



OWASP y las Tendencias en Seguridad de Aplicaciones

OWASP
Capítulo Chile

Juan Carlos Calderon Rojas
Líder proyecto de OWASP
internationalization y Spanish
OWASP
Juan.calderon@owasp.org

Copyright 2010 © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

The OWASP Foundation
<http://www.owasp.org>

¿Cómo estamos?

■ Cyber Crimes Cost Firms \$1 Trillion Annually

McAfee, Unsecured Economies: Protecting Vital Information (2009)

■ The majority of breaches in 2009 (95%) were perpetrated by remote organized criminal groups hacking websites.

WhiteHat Website Security Statistic Report – Fall 2010, 10th Edition

■ 80% of Cyber Crimes Are Preventable

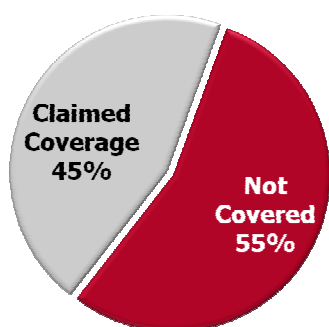
Wired, Senate Panel: 80 Percent of Cyber Attacks Preventable (2009)

¡Advertencia de Salud Pública!



- XSS y CSRF han evolucionado
- Cualquier sitio que visite puede infectar su navegador
- Un navegador infectado puede hacer cualquier cosa que usted puede hacer
- Un navegador infectado puede escanear, infectar, reproducirse
- 70-90% de las aplicaciones son 'portadoras'

Herramientas – 45% en el mejor caso



- MITRE encontró que todos los ofrecimientos de las herramientas de seguridad en aplicaciones juntas solo cubren el 25% de las vulnerabilidades conocidas (mas de 600 de el CWE)
- Encontraron muy poca repetición entre las herramientas, así que para tener el 45% necesaria tenerlas todas (si es que sus ofrecimientos son ciertos)



Que es OWASP?

- "The Open Web Application Security Project (OWASP) is a 501c3 not-forprofit worldwide charitable organization focused on improving the security of application software. Our mission is to make application security visible, so that people and organizations can make informed decisions about true application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license. "



OWASP en Números ...

Fundada en 2001, la comunidad de OWASP en el mundo ha crecido rápidamente: Hay **21,000** personas que están involucradas activamente con OWASP. Hay gente que atiende a las juntas de capítulo, participa en las listas de distribución y tiene cuentas en nuestro wiki. Hay **326** listas de distribución de OWASP (proyectos, comités, eventos y capítulos)

- ★ **7** Comités globales con **39** voluntarios
- ★ **160** Capítulos
- ★ **117** proyectos (Top 10, Guías de pruebas, Guías de desarrollo etc..)
- ★ **17** libros de OWASP
- ★ **18 eventos de 1 o mas días** y conferencias en todo el mundo

OWASP es la mayor base de conocimientos sobre seguridad en aplicaciones en el mundo. Con **6,381** artículos y **76,865** ediciones. **200** actualizaciones diarias de la wiki. Mas de **100,000** paginas visitadas por semana. **32** millones de visitas totales.



Gente

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

Guías de OWASP

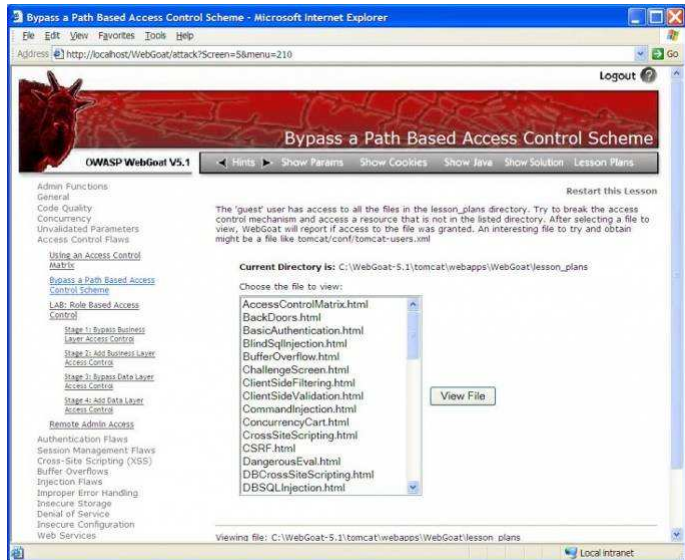
- Libres y de código abierto
- Copias impresas baratas
- Cubre todos los controles críticos
- Cientos de expertos involucrados
- Todos los aspectos de seguridad en aplicaciones



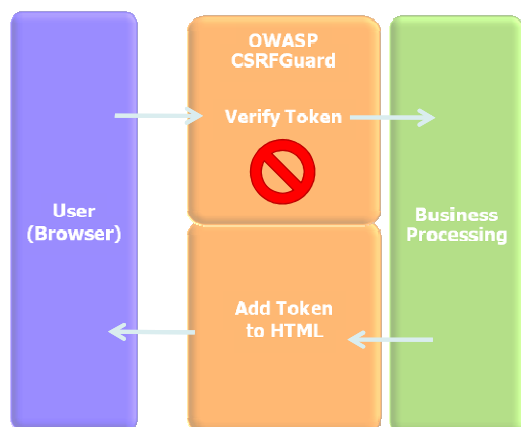
Herramientas



OWASP WebGoat



OWASP CSRFGuard 2.0

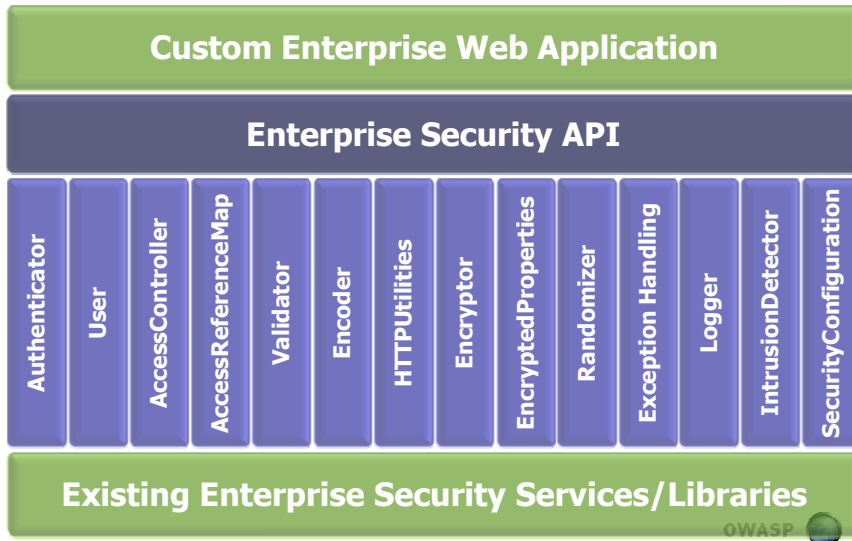


- Adds token to:
 - ▶ href attribute
 - ▶ src attribute
 - ▶ hidden field in all forms

- Actions:
 - ▶ Log
 - ▶ Invalidate
 - ▶ Redirect

<http://www.owasp.org/index.php/CSRFGuard>

The OWASP Enterprise Security API 2.0



Procesos

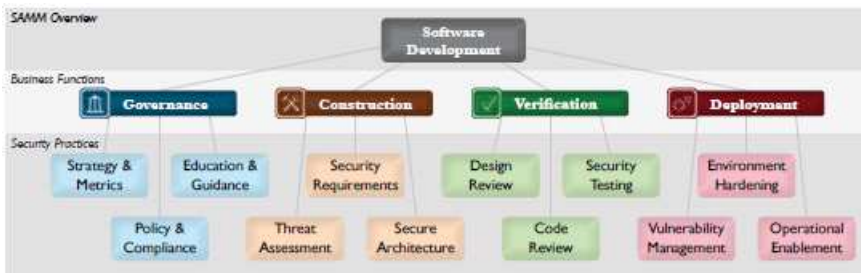
Estándar de OWASP para la verificación de seguridad en aplicaciones

- Estándar para verificar la seguridad de las aplicaciones Web



- Cuatro niveles
 - ▶ Automatizado
 - ▶ Manual
 - ▶ Arquitectura
 - ▶ Interno

Modelo OWASP de Madurez para el Aseguramiento de Software



Hay Muchos Más Proyectos de OWASP

https://www.owasp.org/index.php/Category:OWASP_Project

Category:OWASP Project

An OWASP project is a collection of individuals that have a defined roadmap and team members. OWASP project leaders are responsible for defining the vision, road map, and goals for the project. The project leader also provides the project and its description.

It is a good idea to have a project description that includes the following information:

- Project name and description
- Project goals and objectives
- Project status and progress
- Project team and members
- Project website and resources
- Project contact information

Every project has an associated website. The website of the project, its roadmap, and its description are the OWASP Project Website.

Release/Clarify Projects

Release/Clarify projects are projects that are in the process of being released or clarified. These projects are in the process of being released or clarified and are currently in the process of being released or clarified.

OWASP ASIS Project

OWASP ASIS Project is a project that is currently in the process of being released or clarified.

OWASP ASIS Project

OWASP ASIS Project is a project that is currently in the process of being released or clarified.

OWASP ASIS Project

OWASP ASIS Project is a project that is currently in the process of being released or clarified.

OWASP ASIS Project

OWASP ASIS Project is a project that is currently in the process of being released or clarified.

www.owasp.org (nuestro wiki)

- News
- OWASP Projects
- Downloads
- Local Chapters
- Global Committees
- Associations
- Presentations
- Video
- OWASP Blogs
- OWASP News
- Meeting Lists
- OWASP Wiki
- MemberShip


Bienvenido a OWASP

la comunidad libre y abierta sobre seguridad en aplicaciones

About • For-Admin • Editing • New Article • OWASP Categories

Substans • Recent Changes

El proyecto abierto de seguridad de aplicaciones Web (OWASP) por sus siglas en inglés es una comunidad abierta y libre de nivel mundial enfocada en mejorar la seguridad en las aplicaciones de software. Nuestra misión es ayudar a la seguridad en aplicaciones "abierto", de manera que las organizaciones pueden hacer decisiones informadas sobre los riesgos en la seguridad de aplicaciones. Todo mundo es libre de participar en OWASP, sin importar sus antecedentes o experiencia. Si quieres ser parte de nuestra libre y abierta Fundación OWASP, es una organización sin ánimo de lucro 501(c)3 que asegura la disponibilidad a largo plazo de nuestro trabajo.



Encuentra más sobre OWASP aquí en nuestro Wiki. Por favor, si tienes ideas para hacer cambios y mejorar nuestro sitio. Hay cientos de personas en todo el mundo que ven los cambios al sitio para ayudar a mejorar la calidad del contenido. Si es nuevo, puedes hacer nuestra lista de distribución. Sus preguntas y comentarios deben ser enviados a info@owasp.org. Si la gente lo que ve aquí y quiere apoyar nuestros esfuerzos, por favor contáctenos **convirtiendo en un miembro**.

OWASP Foundation has over 100 Local Chapters all meetings are FREE simply sign up on the appropriate mailing list and introduce yourself. All chapter and visiting lists can be found here.

2010 Annual Report - Click Here

Citations - Click Here

Supporters - Click Here

Podcast - Listen Now

Blog - Click Here

Twitter - Follow

Periodicos OWASP

Los periódicos OWASP reportan eventos, proyectos, gente, mantenimiento, actualizaciones del Wiki y más sobre noticias de seguridad en aplicaciones en OWASP.

Fondos de investigación sobre seguridad en aplicaciones de OWASP

Los fondos de OWASP promueven a los investigadores de seguridad en aplicaciones con proyectos de fondos para herramientas, guías, encuestas y mucho más. La membresía va directamente a la financiación de estos proyectos. Por favor, vea la página de conexiones OWASP para saber cómo emitir una propuesta de conexión.

Inicio un Proyecto

Conexiones

Talento de Trabajo



Relevancia

Algunas Referencias a Materiales de OWASP

- Consejo de seguridad de PCI. Requerimiento 6.6 PCI-DSS
- Metricas de "CIS Security"
- Clouds Security Alliance.
- Agencia de sistemas de información de la defensa (DISA) USA, Application Security Checklist
- Agencia Europea de redes de seguridad de la información (ENISA) Cloud computing Risk Assessment
- GovCert UK
- Ministerio de ecología y energía de Francia. Guía de desarrollo para PHP
- Instituto Nacional de Estándares de tecnología (NIST) USA
 - ▶ Framework and roadmap for Smart Grids Interoperability Standards
 - ▶ Smart Grid Cyber Security Strategy and Requirements

Aun no está listado?



Universidades apoyando a OWASP



¿Que ofrece OWASP?

- ▶ Difusión y Capacitación por medio de capítulos locales
 - Charlas públicas y cursos privados sobre seguridad en aplicaciones en todos los niveles
- ▶ Desarrollo de nuevos proyectos
 - Posibilidad de utilizar las herramientas y colaboradores disponibles para generar nuevos proyectos
- ▶ Becas de Investigación
 - OWASP otorga becas a investigadores de la seguridad en aplicaciones para desarrollar herramientas, guías, publicaciones, etc.

Mas de \$100,000 USD han sido otorgados al día de hoy en becas de investigación

¿Como puedo participar siendo una universidad o centro educativo?

- ▶ Las universidades y centros educativos que apoyan a OWASP cuentan con los siguientes beneficios:
 - Aumentar la visibilidad de la universidad en todo el mundo
 - OWASP y la Universidad pueden conjuntamente organizar eventos que proporcionen a los estudiantes financiamiento para realizar investigaciones basadas en la seguridad de aplicaciones
 - OWASP y la Universidad pueden colaborar en la organización de seminarios para proporcionar sesiones de capacitación para estudiantes en herramientas OWASP, documentación y conocimientos de seguridad.
 - **SIN COSTO!**

Nota: Esto apunta a que la Universidad en su conjunto se involucre con OWASP. Esto no implica la membresía individual u organizacional de los estudiantes y/o profesores de la Universidad. Sin embargo, se invita a todos los estudiantes y profesores a explorar los beneficios de convertirse en un miembro OWASP.

¿Como puedo participar siendo una individuo o institución privada o pública?

- ▶ Únase al capítulo de OWASP Chile
- ▶ Patrocine las reuniones del capítulo
- ▶ Fomente los materiales y herramientas de OWASP en su empresa o institución
- ▶ Hágase miembro de OWASP
 - Individual
 - Corporativa
- ▶ Forme parte de un proyecto de OWASP (el de Español es un muy buen comienzo)

Preguntas Frecuentes

- ¿Compite OWASP con la asociación ABC o XYZ?
- ¿Tiene OWASP una Certificación?
- Tengo una gran idea para un proyecto de OWASP...
- ¿Qué necesito para formar parte del capítulo de OWASP en Chile?
- ¿Cómo puedo yo o mi compañía participar?

Reconocimientos

■ Materiales de OWASP publicados por las siguientes personas han sido referidos o incluidos en esta presentación

- ▶ Jeff Williams
- ▶ Tom Brennan
- ▶ Fabio Cerullo
- ▶ Sebastien Deleersnyder
- ▶ Dinis Cruz
- ▶ Jason Li