



Desarrollos (inseguros) de 'software': panorama actual

Vicente Aguilera Díaz

OWASP Spain Chapter Leader

Hoy 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)

tra 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 (¡y deberían!) ser integrados en cualquier proceso de desarrollo de *software* para reforzar e incrementar su nivel de seguridad.

Key Application Security Vulnerabilities



OWASP
The Open Web Application Security Project
<http://www.owasp.org>

http://www.owasp.org/index.php/Title=Top_10_2007

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 seguridad, 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 coches 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: *Information Gathering, Business Logic, Authentication, Session Management, Data Validation, DoS, Web Services* y *AJAX*.

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. ☒