15 de Marzo, 2010

OWASP Conferencias AppSec

2 de Junio, 2010
Froc 2010
Denver, Colorado

Junio 3-4, 2010
OWASP Day Mexico
Aguascalientes, Mexico

Junio 21-24, 2010
AppSec Research 2010
Stockholm, Noruega

Septiembre 7– 10, 2010
AppSec USA 2010
Irvine, California

Noviembre 16–19, 2010
AppSec Brasil 2010
Campinas, Brasil

Miembros del Consejo Directivo OWASP

Jeff Williams
Dinis Cruz
Dave Wichers
Tom Brennan
Sebastien Deleersnyder
Eoin Keary
Matt Tesauro

OWASP
The Open Web Application Security Project

OWASP Security Spending Project Survey
Boaz Gelbord

El proyecto **OWASP Security Spending Benchmarks** busca aportar orientación y un valor de referencia aceptado por la industria para justificar el gasto global en aplicaciones Web. Este proyecto OWASP publica informes periódicos recopilando los resultados de encuestas como esta.

La encuesta es totalmente anónima y no recopila ningún tipo de información personal de los encuestados. Se pondrá disposición de toda la comunidad, además de nuestro informe, todas las respuestas de las encuestas realizadas. Junto con nuestro informe se publicarán también todas las respuestas para ponerlas a disposición toda la comunidad. La nueva versión de este proyecto **OWASP Security Spending Benchmarks** quedará publicado hasta el 15 de Abril.

https://www.surveymonkey.com/s/TPYZLXK
Contraseña: OWASP_Spending

OWASP AppSec USA, California 2010 Call for Papers

El evento tendrá lugar en el centro de conferencias de la UC Irvine en Orange County, California del 7 al 10 de Septiembre de 2010.

Las propuestas deben incluir:

- Nombre o nombres de los ponentes
- E-mail y/o teléfono de contacto
- Biografía
- Título
- Resumen
- Cualquier material de la investigación o herramientas (no se publicará fuera del grupo de selección de los trabajos)

El plazo de entrega de las propuestas finalice el 6 de Junio a las 12PM PST (GMT-8). Enviar las propuestas a: http:www.easychair.org/conferences/?conf=appsec2010

Conference Website

Financiación de Proyectos y Comité Global

El modelo de afiliación se ha extendido a los proyectos y al Consejo Global. Estos grupos podrán encontrar sus propios patrocinadores para crear su propia fuente de ingresos para apoyar el proyecto o el Consejo Global.

Como funciona:

Los proyectos y los Consejos pueden encontrar sus propios patrocinadores para aportar fondos al proyecto o Consejo. La Fundación OWASP gestionará dichos fondos y los compartirá del mismo modo que con los Capítulos, es decir, 40/60 para los miembros corporativos.

Los fondos recaudados pueden ser utilizados para cubrir los gastos relacionados con el proyecto, pero no para pagar a miembros de OWASP.

Ejemplos de en qué destinar los fondos recaudados:

- Cubrir los gastos de viaje de un miembro del proyecto que fuese a presentarlo en una charla.
- Impresión de la documentación referente a un proyecto para ser difundida en eventos.
- Etiquetado de CDs.

Los fondos no pueden ser utilizados para incentivar a un miembro del proyecto por el tiempo que ha dedicado a trabajar en el proyecto.

Contactar con Kate Hartmann para recaudar fondos de los patrocinadores o si se quiere formular cualquier pregunta en referencia a como se está organizando esta nueva iniciativa.

OWASP Podcasts Series

Presentado por Jim Manico

Ep 60 Jeremiah Grossman and Robert Hansen (Google pays for vulns)

Ep 59 AppSec Roundtable with Boaz Gelbord, Ben Tomhave, Dan Cornell, Jeff Williams, Andrew van der Stock and Jim Manico (Aurora+)

Ep 58 Interview with Ron Gula (Web Server Scanning, IDS/IPS)

¿Buscando empleo en AppSec? Visita la página de empleos OWASP

¿Ofertas algún empleo de AppSec?

Contacto: Kate Hartmann

OWASP Italy Days
Matteo Meucci

El pasado 5 y 6 de Noviembre OWASP organizó dos importantes eventos OWASP en Roma y Milán, Italia.

El primero fue realizado en colaboración con CONSIP, una compañía del Ministerio Italiano de Economía y Finanzas (MEF), que trabaja para la Administración Pública italiana. Más concretamente, el evento se denominó "*The Application Security as trigger for the Italian E-Government.*" La audiencia estaba formada por los CISO de todos los ministerios y Administración Pública italiana. Las presentaciones se encuentran publicadas en la dirección: http://www.owasp.org/index.php/Italy_OWASP_Day_E-gov_09

OWASP—Italy Day IV en Milán– El segundo día fue en Milán contando con más de 100 asistentes. Hemos dejado presentaciones, fotografías y videos en esta dirección.

OWASP—Italy Day en Security Summit 2010

18 de Marzo - OWASP– Italia presentará "Directrices OWASP y herramientas para la seguridad en aplicaciones Web" en el Security Summit 2010 de Milán, Italia.
https://www.securitysummit.it/eventi/view/73

Explicación del ataque "Hombre en el Medio" - MitM
Del Blog de Michael Coates 3/3/2010

"¡Es vulnerable a un ataque de hombre en el medio!"

Seguro que esto lo habrás escuchado con anterioridad, pero veamos los detalles de este ataque y entendamos exactamente cómo funciona.

Definición

Primero, una rápida definición, un ataque de "hombre en el medio" (en inglés *MitM - Man-in-The-Middle*) es un ataque en el cual la comunicación que se intercambia entre dos usuarios es monitorizada clandestinamente y con posibilidad de ser modificada por un tercero no autorizado. Además, este tercero estará realizando el ataque en tiempo real (por ejemplo, la obtención de registros de eventos o la revisión del tráfico capturado no se califica como *MitM*).

Aunque un ataque *MitM* pueda ser llevado a cabo contra cualquier protocolo o comunicación, hablaremos de él a continuación refiriéndonos a tráfico HTTP.

Requisitos para el ataque

Un ataque de *MitM* puede realizarse de dos formas:

1. El atacante tiene el control del router a lo largo del punto normal de comunicación entre la víctima y el servidor con el que se está comunicando.

2.a. El atacante se encuentra en el mismo dominio de *broadcast* (es decir, subred) que la víctima.

2.b. El atacante se encuentra en el mismo dominio de *broadcast* (es decir, subred) al igual que cualquier otro *router* utilizado por la víctima para encaminar el tráfico.

El ataque

El artículo completo se encuentra en el blog de Michael Coates

Lanzamiento—OWASP ESAPI ver. 1.4.4 para JAVA ver. 1.4 y superiores
Jim Manico

Control de cambios:

http://owasp-esapi-java.googlecode.com/svn/branches/1.4/changelog.txt

Otros enlaces importantes:

Descargar el .zip: http://owasp-esapi-java.googlecode.com/files/ESAPI-1.4.4.zip

Los Javadocs de ESAPI 1.4.4 se encuentran aquí: http://owasp-esapi-java.googlecode.com/svn/trunk_doc/1.4.4/index.html

¿Dudas sobre el uso de ESAPI y su configuración? Visitar el enlace: https://lists.owasp.org/mailman/listinfo/esapi-user y suscribirse a nuestra lista de correo.

¿Interesado en contribuir? Únete a la lista de desarrollo: https://lists.owasp.org/mailman/listinfo/esapi-dev

Proyecto de numeración común OWASP
Mike Boberski

Un desarrollo emocionante, un nuevo sistema de numeración que será común entre las guías de OWASP se ha desarrollado. La numeración es resultado del esfuerzo de un equipo dirigido por Mike Boberski (líder del proyecto ASVS y coautor). Los colaboradores y coordinadores de los proyectos de la Guía, Referencia y Top Ten OWASP, así como la dirección de OWASP, han trabajado juntos para desarrollar la numeración que permite la correlación sencilla de guías y referencias de OWASP, y que permitiría, por un período de transición que tanto guías como referencias se actualicen para reflejar el nuevo sistema de numeración. Este proyecto localizará números retirados y proporcionará un repositorio centralizado con información sobre su correlación. Visitar la página del proyecto para más información:

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

OWASP ASVS
Mike Boberski

Se ha completado la primera traducción al japonés, y se está desarrollando un apéndice con una guía de conceptos ASVS en también en japonés. Se encuentran en proceso las traducciones al francés, alemán, chino, húngaro y malayo. El proyecto siempre se encuentra abierto a colaboraciones, contactar con mike.boberski@owasp.org en caso de estar interesado.

Guía de Desarrollo OWASP - OWASP Development Guide
Mike Boberski

El trabajo en la nueva iteración de la guía ha comenzado. La próxima versión de la guía de desarrollo OWASP será, en efecto, una guía de diseño detallada sobre los requisitos de OWASP ASVS. Un equipo de más de 26 voluntarios ya se han registrado. El proyecto sigue abierto a colaboraciones. Página del proyecto de la Guía de Desarrollo OWASP:

OWASP Development Guide Project Page

OWASP ESAPI para PHP
Mike Boberski

Sigue la migración de ESAPI a PHP. La mayoría de las clases principales se han terminado o se encuentran en la última fase de su desarrollo inicial, incluyendo las secciones *Security Configuration*, *Validator*, *Encoder*, y *Logger*. Ha surgido un conjunto de usuarios *early-adopters* o tempranos. Visitar la página del proyecto para obtener más información.

Dos nuevos proyectos
Paulo Coimbra

OWASP Broken Web Application Project

http://www.owasp.org/intex.php/OWASP_Broken_Web_Applicaitons_Project#tab=project_Details

Proyecto patrocinado en parte por: Mandiant.

OWASP Ecosystem Project

Prevemos una asociación entre los fabricantes de plataformas de tecnología y un próspero ecosistema centrado en la seguridad de su tecnología. El ecosistema incluirá investigadores (tanto creadores como reticentes), herramientas, bibliotecas, directrices, materia de concienciación, normas, educación, conferencias, foros, canales, anuncios, y mucho más.

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

¡134 mil personas estuvieron un total de 1.5 millones de minutos en la web de OWASP en

Donaciones Haiti:

Donación total de OWASP: $1378.67

Enviado a: Médicos sin fronteras

Los fondos fueron destinados como ayuda humanitaria para Haiti.

Gracias a nuestros miembros corporativos que han renovado su aporte a la fundación OWASP en Enero y Febrero.

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

Editor del boletín: Lorna Alamri

Traducción del boletín: Christian Navarrete y José A.Guasch