PARA SU LANZAMIENTO INMEDIATO:

OWASP TOP 10 PARA EL 2010 PUBLICADO

¿Nos ayudarás a que llegue a todos los desarrolladores del mundo?

Columbia, MD 4/19/2010 —

Desde 2003, los expertos e investigadores de seguridad en aplicaciones de todo el mundo en el proyecto OWASP han monitorizado cuidadosamente el estado de la seguridad en aplicaciones web, y han producido un documento de concienciación el cual conocen y en el que confían organizaciones de todo el mundo, incluyendo PCI, el Departamento de Defensa, la Comisión Federal de Comercio, y muchas otras.

Hoy, OWASP ha publicado un informe actualizado recopilando el TOP de los diez riesgos asociados con el uso de las aplicaciones web en una compañía. Este informe de 22 páginas incluye ejemplos y detalles que explican estos riesgos a desarrolladores de software, managers, y cualquier persona interesada en el futuro de la seguridad web. Todo en OWASP es gratis y libre para todo el mundo, pudiendo descargar el informe con el Top 10 de OWASP gratuítamente en:

http://www.owasp.org/index.php/Top_10

Dave Wichers, miembro del consejo OWASP y jefe de Operaciones de Aspect Security, ha liderado el proyecto desde su inicio. "Este año hemos modernizado el TOP 10 para dejar claro que estamos hablando de riesgos, y no de vulnerabilidades únicamente. El intento de priorizar vulnerabilidades sin contexto no tiene sentido alguno. No se pueden tomar decisiones de negocio adecuadas sin entender la amenaza e impacto que suponen para tu negocio." Este nuevo enfoque sobre los riesgos tiene como objetivo impulsar a las organizaciones a madurar más su comprensión y gestión de la seguridad en las aplicaciones a través de su organización.

Ha llegado la hora de conseguir la concienciación de seguridad en aplicaciones fuera de la comunidad de seguridad y directamente a las personas que más la necesitan conocer. Este año, nuestro intrépido objetivo es el de conseguir que el TOP 10 de OWASP llegue **a las manos de cualquier desarrollador web del mundo** -- pero necesitamos tu ayuda. Le pedimos a todo el que esté leyendo esto: ¿serías capaz de llevar a cabo una única acción para ayudar a proteger el futuro de Internet? Si conoces a gente que programe para la web, ¿podrías re-enviarle el Top 10 de OWASP y preguntarle amablemente...

¿Estás familiarizado con todos los riesgos descritos en el Top 10 de OWASP?

¿Se compromete hoy a proteger su código contra lo descrito en el Top 10 de OWASP?

Durante mucho tiempo, muchas organizaciones han confiado exclusivamente en un análisis ocasional o un test de intrusión para asegurar sus aplicaciones web internas y externas. Estas acciones son caras y no abarcan lo suficiente. Al igual que ocurre con otros tipos de seguridad, la seguridad en aplicaciones requieren un programa de control de riesgos que proporcionen visibilidad a lo largo del portfolio al completo y los controles estratégicos para mejorar la seguridad. Si tu organización está preparada para abordar la seguridad en aplicaciones, existen docenas de libros gratis, herramientas, proyectos, foros, listas de correo y más en OWASP. También es posible unirse a uno de los 180 capítulos locales de todo el mundo o asistir a nuestras conferencias AppSec de gran calidad y asequibles.

El Top 10 de OWASP para el 2010 es:

A1: Inyección
A2: Cross-Site Scripting (XSS)
A3: Control de sesiones y autenticación rota
A4: Referencias a objetos directos inseguros
A5: Cross-Site Request Forgery (CSRF)
A6: Mala configuración de seguridad
A7: Almacenamiento con cifrado inseguro
A8: Fallo en la restricción de direcciones URL
A9: Protección de la capa de transporte insuficiente
A10: Re-envíos y re-direcciones no validadas

La actualización del 2010 está basada en más fuentes de información de vulberabilidades en aplicaciones web que en anteriores versiones al determinar el nuevo Top 10. También presentan esta información de una forma más concisa, amena y más cómoda, incluyendo muchas referencias a los muchos nuevos recursos actualmente disponibles, particularmente los nuevos proyectos de OWASP Enterprise Security API (ESAPI) y Application Security Verification Standard (ASVS).

SOBRE OWASP

El proyecto abierto de seguridad en aplicaciones Web (OWASP por sus siglas en inglés) es una comunidad abierta y libre de nivel mundial enfocada en mejorara la seguridad en las aplicaciones de software. Nuestra mision es hacer la seguridad en aplicaciones "visible", de manera que las organizaciones pueden hacer desiciones informadas sobre los riesgos en la seguridad de aplicaciones. Todo mundo es libre de participar en OWASP y en todos los materiales disponibles bajo una licencia de software libre y abierto. La fundación OWASP es una organización sin ánimo de lucro 501c3 que asegura la disponibilidad y apoyo permanente paraa nuestro trabajo de nuestros miemrbos: Individuales, Miembros organizativos & Instituciones educativas.

Entrevistas: Jeff Williams – Presidente de OWASP y fundador del Proyecto Top 10 (jeff.williams@owasp.,org)
Entrevistas: Dave Wichers – Miembro del consejo OWASP y jefe del proyecto Top 10 (dave.wichers@owasp.org)
Contacto: Lorna Alamri – Connections Committee (lorna.alamri@owasp.org)
Nombre de la compañía: Open Web Application Security Project (OWASP)
Dirección web: http://www.owasp.org
Traducción: José A. Guasch

# # #