Nuevo OWASP Top 10 2017

¿Qué es OWASP?

OWASP es un proyecto de seguridad en aplicaciones web (Open Web Application Security Project) compuesto por una comunidad abierta dedicada a facultar a las organizaciones a desarrollar, adquirir y mantener aplicaciones que pueden ser confiables.

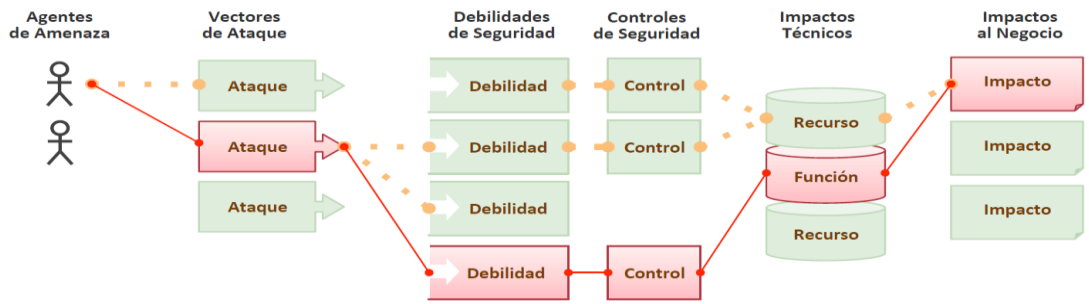
En OWASP encontramos:

- Herramientas y estándares de seguridad en aplicaciones
- Libros completos de revisiones deseguridad en aplicaciones, desarrollo de código fuente seguro y revisiones de seguridad en código fuente.
- Controles de seguridad estándar y librerías.
- Etc.

Todas las herramientas, documentos y recursos son gratuitos y abiertos a cualquier interesado en mejorar la seguridad en aplicaciones.

Riesgos en seguridad de aplicaciones web

OWASP define el siguiente cuadro para valorar los riesgos de una vulnerabilidad:



Los atacantes pueden usar diferentes vectores de ataque a través de la aplicación para hacer daño a su organización. Cada uno de los diferentes vectores puede ser, o no, suficientemente grave como para justificar atención sobre el problema.

A veces, estas rutas son "sencillas" de encontrar y explotar, y a veces muy dificiles. Del mismo modo pueden no tener repercusión en el sistema o dejarlo fuera de servicio.

¿Cómo se calcula el riesgo?

OWASP Top 10 se centra en la identificación de riesgos más serios para una amplia gama de organizaciones. Para cada uno de estos riesgos hemos determinado el siguiente esquema de calificaciones.

Agente de Amenaza	Vectores de Ataque	Prevalencia de Debilidades	Detectabilidad de Debilidades	Impacto Técnico	Impacto al Negocio
Específico de la aplicacion	Fácil	Difundido	Fácil	Severo	**Específico de la aplicación /negocio**
	Promedio	Común	Promedio	Moderado	
	Difícil	Poco Común	Difícil	Menor	

Sólo las organizaciones saben los detalles especificos de su negocio. Para una aplicación determinada, podría no existir un agente de amenaza que pueda ejecutar el ataque en cuestión. Por lo tanto, usted es quien debe evaluar cada riesgo y el impacto que podria suponer para el negocio.

OWASP Top 10

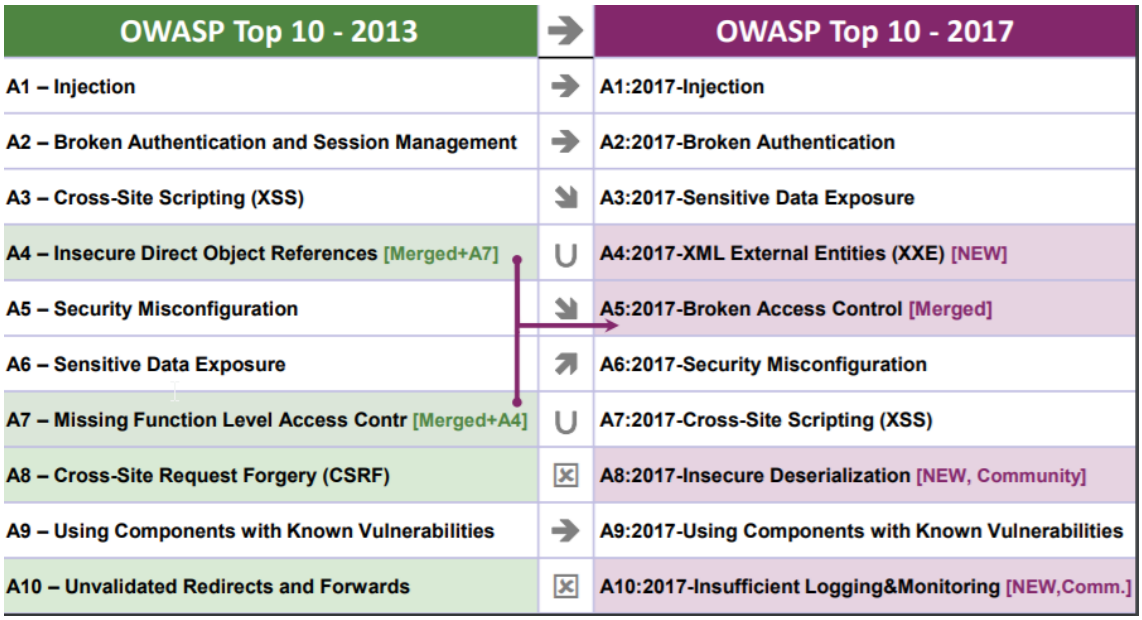
Respecto a todos los criterios expuestos anteriormente OWASP define un documento Top 10, ponderando las vulnerabilidades más comunes y con mayor riesgo en las aplicaciones Web que sirven como base a la mayoría de las empresas y especialistas de seguridad para tener una metodología estándar común.

Este documento con el listado de las 10 vulnerabilidades más comunes, se actualiza cada 3 años ya que muchas de las vulnerabilidades, riesgos o formas de explotación de las mismas, como es lógico, también evolucionan a lo largo del tiempo

El ultimo Top 10 reconocido databa de 2013, siguiendo la estructura de los tres años, debería haber salido el mismo el año pasado, en cambio, la organización, debido a los pocos cambios en las vulnerabilidades existentes decidió retrasarla un año y sacarla en 2017.

OWASP Top 10 2013 vs OWSP Top 10 2017

En la siguiente imagen se puede observar las diferencias más significativas entre la versión anterior y la nueva:



Como se puede observar ha cambiado solo en varias vulnerabilidades, quedando la estructura principal de las más comunes intacta de la misma forma. Algunas de las principales novedades de la nueva versión de 2017 son:

- Desaparece el A8 - CSRF, como vulnerabilidad dentro del Top 10, ya que debido a ciertos controles que tienen las aplicaciones, el estudio que se ha realizado define que solo se encuentra en el 5% de las aplicaciones web actuales.
- Aparecen nuevas vulnerabilidades que hacen referencia al código de la aplicación, como por ejemplo, el A4 que hace referencia a inyecciones XML que se detectan en este tipo de análisis del código.
- Se fusionan el A4 y el A7 del antiguo del 2013 para generar una nueva vulnerabilidad que engloba ambas dos, y que hace referenciaa la incorrecta gestión del acceso a aciertas partes/recursos de la información que manejan las aplicaciones.
- Se define otra vulnerabilidad nueva debido a la incorrecta monitorización y gestión de logs para poder valorar la seguridad de las aplicaciones en caso de un ataque o de una intrusión

Aunque se lleva remodelando el Top 10 anterior desde primeros del 2017, no ha sido hasta finales del mismo hasta que ha salido su última versión y que parece ser la definitiva. En la actualidad, la misma esta en proceso de traducción a varios idiomas, incluido el castellano, por lo que posiblemente la misma no sufra demasiados cambios relevantes.

En Áudea, no solo seguimos el Top 10 comentado para realizar todas nuestras auditorias de aplicaciones web, si no que seguimos la metodología OWASP comentada en el presente articulo para realizar todas las pruebas en las mismas en las que se incluyen todos los problemas de seguridad que se pueden dar en las mismas.

Fernando Saavedra

Cibersecurity Manager

Áudea Seguridad de la Información