Enero 18, 2010

OWASP Conferencias AppSec

Junio 21-24, 2010

AppSec Research 2010

Estocolmo

Miembros del Consejo Directivo OWASP 2010

Jeff Williams

Dinis Cruz

Dave Wichers

Tom Brennan

Sebastien Deleersnyder

Eoin Keary

Matt Tesauro

OWASP
The Open Web Application Security Project

AppSec USA 2010 Announcement

El Comité Global de Conferencias se complace en anunciar la fecha y el lugar de la conferencia OWASP AppSec US 2010.

La Conferencia AppSec US 2010 se celebrará del 7 al 10 de septiembre de 2010 y será conducida por el Capítulo Área de la Bahía de la Universidad de California en Irvine, la única escuela en el sistema de universidades de California con una dedicada a las Ciencias de la Información y Computación. En breve se enviará más información, incluyendo la convocatoria de los oradores y de la formación. El comité extiende sus felicitaciones al capítulo de Minneapolis por el envío de su increíble propuesta. Aunque no fueron seleccionados para el AppSec US 2010, esperamos poder llegar a la zona norcentral y central de

OWASP AppSec Research 2010 Call for Papers

La Conferencia OWASP AppSec de investigación está buscando propuestas que se dividen en tres categorías:

Publish or Perish: Documentos de investigación para su revisión paritaria. Enviar: máximo 12 páginas, formato LNCS

Demo or Die: Presentación y Demostración. Presentar: 1 página resumen + Captura de pantalla

Present or Repent: Presentación solamente. Enviar: 2 páginas de resumen extendido.

http://tinyurl.com/yjv2otg Fecha límite: 7 de febrero.

IBWAS 09

Alrededor de 40 participantes y varias decenas de estudiantes de tecnología y sus profesores asistieron a la Conferencia Ibérica de aplicación de Seguridad Web (IBWAS'09) que se celebró en la Escuela Universitaria de Ingeniería Técnica de Telecomunicación, Universidad Politécnica de Madrid, España, el 10 y el 11 de diciembre del 2009.

La conferencia, que fue un enorme éxito, fue organizado por los capítulos de OWASP españoles y portugueses con el objetivo de reunir a expertos en seguridad de aplicaciones, investigadores, educadores y profesionales de la industria y la academia para discutir abiertamente los problemas y nuevas soluciones en seguridad de aplicaciones.

A través de la apasionada discusión celebrada durante el panel "Web Application Security: ¿Qué deberían hacer los gobiernos en el 2010?", varias conclusiones se han alcanzado.

Estas conclusiones reflejan las decisiones tomadas por el grupo y debe ser debatido, actualizado y, finalmente, publicado por la OWASP como un conjunto de recomendaciones.

1. Desafiamos a los gobiernos a trabajar con OWASP para aumentar la transparencia de la seguridad de aplicaciones Web, especialmente con respecto a la salud financiera, y todos los demás sistemas en que los datos de privacidad y confidencialidad son fundamentales;
2. OWASP buscará participación con los gobiernos de todo el mundo para desarrollar recomendaciones para la incorporación de requisitos específicos de seguridad en aplicación y el desarrollo de marcos adecuados de certificación en los procesos de adquisición de programas gubernamentales;
3. Ofrecemos nuestra ayuda para aclarar y modernizar las leyes de seguridad informática, permitiendo que el Gobierno, los ciudadanos y organizaciones a tomar decisiones informadas acerca de la seguridad;
4. Pedimos a los gobiernos alentar a las empresas a adoptar las normas de seguridad de aplicaciones que, en seguida, le ayudará a proteger a todos de las brechas de seguridad, lo que podría exponer la información confidencial, permitir las operaciones fraudulentas y incurrirá en responsabilidad jurídica;
5. Ofrecemos a trabajar con los gobiernos locales y nacionales para establecer cuadros de mando de seguridad de aplicaciones que proporcionen una visibilidad en el gasto y apoyo a la seguridad de aplicaciones.

OWASP Podcasts Series

Presentado por Jim Manico

Ep 57 David Linthicum (cloud Computing)

Ep 56 Adar Weidman (Regular Expression DOS)

Ep 55 AppSec Justification Roundtable with Boaz Gelbord, Jason Lam, Jim Manico and Jeff Williams

Ep 54 George Hesse

Ep 53 Amichai Shulman (WAF)

¿Buscando un empleo en AppSec? Revisa la página de empleos de OWASP

¿Ofreces algún empleo de AppSec que necesitas que sea publicado?

Contacto:

Kate Hartmann

Comparación entre WASC Threat Classification v2 /OWASP Top Ten 2010 RC1 Blog de Jeremiah Grossman

Copiado, con permiso del blog Jeremiah Grossman http://jeremiah-grossman.blogspot.com/

"Con la mayor parte del trabajo realizado por Bil (@bilcorry), aquí se muestra una primera version de la comparación entre la recién publicada version 2 de la WASC's Threat Classification y el RC1 del Top 10 2010 de OWASP. Esto debería ayudar a aquellos que utilizan uno o ambos documentos.

WASC Threat Classification v2	OWASP Top Ten 2010 RC1
WASC-19 SQL Injection	A1 - Injection
WASC-23 XML Injection	
WASC-28 Null Byte Injection	
WASC-29 LDAP Injection	
WASC-30 Mail Command Injection	
WASC-31 OS Commanding	
WASC-39 XPath Injection	
WASC-46 XQuery Injection	
WASC-08 Cross-Site Scripting	A2 –Cross Site Scripting (XSS)
WASC-01 Insufficient Authentication	A3 - Broken Authentication and Session
WASC-18 Credential/Session Prediction	
WASC-37 Session Fixation	
WASC-47 Insufficient Session Expiration	
WASC-01 Insufficient Authentication	A4 - Insecure Direct Object References
WASC-02 Insufficient Authorization	
WASC-33 Path Traversal	
WASC-09 Cross-site Request Forgery	A5 - Cross-Site Request Forgery
WASC-14 Server Misconfiguration	A6 - Security Misconfiguration
WASC-15 Application Misconfiguration	
WASC-02 Insufficient Authorization	A7 - Failure to Restrict URL Access
WASC-10 Denial of Service	
WASC-11 Brute Force	
WASC-21 Insufficient Anti-automation	
WASC-34 Predictable Resource Location	
WASC-38 URL Redirector Abuse	A8 - Unvalidated Redirects and Forwards
WASC-50 Insufficient Data Protection	A9 - Insecure Cryptographic Storage
WASC-04 Insufficient Transport Layer Protection	A10 -Insufficient Transport Layer Protection

OWASP TOP 10 2010 RC1—Actualización Dave Wichers

La primera version candidata (RC1) del TOP 10 del 2010 de OWASP fué liberada en la AppSec DC. El plazo de comentarios finalizó el 31/Dic/09. El equipo del proyecto espera poder publicar la actualización el 4/Feb/2010.

Se puede consultar más información en la página del proyecto del Top 10:

http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

OWASP JBroFuzz

El proyecto de OWASP JBroFuzz ha sido revisado mediante la version 2 del OWASP Assessment Criteria y su última version publicada (JBroFuzz 1.7) se ha definido como *Stable* desde el **2/Dic/2009.**

http://www.owasp.org/index.php/Category:OWASP_JBroFuzz

http://www.owasp.org/index.php/Category:OWASP_JBroFuzz_Project_-_Version_1.7_Release_-_Assessment

http://www.owasp.org/index.php/Assessment_Criteria_v2.0

Enhorabuena al líder del proyecto, Yiannis Pavlosoglou, y al equipo, Matt Tesauro y Leonardo Cavallari Militelli, que realizaron la primera revision basándose en el nuevo *OWASP assessment criteria*.

Comité Global de Industria
Colin Watson

La misión del Comité Industria es la de expander la concienciación y promover la inclusion de las buenas practices sobre seguridad software en los sectores públicos y privados. El comité también quiere convertirse en la voz de aquellas organizaciones junto con OWASP, promoviendo sus puntos de vista y requisitos.

Para lograr este cometido, nos comprometemos a superarlo incluyendo presentaciones, contribuciones a otros esfuerzo de las organizaciones y esfuerzos colaborativos donde esto pueda identificarse y los recursos lo permitan.

Durante el 2009, Rex Booth y David Campbell en Norteamérica, y Georg Hess, Eoin Keary y Colin Watson en Europa, junto con Tom Brennan como representación de nuestra mesa OWASP, llevaron a cabo 19 acciones, lideraron o ayudaron con respuestas a 9 borradores de buenas practicas, artículos de opinión y estándares, y comenzaron a documentar recursos en lugares donde se referenciase a OWASP y a sus proyectos. En 2010 se les unieron tres nuevos miembros, Joe Bernik, Alexander Fry y Yiannis Pavlosoglou, y nuestro nuevo representante del consejo directivo, Dave Wichers. Esperamos poder tener un rol más proactivo con personas no relacionadas ni con las tecnologías de la información ni con seguridad, en sectores tales como energéticos, medicos, financieros y gubernamentales, además de promover los proyectos y recursos de OWASP a toda la comunidad. Donde la gente de OWASP tenga contactos, allí queremos ayudarles a dialogar entre organizaciones.

Enlaces de utilidad:

Comité de Industria Global OWASP: http://www.owasp.org/index.php/Global_Industry_Committee

Lista de Correo del Comité de Industría http://lists.owasp.org/mailman/listinfo/global_industry_committee

OWASP Citations:

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

Actualización del Proyecto OWASP
Paulo Coimbra

Nuevo proyecto:

OWASP Computer Based Training Project *(OWASP CBT Project)*, liderado por *Nishi Kumar*

Publicaciones:

OWASP ModSecurity Core Rule Set Project - ModSecurity 2.0.3 A revisar por: Ivan Ristic & Leonardo Cavallari.

The OWASP EnDe Project

OWASP Vicnum Project OWASP Vicnum - Release 1.4 (12/31/2009) .

OWASP Content Validation using Java Annotations Project

OWASP Application Security Verification Standard (ASVS) – Versiones en borrador de las traducciones a Francés y a Japonés. En desarrollo: Traducciones a alemán y a chino.

Unidades de revisión: El GPC está apunto de lanzar una unidad de revision.

Las publicaciones serán revisadas basándose en la versión 2 del *OWASP Assessment Criteria*.

Miembros

Miembros particulares: 767

- Altas en Diciembre: 26
- Renovaciones en Diciembre: 0
- Bajas en Diciembre (que no renovaron): 9
- Miembros particulares: $900

Organizaciones miembro: 27

- Altas en Diciembre: 0
- Renovaciones en Diciembre: 1 (*Nokia*)
- Bajas en Diciembre (que no renovaron): 1 (*Corporate One Federal Credit Union*)

Ingresos en Diciembre por parte de miembros: $5,900

Dinis Cruz exponiendo en la IBWAS 09

Ponentes del panel IBWAS 09

Gracias a Nokia que ha renovado su soporte con la Fundación OWASP en Diciembre.

NOKIA

Fundación OWASP

9175 Guilford Road
Suite #300
Columbia, MD 21046

Teléfono: 301-275-9403
Fax: 301-604-8033
E-mail:
Kate.Hartman@owasp.org

La comunidad libre y abierta de seguridad en aplicaciones.

El proyecto abierto de seguridad en aplicaciones Web (OWASP por sus siglas en inglés) es una comunidad abierta dedicada a habilitar a las organizaciones para desarrollar, comprar y mantener aplicaciones confiables. Todas la herramientas, documentos, foros y capítulos de OWASP son gratuitos y abierto a cualquiera interesado en mejorar la seguridad de aplicaciones. Abogamos por resolver la seguridad de aplicaciones como un problema de gente, procesos y tecnología porque las soluciones mas efectivas incluyen mejoras en todas estas áreas. Nos puede encontrar en www.owasp.org.

OWASP es un nuevo tipo de organización. Nuestra libertad de presiones comerciales nos permite proveer información sobre seguridad en aplicaciones sin sesgos, práctica y efectiva.

OWASP no está afiliada a ninguna compañia de tecnología, aunque soportamos el uso informado de tecnologías de seguridad comerciales. Parecido a muchos proyectos de software de código abierto, OWASP produce muchos materiales en una manera abierta y colaborativa.

La Fundación OWASP es una entidad sin ánimo de lucro para asegurar el éxito a largo plazo del proyecto .

Patrocinadores de la Organización OWASP

Editor del boletín: Lorna Alamri, Fotografías de IBWAS : Carlos Serrao, Traducción del boletín: Christian Navarrete , y José A.Guasch