



OWASP LatamTour
Chile 2013

OWASP BWA: Hacking the Web, como aprender y practicar sin terminar en la cárcel

Felipe Sánchez Fabre
Perito Informático – Especialista en Delitos Informáticos e Informática Forense
fsanchez@peritajesinformaticos.cl - fsanchez@fci.cl

 **OWASP**
The Open Web Application Security Project

 **OWASP**
LATAM TOUR 2013




About Me

 **OWASP**
The Open Web Application Security Project

- Felipe Sánchez Fabre fsanchez@fci.cl
 - Ingeniería de Ejecución en Computación e Informática – Universidad de Santiago de Chile.
 - Diplomado en Peritaje Informático – Universidad de Santiago de Chile.
 - Perito Informático – Academia Superior de Estudios Policiales, Policía de Investigaciones de Chile.
 - Diplomado en Criminalística y Metodología Forense – Universidad de Valparaíso.
 - Diplomado en Control, Seguridad y Auditoría Computacional – Universidad de Santiago de Chile.
 - Magister en Seguridad, Peritaje y Auditoría Procesos Informáticos - Universidad de Santiago de Chile (actualmente cursando 2do Año).
 - Perito Judicial Informático – Ilustres Cortes de Apelaciones de Santiago, Valparaíso, San Miguel y Rancagua.
 - Profesor Universidad de Santiago de Chile - Diplomado en Peritaje Informático. Cursos: "Peritaje Informático Avanzado" e "Informática Forense".
 - Profesor Universidad de Santiago de Chile – Ingeniería Informática (Civil y Ejecución). Curso: "Seguridad de la Información".
 - Socio de FCI - Prevención, Detección e Investigación de Delitos Informáticos.

 **Forensic & Cybercrime Investigation**

Temario



OWASP
The Open Web Application Security Project

Temario

- Realidad sobre seguridad en sitios web nacionales.
- Legislación Nacional sobre Delitos Informáticos.
- Análisis de Caso Real.
- Investigación de Delitos Informáticos.
- OWASP Top Ten 2010
- OWASP BWA (Broken Web Applications).
- Demostración de BWA
- Reflexiones Finales.

Realidad sobre seguridad en
sitios web nacionales



OWASP
The Open Web Application Security Project

"Hackean" sitio web oficial del Ministerio de Justicia

La intervención en la página se la atribuye la agrupación LulzSecPeru, quienes ya habían realizado la misma acción con diversos portales.

Emoi Lunes, 25 de Febrero de 2013, 23:53



Foto: Pantallazo página Ministerio de Justicia

SANTIAGO.- El sitio web oficial del Ministerio de Justicia de Chile fue víctima esta noche de un ataque cibernético, más conocido como "hacking".


Al ingresar a www.minjusticia.gob.cl es posible encontrarse con una foto y un mensaje que dice "Eso les pasa por meterse con nosotros , nada personal".

La intervención al sitio web se la atribuye la organización LulzSecPeru, quienes ya habían realizado esta misma acción con otros portales.

Incluso el mismo Ministerio de Justicia ya había sido víctima del "hacking" de LulzSecPeru. Ocurrió el pasado 5 de septiembre, donde publicaron un mensaje en contra de Sebastián Piñera. "A la mierda Piñera, estamos con ustedes", decía ese mensaje.

Acompañado de la imagen, se escucha una canción "villera" argentina. Además, en su [cuenta de Twitter](#) escribieron: "minjusticia.gob.cl/ #hacked #defaced".

Realidad sobre seguridad en sitios web nacionales




OWASP
The Open Web Application Security Project

10 DE FEBRERO DE 2013

Hackean sitio web de la Subsecretaría de Defensa Nacional

Sin embargo, este no fue el único sitio que sufrió ataques durante esta madrugada, ya que la Agrupación Nacional por la Tenencia Responsable de Armas (ANTRA) y otro sitio de Venezuela también fueron intervenidos por hackers.

por EL MOSTRADOR ✉ ENVIAR ✎ RECTIFICAR 🖨 IMPRIMIR



Un hacker, identificado como Rooterror, intervino este domingo el sitio web de la Subsecretaría de Defensa Nacional, el cual al ingresar se podía observar un fondo blanco más el mensaje dejado por el pirata cibernético.

Sin embargo, este no fue el único sitio que sufrió ataques durante esta madrugada, ya que la Agrupación Nacional por la Tenencia Responsable de Armas (ANTRA) y otro sitio de Venezuela también fueron intervenidos por hackers.

La Subsecretaría aún no entrega una versión oficial de lo ocurrido, mientras ya se restableció su sitio web.

Realidad sobre seguridad en sitios web nacionales



OWASP
The Open Web Application Security Project

14 de enero de 2013 • 22:48 • actualizado a las 01:24

Hackean sitios web del Ejército de Chile



Los sitios web del Ejército de Chile y de su Escuela de Suboficiales fueron hackeados la noche de este lunes.

El portal, al que se puede acceder a través de www.ejercitochile.cl o www.ejercitodechile.cl, apareció esta noche con fondo negro y un mensaje que dice "Hacked by LulzSecPeru".

Lo mismo ocurrió en la web de la Escuela de Suboficiales del Ejército, www.escueladesuboficiales.cl.

El grupo responsable de la vulneración sería el mismo que anteriormente intervino los sitios del Ministerio de Justicia y Chilevisión.

La situación generó diversos comentarios en las redes sociales.



Foto: Reproducción

Realidad sobre seguridad en sitios web nacionales



OWASP

The Open Web Application Security Project

POLÍTICA
Sábado 18 de agosto de 2012 / Las Últimas Noticias

“Me da lo mismo”, reaccionó Evelyn Matthei, una de las afectadas

Hackean web de la UDI y publican lista con celulares de ministros y políticos

“Somos ovejas descarriadas”, declaran los autores. “Nos querellaremos”, dice Patricio Melero.

SERGIO MARDONES

Un grupo de intrusos de la web, más conocidos como hackers, logró ingresar ayer al sitio de la UDI en Internet, del cual extrajo celulares, teléfonos y datos privados de casi todos los ministros del Gobierno, más el de la Primera Dama, de numerosos senadores y diputados de la Alianza y asesores de los mismos. La información fue hecha pública por Run Caos, que asegura así que 15 minutos de fama y está siendo replicada en las redes sociales, por “AML3K”. Los autores serían los mismos que el jueves hackearon la página de la Municipalidad de Santiago. El caso lo lleva la Brigada del Ciber Crimen de la PDI.

Los responsables del hackeo, @RunCaos, postearon por la tarde: “Somos ovejas descarriadas, ya que no seguimos al rezo, somos ‘diferentes’. Créame que se puede ser mejor, pero el que lo intenta es un ‘hacker’, ‘terrorista’, ‘comunista’. Atacamos al oficialismo porque



Emergencia o Servicio	EDUCACIÓN	División o separación	FELIPE BUENOS SERPANO	MINISTERIO	Cargo	MINISTRO
Teléfono						
Dirección						
Privada - Modificar - Ver más						
Nombre	EMERGENCIA	FELIPE KASTNER				
Emergencia o Servicio	MINYU	RECONSTRUCCION	CARGO			NO LO SE
Teléfono						
Dirección						
Modificar - Ver más						
Nombre	HACIENDA	FELIPE LARRAÍN BASCUNÁN				
Emergencia o Servicio		MINISTERIO	CARGO			MINISTRO
Teléfono						
Dirección						

son el gobierno actual”.

En la UDI, su presidente, Patricio Melero, acompañado por el subcomisario de la PDI Pablo Pereira, calificó el hackeo de “grave” y anticipó que el abogado Luis Hermsillo presentará el lunes una querrela. Contó también que ya algunos de los afectados habían recibido insultos anónimos y que perseguirán a quienes cometan “estos ilícitos informáticos”.

El subcomisario Pereira sostuvo que el hackeo se produjo alrededor de las 9 de la mañana de ayer. “Ya

Así se ve la información en la web.

contamos con datos importantísimos, que no podemos revelar”, mencionó, aunque en el listado aparece aún como ministro Felipe Buñes, por lo que no está muy actualizado. “Una de las afectadas fue Evelyn Matthei, ministra del Trabajo”. “Me da lo mismo, mi teléfono no tiene mucha gente”, dijo.

¿Acciones legales?

“Por lo menos yo... estoy en otra. No sé si es grave o no, pero yo no estoy complicada.

Mario Desobres, secretario general de RN, comentó: “Qué le va-

mos a hacer. Si alguien me llama para recordar algún pariente, yo les recordaré a los suyos. Espero si que cuando se dé con los autores, se publiquen sus direcciones para que se pueda ir a sus casas a verlos”.

Entre los grandes aparece José Hornaizal, encargado de Emergencias de la municipalidad de Recoleta. “Primera noticia que tengo. Tendré que informar a la administración”, dice. Sobre su presencia entre tanto político top, cree que “deben haberse cruzado las bases de datos”.

Realidad sobre seguridad en sitios web nacionales



OWASP

The Open Web Application Security Project

Hackean sitio web del organismo Anatel

Mensaje en la página web acusa al organismo de defender el modelo de televisión pagada para la televisión digital.

por La Tercera - 30/05/2012 - 16:48

LAS OPINIONES TIENEN UN PUNTO DE PARTIDA

Twitter (4)

Me gusta (1)

Post



El sitio web de la **Asociación Nacional de Canales de Televisión (Anatel)**, entidad que reúne a los canales de televisión abierta con cobertura nacional que operan en el país, fue hackeado durante esta tarde.

En la página se podía leer un mensaje donde se acusa al organismo de defender el modelo de televisión pagada para la televisión digital. “Nosotros como pobladores no dejamos fuera a los canales como Parinacota Tv, el Canal 2 de la Victoria, entre otros”, escribió el grupo que se denomina Audisoft hacker team.

Además, se podía ver una encuesta donde se instaba a que se contestara si las personas estaban de acuerdo en que se cobrara por la televisión digital.

Actualmente, no se puede ver el mensaje pues el sitio fue bajado.

Realidad sobre seguridad en sitios web nacionales

OWASP

The Open Web Application Security Project

Hackean página web de la Universidad Católica con sitios pornográficos

La casa de estudios superiores sufrió el ataque en su sitio de Internet que, aunque era casi imperceptible a la vista, fue ampliamente difundido a través de las redes sociales.

por La Tercera - 13/03/2012 - 10:02

LAS OPINIONES TIENEN UN PUNTO DE PARTIDA

27
 Me gusta 31
 0

La Pontificia Universidad Católica de Chile se transformó anoche en una nueva víctima de los ataques informáticos, puesto que cerca de la medianoche su página web sufrió el hackeo del código fuente de su portada, en la cual se pudo ver por un largo rato varios enlaces a sitios de pornografía.

Aunque el ataque era prácticamente imperceptible a la vista, pues los enlaces estaban ofrecidos a través de una fuente pequeña y en un lugar no muy visible, las redes sociales fueron las encargadas de difundirlo y convertir el hashtag #pornoUC en trending topic de Twitter.

Tras verificar el ataque, los encargados de la página web de la PUC bajaron el sitio por un par de horas, con un mensaje que señalaba que el sitio se encontraba en mantención, y durante la mañana ya estaba todo corregido.

Hasta ahora nadie se ha adjudicado públicamente el ataque.

Realidad sobre seguridad en sitios web nacionales

OWASP

The Open Web Application Security Project

Legend:
 H - Homepage defacement
 M - Mass defacement (click to view all defacements of this IP)
 R - Redefacement (click to view all defacements of this site)
 L - IP address location
 ★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★	Domain	OS	View
2013/03/14	Titsk Security Team	H	M	R			alphanetchile.cl	Linux	mirror
2013/03/14	cyber-hack security	H					colegiodeabogadosdeatacama.cl	Linux	mirror
2013/03/14	sultan - S11	H	M				10-0-d	Linux	mirror
2013/03/14	Index Php		M				www.nv.cl/index.php	Linux	mirror
2013/03/14	Index Php	H	M				santiagopropiedades.cl	Linux	mirror
2013/03/14	Index Php	H	M				www.elitewebdesign.cl	Linux	mirror
2013/03/14	Index Php	H	M				www.damasoguardo.cl	Linux	mirror
2013/03/14	Index Php	H	M				www.eliminaciondeacaros.cl	Linux	mirror
2013/03/14	Index Php	H	M				www.beckhaus.cl	Linux	mirror
2013/03/14	Index Php	H	M				www.caes.cl	Linux	mirror
2013/03/14	Index Php	H	M				www.animalia.cl	Linux	mirror
2013/03/14	Index Php	H	M				identifik.cl	Linux	mirror
2013/03/14	Index Php	H	M	R			bicentrega.cl	Linux	mirror
2013/03/14	Index Php	H	M				burgoseiri.cl	Linux	mirror
2013/03/14	Index Php	H	M				www.coeficiente.cl	Linux	mirror
2013/03/14	Hmei7		M				eder.d/x.htm	Linux	mirror
2013/03/13	TurkHackArmy		H				ecomadera.cl	Linux	mirror
2013/03/13	Hmei7						www.vallescosteros.cl/x.htm	Linux	mirror
2013/03/13	Hmei7						www.cooltv.cl/x.htm	Linux	mirror
2013/03/13	Hmei7						www.cedco.cl/x.htm	Linux	mirror
2013/03/13	Hmei7						www.florialisaromos.cl/x.htm	Linux	mirror
2013/03/13	Hmei7					R	radiobknes.cl/x.htm	Linux	mirror
2013/03/13	Hmei7						bioes.cl/x.htm	Linux	mirror
2013/03/13	Hmei7						www.productoracairoi.cl/x.htm	Linux	mirror
2013/03/13	Hmei7					M	officespa.cl/x.htm	Linux	mirror

Realidad sobre seguridad en sitios web nacionales




OWASP
The Open Web Application Security Project



Legend:
 H - Homepage defacement
 M - Mass defacement (click to view all defacements of this IP)
 R - Redefacement (click to view all defacements of this site)
 L - IP address location
 * - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	Domain	OS	View
2013/02/14	rooterror		M			www.ssffaa.gov.cl/wp-content/	Linux	mirror
2013/02/14	rooterror		M			www.ssffaa.gov.cl/wp-content/	Linux	mirror
2013/02/10	rooterror	H	M			www.ssdefensa.gov.cl	Linux	mirror
2013/02/10	rooterror	H	M			www.ssdefensa.gov.cl	Linux	mirror
2013/01/25	Sejeal					med.minjusticia.gov.cl/sejeal.jpg	Linux	mirror
2013/01/20	LUN4T1C00		M			gorev.gov.cl/x.txt	Linux	mirror
2013/01/20	LUN4T1C00		M			gorev.gov.cl/x.txt	Linux	mirror
2013/01/20	LUN4T1C00		M			gorevalparaiso.gov.cl/x.txt	Linux	mirror
2013/01/20	LUN4T1C00		M			gorevalparaiso.gov.cl/x.txt	Linux	mirror
2013/01/12	KriptekS	M	R			www.mcdonalds.cl/trabzonx.html	Unknown	mirror
2013/01/07	Sejeal					rpc.minjusticia.gov.cl/sejeal.jpg	Linux	mirror
2013/01/06	HighTech	H	M			sgs.dellibertador.gov.cl	Linux	mirror
2013/01/06	HighTech	H	M			intranet.dellibertador.gov.cl	Linux	mirror
2013/01/06	HighTech	H	M			sgs.gorehiggins.gov.cl	Linux	mirror
2013/01/06	HighTech	H	M			www.gorehiggins.gov.cl	Linux	mirror
2013/01/06	HighTech	H	M			db.gorehiggins.gov.cl	Linux	mirror
2013/01/06	HighTech	H	M			w.dellibertador.gov.cl	Linux	mirror
2013/01/06	HighTech	H	M			intranet.gorehiggins.gov.cl	Linux	mirror
2013/01/06	HighTech	H	M			www.dellibertador.gov.cl	Linux	mirror
2013/01/06	HighTech	H	M			www.dellibertador.gov.cl	Linux	mirror
2013/01/06	HighTech	H	M			intranet.gorehiggins.gov.cl	Linux	mirror
2013/01/06	HighTech	H	M			sgs.dellibertador.gov.cl	Linux	mirror
2013/01/06	HighTech	H	M			sgs.gorehiggins.gov.cl	Linux	mirror
2013/01/06	HighTech	H	M			w.gorehiggins.gov.cl	Linux	mirror
2013/01/06	HighTech	H	M			w.dellibertador.gov.cl	Linux	mirror

Legislación Nacional sobre Delitos Informáticos



OWASP
The Open Web Application Security Project

Ley 19.223

Tipifica figuras penales relativas a la Informática

Análisis de la Ley


- Sujeto activo
- Parte Subjetiva
- Parte Objetiva
- Figuras Penales

- 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

Análisis de Caso Real




OWASP
The Open Web Application Security Project

Byond Hacker Team

- Conformado por 2 adultos y 2 menores de edad.
- Uno de los imputados señalo **“que él realizaba “defacements”** en español, “desfaces” lo cuál constituiría un desfiguramiento de las páginas Web, un cambio al index, en donde los archivos se reemplazaban y se sustituían las imágenes, siendo esto una rama de la actividad de los hackers. A su vez, también indicó que **los fallos, serían errores de programación en las páginas, algo así como una ventana abierta por dónde podían ingresar.** El “index” vendría a ser la cara representativa visual de lo que se ve al abrir una página de Internet, un archivo de la raíz del portal Web que se encuentra en el servidor.”


Realidad sobre seguridad en sitios web nacionales



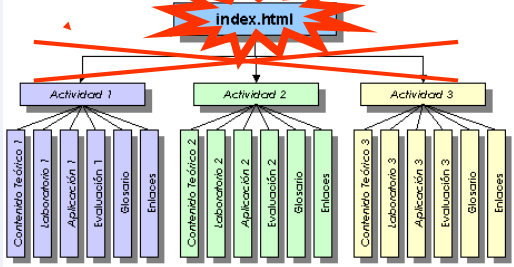
OWASP
The Open Web Application Security Project

Defacement

<http://www.ventas.cl>




**No a la guerra!!!
Si a la paz mundial!!!**



```

graph TD
    Index[index.html] --> A[Actividad 1]
    Index --> B[Actividad 2]
    Index --> C[Actividad 3]
    A --> A1[Contenido Teórico 1]
    A --> A2[Laboratorio 1]
    A --> A3[Aplicación 1]
    A --> A4[Evaluación 1]
    A --> A5[Glosario]
    A --> A6[Enlaces]
    B --> B1[Contenido Teórico 2]
    B --> B2[Laboratorio 2]
    B --> B3[Aplicación 2]
    B --> B4[Evaluación 2]
    B --> B5[Glosario]
    B --> B6[Enlaces]
    C --> C1[Contenido Teórico 3]
    C --> C2[Laboratorio 3]
    C --> C3[Aplicación 3]
    C --> C4[Evaluación 3]
    C --> C5[Glosario]
    C --> C6[Enlaces]
  
```

Análisis de Caso Real




OWASP
The Open Web Application Security Project

Beyond Hacker Team

- Tercer Tribunal de Juicio Oral en lo Penal de Santiago, con fecha 14 de mayo de 2007.
- A) Que se condena a Imputado 1 y Imputado 2, ya antes individualizados, a sufrir la pena de tres años de presidio menor en su grado medio, a las accesorias de suspensión de cargo u oficio público durante el tiempo de la condena y al pago de las costas de la causa, **como autores del delito reiterado de sabotaje informático; ilícito tipificado y sancionado en el artículo 1º inciso primero de la Ley Nº19.223**, cometidos con fechas 18 al 22 de noviembre del 2005, y durante el año 2006.

Investigación de Delitos Informáticos



OWASP
The Open Web Application Security Project


Código Procesal Penal

Artículo 314. Inciso segundo.

Procederá el informe de peritos en los casos determinados por la ley y siempre que **para apreciar algún hecho o circunstancia relevante para la causa fueren necesarios o convenientes conocimientos especiales de una ciencia, arte u oficio.**

Perito Publico	Perito Privado
<ul style="list-style-type: none"> • Funcionario Publico. • Dependiente de un organismo público (Ej. Policías, Ministerio Publico, y Servicio Médico Legal). • Sueldo cancelado por el organismo publico al cual pertenece. 	<ul style="list-style-type: none"> • Profesional en libre ejercicio de la profesión. • Honorarios cancelados por la parte de solicita sus servicios.

Investigación de Delitos Informáticos




OWASP
The Open Web Application Security Project

Código Procesal Penal

Artículo 222. Inciso quinto.
“... un listado actualizado de sus rangos autorizados de direcciones IP y un registro, **no inferior a un año, de los números IP de las conexiones que realicen sus abonados.**”

Artículo 295.
Libertad de prueba. Todos los hechos y circunstancias pertinentes para la adecuada solución del caso sometido a enjuiciamiento podrán ser **probados por cualquier medio producido** e incorporado en conformidad a la ley.

Investigación de Delitos Informáticos



OWASP
The Open Web Application Security Project

ISO 27.037 “Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence”

Propone directrices para el tratamiento de la evidencia digital, específicamente para la identificación, recolección, adquisición y preservación.

Abarca diversos tipos de dispositivos o funciones para diversas circunstancias, tales como:

- Dispositivos de almacenamiento secundario (discos duros, pendrive, memorias flash, etc.)
- Dispositivos portables (smartphones, tables, GPS).
- Video vigilancia o CCTV (DVR)
- Transmisiones por redes de datos.



OWASP
The Open Web Application Security Project

OWASP Top Ten 2010

El objetivo del proyecto Top 10 es crear conciencia sobre la seguridad en aplicaciones mediante la identificación de algunos de los riesgos más críticos que enfrentan las organizaciones.

Top 10 de riesgos, no el Top 10 de las debilidades más comunes.

Actualmente se encuentra la versión 2013 en etapa de comentarios.

https://www.owasp.org/index.php/Top_10

A1 – Inyección	A6 – Defectuosa configuración de seguridad
A2 – Secuencia de comandos en sitios cruzados (XSS)	A7 – Almacenamiento Criptográfico Inseguro
A3 – Pérdida de Autenticación y Gestión de Sesiones	A8 – Falta de Restricción de Acceso a URL
A4 – Referencia Directa Insegura a Objetos	A9 – Protección Insuficiente en la capa de Transporte
A5 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	A10 – Redirecciones y Reenvíos no validados

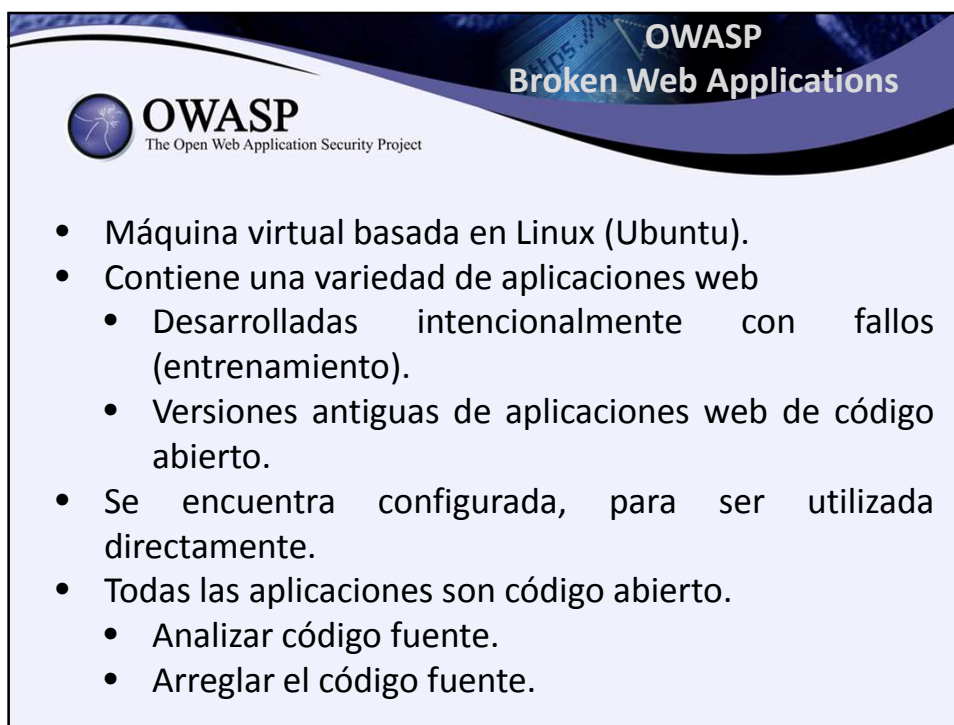


OWASP
The Open Web Application Security Project


OWASP Broken Web Applications

Este proyecto consiste en una máquina virtual en la que se ejecutan una variedad de aplicaciones web con vulnerabilidades conocidas, para quienes estén interesados en temas como:


- Aprender sobre seguridad de aplicaciones web
- Pruebas manuales de evaluación de técnicas
- Pruebas de herramientas automatizadas, Pruebas sobre herramientas de análisis de código
- Analizar ataques web
- Probar WAFs (Web Application Firewall) y tecnologías similares.



OWASP
Broken Web Applications

 **OWASP**
The Open Web Application Security Project

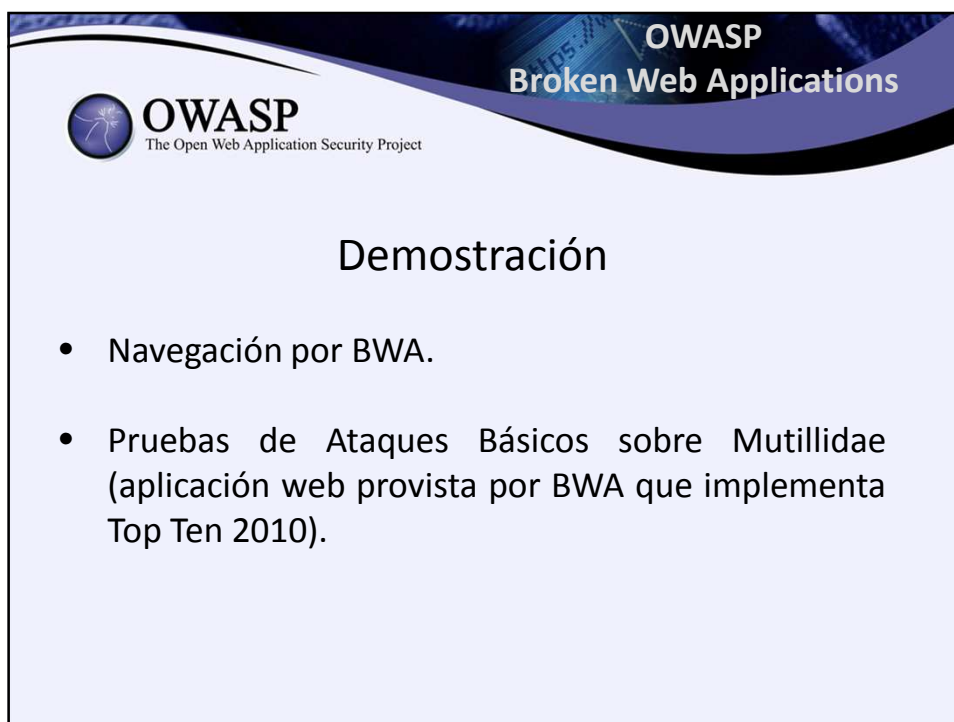
- Máquina virtual basada en Linux (Ubuntu).
- Contiene una variedad de aplicaciones web
 - Desarrolladas intencionalmente con fallos (entrenamiento).
 - Versiones antiguas de aplicaciones web de código abierto.
- Se encuentra configurada, para ser utilizada directamente.
- Todas las aplicaciones son código abierto.
 - Analizar código fuente.
 - Arreglar el código fuente.



OWASP
Broken Web Applications

 **OWASP**
The Open Web Application Security Project

- Máquina virtual en formato VMware.
- Se puede utilizar con VMPlayer (gratuito).
- Entre los software instalados destacan: Apache, PHP, Perl, MySQL, Tomcat, OpenJDK y Mono.
- Archivos Log se encuentran en las ubicaciones por omisión.
- Actualmente se encuentra disponible la versión 1.0
- https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project



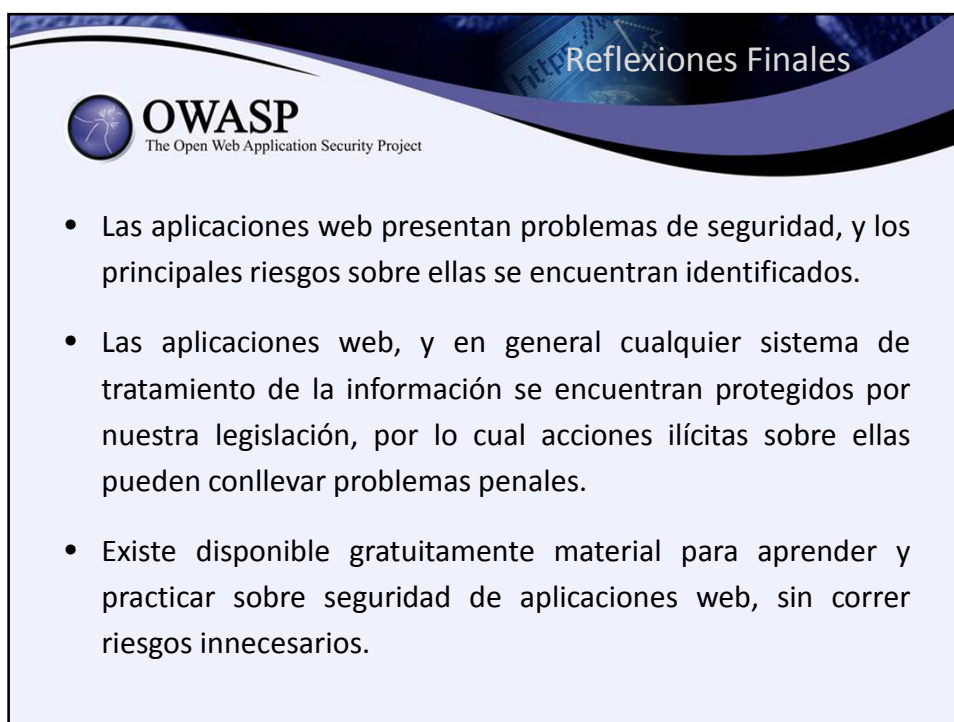
The slide features a blue header with the OWASP logo on the left and the text "OWASP Broken Web Applications" on the right. The main content area is white with a light blue background. The title "Demostración" is centered. Below it is a bulleted list of two items.

OWASP
The Open Web Application Security Project

OWASP
Broken Web Applications

Demostración

- Navegación por BWA.
- Pruebas de Ataques Básicos sobre Mutillidae (aplicación web provista por BWA que implementa Top Ten 2010).



The slide features a blue header with the OWASP logo on the left and the text "OWASP Reflexiones Finales" on the right. The main content area is white with a light blue background. The title "Reflexiones Finales" is centered. Below it is a bulleted list of three items.

OWASP
The Open Web Application Security Project

OWASP
Reflexiones Finales

Reflexiones Finales

- Las aplicaciones web presentan problemas de seguridad, y los principales riesgos sobre ellas se encuentran identificados.
- Las aplicaciones web, y en general cualquier sistema de tratamiento de la información se encuentran protegidos por nuestra legislación, por lo cual acciones ilícitas sobre ellas pueden conllevar problemas penales.
- Existe disponible gratuitamente material para aprender y practicar sobre seguridad de aplicaciones web, sin correr riesgos innecesarios.

