对Web资产实施策略保护以实现业务目标

Rational. software

IBM

IBM Rational AppScan生命周期解决方案：在软件和系统交付中确保Web应用程序安全性

在线攻击是否让您的业务暴露在风险中?

如今，许多公司依赖基于Web的软件和系统运营其业务流程、与供应商进行交易、向客户提供更加成熟的服务。 在一个治理结构良好的组织中，于在线部署的每个应用程序上构建安全性应该是软件和系统交付业务流程的一部分。 不幸的是，为了保持竞争能力的领先地位，许多公司对此漠不关心，而只是不断地加快新产品的面市速度。 结果，这些漏洞让黑客得以轻松访问或偷窃公司个人数据，可能导致整个公司处于风险之中。

IBM Rational® AppScan® 是一套行业领先的Web应用程序安全解决方案，为组织提供了必要的可见性和控制能力以解决这一关键问题。 该套件包括：

- IBM Rational AppScan Standard Edition(可作为桌面应用程序或软件即服务 [SaaS]使用)。
- IBM Rational AppScan Tester Edition(可作为桌面应用程序使用)。
- IBM Rational AppScan Enterprise Edition(可用于基于Web的解决方案或SaaS)。

这些全面的解决方案都能提供扫描、报告和修复建议，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。

与IBM Rational Software Delivery Platform的其他生命周期解决方案一样，Rational AppScan产品让用户在类似的技术环境中工作，并能与领先的QA工具和集成的开发环境(IDE)几乎无缝地集成。该应用程序允许您执行连续安全审核，帮助软件开发团队一步步在Web应用程序中构建安全性，甚至能在部署应用程序之前帮助转移业务风险。

保护基于Web的关键业务资产

Rational AppScan Standard、Rational AppScan Tester和Rational AppScan Enterprise解决方案提供了全面的安全性，能覆盖复杂的Web站点，解决方案扫描并测试常见的Web应用程序漏洞，包括Web Application Security Consortium(WASC)威胁分类标识的那些漏洞。Rational AppScan解决方案使用功能更加强大、更加灵活的核心功能，以提供健壮的应用程序扫描，覆盖了最新的Web 2.0技术，包括增强了对Flash和Java™ Script语言的支持，以及对Ajax编程语言(包括专门针对JavaScript Object Notation [JSON]和Web服务参数的测试)的全面支持。

Rational AppScan针对扫描有效性和易用性的核心功能包括：

- 用户界面带有应用程序树视图选择器、分层安全结果列表，开发人员修改视图和细节面板。
- 灵活的测试过程，允许分析应用程序参数，允许仅选择相关的测试，而不影响开发过程。
- 复杂的验证支持，允许对Web应用程序执行多步骤验证流程，包括全自动区分计算机和人类的图灵测试(Completely Automated Public Turing Test to Tell Computers and Humans Apart，CAPTCHA)分布验证、多因素验证(multifactor authentication)、一次性密码、通用串行总线(USB)秘钥、智能卡和相互验证。
- 先进的会话管理，必要时可执行自动重登录。
- 实时结果视图，允许用户在扫描完成前对问题执行操作。
- 模式搜索法则，方便围绕信用卡、社会保障或其他数列的安全测试。

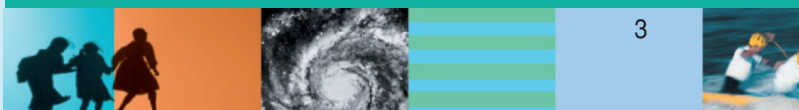
IBM Rational AppScan 安全顾问视图

Rational AppScan自定义和控件的核心功能包括：

- Rational AppScan extensions Framework技术，使用户能够创建、分享、加载强大的插件扩展测试功能。
- Pyscan和Rational AppScan的组合，具有Python脚本功能，允许用户不受用户界面的限制利用扫描能力。能够实现安全专家和入侵测试人员从未能实现的自定义。
- Rational AppScan软件开发套件(SDK)，提供调用动作的能力，从执行长时间扫描到提交定制测试。SDK界面的设计易于集成，支持自定义扫描引擎支持，还支持Rational AppScan extensions Framework和Pyscan选项。

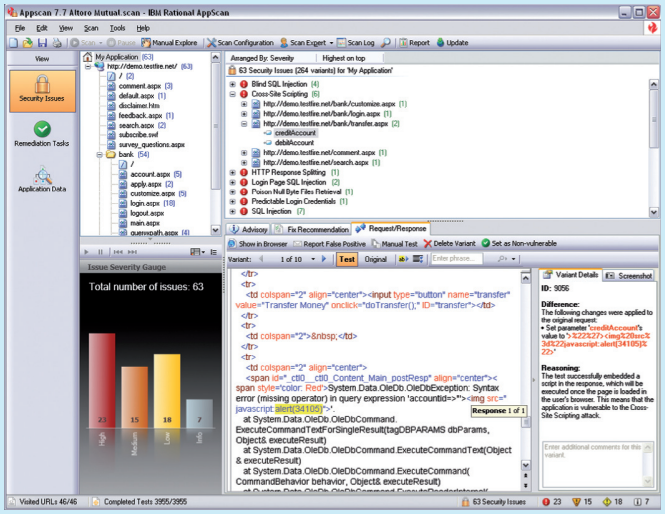
Rational AppScan漏洞检测的核心功能包括：

- 全面的有效性测试，分析非故意触发问题、Secure Sockets Layer(SSL)测试(测试 SSL 证书有效性)、跨站点伪造请求测试(cross-site request forgery，CSRF)的相应。
- 黑客模拟覆盖了Open Web Application Security Proje-ct (OWASP)的前10项和System Administration, Networking, and Security Institute (SANS)的前20项漏洞。
- 最新的威胁信息，启动Rational AppScan产品时自动更新。
- 捆绑的可用性套件，帮助入侵测试人员和安全咨询人员开发、测试和调试Web应用程序。

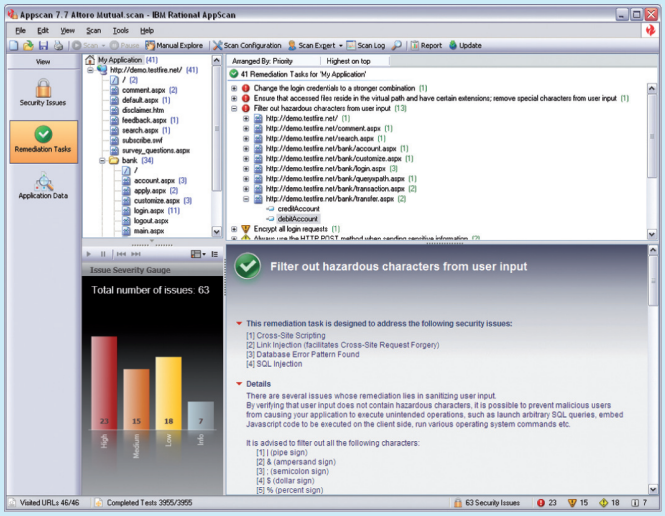


Rational AppScan报告和补救的核心功能包括：

- 与40多个全球法规遵从性和标准有关的测试，包括：National Institute of Standards and Technology Special Publication(NIST SP)800-53和OWASP的前10项(2007年更新)。Rational AppScan Version 7.7还包括Family Education Rights和Privacy Act(FERPA)、Freedom of Information and Protection of Privacy Act(FIPPA)和Payment Application Best Practices(PABP)。
- 针对HTML代码的有效性高亮显示，包括漏洞和对问题的解释。其他功能还可以显示修改后的HTML代码。
- 补救报告包括Hypertext Preprocessor(PHP)修复建议和开发人员人物列表。这些报告还允许查看与应用程序有关的问题以及体系结构问题，并能删除变量并标记为not vulnerable以供将来查看。
- 详细的可疑内容报告可以列出HTML注释中的敏感数据以及与可疑内容有关的HTTP活动。
- 测试描述包括数据库常见漏洞和漏洞(CVE)的ID。
- 还能够将Rational AppScan内置浏览器的屏幕截图合并到报表中，能够提取、压缩、加密特定的电子邮件测试的非私有信息。Rational AppScan软件还允许您向IBM Rational AppScan安全研究团队报告错误事件，这将有助于提高产品的准确性。



IBM Rational AppScan问题视图



IBM Rational AppScan补救视图

使用Rational AppScan Standard Edition软件进行产品安全审核和产品监控

安全审核人员和入侵测试人员的自动Web应用程序测试需要高级智能扫描技术。Rational AppScan Standard Edition包括：专门为支持中高级用户设计的特殊功能。这些功能包括：

- **扫描专家** 基于最佳实践提供扫描创建和设置指南，包括使用其他工具。用户可以授权预扫描，以熟悉目标应用程序并得到成功扫描所需的建议。
- **状态诱导器** 扫描和测试复杂的业务流程，比如多步骤在线购物和跟踪，并在整个过程中维护参数值和 cookies。
- **预定义的扫描模版** 允许用户快速选择和启动配置选项。
- **快速扫描配置向导** 引导用户进行重要设置、通过代理/平台验证和内部会话检测信息的各种条件步骤。
- **新的请求/响应选项卡** 提供语法高亮显示、请求/响应、收起/展开、即时搜索和其他右键单击选项。
- 基于Microsoft® Word模版的报告，用于设计遵守公司标准的定制格式。模版具有一个内容表格，扫描启动和结束时间以及各种图片。
- 内嵌的基于Web的培训 (WBT) 模块，帮助解释问题并演示开发、结果验证等，以帮助促进对漏洞的理解和交流。

使用Rational AppScan Tester Edition软件将安全测试作为质量管理的一部分

Rational AppScan Tester Edition提供各种功能，帮助QA团队在现有的安全管理过程中集成安全测试，从而减轻了安全专家的负担。

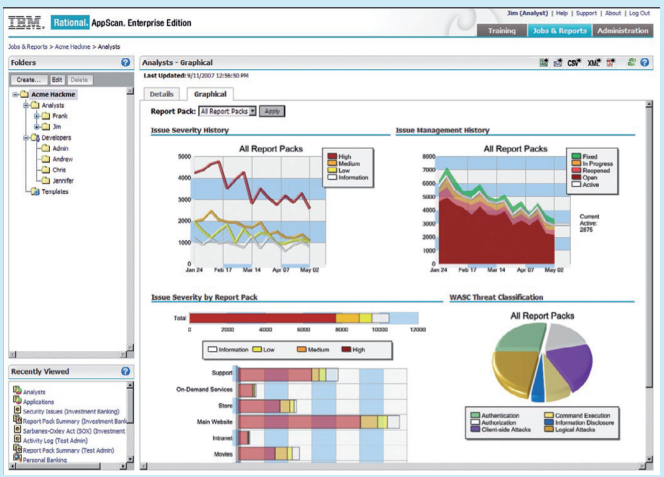
由于它集成了现有的测试系统，所以QA专家可以使用Rational AppScan功能测试脚本、在熟悉的测试环境中执行安全检查、促进安全测试的采用以及功能和性能测试。

使用Rational AppScan Enterprise Edition软件在整个企业扩展应用程序安全测试

Rational AppScan Enterprise Edition软件具有基于Web的架构，这种设计能帮助组织确定多个相关人各自的安全测试责任，帮助用户在Web应用程序交付周期内轻松发现漏洞，同时能轻松有效的进行修复。

除了集中管理的便捷和可扩展外，Rational AppScan Enterprise Edition还能够：

- 在一个复杂的Web站点上同时扫描和测试成千上万个应用程序，并能根据更改频繁重新测试。
- 提供一个简单的快速扫描测试工具，执行管理员为开发人员和其他非安全专家定义的扫描模版，无需桌面。
- 提供一个中心存储数据库，能自动存储和集合测试结果，供整个企业范围内的访问和生成多个视图。用户可以根据业务单元、地理位置和第三方提供者分割漏洞并分析趋势。
- 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。用户可以过滤或优先处理某些问题并指定其状态：open、in progress还是closed。
- 管理人员指示板和δ分析高亮显示两次扫描的变化，包括修复的、挂起的和最新的安全问题。
- Centralized controls for monitoring and controlling集中式控件用于监控和控制整个组织的Web应用程序漏洞测试。
- 内嵌的WBT模型解释问题，并演示开发、结果验证等，以帮助促进对漏洞的理解和交流。



IBM Rational AppScan Enterprise Edition指示板视图

Rational AppScan Standard和Rational AppScan Enterprise功能可作为SaaS

通过作为管理服务访问Rational AppScan功能，您可以利用产品的优势，而无需额外的员工和硬件。

一流的安全环境

这些服务重点保护操作环境，它们是使用一流的安全工具和技术构建的。

拥有了专门的安全性和遵从性专家

Rational AppScan Standard或Rational AppScan Enterprise客户可以雇用IBM Rational security分析师帮助您：

- 配置和调优扫描，帮助确定涵盖了每个应用程序。
- 检查和分析结果，帮助减少错误、确定模式、优先处理关键问题、确定关键补救任务。
- 跟踪补救过程，维护趋势数据、跟踪解析每次扫描的关键问题、报告补救效果。
- 训练QA职员在整个Web应用程序交付周期使用Rational AppScan，帮助一步步在应用程序中构建安全和遵从性管理体系。

通过基于Web的培训解决组织的安全和遵从性管理问题

该IBM Rational AppScan产品家族包括基于Web的培训、基于经验丰富的专家的在线自助式培训、从复杂的Web环境客户部署实践中总结的最佳实践。除了基本的产品介绍外，该服务还为开发人员、QA团队和安全专家提供有针对性的建议。

该服务模块每15分钟便提交一次并进行归档，用户可从任何地方在任何时间进行访问。在特定的专家实验时间，用于还可以通过Rational AppScan访问实时向导。

整个指导过程有三个级别的产品知识证书测试，管理员可以通过在线管理指示板或者Rational AppScan Enterprise Edition中的指示板跟踪员工的学习过程。

系统要求

处理器	Intel® Pentium® P4, 1.5GHz (建议2.4GHz)
内存	512MB RAM (1GB recommended for scanning large)
硬盘空间	1GB (10GB recommended for scanning large sites)
网络	One 10Mbps Network Interface Card)NIC) for network commu®nication with configured TCP/IP (100 Mbps recommended)
操作系统	Microsoft Windows® XP、Windows 2000、Windows 2003 Enterprise Edition、Windows Vista
® Web 浏览器	Microsoft Internet Explorer 5.5 or higher (6.0 or higher recommended)
	Microsoft NET框架 2.0，或更高版本
	Java Runtime Environment (JRE) 5.0 (for Rational AppScan HTTP proxy only)

了解更多信息

要了解IBM Rational AppScan产品的更多信息，请联系IBM销售代表或IBM Business Partner，或者访问：

ibm.com/software/rational/offerings/testing/webapplicationsecurity

WSD1 4001-USEN-00