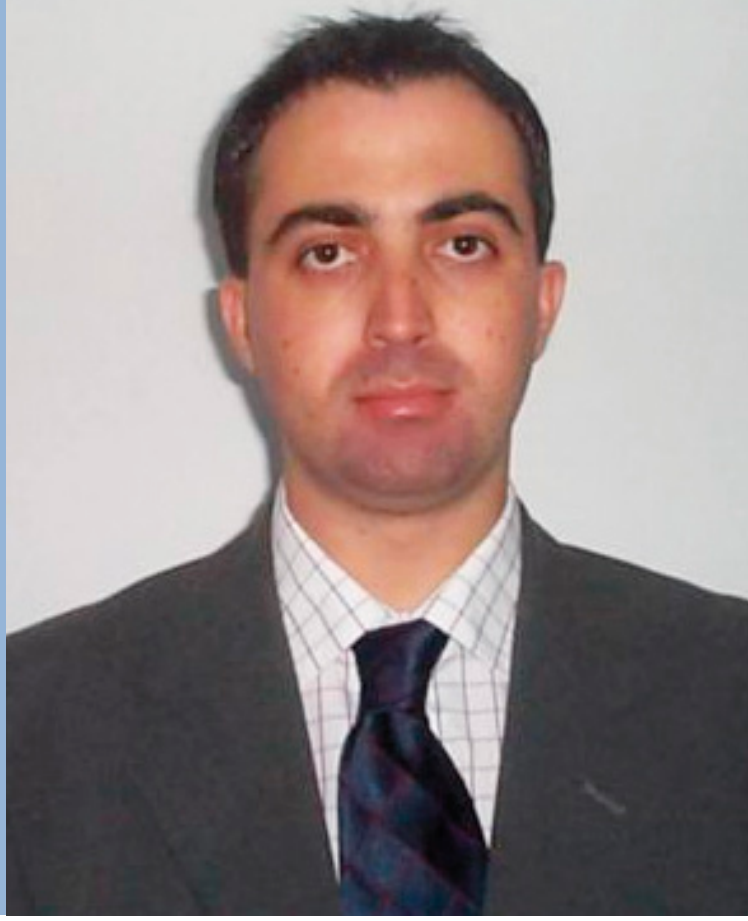
Vicente Aguilera

Presidente del capítulo español de 'Open Web Application Security Projet' (OWASP)



Defensor acérrimo de que la seguridad en las aplicaciones y sistemas es mayor en código abierto que en código propietario, y seguro de su convencimiento de que el *software* libre ofrece una mayor capacidad de reacción y distribución, en caso de ataques y vulnerabilidades, Vicente Aguilera quiso compartir estos conocimientos, y otros muchos que ya tenían total aceptación fuera de nuestro país, con profesionales españoles. Para ello, fundó el capítulo español de OWASP.

"No todos entienden aún la seguridad como una medida más del nivel de calidad"

Tx: Mercedes Oriol Vico.
Ft: OWASP.

¿Cuándo nació OWASP?
OWASP fue creado en 2000 por Mark Curphey (quien desde octubre de 2007 lidera el ACE Team de Microsoft en Europa). Por aquel entonces, la seguridad en la capa de aplicación era, en general, prácticamente inexistente y relegada por la capa de red en la que se concentraban la mayor parte de los esfuerzos. De ahí que OWASP naciera con un claro objetivo: ayudar a incrementar el nivel de seguridad de las aplicaciones dando a conocer los riesgos existentes, desarrollando guías y metodologías, creando herramientas, organizando conferencias y siguiendo una premisa hasta las últimas consecuencias: todo el material de OWASP tenía que ser libre y gratuito. Este hecho ha contribuido, sin lugar a dudas, al gran crecimiento y la rápida evolución de nuestros proyectos. Además, su carácter independiente, no ligado a ningún fabricante, ha favorecido su difusión y aceptación por la comunidad internacional.

¿Y su fundación cuándo surgió?
La fundación OWASP es una asociación sin ánimo de lucro, no vinculada a ningún producto o servicio comercial, en la que sus miembros colaboran de forma totalmente voluntaria. Nace en 2004, con idea de facilitar la infraestructura necesaria y apoyar el trabajo que realizan sus miembros. De esta forma, la fundación OWASP proporciona los servidores y ancho de banda necesarios así como soporte legal para nuestros proyectos.

¿Cuándo arranca el capítulo español de OWASP, y motivados por qué razón y con qué objetivo?
El capítulo español fue creado en diciembre de 2005, tras ser propuesto a Jeff Williams (presidente de la fundación OWASP) y aceptado por su comité. Mi experiencia en el sector de la seguridad, y más concretamente en el de la auditoría de aplicaciones, me permitía conocer el grado de inmadurez en

el que se encontraban los desarrollos en nuestro país.

Anteriormente, conocía los proyectos de OWASP y me mantenía informado a través de sus listas de correo y los contactos con la Dirección, lo que me motivó a la creación del capítulo español con la idea de trasladar y difundir dicho conocimiento en España.

¿Cuáles son sus líneas de actuación y sus recomendaciones básicas como asociación?

Nuestro trabajo y objetivo sigue las mismas pautas que el definido desde la Dirección de la fundación OWASP. La ventaja es que, al tener representación local, podemos tener un contacto más directo con todos aquellos que, de una forma u otra, se encuentran relacionados con la seguridad en las aplicaciones y servicios Web.

Por nuestra parte, actualmente organizamos dos eventos al año en los que, a modo de conferencias, se exponen conocimientos y experiencias de la mano de figuras destacadas del sector de la seguridad en nuestro país.

Asimismo, este año hemos iniciado el proyecto "Especificación de requisitos legales para las aplicaciones Web", en el que analizamos la legislación española para extraer aquellos aspectos relacionados con la especificación de requisitos para las aplicaciones Web y crear un documento base de referencia. En este proyecto colabora, de forma totalmente altruista, personal de distintas universidades, abogados, auditores y consultores de seguridad.

Por otro lado, nuestros miembros escriben artículos, participan en foros de seguridad, desarrollan herramientas y colaboran en distintos proyectos con la idea de difundir la cultura de la seguridad en las aplicaciones.

Por último, mantenemos y gestionamos la página del capítulo español (http://www.owasp.org), así como nuestra lista de correo en la que informamos de las distintas novedades que se producen en nuestro entorno.

¿Con cuántos miembros cuenta hoy OWASP? ¿Y su capítulo español?

La comunidad OWASP cuenta en la actualidad con 144 capítulos locales y cerca de diez mil miembros repartidos en dichos capítulos, de los cuales la mitad de ellos colabora de forma activa en nuestros proyectos. En el capítulo español contamos con 257 miembros, y somos el capítulo de Europa más numeroso. Este hecho indica el gran interés que despierta la seguridad en las aplicaciones Web en nuestro país y refleja el trabajo que, entre otros, viene desarrollando nuestro capítulo.

OWASP es una asociación independiente. ¿Qué relación mantiene con Internet Security Auditors?

Como fundador y presidente de OWASP Spain y socio co-fundador de Internet Security Auditors (ISECAuditors), tengo un pie en ambos sitios. Mis socios en ISECAuditors apoyan mi trabajo en OWASP y desde el inicio de nuestro capítulo, ISECAuditors quiso ser nuestro patrocinador (al que espero se unan otras entidades y organismos, a los que animo desde aquí), lo que ha permitido, entre otras cosas, poder organizar periódicamente nuestros eventos.

> "Hasta hace unos años, la seguridad de las aplicaciones Web había sido sorprendentemente olvidada"

En cualquier caso, OWASP Spain es fiel a sus principios y siempre se mantedrá independiente de cualquier tecnología, fabricante, producto o servicio.

Cada vez proliferan más las asociaciones vinculadas con la seguridad en todos sus ámbitos, ¿a qué cree que se debe esto?

Como comentaba al inicio, hasta hace unos años y desde el punto de vista de la seguridad, las aplicaciones Web habían sido sorprendentemente olvidadas, más aún cuando el número de ellas crecía a un ritmo vertiginoso al igual que nuestra dependencia sobre las mismas. Posiblemente sean el componente de nuestras infraestructuras telemáticas que mayor atención requiera, pero no es el único. La complejidad e interconexión, cada vez mayor entre los distintos componentes, requiere abordar la seguridad de una forma global y el primer paso consiste en ser conscientes de esta necesidad.

No cabe duda de que las asociaciones vinculadas con la seguridad realizan un gran trabajo y posibilitan la difusión de los riesgos existentes en este sentido, además de ofrecer un foro de conocimiento y nexo de unión entre los profesionales del sector. La proliferación de estas asociaciones puede deberse, por un lado, a la necesidad actual de cubrir todos los ámbitos de la seguridad y, por otro, a la demanda de conocimientos y mejora de los mismos por parte de los profesionales.

¿Qué parcela defienden ustedes desde OWASP?

Nosotros nos focalizamos en las aplicaciones y servicios Web, que no es poco. En este sentido, hemos desarrollado y puesto a disposición de la comunidad cerca de 100 proyectos sobre herramientas y documentación (http://www.owasp.org/index.php/Category:OWASP_Project). Algunos de estos proyectos se han convertido en material de referencia imprescindible para arquitectos, desarrolladores, diseñadores, auditores y, en general, para cualquier persona interesada en la seguridad de las aplicaciones. Otros proyectos se han convertido en un estándar *de facto* en cuanto a seguridad a nivel de aplicación, como el "*Top Ten*", una lista consensuada sobre las diez vulnerabilidades más críticas hoy en día que sufren las aplicaciones Web y que ha sido adoptado, entre otros muchos, por el estándar *Payment Card Industry* (PCI). Y todo al estilo OWASP: abierto y libre.

¿Qué colaboración mantienen con otras asociaciones del sector?

La colaboración con otras asociaciones a nivel nacional es uno de los aspectos que tenemos que potenciar y en los que vamos a trabajar el próximo año. Actualmente mantenemos relación con la Asociación de Técnicos de Informática

(ATI) y hemos iniciado contactos con capítulos de la *Information Systems Audit and Control Association* (ISACA).

En los últimos meses, han celebrado el OWASP Summit EU Portugal y el OWASP Spain Chapter Meeting. ¿Nos podría contar las conclusiones de estos foros?
Ambos eventos se celebraron el pasado mes de noviembre. En cuanto al *OWASP Spain Chapter Meeting*, se trataba de nuestro cuarto evento celebrado en Barcelona y al que se inscribieron 130 profesionales. En esta ocasión, se presentaron las actividades realizadas durante 2008 relacionadas con nuestro capítulo, así como el plan de acciones previsto para el próximo año. En cuanto a las conferencias, como ponentes contamos con José Ramón Palanco (Hazent Systems), Jesús Olmos González (Internet Security Auditors), Simón Roses Femerling (Microsoft) y Christian Martorella (S21Sec).

Respecto al OWASP Summit, se realizó en Portugal durante la primera semana de noviembre en un marco envidiable: el Algarve. Esta cumbre permitió reunir a expertos de más de 20 países entre los que figuraban las personas más destacadas de la comunidad OWASP (Jeff Williams, Dave Wichers, Tom Brennan, Dinis Cruz, Arturo Busleiman, Rogan Dawes, Matteo Meucci, Juan Carlos Calderón, y un largo etcétera). El evento se organizó en sesiones de formación, sesiones de presentación de herramientas y documentos, y unas productivas sesiones de trabajo. Como resultado, además de un gran número de buenas ideas y contactos, se establecieron compromisos con otras entidades (como PCI, que solicitará a las empresas certificadas como *Approved Scanning Vendor* (ASV), datos para alimentar el proyecto OWASP "*Top Ten*"); se crearon siete nuevos comités para trabajar en aspectos clave; se presentaron nuevas herramientas de seguridad; se explotaron problemas de seguridad no conocidos hasta el momento; y se presentó un nuevo formato de seminarios gratuitos para universidades, entre otras muchas acciones. Realmente interesante.

¿Qué otras actividades están realizando desde OWASP y cuáles tienen previstas para 2009?
Además de las jornadas de conferencias que organizamos periódicamente (y que queremos organizar en Madrid el próximo año), entre las acciones más detacadas de 2008 hemos participado en el VI Foro de seguridad de RedIRIS, en las jornadas técnicas organizadas por la Universitat Oberta de Catalunya (UOC) y en la cumbre europea de OWASP, presentando una nueva herramienta e impartiendo una de las sesiones de formación, además de participar en proyectos de traducción a español del material OWASP.

> "Si la lucha entre código abierto y propietario contribuye a la mejora de la seguridad, le deseo una larga vida"

De cara al próximo año queremos ampliar el formato de nuestros eventos y contar con nuevos patrocinadores, buscar vías de colaboración con asociaciones y entidades nacionales, potenciar la colaboración con otros capítulos europeos de OWASP e impulsar nuevos proyectos locales, como el ya propuesto "*Top Ten*", a nivel español.

¿Qué impresiones reciben ustedes de sus asociados respecto al panorama actual de la seguridad TIC?
Respecto al ámbito en el que trabajamos desde OWASP, por suerte estamos observando cómo las empresas están tomando conciencia de los riesgos e implicaciones en la seguridad que suponen los desarrollos de aplicaciones que no incorporan la capa de seguridad a lo largo del *Software Development Life Cycle* (SDLC). Este hecho motiva, por un lado, que quienes se encuentran relacionados con los proyectos de desarrollo demanden formación específica en seguridad de acorde al rol que desempeñan, y quienes se proveen de estos desarrollos exijan unos requerimientos mínimos de seguridad a sus proveedores. Como resultado, se está mejorando el nivel de seguridad de las aplicaciones que se despliegan actualmente.

No obstante, aún hay mucho trabajo por hacer: no todos entienden un problema de seguridad de la misma forma que un problema funcional, ni la seguridad como una medida más del nivel de calidad. Hasta que la seguridad no sea un requerimiento, y desde la Dirección no se adopte el compromiso de no desplegar aquellas aplicaciones que no cumplan los requerimientos de seguridad exigidos, seguiremos sufriendo aplicaciones vulnerables.

¿Qué puede aportar el código abierto a la mejora y fortalecimiento de la seguridad en las comunicaciones?
En primer lugar, un tiempo de reacción infinitamente mayor (comparado con el código propietario) ante cualquier problema de seguridad. Recuerdo un problema que notifiqué a Oracle y que tardó cerca de dos años en ser corregido en el CPU correspondiente, cuando algo similar en un producto de código abierto como SquirrelMail, no tardó más de una semana en ser solucionado. El hecho de poder ver el código que ejecutamos permite detectar y solucionar más rápidamente los problemas de seguridad. Por otro lado, permite que el código pueda ser distribuido mucho más rápido (se permite su copia) y que pueda ser adaptado y mejorado para casuísticas especiales, lo que facilita su evolución.

En OWASP contamos con proyectos, por supuesto de código abierto, que facilitan la construcción de código seguro, como el conjunto de métodos Enterprise Security API (ESAPI); el filtro J2EE CSRFGuard; o el proyecto AntiSamy, una API para evitar inyecciones de tipo XSS y ataques de *phishing*.

¿Piensa que algún día acabará la "lucha encarnizada" entre código abierto y código propietario?
Es un tema recurrente y siempre polémico. Posiblemente no acabe nunca, pero si esa lucha que comenta puede contribuir de alguna manera a la mejora de la seguridad, le deseo una larga vida.