Strategischer Schutz für Webressourcen
zur Unterstützung Ihrer Geschäftsziele

Rational. software

Die IBM Rational AppScan-Lifecycle-Lösung: Sicherheit für Webanwendungen bei der Software- und Systembereitstellung

Stellen Sicherheitslücken in Onlineanwendungen ein Risiko für Ihr Unternehmen dar?

Eine Vielzahl von Unternehmen nutzt heute webbasierte Software und Systeme für ihre Geschäftsprozesse, für die Transaktionen mit Lieferanten und für die Bereitstellung innovativer Services für ihre Kunden. In einem effizient geführten Unternehmen sollte deshalb bei der Bereitstellung von Software und Systemen dringend darauf geachtet werden, dass alle Anwendungen, die online implementiert werden sollen, mit den erforderlichen Sicherheitsmechanismen ausgestattet sind. Bedauerlicherweise sind viele Unternehmen aber so auf die Behauptung ihrer Wettbewerbsposition und die rasche Einführung neuer Produkte konzentriert, dass sie es versäumen, sich ernsthaft um die bestehenden Sicherheitsrisiken zu kümmern. Die dadurch entstehenden Sicherheitslücken bieten aber Hackern vielfältige Möglichkeiten, auf Unternehmensinformationen oder personenbezogene Daten zuzugreifen – mit den entsprechenden Risiken für das gesamte Unternehmen.

IBM Rational AppScan bietet hier eine Suite mit führenden Sicherheitslösungen für Webanwendungen, die Unternehmen die erforderliche Transparenz und die entsprechenden Kontrollmechanismen zur Verfügung stellt. Die Suite umfasst folgende Produkte:

- **IBM Rational AppScan Standard Edition** *(als Desktopanwendung oder „Software as a Service" (SaaS) erhältlich).*
- **IBM Rational AppScan Tester Edition** *(als Desktopanwendung erhältlich).*
- **IBM Rational AppScan Enterprise Edition** *(als webbasierte Lösung oder als SaaS erhältlich).*

Jede dieser umfassenden Lösungen bietet Empfehlungen für das Scannen, die Berichterstellung und Programmkorrektur und eignet sich für alle Arten von Sicherheitstests durch unterschiedliche Benutzer, seien es Anwendungsentwickler, Qualitätssicherungsteams, Penetration Tester (die unbefugte Zugriffe simulieren), Sicherheitsprüfer oder leitende Führungskräfte.

Wie andere Lifecycle-Lösungen der IBM Rational Software Delivery Platform bieten auch die Rational AppScan-Produkte dem Benutzer die Möglichkeit, in seiner vertrauten IT-Umgebung zu arbeiten. Dies ermöglicht praktisch nahtlos den Einsatz gängiger QA-Tools und integrierter Entwicklungsumgebungen (IDEs). Die Anwendungen erlauben es, kontinuierlich Sicherheitsprüfungen durchzuführen, d. h., die Teams, die die Software bereitstellen, können die Webanwendungen von Anfang an mit den erforderlichen Sicherheitsmechanismen ausstatten und so den beschriebenen Risiken schon vor der Implementierung der Anwendungen zu begegnen.

Schutz Ihrer geschäftskritischen Webressourcen

Die Lösungen Rational AppScan Standard Edition, Rational AppScan Tester Edition und Rational AppScan Enterprise Edition bieten umfassende Sicherheitsfunktionen für komplexe Websites. Hierzu ermöglichen sie das Scannen und Testen von Webanwendungen, um gängige Sicherheitslücken zu ermitteln – unter Berücksichtigung der Risikoklassifizierung des Web Application Security Consortium (WASC). Allen Rational AppScan-Lösungen gemeinsam sind eine Reihe leistungsfähiger, flexibler Basisfunktionen für das Scannen von Anwendungen der neuesten Web 2.0-Generation. Dies schließt auch die Unterstützung von Flash und erweiterter Java™ Script-Sprachen sowie der Programmiersprache Ajax ein (einschließlich dedizierter Tests von JavaScript Object Notation (JSON) und Web-Service-Parametern).

Rational AppScan-Basisfunktionen für effiziente Scanfunktionalität und hohen Bedienungskomfort:

- *Eine Benutzeroberfläche mit wählbaren Ansichten für die Anwendungsbaumstruktur, hierarchischen Listen der gefundenen Sicherheitsprobleme, Korrekturansichten für Entwickler und diversen Detailansichten.*
- *Einen adaptiven Testprozess, der Ihnen die Möglichkeit gibt, Anwendungsparameter zu analysieren und nur relevante Tests auszuwählen, die den Entwicklungsprozess nicht beeinträchtigen.*
- *Unterstützung komplexer Authentifizierungen, sodass in mehreren Schritten ausgeführte Authentifizierungsprozeduren in Webanwendungen getestet werden können, wie z. B. gestufte CAPTCHA-Authentication (Completely Automated Public Turing Test to Tell Computers and Humans Apart), Multifactor Authentication, One-time Passwords, USB-Keys, Smart Cards und Mutual Authentication.*
- *Erweitertes Session-Management mit automatischer Wiederanmeldung (bei Bedarf).*
- *Ansichten mit Echtzeitergebnissen, die es den Benutzern ermöglichen, Probleme schon zu bearbeiten, bevor der Scanvorgang beendet ist.*
- *Suchregeln nach Mustern (Pattern), die bestimmte Sicherheitstests vereinfachen (z. B. im Zusammenhang mit Kreditkarten- oder Sozialversicherungsnummern oder anderen Ziffernfolgen).*

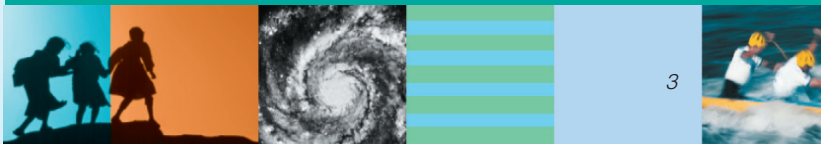
IBM Rational AppScan-Ansicht mit Sicherheitshinweisen.

Rational AppScan-Basisfunktionen zur Anpassung und Steuerung:

- *Die Rational AppScan eXtensions Framework-Technologie erlaubt es Benutzern, leistungsfähige Add-ons für erweiterte Testfunktionen zu erstellen, gemeinsam zu nutzen und zu laden.*
- *Pyscan, das Rational AppScan mit der Funktionalität von Python-Scripts kombiniert und dadurch Benutzern das Scannen ohne die Limitierung einer Benutzeroberfläche zur Verfügung stellt; dies bietet Sicherheitsspezialisten und Penetration-Testern, die unbefugte Zugriffe simulieren, völlig neue Anpassungsmöglichkeiten.*
- *Rational AppScan SDK (Software Development Kit) zum Aufrufen unterschiedlichster Aktionen – von der Ausführung langer Scanvorgänge bis zur Durchführung angepasster Tests. Die SDK-Oberflächen vereinfachen die Integration und unterstützen die bedarfsgerechte Nutzung der Scan-Engine mit Rational AppScan eXtensions Framework- und Pyscan-Optionen.*

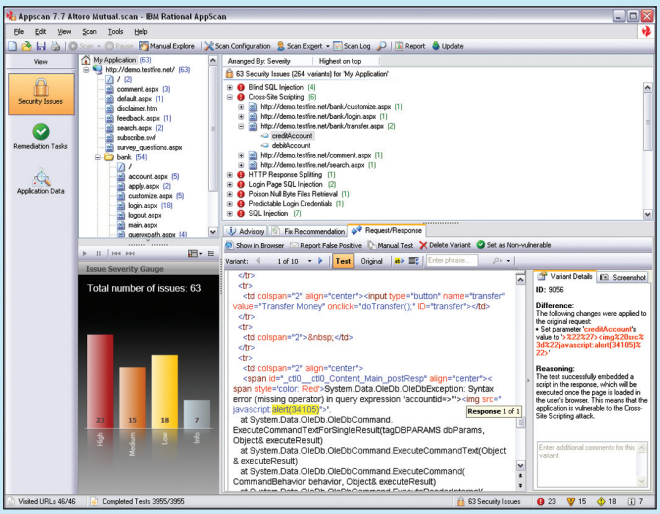
Rational AppScan-Basisfunktionen zur Erkennung von Sicherheitslücken:

- *Globale Validierung zur Analyse von Test-Responses für unbeabsichtigt verursachte Probleme, SSL-Tests (Secure Sockets Layer) zur Gültigkeitsprüfung bei SSL-Zertifikaten und CSRF-Tests (Cross-Site Request Forgery).*
- *Hackersimulationen, unter Berücksichtigung der „Top 10 Vulnerabilities“ des Open Web Application Security Project (OWASP) und der „Top 20 Vulnerabilities“ des System Administration, Networking, and Security Institute (SANS).*
- *Informationen zu den neuesten Bedrohungen, die automatisch aktualisiert werden, wenn ein Rational AppScan-Produkt gestartet wird.*
- *Ein Paket mit Dienstprogrammen, mit dem Penetration-Tester und Sicherheitsberater Webanwendungen entwickeln und testen und ein Debugging vornehmen können.*



Rational AppScan-Basisfunktionen für die Berichterstellung und Fehlerbehebung:

- *Tests in Bezug auf mehr als 40 weltweit gültige Compliance-Anforderungen und -Standards, wie z. B. National Institute of Standards und Technology Special Publication (NIST SP) 800-53 und die „Top 10" von OWASP (aktualisiert im Jahr 2007); Rational AppScan deckt in Version 7.7 des Weiteren verschiedene gesetzliche Standards in den USA ab, wie z. B. Family Education Rights and Privacy Act (FERPA), Freedom of Information and Protection of Privacy Act (FIPPA) und Payment Application Best Practices (PABP).*
- *Hervorhebungsfunktion für die Validierung zur Kennzeichnung von HTML-Code mit Sicherheitslücken (einschließlich Erläuterungen zu dem Problem); eine Vergleichsfunktion zeigt den geänderten HTML-Code an.*
- *Berichte zur Fehlerhebung, die Korrekturempfehlungen zu Hypertext Preprocessor (PHP) und Listen mit Aufgabenstellungen für Entwickler enthalten. Die Berichte geben Ihnen auch die Möglichkeit, anwendungsbezogene oder infrastrukturelle Problemstellungen (oder beides) anzuzeigen, Varianten zu löschen oder sie als* **nicht anfällig** *zu markieren und erst später wieder zu prüfen.*
- *Detaillierte Berichte zu verdächtigen Inhalten, in denen z. B. sensible Daten in HTML-Kommentaren oder HTTP-Aktivitäten im Zusammenhang mit verdächtigen Inhalten aufgezeichnet sind.*
- *Testbeschreibungen mit IDs gängiger Sicherheitslücken und Bedrohungen (Common Vulnerabilities and Exposures, CVEs) aus der Datenbank, in der die Sicherheitslücken verzeichnet sind.*
- *Möglichkeit, Screenshots aus dem internen Browser von Rational AppScan in Berichte zu integrieren und nicht proprietäre Informationen aus bestimmten Tests für den E-Mail-Versand zu extrahieren, zu komprimieren und zu verschlüsseln; Rational AppScan bietet außerdem die Möglichkeit, Fehlalarme (False Positives und False Negatives) an das IBM Rational AppScan-Sicherheitsteam zu melden, um die Treffergenauigkeit des Produkts ständig zu erhöhen.*



IBM Rational AppScan-Ansicht für Sicherheitsprobleme.

IBM Rational AppScan-Ansicht für die Fehlerbehebung.

Sicherheitsprüfungen und Überwachung des Produktionsbetriebs mit Rational AppScan Standard Edition-Software

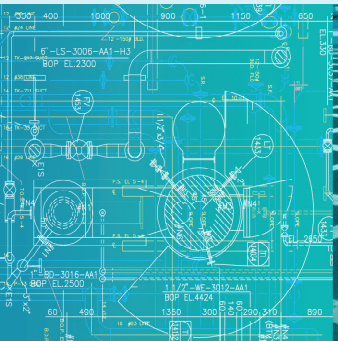
Die Automatisierung von Webanwendungstests für Sicherheitsprüfer und Penetration-Tester erfordert hoch entwickelte, intelligente Scanning-Technologien. Rational AppScan Standard Edition enthält spezielle Funktionen für Benutzer mit durchschnittlichen und sehr hohen Anforderungen. Folgende Funktionen sind enthalten:

- *Der Scan Expert, der Benutzer bei der Erstellung und Einrichtung von Scans mit Best-Practices-Verfahren unterstützt (einschließlich der Verwendung zusätzlicher Tools); Benutzer können einen Prescan durchführen, der die Zielanwendung beschreibt und Aktionen empfiehlt, die für einen erfolgreichen Scanvorgang erforderlich sind.*
- *Der State Inducer, der komplexe Geschäftsprozesse scannt und testet (wie z. B. Online-Shopping und -Tracking in mehreren Schritten) und der dabei Parameterwerte und Cookies verwaltet.*
- *Vordefinierte Scanvorlagen (Scan Templates), mit denen die Benutzer Konfigurationsoptionen in kürzester Zeit auswählen und starten können.*
- *Ein Assistent zur raschen Scankonfiguration, der den Benutzer bei wichtigen Einstellungen und bedingten Prozessschritten für die Proxy-/Plattformauthentifizierung und Session-interne Erkennungsinformationen unterstützt.*
- *Neue Request/Response-Tabs, die Syntaxhervorhebung, Request/Response, Ein-/Ausblenden, Sofortsuche (As-you-type Search) und zusätzliche Rechtsklickoptionen bieten.*
- *Auf Microsoft® Word-Vorlagen basierende Berichte für den Entwurf von angepassten Formaten, die den Unternehmensstandards entsprechen; Vorlagen enthalten ein Inhaltsverzeichnis, den Anfangs- und Endzeitpunkt des Scanvorgangs sowie Grafiken.*
- *Integrierte WBT-Module (Web-based Training), die die Problemstellungen erläutern und den Nutzen demonstrieren (einschließlich der Verifizierung der Ergebnisse), um das Verstehen und Kommunizieren der Sicherheitslücken zu vereinfachen.*

Integration der Sicherheitstests in das Qualitätsmanagementprogramm – mit Hilfe der Rational AppScan Tester Edition-Software

Durch die Funktionalität von Rational AppScan Tester Edition können QA-Teams die Sicherheitstests in die bestehenden Qualitätsmanagementprogramme integrieren, wodurch die für die IT-Sicherheit zuständigen Mitarbeiter deutlich entlastet werden.

Da das Produkt zusammen mit führenden Testsystemen eingesetzt werden kann, haben die QA-Mitarbeiter die Möglichkeit, Rational AppScan-Funktionen in Testscripts zu verwenden. So können Sicherheitsprüfungen in der vertrauten Testumgebung vorgenommen werden, was die Ausführung zusammen mit Funktions- und Leistungstests vereinfacht.



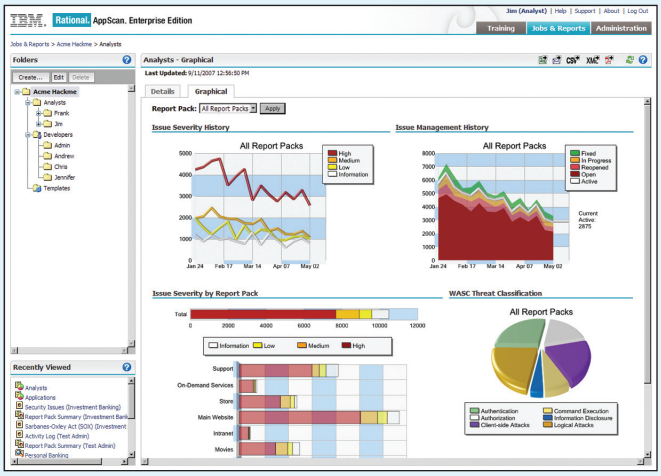


Skalierung von Anwendungssicherheitstests im gesamten Unternehmen mit Rational AppScan Enterprise Edition-Software

Die webbasierte Architektur von Rational AppScan Enterprise Edition gibt Unternehmen die Möglichkeit, die Verantwortlichkeit für Sicherheitstests unter mehreren Beteiligten zu verteilen und die Benutzer dabei zu unterstützen, Sicherheitslücken schon früh im Bereitstellungszyklus von Webanwendungen aufzuspüren – also dann, wenn diese Lücken noch einfach und ohne großen Kostenaufwand beseitigt werden können.

Neben dem Komfort und den Erweiterungsmöglichkeiten der zentralen Verwaltung bietet Rational AppScan Enterprise Edition folgende Vorteile:

- *Funktionalität, bei komplexen Websites mehrere Tausend Anwendungen gleichzeitig zu scannen und zu testen, sowie die Möglichkeit, nach Änderungen erneute Tests durchzuführen.*
- *Einfaches Quick-Scan-Testtool zur Ausführung von Scanvorlagen (Scan Templates), die der Administrator definiert hat; das Tool richtet sich an Entwickler und andere Mitarbeiter, die nicht zum Sicherheitsteam gehören; das Tool erfordert keine Installation oder Konfiguration auf dem Desktop.*
- *Zentrales Datenrepository, das die Testergebnisse speichert und zusammenfasst, um einen unternehmensweiten Zugriff und verschiedene Ansichten zu ermöglichen; die Benutzer können die gefundenen Sicherheitslücken nach Geschäftsbereich, Region oder Lieferant segmentieren und so Trends ermitteln.*
- *Eine webbasierte Reporting-Konsole ermöglicht einen rollenbasierten Zugriff auf Sicherheitsberichte und erleichtert die unternehmensweite Kommunikation; die Benutzer können nach Problemen filtern, priorisieren und einen Status vergeben: geöffnet, in Bearbeitung oder geschlossen.*
- *Statusansichten für Führungskräfte (Dashboards) und Deltaanalyseberichte zur Verdeutlichung der Änderungen zwischen einzelnen Scans, einschließlich korrigierter, anstehender und neuer Sicherheitsprobleme.*
- *Zentrale Überwachung und Steuerung der unternehmensweiten Tests zur Ermittlung von Sicherheitslücken bei Webanwendungen.*
- *Integrierte WBT-Module, die die Problemstellungen erläutern und den Nutzen demonstrieren (einschließlich der Verifizierung der Ergebnisse), um das Verstehen und Kommunizieren der Sicherheitslücken zu vereinfachen.*



IBM Rational AppScan Enterprise Edition-Statusansicht (Dashboard).

Rational AppScan Standard Edition und Rational AppScan Enterprise Edition als „Software as a Service“ (SaaS) verfügbar
Durch die Nutzung der Funktionen von Rational AppScan als Service, der von einem externen Anbieter betrieben wird, profitieren Sie von den Vorteilen des Produkts, ohne entsprechende Personal- und Hardwarekosten.

Technologisch ausgereifte Sicherheitsumgebung
Die Services basieren auf ausgereiften Sicherheitstools und -verfahren und verfolgen so das primäre Ziel, Ihre Betriebsumgebung zu schützen.

Ihr eigener Experte für Sicherheits- und Compliance-Fragen
Als Kunde, der Rational AppScan Standard Edition oder Rational AppScan Enterprise Edition einsetzt, können Sie einen IBM Rational-Sicherheitsanalysten damit beauftragen, Sie in folgenden Bereichen zu unterstützen:

- *Konfiguration und Optimierung von Scans, um sicherzustellen, dass alle Anwendungen unterstützt werden.*
- *Überprüfung und Analyse der Ergebnisse, um Fehlalarme (False Positives und False Negatives) nach Möglichkeit zu vermeiden, Muster zu erkennen, wichtige Probleme zu priorisieren und vorrangige Korrekturmaßnahmen hervorzuheben.*
- *Verfolgung des Korrekturprozesses durch die Pflege von Trenddaten, die Protokollierung von wichtigen Problemlösungen von Scan zu Scan und die Erstellung von Berichten zur Effektivität der Korrekturmaßnahmen.*
- *Ausbildung Ihrer QA-Mitarbeiter für den Einsatz von Rational AppScan während des gesamten Bereitstellungszyklus der Webanwendungen sowie umfassende Integration des Sicherheits- und Compliance-Managements in Ihre Anwendungen.*

Adressierung organisatorischer Probleme im Bereich des Sicherheits- und Compliance-Managements durch webbasierte Ausbildung

Die IBM Rational AppScan-Produktfamilie bietet webbasierte Schulungen, ein online verfügbares Ausbildungsprogramm zum Selbststudium, in dem Sie von jahrelangen Erfahrungen profitieren, sowie bewährte Verfahren (Best Practices), die auf der Grundlage zahlreicher praktischer Kundenimplementierungen in herausfordernden komplexen Webumgebungen entwickelt wurden. Neben grundlegenden Informationen zum Produkt umfasst der Service gezielte Beratung für Entwickler, QA-Teams und Sicherheitsspezialisten.

Die Servicemodule werden in 15-Minuten-Intervallen online bereitgestellt und dann archiviert. Der Zugriff ist jederzeit – und unabhängig vom Standort – möglich. Zu bestimmten Zeiten können die Benutzer auch die Unterstützung von Rational AppScan-Sicherheitsexperten in Anspruch nehmen – in Echtzeit.

Für drei Zertifizierungsgrade der Produktkompetenz stehen während des gesamten Ausbildungsprozesses Onlinetests zur Verfügung, und die Manager können die Lernfortschritte der Mitarbeiter über ein spezielles „Management Dashboard“ verfolgen, das online und in Rational AppScan Enterprise Edition zur Verfügung steht.

Systemvoraussetzungen

Prozessor	Intel® Pentium® P4, 1,5 GHz (2,4 GHz empfohlen)
Hauptspeicher	512 MB RAM (1 GB für das Scannen umfangreicher Sites empfohlen)
Freier Plattenspeicherplatz	1 GB (10 GB für das Scannen umfangreicher Sites empfohlen)
Netzwerk	Eine 10-Mb/s-Netzwerkkarte für TCP/IP-Netzwerkkommunikation (100 Mb/s empfohlen)
Betriebssystem	Microsoft Windows® XP, Windows 2000, Windows 2003 Enterprise Edition, Windows Vista
Web-Browser	Microsoft Internet Explorer ab Version 5.5 (6.0 oder höher empfohlen)
	Microsoft .NET Framework ab Version 2.0
	Java Runtime Environment (JRE) 5.0 (nur für Rational AppScan-HTTP-Proxy)

Weitere Informationen

Weitere Informationen zu IBM Rational AppScan-Produkten erhalten Sie bei Ihrem IBM Ansprechpartner oder IBM Business Partner oder auf folgender Website:

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

IBM Deutschland GmbH
70548 Stuttgart
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

Gedruckt in den USA
12-07

RAB14001-DEDE-00