

The banner features a blue background with a grid pattern and a large white padlock icon. The text "LatamTour Owasp 2017" is prominently displayed in white. Below this, the name "Carlos Allendes" is written in a dark blue font, followed by "Presidente Owasp Chile" in a smaller dark blue font. The OWASP logo, which consists of a stylized globe with a network of lines, is shown next to the text "OWASP" and "The Open Web Application Security Project".

LatamTour
Owasp 2017

LatamTour Owasp 2017

Carlos Allendes
Presidente Owasp Chile



OWASP
The Open Web Application Security Project

The slide has a blue header with the text "Antecedentes del Expositor" in white. The OWASP logo and name are in the top left. The main content area is white with black text. It lists the speaker's name and email, followed by a bulleted list of his roles and experiences.

 **OWASP**
The Open Web Application Security Project

Antecedentes del Expositor

Carlos Allendes Droguett (carlos.allendes@owasp.org)

- Presidente del capítulo chileno OWASP
- Co-fundador OWASP Honduras y Rep.Dominicana
- Socio Fundador en www.QualityFactory.cl
- Experiencia y proyectos
 - PCI DSS, acreditación en seguridad
 - ITIL, implantación de procesos para servicios
 - CMMi, AGILE, Ingeniería de Software
 - QA y Testing, Pruebas de Software y Aseguramiento Calidad

**OWASP**
The Open Web Application Security Project

Antecedentes
del Expositor



¿Qué Estudiar?

**OWASP**
The Open Web Application Security Project

Antecedentes
del Expositor






OWASP
 The Open Web Application Security Project

Qué es y que hace OWASP?


<https://goo.gl/084Maa>
<https://goo.gl/giPWzD>



7


OWASP
 The Open Web Application Security Project

Qué es y que hace OWASP?

OPEN WEB APPLICATION SECURITY PROJECT


WASP = google { define:wasp } = avispa

- Nació en el 2001, por un grupo de personas que se preguntaron:
Porque nos confiamos de aplicaciones Web, que tipo de estándar de seguridad nos brinda confianza ?
- Comunidad LIBRE y OPEN SOURCE de todos los proyectos que se desarrollan.
- Organización **NO LUCRATIVA**



OWASP

The Open Web Application Security Project

Qué es y que hace OWASP?


- Porque se volvió **FAMOSA** a nivel **INTERNACIONAL**.
- **Porque:**
 - NO** apoya ninguna marca, tecnología o producto, apoya el **CONOCIMIENTO**.



Finalmente, por que la NSA (**National Security Agency**) adopto y apoyo el proyecto del TOP TEN y lo mantiene como un estándar a nivel internacional de las **10 amenazas mas criticas** en aplicaciones Web.




1

OWASP

The Open Web Application Security Project

Qué es y que hace OWASP?



- OWASP es una organización mundial sin fines de lucro, que se dedica a identificar y combatir las causas que hacen inseguro el software.
- Creamos documentación y metodologías que son de aplicación práctica en ambientes empresariales y son de “código abierto” (www.owasp.org)



OWASP
The Open Web Application Security Project

Qué es y que hace OWASP?



16 Años existencia

200+ Capítulos activos

Map data ©2011 MapLink, Tele Atlas - Terms of Use



OWASP
The Open Web Application Security Project

Qué es y que hace OWASP?

50,000+ Voluntarios

150+ Proyectos



OWASP
The Open Web Application Security Project

Qué es y que hace OWASP?





OWASP Top 10 - 2013
Los diez riesgos más críticos en Aplicaciones Web

- A1: Injection
- A2: Broken Authentication and Session Management
- A3: Cross-Site Scripting (XSS)
- A4: Insecure Direct Object References
- A5: Security Misconfiguration
- A6: Sensitive Data Exposure
- A7: Missing Function Level Access Control
- A8: Cross-Site Request Forgery (CSRF)
- A9: Using Known Vulnerable Components
- A10: Unvalidated Redirects and Forwards

OWASP crea y posiciona estándares, normas y procesos cuyo foco es el fortalecimiento de la seguridad en el desarrollo y ambientes web.

OWASP
The Open Web Application Security Project

Qué es y que hace OWASP?

Capítulo OWASP Chile

- 6 años de trabajo y conferencias
- 32 eventos, talleres y cursos
- Co-fundación de chapters en el Caribe








OWASP
The Open Web Application Security Project

Qué es y que hace OWASP?



OWASP
The Open Web Application Security Project

Laboratorio de Hacking, en 5 minutos

- ✓ Aprender/practicar ataques y defensa de aplicaciones.
- ✓ Sin afectar a empresas reales y que no sea ilegal.



OWASP
The Open Web Application Security Project

Esta pasando a diario

Geeks Everywhere...




OWASP
The Open Web Application Security Project

Esta pasando a diario

Mega-Robos de Información



**Master Hacker
Albert Gonzalez**
By **CI ARIF RINOVATI**
Wednesday, Aug 19, 2009

Albert Gonzalez, 28, was indicted August 17, 2009 on charges that he carried out the largest hacking and identity-theft case in US history.

2009

[Agosto 2009] Culpable de robar más de 130 millones de números de tarjetas de crédito y débito



Esta pasando
a diario

OWASP
The Open Web Application Security Project

Hacking masivos y frecuentes

A blue curved arrow points from left to right, indicating a timeline of cyberattacks. Along the arrow, three points are marked with blue circles and labeled with the month and year of the attack. Below each point is a small thumbnail image of a news article about the attack.

- Diciembre 2013**
TARGET hacked!
Target: Hacking hit up to 110 million customers
- Mayo 2014**
eBAY hacked!
eBay asks 145 million users to change passwords after cyber attack
- Septiembre 2014**
Home Depot hacked!
Massive Home Depot Hack: Over 40 Million Credit Cards Hacked Linked To Russian Hackers? Adds Security Pressure, Home Depot Investigates

21

Esta pasando
a diario

OWASP
The Open Web Application Security Project

Hacking masivos y frecuentes

A screenshot of a web browser showing a news article from 'Diario de Sevilla'. The article is titled 'Holanda evitará la informática en las elecciones por miedo a un ciberataque' (Netherlands will avoid computers in elections for fear of a cyberattack). The article is categorized under 'MUNDO' (World). The text of the article states that the Netherlands will count votes by hand and communicate results by phone to avoid a possible 'hack' that could influence the results.

Diario de Sevilla

SEVILLA PROVINCIA ANDALUCÍA PANORAMA SEVILLA FC REAL BETIS CULTURA COFRADÍAS OPINIÓN

ESPAÑA MUNDO ECONOMÍA

MUNDO

Holanda evitará la informática en las elecciones por miedo a un ciberataque

- Contabilizará a mano todas las papeletas, y comunicará los resultados por teléfono posible 'hacking' que pueda influir en los resultados.

22

OWASP y PCI-DSS


 **OWASP**
The Open Web Application Security Project

Estamos expuestos...

...y ahora??




OWASP y PCI-DSS

 **OWASP**
The Open Web Application Security Project

“PCI Security Standards Council”
“Consejo de normas de seguridad PCI”

Foro mundial, implementado en 2006, por las marcas:

- Visa
- MasterCard
- American Express
- Discover Financial Services
- JCB International.





OWASP
 The Open Web Application Security Project

**OWASP y
PCI-DSS**

PCI-DSS Norma de Seguridad ...para que sirve?


PCI busca aumentar la seguridad de los datos de cuentas de pago.

y de las aplicaciones de comercio electrónico

Es aplicable a todos los actores que participan en alguna parte del ciclo de la transacción electrónica









OWASP
 The Open Web Application Security Project


**OWASP y
PCI-DSS**

PCI-DSS Norma de Seguridad

Por qué usarla...??



OWASP y
PCI-DSS



OWASP
 The Open Web Application Security Project

Qué medidas sugiere PCI DSS ?

PCI DSS tiene 6 objetivos de control y 12 requisitos de seguridad.


Normas de seguridad de datos de la PCI: descripción general de alto nivel	
Desarrolle y mantenga redes y sistemas seguros.	1. Instale y mantenga una configuración de firewall para proteger los datos del titular de la tarjeta. 2. No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.
Proteger los datos del titular de la tarjeta	3. Proteja los datos del titular de la tarjeta que fueron almacenados 4. Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.
Mantener un programa de administración de vulnerabilidad	5. Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente. 6. Desarrollar y mantener sistemas y aplicaciones seguros
Implementar medidas sólidas de control de acceso	7. Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa. 8. Identificar y autenticar el acceso a los componentes del sistema. 9. Restringir el acceso físico a los datos del titular de la tarjeta.
Supervisar y evaluar las redes con regularidad	10. Rastree y supervise todos los accesos a los recursos de red y a los datos del titular de la tarjeta 11. Probar periódicamente los sistemas y procesos de seguridad.
Mantener una política de seguridad de información	12. Mantener una política que aborde la seguridad de la información para todo el personal

OWASP y
PCI-DSS



OWASP
 The Open Web Application Security Project

Qué medidas sugiere PCI DSS ?

PCI DSS tiene 6 objetivos de control y 12 requisitos de seguridad.

Normas de seguridad de datos de la PCI: descripción general de alto nivel		
Desarrolle y mantenga redes y sistemas seguros.	1. Instale y mantenga una configuración de firewall para proteger los datos del titular de la tarjeta. 2. No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.	✓
Proteger los datos del titular de la tarjeta	3. Proteja los datos del titular de la tarjeta que fueron almacenados 4. Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.	✓
Mantener un programa de administración de vulnerabilidad	5. Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente. 6. Desarrollar y mantener sistemas y aplicaciones seguros	
Implementar medidas sólidas de control de acceso	7. Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa. 8. Identificar y autenticar el acceso a los componentes del sistema. 9. Restringir el acceso físico a los datos del titular de la tarjeta.	✓
Supervisar y evaluar las redes con regularidad	10. Rastree y supervise todos los accesos a los recursos de red y a los datos del titular de la tarjeta 11. Probar periódicamente los sistemas y procesos de seguridad.	✓
Mantener una política de seguridad de información	12. Mantener una política que aborde la seguridad de la información para todo el personal	✓

OWASP y
PCI-DSS


OWASP
 The Open Web Application Security Project

Que medidas sugiere PCI DSS ?


PCI DSS tiene 6 objetivos de control y 12 requisitos de seguridad.



6. Desarrollar y mantener sistemas y aplicaciones seguros


<p>6.3.a Revise los procesos de desarrollo de software escritos para verificar que se basen en las normas o en las mejores prácticas de la industria.</p> <p>6.3.b Revise los procesos de desarrollo de software escritos y verifique que se incluya la seguridad de la información durante todo el ciclo de vida.</p> <p>6.3.c Evalúe los procesos de desarrollo de software escritos y verifique que las aplicaciones de software se desarrollen de conformidad con las PCI DSS.</p> <p>6.3.d Entreviste a los desarrolladores de software para verificar que se implementen los procesos de desarrollo de software escritos.</p> <p>6.3.2.a Revise los procedimientos de desarrollo de software escritos y entreviste al personal responsable para verificar que todos los cambios de código de las aplicaciones personalizadas (ya sea mediante procesos manuales o automáticos) se revisen de la siguiente manera:</p> <ul style="list-style-type: none"> Individuos que no sean el autor que originó el código e individuos con conocimiento en técnicas de revisión de código y prácticas de codificación segura revisan los cambios en los códigos. Las revisiones de los códigos aseguran que estos se desarrollan de acuerdo con las directrices de codificación segura (consulte el requisito 6.5 de las PCI DSS). 	<p>6.5.a Revise las políticas y los procedimientos de desarrollo de software y verifique que a los desarrolladores se les exija una capacitación actualizada en técnicas de codificación segura, según las guías y las mejores prácticas de la industria.</p> <p>6.5.b Revise los registros de capacitación para verificar que los desarrolladores de software hayan sido capacitados en técnicas de codificación segura por lo menos anualmente, en las que se incluya cómo evitar las vulnerabilidades de codificación comunes.</p> <p>6.5.c Verifique que los procesos implementados protejan las aplicaciones, al menos, contra las siguientes vulnerabilidades:</p>
--	---

OWASP Top 10 de Riesgos de Seguridad en Aplicaciones

OWASP y
PCI-DSS


OWASP
 The Open Web Application Security Project



OWASP
The Open Web Application Security Project

**OWASP y
PCI-DSS**

99% de malware hashes son vistos por sólo 58 segundos o menos

Figure 36.
Count of hashes by lifespan in seconds, (n=2.8 million)

La solución debe ser preventiva!

(fuente: Verizon Data Breach Report 2016)




OWASP
The Open Web Application Security Project

**OWASP y
PCI-DSS**

362.000 nuevas variantes de cripto-ransomware identificadas en 2015 (1000 /dia...?)


La solución debe ser preventiva!

(fuente: Symantec)

**OWASP**
The Open Web Application Security Project

OWASP y
PCI-DSS


El 93% de las fugas de datos, demoraron minutos o menos (data compromise Time)



Time Unit	Percentage
Seconds	11%
Minutes	81.9%
Hours	6%
Days	<1%
Weeks	<1%
Months	<1%
Years	<1%


La solución debe ser preventiva!

(fuente: Verizon Data Breach Report 2016)

**OWASP**
The Open Web Application Security Project

OWASP y
PCI-DSS

El 63% de las fugas de datos (confirmadas) se relacionan con contraseñas triviales o robadas.



La solución debe ser preventiva!

(fuente: Verizon Data Breach Report 2016)



OWASP
The Open Web Application Security Project


OWASP y PCI-DSS

La solución debe ser preventiva!

- **Aprender**
- **Practicar**
- **Perfeccionarse**





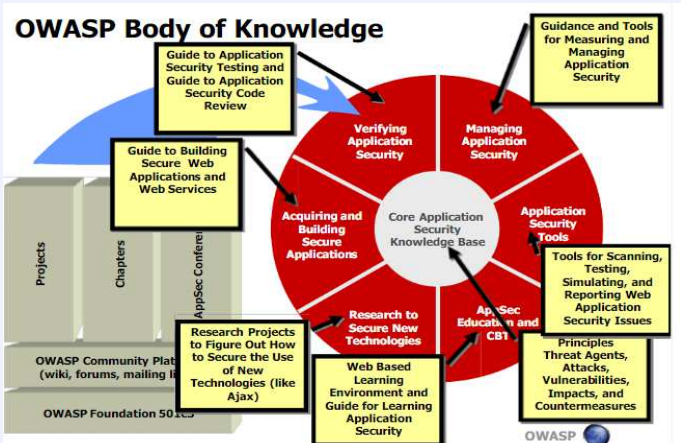




OWASP
The Open Web Application Security Project

OWASP y PCI-DSS

Aprender y Perfeccionarse

OWASP Body of Knowledge





OWASP


The Open Web Application Security Project

Qué dice la ley chilena?


Ley 19.223

Tipifica figuras penales relativas a la Informática

- 1.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento.
- 2.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él.
- 3.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.
- 4.- El que maliciosamente revele o difunda los datos contenidos en un sistema de tratamiento de información. Si quien incurre en estas conductas es el responsable del sistema de tratamiento de información se aumenta un grado.



Sabotaje



Espionaje



OWASP

The Open Web Application Security Project

OWASP y PCI-DSS

OWASP Vulnerable Web Applications Directory Project (VWAD)

- About OWASP
- Acknowledgements
- Advertising
- AppSec Events
- Books
- Brand Resources
- Chapters
- Donate to OWASP
- Downloads
- Funding
- Governance
- Initiatives
- Mailing Lists
- Membership
- Merchandise
- News
- Portal de la comunidad
- Presentations

Main

On-Line apps

Off-Line apps

Virtual Machines or ISOs

Acknowledgements

Road Map and Getting Involved

Project About



OWASP


Open Web Application Security Project

OWASP Vulnerable Web Applications Directory Project

[editar | editar código]

What is VWAD?

[editar | editar código]




OWASP
 The Open Web Application Security Project

**OWASP y
PCI-DSS**

OWASP Vulnerable Web Applications Directory Project (VWAD)

Provee una lista de 87 aplicaciones vulnerables para practicar hacking y tareas ofensivas en entornos web realistas y ... sin ir a la cárcel :)

Tipos	Cantidad
VM_ISO	21
OnLine_Apps	24
OffLine_Apps	42
Total general	87



OWASP
 The Open Web Application Security Project

**OWASP y
PCI-DSS**

Practicar... y Practicar...

https://www.owasp.org/index.php/OWASP_Vulnerable_Web_Applications_Directory_Project#tab=On-Line_apps

[Aplicaciones](#)
[Isttd](#)
[house mix](#)
[blog](#)
[tour17](#)
[revista](#)
[musica](#)
[pci](#)
[scl](#)
[testing](#)
[gf](#)
[lin](#)
[mios](#)
[Tx](#)

[Página](#)
[Discusión](#)

OWASP Vulnerable Web Applications Directory Project

[Main](#)
[On-Line apps](#)
[Off-Line apps](#)
[Virtual Machines or ISOs](#)
[Acknowledgements](#)
[Road Map and Getting](#)

App Name / Link	Technology	Author
Acuart@	PHP	Acunetix
Acublog@	NET	Art shopping
Acuforum@	ASP	
Altoro Mutual@		
BGA Vulnerable BANK App@	NET	
Crack Me Bank@		
Enigma Group@		
Gruyere@	Python	
Firing Range@		
Hackademic Challenges Project@	PHP - Joomla	
Hacker Challenge@		
Hackazon@	AJAX, JSON, X	
Hacking Lab@		
Hack.mes@		

Tipos	Cantidad
VM_ISO	21
OnLine_Apps	24
OffLine_Apps	42
Total general	87

OWASP
The Open Web Application Security Project

OWASP y PCI-DSS

Practicar... y Practicar...

Version: 2.6.3.1 Security Level: 0 (Hosed) Hints: Disabled (0 - 1 by harder) Not Logged In

Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data Hide Popup Hints Enforce SSL

OWASP Top 10

- A1 - SQL 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 - Insecure Cryptographic Storage
- A8 - Failure to Restrict URL Access
- A9 - Insufficient Transport Layer Protection
- A10 - Unvalidated Redirects and Forwards

Web Services

- SQL - Extract Data
- SQL - Bypass Authentication
- SQL - Insert Injection
- Blind SQL via Timing
- SQLMAP Practice
- SQLMAP Practice Targets
- Login
- View Someone's Blog
- User Info

HTML 5

- SQL - Insert Injection
- Blind SQL via Timing
- SQLMAP Practice
- SQLMAP Practice Targets
- Login
- View Someone's Blog
- User Info

Others

- SQL - Extract Data
- SQL - Bypass Authentication
- SQL - Insert Injection
- Blind SQL via Timing
- SQLMAP Practice
- SQLMAP Practice Targets
- Login
- View Someone's Blog
- User Info

Documentation

- SQL - Extract Data
- SQL - Bypass Authentication
- SQL - Insert Injection
- Blind SQL via Timing
- SQLMAP Practice
- SQLMAP Practice Targets
- Login
- View Someone's Blog
- User Info

Resources

- SQL - Extract Data
- SQL - Bypass Authentication
- SQL - Insert Injection
- Blind SQL via Timing
- SQLMAP Practice
- SQLMAP Practice Targets
- Login
- View Someone's Blog
- User Info

Release Announcements

Listing of vulnerabilities

Bug Report Email Address


What's New? Click Here


Release Announcements

OWASP
The Open Web Application Security Project

OWASP y PCI-DSS

Practicar... y Practicar...



 **OWASP**
The Open Web Application Security Project

Preguntas

Carlos Allendes
carlos.allendes@owasp.org

