17 de Julio, 2010

Congresos sobre seguridad en aplicaciones

Septiembre 7-10, 2010, Irvine, CA - USA ¡Abierto el proceso de registro! http://www.appsecusa.org/register-now.html

Septiembre 16-17, 2010, Dublin Irlanda

CFP y CFT ABIERTOS – http://www.owasp.org/index.php/OWASP_IRELAND_2010#Call_for_Papers REGISTRO ABIERTO - http://www.owasp.org/index.php/OWASP_IRELAND_2010#Registration

Octubre 20-21, 2010, Rochester, NY – USA CFP ABIERTO - http://www.rochestersecurity.org/call-for-presentations

Octubre 20, 2010, Nurnbeg, Alemania

CPF OPEN - http://www.owasp.org/index.php/OWASP_AppSec_Germany_2010_Conference#tab=Call_for_Papers_-_English_Version

Octubre 20-23, 2010, Beijing, China CFP/CFT ABIERTOS - http://www.owasp.org/index.php/OWASP_China_Summit_2010#tab=Call_For_Paper

Octubre 29, 2010, Austin, TX - USA

CFP ABIERTO - http://www.owasp.org/index.php/Lonestar_Application_Security_Conference_2010#tab=Call_for_Papers

Noviembre 8-11, 2010, Washington, DC – USA

CFP/CFT ABIERTOS - http://www.owasp.org/index.php/OWASP_AppSec_DC_2010#tab=CFP

ABIERTO REGISTRO- http://www.owasp.org/index.php/OWASP_AppSec_DC_2010#tab=Registration

Noviembre 11-12, 2010, Lisbon, Portugal

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

Noviembre 16-19, 2010, Campinas, SP, Brasil

CFP y CFT ABIERTOS - http://www.owasp.org/index.php/AppSec_Brasil_2010#tab=Calls

OWASP Podcasts Series

Presentado por:
Jim Manico

Ep 72 Interview with Ivan Ristic (WAF)

Ep 73 Jeremiah Grossman and Robert Hansen

Gracias a nuestros miembros corporativos quienes renovaron su apoyo a la Fundación OWASP en junio y julio.

Entrevista con Matt Tesauro

Lorna Alamri

Una de las cosas más excepcionales sobre OWASP es que permite a personas que son apasionadas por la seguridad de la aplicación un foro de discusión. Matt Tesauro es responsable del proyecto LiveCD. Su participación en OWASP le permitió crecer su carrera y aumentar su base de conocimientos en OWASP y la conciencia alrededor de seguridad de las aplicaciones.

¿Por qué decidiste hacer el primer LiveCD?

Hice la OWASP Live CD como parte de la OWASP Summer of Code del 2008. Recibí el correo electrónico de OWASP acerca del SoC y cuando leí que era acerca de un proyecto que combinaba la seguridad de las aplicaciones y Linux, sabía que era para mí ya que son dos de mis cosas favoritas .

¿Cuál fue tu objetivo original con el LiveCD? ¿Eso ha cambiado? Si entonces, ¿cómo?

El objetivo original del Live CD era tener uno trabajando por el plazo de la SoC. ;)

En realidad, estaba intentando reunir las mejores herramientas de seguridad en aplicaciones en un paquete fácil de usar. Mantuve las herramientas centradas en seguridad de aplicaciones en lugar de hacer un CD de herramientas de "hacking" general.

El Live CD definitivamente ha cambiado desde su primera versión en septiembre de 2008. El primer gran cambio fué el surgimiento de varios sub-proyectos fuera del Live CD. El primero de ellos fueron instalaciones virtuales para VMware y VirtualBox. Conseguimos uno, pero extremadamente lento, mientras que la VM en versión USB trabajó sin problema .

La verdad es que llegó a ser mucho más que sólo un Live CD. Por esa razón, la última versión se ha renombrado a OWASP WTE o Entorno de prueba Web. Hemos tomado la base del CD Live de OWASP, migrado de SLAX a Ubuntu Linux y creado paquetes individuales e instalables para todas las herramientas en WTE .

La gran mejora que esto permitirá es el desarrollo más fácil de los métodos para obtener herramientas de pruebas en manos de los profesionales en seguridad. Con los últimos paquetes, puedes tener una instalación estándar de Ubuntu, apuntando hacia el repositorio de WTE, y en pocos minutos, todas las herramientas instaladas de WTE .

¿Cómo se ha desarrollado el proyecto ?

Como he mencionado anteriormente, su pasado de ser sólo un CD de arranque aun montón de métodos distintos para obtener las herramientas que desee. Tan pronto como completemos la migración de SLAX a Ubuntu, vamos a tener un montón de métodos distintos de obtener WTE para los usuarios finales :

- Live CD
- Instalaciones Virtuales (VMware, VirtualBox, Parallels, ...)
- Agregando paquetes a instalaciones de Ubuntu existentes
- WTE en un stick USB
- Wubi - un método de booteo dual para Windows y Ubuntu sin reparticionar
- Versión personalizada como la colección de herramientas estáticas de Java, una version con herramientas, objetivos de ataque, etc
- Nuevas categorías de herramientas como la de herramientas de análisis estático

También he tenido la suerte de contar con varias personas que colaboran en el proyecto. Nishi Kumar hizo la gráfica para las liberaciones. Brad Causey y Drew Beebe han contribuido muchas, muchas horas al proyecto también. Ellos también merecen una mención por la ayuda que han proporcionado .

Tengo que admitir que desde que me mudé a SpiderLabs Trustwave, he invertido mas tiempo acostumbrarme a un lugar nuevo y maravilloso para trabajar, que a la actualización del proyecto. He disfrutado mucho el calibre de mis compañeros de trabajo en SpiderLabs y pasó más tiempo hablando que haciendo paquetes de Debian para WTE. Nada que temer, sin embargo, sigo encontrándome trabajando en una instalación virtual de WTE por lo que es sólo cuestión de tiempo antes de que empiece a nuevamente.

¿Cuál fue la aplicación más popular en el LiveCD? la más controvertida? tu favorita?

Por un largo camino, la más comentada, preguntada y probablemente las mas utilizada en el Live CD ha sido WebGoat. Creo que el hecho de que WebGoat fuera un arranque rápido para estar preparados y fue una gran bendición para muchas personas ya sea en el aprendizaje seguridad de las aplicaciones así como para los que dan clases.

No estoy seguro si realmente ha habido una aplicación polémica agregada - tal vez Metasploit que no es estrictamente una herramienta de seguridad para aplicación web . Además, he tenido un poco de tristeza por Maltego CE que es una versión de prueba de código cerrado. Las ventas de Maltego es lo que mantiene un techo sobre la cabeza de la persona que lo escribió, así que no mantengo nada contra el.

En cuanto a un favorito personal - No me gusta destacar sólo uno. Algunos de los que utilizo con mayor frecuencia son WebScarab, BurpSuite, JBroFuzz, Nikto y DirBuster. Hay también algunos nuevos favoritos, que se añadirán a WTE en la próxima versión.

Sabiendo lo que sabes ahora, ¿qué harías de otra manera, hay algo?

Me gustó mucho SLAX para hacer un Live CD. Fue muy bueno para ese fin. Sin embargo, el momento que mas se nos extendió fueron las máquinas virtuales y tratar de actualizar el Live CD de forma dinámica, es simplemente que el sistema no es el mas adecuado.

Entonces, si tuviera algo más que ver, me gustaría comenzar con una versión de Linux con un sistema adecuado de gestión de paquetes. Debian ha tenido muchos años para elaborar los problemas de la gestión de paquetes, ¿Por qué se ponerse sobre los hombros de esos gigantes? Por cierto, RPM es también un sistema de gestión de paquetes muy bueno. Si usted es un asistente de RPM, me encantaría trabajar con usted para obtener RPMs a partir de los paquetes .deb para WTE .

¿Cuál fue tu mayor desafío de iniciar el Proyecto LiveCD

Uno de mis retos iniciales fue el mantener la cordura sana. Empecé a buscar en varias herramientas de seguridad en aplicaciones y terminé con una lista de hasta 330 herramientas. Poner en marcha esto a un número sano llevó un tiempo. También, aprender a crear apropiadamente los paquetes es por adelantado fue doloroso, pero ya trabajando, se puede automatizar la actualización de los paquetes una ves que salgan versiones nuevas de las herramientas, esto es un pago a largo plazo.

¿Por qué crees que el Live CD ha sido un éxito ?

La última vez que contaron las descargas, que fue noviembre del 2009, el total fue de poco más de 330.000 descargas desde la primera versión de SoC. Eso es un número enorme de personas que han llegado a conocer OWASP y la seguridad en aplicaciones. También he escuchado de varios profesores que lo han utilizado para las clases de formación. Una de las novedades más sorprendentes fue la inclusión del Live CD de OWASP en un texto universitario. De hecho hace unas semanas en AppSec UE para 2010 en Estocolmo, uno de los asistentes me reconoció y me dió las gracias por la última versión de WTE así que ¿cómo puedo reclamar?

¿Cómo ha afectado el Proyecto LiveCD tu carrera?

Primero, ser activo y participar en OWASP ha sido enorme. Para mí, la OWASP Live CD fue una buena manera de entrar y participar con la comunidad de OWASP. Por el Live CD y hablar lo que he hecho sobre el proyecto, he estado en Portugal, Polonia, Brasil y varios lugares dentro de los EE.UU.. He conocido a un montón de gente realmente brillante y OWASP, tiene mi nombre en la comunidad de seguridad de aplicaciones.

También creo que la labor sobre el Live CD y con la ayuda del Comité Global me ha ayudado a convertirme en un miembro del tablón de la Fundación OWASP. Ayudar y trabajar con los miembros de OWASP en el cumplimiento de la misión de OWASP ha sido una experiencia maravillosa.

En un nivel pragmático, he sido un entrenador pagado varias veces debido a los Live CD. Por no hablar de que la participación activa con tener OWASP y en el consejo de OWASP es un material muy beneficioso para mi carrera. Estoy seguro de que mi experiencia en OWASP es un factor importante en mi situación actual con SpiderLabs Trustwave.

¿Y ahora que sigue?

Para WTE, me gustaría hacer crecer el número de contribuyentes para que no se conviertan en un cuello de botella que he estado a principios de este año. También me gustaría ampliar los paquetes que forman parte de WTE para incluir herramientas de análisis estático, las herramientas de Flash, y tal vez algunas aplicaciones demasiado vulnerable.

Y para mi cargo dentro de OWASP, estoy trabajando activamente en la infraestructura que lleva a cabo las operaciones OWASP. Con suerte, OWASP tendrá una nueva infraestructura que ayudará a llegar a la comunidad a un nuevo nivel de éxito.

¿Algo más que quieras compartir con los fans del proyecto?

No dejaré de agradecer a aquellos que han hecho que licenciar como GPL, Apache o BSD fuese tan fácil. Intentar averiguar si podía incluir tranquilamente herramientas en WTE al final resultó ser más difícil de lo que pensaba. No te puedes imaginar la cantidad de proyectos que tuve que descargar y analizar antes de dar con la licencia.

Lo que quiero compartir con los fans del proyecto es que por favor aporten ideas, sugerencias, quejas o lo que sea mediante la lista o el foro del proyecto. La mejor manera de que el proyecto mejore es que los que trabajamos en él sepamos que funciona o lo que no.

Nuevo patrocinador corporativo en junio y julio:
¡Gracias por su apoyo!

Sigue a OWASP

OWASP tiene un feed de Twitter

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

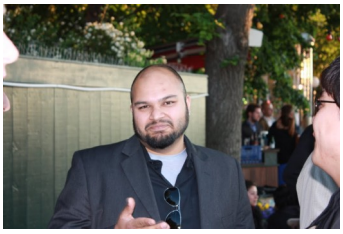
¿Podrías ayudar a OWASP a que todo desarrollador de aplicaciones conozca el Top 10 de OWASP? Comparte este enlace: OWASP_Top_10_-_2010.pdf

Actualización de ESAPI
Jeff Williams

La NSA se ha ofrecido para realizar una revisión de seguridad a fondo de ESAPI y publicar los resultados. Para los que no tengan mucha experiencia con la NSA, una de sus principales misiones es la defensa. En el pasado, apoyaron la National Computer Security Conference, crearon las Rainbow Series y patrocinaron el SSE-CMM. Recientemente se han involucrado en SCAP y SE-Linux.

El equipo NSA que está aportando en OWASP tiene experiencia en criptografía y revisión de aplicaciones ya en marcha y comenzarán su trabajo muy pronto. Se centrarán en primer lugar en la versión Java de ESAPI, y podrían seguir con el resto de lenguajes cuando estén listos—cuando su criptografía esté por lo menos en el nivel Java 2.0. Su primera estimación para la revisión es de varios meses.

Estamos orgullosos de este desarrollo, y os mantendremos informados de su progreso.



Actualizaciones sobre los Proyectos OWASP
Paulo Coimbra, OWASP Project Manager

Nuevos proyectos

http://www.owasp.org/index.php/Projects/ESAPI_Swingset-

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

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

Proyecto con nuevas versions publicadas recientemente

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

Proyecto en busca de contribuidores para publicar una nueva versión

http://www.owasp.org/index.php/Category:OWASP_Testing_Project#tab=Project_About (Testing Guide V 4.0)

Proyecto que se ha re-publicado

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

El proyecto OWASP ESAPI Swingset Project tiene un nuevo líder

Cathal Courtney. ¡Démosle la bienvenida!

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

Este proyecto ya tiene publicada una versión, ESAPI Swingset RC 4, que se acaba de publicar—por favor, echadle un vistazo.

http://www.owasp.org/index.php/Projects/ESAPI_Swingset/Rzeleases/Current

Página de OWASP Google Analytics

Visitas en Mayo: 233,765
Páginas vistas: 573,144
Páginas por visita 2.45
Tiempo medio de permanencia en sitio: 00:02:57
Porcentaje de nuevas visitas: 58.3%
http://conf.oss.my
Según contenido:
/index.php/Main_Page 63,070 visitas
/index.php/Category:OWASP_Top_Ten_Project 21,610 visitas
/index.php/Category:OWASP_WebScarab_Project 16,615 visitas
/index.php/Category:OWASP_WebGoat_Project 13,502 visitas
/index.php/Category:OWASP_Project 10,915 visitas
TOP palabras clave:
Owasp, webscarb, owasp top 10, webgoat, sql injection.

Plataforma OWASP O2
Dinis Cruz

Me es grato comunicar que finalmente he publicado la primera versión de la plataforma OWASP O2 Platform (con instalador, documentación y videos y un conjunto de funcionalidades claves y únicas).

Posee una nueva interfaz que aporta una gran diferencia en comparación a los scripts disponibles, herramientas y APIS que forman O2 (si probasteis versiones anteriores lo comprobaréis rápidamente). Podréis ver más sobre la interfaz y acceder a su descarga en la página : http://www.o2platform.com/wiki/O2_Release/v1.1_Beta

PROBADLA POR FAVOR, y hacedme llegar todo tipo de comentarios: lo que os gusta, que funciona, que no funciona, que podría mejorarse, etc... (si queréis enviar cualquier bug, por favor utilizar este mecanismo http://code.google.com/p/o2platform/issues/list)

Esta versión de O2 contiene las suficientes funcionalidades y capacidades como para tener la confianza suficiente de plantearos esta petición directa, sabiendo que sin importar el área de Seguridad en Aplicaciones Web en la que os encontréis, habrá un Script/Módulo/Herramienta de O2 que os ayude.

Debido a que la nueva interfaz es muy reciente, la mayoría de la documentación y videos disponibles comienzan con la anterior versión. Pero como ahora puedo crear documentación en el WIKI fácilmente o videos usando O2, mi intención es responder a vuestras preguntas así)por ejemplo con una página en el wiki o un video)

Resumen OWASP AppSec Research
John Wilander

La versión europea del congreso OWASP AppSec tuvo lugar en Estocolmo, del 21 al 24 de Junio. 3 capítulos locales - Suecia, Noruega y Dinamarca—junto con la Universidad de Stockholm presentaron este evento y dio la bienvenida a 275 asistentes a una soleada Escandinavia.

Los primeros dos días se ofreció formación en desarrollo seguro, pentest, análisis de malware y revisión de arquitectura. Durante la cena en conjunto del Lunes los invitados americanos aprendieron a comer hamburguesas con tenedor y cuchillo—Una especialidad sueca :)

Para las charlas se contó con 3 tracks paralelos con ponencias y demostraciones tanto desde el ámbito empresarial como académico. Las ponencias principales giraron en torno al futuro de la seguridad en navegadores y en el desarrollo del Ciclo de Vida del Software desde los 90. En los stands de los patrocinadores se contó con 12 compañías encabezadas por el patrocinador Diamante Microsoft.
El miércoles por la noche, los asistentes así como otros fueron bienvenidos en el Stockholm City Hall con una cena de gala compuesta por tres platos y entretenimiento. Una celebración fabulosa en conjunto patrocinada por Google. Durante la cena en las mesas se sirvió champán en tres categorías—cultura, frikismo y arte. El último reto que consistía en construir la estatua inspirada en OWASP a base de desatasca tuberías se incentivó con mucha creatividad. ¿O era vino?
Los organizadores desean agradecer a todos los que apoyaron y formaron parte de esta primera OWASP AppSec Research. ¡Nos vemos el año que viene en Dublín!

¿Buscando trabajo sobre seguridad en aplicaciones? Revisa la página de empleo OWASP

¿Necesitas ofrecer algún trabajo?

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: Lorna Alamri, **Fotos de la AppSec Research de Estocolmo**: Boris Hemkemeier **Traducción**: Jose A. Guasch, Christian (chr1x) Navarrete