Protección estratégica de sus activos Web
para darles soporte a sus objetivos empresariales

Rational. software

IBM

Solución del ciclo de vida IBM Rational AppScan: crear la seguridad de las aplicaciones de la Web en la entrega de software y sistemas.

¿Están las vulnerabilidades en línea poniendo en riesgo a su empresa?

Hoy en día, muchas organizaciones dependen del software y de los sistemas basados en la Web para ejecutar sus procesos empresariales, realizar transacciones con sus proveedores y brindar a sus clientes servicios más sofisticados. La creación de la seguridad en cada aplicación destinada al despliegue en línea debería formar parte de los procesos empresariales para la entrega de software y sistemas en una organización bien administrada. Desafortunadamente, en la carrera por permanecer un paso adelante de la competencia, muchas compañías dan un pequeño giro a estas preocupaciones al apresurarse a acelerar los nuevos ofrecimientos al mercado. Y las vulnerabilidades resultantes pueden proporcionar a los hackers una gran oportunidad para acceder a los datos empresariales o personales, o para robarlos poniendo en riesgo a toda la empresa.

IBM Rational® AppScan® es un conjunto de soluciones de seguridad de las aplicaciones líderes de la Web en el mercado que les brindan a las organizaciones la visibilidad y el control necesarios para abordar este desafío crítico. Entre ellas encontramos las siguientes:

- **IBM Rational AppScan Standard Edition** (disponible como una aplicación de desktop o como software as a service [SaaS]).
- **IBM Rational AppScan Tester Edition** (disponible como una aplicación de desktop).
- **IBM Rational AppScan Enterprise Edition** (disponible como una solución basada en la Web o un SaaS)

Cada una de estas amplias soluciones permite obtener escaneos, informes y recomendaciones de arreglos, y es apropiada para todos los tipos de pruebas de seguridad por parte de una variedad de usuarios, incluyendo los desarrolladores de aplicaciones, los equipos de quality assurance (QA), los probadores de penetración, los auditores de seguridad y los gerentes senior.

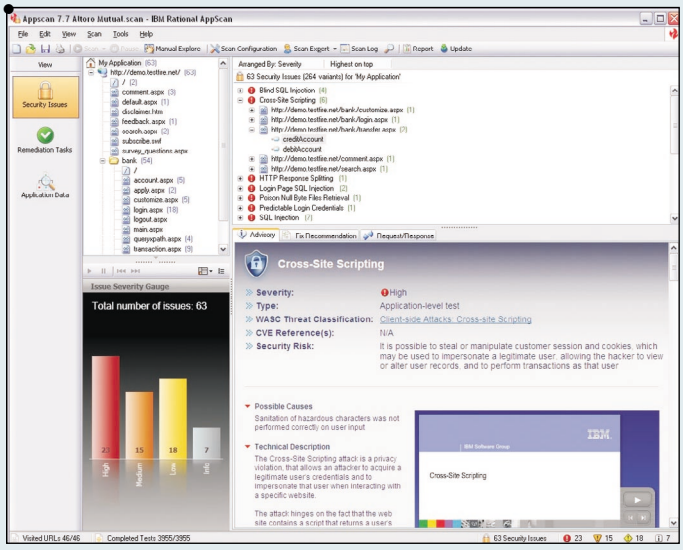
Al igual que otras soluciones del ciclo de vida de IBM Rational Software Delivery Platform, los productos de Rational AppScan les permiten a los usuarios trabajar dentro de un entorno tecnológico familiar, permitiendo una integración virtualmente fluida con las herramientas de QA y los entornos de desarrollo integrado (IDEs) más importantes. Además, las aplicaciones permiten realizar una auditoría continua de la seguridad, ayudando a los equipos de entrega de software a reforzar la seguridad de las aplicaciones de la Web partiendo de cero, y a mitigar el riesgo empresarial incluso antes de desplegar sus aplicaciones.

Protección de sus activos empresariales críticos basados en la Web

Las soluciones de Rational AppScan Standard, Rational AppScan Tester y Rational AppScan Enterprise escanean y prueban vulnerabilidades comunes de las aplicaciones de la Web, incluyendo las identificadas por la clasificación de amenazas de Web Application Security Consortium (WASC), proporcionando una amplia cobertura de la seguridad para los sitios Web complejos. Las soluciones de Rational AppScan comparten una extensa gama de dispositivos fundamentales poderosos y flexibles para el suministro de una sólida cobertura de escaneo de las aplicaciones para las últimas tecnologías Web 2.0, incluyendo un mejor soporte para los lenguajes Flash y Java™ Script avanzado, junto con un amplio soporte para el lenguaje de programación Ajax (incluyendo pruebas dedicadas para JavaScript Object Notation [JSON] y parámetros de servicios Web).

Entre los principales dispositivos de Rational AppScan para la eficiencia del escaneo y la facilidad de uso se encuentran los siguientes:

- Una interfaz de usuario con un selector de visualización para el árbol de aplicaciones, listas de resultados de los problemas de seguridad ordenados jerárquicamente, visualización de soluciones por parte del desarrollador y panel de detalles.
- Un proceso de prueba adaptativo que le permite a usted analizar los parámetros de la aplicación y seleccionar sólo las pruebas pertinentes que no impidan el proceso de desarrollo.
- Un soporte de autenticación compleja que permite probar procedimientos de autenticación de múltiples pasos en aplicaciones Web, entre las cuales encontramos la autenticación por pasos Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA), la autenticación multifactor, las contraseñas únicas, las claves de Universal Serial Bus (USB), las tarjetas inteligentes y la autenticación mutua.
- Una administración avanzada de las sesiones que realiza reconexiones automáticas cuando es necesario.
- Visualización de resultados en tiempo real, lo cual permiten a los usuarios actuar sobre los problemas antes de que se complete un escaneo.
- Normas de patrones de búsqueda que facilitan las pruebas de seguridad relacionadas con las secuencias numéricas de tarjetas de crédito, seguridad social u otros.



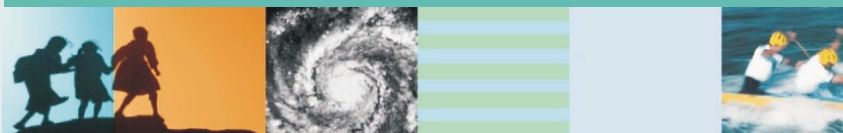
Vista asesora de seguridad de IBM Rational AppScan

Entre los dispositivos esenciales de Rational AppScan para la adaptación y el control encontramos los siguientes:

- La tecnología de Rational AppScan eXtensions Framework, permite a los usuarios crear, compartir y cargar poderosos complementos que extienden las capacidades de prueba.
- Pyscan se suma a Rational AppScan con las capacidades de scripts Python para permitir a los usuarios apalancar las capacidades de escaneo sin las limitaciones de una interfaz de usuario. El resultado es un nivel de adaptación para los profesionales de la seguridad y los probadores de penetración que no estaba disponible anteriormente.
- Rational AppScan software development kit (SDK), provee la capacidad de invocar acciones, desde la ejecución de un largo escaneo hasta la presentación de una prueba del cliente. Las interfaces de SDK han sido diseñadas para facilitar la integración y dar soporte al uso personalizado del motor de escaneo, junto con las opciones de Rational AppScan eXtensions Framework y de Pyscan.

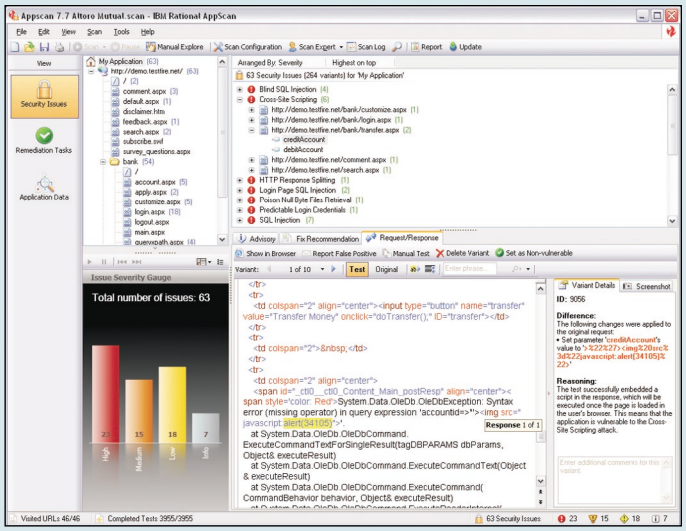
Los principales dispositivos de Rational AppScan para la detección de vulnerabilidades son los siguientes:

- Cobertura de validación global que analiza las respuestas de prueba a los problemas activados de forma involuntaria, prueba de Secure Sockets Layer (SSL) (para probar la validez del certificado SSL) y pruebas de cross-site request forgery (CSRF).
- Simulaciones de hacker que comprenden las 10 vulnerabilidades principales de Open Web Application Security Project's (OWASP's) y las 20 más importantes de System Administration, Networking, and Security Institute's (SANS).
- Información sobre las amenazas más recientes, que se actualiza automáticamente cuando usted lanza un producto de Rational AppScan.
- Un conjunto de herramientas empaquetadas para ayudar a los probadores de penetración y a los asesores de seguridad a desarrollar, probar y depurar aplicaciones Web.

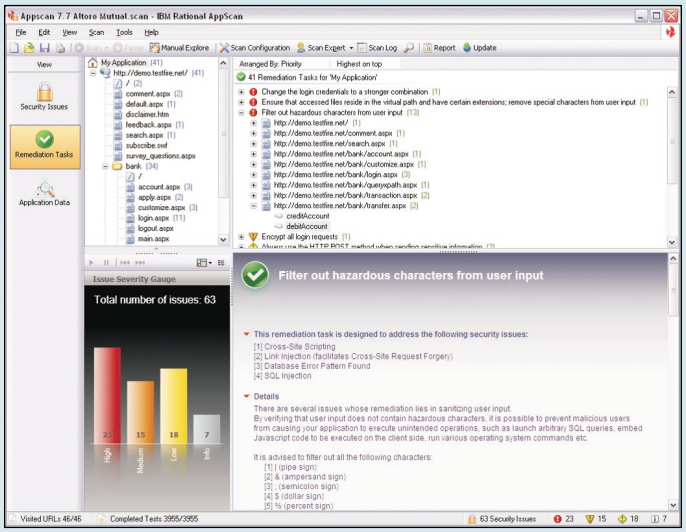


Entre los dispositivos esenciales de Rational AppScan para los informes y la reparación encontramos:

- Pruebas relacionadas con más de 40 problemas y estándares de cumplimiento reglamentario, incluyendo National Institute of Standards and Technology Special Publication (NIST SP) 800-53 y las 10 vulnerabilidades principales de OWASP (actualizada en el 2007). La versión 7.7 de Rational Pazcan también incluye la cobertura de Family Education Rights and Privacy Act (FERPA), Freedom of Information and Protection of Privacy Act (FIPPA) y Payment Application Best Practices (PABP).
- Distinción de la validación que localiza las vulnerabilidades del código HTML y explica el problema. Un dispositivo señalador despliega el código HTML modificado.
- Informes de reparación que incluyen recomendaciones de arreglos de Hypertext Preprocessor (PHP) y listas de tareas del desarrollador. Estos informes también permiten visualizar los problemas relacionados con las aplicaciones, o los problemas de infraestructura, o ambos, y eliminar variantes o marcarlas como no vulnerables para una revisión posterior.
- Informes detallados de contenido sospechoso que enumeran los datos sensibles en los comentarios HTML, y la actividad HTTP relacionada con contenido sospechoso, entre otros.
- Pruebas descriptivas que incluyen IDs para common vulnerabili- ties and exposures (CVEs) de la base de datos de las vulnerabilidades.
- La capacidad de incorporar las vistas de pantallas del navegador interno de Rational AppScan en los informes, y extraer, comprimir y cifrar la información no privada de las pruebas específicas para el envío de correos electrónicos. El software Rational Pazcan permite además informar sobre incidentes falsos positivos (o negativos) al equipo de investigación de la seguridad de IBM Rational AppScan, lo cual resulta útil para mejorar de manera continua la precisión del producto.



Vista de los problemas de seguridad de IBM Rational AppScan



Vista de la reparación de IBM Rational AppScan

Realice las auditorías de seguridad y el seguimiento de la producción con el software Rational AppScan Standard Edition

Para la automatización de pruebas de aplicaciones Web para los auditores de seguridad y los probadores de penetración se requieren tecnologías de escaneo sofisticadas e inteligentes. Rational AppScan Standard Edition incluye dispositivos específicos que están diseñados para dar soporte a usuarios regulares y avanzados. Entre estos dispositivos encontramos:

- El experto en escaneo, el cual brinda una guía para la creación y la instalación del escaneo basada en las mejores prácticas, incluyendo el uso de herramientas adicionales. Los usuarios pueden autorizar un escaneo previo que presente la aplicación donde se va a realizar el escaneo y recomiende las acciones requeridas para un escaneo exitoso.
- El inductor de estado escanea y prueba los procesos empresariales complejos, tales como las compras y el seguimiento en línea de múltiples pasos, y mantiene los valores de los parámetros y las cookies en toda la extensión.
- Plantillas de escaneo predefinidas que permiten a los usuarios elegir y fijar rápidamente opciones de configuración.
- Un asistente de configuración de escaneo rápido que guía a los usuarios a través de escenarios importantes así como también en los pasos condicionales para autenticación de Proxy /plataforma e información de detección en sesión.
- Nuevas pestañas de solicitud/respuesta que permiten resaltar la sintaxis, pregunta/respuesta, colapsar/expandir, mientras se ingresa una búsqueda y opciones adicionales para el uso del botón derecho del mouse.
- Informes basados en plantillas de Microsoft® Word para el diseño de formatos personalizados que se ajusten a los estándares corporativos. Las plantillas tienen una tabla de contenido, tiempos de inicio y finalización de escaneo, y gráficos.
- Módulos Web-based Training (WBT) que ayudan a explicar los problemas y demostrar la explotación junto con la verificación de los resultados para ayudar a facilitar la comprensión y la comunicación de las vulnerabilidades

Haga que las pruebas de seguridad formen parte de su programa de administración de la calidad con el software Rational AppScan Tester Edition

Rational AppScan Tester Edition ofrece capacidades para ayudar a los equipos de QA a integrar las pruebas de seguridad a los procesos existentes de administración de la calidad, aliviando así la carga de los profesionales de la seguridad.

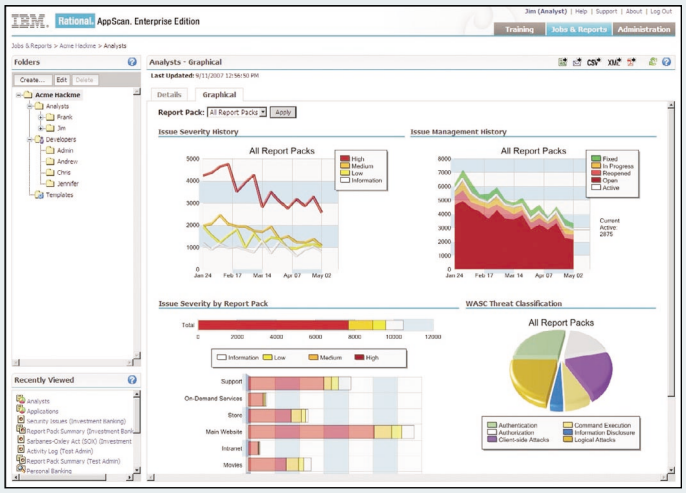
Dado que éste se integra con los principales sistemas de prueba, los profesionales de QA pueden usar la funcionalidad de Rational AppScan en scripts de prueba y llevar a cabo las verificaciones de seguridad dentro de entornos de prueba familiares, facilitando la adopción de las pruebas de seguridad junto con las pruebas funcionales y de performance.

Escale pruebas de seguridad de las aplicaciones en toda la empresa con el software Rational AppScan Enterprise Edition

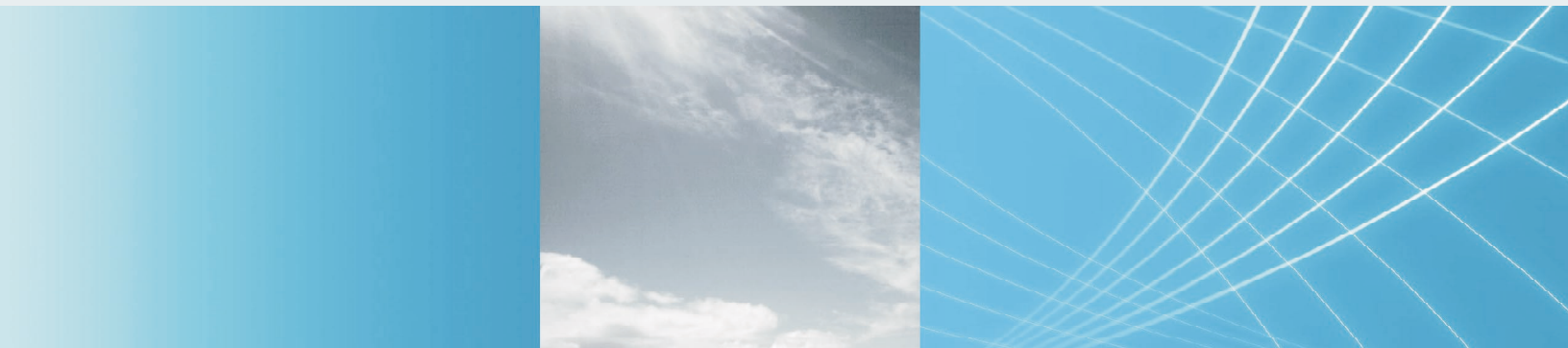
Con su arquitectura basada en la Web, el software de Rational AppScan Enterprise Edition está diseñado para ayudar a las organizaciones a distribuir la responsabilidad de las pruebas de seguridad entre múltiples participantes, y para ayudar a los usuarios a descubrir de manera anticipada las vulnerabilidades en el ciclo de vida de la entrega de las aplicaciones Web, cuando son fáciles de establecer y eficientes en costos.

Además de la conveniencia y la extensibilidad de la administración centralizada, Rational AppScan Enterprise Edition ofrece:

- La capacidad de escanear y probar miles de aplicaciones simultáneamente en un sitio Web complejo, y luego volver a probarlas con frecuencia, siguiendo así los cambios.
- Una herramienta simple de prueba de rápido escaneo para ejecutar plantillas definidas por el administrador para desarrolladores y otros profesionales no dedicados a la seguridad, sin instalación o configuración de escritorio.
- Un depósito central de datos que almacena automáticamente y agrega los resultados de las pruebas para el acceso en toda la empresa y múltiples vistas. Los usuarios pueden segmentar y establecer las vulnerabilidades por unidad de negocios, geografía o proveedor tercero.
- Una consola de informes basados en la Web que proporciona acceso basado en roles a informes de seguridad y facilita la comunicación en toda la organización. Los usuarios pueden filtrar y establecer la prioridad de los problemas, y especificar el estado de los mismos: abierto, en progreso o cerrado.
- Tableros de mando ejecutivos e informes de análisis delta que destacan los cambios entre un escaneo y otro, Incluyendo problemas de seguridad fijos, pendientes y nuevos.
- Controles centralizados para monitorear y controlar pruebas de vulnerabilidad de aplicaciones Web en toda la organización.
- Módulos Web-based Training (WBT) incorporados que explican los problemas y demuestran la explotación, junto con la verificación de los resultados para ayudar a facilitar la comprensión y la comunicación de las vulnerabilidades.



Vista del dashboard de IBM Rational AppScan Enterprise Edition



Capacidades de Rational AppScan Standard y Rational AppScan Enterprise disponibles como SaaS

Al acceder a las capacidades de Rational AppScan como un servicio administrado, usted puede aprovechar los beneficios del producto sin el costo por agregar personal o hardware.

Un entorno de seguridad de tecnología de punta

Con el fin de proteger su entorno operativo, estos servicios han sido construidos con herramientas y técnicas de seguridad sofisticadas.

Su propio experto en seguridad y cumplimiento dedicado

Como cliente de Rational AppScan Standard o de Rational AppScan Enterprise, usted puede acceder a un analista de seguridad de IBM Rational para que lo ayude a:

- Configurar y ajustar los escaneos para ayudarlo a asegurar la cobertura de todas las aplicaciones.
- Revisar y analizar los resultados para eliminar positivos o negativos falsos, identificar patrones, priorizar problemas claves y destacar las principales tareas de reparación.
- Hacer un seguimiento del progreso de la reparación manteniendo los datos de las tendencias, rastreando la solución de los problemas más importantes de un escaneo al otro e informando la efectividad de la reparación.
- Capacitar a su personal de QA para usar Rational AppScan en todo el ciclo de vida de la entrega de las aplicaciones Web, y ayudar a construir la administración de seguridad y del cumplimiento en sus aplicaciones desde cero.

Aborde los problemas de la administración de la seguridad y del cumplimiento organizativo con una capacitación basada en la Web

La familia de productos de IBM Rational AppScan incluye capacitación basada en la Web, un programa de capacitación en línea auto administrado basado en una década de experiencia, así como también las mejores prácticas deducidas de los despliegues prácticos de los clientes en entornos Web desafiantes y complejos. Además de la instrucción básica sobre el producto, el servicio provee un asesoramiento dirigido para desarrolladores, equipos de QA y profesionales de la seguridad.

Los módulos de servicios, que son entregados en línea en intervalos de 15 minutos y archivados, son accesibles para los usuarios desde cualquier lugar, en cualquier momento. Durante horas especiales de laboratorios, los usuarios también pueden acceder a una guía en tiempo real de expertos en seguridad de Rational AppScan

Las pruebas en línea de tres niveles de la certificación de conocimientos del producto están disponibles durante el proceso de capacitación, y los gerentes pueden hacer un seguimiento del progreso del empleado mediante un tablero de mandos de administración disponible en línea y en Rational AppScan Enterprise Edition.

Requisitos de sistema

Procesador	Intel® Pentium® P4, 1.5GHz (se recomienda 2.4GHz)
Memoria	512MB RAM (se recomienda 1GB para escaneo de sitios
Espacio en disco	1GB (se recomienda 10GB para escaneo de sitios grandes)
Red	Una Network Interface Card (NIC) de 10Mbps para comunicación de red con TCP/IP configurado (se recomienda 100 Mbps)
Sistema Operativo	Microsoft Windows® XP, Windows 2000, Windows 2003 Enterprise Edition, Windows Vista
Navegador Web	Microsoft Internet Explorer 5.5 o superior (Se recomienda 6.0 o superior)
	Microsoft .NET framework 2.0 o superior
	Java Runtime Environment (JRE) 5.0 (sólo para Proxy HTTP Rational AppScan)

Para obtener más información

Para aprender más sobre los productos Rational AppScan de IBM, comuníquese con su representante IBM o con un asociado de negocios de IBM, o visite:

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

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Producido en los Estados Unidos de Norteamérica
12-07

RAB14001-USEN-00