



LatamTour
Owasp 2017

LatamTour Owasp 2017

Carlos Allendes
Presidente Owasp Chile

 OWASP
The Open Web Application Security Project



Antecedentes
del Expositor

 OWASP
The Open Web Application Security Project

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



Antecedentes
del Expositor

OWASP
The Open Web Application Security Project



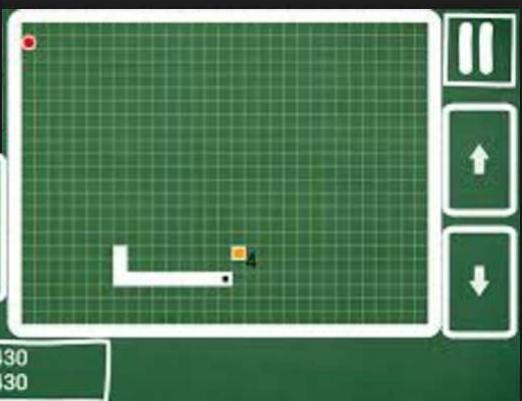
STAR TREK
STAR TREK 40 YEARS
TM & © 2009 CBS Studios Inc. All Rights Reserved. 1991

Antecedentes
del Expositor

OWASP
The Open Web Application Security Project



US\$180



Score: 430
Highscore: 430

Qué es y que hace OWASP?

OWASP
The Open Web Application Security Project

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



7

Qué es y que hace OWASP?

OWASP
The Open Web Application Security Project

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**

Qué es y que hace OWASP?

OWASP
The Open Web Application Security Project

- 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.

Qué es y que hace OWASP?

OWASP
The Open Web Application Security Project



- 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)

Qué es y que hace OWASP?

OWASP
The Open Web Application Security Project



16 Años existencia

200+ Capítulos activos

Map data ©2011 MapLink, Tele Atlas -

SPONSORED BY Google

Qué es y que hace OWASP?

OWASP
The Open Web Application Security Project



50,000+ Voluntarios

150+ Proyectos

Qué es y que hace OWASP?

OWASP
The Open Web Application Security Project

Code Review Guide Book v. 2.0 ALPHA
OWASP Foundation

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.

Qué es y que hace OWASP?

OWASP
The Open Web Application Security Project

Capítulo OWASP Chile

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





The slide features the OWASP logo and tagline 'The Open Web Application Security Project'. The title 'Qué es y que hace OWASP?' is displayed in the top right corner. The main content area is currently empty.

The slide features the OWASP logo and tagline 'The Open Web Application Security Project'. The title 'Laboratorio de Hacking, en 5 minutos' is displayed prominently. Below the title, two bullet points are listed: '✓ Aprender/practicar ataques y defensa de aplicaciones.' and '✓ Sin afectar a empresas reales y que no sea ilegal.' To the right of the text, there is an illustration of a red 'Get Out of Jail Free' card.



The slide features the OWASP logo and the tagline "The Open Web Application Security Project". At the top right, it says "Esta pasando a diario". The main title "Geeks Everywhere..." is in the center. Below the title are two images: one of a hacker in a hooded sweatshirt and mask working on a laptop with binary code and security terms like "access", "information", "email", "password", "internet", "code", and "breach" visible; and another of two young children, a girl and a boy, sitting at a table and laughing while looking at an open book.



The slide features the OWASP logo and the tagline "The Open Web Application Security Project". At the top right, it says "Esta pasando a diario". The main title "Mega-Robos de Información" is in the center. Below the title is a portrait of Albert Gonzalez, identified as the "Master Hacker". To the right of the portrait is a box of text and a small image of several credit cards (American Express, Visa, MasterCard). A red text overlay at the bottom left reads: "[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

21

Esta pasando
a diario

OWASP
The Open Web Application Security Project

Hacking masivos y frecuentes

22



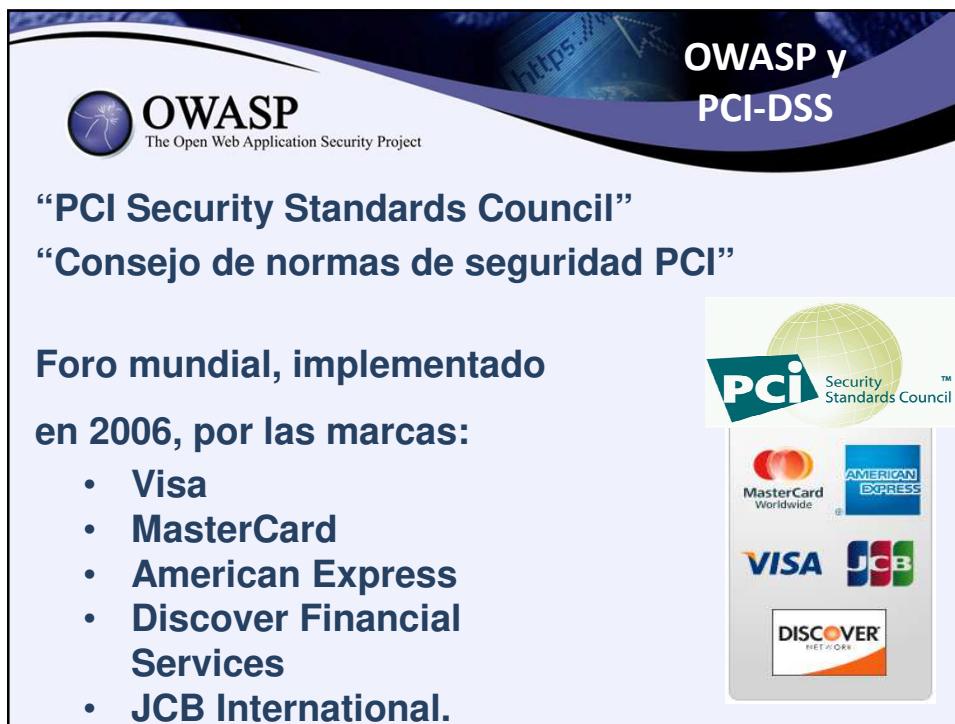
OWASP y
PCI-DSS

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 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

PCI DSS COMPLIANT

PCI PA-DSS VALIDATED

Welcome to the PCI Security Standards Council

MERCHANTS
Find out why and how to implement PCI Security Standards Council

FINANCIAL INSTITUTIONS
Resources to assist with your compliance efforts for your organization

HARDWARE / SOFTWARE
Resources designed for developers and device manufacturers

SERVICES AND PROFESSIONALS
Quick access to resources designed for industry professionals



OWASP y PCI-DSS

PCI-DSS Norma de Seguridad

Por qué usarla...??

MANUFACTURERS
PCI PTS
PIN Transaction Security

SOFTWARE DEVELOPERS
PCI PA-DSS
Payment Application Vendors

MERCHANTS & PROCESSORS
PCI DSS
Data Security Standard

PCI SECURITY STANDARDS & COMPLIANCE

Ecosystem of payment devices, applications, infrastructure and users

**OWASP y
PCI-DSS**

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.
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.
Mantener un programa de administración de vulnerabilidad	3. Proteja los datos del titular de la tarjeta que fueron almacenados
Implementar medidas sólidas de control de acceso	4. Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.
Supervisar y evaluar las redes con regularidad	5. Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente.
Mantener una política de seguridad de información	6. Desarrollar y mantener sistemas y aplicaciones seguros
	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.
	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.
	12. Mantener una política que aborde la seguridad de la información para todo el personal

**OWASP y
PCI-DSS**

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. <input checked="" type="checkbox"/>
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. <input checked="" type="checkbox"/>
Mantener un programa de administración de vulnerabilidad	3. Proteja los datos del titular de la tarjeta que fueron almacenados
Implementar medidas sólidas de control de acceso	4. Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.
Supervisar y evaluar las redes con regularidad	5. Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente.
Mantener una política de seguridad de información	6. Desarrollar y mantener sistemas y aplicaciones seguros 
	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.
	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.
	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

6. Desarrollar y mantener sistemas y aplicaciones seguros

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.	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.
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.	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.
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.	6.5.c Verifique que los procesos implementados protejan las aplicaciones, al menos, contra las siguientes vulnerabilidades:
6.3.d Entreviste a los desarrolladores de software para verificar que se implementen los procesos de desarrollo de software escritos.	OWASP Top 10 de Riesgos de Seguridad en Aplicaciones
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: <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). 	

**OWASP y
PCI-DSS**

OWASP
The Open Web Application Security Project

**OWASP y
PCI-DSS**

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

Analysis of one of our larger datasets showed that 99% of malware hashes are seen for only 58 seconds or less. In fact, most malware was seen only once. This reflects how quickly hackers are modifying their code to avoid detection.

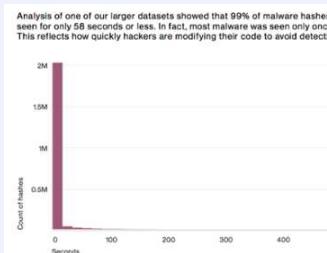


Figure 36.
Count of hashes by lifespan in seconds, (n=2.3 million)

La solución debe ser preventiva!

(fuente: Verizon Data Breach Report 2016)

**OWASP y
PCI-DSS**

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



La solución debe ser preventiva!

(fuente: Symantec)

**OWASP y
PCI-DSS**

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



Time Category	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 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 y
PCI-DSS**

La solución debe ser preventiva!

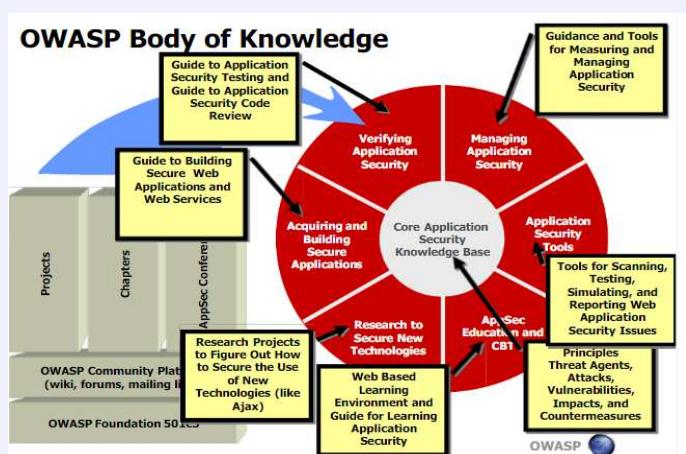
- Aprender
- Practicar
- Perfeccionarse



**OWASP y
PCI-DSS**

Aprender y Perfeccionarse

OWASP Body of Knowledge



The diagram illustrates the OWASP Body of Knowledge structure. At the center is the "Core Application Security Knowledge Base". Surrounding it are eight segments, each with associated resources:

- Verifying Application Security**: Associated with "Guide to Application Security Testing and Guide to Application Security Code Review".
- Managing Application Security**: Associated with "Guidance and Tools for Measuring and Managing Application Security".
- Application Security Tools**: Associated with "Tools for Scanning, Testing, Simulating, and Reporting Web Application Security Issues".
- Ap. Sec. Education and CBT**: Associated with "Principles, Threat Agents, Attacks, Vulnerabilities, Impacts, and Countermeasures".
- Research to Secure New Technologies**: Associated with "Research Projects to Figure Out How to Secure the Use of New Technologies (like Ajax)".
- Acquiring and Building Secure Applications**: Associated with "Guide to Building Secure Web Applications and Web Services".
- Web Based Learning Environment and Guide for Learning Application Security**: Associated with "OWASP Foundation 501(c)3".
- Projects**: Associated with "Chapters", "AppSec Conferences", and "OWASP Community Platform (wiki, forums, mailing lists)".

Qué dice la ley chilena?

OWASP
The Open Web Application Security Project

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 y PCI-DSS

OWASP
The Open Web Application Security Project

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](#)



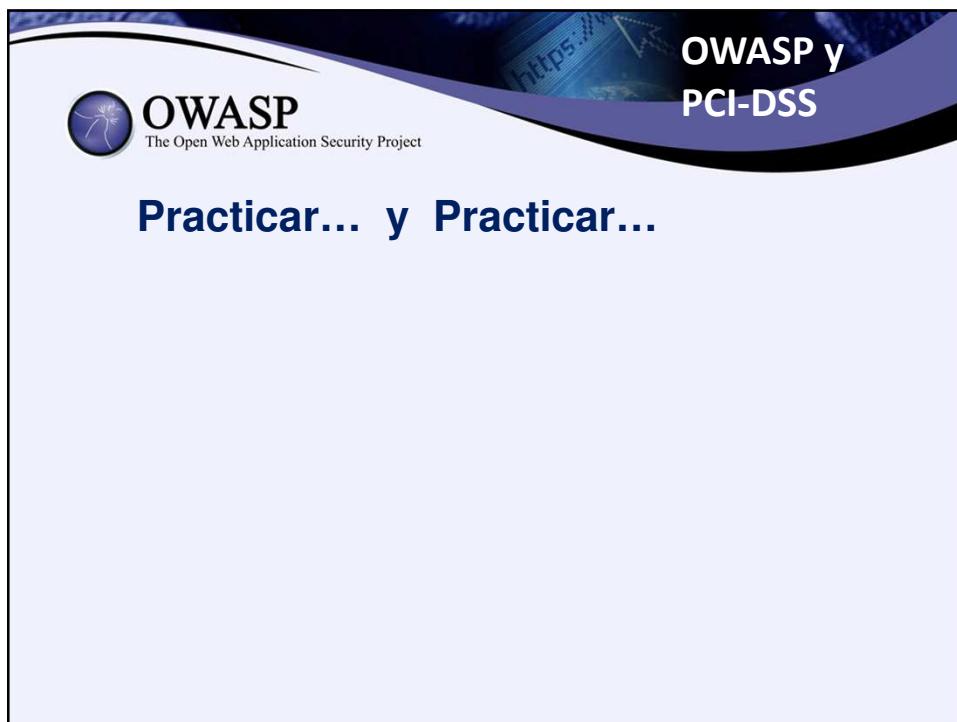
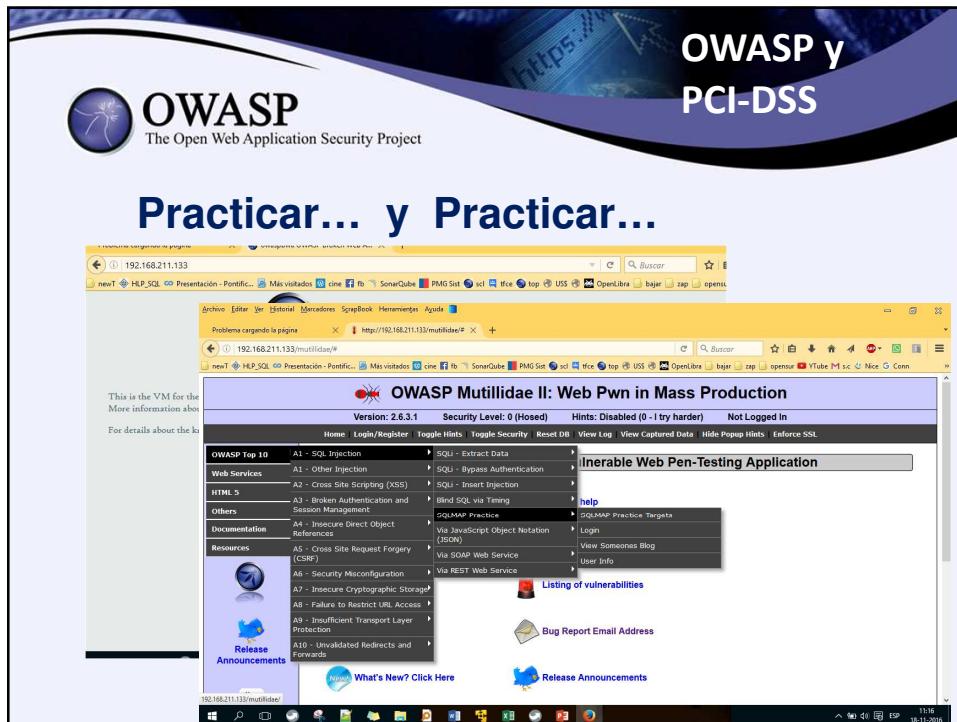
OWASP Vulnerable Web Applications Directory Project

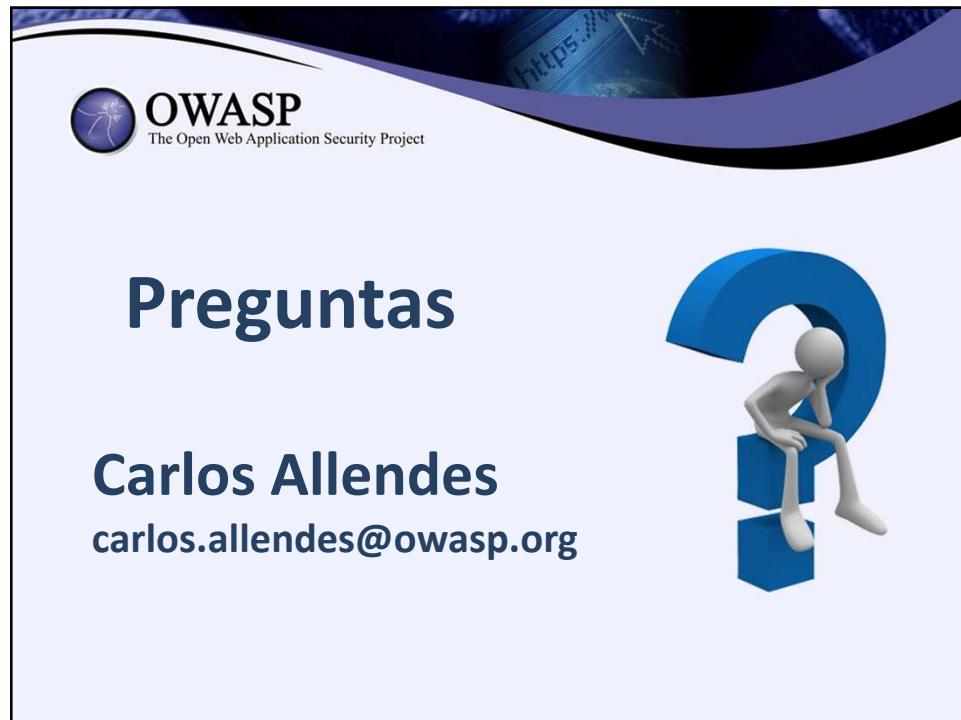
What is VWAD?
[\[editar | editar código \]](#)

OWASP VWAD project

Tipos	Cantidad
VM_ISO	21
OnLine_Apps	24
OffLine_Apps	42
Total general	87

Tipos	Cantidad
VM_ISO	21
OnLine_Apps	24
OffLine_Apps	42
Total general	87





The banner features the OWASP logo (a blue circle with a white stylized 'W') and the text "OWASP" in a large, bold, blue sans-serif font. Below it, in a smaller, smaller blue font, is "The Open Web Application Security Project". The background of the banner is a dark blue gradient with a subtle wavy pattern.

Preguntas

Carlos Allendes
carlos.allendes@owasp.org



A 3D white humanoid figure is sitting on a large, blue, blocky question mark. The figure is in a thinking pose, with one hand on their chin. The question mark is positioned to the right of the text block.