IBM Rational AppScan-Lösungen für SAP-Sicherheit

Reduzieren Sie das Risiko durch Sicherheitslücken in Ihren geschäftskritischen Anwendungen

Highlights

- Erkennung und Beseitigung von Sicherheitslücken in SAP-Anwendungen
- Automatisierung des Tests von SAP-Webportalen mit erweiterten dynamischen Analysen (Black-Box-Analysen)
- Analyse des ABAP-Quellcodes mit statischen Analysen (White-Box-Analysen) zur Erkennung von Sicherheitsmängeln
- Integration von Sicherheitstests in die Entwicklung von SAP-Anwendungen
- Management der Anwendungssicherheit und des Risikos für Ihre implementierten SAP-Anwendungen
- Management der Einhaltung von Vorschriften wie PCI, GLBA und HIPAA

Sind SAP-Anwendungen von zentraler Bedeutung für Ihr Unternehmen, stellen Sicherheitslücken in diesen Anwendungen ein enormes Risiko für Ihre kritischsten Prozesse und vertraulichen Daten dar. Wenn Sie SAP-Lösungen für Rechnungslegung, Personalmanagement, Supply Chain Management (SCM), Customer Relationship Management (CRM) und weitere Aufgaben verwenden, benötigen Sie daher eine Lösung, die Sicherheitslücken erkennt, beseitigt und so das Risiko von Sicherheitsverletzungen und Datenverlusten reduziert.

Viele Unternehmen glauben, dass für den Schutz ihrer SAP-Lösungen die Aufgabentrennung und das Management von Zugriffsrechten entscheidend sind, da sie damit den Zugriff auf Systeme und Anwendungen auf berechtigte Benutzer beschränken können. Doch Sicherheitslücken stellen ebenfalls ein großes Risiko dar. Denn sie können für Angriffe auf Anwendungen ausgenutzt werden, die Zugriffskontrollen umgehen. Beispielsweise sind ungeprüfte Eingaben eine häufige Schwachstelle bei allen Anwendungen – auch bei SAP-Anwendungen. Sie ermöglichen SQL-Injection-Attacken, durch die Angreifer ohne Berechtigung auf Daten zugreifen und Daten erstellen, ändern oder löschen können. Stellen Sie sich vor, welche Folgen eine SQL-Injection-Attacke auf Ihre geschäftskritischen SAP-Systeme hätte, die Sie für die Rechnungslegung oder das Management von Kundendaten einsetzen.

Sicherheitslücken sind wie Qualitätsmängel: Sie kommen normalerweise in jedem Anwendungsentwicklungsprozess vor. Deshalb benötigen Unternehmen Tools und Lösungen für die Erkennung und Beseitigung dieser Sicherheitslücken im Entwicklungsprozess und während des gesamten Anwendungslebenszyklus. SAP-Anwendungen – sowohl Webportale als auch ABAP-Anwendungen (Advanced Business Application Programming) – sind mit den gleichen Sicherheitsrisiken wie die meisten anderen Anwendungen konfrontiert, wie z. B. Angriffen durch SQL Injections. Herkömmliche Lösungen für die Sicherheit von Webanwendungen können zwar SAP-Webportale schützen, doch ABAP-Anwendungen erfordern spezielles SAP-Know-how und erweiterte Sicherheitstests zur Analyse des ABAP-Quellcodes.

Erkennung und Beseitigung von Sicherheitslücken in SAP-Anwendungen

IBM Rational AppScan-Lösungen für den Test der Anwendungssicherheit automatisieren die Analyse von SAP-Anwendungen – sowohl von Webportalen als auch ABAP-Anwendungen –, um Sicherheitslücken zu finden und das Risiko für die Anwendungen zu managen. Das Rational AppScan-Portfolio beinhaltet Lösungen für Anwendungstests, die auf dynamischen und statischen Analysen sowie einer Kombination beider Methoden basieren. Diese Lösungen haben sich bereits bei den anspruchsvollsten Webanwendungen bewährt. Um eine Lösung für ABAP-Anwendungen bereitzustellen, entwickelte IBM gemeinsam mit den SAP-Sicherheitsexperten der Virtual Forge GmbH den CodeProfiler for Rational AppScan Source Edition, der erweiterte statische Analysen des ABAP-Quellcodes durchführt.

IBM Rational AppScan-Lösungen für die Sicherheit von SAP-Anwendungen kombinieren Folgendes:

- Fundierte Sicherheitsforschung
- SAP-Know-how
- Anleitungen zur Beseitigung von Sicherheitslücken
- Integration in Entwicklungsprozesse
- Application-Lifecycle-Management (ALM)
- Unternehmensweite Berichterstellung und Risikomanagement für Anwendungen

Schutz von SAP-Webportalen und SOA-Middleware

Die meisten Unternehmen sind sich des enormen Risikos bewusst, das aus potenziellen Sicherheitslücken in ihren mit dem Internet verbundenen, öffentlich zugänglichen Webanwendungen entsteht. Doch Sicherheitslücken bei internen Anwendungen und Implementierungen, z. B. SAP-Webportalen und SOA-Middleware (serviceorientierte Architektur), können aufgrund des Zwecks dieser Anwendungen ähnliche Risiken hervorbringen. Webportale und SOA-Middleware erweitern SAP-Anwendungen im gesamten Unternehmen, um mehr Mitarbeiter zu erreichen, ihnen Zugriff auf geschäftskritische Informationen zu gewähren, die Datenintegration zu unterstützen, unterschiedliche Systeme zu verbinden und vieles mehr.

Angriffe auf diese internen Anwendungen können von Insidern, die als vertrauenswürdig eingestuft werden, oder Hackern, die Sicherheitsvorkehrungen zum Schutz des Netzwerks umgehen, oder beiden initiiert werden. Webportale sind allein schon aufgrund der wichtigen Daten, die sie enthalten, und der kritischen Prozesse, die von SAP-Anwendungen ausgeführt werden, ein lohnendes Ziel für Angreifer. Die Sicherheit Ihrer SAP-Implementierung ist nur so stark wie das schwächste Glied. Bei Verbindungen zu externen Niederlassungen oder Geschäftspartnern können Sie die Sicherheit auf Endbenutzerseite häufig nicht kontrollieren.

Für den Schutz von SAP-Webportalen und SOA-Middleware sorgt das Rational AppScan-Portfolio mit dynamischen Analysen (Black-Box-Analysen), die mit der Rational AppScan Standard Edition und der Rational AppScan Enterprise Edition ausgeführt werden können. Diese Lösungen automatisieren den Test kompilierter Anwendungen, sodass Unternehmen Sicherheitstests in den Entwicklungsprozess für neue Anwendungen integrieren und bereits implementierte Anwendungen regelmäßig überprüfen können.

Die zugrunde liegende Technologie von Webportalen und SOA-Middleware in SAP-Implementierungen ist mit Nicht-SAP-Anwendungen konsistent. Somit können Kunden Rational AppScan Standard Edition oder Rational AppScan Enterprise Edition verwenden, um Sicherheitstests sowohl für SAP- als auch Nicht-SAP-Webanwendungen und SOA-Middleware zu automatisieren.

Erkennung von Sicherheitslücken im ABAP-Quellcode

Kunden mit SAP-Anwendungen setzen individuell angepasste ABAP-Programme in ihrer IT-Infrastruktur ein. Sicherheitslücken bei diesen Systemen bringen eine Reihe von Risiken mit sich. CodeProfiler for Rational AppScan Source Edition, eine Lösung für Sicherheitstests auf der Basis statischer Analysen, unterstützt Sie bei der Erkennung von Sicherheitslücken im ABAP-Quellcode, der Prüfung von Datenflüssen und der Ermittlung des Risikos für jede Ihrer SAP-Anwendungen. CodeProfiler kann bereits während der Entwicklung implementiert werden. Dadurch werden Sicherheitslücken schon vor der produktiven Einführung der Anwendungen aufgezeigt. Sicherheitstests sollten jedoch auch Produktionsanwendungen einschließen. Deshalb bietet CodeProfiler for Rational AppScan Source Edition Prüf- und Compliance-Tests, die den Verantwortlichen einen umfassenden Überblick über den gesamten Lebenszyklus der Softwareentwicklung verschaffen.

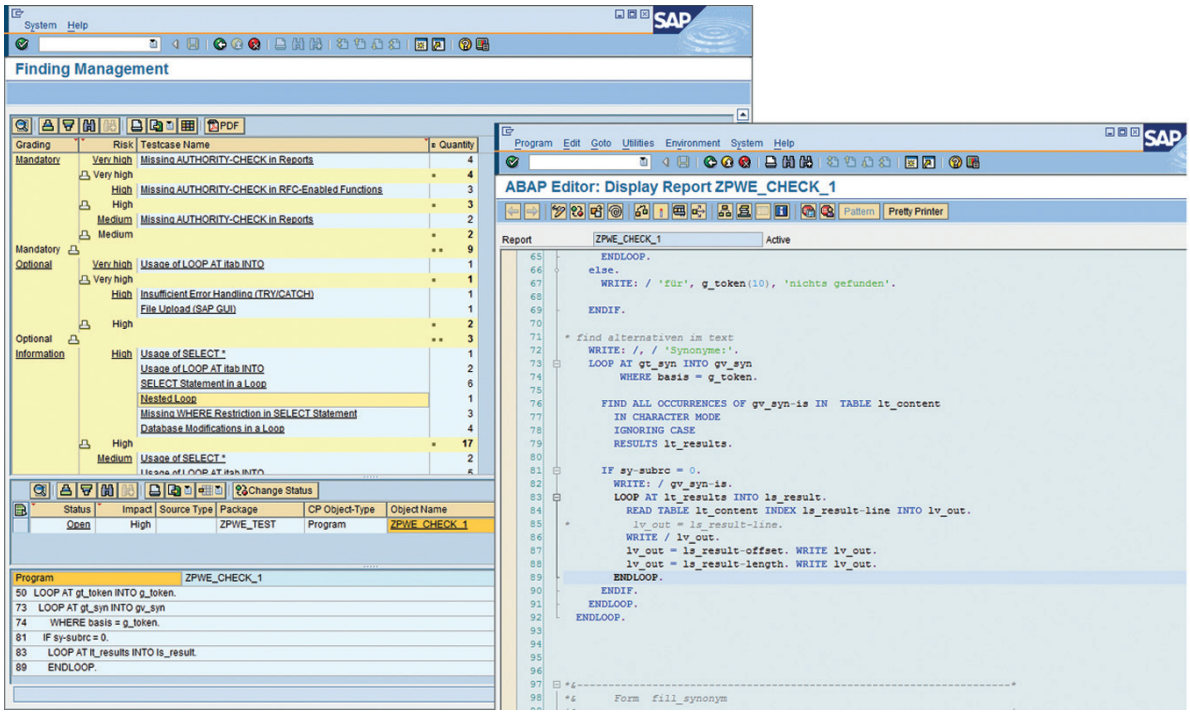
CodeProfiler for Rational AppScan Source Edition ermöglicht die Entwicklung von sicherem Code sowie zentralisierte Sicherheitstests, bevor die Anwendungen in Betrieb genommen werden. Die Lösung enthält Tools für Teamarbeit und Management, die die Zusammenarbeit zwischen den für Entwicklung und Sicherheit zuständigen Teams erleichtern.

Sichere Entwicklung in der ABAP Workbench und SAP-Benutzeroberfläche

Viele Unternehmen wissen, dass sich die Anwendungssicherheit nicht nur auf Sicherheitstests beschränken sollte, sondern dass Entwickler von Anfang an sicheren Code schreiben sollten, um sichere Anwendungen zu erstellen. Daher müssen Unternehmen zunächst ihre Entwickler in notwendigen Sicherheitsmaßnahmen schulen und ihnen dann helfen, Sicherheitslücken in ihrem Code zu erkennen und zu beseitigen. Mit CodeProfiler for Rational AppScan Source Edition können Entwickler sicheren Code schreiben und Sicherheitslücken beseitigen, für die sie verantwortlich sind – und das alles von der ABAP Workbench und SAP-Benutzeroberfläche aus.

Die ABAP Workbench und SAP-Benutzeroberfläche sind ideal für Entwickler, um Sicherheitslücken zu erkennen und sicheren Code zu erstellen, ohne dass sie ihre integrierte Entwicklungsumgebung (IDE) verlassen müssen. Da Entwickler nur selten gleichzeitig auch Sicherheitsexperten sind, bietet ihnen CodeProfiler for Rational AppScan Source Edition Folgendes:

- Methode für die schnelle Codeprüfung ohne komplexe Einrichtung und Konfiguration
- Detaillierte technische Informationen, die die Ursache der Sicherheitslücke erklären
- Erklärung des Risikos und der möglichen Folgen der Sicherheitslücke
- Anleitung zur schnelleren Beseitigung der Sicherheitslücke mit Vorschlägen zur Korrektur des Codes

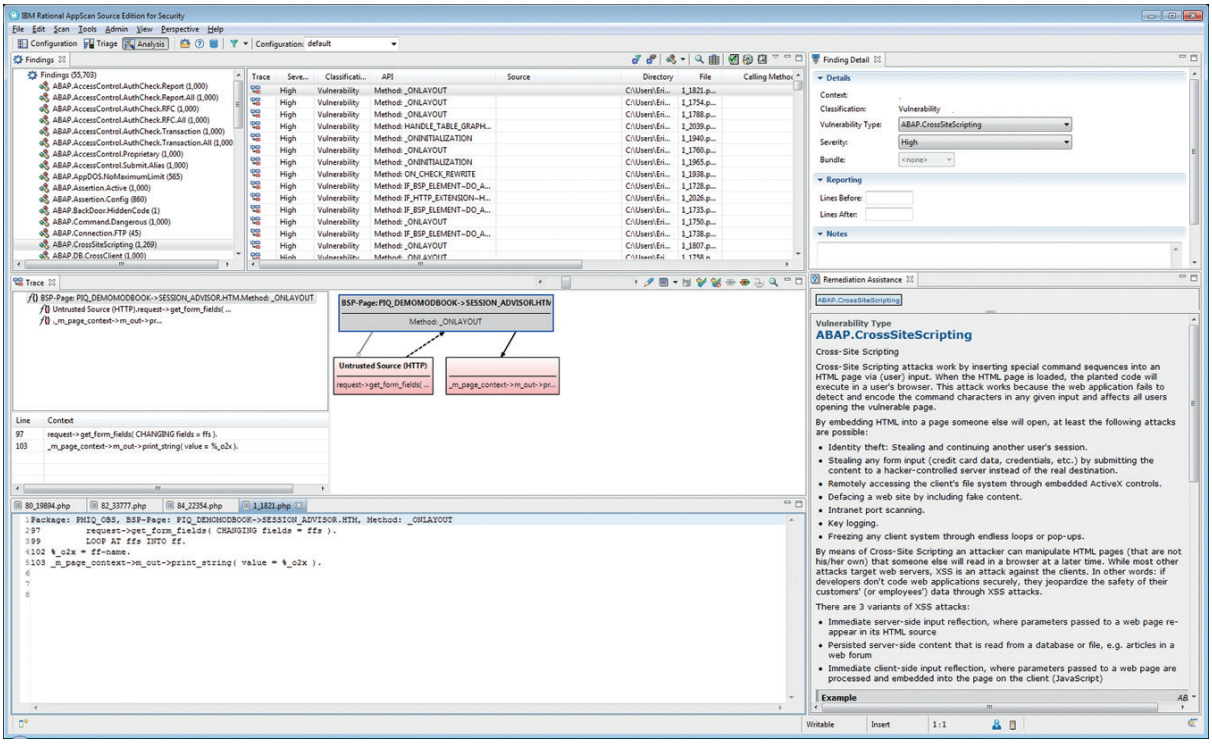


Führen Sie Prüfungen und eine Selektierung nach dem Risikograd durch – von innerhalb der SAP-Oberfläche. Jedes Problem verweist auf die exakte Codezeile im ABAP Editor.

Obwohl das Management von Sicherheitstests in der SAP-Umgebung erfolgt, werden die eigentlichen Tests außerhalb des SAP-Systems durchgeführt, um die Auswirkungen auf die Leistung zu minimieren. Der Code wird – für den Benutzer nicht sichtbar – mittels Remote Function Call aus dem System extrahiert und auf einem dedizierten Virtual Forge CodeProfiler-System überprüft.

Durchsetzung von Service-Level-Agreements und Überprüfung des Codes Dritter

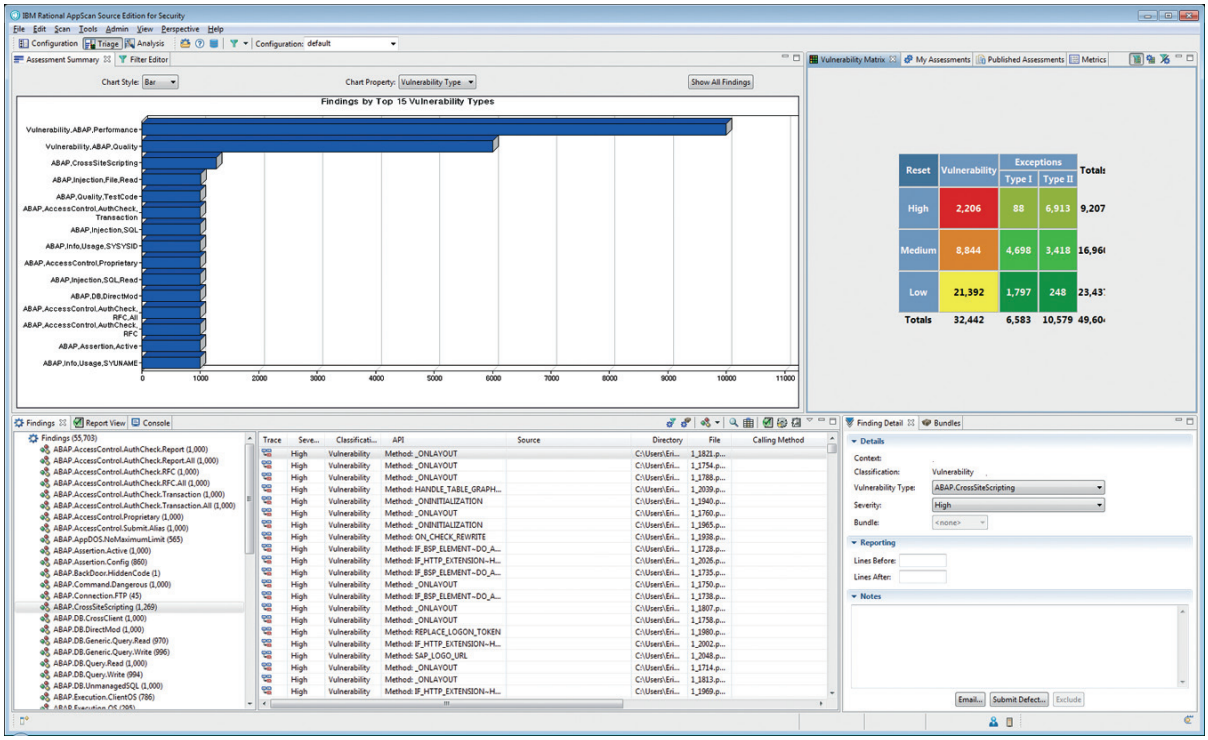
Viele Unternehmen übertragen die Entwicklung ihrer SAP-Anwendungen im Rahmen von Outsourcing-Vereinbarungen an externe Provider. Das Rational AppScan-Softwareportfolio und CodeProfiler for Rational AppScan Source Edition unterstützen diese Unternehmen bei der Durchsetzung von Service-Level-Agreements (SLAs) im Rahmen des Managements der Sicherheitsanforderungen für ABAP- und Webanwendungen. Jetzt, da Unternehmen eine Möglichkeit zur Durchsetzung von Sicherheitsanforderungen haben, können sie Sicherheitsspezifikationen in die Ausschreibung für Outsourcing-Entwicklungsprojekte aufnehmen. Mit dem Rational AppScan-Portfolio und CodeProfiler for Rational AppScan Source Edition können Unternehmen automatisch verifizieren, dass diese Anforderungen erfüllt werden, und so ungeplante und zeitaufwendige Änderungsanforderungen vermeiden.



Zentralisieren Sie das Risikomanagement und Sicherheitstests für SAP und alle übrigen Anwendungen. Analysieren, selektieren und managen Sie ABAP-Sicherheitslücken, die der CodeProfiler for AppScan Source Edition festgestellt hat.

Integration der SAP-Sicherheit in das Risikomanagement für Anwendungen

Viele für die Anwendungssicherheit zuständigen Teams führen nicht nur jährliche Prüfungen und Tests vor der Einführung von Anwendungen in der Produktionsumgebung durch, sondern wenden auch bewährte Verfahren für das Risikomanagement für Anwendungen an. Zum Rational AppScan-Portfolio gehört auch die Rational AppScan Enterprise Edition-Plattform, die das mit Sicherheitslücken bei Anwendungen verbundene Risiko für das Unternehmen ermitteln, überwachen und reduzieren kann. In Verbindung mit CodeProfiler for Rational AppScan Source Edition können jetzt ABAP-Anwendungen in die unternehmensweite Sicht des Anwendungsrisikos einbezogen werden. Sicherheitsverantwortliche und -prüfer profitieren von mehr als 40 in die Software integrierten Compliance-Berichten und Trendanalysen, die nützlich für die Messung und Reduzierung des Risikos bei Anwendungen sind.



AppScan-Lösungen liefern genaue Ereignisdetails mit Problembeschreibungen, die das jeweilige Risiko hervorheben, auf die exakte Codezeile verweisen und eine Lösung empfehlen.

Zusammenarbeit mit Entwicklerteams

In vielen Unternehmen sind Tests der Anwendungssicherheit Teil eines größeren Bereichs des Application-Lifecycle-Managements. Unternehmen wünschen sich bessere Transparenz, Kontrolle und Automatisierung im Lebenszyklus der Softwareentwicklung, sowohl für SAP- als auch Nicht-SAP-Systeme. Mit IBM Rational erhalten sie bewährte Lösungen für den gesamten Softwareentwicklungszyklus.

Virtual Forge CodeProfiler for Rational AppScan Source Edition und das AppScan-Portfolio können wesentliche Bestandteile des Application-Lifecycle-Managements für SAP- und Nicht-SAP-Systeme sein. Der mit der AppScan Enterprise Edition kombinierte Virtual Forge CodeProfiler bietet Sicherheitsteams die Möglichkeit, ihre Maßnahmen auf andere Aspekte des Softwarelebenszyklus abzustimmen.

Mit Rational-Lösungen können Kunden die Softwarebereitstellung und Automatisierung für SAP- und Nicht-SAP-Umgebungen noch besser integrieren, um folgende Aufgaben zu meistern:

- Definition, Visualisierung und Verbesserung der Rückverfolgbarkeit von SAP-Anforderungsprozessen und Assets in allen Anwendungsumgebungen des Unternehmens mit Rational-Lösungen für das Anforderungsmanagement
- Priorisierung von geschäftskritischen Änderungen und Optimierung der Ressourcenauslastung bei Standardsoftware, traditionellen und selbst entwickelten Anwendungen mit Rational-Lösungen für das Change-Management
- Verbesserung der Qualität und frühere Erkennung von Sicherheitslücken, um Kosten zu senken und den Erfolg der Implementierung zu erhöhen, mit Rational-Lösungen für das Qualitätsmanagement
- Reduzierung von Sicherheitsrisiken und Senkung der Analysekosten mit Rational-Lösungen für die Sicherheit von Webanwendungen

Machen Sie Ihre Anwendungen von Grund auf sicher

Mit Lösungen für Anwendungssicherheit und Risikomanagement hilft das IBM Rational AppScan-Portfolio Unternehmen, ihre Anwendungen von Grund auf sicher – „secure by design“ – zu machen. Dieses Konzept integriert Sicherheitstests in den Softwareentwicklungszyklus – von der Codierung bis zur Einführung in der Produktionsumgebung – und stellt Ihnen die Tools bereit, die Sie für die Erstellung sicherer Anwendungen brauchen.

Um geschäftskritische SAP-Anwendungen vor Gefahren aus dem Web und Sicherheitslücken bei Anwendungen zu schützen, müssen Risiken und Compliance-Probleme bereits auf Codeebene ermittelt werden. IBM bietet zusammen mit der Virtual Forge GmbH den CodeProfiler for Rational AppScan Source Edition an, um die Sicherheit von SAP-Anwendungen zu gewährleisten.

Zusammenfassung

Mit dieser Lösung, die Sicherheitstests in den Softwareentwicklungszyklus integriert, können Ihre für Sicherheit und Entwicklung zuständigen Teams die Anwendungssicherheit verbessern, vertrauliche Daten schützen und die Einhaltung von Vorschriften managen. Die Lösung erkennt Fehler bereits in einer frühen Phase des Entwicklungszyklus und hilft Ihnen so, die Kosten für die Behebung dieser Fehler zu senken. Wenn Sie die Entwicklung von SAP-Anwendungen auslagern, können Sie die ABAP-Sicherheitsanforderungen in die Ausschreibung aufnehmen und so sicherstellen, dass Änderungsanforderungen minimiert werden.

Durch die Kombination der Rational AppScan-Software mit CodeProfiler for Rational AppScan Source Edition können Sicherheitslücken bei SAP-Anwendungen automatisch erkannt und beseitigt werden. So können Ihre für Entwicklung und Sicherheit zuständigen Teams Probleme vermeiden, bevor diese kostenintensive und weitreichende Folgen haben.

Virtual Forge CodeProfiler for AppScan Source Edition auf einen Blick

Systemvoraussetzungen:
- Prozessor: Dual-Core-CPU, kompatibel mit AMD64/EM64T im 64-Bit-Modus
- Hauptspeicher: 4 GB RAM
- Plattenspeicher: 50 GB

Betriebssysteme:
- 64-Bit Linux 2.6
- Windows® Server 2003 R2 x64
- Windows Server 2008 R2 x64

Browser:
- Firefox 3.x

Zusätzliche Software:
- Oracle Java™ 1.6 64 Bit

Weitere Informationen

Wenn Sie mehr über IBM Rational-Lösungen für die SAP-Sicherheit erfahren möchten, wenden Sie sich bitte an Ihren IBM Vertriebsbeauftragten oder IBM Business Partner oder besuchen Sie die folgende Website: http://www-01.ibm.com/software/de/rational/appscan/

Finanzierungslösungen von IBM Global Financing ermöglichen ein effektives Cash-Management, sorgen dafür, dass Sie technologisch immer auf dem neuesten Stand sind, optimieren die Gesamtbetriebskosten und verbessern den Return on Investment (ROI). Mit unseren Global Asset Recovery Services können Sie durch neue Lösungen mit mehr Energieeffizienz einen Beitrag zum Schutz unserer Umwelt leisten. Weitere Informationen zu IBM Global Financing finden Sie unter: **ibm.com**/financing/de

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

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

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

IBM, das IBM Logo, ibm.com und Rational sind Marken der IBM Corporation in den USA und/oder anderen Ländern. Sind diese und weitere Markennamen von IBM bei ihrem ersten Vorkommen in diesen Informationen mit einem Markensymbol (® oder ™) gekennzeichnet, bedeutet dies, dass IBM zum Zeitpunkt der Veröffentlichung dieser Informationen Inhaber der eingetragenen Marken oder der Common-Law-Marken (common law trademarks) in den USA war. Diese Marken können auch eingetragene Marken oder Common-Law-Marken in anderen Ländern sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite „Copyright and trademark information“ unter

ibm.com/legal/copytrade.shtml

Java und alle auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken der Oracle Corporation und/oder ihrer verbundenen Unternehmen.

Windows ist eine Marke der Microsoft Corporation in den USA und/oder anderen Ländern.

Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein.

Der Kunde ist für die Einhaltung der geltenden Gesetze und Verordnungen selbst verantwortlich. IBM erteilt keine Rechtsberatung und gibt keine Garantie bezüglich der Konformität von IBM Produkten oder Services mit jeglichen relevanten Gesetzen und Verordnungen.

© Copyright IBM Corporation 2011
All Rights Reserved

Bitte der Wiederverwertung zuführen

RAD14121-DEDE-00