

# Desarrollos (inseguros) de 'software': panorama actual

Vicente Aguilera Díaz

OWASP Spain Chapter Leader

oy en día hablar de seguridad pasa, indefectiblemente, por hablar de la seguridad en las aplicaciones web. La tendencia a incrementar la interactividad con los usuarios (la ahora tan oída "Web 2.0") surgió a principios de los noventa con la primera generación de Common Gateway Interface (CGI). Desde entonces ha llovido mucho y el incremento de servicios web, así como la complejidad de las aplicaciones en las que la capa de seguridad es más un añadido que un requisito, ha generado un escenario en el que los protagonistas, las aplicaciones y servicios web, se han convertido en el blanco perfecto de la mayoría de los ataques contra las infraestructuras presentes en Internet.



No es de extrañar, por lo tanto, que informes como el "Application Security Trends Q1 2007", elaborado por Cenzic (www.cenzic.com/pdfs/Cenzic\_AppSecTrends\_Q1-07.pdf), nos alerten de que el 67 por

ciento de las vulnerabilidades reportadas (incluyendo, entre otras bases de datos de vulnerabilidades, Security Tracker, OSVDB, CVE, y SANS) en el primer trimestre de este año afecten a servidores web, aplicaciones web y navegadores web. Si a este hecho añadimos que siete de cada diez aplicaciones web sufren vulnerabilidades de carácter crítico y que el 71 por ciento de las vulnerabilidades reportadas se consideran de explotación fácil o trivial, tenemos los ingredientes necesarios para que estos componentes resulten, además de atractivos, efectivos desde el punto de vista de un atacante.

Pero esto no significa que no existan soluciones, sino todo lo contrario: existen, pero se desconocen (no sabemos qué es lo que no sabemos) o se implementan de forma deficiente. A estas alturas, todos deberíamos conocer que, como aliado en esta travesía contamos con la inestimable ayuda de la OWASP (www.owasp.org). La OWASP Foundation, liderada por Jeff Williams (CEO de Aspect Security) es una asociación sin ánimo de lucro, no asociada a ningún producto o servicio comercial, cuyo objetivo principal es la divulgación de la seguridad para la creación de software más seguro.

### Capítulo español

La comunidad OWASP se organiza a modo de capítulos locales y trabaja en el desarrollo de proyectos de documentación y herramientas *open-source*, así como en la organización de conferencias relacionadas con la seguridad en las aplicaciones *web*. El capítulo español de la OWASP (www.

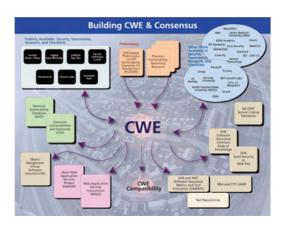
owasp.org/index.php/Spain) cuenta en la actualidad con 107 miembros, entre los que se encuentran representantes y expertos de seguridad del país, siendo el cuarto capítulo a nivel europeo con mayor número de miembros y uno de los capítulos con mayor crecimiento a nivel mundial.

La primera semana de julio, en el segundo congreso del capítulo español de la OWASP realizado en Barcelona, Pedro Sánchez, responsable de seguridad de ATCA, apuntaba directamente a uno de los focos problemáticos hoy en día: el mantenimiento de las aplicaciones. Seguramente, en nuestros nuevos desarrollos hayamos aprendido de los errores pasados y esa experiencia redunde en un incremento de la seguridad en dichos desarrollos, pero ¿qué ocurre con las aplicaciones ya existentes? En el mejor de los casos habremos aplicado parches con el objetivo de corregir aquellas vulnerabilidades más críticas, pero resultará una medida insuficiente. En el peor de los casos, contaremos con aplicaciones obsoletas vulnerables y fácilmente explotables de las que quizás, incluso, desconozcamos su existencia.

# Seguridad en las aplicaciones

La seguridad de las aplicaciones web afecta, por igual, a tres áreas clásicas: personas, procesos y tecnología. Aproximaciones centradas únicamente en una de estas áreas adolecen de problemas que impiden alcanzar el nivel de seguridad requerido por nuestra organización.

Es práctica común encontrar organizaciones que piensan que incrementar el nivel de seguridad significa invertir en tecnología, descuidando aspectos tanto o más im-



portantes como la formación de su personal. Por otro lado, tal y como se recoge en "Finding and Fighting the Causes of Insecure Applications" (www.owasp.org/images/d/d6/OWASP\_NY\_Keynote.ppt), si ejecutáramos la totalidad de escáneres de vulnerabilidades existen-



"Finding and Figthing the Causes of Insecure Applications". Jeff Williams

tes en el mercado únicamente detectaríamos el 45 por ciento del total de vulnerabilidades existentes según Common Weakness Enumeration (CWE) (http://cwe.mitre.org).

# Seguridad en los procesos

Otra aproximación errónea a la seguridad consistiría en centrarse en los procesos. De esta forma, la organización puede emplear un tiempo excesivo validando y documentando todas sus actividades, aunque como contrapartida, la rotación de personal no afectaría a la correcta ejecución de los procesos y se reduciría la existencia de personal clave en el proyecto, ya que todos los miembros del equipo tendrían claramente definidas sus actividades.

Por otro lado, basar la seguridad en los miembros del equipo también tiene sus limitaciones. ¿Qué ocurre, por ejemplo, cuando estas personas están de vacaciones o abandonan la organización? ¿Somos capaces de reaccionar de forma efectiva ante una incidencia de seguridad? Todos los miembros del equipo deben conocer nuestras políticas y estándares y ser capaces de seguirlos. Además, debemos ser conscientes de que han de recibir la formación y adquirir los conocimientos adecuados. Aún así, todas las personas somos propensas a cometer errores, por lo que debemos apoyarnos en los procesos y en la tecnología para mitigar estas deficiencias.

El mayor error es pensar que podemos resolver los problemas de seguridad cuando el código se encuentra ya en producción. En este estadio, las auditorías de aplicación son necesarias pero sólo forman una de las múltiples actividades a realizar cuando nuestra intención es la de mejorar el Software Development Lifecycle (SDLC) clásico incluyendo la capa de seguridad en cada una de las etapas, convirtiéndolo en el llamado Secure Software Development Lifecycle (SSDLC).



La raíz del problema es que no entendemos ni tratamos un fallo de seguridad de la misma forma que un problema funcional

Llegado este momento, debemos conocer proyectos como *Comprehensive, Lightweight Application Security Process* (CLASP) (www.owasp.org/images/d/d6/OWASP\_NY\_ Keynote.ppt), uno de los proyectos de documentación de la OWASP, consistente en un conjunto de procesos que pueden (jy deberían!) ser integrados en cualquier proceso de desarrollo de *software* para reforzar e incrementar su nivel de seguridad.

### **Key Application Security Vulnerabilities**



CLASP se adapta perfectamente al proceso de desarrollo que estemos utilizando actualmente, y ha sido diseñado para que podamos integrar fácilmente en él las actividades relacionadas con la seguridad. Además, CLASP ofrece distintos enfoques de forma que todos los miembros del equipo (gestores de proyectos, auditores de seguridad, desarrolladores, arquitectos, etc.) puedan entender y adoptar perfectamente estas actividades en su trabajo habitual.

La raíz del problema con el que nos encontramos actualmente es que no entendemos ni tratamos un fallo de seguridad de la misma forma que un problema funcional. Claro está que esto implica que debemos ser capaces de detectar dichos fallos de se-

guridad, y ello puede no resultar tan obvio como la detección de un problema funcional. Por lo tanto, tenemos que ser exhaustivos en nuestras revisiones y validar los tres factores comentados anteriormente: personas, procesos y tecnología.

El proyecto *Testing Guide* de la OWASP (www.owasp.org/index.php/OWASP\_

Testing\_Project) puede ayudarnos en este sentido. Necesitamos conocer y entender qué causa los problemas de seguridad que sufrimos para adoptar las medidas y controles más adecuados, ya que esto también forma parte de nuestras responsabilidades. Como se cita en esta guía, Denis Verdon (responsable de seguridad en Fidelity National Financial) expresó en la OWASP AppSec 2004 Conference en Nueva York la siguiente analogía: "Si los co-

ches se construyeran como las aplicaciones, los test de seguridad únicamente asumirían impactos frontales. Los coches no serían testados para analizar la estabilidad en maniobras de emergencia, la efectividad de los frenos, impactos laterales o la resistencia al robo".

La pregunta entonces es: ¿qué test de seguridad debo realizar sobre mis aplicaciones? La respuesta la encontramos en la misma guía, que enumera, describe y clasifica los distintos test en ocho grupos grupos: Information Gathering, Business Logic, Authentication, Session Management, Data Validation, DoS, Web

Podemos concluir que, desde el punto de vista de la seguridad en las aplicaciones, el panorama actual no es nada alentador. O sí, ya que tenemos mucho trabajo por hacer y disponemos de los conocimientos, información y medios necesarios para conseguir que, entre todos, un proyecto de desarrollo no acabe generando un producto que se convierta en la principal puerta (trasera) de entrada a nuestra red.

Services y AJAX.