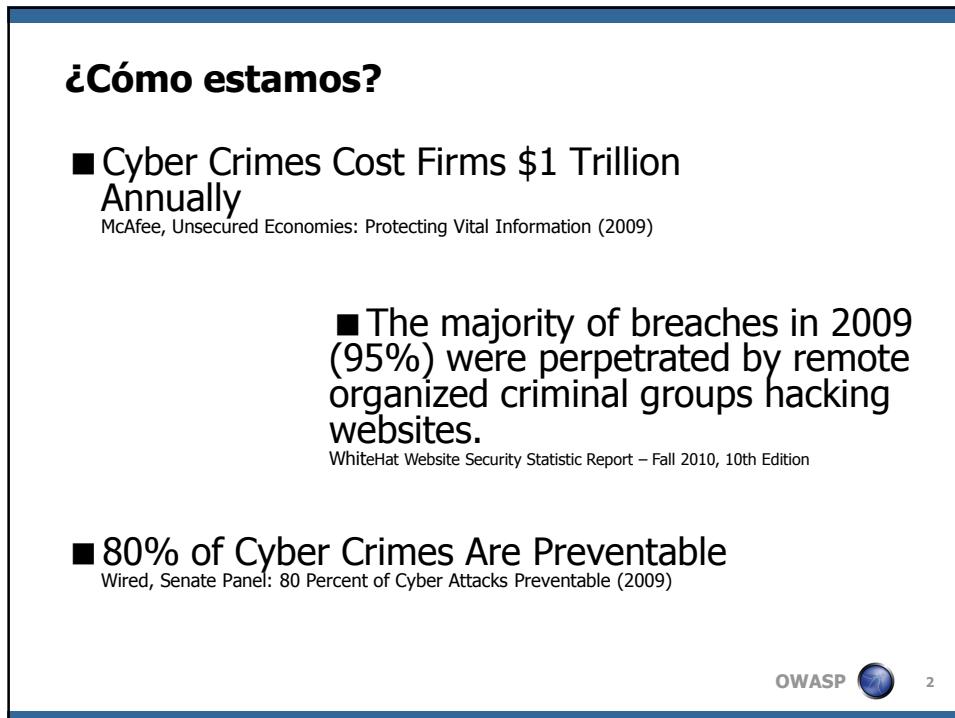




The slide features a blue header bar at the top. Below it is a decorative graphic with a blue and green grid pattern. In the center, there's a circular logo with a stylized figure. To the right of the logo, the title "OWASP y las Tendencias en Seguridad de Aplicaciones" is displayed in bold black text. Below the title, the name "Juan Carlos Calderon Rojas" and his role "Líder proyecto de OWASP internationalization y Spanish OWASP" are listed, along with his email address "Juan.calderon@owasp.org". At the bottom of the slide, a copyright notice from The OWASP Foundation is present, followed by the text "The OWASP Foundation" and the website "http://www.owasp.org".



The slide has a white background with a blue header bar at the top. The main heading is "¿Cómo estamos?". Below it, there are three bullet points with supporting text:

- 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)

In the bottom right corner, there's a small OWASP logo and the number "2".

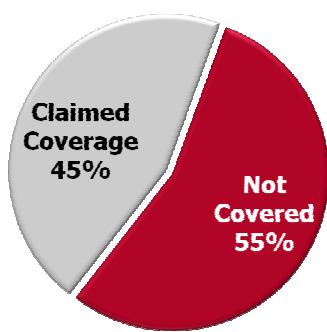
iAdvertencia de Salud Pública!



- 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'

OWASP  3

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% necesitaría tenerlas todas (si es que sus ofrecimientos son ciertos)

OWASP  4

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  5

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.

OWASP  6



Gente

OWASP  7

Key Application Security Vulnerabilities

A1: Cross Site Scripting (XSS)	A2: Injection Flaws	A3: Malicious File Execution	A4: Insecure Direct Object Reference
A5: Cross Site Request Forgery (CSRF)	A6: Information Leakage and Improper Error Handling	A7: Broken Authentication and Session Management	A8: Insecure Cryptographic Storage
A9: Insecure Communications	A10: Failure to Restrict URL Access		

 OWASP
The Open Web Application Security Project
http://www.owasp.org/index.php?title=Top_10_2007

OWASP  8

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



OWASP 9



Herramientas



OWASP 10

OWASP WebGoat

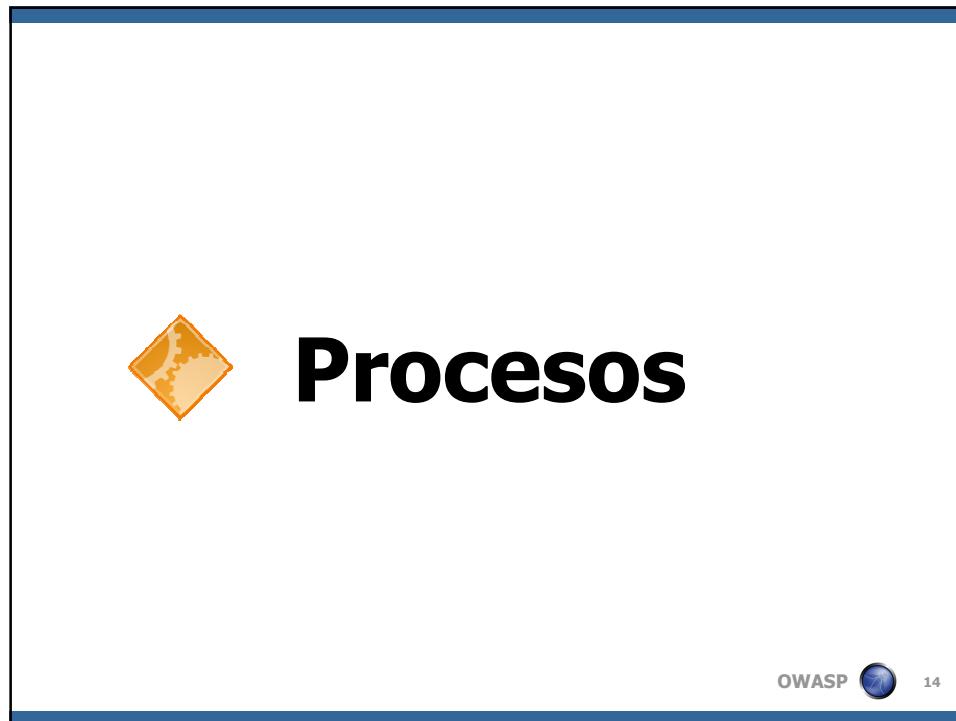
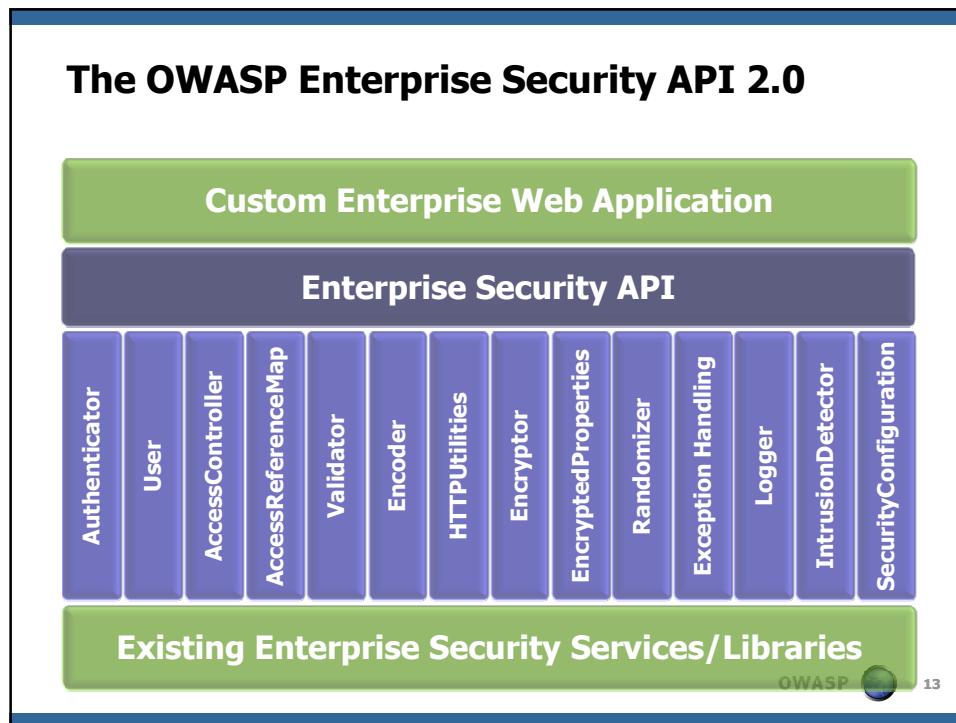
The screenshot shows a Microsoft Internet Explorer window displaying the OWASP WebGoat V5.1 interface. The title bar reads "Bypass a Path Based Access Control Scheme - Microsoft Internet Explorer". The main content area is titled "Bypass a Path Based Access Control Scheme". A sidebar on the left lists various security categories and stages. The central area contains a file selection dialog box with a list of files from the "lesson_plans" directory, including "AccessControlMatrix.html", "BackDoors.html", etc. A "View File" button is visible at the bottom of the list.

OWASP CSRFGuard 2.0

The diagram illustrates the OWASP CSRFGuard 2.0 architecture. It consists of three main components: "User (Browser)" (purple), "OWASP CSRFGuard" (orange), and "Business Processing" (green). The "User (Browser)" component interacts with the "OWASP CSRFGuard" component, which contains two stacked boxes: "Verify Token" (top) and "Add Token to HTML" (bottom). Arrows show the flow from the User to the Verify Token step, then to the Business Processing step, and finally back to the User from the Add Token to HTML step. To the right of the diagram, two bulleted sections describe the functionality:

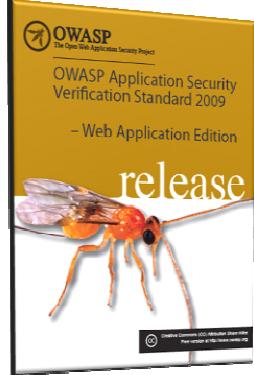
- Adds token to:
 - ▶ href attribute
 - ▶ src attribute
 - ▶ hidden field in all forms
- Actions:
 - ▶ Log
 - ▶ Invalidate
 - ▶ Redirect

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



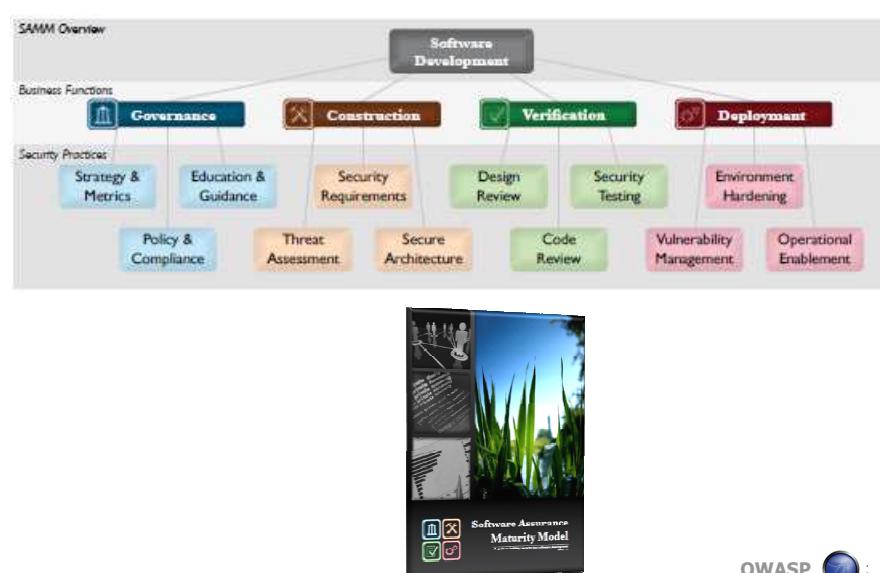
Estándar de OWASP para la verificación de seguridad en aplicaciones

- Estándar para verificar la seguridad de las aplicaciones Web
- Cuatro niveles
 - ▶ Automatizado
 - ▶ Manual
 - ▶ Arquitectura
 - ▶ Interno



OWASP : 15

Modelo OWASP de Madurez para el Aseguramiento de Software



Software Development

SAMM Overview

Business Functions

- Governance
- Construction
- Verification
- Deployment

Security Practices

- Strategy & Metrics
- Education & Guidance
- Threat Assessment
- Secure Architecture
- Design Review
- Code Review
- Security Testing
- Vulnerability Management
- Environment Hardening
- Operational Enablement

OWASP : 16



Relevancia

OWASP  19

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

OWASP  20

Aun no está listado?

OWASP  21

Universidades apoyando a OWASP

OWASP  22

¿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