.3.6 科学化的漏洞分析“信心矩阵”

在扫描结果的筛选分析模块，AppScan Source edition 提供漏洞信心矩阵，如下图，矩阵的竖坐标表示安全隐患的安全级别，从下到上，依次是“低，中，高”；级别越高，被利用以后造成的安全风险愈大；横坐标表示“漏洞-异常（类型 I）-异常（类型 II）依次表示该安全漏洞存在的信心（确凿性），如果是”漏洞“，说明该问题明确存在，如从输入到后台数据库的调用过程，该参数都没有进行安全检查和过滤，则肯定存在注入隐患。如果为异常（类型 I）说明该问题很可能存在，同时需要人员进行确认和扫描规则的确定，如发现一个未知的过程处理函数，需要人员来确认是否是安全过滤功能等。

如果是异常（类型 II），则认为该问题是潜在问题，需要更多证据来判断。

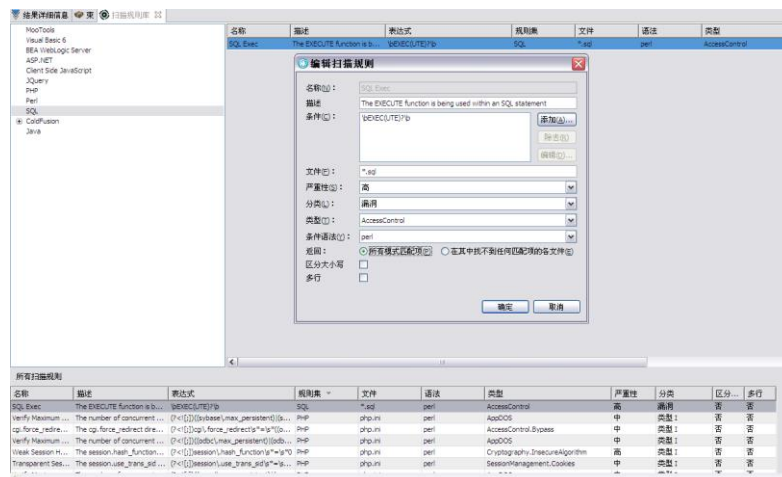
通过该信心矩阵，可以快速帮助客户确定问题的严重性和存在的可能性，从而定位关键问题，快速解决紧要问题。



图表3 漏洞信心矩阵

2.4.3.7 图形化的定制安全规则

AppScan source edition 中有两种扫描规则，分别是模式匹配和非模式匹配（规则匹配）；前者的作用是查询指定类型文件，根据字符串匹配判断是否存在威胁，如在.sql 文件中查询到 EXECUTE 或者 EXEC 就认为存在 Access Control 类型的安全问题：这种类型的扫描规则都可以在菜单“察看”“扫描规则库”部分察看，并支持新增。如下图：



图表4 Pattern 类型的扫描规则库

另外一种扫描规则是指定对应的代码或者函数为“（易受感染的）接收器(Sink)“或者“（感染）源 (Source)”; 并且选择该问题对应的漏洞类型。然后在扫描过程中，AppScan source edition 分析从



“(感染)源”到“接收器”之间的数据流，如果没有发现有效的安全验证调用，则认为存在这种类型的安全问题。



图表5 指定方法/接口 对应的规则类型

2.4.3.8 在开发工具中进行安全测试：和开发工具集成工作

AppScan Source 可以和 Eclipse、Security Application Developer、Visual Studio 等主流开发工具集成，因此方便开发人员在日常开发中顾及应用安全。安全分析人员将扫描发现的安全隐患进行某种归类，创建出不同的 Bundle（问题包），将这些问题包给到开发人员。开发人员在集成好 AppScan Source for Developer 或 AppScan Source for Remediation 的开发环境中，可以直接打开该 Bundle（问题包）。如下图所示为将 AppScan Source for Developer 和 Security Application Developer 的集成。

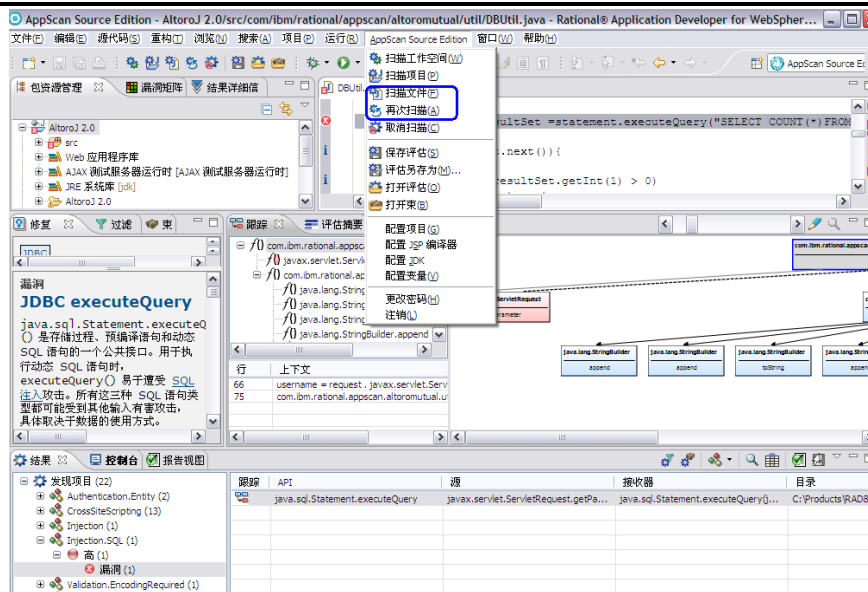


图6 AppScan 和开发工具 Security Application Developer 的集成

2.4.3.9 系统的报告归档和汇总分析

扫描结束以后,可以把报告上传到专业的应用安全报告平台,其是一个基于 WEB 的应用安全管理报告系统;可以专业化地进行报告的汇总,合并,趋势分析等,从而集中管理报告和专业化的展现;并可以产生多种合规性报告和行业标准的报告。

相关项目人员不需要安装任何工具,只要打开浏览器,访问 AppScan 企业版的页面,即可直接察看安全扫描结果等。

2.4.3.10 支持和 WEB 应用安全扫描工具结果关联分析

IBM Security 提供全面的应用安全测试解决方案,其中 AppScan Source edition 专注在代码级别的安全测试,即“白盒/静态”测试;同时, AppScan standard edition 和 AppScan enterprise edition 都可以提供针对 WEB 应用的安全测试,即“黑盒”的动态测试;这两种测试方案各有特点,而我们可以通过汇总这两种类型的测试结果,进而进行关联性分析,从而互为补充,通过黑盒准确定位问题,进而到在 AppScan source edition 中看到问题具体存在的代码行,根据修改建议快速修改问题。

2.4.3.11 全面化的中文支持

AppScan 系列产品,从界面到帮助文档,安装手册,全面提供中文版本,本土化的支持体现了产品的价值,更方便了客户的使用。



2.4.3.12 移动应用支持

AppScan Source 可支持 Android 及 iOS(iPhone 和 iPad)上的 Native APP 扫描。



第3章 IBM 方案优势

➤ 真正的企业级架构应用安全平台

Security AppScan 企业版具有基于 Web 的架构，通过分布式部署，可以将同一套平台提供给开发、测试以及运维多个部门使用，帮助组织明确各部门的安全测试责任。经过多个部门的多次扫描、修复和验证后，极大的提升了 web 应用系统的安全性。强大的分布式部署能力保障了应用扫描的准确性、快速性。

➤ 最有效率的检测系统

AppScan 企业版可以帮助客户在一个复杂的 Web 站点上，同时扫描和测试成千上万个 URL 或应用程序，并能根据更改频繁重新测试。通过扩展 Agent 的个数，配置多台机器（Agent）扫描一个复杂、大型的 web 应用，大大缩短开发、测试以及运维各个环节中的 web 漏洞全面扫描的时间，从而使得定期漏洞扫描可以每月、每周、每天进行一次。

➤ 最为全面的规则库

作为安全工具的核心能力，AppScan 拥有业界公认的最为全面强大的漏洞扫描能力。在加入 IBM 之后，结合 IBM 强大的技术力量，Security 的技术团队维护了最全面的规则库，也提供了业界最快的漏洞库更新频率。所有的这些都是保障 Security 客户的基石。

➤ 不仅仅发现问题，更注重解决问题

AppScan 不仅仅发现问题，更聚焦在如何解决问题。基于 Web 的报告控制台，可提供对安全报告基于角色的访问，并能促进整个组织的交流。通过 AppScan 内置的漏洞管理流程，可以跟踪漏洞的状态，如 open、in progress、closed 等状态。当漏洞被扫描出来后，可以通过该流程分配给开发人员进行修复，并提交测试人员进行测试，从而实现了 web 漏洞“扫描-修复-测试-验证”的全生命周期的管理。另外，AppScan 企业版还提供了邮件通知等功能，实现了客户内部开发、测试以及运维各部门间的及时通知和沟通。

另外，针对不同开发语言，AppScan 还提供了解决建议（包括.net，J2EE 等），这也是业界独一无二的。

➤ 强大的报告分析能力

AppScan 还提供了一系列报告功能，包括合规性检查，可以检查 40 多种国际行业标准和法规；能够提供给开发人员详细的漏洞测试报告，包括了测试用例的执行过程数据；提供给各个管



理人员统计分析报告，可以比对不同部门、不同应用漏洞发现的情况、趋势、分布；等等。企业不同角色人员都可以定义 dashboard，极大的加强了安全管理能力。

➤ 最可靠的安全平台

基于角色的权限控制，确保了不同人员只能查看权限范围内的漏洞结果和报告，避免了应用漏洞信息的外泄，避免了对生产环境的应用安全造成影响。同时，通过权限控制，可以有效隔离开发、测试以及运维三个部门，使得三个部门责权分明，互不影响；同时，也能够相互验证，提升 web 应用的安全性。作为安全负责人，则可以同时查看三个部门的工作结果，并进行对比、趋势分析，从而有效的管理各部门的工作结果和效率。

➤ 在线漏洞攻击培训，提升安全防范水平

内置的在线 web 漏洞培训指导，阐述了每个漏洞的详细形成原理、过程，并演示了验证、修复等内容，从而可以帮助客户的技术人员促进对漏洞的理解和交流，提升组织的安全防范能力和水平。



第4章 为什么选择 IBM

IBM Security AppScan 在市场占有率、产品发展、技术支持方面都占有很大优势，并有三方评测结果得以验证。

市场占有率

AppScan 在被收购到 IBM 之前就是安全脆弱性评估市场的领头羊，占有全球份额的 30%。在加入 Security 产品线之后，借助 IBM 的力量市场占有率更高。

产品发展

AppScan 在 2008 年后得到更大的发展，Security 强大的开发力量保障了产品的稳定发展。多个版本的更新更是最大化的加强了产品的可用性。同时 AppScan 陆续推出了开发人员、构建人员版本，丰富了整个产品线

技术支持

Security 目前在国内的研发、测试、售前、售后、销售队伍超过了 300 人。我们不仅仅关注产品的市场推广，更关注于国内客户的实施应用。

第三方评测

下面是一些第三方机构的评测结论：

- 1) IDC 报告：2007~2011 年市场第一名是 AppScan

IDC #207658 :Worldwide Security and Vulnerability Management Software 2007-2011 Forecast and Analysis ——The No1 is IBM Security AppScan

- 2) IDC 信息安全产品研究总监评论：...AppScan 在十年间一直是市场领导产品...

.....from nearly a decade, AppScan has been at the forefront of the market with technologically advanced solutions, and as the market's leading product.

——Charles Kolodgy, Research Director, Secure Content and Threat Management Products, IDC 2008

- 3) Information week web2.0 安全调研报告：...强烈推荐 web2.0 时代关注安全的公司采用 AppScan.....

AppScan was a no-brainer for the Editor's Choice award. Not only was it the only entry to fulfill the original purpose of the review—Ajax scanning—it met or exceeded the



best features of all the other products without any of the accompanying problems. We recommend it for any company concerned about Web 2.0 security.