OWASP Top 10 2013: actualización de los riesgos más extendidos asociados a las aplicaciones web

El proyecto OWASP Top 10, referente y uno de los más emblemáticos de esta organización, ha visto recientemente una nueva actualización. Con una mentalidad de divulgación y con el claro objetivo de educar, tanto a las organizaciones como a todas aquellas personas que, de una u otra manera, están implicadas en el ciclo de vida de las aplicaciones, este Top 10 enumera y describe los diez riesgos más críticos y extendidos que sufren las aplicaciones web en la actualidad. Respecto a su anterior versión, la de 2010, cabe destacar la incorporación de una nueva categoría para considerar el riesgo asociado al uso de componentes vulnerables conocidos.

Vicente Aguilera Díaz

El doce de junio de este año, Dave Wichers (líder del proyecto OWASP Top 10) anunciaba la publicación del Top 10 2013 [1] en la lista de correo de los líderes de los capítulos locales de OWASP [2]. Habían transcurrido cuatro meses desde que se publicara una versión abierta a comentarios, y el proyecto alcanzaba así el nivel de madurez requerido para ser publicado en su versión final.

El Top 10 es uno de los principales proyectos de OWASP y, seguramente, uno de los más conocidos internacionalmente al ser referenciado por numerosos organismos, estándares y libros en la definición de los requerimientos mínimos de seguridad exigidos en los desarrollos de aplicaciones web. Entre ellos, cabe destacar MITRE, PCI DSS, DISA (*Defense Information Systems Agency*) y FTC (*Federal Trade Commission*), entre un largo etcétera.

Publicada su primera versión en enero de 2003 (con versiones posteriores en 2004, 2007, 2010 y 2013), el proyecto OWASP Top 10 pretende identificar los diez riesgos de seguridad más críticos y extendidos en el ámbito de las aplicaciones web. Esta tarea resulta compleja en sí misma, ya que no todos entienden de la misma manera qué implica la seguridad en las aplicaciones web. De esta forma, tras su primera publicación, habían quienes opinaban que el Top 10 debía centrarse únicamente en aquellos aspectos de seguridad que afectaban a la codificación de código propietario y, por otro lado, quienes defendían un concepto más amplio y argumentaban la inclusión de aspectos de seguridad que no sólo afectasen a desarrolladores, como es el caso de deficiencias en la configuración del servidor web o protocolos utilizados en la capa de aplicación.

***Si se consulta el proyecto de seguridad en dispositivos móviles de OWASP, se constata que hay contemplar las amenazas en cada uno de los componentes involucrados y que incluye tres capas: el propio dispositivo móvil, las comunicaciones y el* backend.**

OWASP optó por una visión amplia del concepto de seguridad en aplicaciones web, pero manteniendo fuera todos aquellos aspectos que afectaban a la seguridad a nivel de red e infraestructura. Así, se intentó enumerar y describir los riesgos más críticos a los que deben enfrentarse la mayoría de las organizaciones con el objetivo de crear conciencia sobre seguridad en aplicaciones. Y, a juzgar por la evolución y amplia difusión de este proyecto, creo que se consiguió con creces el objetivo.

El Top 10 2013 no sólo se limita a recoger los principales riesgos de seguridad que afectan a la capa de aplicación sino que, para cada uno de estos diez riesgos críticos, define pautas para verificar si las aplicaciones son vulnerables, proporciona técnicas básicas que ayudan en la protección de las aplicaciones, muestra distintos ejemplos de escenarios de ataque y, finalmente, facilita referencias para ampliar la información sobre los mismos. En definitiva, pretende educar a las organizaciones y a todos aquellos roles que, de una u otra forma, intervienen en la creación de aplicaciones, sobre las consecuencias que se derivan en la explotación de las principales deficiencias de seguridad en las aplicaciones web.

A continuación se describen brevemente cada uno de estos riesgos críticos de obligado conocimiento y entendimiento por parte de todos los profesionales de la seguridad en TI.

A1 – Injection

Se trata de un problema clásico y que siempre ha estado en el podio del Top 10. Está relacionado con la validación de datos, y en permitir que datos no confiables (aquellos que directa o indirectamente pueden ser alterados por el usuario) formen parte de la ejecución de un comando o una consulta.

La explotación de esta vulnerabilidad puede provocar el acceso, pérdida o alteración de la información almacenada, pérdida de trazabilidad del usuario, o la caída del servicio afectado. En determinados casos, el servidor puede verse totalmente comprometido.

A2 – Broken Authentication and Session Management

En la versión de 2007, este riesgo se encontraba en una posición más alejada, pero en los últimos años ha escalado hasta situarse tras los problemas de inyección.

Fugas de información, deficiencias en el proceso de autenticación o en la gestión de sesiones, posibilitan la suplantación de usuarios pudiendo así realizar cualquier acción en nombre de la víctima. Lógicamente, las cuentas con mayor nivel de privilegio resultan las más atractivas y perseguidas.

A3 – Cross-site Scripting (XSS)

Situado siempre entre los cinco riesgos

más críticos del Top 10, continúa siendo ampliamente explotado en la actualidad.

Al igual que los problemas de inyección, su origen reside en una validación deficiente de los datos facilitados por el usuario. La explotación de esta vulnerabilidad permite hacerse con el control del navegador, lo que permitiría suplantar sesiones de usuario, mostrar contenido no autorizado, o capturar las teclas pulsadas por el usuario, entre otras muchas acciones.

Oracle ha sufrido esta vulnerabilidad en numerosas ocasiones. Un ejemplo lo encontramos en Oracle AS Portal [3] y en Oracle Reports Web Cartridge [4].

A4 – Insecure Direct Object References

Desde 2007 tiene el "honor" de haberse ganado esta cuarta posición y mantenerla en la versión del Top 10 2013.

En este caso nos encontramos ante un problema de autorización, que resulta enormemente fácil de explotar. Como resultado, el usuario es capaz de acceder a un objeto del sistema al que no está autorizado. Su impacto: la exposición de datos privados hacia el resto de usuarios de la aplicación.

A5 – Security Misconfiguration

En las primeras versiones del Top 10 se encontraba relegado a la última posición, pero desde 2010 este riesgo lo encontramos en la mitad de la tabla.

La explotación de esta vulnerabilidad permite el acceso no autorizado a datos del sistema o funcionalidades de la aplicación, y puede afectar a cualquier nivel de la capa de aplicación: desde el código propietario, al *framework* utilizado, pasando por el servidor web, servidor de aplicaciones o la base de datos. Es un claro ejemplo que demuestra que todos los roles implicados (en especial, desarrolladores y administradores de sistemas) deben trabajar juntos para ofrecer seguridad al conjunto de componentes que forman la aplicación.

A6 – Sensitive Data Exposure

Se trata de la unión de los riesgos "A7 – Insecure Cryptographic Storage" y "A9 – Insufficient Transport Layer Protection" recogidos en la versión de 2010, donde se han incluido también los riesgos asociados a la exposición de datos sensibles en la parte del navegador.

Hace referencia a la protección de datos sensibles desde el momento en que son facilitados por el usuario, enviados y almacenados por la aplicación, hasta que son finalmente retornados de nuevo por el navegador.

A7 – Missing Function Level Access Control

Se ha ampliado el riesgo "A8 – Failure to Restric URL access", recogido en 2010, para incluir el control de acceso a todas las funcionalidades (y no limitarse únicamente a aquellas accedidas a través de la URL).

La explotación de esta vulnerabilidad posibilita el acceso no autorizado a determinadas funcionalidades ofrecidas por la aplicación. Aquellas que otorgan capacidades de administración resultan las más abusadas.

A8 – Cross-Site Request Forgery (CSRF)

A pesar de encontrarse en la parte baja del Top 10, resulta un riesgo con gran impacto y de trivial explotación.

Aprovechándose del hecho que el navegador transmite de forma automática las cookies del usuario en cada petición y, en determinadas circunstancias, dichas *cookies* pueden autenticar por sí mismas al usuario, es posible forzar a que un usuario realice, sin su conocimiento ni consentimiento, una acción en la aplicación afectada por esta vulnerabilidad. El impacto dependerá de las funcionalidades ofrecidas por la aplicación.

Recientemente se ha publicado una vulnerabilidad [5] en la red social LinkedIn que explotaba este problema.

A9 – Using Components with Known Vulnerabilities

Este riesgo se había tratado como parte de "A6 – Security Misconfiguration" en la versión de 2010, pero dado el incremento del desarrollo basado en componentes (tanto de terceros como propios), se ha definido una nueva categoría en 2013 para recogerlo con entidad propia.

A menudo, los desarrolladores no conocen las versiones de todas las librerías que utilizan (lo que permitiría detectar código desactualizado) así como otros componentes con los que existen dependencias. Este escenario provoca que puedan utilizarse componentes vulnerables (con los mismos problemas de seguridad que cualquier otro software) que pueden ser detectados y explotados por otros usuarios.

OWASP Top 10 2010 (versión anterior)	OWASP Top 10 2013 (versión actual)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	A5 – Security Misconfiguration
A7 – Insecure Cyrptographic Storage (combinado con 2010-A9)	A6 – Sensitive Data Exposure
A8 – Failure to Restrict URL Access (ampliado en 2013-A7)	A7 – Missing Function Level Access Control
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
Incluído en la categoría 2010-A6	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	Combinado con 2010-A7 en la nueva categoría 2013-A6

Usar la nube para albergar las aplicaciones no está exento de riesgos: pérdida de transparencia y del know-how necesario para garantizar la continuidad del servicio, así como de trazabilidad; además de que el hecho de que nuestra información pueda estar en cualquier rincón del mundo hace que los datos privados de los usuarios crucen fronteras jurisdiccionales. A todo esto, hay que sumar los riesgos debidos a deficiencias en la configuración o ejecución del servicio en la nube.

A10 – Unvalidated Redirects and Forwards

Tras aparecer por primera vez en el Top 10 de 2010 y en última posición, en la versión de 2013 sigue cerrando la lista.

El uso de redirecciones (parámetros que reciben como valor un recurso hospedado en un servidor externo) no validadas, puede ser fácilmente explotado ya que el recurso al que está accediendo el usuario pertenece a un dominio en el cual confía. Así, por ejemplo, este escenario puede ser aprovechado para instalar malware o intentar hacer creer al usuario que aún se encuentra en la aplicación legítima para obtener información sensible. La red social Facebook también ha sufrido esta vulnerabilidad [6]. En el caso de los reenvíos a recursos internos, puede ser abusado para sobrepasar el control de acceso a recursos privados.

COMO PUNTO DE PARTIDA

El Top 10 de OWASP no debe ser sobrevalorado. Es decir, tener claro los riesgos que recoge este documento y adoptar las medidas para evitarlos, no significa que nuestra aplicación no adolezca de otros problemas de seguridad que puedan comprometer la plataforma, el servicio o los datos que manejamos. El Top 10 debe ser considerado un punto de partida (que ha de completarse con otras buenas prácticas), pero nunca una meta.

Asimismo, el mercado actual está cambiando y OWASP no es un actor ajeno a esta situación. La presión cada vez mayor en la reducción de costes ha llevado a analizar nuevas vías que permitan incrementar nuestra productividad, llevando el negocio de nuestras empresas a cualquier lugar y en las mismas condiciones que si nos encontráramos en nuestro puesto de trabajo habitual.

Este nuevo escenario está generando un nuevo mercado de soluciones de movilidad, en la que se nos brindan nuevas oportunidades pero también nuevos riesgos. Estamos tentados a adoptar nuevas tecnologías, pero debemos analizar primero si van a resolver un problema de nuestra organización o si, por el contrario, nos estamos dejando arrastrar por una moda en la que ni siquiera analizamos sus implicaciones desde el punto de vista de la seguridad.

El hecho de utilizar la nube para albergar nuestras aplicaciones no está exento de riesgos. Por un lado, la pérdida de transparencia hace más difícil demostrar el cumplimiento (SOX, HIPAA, PCI, etc.) para los propietarios de la información. Por otro, el *know-how* necesario para garantizar la continuidad del servicio se encuentra en manos de un tercero. A pesar de que nuestro proveedor cumpla con los estándares exigidos, ¿qué ocurriría si el proveedor de la nube es comprado por nuestra competencia?

También se pierde trazabilidad y el hecho de que nuestra información pueda estar en cualquier rincón del mundo hace que los datos privados de los usuarios crucen fronteras jurisdiccionales. ¿Sabemos qué uso se hace de estos datos? ¿Se ceden a terceros? ¿Con qué fines? En definitiva, perdemos el control de nuestra información.

A todo esto, hay que sumar los riesgos de seguridad debidos a deficiencias en la configuración o ejecución del servicio en la nube. Hemos visto como Amazon EC2 [7] y Wordpress [8], entre otros, han sufrido diversos problemas de seguridad en este sentido.

La realización de operaciones transaccionales desde los dispositivos móviles, es una realidad desde hace algunos años y, sin duda, aporta un gran valor para la empresa. No obstante, ¿se han analizado en profundidad las nuevas amenazas derivadas de este escenario? En una encuesta publicada por Check Point [9], queda patente que la amplia mayoría de los profesionales de TI considera que la inclusión de los dispositivos móviles en las organizaciones ha generado nuevos incidentes de seguridad. ¿Se está preparado para identificar los nuevos riesgos? ¿Qué planes tenemos al respecto?

OWASP puede aportarnos algo de luz al respecto. Si se consulta el proyecto de seguridad en dispositivos móviles de OWASP [10], se constata que hay contemplar las amenazas en cada uno de los componentes involucrados y que incluye tres capas: el propio dispositivo móvil, las comunicaciones y el *backend.* Adicionalmente, se puede consultar el OWASP Top 10 de riesgos en la nube [11], donde se encuentran recomendaciones para mitigar algunos de los ya comentados en este artículo. ■

Vicente Aguilera Díaz
OWASP Spain Chapter Leader
Socio. Director del Dpto. de Auditoría
INTERNET SECURITY AUDITORS
vaguilera@isecauditors.com

Referencias

[1] OWASP Top 10 2013
https://www.owasp.org/index.php/Top_10_2013

[2] OWASP (Open Web Application Security Project)
http://www.owasp.org

[3] XSS in Oracle Portal Database Access Descriptor
http://www.isecauditors.com/advisories-2010#2010-007

[4] Oracle Reports Web Cartridge (RWCGI60) vulnerable to XSS
http://www.isecauditors.com/advisories-2007#2007-001

[5] CSRF vulnerability in LinkedIn
http://www.isecauditors.com/advisories-2013#2013-001
http://www.youtube.com/watch?v=U6xRNkHbVAw

[6] Facebook social network vulnerable to Open Redirect
http://www.isecauditors.com/advisories-2011#2011-001

[7] MIT's attack on Amazon EC2 an academic exercise
http://chenxiwang.wordpress.com/2009/11/02/mit%E2%80%99s-attack-on-amazon-ec2-an-academic-exercise/x

[8] WordPress and the Dark Side of Multitenancy
http://smoothspan.wordpress.com/2010/06/11/wordpress-and-the-dark-side-of-multitenancy/

[9] The Impact of Mobile Devices on Information Security: A Survey of IT Professionals
http://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report.pdf

[10] OWASP Mobile Security Project
https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

[11] OWASP Cloud Project
https://www.owasp.org/index.php/Category:OWASP_Cloud_-_10_Project