



OWASP Day Costa Rica

En contra de la delincuencia
Cibernética



OWASP

The Open Web Application Security Project

Michael Hidalgo

michael.hidalgo@owasp.org

Chapter Leader OWASP Costa Rica

Colaborador OWASP O2 Platform Project

Acerca de Mi



OWASP

The Open Web Application Security Project

- Software Developer Engineer en

Fiserv, Digital Channels- Corillian Online ASP team.

- Desarrollador de Software para Instituciones Financieras.
- Web Services, Análisis estático de Código (a.k.a SAST)

- Líder del Capítulo OWASP Costa Rica

- Participación OData Protocol (REST)

- Contribuyente en Proyectos OWASP

- OWASP O2 Platform (*Dinis Cruz*)
- REST Security Cheat Sheet (*Jim Manico*)



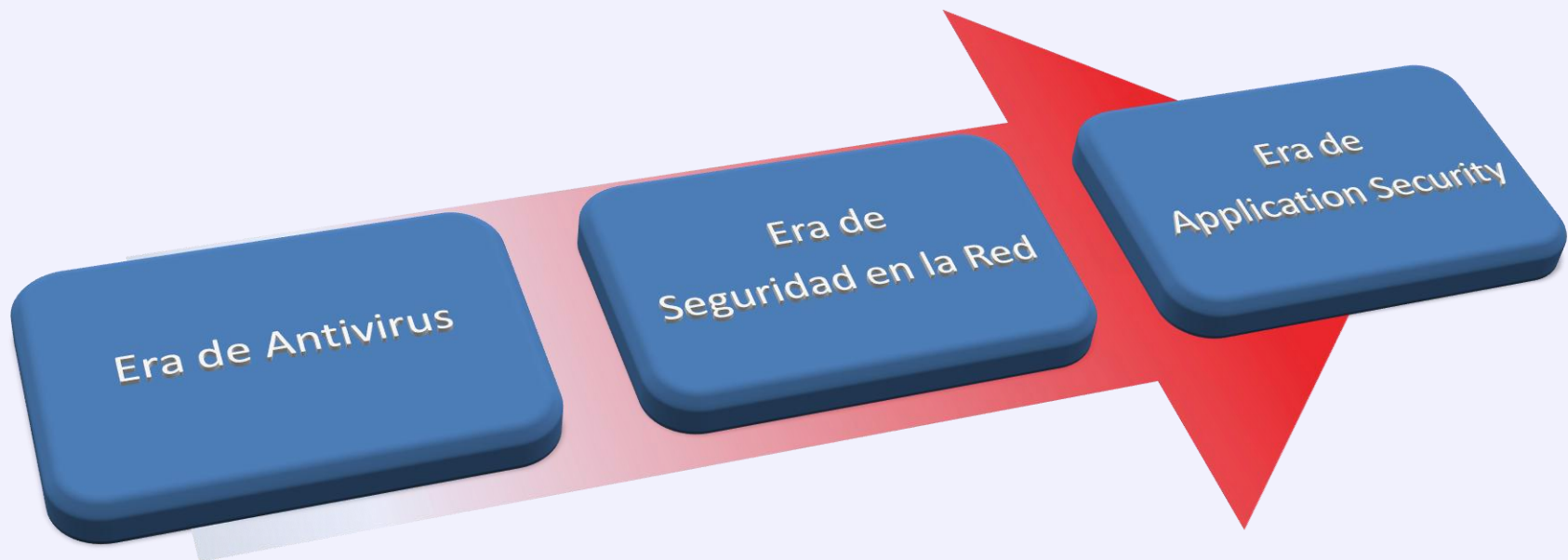
¿Porqué ésta presentación?



OWASP

The Open Web Application Security Project

Vivimos en un mundo digital, un mundo conectado!



- ❖ La mayoría de los sitios Web son vulnerables a ataques.
- ❖ 75% de los ataques ocurren en la capa de aplicación(*Source: Gartner*).
- ❖ Importante % de negocios basados en la Web(*Servicios, Tiendas virtuales, cuidado personal*).

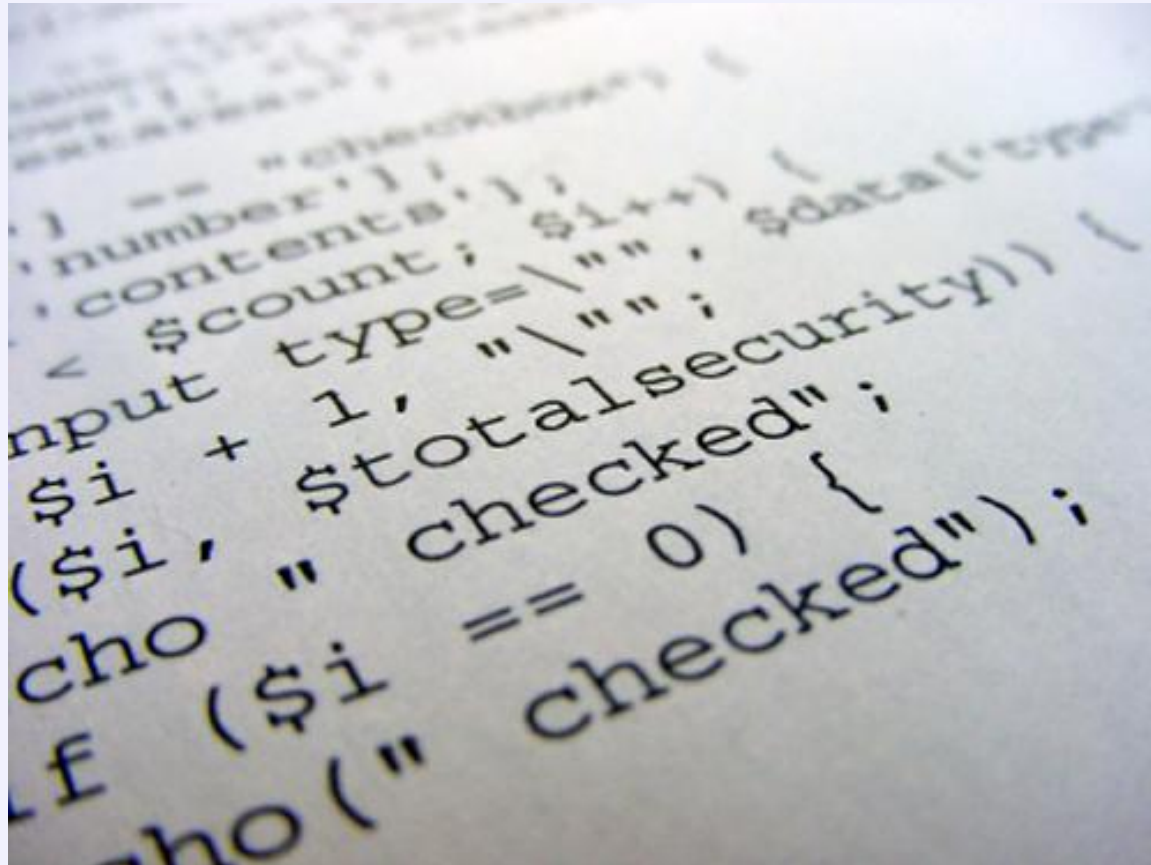
Pero también porque...



OWASP

The Open Web Application Security Project

Hay una necesidad de desarrollar aplicaciones de Software que sean seguras!



Agenda



OWASP

The Open Web Application Security Project

- ¿Qué es OWASP?, ¿Dónde estamos?, ¿Para dónde vamos?
- La necesidad de Desarrollar aplicaciones seguras
- Estadísticas de ataques informáticos globales
 - Evaluación de ~7000 sitios Web.



OWASP

The Open Web Application Security Project

The Open Web Application Security Project

OWASP:



Enjambres de abejas:

Capítulos locales en todo el mundo!





OWASP

The Open Web Application Security Project

Celebrando 11 años...



<http://web.archive.org> Dec 2011

OWASP
OPEN WEB APPLICATION SECURITY PROJECT

Home - About OWASP

OWASP PROJECT COMMITTEE

The Project Committee is responsible for the organisation of OWASP including running this web site, funding, setting up the OWASP foundation. It also organizes speaking opportunities on behalf of the project and deals with press and publishing.

Mark Curphey Chair Charles Schwab	Dennis Croves Vice Chair	Kavon Jeong Site Manager
--	------------------------------------	------------------------------------

OWASP TECHNICAL STEERING COMMITTEE

The Technical Committee is made up of renowned application security experts who ensure that the work and ideas are technically sound. These people have a wealth of experience and knowledge and will be guiding much of the direction of the work in various areas. As well as participating on the mailing list the technical committee has a monthly conference call to discuss progress. They are the OWASP technical think tank!

Greg Hoglund CIS/TOSSure	Eliel Levy SecurityFocus	John Viega Secure Software	Chris Vysopal @State
------------------------------------	------------------------------------	--------------------------------------	--------------------------------

OWASP USER COMMITTEE

The User Committee was created to solicit feedback from the end users and developers of web applications and web systems. We have received lots of ideas on what work people feel is needed or where knowledge is lacking and the user committee gives us the ability to formally capture that feedback from the people that own and build these systems. This also ensures that the technical correct work is useful in the real world. The committee is run by **Robert Rodger** of the Bank of Bermuda.

Robert "Bob" Rodger Bank of Bermuda	John Bumenthal
---	-----------------------

OWASP ACTIVE CONTRIBUTORS

Jeremiah Grossman White Hat Security	Itzhak El-Gad Santum	David Endler iChime	Martin Eitzner
Bill Hau IBM	Svenn Huseby	Bill Pennington Guarent	Tim Smith Dimension Data
Nigel Tranter Transter	David Zimmer	David Wong Foundation	

Home - Get Involved - Projects - Schedule - Tools - Tutorials - Contact

Copyright © 2011 The Open Web Application Security Project

¿Qué es OWASP?



OWASP

The Open Web Application Security Project

Nuestra Misión

Sin fines de lucro | Global | Imparcial

OWASP no avala ni recomienda productos o servicios comerciales

¿Qué es OWASP?



OWASP

The Open Web Application Security Project

Impulsado por la Comunidad

~30,000 participantes en listas de correos

~200 Capítulos activos en 70 países

1600+ Miembros, **56** Patrocinadores

69 Patrocinadores académicos

En todo el mundo!



OWASP

The Open Web Application Security Project

200 Capítulos, 1 600+ Miembros



¿Qué es OWASP?



OWASP

The Open Web Application Security Project

Recursos de Calidad

200+ Proyectos

15,000+ descargas herramientas,
documentación

250,000+ visitantes únicos

800,000+ páginas vistas (mensual)

Recursos de Calidad



OWASP

The Open Web Application Security Project

Código

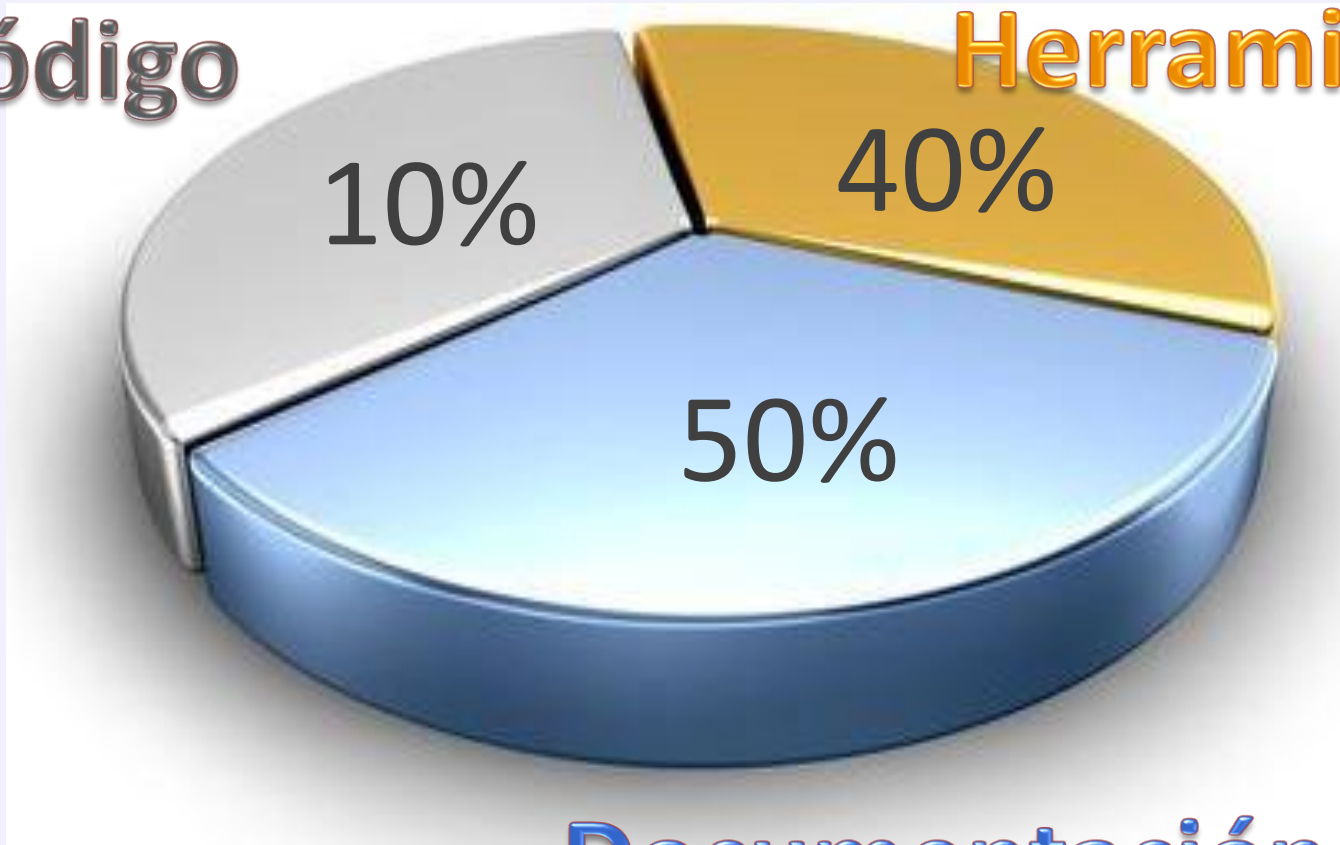
10%

Herramientas

40%

50%

Documentación



~140 Proyectos

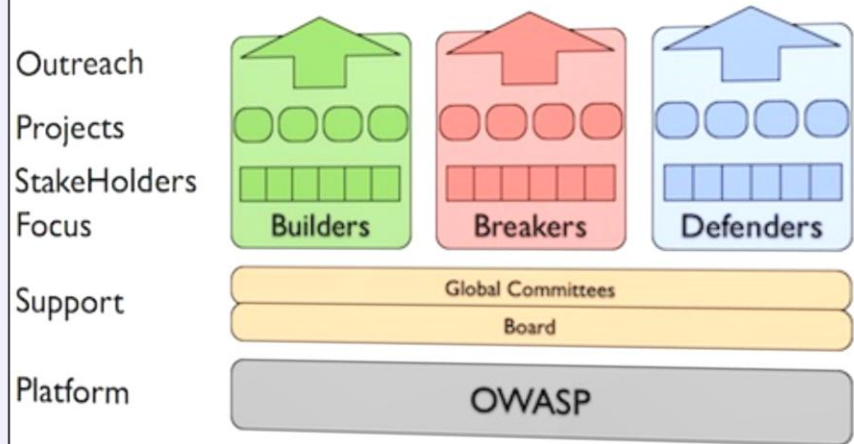


OWASP

The Open Web Application Security Project

- **PROTEGER** - Se trata de herramientas y documentos que pueden ser utilizados para proteger de vulnerabilidades asociadas al diseño.
- **DETECTECTAR** - Se trata de herramientas y documentos que pueden ser utilizados para encontrar vulnerabilidades asociadas al diseño.
- **Ciclo de Vida**- Se trata de herramientas y documentos que pueden ser utilizadas en el Ciclo de vida de las aplicaciones de software(SDLC).

A Vision for OWASP

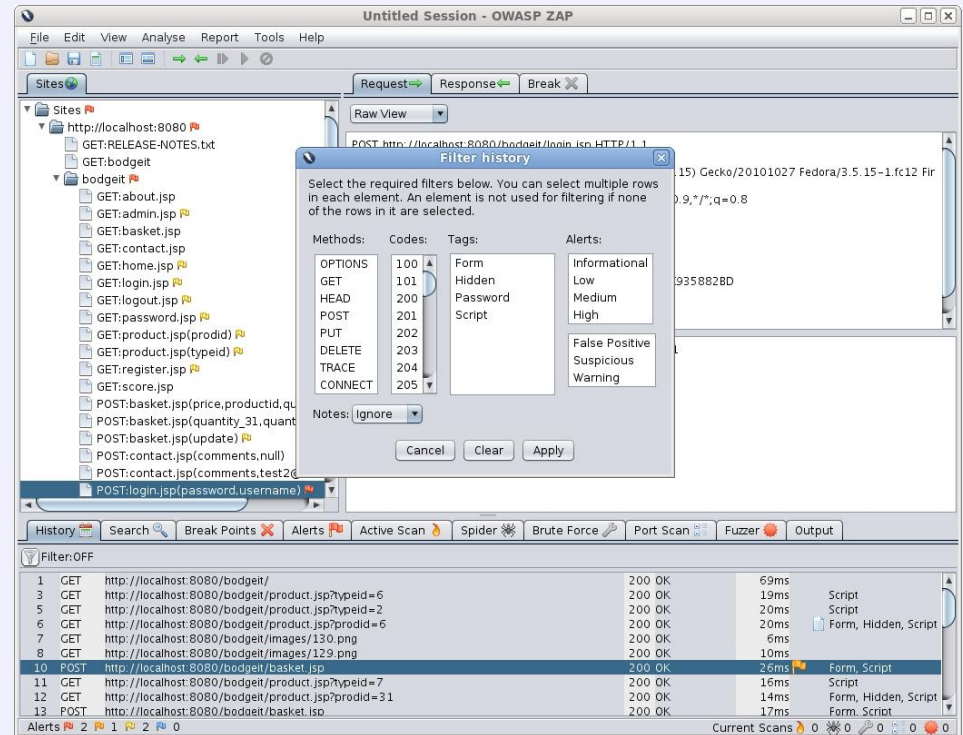


Productos destacados



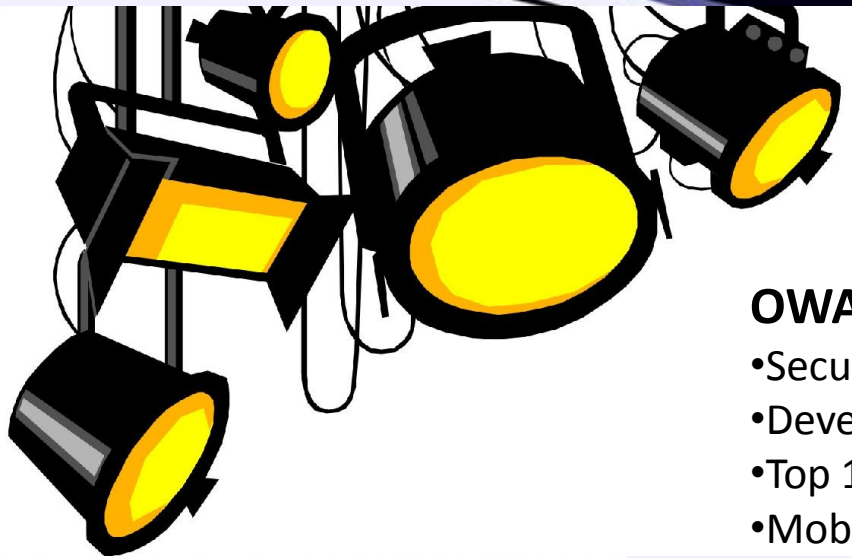
Zed Attack Proxy (ZAP):

- Proxy
- Scanner automatizado
- Scanner pasivo
- Scanner de fuerza bruta.
- Scanner de puertos
- Certificados SSL dinámicos.
- API



- 5 desarrolladores, 15 contribuyentes
- Internacional
- Translated into 9 languages: Brazilian Portuguese, Chinese, French, German, Greek, Indonesian, Japanese, Polish, Spanish

Productos destacados



OWASP Seguridad Móvil:

- Security testing
- Development guidance
- Top 10 controls
- Mobile threat model
- GoatDroid
- Top 10 risks

Top 10 Mobile Risks:

1. Insecure Data Storage
2. Weak Server Side Controls
3. Insufficient Transport Layer Protection
4. Client Side Injection
5. Poor Authorization and Authentication
6. Improper Session Handling
7. Security Decisions Via Untrusted Inputs
8. Side Channel Data Leakage
9. Broken Cryptography
10. Sensitive Information Disclosure



Enterprise Security API



OWASP

The Open Web Application Security Project

Líder del Proyecto: Chris Schmidt, Chris.Schmidt@owasp.org

Propósito: Librería de controles para la seguridad de aplicaciones Web, libre y de código abierto que ayuda a los programadores a escribir aplicaciones de bajo riesgo

Security controls that are included:

There are reference implementations for each of the following security controls:

- Authentication
- Access control
- Input validation
- Output encoding/escaping
- Cryptography
- Error handling and logging
- Communication security
- HTTP security
- Security configuration



for Reboot

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

Hojas de Trucos



OWASP

The Open Web Application Security Project

Developer Cheat Sheets

- OWASP Top Ten Cheat Sheet
- Authentication Cheat Sheet
- Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet
- Cryptographic Storage Cheat Sheet
- Input Validation Cheat Sheet
- XSS (Cross Site Scripting) Prevention Cheat Sheet
- DOM based XSS Prevention Cheat Sheet
- Forgot Password Cheat Sheet
- Query Parameterization Cheat Sheet
- SQL Injection Prevention Cheat Sheet
- Session Management Cheat Sheet
- HTML5 Security Cheat Sheet
- Transport Layer Protection Cheat Sheet
- Web Service Security Cheat Sheet
- Logging Cheat Sheet
- JAAS Cheat Sheet

Mobile Cheat Sheets

- IOS Developer Cheat Sheet
- Mobile Jailbreaking Cheat Sheet

Draft Cheat Sheets

- Access Control Cheat Sheet
- REST Security Cheat Sheet
- Abridged XSS Prevention Cheat Sheet
- PHP Security Cheat Sheet
- Password Storage Cheat Sheet
- Secure Coding Cheat Sheet
- Threat Modeling Cheat Sheet
- Clickjacking Cheat Sheet
- Virtual Patching Cheat Sheet
- Secure SDLC Cheat Sheet
- Web Application Security Testing Cheat Sheet
- Application Security Architecture Cheat Sheet

OWASP Top Ten

TOP 10 WEB APPLICATION SECURITY RISKS

A1: Injection

A2: Cross Site Scripting (XSS)

A3: Broken Authentication and Session Management

A4: Insecure Direct Object References

A5: Cross Site Request Forgery (CSRF)

A6: Security Misconfiguration

A7: Failure to Restrict URL Access

A8: Unvalidated Redirects and Forwards

A9: Insecure Cryptographic Storage

A10: Insufficient Transport Layer Protection



OWASP Appsec Tutorial Series (**Videos**)

Más recursos!



NOTICIAS

BLOG

PODCAST

MEMBRESIAS

LISTAS DE CORREOS

NEWSLETTER

APPLE APP STORE

VIDEO TUTORIALES

**SESIONES DE
ENTRENAMIENTO**

REDES SOCIALES



7 Comités Globales



OWASP

The Open Web Application Security Project

OWASP GLOBAL COMMITTEES

OWASP GLOBAL COMMITTEE	Projects	Membership	Education	Conferences	Industry	Chapters	Connections
Committee Chair	Jason Li	Helen Gao	Martin Knobloch	Mark Bristow	Rex Booth	Josh Sokol	Jim Manico
Members	<ul style="list-style-type: none"> • Brad Causey • Chris Schmidt • Justin Searle • Larry Casey • Keith Turpin 	<ul style="list-style-type: none"> • Dan Cornell • Ofer Maor • Aryavalli Gandhi 	<ul style="list-style-type: none"> • Eduardo Neves • Cecil Su • Fabio Cerullo • Kuai Hingosa • Sebastien Gioria • Tony Gottlieb • Carlos Serrão • Luiz Otavio Duarte 	<ul style="list-style-type: none"> • Lucas Ferreira • John Wilander • Richard Greenberg • Ralph Durkee • Mohd Fazli Azran • Lorna Alamri • Benny Ketelslegers 	<ul style="list-style-type: none"> • Mauro Flores • Alexander Fry • Eoin Keary • Mateo Martinez • Colin Watson • Marco Morana 🇮🇹 • Christian Papathanasiou • Tobias Gondrom 	<ul style="list-style-type: none"> • Seba Deleersnyder • Tin Zaw • L. Gustavo C. Barbato • Ivy Zhang 	<ul style="list-style-type: none"> • Ludovic Petit • Luiz Eduardo Dos Santos • Justin Clarke • Jerry Hoff
Applicants				<ul style="list-style-type: none"> • Zhendong Yu 	<ul style="list-style-type: none"> • Michael Scovetta 		
Committee Looking For	New Members with OWASP Project Leadership Experience	More Members	New Members with Education Background	More Members Outside U.S.	More Members Outside U.S. and Europe	More Members Outside U.S.	More Members

Agenda



OWASP

The Open Web Application Security Project

- ¿Qué es OWASP?, ¿Dónde estamos?, ¿Para dónde vamos?
- La importancia de escribir aplicaciones Seguras
- Estadísticas de ataques informáticos globales
 - Evaluación de ~700 Sitios Web.

La importancia de desarrollar aplicaciones seguras



- El Software está en todas partes:



- El software puede causar pérdidas humanas y económicas.



The Lessons of AF 447

Did Faulty Computer Indicator Reinforce Pilot Errors?

By Gerald Traufetter



REUTERS

Brazilian Navy sailors pick a piece of debris from Air France flight AF447 out of the Atlantic Ocean, a week after the crash happened on June 1, 2009.

- Air France 447, 220 tripulantes
- Río Janeiro- París
- El Airbus A330 tiene uno de los más sofisticados sistemas automatizados de pilotaje en la industria aérea



OWASP

The Open Web Application Security Project

- Fallo informático Knight Capital \$440 millones

Los errores informáticos más costosos

Knight Capital, la NASA, General Electric y el Y2K protagonizaron varios de las pifias millonarias; los mercados se han vuelto más vulnerables con el aumento del trading computarizado.

Publicado: Viernes, 10 de agosto de 2012 a las 16:18

CNNMoney.com



La pérdida de Knight Capital casi cuadruplicó las ganancias de 2011. (Foto: Cortesía CNNMoney)

Por: Brian Patrick Eha

NUEVA YORK — Cuando se trata de virus letales, el fallo informático que pulverizó 440 millones de dólares (mdd) de los fondos de Knight Capital Group el miércoles de la semana pasada está a la par de la mosca tse-tse.

En menos de una hora, los ordenadores de Knight Capital ejecutaron una serie de órdenes automáticas que se suponía iban a distribuirse en un período de días. Millones de acciones cambiaron de manos. La pérdida resultante, que casi cuadruplicó las ganancias de la compañía en 2011, paralizó a la firma de corretaje y la llevó al borde de la quiebra.

Fuente CNN: <http://www.cnnexpansion.com/economia/2012/08/10/los-errores-informaticos-mas-costosos>



- 6,46 millones de contraseñas de LinkedIn filtradas(06 Junio 2012)

A screenshot of a BBC News Technology article. The page has a red header with the BBC logo and navigation links for News, Sport, Weather, Travel, and Future. Below the header, the word "NEWS" is in large white letters, followed by "TECHNOLOGY" in smaller white letters. A secondary navigation bar includes links for Home, UK, Africa, Asia, Europe, Latin America, Mid-East, US & Canada, Business, Health, and Sci/Environment. The article is dated "6 June 2012" and was last updated at "23:28 GMT". It has 13K shares and social media icons for Facebook, Twitter, Email, and Print. The headline is "LinkedIn passwords leaked by hackers". The text states: "Social networking website LinkedIn has said some of its members' passwords have been 'compromised' after reports that more than six million passwords had been leaked onto the internet. Hackers posted a file containing encrypted passwords onto a Russian web forum. They have invited the hacking community to help with decryption." To the right of the text is an image of a smartphone screen showing the LinkedIn mobile app login page with the text "To join LinkedIn, sign up below ... it's free!" and a "First Name:" input field. A "REUTERS" watermark is visible in the bottom right corner of the image. Below the image, a caption reads: "The site had earlier issued a change to its mobile apps after a privacy flaw was uncovered".





OWASP

The Open Web Application Security Project

- Mas de 100 Universidades hackeadas por GhostShell (Octubre 02 2012)
- 120,000 registros de estudiantes filtrados.

Topic: Security

Follow via:  

GhostShell university hack: By the numbers

Summary: Yesterday, hacktivist group GhostShell claimed to have breached 100 top university servers, releasing 120,000 records. But how much information was sensitive?



By Charlie Osborne for Zero Day | October 3, 2012 -- 16:18 GMT (09:18 PDT)

 Follow @ZDNetCharlie

Records stolen from university databases including the University of Michigan, New York University, Princeton and Harvard were made publicly available yesterday, after hacker group leader 'DeadMellox' tweeted a link to the release posted on Pastebin.



OWASP

The Open Web Application Security Project

- Ataque informático en el estado de Carolina del Sur (26 Octubre 2012)
- 3.6 millones de SSN expuestos

3.6 million SC Social Security numbers exposed to cyber attack

NIKKI HALEY | OCTOBER 26, 2012 | BY: ROSALIE THOMPSON | + [Subscribe](#)



South Carolina Governor Nikki Haley
Credits: Chris Keane/Getty Images

Agenda



OWASP

The Open Web Application Security Project

- ¿Qué es OWASP?, ¿Dónde estamos?, ¿Para dónde vamos?
- La importancia de escribir aplicaciones Seguras
- Estadísticas de ataques informáticos globales
 - Evaluación de ~7,000 Sitios Web.



OWASP

The Open Web Application Security Project

- WhiteHat Security Reporte de estadísticas en Sitios Web.
- Evaluación de 7,000 sitios Web.
- Reducción significativa en vulnerabilidades.
- Firewalls están ofreciendo una nueva oportunidad.



- Promedio de vulnerabilidades críticas fue de **79 en 2011, 230 en 2010 y 1,111 en 2007.**
- XSS es la vulnerabilidad prevaleciente (**55%**).
- Firewalls han ayudado a mitigar el riesgo de al menos **71%** de las vulnerabilidades.
- El sector bancario con el menor porcentaje de vulnerabilidades.



OWASP

The Open Web Application Security Project

- Estado en la seguridad de los sitios Web

AT A GLANCE: THE CURRENT STATE OF WEBSITE SECURITY

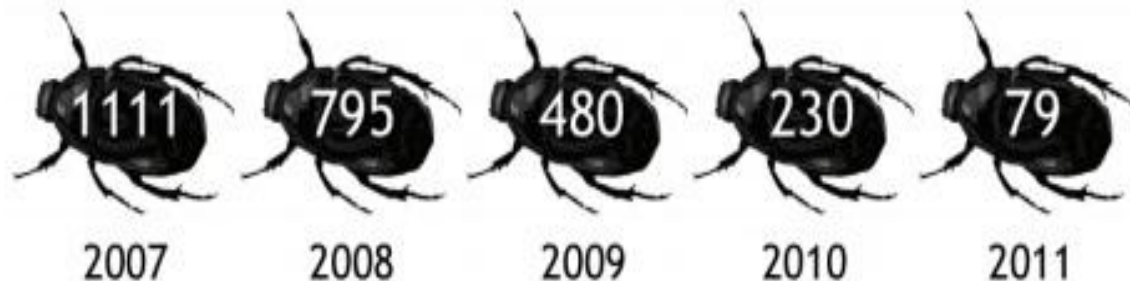


Figure 1. Vulnerability Historical Trend

The annual average number of serious* vulnerabilities discovered per website per year

The annual average number of serious* vulnerabilities discovered per website per year

Figure 1. Vulnerability Historical Trend



OWASP

The Open Web Application Security Project

Cross-Site Scripting se ha encontrado en 55% de los sitios Web

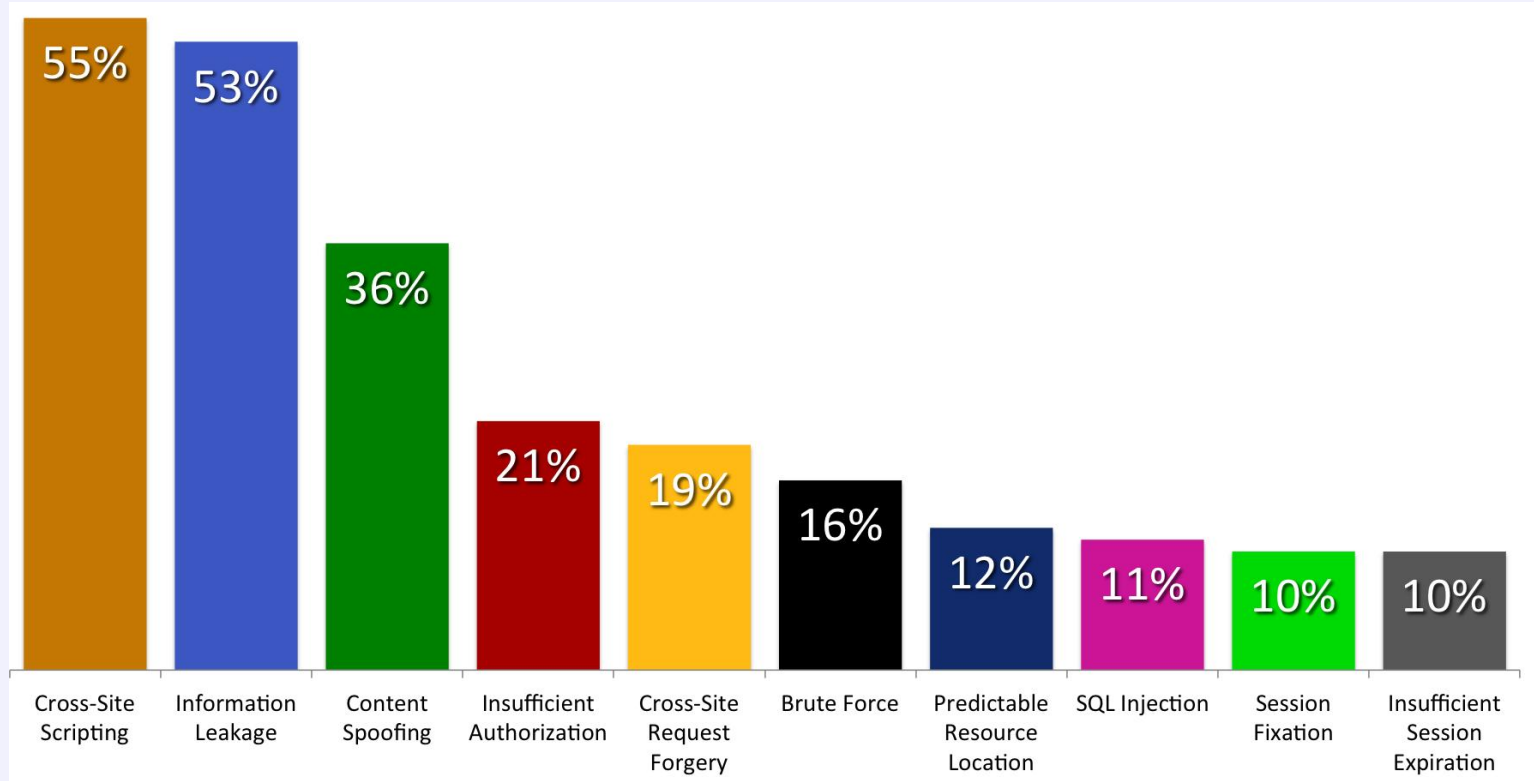


Figure 3. Top Ten Vulnerability Classes (2011) Percentage likelihood that at least one serious* vulnerability will appear in a website.

Fuente: WhiteHat http://img.en25.com/Web/WhiteHatSecurityInc/WPstats_summer12_12th.pdf



OWASP

The Open Web Application Security Project

- Industrias Comparadas:

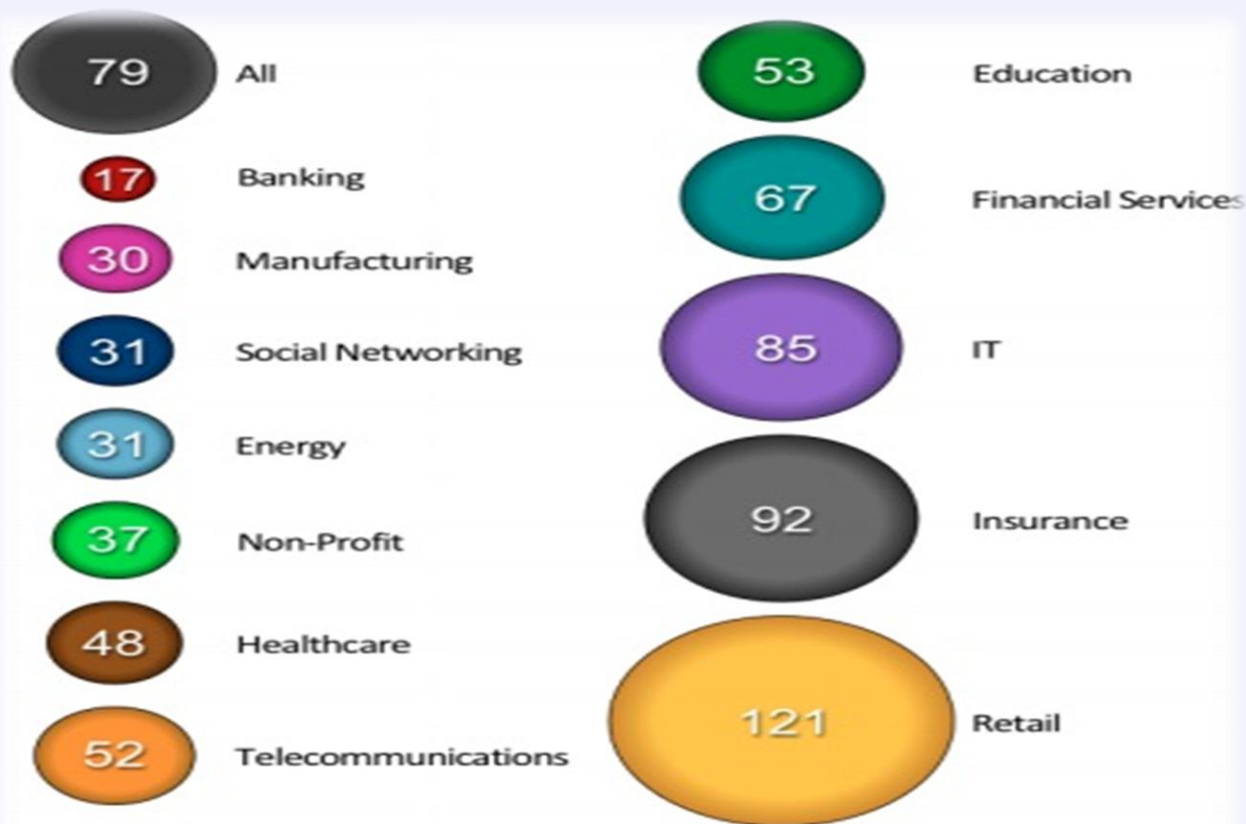


Figure 18. Average Number of Serious* Vulnerabilities (2011)
(Sorted by industry)



OWASP

The Open Web Application Security Project

- ScoreCard: Industria Bancaria

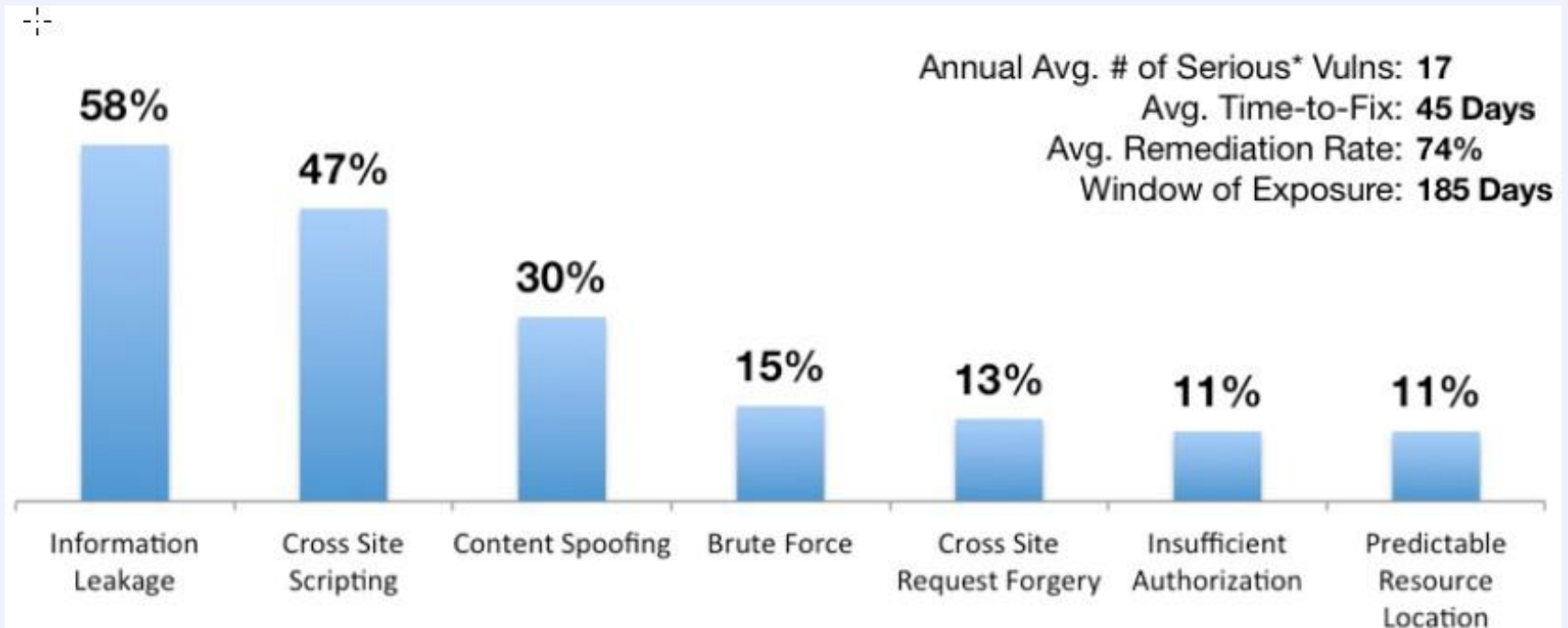


Figure 6. Banking Industry: Website Security Scorecard



OWASP

The Open Web Application Security Project

- ScoreCard: Educación

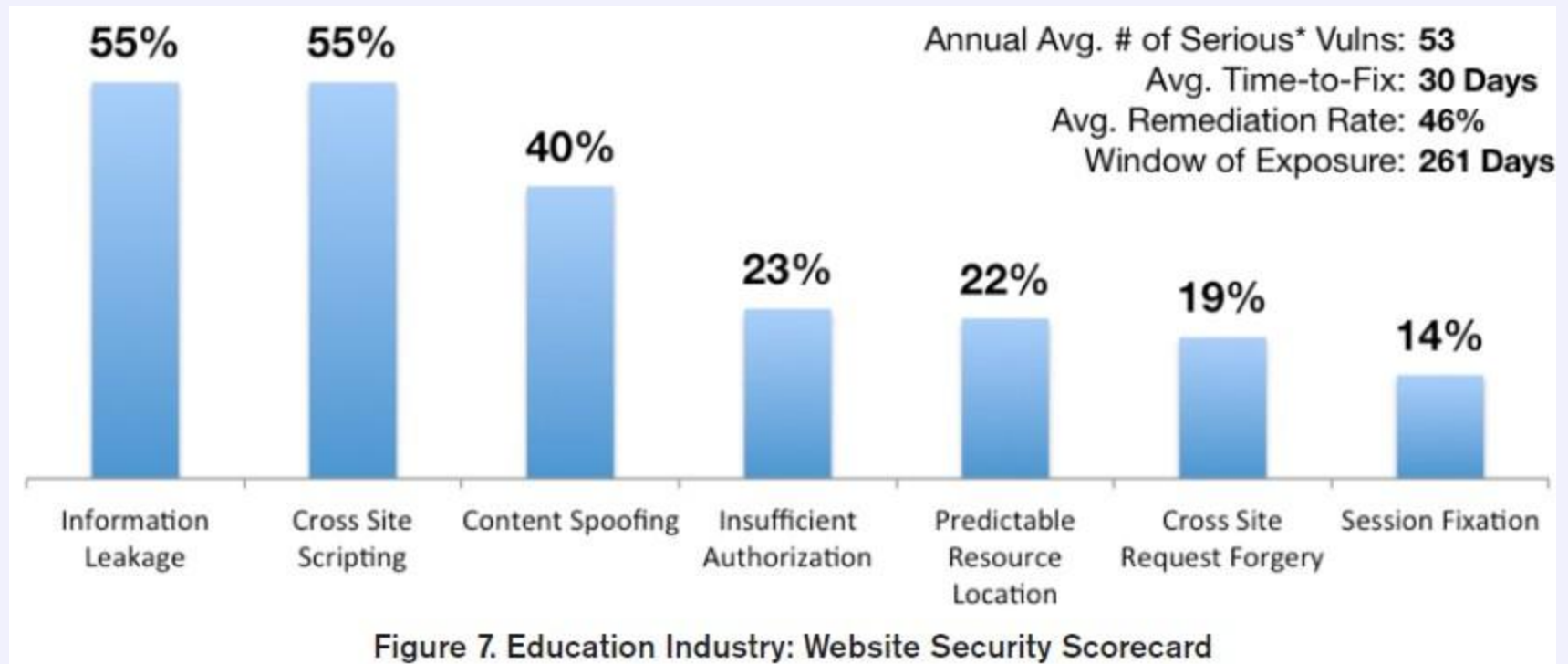


Figure 7. Education Industry: Website Security Scorecard.

Fuente: WhiteHat http://img.en25.com/Web/WhiteHatSecurityInc/WPstats_summer12_12th.pdf



OWASP

The Open Web Application Security Project

- ScoreCard: Servicios Financieros

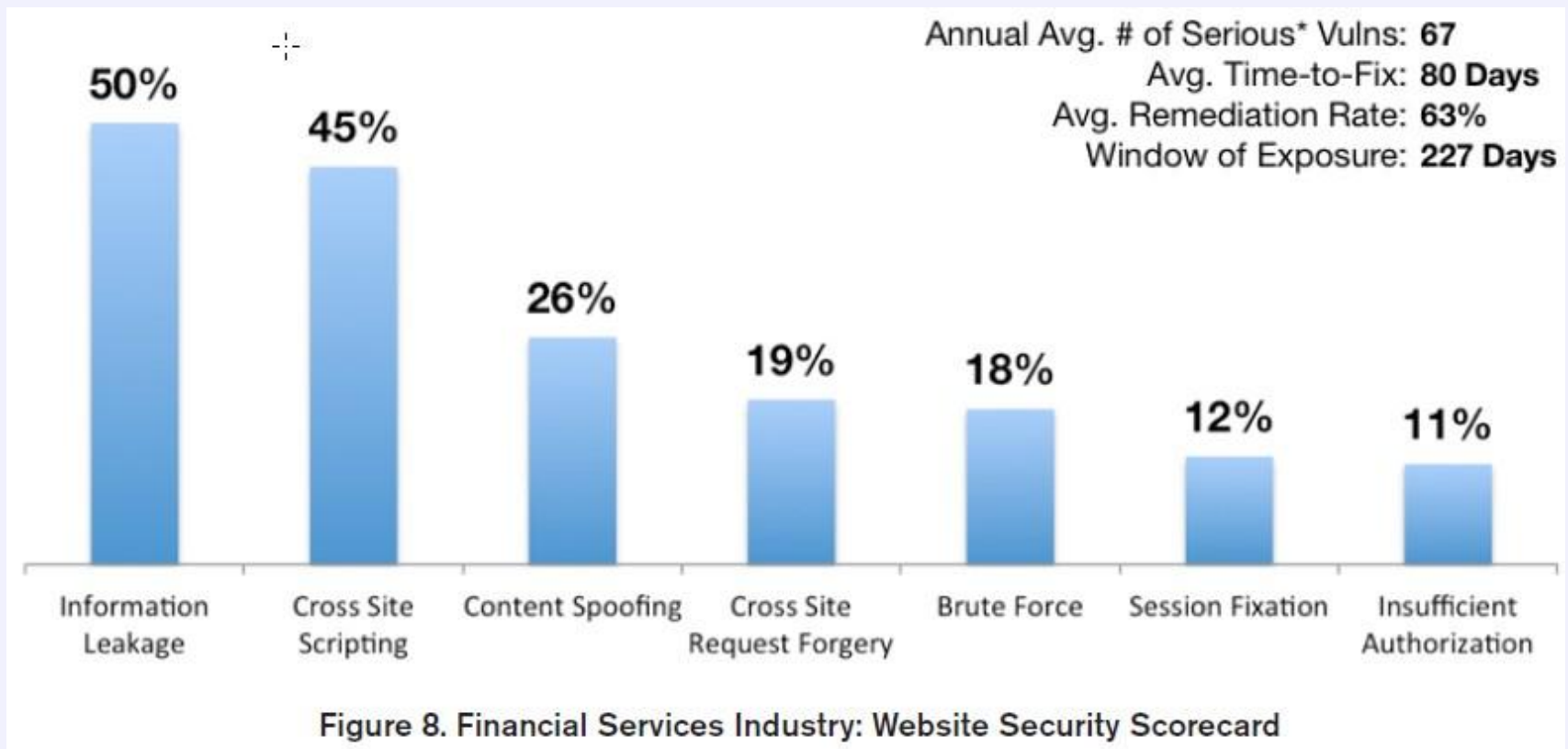


Figure 8. Financial Industry: Website Security Scorecard.

Fuente: WhiteHat http://img.en25.com/Web/WhiteHatSecurityInc/WPstats_summer12_12th.pdf



- ScoreCard: Sector Salud

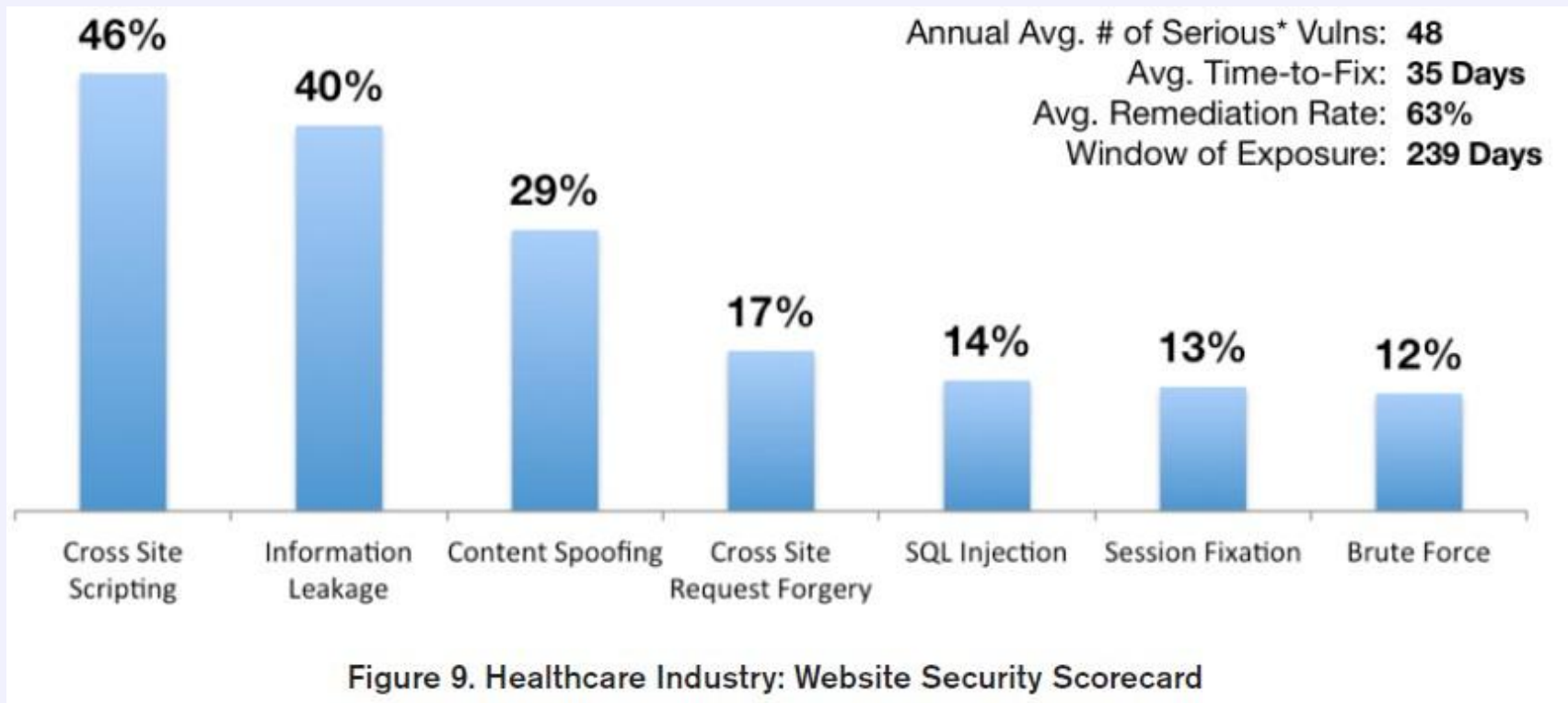


Figure 9. Health Industry: Website Security Scorecard.

El conocimiento es riqueza,
El conocimiento debe fluir



OWASP

The Open Web Application Security Project

“Si usted creé que la educación es cara,
Pruebe con la ignorancia!”

Abraham Lincoln



Trabajo en Equipo



TEAM es sinónimo de... **T**ogether **E**ach **A**chieves **M**ore

Todos ustedes son bienvenidos a atender nuestras charlas y reuniones en OWASP.

El Capítulo Local de OWASP Costa Rica les da la Bienvenida!



Q&A



OWASP

The Open Web Application Security Project



Michael Hidalgo

michael.hidalgo@owasp.org