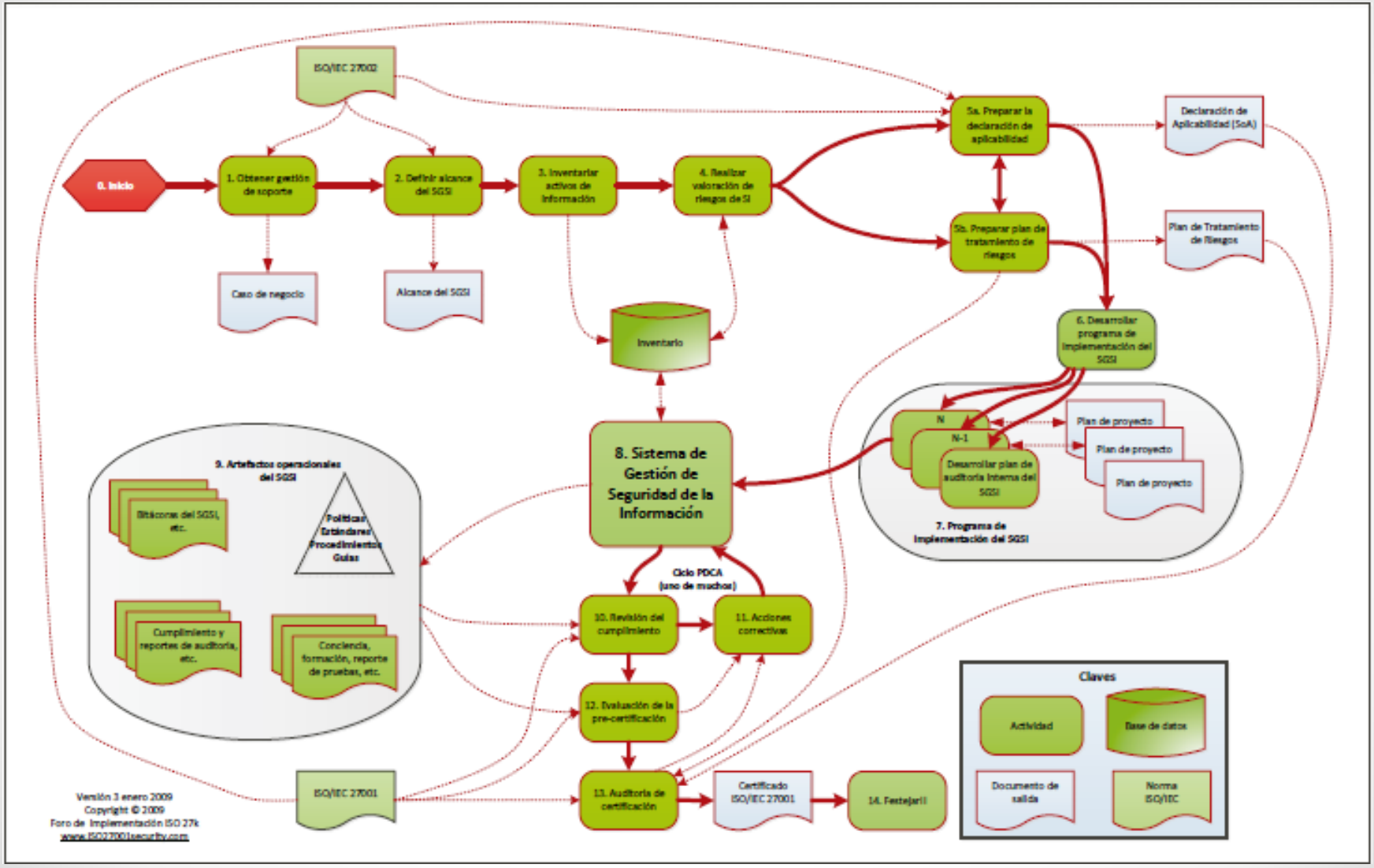
Riesgos de Seguridad Web OWASP Top 10

Rommel Macas
CID Secure

CIDSECURE
seguridad de la información

Seguridad !!



CIDSECURE
seguridad de la información

Por qué Asegurar mi entorno Web

- Mayores Niveles de Riesgo
  - Amenazas
  - Vulnerabilidades

Riesgos

Apple, última víctima de ola de ciberataques a tecnológicas de EU

A+ A- Síguenos en:

Nota

Los hackers parece
de tecnología. AR

recientes a firm

"El malware (so
de un sitio web

"Hemos identificado un pequeño número de sistemas de Apple que estaban infectados y los aislamos de nuestra red".

El software malicioso se aprovechó de una vulnerabilidad en el programa Java utilizado como "plug-in" para los programas de navegación web.

Consejo Electoral de Ecuador revela intento de entrar en sistema informático

A+ A- Síguenos en:

Nota Fotogalería

América Latina | Piratería | Hackers | Elecciones en Ecuador

la electoral en

policía para atrapar a
parecen estar
aques cibernéticos

y se extendió a través
uesta a una consulta.

- Domingo Paredes, presidente del consejo informa la alarmante situación

El Consejo Nacional Electoral del país sudamericano asegura que hubo un intento para penetrar sus datos electorales

QUITO, ECUADOR (17/FEB/2013).- El presidente del Consejo Nacional Electoral (CNE) de Ecuador, Domingo Paredes, reveló hoy que esa entidad detectó un intento de penetración en su sistema informático, mientras los ecuatorianos acuden a las urnas para elegir Presidente, Vicepresidente y legisladores.

"No podría dar más detalles, eso está bajo investigación", dijo Paredes a Efe al apuntar que, en todo caso, están demostrando "que hay control de la situación" y que el software desarrollado es "altamente seguro".

Twitter revela un ataque informático que afectó a 250.000 usuarios

Feb 2, 2013 | Cinco Días

Me gusta Sé el primero de tus amigos al que le gusta esto. Compartir

"Descubrimos un ataque en marcha y fuimos capaces de frenarlo pocos momentos después (...) Este ataque no era el trabajo de amateurs, y no creemos que haya sido un incidente aislado", explicó en una entrada de su blog de Twitter, Bob Lord, director de seguridad de la compañía. Lord agregó que "los atacantes eran extremadamente sofisticados, y creemos que otras compañías y organizaciones también han sido atacados recientemente.

Entre la información captada, figuran nombres de usuarios, cuentas de correo y contraseñas cifrados. "Aunque solo un porcentaje pequeño usuarios ha sido potencialmente afectado, animamos a los usuarios a fortalecer sus claves y contraseñas", señaló Lord, quien recomendó mezclar en las contraseñas números, letras y otros iconos.

Riesgos

Ciberespías se infiltran en los sistemas del banco central de Australia

Gabriela Villarreal | 11.03.2013 21:02 MSK | Comentar

Se ha descubierto que los sistemas del Banco de Reserva de Australia (Reserve Bank of Australia), el banco central de este país, han
re los planes económicos

Un camaleón virtual roba millones de dólares a empresas publicitarias

Gabriela Villarreal | 21.03.2013 13:55 MSK | Comentar

Se ha descubierto una red zombi diseñada para pulsar en anuncios publicitarios de Internet. Esto causa serios daños económicos a las agencias publicitarias, costándoles hasta 6 millones de dólares por mes.

La empresa de seguridad Spider.io anunció el descubrimiento de la red zombi, llamada Chamaleon. Se estima que Chamaleon ha infectado "por lo menos" 120.000 equipos, el 95% de los cuales se encuentra en los Estados Unidos. También se ha detectado la amenaza en 202 sitios web.

La red zombi está especialmente diseñada para actuar como si un humano estuviera visitando los sitios web y pulsando en los avisos. Como las empresas publicitarias deben pagar al sitio web cada vez que alguien pulsa en sus avisos, este ataque roba dinero a las empresas y enriquece a los sitios web afectados.

Los bots visitan el mismo grupo de sitios web, con pocas variaciones. "Es difícil imaginar por qué alguien soltaría este tipo de red zombi en 202 sitios web sin tener la intención de cometer fraude publicitario", dijeron los especialistas de Spider.io. "Por desgracia, no podemos definir con certeza quién está detrás de esto. Hasta podría ser un individuo dentro de una compañía, haciéndolo sin el conocimiento de sus colegas o jefes", explicaron los expertos.

Este tipo de ataques no es común porque requiere un nivel de complejidad avanzado. En este caso, todos los bots se hacen pasar por Internet Explorer 9 funcionando en Windows 7, tienen patrones de click aleatorios y utilizan Flash y JavaScript para "humanizar" su actividad.

lectar información
En aquel entonces, se
omía.

on a ejecutivos del banco,
ue supuestamente
y título eran posibles",

mido que contenía el
s de spam porque no

sponsable de los
erno chino, por supuesto,

¿Preguntas?

- ¿Cuánto cuesta realmente una empresa cuando su servidor web es atacado?
- ¿Qué pasa si se interrumpe la disponibilidad de los sistemas críticos Web?
- ¿Cuáles son los costos asociados a un hackeo o robo de información propietaria?
- ¿Qué gana nuestro competidor desde un servidor web no seguro?

¿Qué es un riesgo?

- Es la probabilidad o posibilidad de que ocurra un acontecimiento indeseado o se realice una acción no deseada de modo que afecte negativamente a la organización, a sus activos y/o a la consecución de sus fines, objetivos y resultados.

¿Qué necesito saber para identificar riesgos?

- Valor del Activo * Probabilidad de Ocurrencia * Impacto = Riesgo

- Determinar Activos
- Identificar Vulnerabilidades
- Determinar Amenazas
- Probabilidad de Ocurrencia
- Impacto

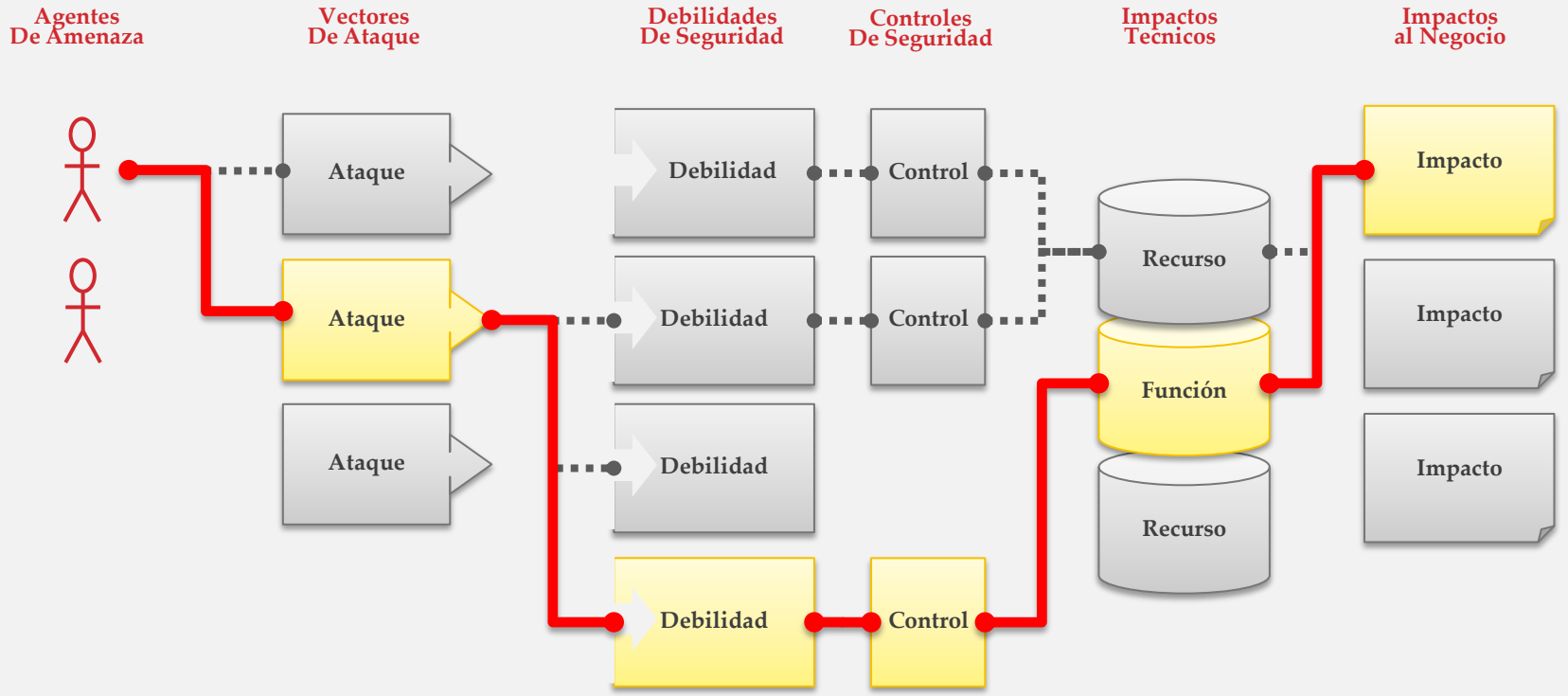
Riesgos de Seguridad

- Atentar con:

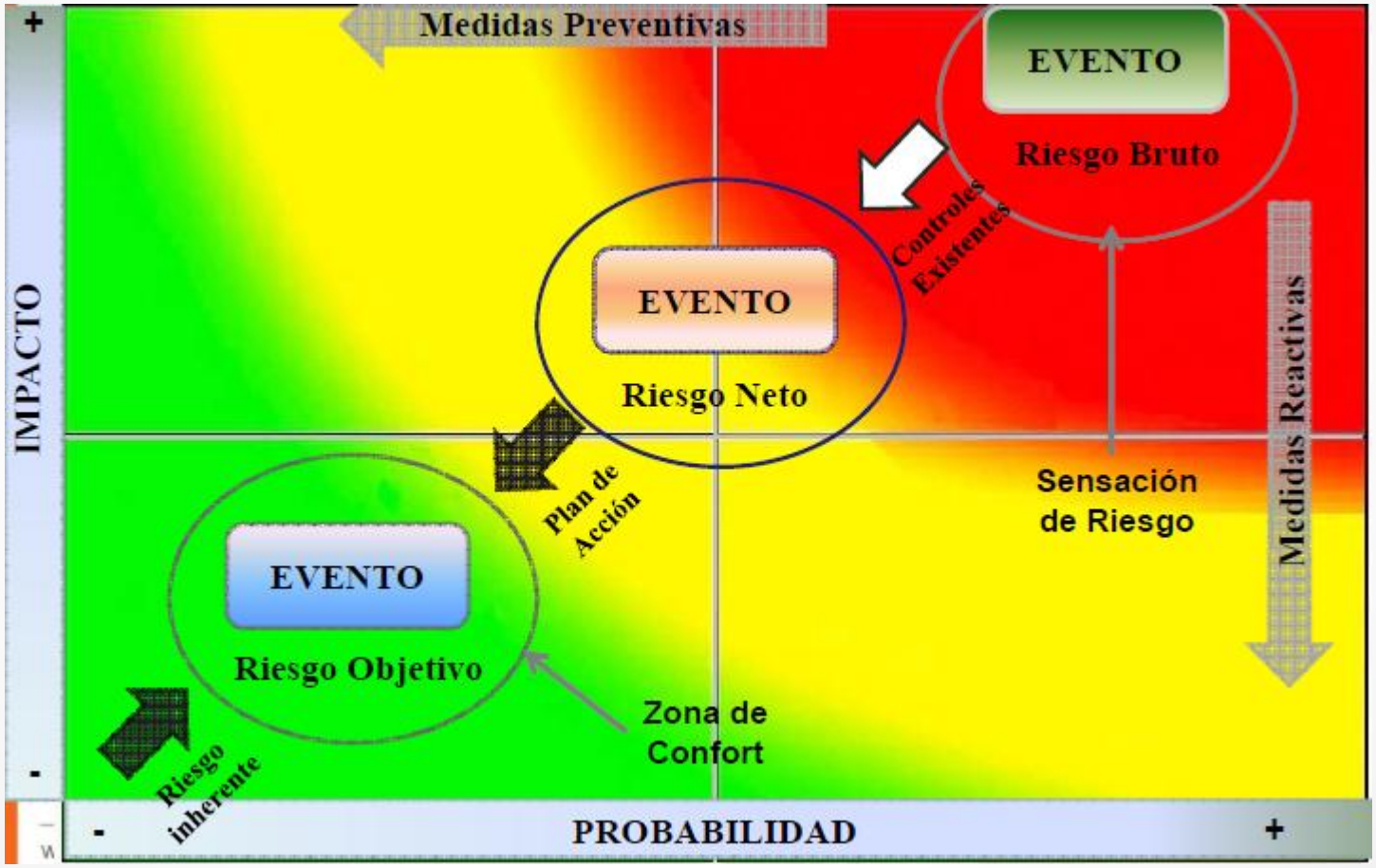
- Confidencialidad
- Integridad
- Disponibilidad

¿Qué son los riesgos de seguridad en aplicaciones?

Los atacantes pueden potencialmente usar muchas diferentes rutas a través de su aplicación para causar daño en su negocio u organización. Cada una de estas rutas representa un riesgo que puede, o no, ser lo suficientemente serio como para merecer atención.



Mapa de Riesgos




SÍ, CLARO QUE ESCUCHÉ DE LOS HACKERS... SON PERSONAS QUE A TRAVÉS DE LA RED SE PUEDEN METER EN TU COMPUTADORA

¿Realidad?

¿Qué hacer?

• • •

OWASP

CIDSECURE
seguridad de la información

OWASP

- Open Web Application Security Project
  - Sin fines de lucro, organización de voluntarios
    - Todos los miembros son voluntarios
    - Todo el trabajo es donado por los patrocinadores
  - Proporcionar recursos gratuitos para la comunidad
    - Publicaciones, artículos, normas
    - Software de Testeo y Capacitación
    - Capítulos locales & Listas de correo
  - Soportada a través de patrocinios
    - Apoyo financiero a través de empresas o patrocinadores
    - Patrocinios personales de los miembros

OWASP TOP 10

OWASP Top 10 – 2007 (Previo)	OWASP Top 10 – 2010 (Nuevo)
A2 – Fallas de inyección	A1 – Inyección
A1 – Secuencia de Comandos en Sitios Cruzados (XSS)	A2 – Secuencia de Comandos en Sitios Cruzados (XSS)
A7 – Pérdida de Autenticación y Gestión de Sesiones	A3 – Pérdida de Autenticación y Gestión de Sesiones
A4 – Referencia Directa Insegura a Objetos	A4 – Referencia Directa Insegura a Objetos
A5 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	A5 – Falsificación de Peticiones en Sitios Cruzados (CSRF)
<T10 2004 A10 – Administración Insegura de Configuración>	A6 – Defectuosa Configuración de Seguridad (NUEVO)
A8 – Almacenamiento Criptográfico Inseguro	A7 – Almacenamiento Criptográfico Inseguro
A10 – Falla de Restricción de Acceso a URL	A8 – Falla de Restricción de Acceso a URL
A9 – Comunicaciones Inseguras	A9 – Protección Insuficiente en la Capa de Transporte
<no disponible en T10 2007>	A10 – Redirecciones y reenvíos no validados (NUEVO)
A3 – Ejecución Maliciosa de Ficheros	<removido del T10 2010>
A6 – Filtrado de Información y Manejo Inapropiado de Errores	<removido del T10 2010>

OWASP TOP 10 2013 RC1

OWASP Top 10 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	A5 – Security Misconfiguration
A7 – Insecure Cryptographic Storage – Merged with A9 →	A6 – Sensitive Data Exposure
A8 – Failure to Restrict URL Access – Broadened into →	A7 – Missing Function Level Access Control
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<buried in A6: Security Misconfiguration>	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	Merged with 2010-A7 into new 2013-A6

Riesgos de Seguridad Web – OWASP Top 10

A1 – Inyección	• Las fallas de inyección, tales como SQL, OS, y LDAP, ocurren cuando datos no confiables son enviados a un interprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al interprete en ejecutar comandos no intencionados o acceder datos no autorizados.
A2 – Secuencia de comandos en sitios cruzados (XSS)	• Las fallas XSS ocurren cada vez que una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada. XSS permite a los atacantes ejecutar secuencia de comandos en el navegador de la victima los cuales pueden secuestrar las sesiones de usuario, destruir sitios web, o dirigir al usuario hacia un sitio malicioso.
A3 – Pérdida de Autenticación y Gestión de Sesiones	• Las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son frecuentemente implementadas incorrectamente, permitiendo a los atacantes comprometer contraseñas, llaves, token de sesiones, o explotar otras fallas de implementación para asumir la identidad de otros usuarios.

Riesgos de Seguridad Web – OWASP Top 10

A4 – Referencia Directa Insegura a Objetos	• Una referencia directa a objetos ocurre cuando un desarrollador expone una referencia a un objeto de implementación interno, tal como un fichero, directorio, o base de datos. Sin un chequeo de control de acceso u otra protección, los atacantes pueden manipular estas referencias para acceder datos no autorizados.
A5 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	• Un ataque CSRF obliga al navegador de una victima autenticada a enviar una petición HTTP falsificado, incluyendo la sesión del usuario y cualquier otra información de autenticación incluida automáticamente, a una aplicación web vulnerable. Esto permite al atacante forzar al navegador de la victima para generar pedidos que la aplicación vulnerable piensa son peticiones legítimas provenientes de la victima.
A6 – Defectuosa configuración de seguridad	• Una buena seguridad requiere tener definida e implementada una configuración segura para la aplicación, marcos de trabajo, servidor de aplicación, servidor web, base de datos, y plataforma. Todas estas configuraciones deben ser definidas, implementadas, y mantenidas ya que por lo general no son seguras por defecto. Esto incluye mantener todo el software actualizado, incluidas las librerías de código utilizadas por la aplicación.

Riesgos de Seguridad Web – OWASP Top 10

A7 – Almacenamiento Criptográfico Inseguro	• Muchas aplicaciones web no protegen adecuadamente los datos sensibles, tales como tarjetas de crédito, NSSs, y credenciales de autenticación con mecanismos de cifrado o hashing. Atacantes pueden modificar o robar tales datos protegidos inadecuadamente para conducir robos de identidad, fraudes de tarjeta de crédito u otros crímenes.
A8 - Falla de Restricción de Acceso a URL	• Muchas aplicaciones web verifican los privilegios de acceso a URLs antes de generar enlaces o botones protegidos. Sin embargo, las aplicaciones necesitan realizar controles similares cada vez que estas páginas son accedidas, o los atacantes podrán falsificar URLs para acceder a estas páginas igualmente.

Riesgos de Seguridad Web – OWASP Top 10

A9 – Protección Insuficiente en la capa de Transporte	• Las aplicaciones frecuentemente fallan al autenticar, cifrar, y proteger la confidencialidad e integridad de tráfico de red sensible. Cuando esto ocurre, es debido a la utilización de algoritmos débiles, certificados expirados, inválidos, o sencillamente no utilizados correctamente.
A10 – Redirecciones y Reenvíos no validados	• Las aplicaciones web frecuentemente redirigen y reenvían a los usuarios hacia otras páginas o sitios web, y utilizan datos no confiables para determinar la página de destino. Sin una validación apropiada, los atacantes pueden redirigir a las víctimas hacia sitios de phishing o malware, o utilizar reenvíos para acceder páginas no autorizadas.

Resumen General

RIESGO	Agentes De Amenaza	Vectores de Ataque	Vulnerabilidades de Seguridad		Impactos Técnicos	Impactos al Negocio
		Explotación	Prevalencia	Detección	Impacto	
A1-Inyeccion		FACIL	COMUN	MEDIA	SEVERO	
A2-XSS		MEDIA	MUY DIFUNDIDA	FACIL	MOERADO	
A3-Autent'n		MEDIA	COMUN	MEDIA	SEVERO	
A4-DOR		FACIL	COMUN	FACIL	MODERADO	
A5-CSRF		MEDIA	MUY COMUN	FACIL	MODERADO	
A6-Config		FACIL	COMUN	FACIL	MODERADO	
A7-Crypto		DIFICIL	POCO COMUN	DIFICIL	SEVERO	
A8-Accesso URL		FACIL	POCO COMUN	MEDIA	MODERADO	
A9-Transporte		DIFICIL	COMUN	FACIL	MODERADO	
A10-Redirects		MEDIA	POCO COMUN	FACIL	MODERADO	

Otros Riesgos

- Clickjacking (técnica de ataque recién descubierta en el 2.008)
- Denegación de servicio (estuvo en el Top 10 del 2.004 – Entrada A9)
- Ejecución de archivos maliciosos (estuvo en el Top 10 del 2.007 – Entrada A3)
- Falta de detección y respuesta a las intromisiones
- Fallas de concurrencia
- Filtración de información y Manejo inapropiado de errores (fue parte del Top 10 del 2.007 – Entrada A6)
- Registro y responsabilidad insuficientes (relacionado al Top 10 del 2.007 – Entrada A6)

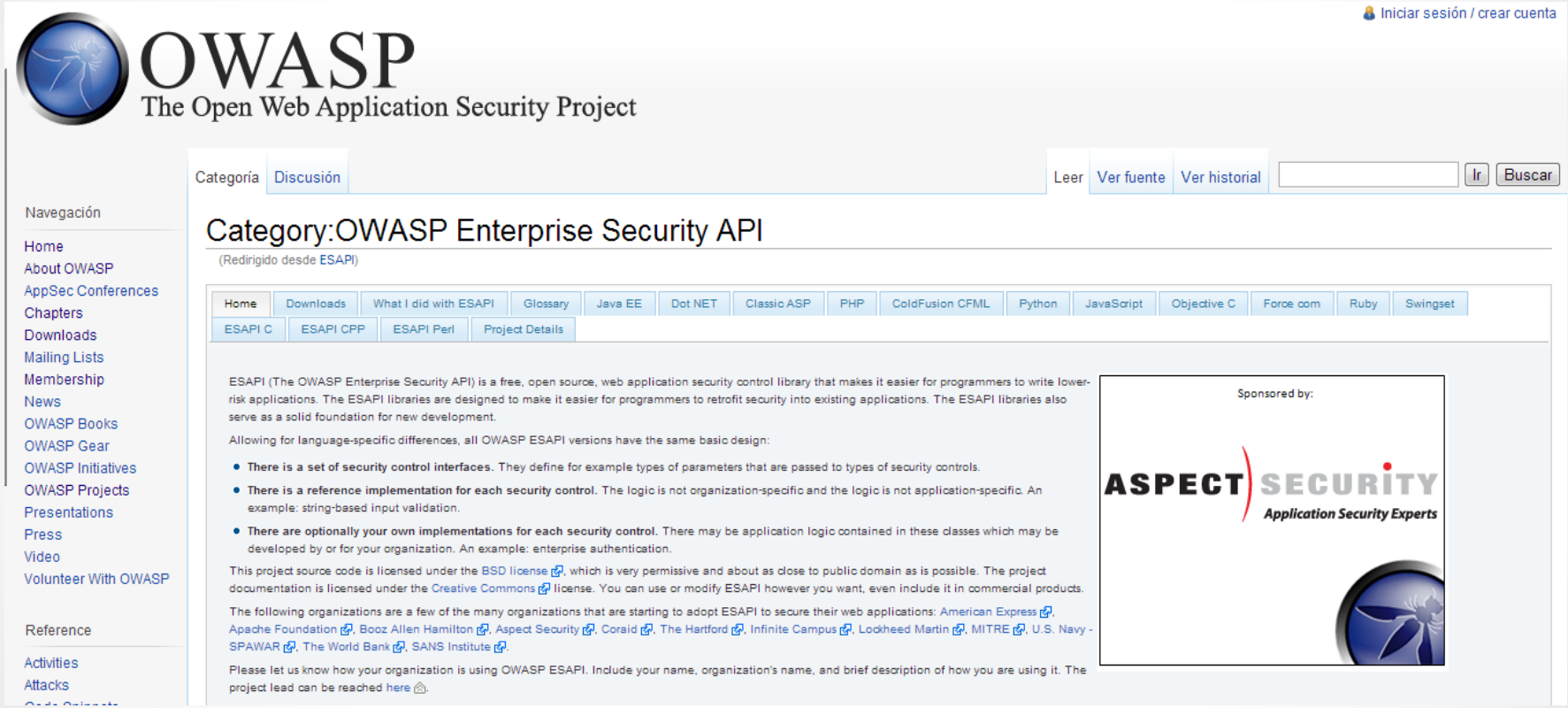
Recomendacioes

• • •

Proyectos OWASP

CIDSECURE
seguridad de la información

ESAPI



Iniciar sesión / crear cuenta

OWASP
The Open Web Application Security Project

Categoría | Discusión | Leer | Ver fuente | Ver historial | Ir | Buscar

Navegación

- Home
- About OWASP
- AppSec Conferences
- Chapters
- Downloads
- Mailing Lists
- Membership
- News
- OWASP Books
- OWASP Gear
- OWASP Initiatives
- OWASP Projects
- Presentations
- Press
- Video
- Volunteer With OWASP

Reference

- Activities
- Attacks

Category:OWASP Enterprise Security API

(Redirigido desde ESAPI)

Home | Downloads | What I did with ESAPI | Glossary | Java EE | Dot NET | Classic ASP | PHP | ColdFusion CFML | Python | JavaScript | Objective C | Force com | Ruby | Swingset | ESAPI C | ESAPI CPP | ESAPI Perl | Project Details

ESAPI (The OWASP Enterprise Security API) is a free, open source, web application security control library that makes it easier for programmers to write lower-risk applications. The ESAPI libraries are designed to make it easier for programmers to retrofit security into existing applications. The ESAPI libraries also serve as a solid foundation for new development.

Allowing for language-specific differences, all OWASP ESAPI versions have the same basic design:

- **There is a set of security control interfaces.** They define for example types of parameters that are passed to types of security controls.
- **There is a reference implementation for each security control.** The logic is not organization-specific and the logic is not application-specific. An example: string-based input validation.
- **There are optionally your own implementations for each security control.** There may be application logic contained in these classes which may be developed by or for your organization. An example: enterprise authentication.

This project source code is licensed under the BSD license, which is very permissive and about as close to public domain as is possible. The project documentation is licensed under the Creative Commons license. You can use or modify ESAPI however you want, even include it in commercial products.

The following organizations are a few of the many organizations that are starting to adopt ESAPI to secure their web applications: American Express, Apache Foundation, Booz Allen Hamilton, Aspect Security, Coraid, The Hartford, Infinite Campus, Lockheed Martin, MITRE, U.S. Navy - SPAWAR, The World Bank, SANS Institute.

Please let us know how your organization is using OWASP ESAPI. Include your name, organization's name, and brief description of how you are using it. The project lead can be reached here.

Sponsored by:

ASPECT SECURITY
Application Security Experts

XSS (Cross Site Scripting) Prevention Cheat Sheet

The following snippets of HTML demonstrate how to safely render untrusted data in a variety of different contexts.

Data Type	Context	Code Sample	Defense
String	HTML Body	UNTRUSTED DATA	• HTML Entity Encoding
String	Safe HTML Attributes	<input type="text" name="fname" value="UNTRUSTED DATA">	• Aggressive HTML Entity Encoding • Only place untrusted data into a whitelist of safe attributes (listed below). • Strictly validate unsafe attributes such as background, id and name.
String	GET Parameter	clickme	• URL Encoding
String	Untrusted URL in a SRC or HREF attribute	clickme <iframe src="UNTRUSTED URL" />	• Cannonicalize input • URL Validation • Safe URL verification • Whitelist http and https URL's only (Avoid the JavaScript Protocol to Open a new Window) • Attribute encoder
String	CSS Value	Selection	• Strict structural validation • CSS Hex encoding • Good design of CSS Features
String	JavaScript Variable	<script>var currentValue='UNTRUSTED DATA';</script> <script>someFunction('UNTRUSTED DATA');</script>	• Ensure JavaScript variables are quoted • JavaScript Hex Encoding • JavaScript Unicode Encoding • Avoid backslash encoding (\" or \' or \\)
HTML	HTML Body	UNTRUSTED HTML	• HTML Validation (JSoup, AntiSamy, HTML Sanitizer)
String	DOM XSS	<script>document.write("UNTRUSTED INPUT: " + document.location.hash);<script/>	• DOM based XSS Prevention Cheat Sheet

Preguntas??

Rommel Macas
rlmacas@cidsecure.com
@rlmacas

CIDSECURE
seguridad de la información