(In)seguridad en las aplicaciones web

No cabe duda de que las aplicaciones web forman parte del perímetro que debe proteger una organización. No ser conscientes de este hecho puede acarrear consecuencias desastrosas para el negocio, además de tirar por la borda toda la inversión realizada en sistemas de protección de la infraestructura telemática. En este contexto, parece que lentamente los responsables de seguridad despiertan de un letargo que duraba demasiado y que ha provocado que, en la actualidad, la mayor parte de los ataques se focalicen contra las aplicaciones web debido a su bajo nivel de seguridad.


Vicente Aguilera Díaz / Christian Martorella

Hoy en día resulta habitual comprar billetes de avión, componentes informáticos o entradas para un espectáculo a través de una aplicación web accesible desde Internet. De hecho, según informa la AIMC (Asociación para la Investigación de Medios de Comunicación) en su séptima encuesta a usuarios de Internet, publicada en febrero pasado, el 63,8% de los encuestados efectuó, en el último año, alguna de las compras mostradas en el ejemplo anterior.

Esto no es más que otra demostración del grado de penetración que han conseguido las aplicaciones web e Internet en nuestra sociedad. Pero también significa, a su vez, que el mundo empresarial basa crecientemente su negocio en este tipo de soluciones.

No es de extrañar, por lo tanto, que las aplicaciones web hayan sufrido una rápida evolución, aumentando su complejidad y su integración con el resto de la infraestructura telemática. Así, encontramos aplicaciones web que ofrecen un gran número de servicios, acceden a diferentes bases de datos, se encuentran distribuidas en distintos servidores, enlazan con aplicaciones de uso interno, utilizan distintos mecanismos de autenticación, etc.

La problemática de las aplicaciones reside en que una misma funcionalidad puede implementarse de tantas formas distintas como desarrolladores intervengan. Este hecho provoca que no exista un patrón común a la hora de detectar una vulnerabilidad, ni que ésta tenga las mismas implicaciones en la seguridad de los sistemas si se produce en dos aplicaciones distintas. En su artículo "Insecure Web Sites", Jeremiah Grossman comenta que mientras los escáneres de red pueden detectar el 95% de las vulnerabilidades, los escáneres de aplicación luchan por conseguir detectar el 50%. Es necesario, por lo tanto, un trabajo manual adicional al que proporcionan estos escáneres, basado en la investigación y conocimiento de la propia aplicación, para poder evaluar de forma más exacta su nivel de seguridad. Es aquí donde entra en juego la pericia de los auditores de aplicaciones.

Las aplicaciones web se encuentran en el ojo del huracán, convirtiéndose en el objetivo principal de los ataques que se llevan a cabo en la actualidad; más del 90% sufren vulnerabilidades y en muchos casos son de carácter especialmente grave.

Las aplicaciones web se encuentran en el ojo del huracán, convirtiéndose en el objetivo principal de los ataques que se llevan a cabo en la actualidad. Este hecho no debería sorprender, y la razón es muy sencilla: por un lado, las aplicaciones resultan fáciles de atacar (el uso de un simple navegador web es suficiente para realizar los ataques) y por otro lado, la mayor parte de las aplicaciones web se han desarrollado sin tener en cuenta los aspectos de seguridad necesarios, por lo que sufren de un gran número de vulnerabilidades.

Si un intruso desea atacar una infraestructura, seguramente lo hará atacando sus aplicaciones web. Esto es lo que se desprende del dato proporcionado por la entidad analista Gartner Inc.: al menos el 75% de los ataques se llevan a cabo a través de las aplicaciones web.

Veámos a continuación qué vulnerabilidades son las más aprovechadas por los intrusos. (Ver **Figura 1**)

Cuando hablamos de vulnerabilidades no podemos dejar de citar el Top Ten de "Open Web Application Security Project" (OWASP). El listado que se muestra en la figura 1 es un consenso de cuáles son los fallos más graves y comunes que se encuentran, a nivel internacional, en las aplicaciones web hoy en día.

Como se puede observar, son muchas las vulnerabilidades con las que se tiene que lidiar en la actualidad. En lo que respecta a la experiencia de los profesionales de Internet Security Auditors realizando auditorías de aplicaciones web en el ámbito español, podríamos decir que nuestro Top 5 es el que vemos en la **Figura 2**.

Está claro que todas las vulnerabilidades derivan de un desarrollo y programación en los cuales no se tuvieron en cuenta los aspectos de seguridad. Si nos fijamos con detenimiento, la mayoría de estas vulnerabilidades podrían ser evitadas simplemente realizando un correcto saneamiento de los datos de entrada a la aplicación.

Estamos seguros de que si los equipos de desarrollo tuvieran en cuenta el Top 10 de OWASP, el panorama de la seguridad en las aplicaciones web cambiaría radicalmente.

Volviendo a la realidad, cabe citar que el 95% de las aplicaciones web auditadas por nuestro equipo el último año contenían alguna de las vulnerabilidades anteriormente descritas, permitiendo, en muchos casos, el acceso no autorizado a las aplicaciones y/o la alteración del flujo lógico de la misma, acceso directo a bases de datos, ejecución de comandos del sistema operativo, etc.

La cuestión que cabe preguntarse es: ¿qué podemos hacer frente a estos problemas?

En primer lugar, tratar de evitarlos de raíz. Esto implica que el equipo de desarrollo esté capacitado, y se le permita desarrollar con la seguridad en mente, siguiendo buenas prácticas y principios de programación segura. Cabe resaltar que, en la planificación del proyecto, debe haberse tenido en cuenta la incorporación de las fases de seguridad necesarias, ya que si no primará la funcionalidad y los plazos de entrega, quedando la seguridad relegada al olvido.

Además, es importante que la seguridad se tenga en cuenta ya en la etapa de requerimientos, y no al final del proyecto, cuando llevar a cabo modificaciones en la aplicación puede suponer un coste, en tiempo y recursos, excesivamente elevado.

Ahora bien, si la aplicación ya se encuentra en producción ¿qué podemos hacer para protegernos?

En primer lugar, sería lógico llevar a cabo una auditoría de la aplicación para conocer el nivel de seguridad del que se dispone actualmente. Es importante destacar el resultado que debe esperarse tras una

Vulnerabilidades principales en aplicaciones web

A1 Entrada no validada

La información de llamadas web no es validada antes de ser usadas por la aplicación web. Los agresores pueden emplear estas fallas para atacar los componentes internos a través de la aplicación web.

A2 Control de acceso interrumpido

Las restricciones de aquello que tienen permitido hacer los usuarios autenticados no se cumplen correctamente. Los agresores pueden explotar estas fallas para acceder a otras cuentas de usuarios, ver archivos sensitivos o usar funciones no autorizadas.

A3 Administración de autenticación y sesión interrumpida

Las credenciales de la cuenta y los *tokens* de sesiones no están propiamente protegidos. Los agresores que pueden comprometer las contraseñas, claves, *cookies* de sesiones u otro *token*, pueden vencer las restricciones de autenticación y asumir la identidad de otros usuarios.

A4 Fallas de Cross Site Scripting (XSS)

La aplicación web puede ser usada como un mecanismo para transportar un ataque al navegador del usuario final. Un ataque exitoso puede comprometer el *token* de sesión del usuario final, atacar la máquina local o enmascarar contenido para engañar al usuario.

A5 Desbordamiento del búfer

Los componentes de aplicaciones web en ciertos lenguajes que no validan adecuadamente las entradas de datos pueden ser derribados y, en algunos casos, usados para tomar control de un proceso. Estos componentes pueden incluir CGI, bibliotecas, rutinas y componentes del servidor de aplicación web.

A6 Fallas de inyección

La aplicación web puede pasar parámetros cuando accede a sistemas externos o al sistema operativo local. Si un agresor puede incrustar comandos maliciosos en estos parámetros, el sistema externo puede ejecutar estos comandos por parte de la aplicación web.

A7 Manejo inadecuado de errores

Condiciones de error que ocurren durante la operación normal que no son manejadas adecuadamente. Si un agresor puede causar que ocurran errores que la aplicación web no maneja, éste puede obtener información detallada del sistema, denegar servicios, causar que mecanismos de seguridad fallen o tumbar el servidor.

A8 Almacenamiento inseguro

Las aplicaciones web frecuentemente utilizan funciones de criptografía para proteger información y credenciales. Estas funciones y el código que integran a ellas han sido difíciles de codificar de forma adecuada, lo cual frecuentemente redunda en una protección débil.

A9 Negación de servicio

Los agresores pueden consumir los recursos de la aplicación web al punto de que otros usuarios legítimos no puedan ya acceder o usar la aplicación. Los agresores también pueden dejar a los usuarios fuera de sus cuentas y hasta causar que falle una aplicación entera.

A10 Administración de configuración insegura

Tener una configuración de servidor estándar es crítico para asegurar una aplicación web. Estos servidores tienen muchas opciones de configuración que afectan la seguridad y no son seguros desde la instalación original del software.

Figura 1: Top Ten 2004 de vulnerabilidades según la OWASP.

auditoría de seguridad:

– Detección de todas las vulnerabilidades que sufre la aplicación: no basta con conocer que la aplicación sufre una vulnerabilidad de carácter muy grave, sino que además interesa conocer todas las vulnerabilidades, clasificadas según su nivel de criticidad y el impacto sobre los sistemas.

– Detalle de las medidas de seguridad que se deben adoptar para corregirlas: las soluciones y/o recomendaciones a las vulnerabilidades detectadas deben ser lo más específicas posibles, huyendo de generalidades y detallando al máximo nivel posible los pasos que se deberían llevar a cabo.

A pesar de que un cortafuegos de aplicación, si se encuentra configurado correctamente, puede aumentar el nivel de seguridad de la aplicación, existen aspectos que deben evaluarse, obligatoriamente, de forma manual.

Una vez adoptadas las medidas de seguridad que corrigen las vulnerabilidades actuales, el siguiente paso está encaminado a protegerse de futuros ataques. Aquí es donde pueden ayudarnos los cortafuegos de aplicación.

Con el advenimiento de la avalancha de ataques a las aplicaciones web surgieron estos dispositivos/software que cuentan con las capacidades de detección y prevención de intrusos. Al trabajar en la capa 7 (o nivel de aplicación, según el modelo OSI) entienden perfectamente el tráfico HTTP, pudiendo identificar carga maliciosa en las peticiones y realizar acciones sobre las mismas.

Estos dispositivos acostumbran a tener, en líneas generales, costes muy elevados, por lo que para muchas

empresas resultan prohibitivos. No obstante, existen soluciones 'libres' como ModSecurity. ModSecurity es un módulo que ofrece capacidades de detección y prevención de intrusos al servidor web Apache. Este módulo es gratuito y de código abierto, por lo que evoluciona rápidamente gracias a la comunidad internacional.

ModSecurity permite un control muy granular de lo que se quiere proteger. Posee capacidades de: filtrado de peticiones, técnicas anti-evasión, comprensión del protocolo HTTP, filtrado HTTPs, filtrado de contenido comprimido, análisis de la carga contenida en el método POST y, además, permite bloquear inyecciones de código SQL, *cross-site scripting*, *buffer overflows*, ataques comunes, etc.

A pesar de que un cortafuegos de aplicación, si se encuentra configurado correctamente, puede aumentar el nivel de seguridad de la aplicación, existen aspectos que deben evaluarse, obligatoriamente, de forma manual.

Vulnerabilidades más comunes

T1 Inyección de código SQL

A través de las entradas de datos a la aplicación (parámetros de URL, campos de formulario, cabeceras HTTP) es posible inyectar código SQL arbitrario que será ejecutado en el servidor. Explotar esta vulnerabilidad, debido a una validación deficiente de los datos de entrada a la aplicación, puede permitir el acceso indiscriminado a la base de datos, la ejecución de procedimientos almacenados o, incluso, de comandos del sistema operativo.

T2 Sistemas de autenticación y gestión de sesiones deficientes

El uso de sistemas de autenticación débiles, o las escasas medidas de seguridad que puedan adoptar estos sistemas, son las causas de accesos no autorizados a zonas privadas de las aplicaciones. Además, una implementación deficiente del sistema de gestión de sesiones permite la suplantación de usuarios y el acceso a datos confidenciales, mediante el uso de técnicas como intercepción, predicción, fuerza bruta o fijación de IDs de sesión.

T3 Manipulación de parámetros

Dar como válido cualquier dato de entrada a la aplicación sin llevar a cabo las oportunas comprobaciones permite alterar el flujo lógico esperado por la aplicación, evadir controles de seguridad como autenticación de usuarios, o acceder a áreas e información privada.

T4 Enumeración de IDs de usuario y obtención de contraseñas débiles

La enumeración de usuarios consiste en la identificación de IDs de usuario válidos de la aplicación. La información obtenida es la base de ataques posteriores como ataques a las contraseñas o el uso de estos IDs en otros servicios (FTP, correo, etc.). Paralelamente, la excesiva permisibilidad en cuanto a la selección de las contraseñas por parte de los usuarios, hace que éstas sean fácilmente deducibles o identificables, permitiendo adquirir la identidad del usuario atacado.

T5 Gestión de errores deficiente

La provocación voluntaria de errores es una de las técnicas más usadas para detectar fugas de información o entender el comportamiento de las aplicaciones. Un error no controlado puede devolver al cliente que lo generó información sensible como sentencias SQL que esté ejecutando el servidor, cadenas identificativas (nombre, tipo, versión, etc.) del servidor web, o la posibilidad de deducir la lógica de la aplicación, entre otros.

Figura 2: Top 5 2004 de vulnerabilidades según Internet Security Auditors.

Conclusiones

Como se comentaba al inicio de este artículo, las aplicaciones web han sido infravaloradas desde el punto de vista de sus implicaciones en la seguridad tanto de la infraestructura telemática como en el propio negocio de la empresa. Este "descuido" ha motivado que, actualmente, más del 90% de las aplicaciones web sufran vulnerabilidades y que, en muchos casos, éstas resulten de carácter especialmente grave.

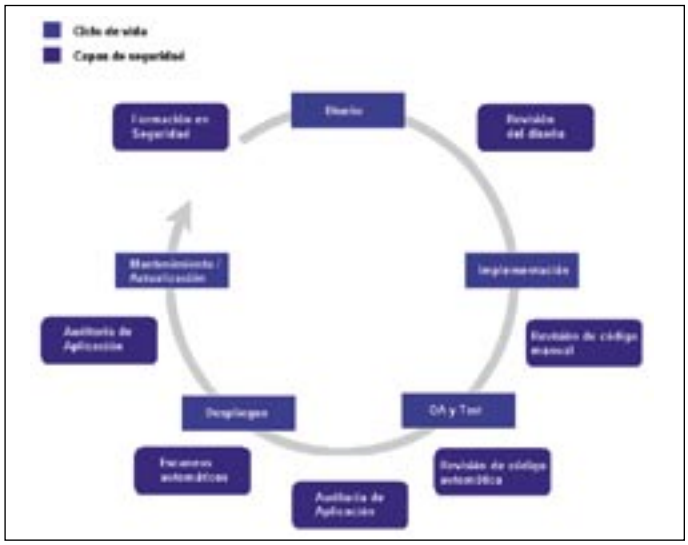

Figura 3: Incorporación de la seguridad al ciclo de vida de las aplicaciones, por Dave Aitel.

No obstante, cada vez son más las empresas que invierten en la seguridad de sus aplicaciones. La tendencia nos hace ser optimistas aunque aún falta mucho por hacer.

Para conseguir el mayor nivel de seguridad posible, es imprescindible incorporar la seguridad al ciclo de vida de las aplicaciones (ver **figura 3**). Así, será necesario una formación previa en seguridad del equipo que participe en el desarrollo, revisión del diseño antes de comenzar la fase de implementación, revisión automática y manual del código de la aplicación, y auditorías de la aplicación, tanto en fase de desarrollo como de forma periódica tras su despliegue. ■

Vicente Aguilera Díaz
vaguilera@isecauditors.com
Christian Martorella
cmartorella@isecauditors.com
INTERNET SECURITY AUDITORS

REFERENCIAS

- Resultados de la 7ª encuesta AIMC a usuarios de internet http://www.aimc.es/03internet/macro2004.pdf
- The Open Web Application Security Project (http://www.owasp.org)
- Open Source Web Application Firewall http://www.modsecurity.org
- "Insecure Web Sites", por Jeremiah Grossman http://www.varbusiness.com/showArticle.jhtml?articleID=18825528&flatPage=true
- "Airline Web Sites Seen As Riddled With Security Holes," Computer World, 4-2-2002. (http://www.computerworld.com/securitytopics/security/story/0,10801,67973,00.html)
- Presentación "Inseguridad de los sistemas de autenticación en aplicaciones web", por Vicente Aguilera http://www.isecauditors.com/downloads/present/inseguridad-autenticacion-aplicaciones-web.pdf
- Artículo "Firewall de aplicación con mod_security", por Christian Martorella http://www.isecauditors.com/downloads/artic/iseclab4.pdf