Diciembre, 2010

Conferencias OWASP

1-2 Diciembre, 2010

BeNeLux 2010

Eindhove, Holanda

16-17 Diciembre, 2010

IBWAS '10

Lisboa, Portugal

8-11 Febrero, 2011

OWASP Global Summit 2011

Lisboa, Portugal

AppSec EU, Dublin

Junio, 2011

AppSec USA Minneapolis

19-23 Septiembre, 2011

OWASP
The Open Web Application Security Project

OWASP AppSec USA 2011—Minneapolis

Muchas gracias a IBM por ser el primer patrocinador de la AppSec USA 2011 y firmar como Patrocinador Oro.

Preparad vuestras ponencias. El proceso de solicitud de ponencias saldrá el 15 de Marzo de 2011.

Utilizaremos http://appsecusa.org como página web, pronto.

IBWAS '10
Carlos Serrao

IBWAS '10, el 2º congreso OWASP Ibero-American Web Application Security se realizará en Lisboa, Portugal el 16 y 17 de Diciembre de 2010. El congreso tundra lugar en el ISCTE—Lisbon University Institute. Las actividades formativas serán el 16 y las conferencias el 17.

Este congreso tiene como objetivo reunir a expertos en seguridad de aplicaciones, investigadores, educadores y profesionales de la industria, educación y comités internacionales como OWASP, para debatir abiertamente sobre la problemática y las nuevas soluciones sobre seguridad en aplicaciones. En el contexto de este ciclo los investigadores de seguridad serán capaces de combinar interesantes resultados con la experiencia de los ingenieros de software y profesionales.

OWASP Summit 2011
Tom Brennan

El OWASP Summit 2011 se acerca, http://www.owasp.org/index.php/Summit_2011 si llevas un tiempo sin estar involucrado, recordamos que anunciamos las elecciones OWASP en el OWASP Summit del 2008 y que se llevaron a cabo el 11 de Noviembre de 2009.

* Archivo Wiki con recordatorio: http://www.owasp.org/index.php/Board_member

El próximo ciclo comenzará en el OWASP Summit 2011 con las elecciones que tendrán lugar el 11 de Noviembre de 2011 por los siguientes miembros de OWASP: http://www.owasp.org/index.php/Membership#Categories_of_Membership_.26_Supporters

Si quieres presentarte a candidato te animamos a conocer los pre-requisitos e involucrarte con el Comité Global de OWASP: http://www.owasp.org/index.php/Global_Committee_Pages

OWASP Podcasts Series

Presentados por Jim Manico

Ep 77 Rafal Los

Ep 78 AppSec Roundtable with Jeff Williams, Andrew van der Stock, Tom Brennan, Samy Kamkar, Jeremiah Grossman and Jim Manico (Complete Chaos)

Ep 79 Tony UV (Threat Modeling)

Sigue a OWASP en twitter

@OWASP

Actualización del proyecto OWASP

Paulo Coimbra

Repasemos a continuación algunos temas sobre actualizaciones en proyectos OWASP desde que se publicó el boletín de Noviembre.

1. Noticias generales sobre proyectos OWASP

1.1 - El liderazgo del proyecto **ASVS** se encuentra en proceso y la comunidad OWASP ha respondido con entusiasmo—cinco candidatos han mostrado interés en liderar o co-liderar este proyecto clave de OWASP. El GPC está en proceso de emitir la recomendación para la decisión del consejo OWASP.

http://www.owasp.org/index.php/Request_For_Proposals/Seeking_New_Project_Leader_For/ASVS

1.2 - En un tiempo record, la guía rápida sobre buenas prácticas en el desarrollo (**OWASP Secure Coding Practices - Quick Reference Guide)** ha producido y ya tiene su tercera edición aprobada y establecida como Estable. Agradecemos al líder del proyecto, Keith Turpin, y a los revisores y contribuidores de esta publicación.

http://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide

1.3 - El proyecto **OWASP AppSensor,** conducido por **Michael Coates**, tiene importantes actualizaciones (nueva herramienta) y se encuentra actualmente en revisión para establecerse como publicación Estable.
http://www.owasp.org/index.php/Category:OWASP_AppSensor_Project

1.4 - La plataforma **OWASP O2, conducida por Dinis Cruz,** tiene importantes actualizaciones (**nueva versión**) y se encuentra **actualmente** en revisión para establecerse como publicación Estable.

http://www.owasp.org/index.php/OWASP_O2_Platform

1.5 - El proyecto **OWASP JBroFuzz** tiene un nuevo coordinador. Agradecemos a Yiannis Pavlosoglou todo el trabajo que ha realizado para sacar este proyecto adelante, dando la bienvenida y deseando todo lo mejor al nuevo coordinador Ranulf Green.

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

2. Proyectos puestos en marcha recientemente

2.1 - **OWASP Uniform Reporting Guidelines, liderado por Vlad Gostomelsky.**

Este proyecto complementará la guía de pruebas OWASP además de la plantilla OWASP RFP. Será una plantilla para informar sobre los descubrimientos de vulnerabilidades que será libre, basada en las mejores prácticas de la industria y será el estándar de-facto.

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

2.2 - **OWASP Zed Attack Proxy Project, liderado por Psiinon.**

Este proyecto proporciona una herramienta fácil de usar para probar aplicaciones web, proporcionando escáneres automatizados además de un conjunto de herramientas que permitirán encontrar vulnerabilidades de seguridad de forma manual.

- http://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project#tab=Project_About

2.3 - **OWASP Secure Web Application Framework Manifesto, liderado por Rohit Sethi.**

Este proyecto es un documento detallando un conjunto de requisitos de seguridad para desarrolladores de frameworks de aplicaciones web al que adherirse.

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

2.4 - **OWASP Mobile Security Project, coordinado por Jack Mannino y Mike Zusman.**

El proyecto OWASP Mobile Security ayudará a la comunidad a entender mejor los riesgos en plataformas móviles y como defenderse ante ellos.

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

2.5 - **Proyecto OWASP Fiddler Addons for Security Testing, coordinado por Chris Weber.**

Este proyecto (también conocido como OWASP FAST) pone en conjunto dos proyectos complementarios, el proyecto **Watcher,** un escáner de vulnerabilidades pasivo y el proyecto **X5s**, para probar activamente Cross-Site Scriptings y detector de codificación de entrada/salida. http://www.owasp.org/index.php/OWASP_Fiddler_Addons_for_Security_Testing_Project

2.6 - **OWASP Application Security Skills Assessment, liderado por Neil Smithline.**

Este proyecto (también conocido como OWASP ASSA) es un juego online de múltiples-respuestas para ayudar a las personas a entender sus conocimientos y debilidades sobre temas específicos en seguridad de aplicaciones.

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

- OWASP Browser Security Project, creado por iniciativa de Dave Wichers & Michael Coates.

Este proyecto no tiene todavía un coordinador definido pero se ha realizado un gran impulso por parte de las personas citadas anteriormente. Se aportarán más detalles pronto.

http://www.owasp.org/index.php/OWASP_Browser_Security_Project#tab=Project_About

3. Proyectos que se realizarán pronto:

3.1 – OWASP ESAPI Objective C

3.2 - OWASP PASSWD

3.3 - OWASP Eclipse plug-in

4. Proyectos a realizar nuevamente:

Todo el contenido relacionado con Cross-Site Request Forgery (CSRF).

3.4 -OWASP Open-sourcing JXT

OWASP A10-Unvalidated Forwards

ESAPI -

* Nuevo coordinador para .Net ESAPI – Michael Weber
* Revisión de código actual para Java ESAPI publicación disponible en general.

OWASP Top 10 disponible ya en Español e Italiano

La OWASP Top 10 2010 se ha traducido al castellano gracias al excelente trabajo del equipo formado por:

Coordinador del proyecto: Fabio Cerullo (1º por la Izquierda) Equipo: Juan Carlos Calderon (2º por la Izquierda) , Rodrigo Marcos (Centro), Vicente Aguilera (2º por la derecha). Edgar Sanchez (1º por la derecha) Sin foto: Daniel Cabezas Molina, José Antonio Guasch, Paulo Corondo.

Puedes encontrar ambas versiones en PPT & PDF en el siguiente enlace:

http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=Spanish_Translation

Enlace a la versión en italiano:

http://www.owasp.org/images/f/f9/OWASP_Top_10_-_2010_ITA.pdf

¡Gracias a los miembros que han renovado y siguen apoyando al proyecto OWASP!

mnemonic -securing your business

Nuevos patrocinadores en Noviembre y Diciembre ¡Gracias por el apoyo!

ADP

AppliedTrust

ORACLE

OWASP busca hosting para www.owasp.org (la web) si alguien quiere brindar alojamiento para el sitio web escribir un e-mail a owasp@owasp.org para más detalles.

Modelo de Capacitación OWASP
Sandra Paiva

Por el esfuerzo que estamos haciendo en estabilizar y consolidar el modelo de capacitación de OWASP (OWASP Training) que puede ser utilizado como una herramienta poderosa para difundir el conocimiento y mensaje de OWASP, OWASP está buscando instructores bajo el lema "**recursos y proyectos OWASP que puedes utilizar hoy**". Será un modelo de capacitación **gratis para miembros de OWASP**, **distribuido por líderes OWASP** (únicamente costeando los gastos de viajes) y **cubriendo los módulos OWASP y/o proyectos. Si eres un coordinador de OWASP y quieres ser incluido en la lista de instructores de OWASP, esta es tu oportunidad—añade tu nombre e información a la base de datos de Instructores OWASP y ¡que cuenten contigo!**

¡Hazlo ahora y conviértete en un instructor OWASP! Visita la base de datos y las condiciones en este enlace: http://www.owasp.org/index.php/OWASP_Training#tab=Trainers_Database_-_Call_for_Trainers.21

Sigue todas las novedades sobre la Formación OWASP aquí http://www.owasp.org/index.php/OWASP_Training.

1. Programa de Capítulos Universitarios OWASP, liderado por Jeff Williams. Esta iniciativa ayudará a extender la seguridad en aplicaciones a las universidades y escuelas de todo el mundo

.2. Proyecto OWASP Alchemist, co-liderado por Bishan Singh, Chandrakanth Narreddy y Naveen Rudrappa. Este proyecto permite a un equipo de desarrollo el realizar aplicaciones muy seguras y defendibles con controles/medidas integradas para evitar los fallos de diseño, programación e implementación.

OWASP China
Helen Gao

El primer congreso OWASP en China tuvo lugar en Beijing, del 20 al 23 de Octubre de 2010. Más de 500 personas asistieron a dicho evento. Uno de los miembros de OWASP, Tom Brennen, inauguró la convención solicitando participantes. Expertos de la seguridad de la información de Estados Unidos, China, Taiwan, Hong Kong, Singapur y otras areas mostraron las últimas novedades sobre los actuales temas de seguridad. En analista de Forester, Dr. Chenxi Wang y el coordinador del proyecto OWASP Pravir Chandra estuvieron entre el elenco de ponentes. Dado el éxito de este congreso, ya podemos anticipar una próxima edición para el año que viene.

Primer OWASP Uruguay Day

El primer evento OWASP en Uruguay tuvo lugar el 9 de Diciembre de 2010. Mateo Martinez, Mauricio Campiglia y Cristian Borghello fueron los ponentes. Más información sobre el evento en este enlace:

http://www.owasp.org/index.php?title=OWASP_Day_Uruguay_2010

En dicho enlace también se podrán ver algunas fotos del evento. Gracias a Mateo Martinez, Fabio Cerullo, Roberto Ambrosoni y Kate Hartmann por organizer este congreso..

Proyecto OWASP CTF
Steven van der Baan

El proyecto Capture the Flag se ha llevado a cabo este año en 8 eventos diferentes (desde la AppSec-EU en Estocolmo, Suecia hasta el GovCert en Singapur, además del OWASP BeNeLux en Eindhoven). El CTF también cuenta con su propio logo (http://www.owasp.org/images/8/87/CTFLogo.jpg) y la infraestructura necesaria para el CTF fue revisada por completo. Este sistema será publicado pronto. Steven van der Baan ha substituido a Martin Knobloch como coordinador del proyecto del CTF.

OWASP Modsecurity CRS v2.0.9
Ryan Barnett

Me complace anunciar la liberación del conjunto de reglas OWASP ModSecurity Core Rule Set (CRS) v2.0.9.
El cambio más significativo es que los usuarios ahora pueden cambiar entre los modos *Traditional* y *Anomaly Scoring Detection*.
http://blog.modsecurity.org/2010/11/advanced-topic-of-the-week-traditional-vs-anomaly-scoring-detection-modes.html

Mejoras:

- Modificado el nombre del fichero de configuración principal a *modsecurity_crs_10_config.conf.example* para no sobre-escribir las actuales configuraciones. Los usuarios deberán renombrar este fichero para activarlo.
- El modo de detección *Traditional* es el modo por defecto.
- Los usuarios ahora podrán cambiar fácilmente entre el modo tradicional/estándar y el modo de puntuación por anomalías editando el fichero *modsecurity_crs_10_config.conf*
- Actualizadas las acciones perjudiciales en la mayoría de las reglas para bloquearse en vez de dejar pasarlas. Esto es para cambiar entre los modos tradicional y el de puntuación por anomalías.
- Suprimidas las acciones de registro de la mayoría de las reglas para así poder ser controladas desde la configuración SecDefaultAction del fichero *modsecurity_crs_10_config.conf*
- Actualizadas las puntuaciones de anomalías del fichero modsecurity_crs_10_config.conf file para asemejarse a las utilizadas en las reglas de PHPIDS. Estas todavía tienen el mismo factor de severidad incluso aunque los propios números sean más pequeños.
- Actualizadas las reglas 49 y 59 para incluir la información registrada que concuerde.
- Actualizada la información TAG para clasificar seguidamente las categorías de las vulnerabilidades/ataques.
- Actualizados los filtros de inyecciones SQL para detectar más ataques booleanos. - Movidos algunos ficheros al directorio optional_rules (phpids, reglas de Emerging Threats).

Corrección de errores:

- Regla 960023 corregida en optional_rules/modsecurity_crs_40_experimental.conf, faltaba una comilla
https://www.modsecurity.org/tracker/browse/CORERULES-63
- Movidas todas las acciones skipAfter en reglas encadenadas a la línea de comienzo de reglas (para ModSec v2.5.13 o superior)
https://www.modsecurity.org/tracker/browse/MODSEC-159
- Fijada la extensión del fichero restringido con expansión de macro
https://www.modsecurity.org/tracker/browse/CORERULES-60
- Actualizada la información de la expansión macro en la variable SQLI TX en los ficheros 49 y 60 para que se compare con lo establecido en el fichero de configuración de inyección SQL.

- Arreglado un error en la expresión regular de la inyección SQL - faltaba una barra invertida en el límite de palabra (\b)
https://www.modsecurity.org/tracker/browse/CORERULES-62

Estadísticas del sitio OWASP Noviembre 2010

258, 568 visitas

654,677 páginas vistas

00:03:03 media de tiempo en sitio

58.28% Nuevas visitas

Mark Bristow en la AppSec DC.

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 compañía 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

Edición del Boletín: Lorna Alamri **Contribuidores**: Leonel Navarro & Jayanthi Srinivasan **Traducción**: José A. Guasch & Christian Navarrete