

Protección estratégica para aplicaciones Web
para respaldar sus objetivos de negocio



Rational software

IBM Rational AppScan: cómo mejorar la seguridad y el cumplimiento regulator de la aplicación Web.



¿Las aplicaciones Web sin probar ponen en riesgo su negocio?

Muchas organizaciones dependen del software basado en la Web para ejecutar sus procesos de negocio, realizar transacciones y entregar servicios cada vez más sofisticados a los clientes. Desafortunadamente, en la carrera por cumplir las fechas de entrega y mantenerse a la cabeza de la competencia, muchas empresas no realizan pruebas de seguridad adecuadas ni se toman el tiempo para asegurarse de que las aplicaciones están en cumplimiento con las normas reguladoras y de la industria. El resultado es que muchas compañías pueden exponer involuntariamente datos corporativos o personales a los delincuentes cibernéticos quienes pueden explotar estas vulnerabilidades por diversión y dinero, poniendo en riesgo a toda la empresa. Además, debido a que muchos requisitos reguladores hacen obligatorio un grado de seguridad de la aplicación, estas organizaciones también corren el riesgo de entrar en incumplimiento en cuanto a los requisitos de auditoría, lo cual puede resultar en multas y reacciones violentas por parte de los clientes. Para ayudar a proteger los activos valiosos de su compañía, es importante probar las aplicaciones Web a lo largo de su ciclo de vida completo, mientras son desarrolladas y después de que se implementan en la producción.

El software IBM Rational® AppScan® es un paquete de soluciones de seguridad y cumplimiento para aplicaciones Web líder del mercado que puede ayudar a resolver los desafíos críticos en cuanto a la seguridad y el cumplimiento de la aplicación. El paquete incluye:

- IBM Rational AppScan Standard Edition
- IBM Rational AppScan Express Edition
- IBM Rational AppScan Tester Edition
- IBM Rational AppScan Developer Edition
- IBM Rational AppScan Build Edition
- IBM Rational AppScan Enterprise Edition
- IBM Rational AppScan Reporting Console
- IBM Rational AppScan OnDemand
- IBM Rational AppScan OnDemand Production Site Monitoring
- Capacitación basada en la Web de IBM Rational para AppScan

Todas las soluciones ofrecen funcionalidad de escaneo, generación de informes y recomendaciones de reparación. Además, están diseñadas para ser efectivas y fáciles de utilizar. De manera que sin importar si su gente es nueva en cuanto a la seguridad de la aplicación Web o son usuarios avanzados quienes pueden crear complementos personalizados para extender las capacidades de prueba de su compañía, podrá aprovechar el portafolio de Rational AppScan.

Proteja sus activos de negocio críticos basados en la Web

Al ofrecer capacidades de seguridad completas para aplicaciones Web complejas, el paquete de software Rational AppScan examina y prueba vulnerabilidades comunes de la aplicación Web, incluyendo aquellas que identificó la clasificación de amenazas del Consorcio de Seguridad de Aplicación Web (WASC). Las soluciones de Rational AppScan comparten una extensa gama de funciones centrales potentes y flexibles para ofrecer una cobertura de examinación de aplicaciones robusta para las últimas tecnologías Web 2.0, incluyendo soporte mejorado para la tecnología Adobe® Flash y los lenguajes JavaScript avanzados, junto con soporte completo para el JavaScript asíncrono y el lenguaje de programación XML (AJAX). Además, cada vez que el usuario lanza una aplicación Rational AppScan, el software descarga notificaciones sobre las amenazas de seguridad más recientes, de manera que usted contará con información actualizada de IBM.





Vista del asesor de seguridad de IBM Rational AppScan

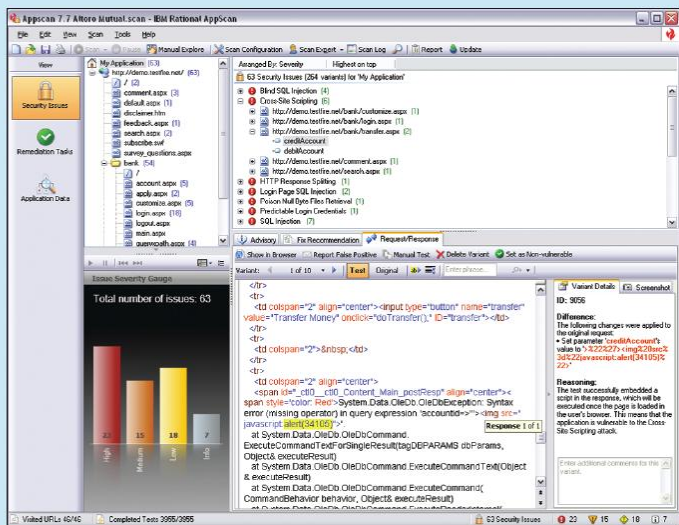
Manténgase por encima de los problemas de cumplimiento

Las ofertas de Rational AppScan incluyen informes de cumplimiento para ayudar a que su compañía rastree su cumplimiento de los requisitos clave reguladores y de la industria, incluyendo la Publicación Especial del Instituto Nacional de Tecnología y Normalización (NIST SP) 800-53 y los 10 principales del Proyecto Abierto de Seguridad en Aplicaciones Web (OWASP), Normas de Seguridad de Datos de la Industrias de Tarjetas de Pago (PCI DSS), la Ley Sarbanes-Oxley, la Ley Gramm-Leach-Bliley (GLBA), Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA), Ley de Derechos Educativos y de Privacidad de la Familia (FERPA), Ley de Libertad de Información y Protección de la Privacidad (FIPPA) y Mejores Prácticas para Aplicaciones de Pagos (PABP). Además, los usuarios pueden producir informes de seguridad personalizados y seleccionar qué puntos de datos se deben incluir en cada informe, lo que permite satisfacer los requisitos de cumplimiento críticos.

Rational AppScan Standard Edition: Lleve a cabo auditorías de seguridad y el monitoreo de la producción

Para automatizar los procesos de prueba de la aplicación Web con la finalidad de ayudar a que los auditores de seguridad y probadores de penetración realicen sus trabajos rápida y eficientemente se requiere tecnologías de examinación sofisticadas e inteligentes. Rational AppScan Standard Edition incluye funciones diseñadas para respaldar a los usuarios moderados y avanzados. Las funciones incluyen:

- El experto de escaneo, una herramienta basada en un asistente que ofrece guía para la creación y configuración de exámenes con base en las mejores prácticas, incluyendo el uso de herramientas adicionales. Los usuarios pueden automatizar un escaneo previo que crea el perfil de la aplicación objetivo y recomienda las acciones que se requieren para un examen exitoso.
- El inductor de estado, el cual escanea y prueba procesos de negocio complejos (tales como carros de compra en línea de múltiples pasos y seguimiento de pedidos), y conserva valores del parámetro y cookies a lo largo del proceso.
- Plantillas de escaneo predefinidas que permiten que los usuarios elijan y lancen rápidamente opciones de configuración.
- Un asistente de configuración de escaneo rápido que guía a los usuarios a lo largo de configuraciones importantes, así como pasos condicionales para la autenticación del proxy/plataforma e información de detección en sesión.
- Generación de informes basados en las plantillas de Microsoft® Word.
- Módulos de capacitación incrustados basados en la Web que ayudan a explicar los problemas y demostrar las explosiones.



Vista de los problemas de seguridad de IBM Rational AppScan



Vista de remediación de IBM Rational AppScan

Rational AppScan Express Edition: Obtenga funciones de seguridad robustas de la aplicación Web a un punto de precio atractivo

Las organizaciones con equipos de desarrollo de aplicaciones pequeños o limitados también necesitan considerar las pruebas de seguridad como parte del ciclo de vida del desarrollo. Sin embargo, estas organizaciones con frecuencia tienen que sacrificar la funcionalidad por la asequibilidad. Rational AppScan Express Edition cumple los requisitos de las organizaciones medianas al entregar la funcionalidad de pruebas de seguridad sin compromiso que se encuentran en IBM Rational AppScan Standard Edition a un punto de precio atractivo. Diseñada para facilitar la implementación, Rational AppScan Express Edition reduce en gran medida el tiempo y los costos asociados con las pruebas manuales de vulnerabilidad, lo que permite que sus equipos se concentren en otras necesidades relacionadas con la TI y seguridad dentro de su organización.

Rational AppScan Tester Edition: Convierta las pruebas de seguridad en una parte de su programa de administración de la calidad

Rational AppScan Tester Edition, disponible como una aplicación de escritorio, ofrece capacidades para ayudar a que los equipos de aseguramiento de la calidad (QA) integren pruebas de seguridad en los procesos existentes de administración de la calidad, de ese modo se aligera la carga sobre los profesionales de seguridad. Debido a que Rational AppScan Tester Edition se integra con los sistemas de prueba líderes, los profesionales de QA pueden utilizar su funcionalidad en los guiones de prueba y realizar verificaciones de seguridad dentro de sus entornos de prueba familiares, lo que facilita la adopción de pruebas de seguridad junto con pruebas de funcionalidad y rendimiento.



Rational AppScan Developer Edition: Incruste pruebas de seguridad en su ambiente de desarrollo

La manera más efectiva de adelantarse a las vulnerabilidades de seguridad de la aplicación es integrar software de manera segura desde el principio. El reto es que la mayoría de los desarrolladores no son expertos en seguridad, y escribir código seguro no siempre es su principal prioridad. De manera que la mejor forma de involucrar el desarrollo en el proceso de la seguridad de la aplicación es brindarles herramientas que funcionan en su ambiente y que generan resultados en lenguajes que comprenden.


Rational AppScan Developer Edition está diseñada para facultar a los desarrolladores para que invoquen pruebas de seguridad de la aplicación Web directamente desde su ambiente de desarrollo. Permite que la organización de desarrollo resuelva el volumen de problemas de seguridad que se pueden introducir en el código, al agilizar el flujo de trabajo del ciclo de vida del desarrollo y ayudar a reducir los costosos cuellos de botella de las pruebas de seguridad que pueden ocurrir al final del ciclo de vida de la liberación.

Rational AppScan Developer Edition utiliza una gama de técnicas de análisis para detectar con precisión los problemas de seguridad en las aplicaciones Web, incluyendo análisis de código estático, análisis dinámicos, análisis de tiempo de ejecución y análisis de cadenas pendiente de patente de IBM.

Rational AppScan Build Edition: Integre análisis de seguridad en el ambiente de desarrollo

Rational AppScan Build Edition soporta pruebas de seguridad automatizadas en la etapa de integración del ciclo de vida de desarrollo del software. Al integrarse en múltiples sistemas de administración de integración, tales como el software IBM Rational Build Forge®, ofrece cobertura de las pruebas de seguridad para las integraciones programadas. También enruta los resultados de vuelta a desarrollo a través de soluciones de rastreo de defectos tales como el software IBM Rational ClearQuest®, o a través de soluciones de informes de seguridad tales como Rational AppScan Enterprise Edition o Rational AppScan Reporting Console. Rational AppScan Build Edition incluye el mismo conjunto de técnicas de análisis que Rational AppScan Developer Edition, al ofrecer un alto nivel de precisión además de la cobertura de código que ayuda a que usted identifique qué código se aprobó.





Rational AppScan Enterprise Edition: Escale las pruebas de seguridad de la aplicación en toda la empresa

Con su arquitectura basada en la Web, Rational AppScan Enterprise Edition está diseñada para ayudar a que las organizaciones distribuyan la responsabilidad de las pruebas de seguridad entre múltiples partes interesadas.

Además de la conveniencia y capacidad de extensión de la administración centralizada, las funciones de Rational AppScan Enterprise Edition incluyen:

- La capacidad de escanear y probar miles de aplicaciones al mismo tiempo en un sitio Web complejo y volver a probarlas con frecuencia, después de los cambios.
- Una herramienta de pruebas de escaneo rápido para ejecutar plantillas de escaneo definidas por el administrador para desarrolladores y otros profesionales que no están relacionados con la seguridad, sin la instalación y configuración del escritorio.
- Un depósito central de datos que almacena y agrega automáticamente los resultados de las pruebas para ofrecer un acceso a nivel empresa y múltiples vistas.
- Una consola de generación de informes basada en la Web que ofrece acceso basado en el rol a los informes de seguridad y facilita la comunicación en toda la organización.
- Tableros ejecutivos de resultados e informes de los análisis Delta que destacan los cambios de un escaneo al siguiente, incluyendo los problemas de seguridad preparados, pendientes y nuevos.
- Controles centralizados para monitorear y controlar las pruebas de vulnerabilidad de la aplicación Web en toda la organización.
- Módulos incrustados de capacitación basados en la Web que ayudan a explicar los problemas y demostrar las explosiones.

Rational AppScan Reporting Console: Acceda a informes centralizados sobre los datos de vulnerabilidad de la aplicación Web

IBM Rational AppScan Reporting Console es una potente aplicación de administración y generación de informes basada en la Web. Totalmente integrada con la Rational AppScan Standard Edition, Rational AppScan Reporting Console está respaldada por una base de datos de clase empresarial que permite que usted consolide los resultados de los escaneos desde múltiples clientes Rational AppScan para crear un depósito centralizado de vulnerabilidades de la aplicación. Los resultados de los escaneos se pueden distribuir fácilmente al departamento de aseguramiento de calidad y equipos de desarrollo sin tener que instalar licencias de escritorio adicionales, lo que ayuda a simplificar el proceso de remediación e integrar análisis de vulnerabilidad en todo el ciclo de vida de desarrollo del software. Rational AppScan Reporting Console le permite crear múltiples tableros de resultados para múltiples usuarios, lo que ofrece a las personas la capacidad de segmentar los datos de seguridad por aplicación, unidad de negocio, geografía o proveedor tercero.

Rational AppScan OnDemand: Administre la seguridad de la aplicación Web sin inversiones iniciales

La oferta IBM Rational AppScan OnDemand es una solución SaaS que permite que usted administre la seguridad de la aplicación Web sin las inversiones iniciales. Al entregar resultados con base en los cuales se puede emprender una acción rápida, el servicio utiliza el software IBM Rational AppScan Enterprise Edition y es alojado y ejecutado por un equipo experimentado de expertos en seguridad y cumplimiento de IBM. Rational AppScan OnDemand ofrece escaneos mensuales sobre la seguridad de la aplicación, capacidades de consolidación de datos y generación de informes, capacidades de remediación, tableros ejecutivos de resultados y generación de informes de cumplimiento para las aplicaciones Web de preproducción en los departamentos de aseguramiento de la calidad y fases de prueba de seguridad. La oferta proporciona una solución que se contrata externamente para pruebas de seguridad de la aplicación Web con un costo inicial económico, un tiempo rápido para obtener valor y un costo total de propiedad competitivo.



Rational AppScan OnDemand Production Site Monitoring: Mantenga la seguridad de la aplicación Web después del lanzamiento de las aplicaciones

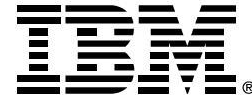
La oferta IBM Rational AppScan OnDemand Production Site Monitoring es un producto SaaS que utiliza un subconjunto no invasivo de la política de prueba de IBM Rational AppScan Enterprise Edition para monitorear las aplicaciones de producción en cuanto a las vulnerabilidades que se pueden producir después de que las aplicaciones entran en producción. Si sus equipos de marketing, negocios electrónicos o Web actualizan, cambian o empujan contenido nuevo a sus aplicaciones Web, pueden introducir nuevas vulnerabilidades que ponen en riesgo la información confidencial de su organización. Además, todos sabemos que las principales liberaciones de aplicación necesitan reparaciones rápidas (hot fixes), soportes para interrupciones del servicio (break fixes) y cambios estructurales que pueden ofrecer nuevos puntos débiles de ataque para los hackers. Para mantener las aplicaciones Web ricas en seguridad, usted debe monitorear continuamente sus sitios Web en cuanto a las vulnerabilidades, mucho después de las fechas en que entran en producción.



Vista del tablero de resultados de IBM Rational Scan Enterprise Edition

Un ambiente de pruebas de seguridad de punta

Tanto Rational AppScan OnDemand como Rational Packaged AppScan OnDemand Production Site Monitoring se ejecutan en un ambiente host escalable y privado con servicios de seguridad avanzados del centro de datos para ayudar a garantizar la seguridad de sus datos. Administrado por ingenieros experimentados y especialistas en seguridad, quienes se dedican a la protección de los datos y sistemas, el ambiente host consiguió la certificación Tipo II de las Declaraciones sobre las Normas de Auditorías (SAS) No. 70. IBM evalúa continuamente los desarrollos y amenazas de seguridad emergentes, al implementar tecnologías probadas y actualizadas para ayudar a garantizar que su información confidencial está protegida.



Ayude a prevenir los problemas de administración de la seguridad y cumplimiento con capacitación basada en la Web

IBM ofrece capacitación de seguridad de la aplicación basada en la Web, la cual se imparte en línea y en intervalos de 15 minutos. Además de instrucciones básicas del producto, el servicio de capacitación ofrece asesoría dirigida para los desarrolladores, equipos de aseguramiento de la calidad y profesionales de seguridad. Las pruebas en línea para los tres niveles de certificación de conocimientos de productos están disponibles a través del proceso instruccional, y los gerentes pueden rastrear el progreso del empleado a través de un tablero de resultados de administración que está disponible en línea y Rational AppScan Enterprise Edition.

Para obtener más información

Para conocer más acerca de cómo puede aprovechar usted los productos de IBM Rational AppScan para hacer que sus aplicaciones Web sean más ricas en cuanto a la seguridad y estén en cumplimiento, póngase en contacto con su representante de IBM o Socio de Negocios de IBM, o visite:

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

© Derechos de Reproducción IBM Corporation 2009

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

Producido en los Estados Unidos de Norteamérica
Abril del 2009
Todos los derechos reservados

IBM, el logotipo de IBM, ibm.com, Rational y AppScan son marcas comerciales o marcas comerciales registradas de International Business Machines Corporation en los Estados Unidos, otros países o ambos. En caso de que éstos y otros términos relacionados con las marcas comerciales de IBM aparezcan marcados en su primera aparición en esta información con un símbolo de marca comercial registrada (® o ™), estos símbolos indican que son marcas comerciales registradas o de derecho consuetudinario en los Estados Unidos propiedad de IBM al momento de la publicación de esta información. Dichas marcas comerciales pueden ser también marcas comerciales registradas o de derecho consuetudinario en otros países. Hay una lista actual de las marcas comerciales de IBM disponible en la Web en "Información sobre los derechos de reproducción y marcas comerciales" en ibm.com/legal/copytrade.shtml

Adobe es una marca comercial registrada o marca comercial de Adobe Systems Incorporated en los Estados Unidos y otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas comerciales de Microsoft Corporation en los Estados Unidos, otros países, o ambos.

Otros nombres de compañías, productos o servicios pueden ser las marcas comerciales, marcas comerciales registradas o marcas de servicio de otras compañías.

Las referencias de esta publicación a los productos o servicios de IBM no implican que IBM pretenda ponerlos a disposición en todos los países en los que opera IBM.

La información contenida en esta documentación se proporciona únicamente para fines informativos. Si bien se realizan esfuerzos para verificar la totalidad y precisión de la información contenida en este documento, se proporciona "como es" sin garantía de ningún tipo, expresa o implícita. Además, esta información se basa en los planes y la estrategia de producto actuales de IBM, los cuales están sujetos a cambio por parte de IBM sin previo aviso. IBM no se hará responsable de ningún daño que surja por el uso de, o de otra forma relacionado con, esta documentación o cualquier otra documentación. Ninguna parte del contenido de esta documentación pretende, ni tendrá el efecto de, crear alguna garantía o representación de IBM (o sus proveedores o licenciarios), o alterar los términos y condiciones del contrato de licencia aplicable que rige el uso del software IBM.

Los clientes de IBM son responsables de asegurar su propio cumplimiento de los requisitos jurídicos. Es responsabilidad exclusiva del cliente obtener asesoría por parte de un asesor jurídico competente en cuanto a la identificación e interpretación de cualquier ley y requisito regulatorio relevantes que puedan afectar el negocio del cliente y cualquier acción que pueda ser necesaria que emprenda el cliente para cumplir dichas leyes.

