

QUALYS GUARD® WEB APPLICATION SCANNING

SEGURIDAD PARA APLICACIONES WEB QUE SE ESCALA HASTA UN NÚMERO ILIMITADO DE SITIOS WEB – BAJO DEMANDA

Actualmente las vulnerabilidades en las aplicaciones Web son el vector más grande para los ataques contra la seguridad empresarial. Las historias acerca de ataques que comprometen los datos delicados suelen mencionar que los culpables son “cross-site scripting”, “SQL injection” y “malas configuraciones de los sitios Web”. Con frecuencia, las vulnerabilidades de este tipo quedan fuera de la experiencia tradicional de los administradores de seguridad de las redes. Por lo tanto, la relativa oscuridad de las vulnerabilidades de las aplicaciones Web las vuelve útiles para los ataques. Como muchas organizaciones han descubierto, estos ataques evadirán las defensas tradicionales de las redes empresariales a menos que se coloquen nuevas defensas. Las vulnerabilidades de la seguridad de las aplicaciones Web por lo general se originan a partir de malas configuraciones o de errores en la programación con un lenguaje de programación de aplicaciones Web (por ejemplo, Java, .NET, PHP, Python, Perl, Ruby), una biblioteca de código, un patrón de diseño o una arquitectura. Estas vulnerabilidades pueden ser complejas y pueden ocurrir bajo muchas circunstancias distintas.

Presentamos QualysGuard® Web Application Scanning

Para ayudar a que sus clientes evalúen y rastreen las vulnerabilidades de las aplicaciones Web, Qualys® está presentando a un nuevo miembro de la suite QualysGuard® Security and Compliance: QualysGuard Web Application Scanning (WAS) 1.0. Este nuevo servicio, que se entrega bajo demanda, ofrece inspección automatizada y pruebas para las aplicaciones Web personalizadas con el fin de identificar la mayoría de las vulnerabilidades que aparecen en OWASP Top 10 y en la clasificación de amenazas WASC, incluyendo “SQL injection” y “cross site scripting”. Los usuarios pueden administrar las aplicaciones Web, ejecutar escaneos y generar reportes empleando la conocida interfaz de usuario de QualysGuard.



Beneficios de QualysGuard WAS

- Reduce el costo total de las operaciones al automatizar los procesos de pruebas que se pueden repetir
- Identifica las vulnerabilidades de la sintaxis y la semántica en las aplicaciones Web personalizadas
- Realiza un perfil de la aplicación y ejecuta auditorías y una inspección autenticada
- Mejora la precisión y reduce los falsos positivos a través de los perfiles de un sitio Web
- Se escala para escanear cualquier número de aplicaciones Web, de producción interna o externa, o entornos de desarrollo, usando la plataforma Software como servicio (SaaS, por las siglas de Software-as-a-Service) de QualysGuard

“Las soluciones de clase empresarial para el escaneo de aplicaciones Web son más amplias y deben incluir un extenso rango de pruebas para las clases más importantes de vulnerabilidades de aplicaciones Web tales como “SQL injection”, “cross site scripting” y “directory traversals”. Una solución empresarial también debe ser capaz de escanear múltiples aplicaciones, rastrear los resultados a través del tiempo, proporcionar reportes robustos (en especial reportes de cumplimiento con normas) y proporcionar reportes personalizados de acuerdo con los requisitos locales.”

Creación de un reporte oficial sobre la seguridad de las aplicaciones Web
Securosis.com

“La cantidad de vulnerabilidades que afectan a las aplicaciones Web ha crecido a un ritmo asombroso. En el 2008, las vulnerabilidades que afectaban a las aplicaciones de un servidor Web representaban un 54 por ciento de todas las apariciones de vulnerabilidades y fueron uno de los principales factores del crecimiento general de las apariciones de vulnerabilidades durante ese año.”

Reporte de tendencias y riesgos 2008
 de IBM X-Force®

Características de QualysGuard WAS:

Inspección y descubrimiento de vínculos — El inspector Web integrado realiza un análisis sintáctico del HTML y de JavaScript para extraer vínculos. Balancea automáticamente la amplitud y la profundidad de los vínculos descubiertos para inspeccionar hasta 5,000 vínculos por cada aplicación Web.

Autenticación — Autenticación basada en HTTP Basic, Digest y NTLM server. Autenticación de forma simple.

Lista negra — Evita que el inspector visite ciertos vínculos en una aplicación Web.

Lista blanca — Instruye al inspector para que sólo visite los vínculos que se definen explícitamente en esta lista.

Ajuste del desempeño — Nivel de ancho de banda determinado por el usuario para el escaneo paralelo con el fin de controlar el impacto sobre el desempeño de las aplicaciones.

Contenido delicado — Permite la búsqueda automatizada de contenido por medio de expresiones en HTML, como números de tarjeta de crédito.

Flujos de trabajo para definir los escaneos y revisar los reportes — Flujos de trabajo lógicos que se proporcionan para cada aplicación Web. Los reportes ofrecen una visibilidad profunda de las vulnerabilidades.



Crear aplicaciones Web



Opciones de escaneo WAS



Resultados del escaneo WAS

Cómo funciona QualysGuard WAS:

Etapa del inspector

El sofisticado mecanismo de escaneo incluye diversas técnicas para realizar una inspección efectiva de un sitio Web. Al proporcionarle sólo un nombre de usuario y una contraseña, el inspector identifica automáticamente un formulario HTML de una página de inicio de sesión, perfila el proceso de autenticación y monitorea el estado de la sesión para garantizar que un escaneo autenticado siga estando autenticado durante toda la inspección. El inspector intenta cubrir la mayor cantidad posible de la funcionalidad de un sitio Web al balancear la amplitud y la profundidad de la inspección además de evitar los vínculos redundantes o recursivos. El inspector también perfila los comportamientos personalizados del sitio Web de destino, como la apariencia de las páginas de error predeterminadas, y usa la información del perfil para reducir los falsos positivos durante la etapa de prueba.

Etapa de la evaluación

La etapa de prueba de WAS busca vulnerabilidades comunes como “SQL injection”, “cross site scripting”, revelación de fuentes y “directory traversals”. El mecanismo de pruebas depende de una mezcla de firmas y de perfilado del sitio para determinar con precisión la presencia de vulnerabilidades. Actualmente las pruebas se enfocan en los problemas de inyección fallida y distinguen entre los problemas explotables y la revelación simple de la información cada vez que sea posible.

Revisión y reportes

El mecanismo de reportes desglosa los problemas en tipos de vulnerabilidades como “cross site scripting” o “SQL injection” para un solo sitio Web, además de que genera información resumida sobre vulnerabilidades a través de grupos de aplicaciones Web. Además, QualysGuard WAS introduce un nuevo mecanismo para administrar el acceso de los usuarios a los escaneos individuales de las aplicaciones Web con el fin de acomodar diferentes flujos de trabajo para remediación y pruebas.

Precios y disponibilidad:

QualysGuard WAS está disponible como parte de la suite QualysGuard Security and Compliance. Las licencias anuales para QualysGuard WAS se entregan de acuerdo con el número de aplicaciones Web, incluyendo un número ilimitado de escaneos WAS, y soporte y actualizaciones las 24 horas del día, los siete días de la semana.



EE.UU. – Qualys, Inc. • 1600 Bridge Parkway, Redwood Shores, CA 94065 • T: 1 (650) 801 6100 • sales@qualys.com

Reino Unido – Qualys, Ltd. • 224 Berwick Avenue, Slough, Berkshire, SL1 4QT • T: +44 (0) 1753 872101

Alemania – Qualys GmbH • München Airport, Terminalstrasse Mitte 18, 85356 München • T: +49 (0) 89 97007 146

Francia – Qualys Technologies • Maison de la Défense, 7 Place de la Défense, 92400 Courbevoie • T: +33 (0) 1 41 97 35 70

Japón – Qualys Japan K.K. • Pacific Century Place 8F, 1-11-1 Marunouchi, Chiyoda-ku, 100-6208 Tokyo • T: +81 3 6860 8296

Emiratos Árabes Unidos – Qualys FZE • P.O. Box 10559, Ras Al Khaimah, United Arab Emirates • T: +971 7 204 1225

China – Qualys Hong Kong Ltd. • Suite 1901, Tower B, TYG Center, C2 North Rd, East Third Ring Rd, Chaoyang District, Beijing • T: +86 10 84417495

