Administración de la seguridad en línea
White paper
Diciembre 2007

Rational. software

Dirty Dozen: prevención de ataques comunes a nivel de las aplicaciones.

Indice

Introducción

Dado que las empresas dependen cada vez más del software en línea, su riesgo de sufrir ataques malintencionados se ha visto agravado. Dichos ataques pueden paralizar los negocios de una firma, provocar pérdidas millonarias por transacciones no realizadas e incluso dañar la imagen de su marca.

Si bien la mayoría de las empresas son capaces de implementar en la red sistemas de seguridad eficaces mediante firewalls y codificaciones, algunas de ellas pueden poner en peligro a la información confidencial, aunque sin advertirlo, tanto de sus clientes como la corporativa, al no proteger el nivel de las aplicaciones. Por lo tanto, si un hacker lograra, pensando como un programador, identificar los defectos que éste hubiera creado, podría, en unas pocas horas, causar estragos en una aplicación vulnerable y su infraestructura adyacente utilizando tan sólo un navegador de Internet.

Por suerte, las organizaciones bien administradas pueden proteger sus aplicaciones Web incluyendo evaluaciones de vulnerabilidad y “hacks” éticos en sus procesos de desarrollo e implementación del software. Al utilizar herramientas automáticas para realizar estos controles durante todo el ciclo de vida de las aplicaciones en línea, los auditores, programadores y profesionales de control de calidad (QA) pueden frustrar a los hackers y reducir la exposición de una empresa a potenciales pérdidas comerciales. En este trabajo, se presenta una descripción de 12 de los ataques más comunes, junto con normas básicas que le permitirán crear aplicaciones Web mucho más resistentes a dichos ataques.

Aspectos destacados

Los expertos de seguridad de IBM Rational trabajaron con clientes de distintas industrias reguladas para identificar las vulnerabilidades de seguridad comunes de las aplicaciones de la Web.

Los ataques comunes incluyen envenenamiento de cookies, manipulación de los campos ocultos y sabotaje de los parámetros.

¿Cuáles son los ataques más comunes?

El equipo técnico de IBM Rational ha logrado identificar y estudiar los 12 ataques más comunes, gracias al trabajo en conjunto llevado a cabo con empresas líderes, pertenecientes a una amplia variedad de industrias reguladas-incluyendo algunas que brindan servicios financieros, entidades gubernamentales y firmas farmacéuticas.

Doce ataques comunes

Tipo de ataque	Fin Ilícito	Cómo se realiza
1. Envenenamiento de cookies	Robo de identidad/ Secuestro de sesiones.	Varias aplicaciones Web utilizan cookies para guardar cierta información, como ID de usuario o una fecha de registro, en la computadora del cliente. Sin embargo, estas cookies no son criptográficamente seguras, de modo tal que un hacker puede modificarlas y engañar a la aplicación para que cambie sus valores- esto significa, en esencia, “envenenar” las cookies. Así, logra acceder a las cuentas de otras personas y realizar transacciones fraudulentas, como por ejemplo, compras o transferencias monetarias.
2. Manipulación de los campos ocultos	Hurto electrónico.	A menudo, los comercios utilizan campos ocultos para guardar información sobre las sesiones de un cliente, eliminando así la necesidad de mantener una base de datos compleja en el servidor. Otros usan también dichos campos para almacenar los precios de las mercaderías. En sitios desprotegidos, los hackers pueden visualizar los códigos fuente, encontrar estos campos ocultos y alterar los precios. Si las empresas no detectaran estas modificaciones, podrían enviarle al hacker mercaderías marcadas con precios alterados y quizás también con importantes descuentos.
3. Sabotaje de los parámetros	Fraude	Algunas aplicaciones no consiguen confirmar la corrección de los parámetros de common gateway interface (CGI), insertos dentro de un hipervínculo. Por consiguiente, los hackers pueden alterar, con facilidad, dichos parámetros. Esto podría permitirles asegurar una tarjeta de crédito con un límite de U$S 500.000, sortear una pantalla de conexión a un sitio o acceder a otras órdenes e información de clientes.

Aspectos destacados

Al aprovecharse de las vulnerabilidades comunes de la seguridad, los hackers pueden atacar las aplicaciones de la Web de las empresas utilizando distintos métodos.

Tipo de ataque	Fin Ilícito	Cómo se realiza
4. Desbordamiento del buffer	Rechazo del servicio	Los hackers pueden, aprovechando alguna imperfección del formulario Web, saturar un servidor con información excesiva, provocando fallas y el cierre del sitio Web.
5. Cross-site scrpting	Usurpación / Robo de Identidad	Los hackers pueden inyectar un código maligno en un sitio Web, el que se ejecuta como si se hubiera originado en el sitio específico. Esto les permite a los atacantes el acceso total al documento recuperado e incluso los habilita el envío de los datos de la página.
6. Explotación de las opciones de backdoor y depuración	Intrusión	Con frecuencia, los programadores insertan opciones de depuración dentro del código para poner a prueba el sitio antes de su puesta en marcha. Si se olvidan de cerrar estos agujeros de seguridad, los hackers pueden acceder, con total libertad, a la información confidencial.
7. Navegación forzada	Interrupción e irrupción	Los hackers pueden alterar el flujo de las aplicaciones, y acceder a la información y los componentes que deberían ser inaccesibles, como por ejemplo, los archivos de conexión, las facilidades de administración y los códigos fuente de las aplicaciones.
8. HTTP response splitting	Suplantación, robo de identidad y e-graffiti	Los hackers pueden envenenar una cache de la Web tanto en el sitio como en los sistemas intermedios, lo que les permite cambiar las páginas de la Web en la cache y atacar a los usuarios de maneras diversas. Además, esta táctica les da la posibilidad de ocultar mejor sus actividades.

Aspectos destacados

Algunas infraestructuras y protocolos insertos que dan soporte a las aplicaciones basadas en XML pueden introducir vulnerabilidades en la infraestructura, los protocolos y los contenidos de un sitio.

Tipo de ataque	Fin Ilícito	Cómo se realiza
9. Sigilo / Troyano	Daños Intencionales	Los hackers pueden ocultar comandos peligrosos por medio de un troyano que desencadena un código maligno o no autorizado dañando así el sitio.
10. Aprovecha-miento de configuración errónea de un tercero	Daños Intencionales	Con frecuencia, los hackers visitan sitios públicos que envían vulnerabilidades y parches. Ellos pueden, aprovechándose de estas configuraciones erróneas, crear una nueva base de datos que impide que el sitio use la base ya Existente.
11. Aprovecha-miento de las vulnerabilidades conocidas	Toma de control del sitio	Algunas tecnologías Web tienen debilidades intrínsecas de las que se puede aprovechar un hacker persistente. Por ejemplo, algunos atacantes pueden comandar un sitio entero debido a que saben cómo acceder a las contraseñas de acceso del administrador, utilizando Microsoft® Active Server Page (ASP)
12. Aprovecha-miento de las vulnerabilidades de XML y los servicios de la Web	Daños intencionales	Ciertas infraestructuras y protocolos externos insertos, que les dan soporte a las aplicaciones basadas en XML pueden introducir vulnerabilidades en las infraestructuras, los protocolos y los contenidos de un sitio. Más aún, algunos tipos de ataques, incluyendo la expansión de entidades, Xpath injection, SQL injection en XQuery y diversos ataques de rechazo del servicio, aprovechan la flexibilidad y riqueza de XML para inflingir daños severos a todos estos elementos.

Aspectos destacados

Para proteger su capital basado en la Web, las empresas pueden mejorar la seguridad de sus aplicaciones y evaluar las vulnerabilidades durante todo el ciclo de vida de desarrollo y entrega.

Creación de aplicaciones más resistentes a los ataques.

Los hackers tienen muchas oportunidades de aprovechar la tecnología de la Web. Por lo tanto, ¿qué puede hacer una empresa para proteger sus activos basados en la Web? En primer lugar, se debe pensar a la defensiva. En lugar de centrarse sólo en cómo atraer usuarios a su sitio, usted debe presuponer que todos ellos tratarán de manipular sus aplicaciones. Podrá contribuir a mejorar la seguridad de sus aplicaciones de la Web analizando las vulnerabilidades a lo largo de todo el ciclo de vida de desarrollo y entrega. El uso de las herramientas automáticas le permitirá asegurarse de examinar todas sus aplicaciones y detectar las vulnerabilidades que podrían escaparse a través de los parches si se realizara un análisis manual. Además, deberá tener en cuenta la siguiente norma: jamás confíe en los datos que provengan de un usuario, y nunca realice suposiciones sobre los límites de la tecnología que éste tiene a su disposición.

En otras palabras, todos los datos que provengan de fuentes externas conllevan un peligro potencial. Recuerde que todo lo que un usuario puede en teoría manipular, será manipulado. Más aún, no presuponga que porque un usuario esté empleando una tecnología específica ello implicará que limitará sus acciones. Por ejemplo, aún si un navegador no mostrara campos ocultos en el código de una página HTML, debería suponer que algunos usuarios podrán encontrar y manipular dichos campos antes de enviar nuevamente las páginas a su servidor.

Aspectos destacados

IBM Rational AppScan es un paquete de vanguardia de soluciones automáticas de seguridad para las aplicaciones de la Web que proporciona recomendaciones inteligentes y medios avanzados de reparación.

Cómo puede IBM ayudar?

IBM Rational AppScan es un paquete de vanguardia de solucionesautomáticas de seguridad para aplicaciones Web que puede buscar y analizar las vulnerabilidades comunes de dichas aplicaciones, incluyendo las doce aquí identificadas. A diferencia de otras soluciones que inundan a los usuarios con datos sobre vulnerabilidad, IBM Rational AppScan proporciona recomendaciones inteligentes y medios avanzados de reparación, tales como listas completas de tareas, que pueden ayudar a los usuarios a reparar vulnerabilidades no cubiertas durante el proceso de búsqueda, con el fin de mejorar la seguridad total de su empresa.

Para obtener más información

Para conocer más sobre la forma en la que las herramientas automáticas de seguridad de IBM Rational pueden ayudarlo a crear aplicaciones Web seguras y prevenir ataques comunes, contacte a su representante o asociado de negocios IBM o 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

RAW14008-USEN-00