May 17, 2010

Conferencias de AppSec OWASP

Junio 2, 2010
Froc 2010
Denver, Colorado

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

Junio 21—24, 2010
AppSec Research 2010
Estocolmo, Suecia

Junio 30, 2010
OWASP Argentina Day
Buenos Aires, Argentina

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

Septiembre 17, 2010
AppSec Ireland
Dublin, Irlanda

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

OWASP
The Open Web Application Security Project

Investigación de AppSec OWASP 2010

La agenda del evento y de la formación está disponible. La cena de gala será el miércoles 23 de junio en el City Hall, lugar dónde se otorgan los premios Nobel. Más información: City Hall

OWASP AppSec Estados Unidos, discursos de 2010 de California

AppSec Estados Unidos tendrá lugar en el centro de conferencias de UC Irvine en Orange County, California, del 7 al 10 de Septiembre del 2010.

Las ponencias serán:

Bill Cheswick—AT&T Research
HD Moore—Metasploit/Rapid7
David Rice—Geekonomics
Jeff Williams—Aspect Security

El sitio Web de la conferencia será publicado pronto y estará disponible en:

www.appsecusa.org

OWASP AppSec, ponencias de Brasil 2010

OWASP AppSec Brasil anuncia que las charlas de apertura se llevarán a cabo por Bruce Schneier y Jeremiah Grossman. El evento se celebrará del 16 al 19 de Noviembre del 2010.

Para obtener más información sobre la conferencia:

http://www.owasp.org/index.php/AppSec_Brasil_2010

OWASP Top 10 2010 liberado

El OWASP Top 10 2010 fue publicado el 19 de abril de 2010. OWASP recibió una gran cobertura de prensa sobre la liberación. A continuación se enumeran algunos vínculos de medios de comunicación y de noticias internacionales en las que se nombra a OWASP. Si aún no lo ha hecho, por favor reserve un momento para revisar el Top 10 del 2010 y acepte el desafío para hacer más visible la seguridad de las aplicaciones.

Para leer el comunicado de prensa:

http://www.owasp.org/index.php/OWASPTop10-2010-PressRelease

Artículos:
Logic Flaws and the OWASP Top 10, Steve Ragan—The Tech Herald

Top 10 Most Critical Web App Security Risks, Ericka Chickowski—Channel Insider

Injection tops list of web application security risks, Angela Moscaritolo—SC Magazine

OWASP Issues Top 10 Web Application Security Risks List, Kelly Jackson—DarkReading

Security: 10 Most Dangerous Web App Se-

Boletín OWASP: convocatoria de artículos

OWASP está buscando artículos de seguridad en aplicaciones para publicarse en el boletín de OWASP:

Las presentaciones candidatas no deben ser de carácter comercial. Contactar con: Lorna.Alamri@owasp.org para obtener más información o enviar presentaciones.

OWASP Podcasts Series

Presentados por Jim Manico

Ep 61 Richard Bejtlich (Network Monitoring)

Ep 62 Amichai Shulman (WAF)

Ep 63 Ed Bellis (eCommerce)

Ep 64 Andy Ellis (Availability)

Ep 65 AppSec Round Table: Boaz Gelbord, Dan Cornell, Jeff Williams, Johannes Ullrich & Jim Manico

Ep 66 Brad Arkin (Adobe)

Ep 67 Top Ten– Jeff Williams (XSS)

Ep 68 Top Ten— Kevin Kenan (Cryptographic Storage)

Ep 69 Top Ten—Eric Sheridan (CSRF)

Ep 70 Top Ten— Michael Coates (TLS)

Ep 71 Top Ten— Robert Hansen (Redirects)

Entrevista con Jim Manico

Lorna Alamri

Una de las cosas más excepcionales de OWASP es que permite reunir a personas apasionadas por la seguridad en aplicaciones. Jim Manico ha elaborado una serie de podcast de renombre donde entrevista a conocidos expertos de seguridad en aplicaciones. Ha sido capaz de usar su talento para desarrollar una serie de podcast de OWASP, crecer en su carrera y aumentar la base de conocimientos OWASP y concienciación alrededor de la seguridad en aplicaciones.

¿Por qué decidiste en hacer el primer podcast?

En octubre de 2008 estaba asistiendo a varias interacciones entre voluntarios OWASP sobre las listas electrónicas de OWASP y me fascinó la profundidad del discurso. Pensé, alguien necesita recopilar esto. Pensé que el podcasting sería fácil por lo tanto sin realmente pedir permiso, directamente empecé a grabar. :) Arshan, Jeff Williams y Jeremiah Grossman se ofrecieron para ser mis primeras víctimas - y desde entonces llevo haciendo el podcast de OWASP. :)

¿Cuál fue su objetivo original con el podcast? ¿Ha cambiado? Si lo ha hecho, ¿cómo?

Mi objetivo original era grabar “de forma sencilla” sobre un servicio de conferencia telefónica gratuita y publicar el mp3 definitivo. Ahora, compré un micrófono de estudio de mejor calidad y estoy centrándome más en la calidad de la producción final, que sea lo mejor posible, a través de cuidado de la edición y masterización profesional. Es un giro de 360º a mis intenciones originales, pero estoy intentando evolucionar constantemente la calidad del show.

¿Cómo se ha desarrollado el proyecto?

Hoy (mediados de Marzo) estoy editando el show 63. Tengo varios programas completados y esperando el lanzamiento a la prensa del Top Ten.

¿Cómo preparas una entrevista?

Empiezo la programación con varios invitados. También tengo una invitación recurrente mensual para el programa de la mesa redonda. Trabajo preguntas con invitados de antemano. Estoy buscando comentarios inteligentes, no sorprender a mis invitados.

¿Cuál fue el programa más popular? ¿el más controvertido? ¿tu favorito?

Las mesas redondas son los programas más populares. Tuvimos la llamada de un invitado que definió a los de OWASP como "un montón de comunistas" que levantó algunas cejas. Mi programa favorito fue con Billy Hoffman de HP - dijo que mi abuela merecía ser hackeada. ;) La llegada de Dave Aitel en el programa fue el más interesante de todos. Richard Stallman vino al programa y me criticó mucho después de que le preguntara cuál era su cuenta de Skype. (PD: ¡sólo publiqué la entrevista de Stallman en OGG! ¡Lo juro!) Pero estoy especialmente agradecido a Andre Gironda, Jeff Williams y Booz por todo su apoyo en el proyecto. Y, francamente, **¡todos mis invitados han sido fantásticos!**

Sabiendo lo que sabe ahora ¿que haría de forma diferente, si es el caso?

¡Nunca proclamaría que un servicio de conferencia telefónica gratuita sería lo suficientemente bueno para grabar un podcast! :)

¿Cuál fue su mayor desafío al inicio el podcast?

El empezar. Una vez se empieza, el espíritu del podcast sigue su curso. :)

¿Por qué sientes que tiene éxito?

Por los invitados. He tenido el placer de contar con invitados increíblemente inteligentes y con talento en el programa. No podríamos haber hecho esto sin esa comunidad.

Si pudieses entrevistar a cualquier persona para el podcast—¿qué persona sería?

¡Me gustaría entrevistar al empleado de MS que inventó el HTTP Only! :) Pero en realidad, Bruce Schneier es una de las personas que todavía estoy persiguiendo para que esté en el programa. Grabé con Bruce en los primeros días del podcast, pero (por mi culpa) la calidad de grabación fue tan mala que no podía publicarlo. ¡Bruce! ¡Lo siento! Por favor, dame una segunda oportunidad. :)

¿Y ahora cual es el siguiente paso?

¡El espectáculo debe continuar! Varias compañías han sido muy amables en donar a OWASP por estar en el programa - que me ha dado un poco de presupuesto para poder adquirir equipamiento para el estudio más profesional para futuros programas. ¡Gracias a Tenable, Adobe, Orbitz y Akamai por sus generosas donaciones de OWASP!

¿Has aprendido alguna lección que te gustaría compartir? ¿Cualquier otra cosa que te gustaría compartir con los oyentes?

He publicado mi lista del equipamiento y el proceso en http://www.owasp.org/index.php/Talk:OWASP_Podcast Esta lista es el resultado de muchas de las lecciones aprendidas en los últimos años.

Lo más importante, ¡gracias por escuchar! ¡El programa no sería un éxito si no fuese por nuestros fantásticos oyentes!

Cualquier comentario, no dudes en escribirme a podcast@owasp.org.

¿Puedes ayudar a OWASP a hacer que cada desarrollador de aplicaciones conozca el Top 10 de OWASP? Comparte este vínculo:

OWASP_Top_10_-_2010.pdf

Capítulo OWASP de Londres
Proyecto de formación OWASP AppSec

El capítulo de OWASP de Londres completó su primer evento de formación el 16 de abril. Completaron un día de presentaciones para abordar las siguientes deficiencias:

- Aparte del Top 10 de OWASP, la mayoría de los proyectos OWASP no se utilizan o no son fácilmente entendibles. En la mayoría de los casos, esto es no debido a la falta de calidad y utilidad de los proyectos de Documentación & Herramientas, y si debido a la falta de comprensión del lugar dónde ubicarlos en el ecosistema de una empresa de seguridad o en el ciclo de vida del desarrollo de aplicaciones Web.
- Este curso pretende cambiar eso proporcionando una selección de proyectos preparados y maduros para empresas con ejemplos prácticos de cómo utilizarlos.
- El curso será muy práctico donde se realizarán demostraciones y ejercicios prácticos para las herramientas que se cubren.

Los materiales pueden descargarse en:

Proyectos OWASP y recursos que se pueden utilizar HOY

Actualmente se están buscando capítulos OWASP para coger los materiales y replicar las clases para los mercados que sirvan.

Gracias a nuestros miembros corporativos que renovaron su apoyo de la Fundación OWASP en marzo y abril

Booz | Allen | Hamilton

cigital

symantec

fishnet SECURITY

Nuevo Patrocinador Corporativo en Abril: Qualys ¡Gracias por su apoyo!

QUALYS

Sigue a OWASP

Feed de twitter OWASP

http://twitter.com/statuses/user_timeline/16048357.rss

IBWAS '10—Call for Papers
Carlos Serrão, Ph.D.

IBWAS'10, segunda edición. El congreso Iber-Americano de Seguridad en Aplicaciones Web será en Lisboa (Portugal), el 11 y 12 de Noviembre de 2010. Este congreso busca reunir a expertos de seguridad en aplicaciones, investigadores, formadores y profesionales de la industria, comunidades internacionales como OWASP, para debatir abiertamente sobre los problemas y nuevas soluciones en la seguridad de aplicaciones. En el contexto de este evento los investigadores serán capaces de combinar interesantes resultados con la experiencia de profesionales e ingenieros de software.

Los organizadores del congreso han publicado el Call For Papers (CFP) y cualquiera que esté interesado en presentar su trabajo al congreso debería hacerlo, según las instrucciones detalladas en el CFP, antes del 24 de Septiembre de 2010. Los temas sugeridos para los trabajos a enviar incluyen (que no limitan):

- Desarrollo seguro de aplicaciones
- Arquitecturas orientadas a la seguridad del servicio
- Frameworks de desarrollo de seguridad
- Modelado de amenazas en aplicaciones web
- Seguridad en la nube
- Vulnerabilidades en aplicaciones web y análisis (revisión de código, test de intrusión, análisis estático, etc)
- Métricas para la seguridad de aplicaciones
- Técnicas de desarrollo seguro
- Plataformas o funcionalidades de seguridad en el lenguaje que ayuden a asegurar las aplicaciones web
- Control de acceso en aplicaciones web
- Privacidad en aplicaciones web
- Estándares, certificaciones y criterios de evaluación de la seguridad para aplicaciones web
- Concienciación y formación de seguridad en aplicaciones
- Ataques y explotación de vulnerabilidades

Todos los trabajos aceptados se publicarán en las actas del congreso, bajo una referencia ISBN. Las actas del congreso se publicarán por Springer en las series Communications in Computer and Information Science (CCIS). Para obtener más información visite:

Call for Papers:

http://www.owasp.org/index.php/IBWAS10#tab=Call_for_Papers

Página web del congreso:

http://www.ibwas.com

Actualización de proyectos OWASP
Paulo Coimbra, OWASP Project Manager

Nuevos Proyectos

Proyecto de traducción de Hungría

http://www.owasp.org/index.php/OWASP_Hungarian_Translation_Project#tab=Project_Details

RFP– Criteria

http://www.owasp.org/index.php/Projects/RFP-Criteria

Nuevas Publicaciones

JSReg: JavaScript regular expression based sandbox

https://code.google.com/p/jsreg/

HTML Reg: Java Script regular expression based sandbox for HTML

http://code.google.com/p/htmlreg/

JavaScript regular expression based sandbox for CSS

http://code.google.com/p/cssreg/

Formación de OWASP

Formación de Londres: Proyectos de la OWASP y recursos se puede utilizar hoy 28 de mayo de 2010

Enlaces de Vídeos de formación

http://www.youtube.com/watch?v=pYp-kJTrzCE&feature=player_embedded

http://www.youtube.com/watch?v=eRRwaAmKhVg&feature=player_e

Actualizaciones sobre traducciones ASVS & proyecto ESAPI para PHP
Mike Boberski

El número de traducciones completadas de ASVS es tres: francés, alemán, japonés Vínculo: Traducciones ASVS
Traducciones de otros idiomas en desarrollo: Malayo, Chino, Húngaro, Persa, Español y Tailandés.

El Proyecto ESAPI para PHP está cerca de su primer lanzamiento, ultimando retoques en el código base para que sea conforme con PEAR , agregando phpdoc, y finalizando unos pocos controles.

Enlace: http://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API#tab=PHP

OWASP
Dando visibilidad a la seguridad en aplicaciones

Este año OWASP se centra en hacer más visible la seguridad de las aplicaciones. Una manera de hacerlo es centrándose en dar charlas en nombre de OWASP en eventos no propios de OWASP. A continuación se detallan algunos de esos eventos dónde OWASP transmitirá su mensaje sobre la seguridad en aplicaciones tanto a organizaciones de seguridad como de desarrollo.

Francia: El Capítulo francés será en el RMML de 2010: http://2010.rmll.info/OWASP.html?lang=en

Sobre RMLL2010: el encuentro de Software Libre (LSM o RMLL en francés para Rencontres Mondiales du Logiciel Libre) es un ciclo de conferencias sobre software libre. LSM es un evento anual que nació en el año 2000 y desde el año 2003, se produce en una ciudad diferente cada año. Los LSM son libres tanto en cerveza como en ponencias :-) Sin tarifas, sin límite de plazas.

El LSM de 2010 tendrá lugar en Burdeos del 6 al 11 de julio. LSM 2010 tendrá 7 temas principales (cada tema será sede de varias sesiones más centradas): Se presentarán algunas herramientas y trucos *appsec* (como un pequeño sucedáneo de la formación de OWASP de Londres): 10 Top 10 2010 + Ejemplos WebGoat/WebScarab.

Grecia: El Capítulo de griego es compatible con AthCon (http://www.athcon.org/), un congreso que se celebrará en Atenas, Grecia, el 3 y 4 de junio de 2010. Los miembros OWASP cuentan con un descuento del 15% en el registro.

Malasia: El Capítulo de OWASP de Malasia estará en Malaysia Open Source Conference 2010. http://conf.oss.mm

Singapur: OWASP Singapur apoyará los siguientes eventos:

1) SecureAsia@Singappore del ISC² el 26 y 27 julio de 2010. http://www.informationsecurityasia.com/

2) Singapore Ministry of Home Affairs'

GovernmentWare, 28-30 septiembre 2010 http://www.govware.sg

Eslovenia: OWASP Eslovenia estará en el congreso OTS 2010 (http://cot.uni-mb.si/ots2010/) que se celebrará en Maribor, Eslovenia, el 15 y 16 de Junio. El OTS celebra su 15º aniversario y OWASP Eslovenia se enorgullece en hacerse cargo de la Sección de Seguridad en Aplicaciones, el miércoles 16 de junio a las 16:15.

Estados Unidos: OWASP tendrá ponentes destacados en ICCS. http://www.iccs.fordham.edu/ El International Conference on Cyber Security es un esfuerzo conjunto entre el FBI y la Universidad de Fordham. Tendrá lugar en el Fordham Law Center de Nueva York, del 2 al 5 de Agosto del 2010.

¿Busca empleo en seguridad en aplicaciones?
Visite la página de empleo de OWASP

¿Necesita publicar una oferta de trabajo sobre seguridad en aplicaciones?
Contacto:
Kate Hartmann

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.

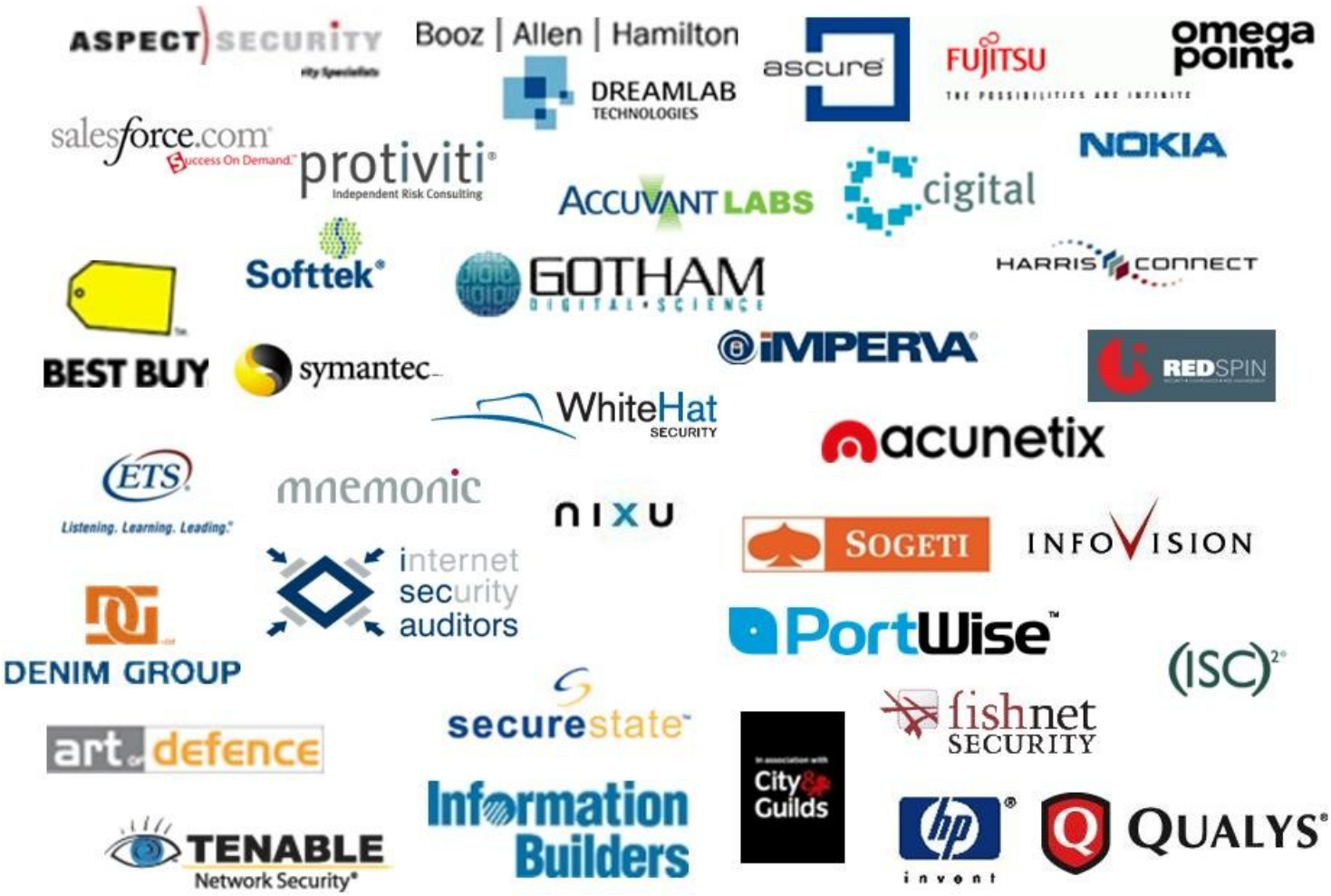
El proyecto abierto de seguridad en aplicaciones Web (OWASP por sus siglas en inglés) es una comunidad abierta dedicada a habilitar a las organizaciones para desarrollar, comprar y mantener aplicaciones confiables. Todas la herramientas, documentos, foros y capítulos de OWASP son gratuitos y abierto 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**: Jose A. Guasch, Christian (chr1x) Navarrete