Una protección estratégica para los activos de Web
a fin de dar soporte a sus objetivos empresariales

Rational. software

IBM

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

¿Vulnerabilidades en línea ponen en riesgo su empresa?

En la actualidad, muchas organizaciones dependen del software y de los sistemas basados en la Web para ejecutar sus procesos empresariales, llevar a cabo transacciones con proveedores y entregar servicios cada vez más sofisticados a los clientes. La seguridad en cada aplicación destinada a un despliegue en línea debe ser una parte integral de los procesos empresariales para la entrega de software y sistemas dentro de una organización bien gobernada. Desafortunadamente en la carrera por permanecer un paso más adelante en la competición, muchas compañías desechan estas preocupaciones a medida que se apuran y aceleran nuevos ofrecimientos en el mercado y las vulnerabilidades resultantes pueden proveer una amplia oportunidad para que los hackers accedan o roben datos corporativos o personales, poniendo potencialmente en riesgo a toda la empresa

IBM Rational® AppScan® es una suite de soluciones de seguridad de las aplicaciones de Web líderes en el mercado que les dan a las organizaciones la visibilidad y el control necesarios para abordar este desafío crítico. La suite incluye:

- IBM Rational AppScan Standard Edition (disponible como una aplicación de desktop o como software como un servicio [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 provee escaneo, informes y recomendaciones de arreglos, y es apropiada para todos los tipos de pruebas de seguridad por parte de una variedad de usuarios, incluyendo desarrolladores de aplicaciones, equipos de aseguramiento de calidad (QA), probadores de penetración, auditores de seguridad y gerentes senior.

Tal como otras soluciones del ciclo de vida de IBM Rational Software Delivery Platform, los productos de Rational AppScan permiten a los usuarios trabajar dentro de un entorno tecnológico familiar, ofreciendo una integración virtualmente fluida con las herramientas líderes de QA y los entornos de desarrollo integrado (IDEs). Además, las aplicaciones le permiten a usted realizar una auditoría continua de la seguridad, ayudando a los equipos de entrega de software a construir con seguridad las aplicaciones de Web de principio a fin, y a mitigar el riesgo empresarial aún antes de que despliegue sus aplicaciones.

La protección de sus activos empresariales críticos basados en la Web

Ofreciendo una amplia cobertura de la seguridad para sitios de Web complejos, las soluciones de Rational AppScan Standard, Rational AppScan Tester y Rational AppScan Enterprise escanean y prueban vulnerabilidades comunes de las aplicaciones de Web, incluyendo las identificadas por la clasificación de amenazas de Web Application Security Consortium (WASC). Las soluciones de Rational AppScan comparten una extensa gama de dispositivos esenciales poderosos y flexibles para proveer una robusta cobertura de escaneo de aplicaciones para las tecnologías más recientes de Web 2.0, incluyendo un soporte mejorado 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 de Web).

Los dispositivos esenciales de Rational AppScan para la eficiencia del escaneo y la facilidad de uso incluyen:

- Una interfaz de usuario con un selector de visualización para el árbol de aplicaciones, listas de resultados de los problemas de seguridad jerárquicos, visualizaciones para la subsanación del desarrollador y panel de detalles.
- Un proceso de prueba adaptable que le permite a usted analizar los parámetros de la aplicación y seleccionar sólo las pruebas relevantes que no impidan el proceso de desarrollo.
- Un soporte de autenticación compleja que permite realizar pruebas para procedimientos de autenticación de múltiples pasos en las aplicaciones de Web, la autenticación por pasos Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA), autenticación multifactor, contraseñas de única vez, claves de Universal Serial Bus (USB), tarjetas inteligentes y autenticación mutua.
- Una administración avanzada de sesiones que realiza reconexiones automáticas cuando se requiera.
- Visualizaciones de resultados en tiempo real que le permiten a los usuarios actuar sobre problemas antes de que se complete un escaneo.P
- atrones de búsqueda para facilitar las pruebas de seguridad con respecto a secuencias numéricas de tarjetas de crédito, seguridad social u otras.

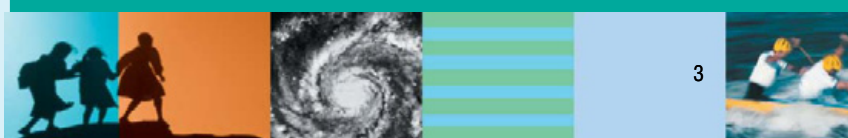
Visión asesora de seguridad de IBM Rational AppScan

Los dispositivos esenciales de Rational AppScan para la adaptación y el control incluyen:

- La tecnología Rational AppScan eXtensions Framework, permite a los usuarios crear, compartir y cargar poderosos agregados que extienden las capacidades de prueba.
- Pyscan se une a Rational AppScan con las capacidades de scripts Python para que los usuarios puedan promover las capacidades de escaneo sin las limitaciones de una interfaz de usuario. El resultado es un nivel de adaptación previamente no disponible para los profesionales de la seguridad y los probadores de penetración.
- El kit de desarrollo de software Rational AppScan (SDK) provee la capacidad de invocar acciones, de ejecutar un largo escaneo a presentar una prueba de cliente. Las interfaces de SDK están diseñadas para facilitar la integración y dar soporte a un uso adaptado del motor de escaneo, junto con las opciones Rational AppScan eXtensions Framework y Pyscan

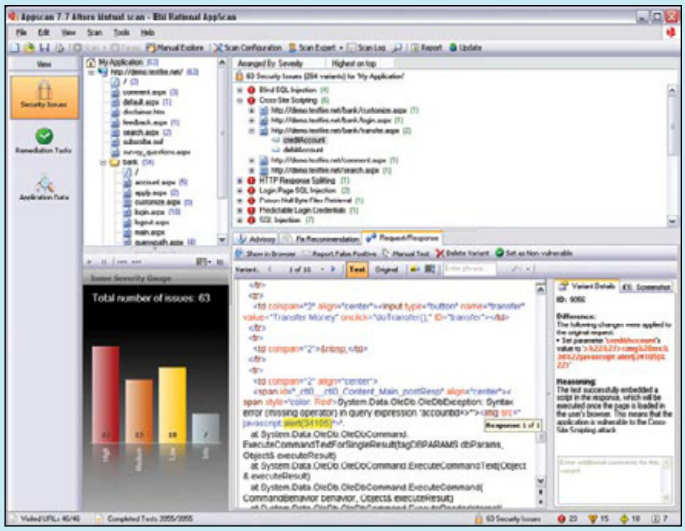
Los dispositivos esenciales de Rational AppScan para la detección de la vulnerabilidad incluyen:

- Cobertura para una validación global que analiza las respuestas de las pruebas para problemas inadvertidamente activados, prueba de Secure Sockets Layer (SSL) (para probar la validez del certificado SSL) y pruebas de cross-site request forgery (CSRF) (falsificación de solicitud a través de sitios).
- Simulaciones de hacker que cubren las vulnerabilidades de Open Web Application Security Project's (OWASP's) top 10 y de System Administration, Networking, and Security Institute's (SANS's) top 20.
- Información sobre las amenazas más recientes, automáticamente actualizada cuando usted lanza el producto Rational AppScan.
- Una suite de utilitarios empaquetados para ayudar a los probadores de penetración y a los consultores de seguridad a desarrollar, probar y depurar aplicaciones de Web.



Los dispositivos esenciales de Rational AppScan para los informes y la subsanación incluyen:

- Pruebas relacionadas con más de 40 problemas y normas de cumplimiento reglamentario, incluyendo la National Institute of Standards and Technology Special Publication (NIST SP) 800-53 y OWASP top 10 (actualizada en el 2007). Rational AppScan, Version 7.7 también incluye cobertura para Family Education Rights and Privacy Act (FERPA), Freedom of Information and Protection of Privacy Act (FIPPA) and Payment Application Best Practices (PABP).
- Destaca la validación y vulnerabilidades del código HTML y explica el problema. Un dispositivo de diferencia despliega el código HTML modificado.
- Informes de subsanación que incluyen recomendaciones de arreglos de Hypertext Preprocessor (PHP) y listas de tareas del desarrollador. Estos informes también le permiten a usted ver problemas relacionados con aplicaciones, problemas de infraestructura o ambos y eliminar variantes o marcarlas como no vulnerables para una revisión posterior.
- Detalla informes de contenido sospechoso que listan ítems tales como datos sensibles en comentarios de HTML, así como también la actividad de HTTP alrededor del contenido sospechoso.
- Pruebas descritptivas que incluyen IDs para vulnerabilidades y exposiciones comunes de base de datos de vulnerables.
- La capacidad de incorporar vistas de pantallas del navegador interno de Rational AppScan a informes, y extraer, comprimir y cifrar información no propietaria de pruebas específicas para e-mailing. El software Rational AppScan también le permite a usted informar incidentes positivos falsos (o negativos) al equipo de investigación de seguridad de IBM Rational AppScan, lo que ayuda a mejorar continuamente la precisión del producto.



Visión de problemas de seguridad de IBM Rational AppScan

Visión de subsanación de IBM Rational AppScan

Realice auditorías de seguridad y monitoreo de producción con el software Rational AppScan Standard Edition

La automatización de pruebas de aplicaciones de Web para auditores de seguridad y probadores de penetración requiere tecnologías de escaneo sofisticadas e inteligentes. Rational AppScan Standard Edition incluye dispositivos específicos que están diseñados para dar soporte a usuarios moderados y poderosos. Los dispositivos incluyen:

- El experto en escaneo el cual ofrece 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 pre-escaneo que perfile la aplicación objetivo y recomiende las acciones requeridas para un escaneo exitoso.
- El inductor de estado escanea y prueba procesos empresariales complejos, tales como compras y rastreo en línea de múltiples pasos y mantiene valores de parámetros y cookies en toda la extensión.
- Plantillas de escaneo predefinidas que permiten a los usuarios elegir y lanzar rápidamente opciones de configuración.
- Configuración Wizard de escaneo rápido que guía a los usuarios a través de escenarios importantes así como también pasos condicionales para autenticación de proxy/plataforma e información de detección en sesión.
- Nuevas pestañas de solicitud/respuesta que ofrecen resaltado de sintaxis, pregunta/respuesta, colapsar/expandir en búsqueda a medida que se escribe y opciones adicionales de clic/correcto.
- Informes basados en plantillas de Microsoft® Word para diseñar formatos de cliente que se ajusten a 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 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 sean 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 pruebas de seguridad a los procesos de administración de la calidad existentes, aliviando así la carga de los profesionales de la seguridad.

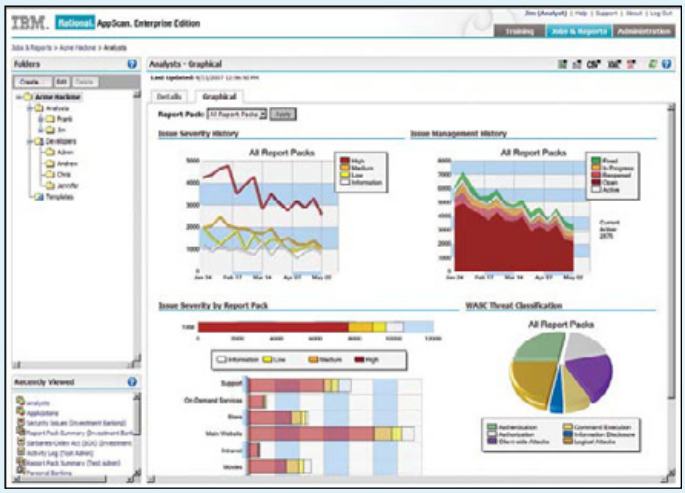
Dado que se integra con sistemas de prueba líderes, los profesionales de QA pueden usar funcionalidad de Rational AppScan en scripts de prueba y llevar a cabo verificaciones de seguridad dentro de sus entornos de prueba familiares, facilitando la adopción de las pruebas de seguridad junto con las pruebas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

Escale pruebas de seguridad de las aplicaciones a través de la empresa con el software Rational AppScan Enterprise Edition

Con su arquitectura basada en la Web, Rational AppScan Enterprise Edition está diseñado para ayudar a las organizaciones a distribuir responsabilidad para las pruebas de seguridad entre múltiples partes interesadas, así como también ayudar a los usuarios a descubrir tempranamente vulnerabilidades en el ciclo de vida de la entrega de aplicaciones de Web, cuando el arreglo sea fácil y efectivo 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 de Web complejo y probarlas nuevamente con frecuencia, siguiendo los cambios.
- Una herramienta simple de prueba de rápido escaneo para ejecutar plantillas definidas por el administrador para desarrolladores y otros profesionales en falta de seguridad, sin instalación o configuración de desktop.
- Un depósito de datos central 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 marcar las vulnerabilidades por unidad de negocios, geografía o un proveedor tercero.
- Una consola de informes basados en la Web que provee un acceso basado en roles a informes de seguridad y facilita la comunicación a través de la organización. Los usuarios pueden filtrar y dar prioridad a problemas y especificar su estado ya sea abierto, en progreso o cerrado.
- Tableros ejecutivos e informes de análisis delta que destacan los cambios de un escaneo al siguiente. Incluyendo problemas de seguridad fijos, pendientes y nuevos.
- Controles centralizados para monitorear y controlar pruebas de vulnerabilidad de aplicaciones de Web a través de la organización.
- Módulos Web-based Training (WBT) incorporados que explican 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 tablero de IBM Rational AppScan Enterprise Edition

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

Accediendo a las capacidades de Rational AppScan como un servicio administrado, usted puede obtener las ventajas de los beneficios del producto sin los costos de agregar personal o hardware.

Un entorno de seguridad de tecnología de punta

Poniendo el enfoque en proteger su entorno operativo, estos servicios están construidos con herramientas y técnicas de seguridad sofisticadas.

Su propio experto en seguridad y cumplimiento dedicado

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

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

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 entrenamiento en línea y auto administrado y basado en una década de experiencia, así como también las mejores prácticas deducidas de despliegues prácticos de clientes en entornos de 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 para tres niveles de la certificación de conocimientos del producto están disponibles a través del proceso instructivo, y los gerentes pueden hacer un seguimiento del progreso del empleado mediante un tablero de administración disponible en línea y en Rational AppScan Enterprise Edition.

Requisitos del sistema

Procesador	Intel® Pentium® P4, 1.5GHz (se recomienda 2.4GHz)
Memoria	512MB RAM (1GB recomendado para escanear grandes sitios)
Espacio libre en disco	1GB (10GB recomendado para escanear grandes sitios)
Red	Un 10Mbps Network Interface Card)NIC) 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 de Web	Microsoft Internet Explorer 5.5 o mayor (se recomienda 6.0 o mayor)
	Microsoft .NET framework 2.0 o mayor
	Java Runtime Environment (JRE) 5.0 (sólo para Rational AppScan HTTP proxy)

Para obtener más información

Para conocer más detalles acerca de los productos de IBM Rational AppScan, comuníquese con su representante IBM o su Asociado de Negocios IBM, o bien visite:

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

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

Produced in the United States of America
12-07

RAB14001-USEN-00