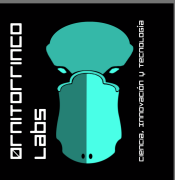


OWASP
The Open Web Application Security Project

Preparación para OWASP Top 10 - 2016



Sebastián Quevedo – Ornitorrinco labs
Sebastian@Ornitorrinco.cl



OWASP
The Open Web Application Security Project

Corporación Ornitorrinco Labs

Somos una organización sin ánimo de lucro dedicada a la investigación en Ciencia, Innovación y Tecnología

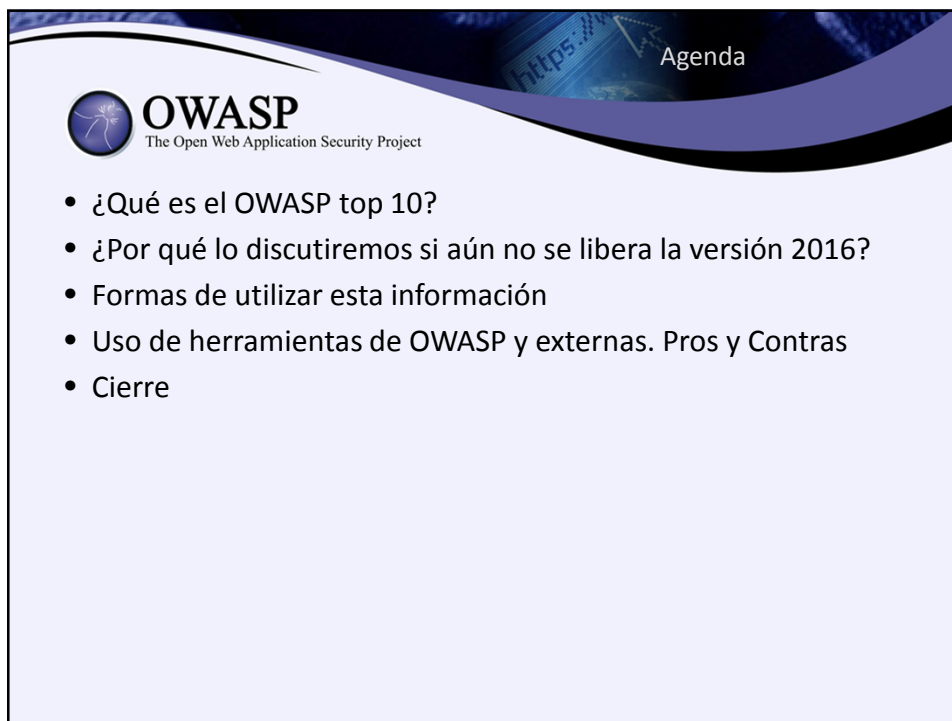
Líneas de investigación:

<ol style="list-style-type: none">1. CIBER RESILIENCIA2. INNOVACIÓN3. FÍSICA APLICADA	→	<ul style="list-style-type: none">▶ Seguridad de la Información/Ciberseguridad▶ Inteligencia de Seguridad▶ Análisis de Malware▶ Criptografía▶ Seguridad en Medios de Pago▶ Seguridad en Infraestructura Crítica▶ Seguridad en la Nube▶ Seguridad en IoT / Smart City
---	---	---


www.Ornitorrinco.cl
[@Ornitorrincolab](https://twitter.com/Ornitorrincolab)



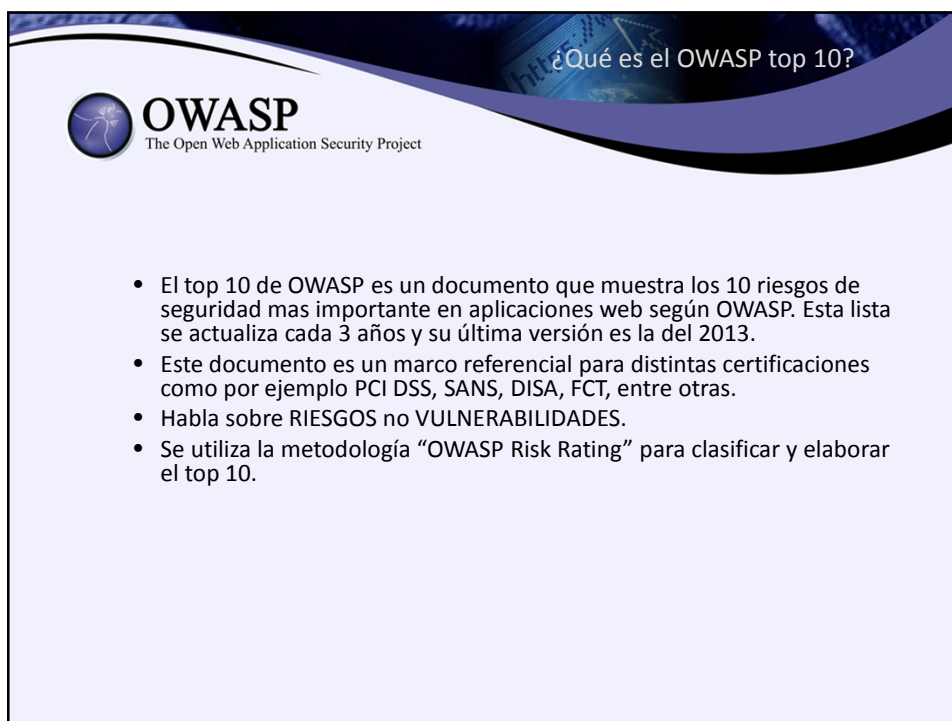
ORNITORRINCO
Labs
CIENCIA, INNOVACIÓN Y TECNOLOGÍA




Agenda

 **OWASP**
The Open Web Application Security Project

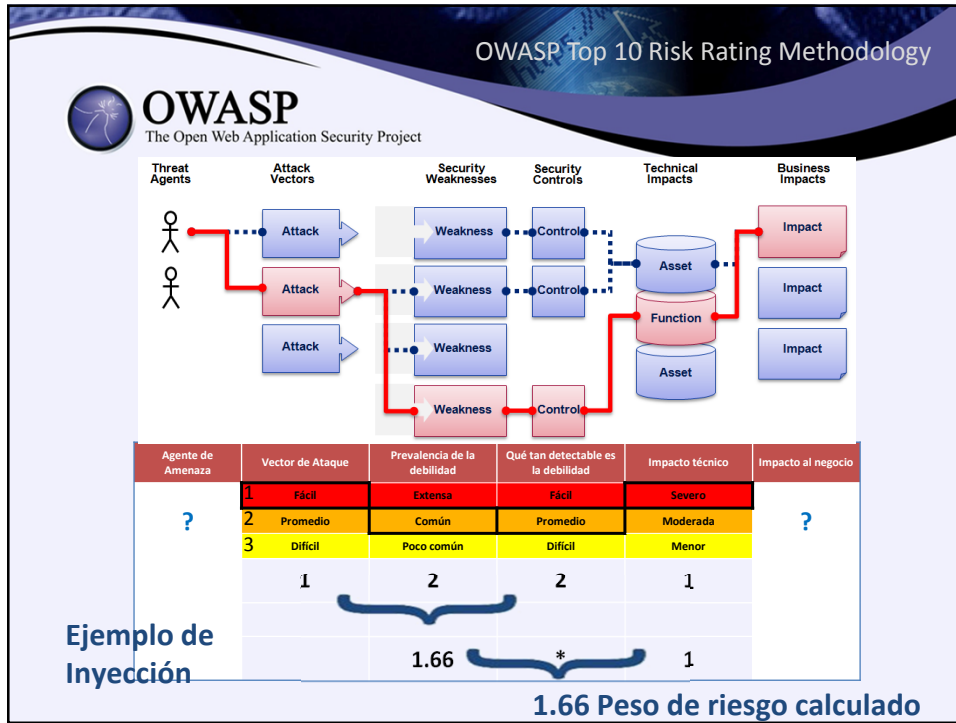
- ¿Qué es el OWASP top 10?
- ¿Por qué lo discutiremos si aún no se libera la versión 2016?
- Formas de utilizar esta información
- Uso de herramientas de OWASP y externas. Pros y Contras
- Cierre



¿Qué es el OWASP top 10?

 **OWASP**
The Open Web Application Security Project


- El top 10 de OWASP es un documento que muestra los 10 riesgos de seguridad mas importante en aplicaciones web según OWASP. Esta lista se actualiza cada 3 años y su última versión es la del 2013.
- Este documento es un marco referencial para distintas certificaciones como por ejemplo PCI DSS, SANS, DISA, FCT, entre otras.
- Habla sobre RIESGOS no VULNERABILIDADES.
- Se utiliza la metodología "OWASP Risk Rating" para clasificar y elaborar el top 10.



¿Qué es el OWASP top 10? – cont.

OWASP Top 10-2003	OWASP Top 10-2004	OWASP Top 10-2007	OWASP Top 10-2010	OWASP Top 10-2013
A1-Entrada no validada	A1-Entrada no validada	A1-Secuencia de comandos en sitios cruzados XSS	A1- Inyección	A1- Inyección
A2-Control de acceso interrumpido	A2-Control de acceso interrumpido	A2-Fallas de inyección	A2-Secuencia de comandos en sitios cruzados XSS	A2-Pérdida de autenticación y gestión de sesiones
A3-Administración de cuentas y sesión interrumpida	A3-Administración de autenticación y sesión interrumpida	A3-Ejecución de ficheros malintencionados	A3-Pérdida de autenticación y gestión de sesiones	A3-Secuencia de comandos en sitios cruzados XSS
A4-Fallas de cross site scripting XSS	A4-Fallas de cross site scripting XSS	A4-Referencia insegura y directa a objetos	A4-Referencia directa insegura a objetos	A4-Referencia directa insegura a objetos
A5-Desbordamiento de búfer	A5-Desbordamiento de búfer	A5-Falsificación de peticiones en sitios cruzados CSRF	A5-Falsificación de peticiones en sitios cruzados CSRF	A5-Configuración de seguridad incorrecta
A6-Fallas de inyección de comandos	A6-Fallas de inyección	A6-Revelación de información y gestión incorrecta de errores	6-Defectuosa configuración de seguridad	A6-Exposición de datos sensibles
A7-Problemas de manejo de errores	A7-Manejo inadecuado de errores	A7-Pérdida de autenticación y gestión de sesiones	A7-Almacenamiento criptográfico inseguro	A7-Ausencia de control de acceso a las funciones
A8-Uso inseguro de criptografía	A8-Almacenamiento inseguro	A8-Almacenamiento criptográfico inseguro	A8-Falla de restricción de acceso a URL	A8-Falsificación de peticiones en sitios cruzados CSRF
A9-Fallas de administración remota(no aplicable)	A9-Negación de servicio	A9-Comunicaciones inseguras	A9-Protección insuficiente en la capa de transporte	A9-Uso de componentes con vulnerabilidades conocidas
A10-Configuración indebida de servidor web y de aplicación	A10-Administración de configuración insegura	A10-Falla de restricción de acceso a URL	A10-Redirecciones y reenvíos no validados	A10-Redirecciones y reenvíos no validados


¿Qué es el OWASP top 10?



OWASP
The Open Web Application Security Project

- A1 - Inyección: Engañar una aplicación para que incluya comandos malintencionados que serán enviados al interprete de base de datos.
- A2 – Pérdida de Autenticación y gestión de sesiones: En HTTP las credenciales viajan con cada petición. Se debe usar TLS para cada autenticación. Existen muchas fallas correspondientes a este punto.
- A3 – Cross-Site Scripting: Se envía información de un atacante a una víctima mediante el navegador de esta. Se puede almacenar, reflejar en el input web o ser enviada de forma directa al cliente de JS.


¿Qué es el OWASP top 10?



OWASP
The Open Web Application Security Project

- A4 – Referencia insegura a objetos: Hace referencia a obligar a utilizar autorización apropiada a elementos y objetos, junto con A7.
- A5 – Configuración de seguridad Incorrecta: Puede afectar desde el SO hasta el servidor de aplicaciones. Sólo piense en todos los lugares que ha viajado su código fuente.
- A6 – Exposición de datos sensibles: No se identifica la información sensible de manera apropiada, su ubicación, dónde se envía o fallan las medidas de protección asociadas a estos puntos.

¿Qué es el OWASP top 10?



OWASP
The Open Web Application Security Project

- A7 – Ausencia de control de acceso a funciones: : Hace referencia a obligar a utilizar autorización apropiada a elementos y objetos, junto con A4.
- A8 – CSRF: Se engaña a una víctima para que introduzca un comando sobre un sitio vulnerable. La vulnerabilidad es causada por un navegador que introduce automáticamente datos de autenticación.
- A9 – Uso de componentes con vulnerabilidades conocidas: Permite explotación con herramientas automatizadas.

¿Qué es el OWASP top 10?



OWASP
The Open Web Application Security Project

- A10 – Redirecciones y envíos no válidos: Un atacante puede redirigir el tráfico de una víctima a voluntad.


FAILED OWASP TOP 10
How many apps fail the OWASP Top 10 upon initial risk assessment?



Industry	Percentage of Apps Failing
Financial Services	58%
Manufacturing	65%
Technology	68%
Healthcare	69%
Retail - Hospitality	70%
Government	76%


VERACODE

¿Por qué lo discutiremos si aún no se libera la versión 2016?



OWASP
The Open Web Application Security Project

- El campo de la seguridad evoluciona rápidamente, pero los riesgos del Top 10 no cambian sustancialmente año a año.
- Buscamos predecir que cambios podrían encontrarse en base a la experiencia en el área.
- OWASP Top 10 Proactive Controls.



OWASP
The Open Web Application Security Project

OWASP Top 10 Proactive Controls

	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 Components with Known Vulnerabilities	A10-Unvalidated Redirects and Forwards
C1: Verify for Security Early and Often	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
C2: Parameterize Queries	✓									
C3: Encode Data	✓		✓							
C4: Validate All Inputs	✓		✓							✓
C5: Implement Authentication Controls		✓								
C6: Implement Appropriate Access Controls				✓			✓			




OWASP
The Open Web Application Security Project

OWASP Top 10 Proactive Controls

C7: Protect Data						✓				
C8: Implement Logging and IDs	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
C9: Leverage Security Frameworks	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
C10: Error and Exception Handling	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Los controles proactivos de OWASP nos servirán, por tanto, para poder prepararnos frente al Top 10 presente y posteriores.



OWASP
The Open Web Application Security Project

¿Para qué podemos utilizar esta información?

- En primer lugar, cada diseño de seguridad de redes debe tomar esta lista en cuenta, y ser capaz de prevenir sus riesgos.
- Se usa como marco referencial para identificar los principales agentes de amenaza y vectores de ataque.
- Cada CIO u Oficial de Seguridad debería usar los top 10 de OWASP como referencia para su organización.
- Cada programador web debería verificar el top 10 de OWASP para prevenir las fallas explicitadas en el documento.


Herramientas de OWASP – Pros y Contras



OWASP
The Open Web Application Security Project


Alternativa de OWASP	Alternativa del mercado
OWASP ZAP	Burp Suite
OWASP WebScarab	Burp Suite
OWASP Cal9000	Múltiples
OWASP Pantera	OWASP ZAP / Acunetix / Otros
OWASP Mantra	Múltiples addons en Firefox
OWASP SQLiX	Sqlinja / SQLinjector
OWASP Wfuzzer	Wfuzz
OWASP LAPSE	Google CodeSearch

Demonstrations




OWASP
The Open Web Application Security Project

Para no apelar a los dioses de las demos en vivos, veamos los siguientes recursos:



OWASP
The Open Web Application Security Project

¡Gracias por su
atención!



MORNINGCO
Labs
ciencia. innovación y tecnología