IBM Rational AppScan: gestión de la seguridad de las aplicaciones y la conformidad con las normativas

Identifique, priorice y resuelva las vulnerabilidades críticas de la seguridad en todo el ciclo de vida de las aplicaciones

IBM

Gestión global de la vulnerabilidad de las aplicaciones

Muchas organizaciones dependen de software basado en web para ejecutar sus procesos empresariales, realizar transacciones y prestar servicios cada vez más sofisticados a sus clientes. Todas las aplicaciones destinadas al despliegue online deben resolver problemas de seguridad como parte integral del proceso de suministro del software. Desgraciadamente, la presión por cumplir plazos y superar a la competencia, hace que muchas empresas no realicen pruebas de seguridad adecuadas, y las consiguientes vulnerabilidades ofrecen grandes oportunidades para que los piratas informáticos puedan acceder a datos corporativos o personales, e incluso robarlos, poniendo en riesgo todo el negocio.

La forma más eficaz de evitar vulnerabilidades en la seguridad consiste en crear el software de forma segura, desde el principio. El reto radica en que la mayoría de los desarrolladores no son expertos en seguridad, y la codificación segura históricamente no se ha considerado prioritaria en comparación con el suministro de funciones a tiempo y dentro de un presupuesto. Como resultado, tanto las aplicaciones basadas en web como las no basadas en web siguen desplegándose repletas de vulnerabilidades, exponiendo claramente los datos confidenciales a una intrusión.

La costosa tarea de identificación y resolución de las vulnerabilidades no puede realizarse correctamente mediante los limitados recursos de seguridad de las TI. Por lo tanto, la mejor manera de implicar a los desarrolladores en el proceso de seguridad de las aplicaciones es proporcionándoles herramientas que se ajusten a su entorno y su flujo de trabajo, y que generen resultados en un lenguaje que comprendan. El conjunto de aplicaciones que integran el software IBM® Rational® AppScan® permite que las organizaciones incorporen pruebas de seguridad de las aplicaciones en todo el ciclo de vida de desarrollo para permitirles disponer de una mayor visibilidad y control, a la vez que emplean una estrategia de limitación de riesgos.

Desde los requisitos, a través del diseño y el proceso de codificación, las pruebas de seguridad hasta la entrada en producción, el software Rational AppScan ayuda a garantizar la identificación, la priorización, el seguimiento y la resolución de las vulnerabilidades críticas de seguridad a lo largo del ciclo de vida de las aplicaciones. En pocas palabras, el software Rational AppScan le ayuda a incorporar la seguridad en el diseño de la infraestructura de sus aplicaciones.

La suite de productos de software IBM Rational AppScan incluye lo siguiente:

Ofertas bajo licencia

- IBM Rational AppScan Express Edition
- IBM Rational AppScan Standard Edition
- IBM Rational AppScan Source Edition
- IBM Rational AppScan Build Edition
- IBM Rational AppScan Tester Edition
- IBM Rational AppScan Reporting Console
- IBM Rational AppScan Enterprise Edition

Ofertas de software como servicio (SaaS)

- IBM Rational AppScan OnDemand
- IBM Rational AppScan OnDemand Premium
- IBM Rational AppScan OnDemand Production Site Monitoring
- IBM Rational AppScan OnDemand Source Code Analysis

Opciones de formación y servicios

- Formación basada en web de IBM Rational para AppScan
- IBM Rational Professional Services

Todas estas soluciones proporcionan funciones de exploración, elaboración de informes y recomendación de soluciones, y cada una está diseñada para distintos tipos de usuarios, incluidos equipos de gestores de seguridad de la información, controladores de intrusiones, auditores de seguridad, desarrolladores de aplicaciones, gestores de compilación y equipos de verificación de calidad (QA).

Proteja sus activos empresariales críticos basados en web

La suite de productos de software Rational AppScan explora y comprueba las vulnerabilidades comunes de las aplicaciones web, incluyendo las vulnerabilidades identificadas por la clasificación de amenazas del WASC (Web Application Security Consortium) a través de su amplia oferta de prestaciones de seguridad globales para aplicaciones web complejas. Las soluciones de Rational AppScan comparten una amplia gama de características principales flexibles para proporcionar una sólida cobertura de exploración de aplicaciones para las tecnologías Web 2.0 más recientes, incluido el soporte ampliado para la tecnología Adobe® Flash y las infraestructuras avanzadas de JavaScript, junto con un soporte global para las aplicaciones basadas en AJAX.

Características principales de IBM Rational AppScan

Característica	Ventajas
Eficacia de la exploración y facilidad de uso	• La interfaz del usuario proporciona un selector de vistas para el árbol de aplicaciones, junto con unas listas jerárquicas de resultados de los problemas de seguridad, vistas de resolución para los desarrolladores y paneles de detalles. • Un proceso adaptativo de prueba ayuda a los usuarios a analizar parámetros de aplicación y a seleccionar únicamente las pruebas relevantes que no impidan el proceso de desarrollo. • Un soporte de autenticación complejo permite realizar pruebas para los procedimientos de autenticación de diversos pasos. • La gestión avanzada de sesiones realiza reinicios de sesión automáticos, si es necesario. • Las vistas de resultados en tiempo real permiten a los usuarios tomar acciones frente a posibles problemas antes de que finalice la exploración. • Las reglas de búsqueda de patrones de serie facilitan las pruebas de seguridad mediante secuencias numéricas de tarjetas de crédito, de números de la seguridad social o de otro tipo.
Personalización y control	• La tecnología Rational AppScan eXtensions Framework ayuda a los usuarios a crear, compartir y cargar complementos potentes que amplían las prestaciones de prueba. • Pyscan, que combina el software Rational AppScan con las prestaciones de scripts de Python, permite a los usuarios aprovechar las funciones de exploración sin las limitaciones de una interfaz de usuario. • El kit de desarrollo de software (SDK) de AppScan ayuda a los usuarios a invocar acciones, desde la ejecución de una exploración extensa hasta el envío de una prueba personalizada. Las interfaces del SDK han sido diseñadas para facilitar las integraciones y dar soporte a un uso personalizado del motor de exploración, junto con las opciones de Rational AppScan eXtensions Framework y de Pyscan.
Detección de vulnerabilidades	• La cobertura para la validación global analiza las respuestas de las pruebas para encontrar problemas desencadenados de forma inadvertida, pruebas de certificados de SSL (Secure Sockets Layer) y pruebas de falsificación de solicitudes de varios sitios (CSRF, Cross-Site Request Forgery). • Las simulaciones de piratas informáticos colaboran en la búsqueda de vulnerabilidades actuales, ya conocidas. • Se suministran automáticamente notificaciones acerca de las amenazas más recientes, cuando los usuarios inician una aplicación Rational AppScan. • Un paquete combinado de utilidades ayuda a los controladores de intrusiones y a los consultores de seguridad a desarrollar, probar y depurar las aplicaciones web. • Cobertura de prueba de seguridad para los servicios web.

"Hemos pasado a IBM Rational porque nos ofrece el liderazgo tecnológico y la amplia experiencia en seguridad necesarios para ayudarnos a implementar una estrategia de análisis que pueda integrarse en nuestro proceso de desarrollo existente. Esto nos ha permitido mejorar ampliamente la seguridad de nuestro software y a la vez reducir costes, mediante la búsqueda de las vulnerabilidades en las fases iniciales, cuando su resolución resulta menos costosa."

—Marek Hlávka, Director de Seguridad (CSO), Skoda Auto

IBM Rational AppScan Express Edition
IBM Rational AppScan Standard Edition

Consiga sólidas características de seguridad de las aplicaciones web

Las organizaciones con equipos de desarrollo pequeños o limitados también deben tener en cuenta las pruebas de seguridad como parte del ciclo de vida de desarrollo. A menudo, estas organizaciones tienen que sacrificar la funcionalidad a cambio de rentabilidad. El software Rational AppScan Express Edition cumple los requisitos de las empresas de tamaño medio mediante el suministro de una excelente funcionalidad de pruebas de seguridad a un precio muy atractivo. Diseñado para desplegarse fácilmente, el software Rational AppScan Express Edition permite reducir el tiempo y los costes asociados a las pruebas de vulnerabilidad manuales, y de esta manera, los equipos pueden centrarse en otras cuestiones relacionadas con la seguridad y las TI dentro de las organizaciones.

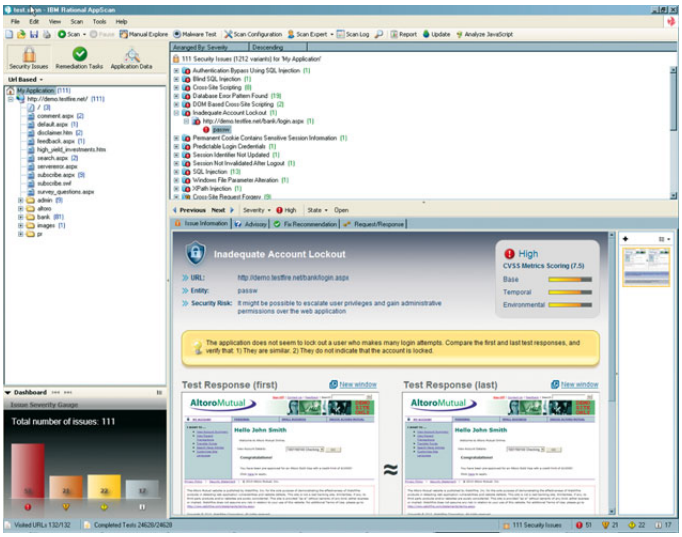

Figura 1: el software Rational AppScan Standard le ayuda a identificar vulnerabilidades en el sitio web antes de que lo hagan los piratas informáticos.

Realice auditorías de seguridad y supervisión de la producción

Los procesos de prueba de aplicaciones web automatizados, que requieren tecnologías de exploración sofisticadas e inteligentes, ayudan a los auditores de seguridad y los controladores de intrusiones a llevar a cabo su trabajo de forma rápida y eficaz. El software Rational AppScan Standard Edition incluye características diseñadas para dar soporte a los usuarios de mediano y gran consumo.

Características del software Rational AppScan Express Edition y Standard Edition

- Analizador de JavaScript: aprovechamiento de los análisis dinámico y estático para generar un análisis híbrido de exploración e identificar vulnerabilidades anteriormente desconocidas.
- Experto de exploración: un asistente que ofrece orientación para la configuración y la creación de exploraciones a partir de prácticas recomendadas, incluida la utilización de herramientas adicionales. Los usuarios pueden autorizar una exploración previa personalizada que realiza un perfil de la aplicación de destino y recomienda las acciones necesarias para una exploración satisfactoria.
- Inductor de estado: explora y prueba procesos empresariales complejos (como seguimiento de pedidos y carros de la compra de varios pasos) y mantiene los valores de parámetro y las cookies a lo largo de todo el proceso.
- Plantillas de exploración predefinidas: ayuda a los usuarios a elegir e iniciar rápidamente las opciones de configuración.
- Asistente de configuración de exploración rápida: orienta a los usuarios a través de las configuraciones importantes y en los pasos condicionales para obtener información de detección en sesión y la autenticación de proxy/plataforma.
- Nuevas pestañas de solicitud/respuesta: ofrecen opciones de resaltado de la sintaxis, solicitud/respuesta, ampliación/reducción, búsqueda a medida que se escribe y opciones adicionales con el botón derecho del ratón.
- Elaboración de informes basados en plantillas de Microsoft® Word.
- Módulos de formación integrados basados en web: ayudan a explicar los problemas y a demostrar los logros obtenidos.
- Valoraciones de servicios web automatizados: ayudan a localizar las vulnerabilidades de las capas de la aplicación, las del analizador SOAP y XML y las de la infraestructura web.

IBM Rational AppScan Build Edition

Automatización de las pruebas de seguridad

El software Rational AppScan Build Edition da soporte a pruebas de seguridad automatizadas en la fase de compilación del ciclo de vida de desarrollo del software. Mediante la integración con múltiples sistemas de gestión de la compilación, como el software IBM Rational Build Forge®, proporciona cobertura de pruebas de seguridad para las compilaciones planificadas. Asimismo, redirecciona los resultados a los desarrolladores, a través de las soluciones de seguimiento de defectos como el software IBM Rational ClearQuest®, o de las soluciones de elaboración de informes de seguridad como el software Rational AppScan Enterprise Edition o Rational AppScan Reporting Console.

El software Rational AppScan Build Edition incluye el mismo conjunto de técnicas de análisis que Rational AppScan Developer Edition, proporcionando un alto nivel de precisión y una cobertura de código que le ayudará a identificar el código que se ha probado.

IBM Rational AppScan Tester Edition

Integre las pruebas de seguridad en el programa de gestión de la calidad

El software Rational AppScan Tester Edition, disponible como aplicación de escritorio, ofrece prestaciones para ayudar a los equipos de QA a integrar las pruebas de seguridad en sus procesos de gestión de la calidad, aliviando con ello la sobrecarga de trabajo de los profesionales de la seguridad.

Dado que el software Rational AppScan Tester Edition se integra con los sistemas de prueba líderes del sector, los profesionales de QA pueden utilizar su funcionalidad en los scripts de prueba y pueden llevar a cabo comprobaciones de seguridad en sus entornos de prueba familiares, lo que facilita la adopción de pruebas de seguridad además de las pruebas funcionales y de rendimiento.

IBM Rational AppScan Reporting Console

Acceso a informes centralizados acerca de los datos de vulnerabilidades de las aplicaciones web

El software IBM Rational AppScan Reporting Console es una aplicación de elaboración de informes y gestión basada en web. Plenamente integrada con el software Rational AppScan Express, Standard, Source, Tester y Edition, el software Rational AppScan Reporting Console tiene como plataforma una base de datos de nivel empresarial que le permite consolidar resultados de exploraciones desde diferentes tipos de clientes de Rational AppScan Express y Standard para crear un repositorio centralizado de vulnerabilidades de aplicaciones. Los resultados de la exploración pueden distribuirse fácilmente a los equipos de QA y de desarrollo sin tener que instalar licencias de escritorio adicionales, ayudando con ello a simplificar el proceso de resolución y a integrar el análisis de vulnerabilidades a lo largo del ciclo de desarrollo de software. Rational AppScan Reporting Console le permite crear paneles de control para varios usuarios, dando a los usuarios individuales la capacidad de segmentar los datos de seguridad por aplicación, por unidad de negocio, por zona geográfica o por proveedor externo.

Características del software Rational AppScan Reporting Console

Además de la comodidad y la capacidad de ampliación de la administración centralizada, entre las características del software Rational AppScan Reporting Console se incluyen las siguientes:

- **Un repositorio de datos centralizado: almacena y agrega automáticamente resultados de pruebas estáticas y dinámicas para su acceso a nivel empresarial y vistas múltiples.**
- **Correlación automatizada de los resultados del análisis de pruebas: estática y dinámica (análisis híbrido).**
- **Una consola de elaboración de informes basada en web: proporciona acceso basado en funciones a los informes de seguridad y facilita la comunicación a toda la organización.**
- **Paneles de control ejecutivos e informes de análisis de diferencias: resaltan los cambios entre las exploraciones, incluidos los problemas de seguridad solucionados, pendientes y nuevos.**
- **Controles centralizados: supervisión y control de las pruebas de vulnerabilidad de las aplicaciones por toda la organización.**

IBM Rational AppScan Source Edition

Pruebas de seguridad integradas de forma sencilla en el ciclo de desarrollo

El modo más eficaz de permanecer protegido frente a posibles vulnerabilidades de seguridad consiste en crear un software de forma segura, desde el principio. El reto radica en el hecho de que la mayoría de los desarrolladores no son expertos en seguridad, y la elaboración de un código que contenga fundamentos sólidos de seguridad no siempre resulta ser su prioridad básica. Por lo tanto, la mejor manera de vincular al equipo de desarrollo en el proceso de la seguridad de las aplicaciones es proporcionarle herramientas que funcionen en su entorno y generen resultados en un lenguaje que dominen.

El software Rational AppScan Source Edition se ha diseñado para ayudar a los desarrolladores a invocar pruebas de seguridad desde dentro de su entorno de desarrollo o compilación. Ayuda a la organización de desarrollo a controlar la cantidad de problemas de seguridad que pueden introducirse en el código, racionalizando el flujo de trabajo del ciclo de vida del desarrollo y ayudando a reducir los costosos cuellos de botella de las pruebas de seguridad, que pueden producirse al final del ciclo de cada versión.

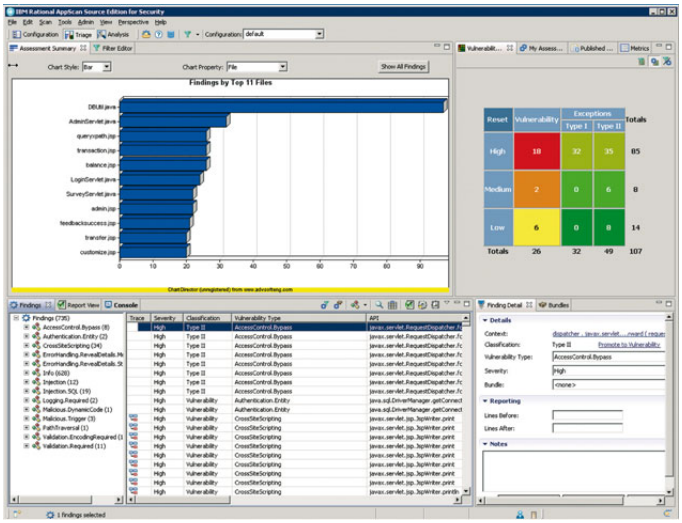

Figura 2: el software Rational AppScan Source Edition proporciona un espacio de trabajo para configurar aplicaciones y proyectos, explorar código, analizar, priorizar y llevar a cabo acciones en relación con las vulnerabilidades prioritarias. Resulta posible publicar valoraciones acerca del software Rational AppScan Enterprise Edition de cara a la correlación.

Características del software Rational AppScan Source Edition

- Corrige la causa raíz de los riesgos de intrusión en los datos a través de la identificación y la resolución de los defectos de seguridad en el origen y en las fases iniciales del ciclo de vida de la aplicación.
- Crea, distribuye y obliga a cumplir unas políticas coherentes y refuerza las métricas a nivel empresarial con una política centralizada y una base de datos de valoración.
- Incluye una cartera extensa de aplicaciones grandes y complejas en una amplia gama de lenguajes.
- Crea una seguridad automatizada en el proceso de desarrollo mediante una integración invisible del análisis de seguridad del código fuente en la exploración automatizada durante el proceso de compilación.
- Facilita la colaboración entre los equipos de seguridad y desarrollo ofreciendo una priorización flexible y una resolución que automatiza el flujo de información entre estos equipos.
- Proporciona un método de certificación de las aplicaciones externalizadas mediante la creación de requisitos de seguridad en los contratos de externalización y el aprovechamiento del software Rational AppScan Source Edition para gestionar los criterios de aceptación.
- Proporciona opciones para la seguridad, el desarrollo y los tipos de resolución de los usuarios.
- Permite a los equipos de seguridad explorar, marcar el nivel de importancia, gestionar políticas de seguridad y priorizar la asignación de resultados para la resolución de vulnerabilidades.
- Ayuda a los equipos de desarrollo a aislar las vulnerabilidades y proporciona consejos de resolución precisos y detallados de cara a obtener unos arreglos rápidos, todo ello dentro del IDE de desarrollo.

IBM Rational AppScan Enterprise Edition

Un escalado de las pruebas de la seguridad de las aplicaciones en toda la empresa

Con su arquitectura basada en web, el software Rational AppScan Enterprise Edition ha sido diseñado para ayudar a las organizaciones a distribuir las responsabilidades en relación con las pruebas de seguridad y a proporcionar visibilidad y acceso a los responsables del proceso. La escalabilidad y un control centralizado facilitan las prestaciones necesarias de gobernanza, colaboración y gestión de riesgos para llevar a cabo de forma eficaz las pruebas de seguridad en toda la empresa. AppScan Enterprise Edition permite garantizar una comunicación y una coordinación oportuna entre los distintos equipos a medida que se priorizan los resultados, se realiza un seguimiento de los mismos y se resuelven. Asimismo, proporciona informes de conformidad con las normativas y una visión global de la conformidad, mientras que las vistas de gestión ofrecen unos paneles de control en tiempo real y las tendencias de la posición de seguridad de la organización. Enterprise Edition también está disponible como oferta de software como servicio (SaaS), permitiéndole aprovechar la experiencia y los procesos demostrados de Rational, su facilidad de escalado y de adición de usuarios a medida que sea necesario, y la obtención de un mayor control sobre los costes.

Características del software Rational AppScan Enterprise Edition

Además de la comodidad y la capacidad de ampliación de la administración centralizada, entre las características del software Rational AppScan Enterprise Edition se incluyen las siguientes:

- La capacidad de distribuir las pruebas de seguridad a varios equipos para aliviar la sobrecarga de pruebas en la organización de seguridad, y para explorar y probar cientos de aplicaciones de forma simultánea, volviéndolas a probar con frecuencia, tras los cambios.
- Una herramienta de pruebas de exploración rápida (QuickScan) para ejecutar plantillas de exploración definidas por el administrador para los desarrolladores y otros profesionales externos a la seguridad, sin tener que realizar configuraciones o instalaciones de escritorio.
- Un repositorio de datos central que almacena y agrega automáticamente resultados de pruebas de análisis estático y dinámico para permitir diversas vistas y acceso a nivel de toda la empresa.
- Una correlación automatizada de resultados de pruebas de análisis estático y dinámico (análisis híbrido) para obtener unos resultados más precisos y para tener la capacidad de aislar los problemas en las líneas de código específicas y acelerar de este modo las tareas de resolución.

Características del software Rational AppScan Enterprise Edition

- Una consola basada en web que proporciona un acceso de usuario basado en roles a los informes de seguridad, seguimiento y tendencias a lo largo del tiempo, lo cual facilita la comunicación en toda la organización.
- Unos paneles de control ejecutivos e informes de análisis de diferencias que resaltan los cambios entre las distintas exploraciones, incluyendo los problemas de seguridad solucionados, pendientes y nuevos.
- Unos controles centralizados para supervisar y controlar las pruebas de vulnerabilidades de las aplicaciones web en toda la organización.

IBM Rational AppScan OnDemand

Aproveche los procesos demostrados y la experiencia en seguridad de IBM en un modelo de software como servicio (SaaS) externalizado listo para entrar en funcionamiento

Mediante el acceso a las características del software Rational AppScan como servicio gestionado, podrá aprovechar las ventajas del producto sin los costes que implican la adición de hardware o la contratación de personal adicional.

Características del software Rational AppScan como servicio gestionado

- Un entorno de pruebas de seguridad de primer nivel.
- Un enfoque centrado en la protección del entorno operativo: estos servicios se han creado con unas técnicas y unas herramientas de seguridad sofisticadas.
- Asistencia personalizada de seguridad y conformidad por parte de los profesionales de IBM.
- Los clientes de tipo SaaS de Rational AppScan Standard Edition o de Rational AppScan Enterprise Edition pueden contactar con un analista de seguridad de IBM y obtener asistencia para:
  - Configurar y ajustar las exploraciones para asegurar preventivamente la cobertura integral de cada aplicación.
  - Revisar y analizar los resultados para ayudar a eliminar falsos positivos, identificar patrones, priorizar problemas y resaltar tareas de resolución.
  - Realizar un seguimiento del progreso de las resoluciones manteniendo datos acerca de las tendencias, siguiendo la resolución entre las distintas exploraciones e informando acerca de la eficacia de la resolución.

Para obtener más información

Para obtener más información acerca de los productos IBM Rational AppScan, póngase en contacto con su representante de IBM o su IBM Business Partner, o visite la dirección: **ibm.com**/software/rational/offerings/testing/webapplicationsecurity

Formación basada en web

IBM ofrece formación en seguridad de aplicaciones basada en web, suministrada online y en intervalos de 15 minutos. Además de la formación básica del producto, el servicio de formación proporciona consejos para desarrolladores equipos de QA y profesionales de la seguridad.

Además, las soluciones financieras de IBM Global Financing pueden permitir una gestión financiera eficiente, una protección frente a la obsolescencia tecnológica, una mejora del coste total de la propiedad y una amortización de la inversión. Es más, nuestros servicios de recuperación global de activos, Global Asset Recovery Services, le ayudarán a mantener bajo control pequeños problemas relacionados con el medio ambiente gracias a sus soluciones nuevas y de mayor eficacia energética. Para obtener más información acerca de IBM Global Financing, visite la dirección: **ibm.com**/financing

IBM Corporation
Software Group
Route 100
Somers, NY 10589
EE.UU.

Producido en los EE.UU.
Diciembre de 2010

Rational. software

RAB14001-ESES-03