Protección estratégica de activos Web
como apoyo para sus objetivos empresariales

Rational. software

IBM

Solución de ciclo de vida IBM Rational AppScan: cómo proteger el acceso a software y sistemas mediante seguridad para aplicaciones Web.

¿Las vulnerabilidades de la Web ponen en peligro su empresa?

Actualmente, numerosas organizaciones dependen de software y sistemas Web para realizar sus procesos, efectuar transacciones con proveedores y ofrecer servicios cada vez más avanzados a sus clientes. Proteger todas las aplicaciones destinadas al despliegue online debe ser parte integral de los procesos de suministro de software y sistemas en toda organización bien dirigida. Por desgracia, en la carrera por adelantarse a la competencia, muchas empresas dedican poco tiempo a esta cuestión debido a la urgente necesidad de comercializar nuevos productos. Las vulnerabilidades resultantes pueden ofrecer grandes oportunidades a los hackers para el acceso o sustracción de información corporativa o personal, posiblemente poniendo en peligro a toda la empresa.

IBM Rational® AppScan® es una suite líder de soluciones de seguridad para aplicaciones Web, creada para dotar a las organizaciones de la visibilidad y control necesarios para afrontar este grave problema. La suite incluye:

- IBM Rational AppScan Standard Edition (disponible como aplicación para ordenador o en forma de software como servicio [SaaS]).
- IBM Rational AppScan Tester Edition (disponible como aplicación para desktop).
- IBM Rational AppScan Enterprise Edition (disponible como solución Web o SaaS).

Todas estas completas soluciones realizan exploraciones, elaboran informes, recomiendan soluciones y son idóneas para cualquier clase de pruebas de seguridad efectuada por diversos tipos de usuarios, incluyendo desarrolladores de aplicaciones, equipos de control de calidad (QA), verificadores de penetración, auditores de seguridad y altos directivos.

Al igual que las demás soluciones de ciclo de vida de la plataforma de desarrollo IBM Rational, los productos Rational AppScan permiten al usuario trabajar en un entorno conocido y ofrecen una perfecta integración con las herramientas de QA y entornos de desarrollo integrados (IDE) más importantes. Estas aplicaciones permiten efectuar auditorías de seguridad continuas, lo que ayuda a los equipos de suministro de software a dotar de seguridad a las aplicaciones Web desde cero, contribuyendo a reducir los riesgos para la empresa antes incluso de desplegar sus aplicaciones.

Protección para sus activos empresariales en la Web

Las soluciones Rational AppScan Standard, Rational AppScan Tester y Rational AppScan Enterprise ofrecen una completa cobertura de seguridad para sitios Web complejos, explorando y comprobando vulnerabilidades comunes en aplicaciones Web, incluyendo aquellas identificadas en la clasificación de amenazas del Web Application Security Consortium (WASC). Las soluciones Rational AppScan comparten una amplia variedad de potentes y flexibles funciones básicas que abarcan la exploración de aplicaciones que utilicen las tecnologías Web 2.0 más recientes, incluyendo compatibilidad ampliada con Flash y lenguajes Java™ Script avanzados, combinada con una completa cobertura para el lenguaje de programación Ajax (con pruebas específicas para JavaScript Object Notation [JSON] y parámetros para servicios Web).

Las funciones básicas de Rational AppScan orientadas a una exploración eficaz y a facilitar su uso incluyen:

- Una interfaz de usuario que permite seleccionar vistas como diagrama de aplicación, listas jerárquicas de problemas de seguridad detectados, vistas de correcciones para los desarrolladores y paneles de detalles.
- Un proceso de prueba adaptativo con el que es posible analizar los parámetros de la aplicación y seleccionar únicamente aquellas pruebas relevantes que no obstruyan el proceso de desarrollo.
- Soporte para autentificaciones complejas destinado a verificar procedimientos de autentificación en varios pasos para aplicaciones Web, incluyendo la autentificación gradual con el método Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA), autentificación multifactor, contraseña única, llaves Universal Serial Bus (USB), tarjetas inteligentes y autentificación mutua.
- Administración avanzada de sesiones, capaz de iniciar sesiones automáticamente cuando sea necesario.
- Vistas de resultados en tiempo real con las que los usuarios pueden corregir problemas antes de que finalice la exploración.
- Reglas para la búsqueda de pautas que facilitan las pruebas de seguridad relacionadas con tarjetas de crédito, números de la seguridad social u otras secuencias numéricas.

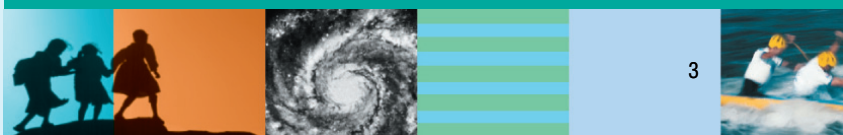
Vista de asesoramiento de seguridad de IBM Rational AppScan

Las funciones básicas de Rational AppScan orientadas a la personalización y el control incluyen:

- Tecnología Rational AppScan eXtensions Framework, que permite a los usuarios crear, compartir y cargar potentes complementos que amplían sus capacidades de verificación.
- Pyscan, que combina Rational AppScan con las capacidades de los scripts Python para permitir a los usuarios emplear las capacidades de exploración del primero sin las limitaciones de una interfaz de usuario. El resultado es un grado de personalización anteriormente fuera del alcance de los profesionales de la seguridad y los verificadores de penetración.
- Kit de desarrollo de software (SDK) Rational AppScan, que permite invocar acciones, desde ejecutar una exploración detallada hasta efectuar una prueba personalizada. Las interfaces del SDK están diseñadas para facilitar la integración y permitir el uso personalizado del motor de exploración, junto con las opciones de Rational AppScan eXtensions Framework y Pyscan.

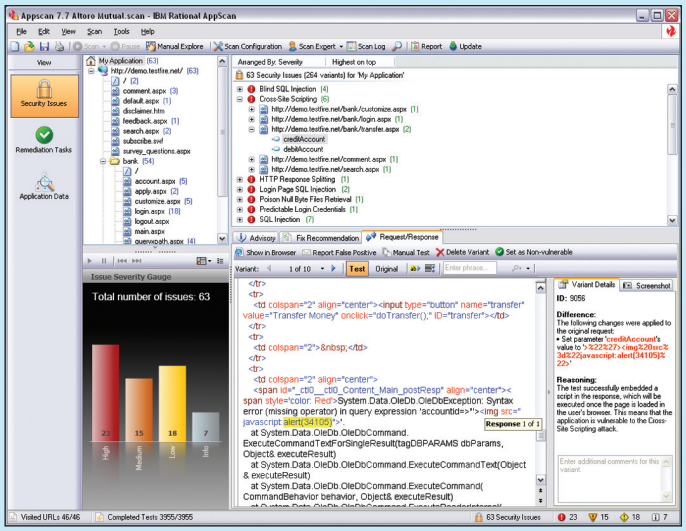
Las funciones básicas de Rational AppScan orientadas a la detección de vulnerabilidades incluyen:

- Cobertura de validación global que analiza las respuestas de las pruebas para detectar problemas activados de forma inadvertida, pruebas Secure Sockets Layer (SSL) (para comprobar la validez de los certificados SSL) y pruebas para detectar falsificaciones de peticiones multisitio (CSRF).
- Simulación de hackers que incluye las 10 principales vulnerabilidades del Open Web Application Security Project (OWASP) y las 20 principales vulnerabilidades del System Administration, Networking, and Security Institute (SANS).
- Información sobre las amenazas más recientes, actualizadas automáticamente cuando se inicia un producto Rational AppScan.
- Una suite de utilidades destinadas a ayudar a verificadores de penetración y consultores de seguridad a desarrollar, probar y depurar aplicaciones Web.

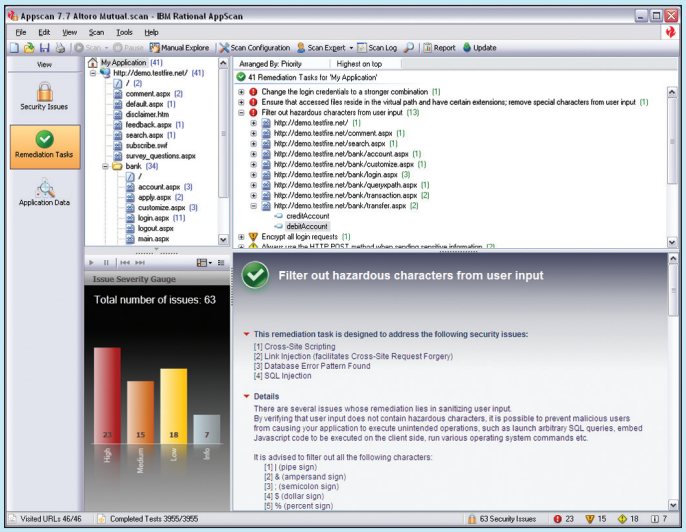


Las funciones básicas de Rational AppScan orientadas a la elaboración de informes y la corrección de problemas incluyen:

- Pruebas relacionadas con más de 40 problemas y estándares de conformidad normativa mundiales, incluyendo la National Institute of Standards and Technology Special Publication (NIST SP) 800-53 y los 10 más importantes según OWASP (actualizados en 2007). La versión 7.7 de Rational AppScan también incluye cobertura para el Family Education Rights and Privacy Act (FERPA), Freedom of Information and Protection of Privacy Act (FIPPA) y Payment Application Best Practices (PABP).
- Resultados de validación que resaltan el código HTML que contiene vulnerabilidades y explican el problema. Una función de comparación muestra el código HTML modificado.
- Informes de corrección que incluyen recomendaciones de corrección Hypertext Preprocessor (PHP) y listas de tareas para los desarrolladores. Estos informes permiten observar problemas relacionados con la aplicación, con la infraestructura o con ambas, así como eliminar variantes o marcarlas como no vulnerables para su posterior revisión.
- Informes detallados de contenidos sospechosos que incluyen elementos como datos confidenciales en comentarios HTML, así como actividad HTTP en torno a contenido sospechoso.
- Descripciones de pruebas que incluyen la ID de vulnerabilidades y riesgos comunes (CVE) incluidos en la base de datos de vulnerabilidades.
- Posibilidad de incorporar capturas de pantalla del explorador interno de Rational AppScan en los informes, así como de extraer, comprimir y codificar información abierta de pruebas específicas para su envío por e-mail. El software AppScan también permite comunicar falsos positivos (o negativos) al equipo de investigación de seguridad de IBM Rational AppScan, lo que contribuye a la mejora constante de la precisión del producto.



Vista de problemas de seguridad de IBM Rational AppScan



Vista de correcciones de IBM Rational AppScan

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

Automatizar las pruebas de aplicaciones Web para los auditores de seguridad y verificadores de penetración requiere tecnologías de exploración sofisticadas e inteligentes. Rational AppScan Standard Edition incluye características específicamente diseñadas para usuarios intermedios y avanzados. Dichas características incluyen:

- Experto en exploración, que proporciona orientación durante la creación y configuración de exploraciones basándose en prácticas recomendadas, incluyendo el uso de herramientas adicionales. Los usuarios pueden autorizar una exploración previa que crea un perfil de la aplicación objetivo y recomienda actuaciones para una exploración válida.
- Inductor de estados, que explora y verifica procesos empresariales complejos, como las compras y seguimiento online en múltiples pasos y conserva los valores de los parámetros y las cookies durante todo el proceso.
- Plantillas de exploración predefinidas que permiten a los usuarios elegir e iniciar rápidamente opciones de configuración.
- Un rápido asistente de configuración que orienta a los usuarios durante los principales ajustes, así como pasos condicionales para la autentificación de proxy/plataforma e información de detección durante la sesión.
- Nuevas pestañas de solicitud/respuesta que ofrecen resaltado de sintaxis, solicitud/respuesta, contraer/expandir, búsquedas durante la escritura y otras opciones disponibles al hacer clic con el botón derecho del ratón.
- Informes creados a partir de plantillas en Microsoft® Word para diseñar formatos personalizados conforme a las normas corporativas. Las plantillas incluyen tabla de contenidos, hora de inicio y finalización de la exploración y gráficas.
- Módulos de formación Web integrados (WBT) que ayudan a explicar los problemas y demostrar las vulnerabilidades, junto con la verificación de resultados, para facilitar su comprensión y comunicación.

Convierta las pruebas de seguridad en parte de su programa de gestión de calidad con el software Rational AppScan Tester Edition

Rational AppScan Tester Edition ofrece funciones que ayudan a los equipos de control de calidad a integrar las pruebas de seguridad en los procesos de gestión de calidad ya existentes, aligerando de este modo la carga de trabajo de los profesionales de la seguridad.

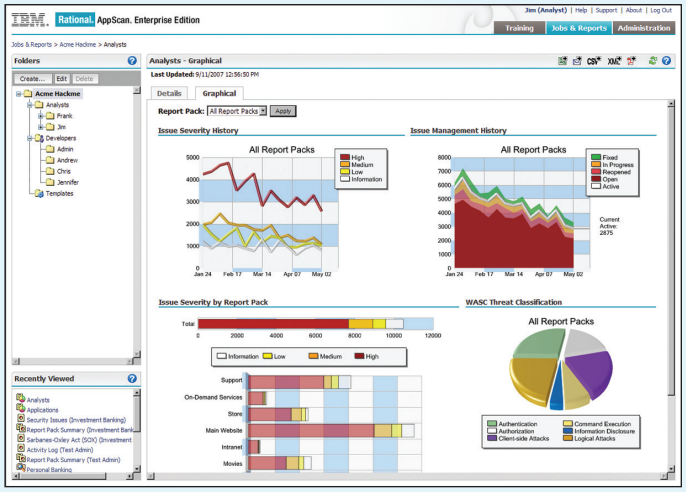
Gracias a su integración en los principales sistemas de pruebas, los profesionales de control de calidad pueden utilizar las funciones de Rational AppScan en scripts de prueba y realizar comprobaciones de seguridad en los entornos que utilizan habitualmente, facilitando así ejecución de las pruebas de seguridad junto con las pruebas de funcionamiento y rendimiento.

Extienda la comprobación de seguridad de las aplicaciones a toda la empresa con el software Rational AppScan Enterprise Edition

El software Rational AppScan Enterprise Edition, con su arquitectura basada en Web, ha sido diseñado para ayudar a las organizaciones a distribuir la responsabilidad de sus comprobaciones de seguridad entre múltiples participantes y ayudar a los usuarios a descubrir vulnerabilidades al principio del ciclo de suministro de aplicaciones Web, cuando corregirlos es sencillo y rentable.

Además de la comodidad y capacidad de ampliación de la administración centralizada, Rational AppScan Enterprise Edition ofrece:

- La posibilidad de explorar y comprobar miles de aplicaciones simultáneamente en un sitio Web complejo y repetir la comprobación frecuentemente después de realizar cambios.
- Una sencilla herramienta de exploración rápida que permite a los desarrolladores y otros profesionales ajenos a la seguridad ejecutar plantillas de exploración definidas por un administrador, sin necesidad de instalarlas o configurarlas en su ordenador.
- Una base central de datos que almacena y recopila automáticamente los resultados de las pruebas para su acceso y visualización desde toda la empresa. Los usuarios pueden segmentar y observar las tendencias de las vulnerabilidades por unidad de negocio, geografía o proveedores externos.
- Una consola de informes basada en Web que proporciona acceso por roles a los informes de seguridad y facilita la comunicación dentro de la organización. Los usuarios pueden filtrar y ordenar los problemas por prioridades, además de especificar su estado: pendiente, en proceso o cerrado.
- Paneles de control ejecutivos e informes de análisis delta destacan los cambios producidos de una exploración a otra, incluyendo problemas de seguridad solucionados, pendientes o de nueva aparición.
- Controles centralizados para la monitorización y control de las pruebas de vulnerabilidad de aplicaciones Web en toda la organización.
- Módulos WBT integrados que explican los problemas y demuestran la vulnerabilidad, además de verificar los resultados, para facilitar la comprensión y comunicación de las vulnerabilidades.



Vista de panel de control de IBM Rational AppScan Enterprise Edition

Las capacidades de Rational AppScan Standard y Rational AppScan Enterprise están disponibles como SaaS

Al acceder a las capacidades de Rational AppScan en forma de servicio administrado, podrá beneficiarse de todas sus ventajas sin el coste que implica agregar nuevo personal o hardware.

Un entorno de seguridad de nueva generación

Creados para proteger su entorno operativo, estos servicios disponen de sofisticadas herramientas y técnicas de seguridad.

Su propio experto en seguridad y conformidad

Como cliente de Rational AppScan Standard o Rational AppScan Enterprise, puede contar con un analista de seguridad IBM Rational para ayudarle a:

- Configurar y ajustar las exploraciones para garantizar la cobertura de todas las aplicaciones.
- Estudiar y analizar los resultados para eliminar falsos resultados positivos y negativos, identificar pautas, asignar prioridades a los principales problemas y destacar las tareas de corrección más importantes.
- Seguir la evolución de las correcciones manteniendo los datos de tendencias, siguiendo la resolución de los principales problemas en cada exploración e informando sobre la eficacia de la corrección.
- Formar a su personal de QA para que utilice Rational AppScan durante el ciclo de suministro de aplicaciones Web, ayudando a dotarlas de seguridad y gestionando la conformidad de sus aplicaciones desde cero.

Resuelva sus problemas de seguridad y gestión de la conformidad mediante la formación a través de la Web

La familia de productos IBM Rational AppScan incluye formación a través de la Web, con contenidos online creados a partir de una década de experiencia y prácticas recomendadas obtenida en despliegues efectuados en difíciles y complejos entornos Web. Además de instrucción básica en el uso del producto, el servicio proporciona asesoramiento específico para desarrolladores, equipos de control de calidad y profesionales de la seguridad.

Impartidos en intervalos de 15 minutos y posteriormente archivados, los módulos del servicio están disponibles para los usuarios desde cualquier lugar y a cualquier hora. En sesiones prácticas especiales, los usuarios también recibirán orientación en tiempo real de los expertos de seguridad de Rational AppScan.

Se ofrecen tests online para obtener la certificación en tres niveles de conocimiento del producto durante todo el proceso de formación. Los directivos pueden seguir los progresos de los empleados por medio de un panel de control disponible tanto online como en Rational AppScan Enterprise Edition.

Requisitos del sistema

Procesador	Intel® Pentium® P4 de 1,5 GHz (recomendado 2,4 GHz)
Memoria	512 Mb de RAM (recomendado 1 Gb para explorar grandes sitios)
Espacio libre en disco	1 Gb (recomendado 10 Gb para explorar grandes sitios)
Red	Tarjeta de interfaz de red (NIC) de 10 Mb/s para la comunicación de red con TCP/IP (recomendado 100 Mb/s)
Sistema operativo	Microsoft Windows® XP, Windows 2000, Windows 2003 Enterprise Edition, Windows Vista
Navegador Web	Microsoft Internet Explorer 5.5 o superior (recomendado 6.0 o superior)
	Microsoft .NET framework 2.0 o superior
	Java Runtime Environment (JRE) 5.0 (solamente para proxy HTTP de Rational AppScan)

Más información

Para obtener más información sobre los productos IBM Rational AppScan, póngase en contacto con su representante IBM o IBM Business Partner o visite:

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

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

Producido en Estados Unidos
Diciembre de 2007

RAB14001-USEN-00