



La Fundación OWASP

El proyecto abierto de seguridad en aplicaciones Web (OWASP por sus siglas en inglés) es una comunidad abierta y libre de nivel mundial enfocada en mejorar a la seguridad en las aplicaciones de software. Nuestra misión es hacer la seguridad en aplicaciones "visible", de manera que las organizaciones pueden hacer decisiones informadas sobre los riesgos en la seguridad de aplicaciones. Todo mundo es libre de participar en OWASP y en todos los materiales disponibles bajo una licencia de software libre y abierto. La fundación OWASP es una organización sin ánimo de lucro 501c3 que asegura la disponibilidad y apoyo permanente para nuestro trabajo.



Comunidad OWASP

La comunidad OWASP ofrece muchas oportunidades para compartir y aprender acerca de Seguridad en Aplicaciones.

- 110+ Capítulos Locales en el Mundo
- Conferencias Mundiales, OWASP Days y Eventos de Capacitación
- OWASP Podcasts
- AppSec Videos y Presentaciones
- Application Security Moderated News Feed
- OWASP Newsletter
- AppSec Job Board
- OWASP Application Security Research Grants

Proyectos OWASP (140+)

Proteger:

OWASP Development Guide
OWASP Enterprise Security API (ESAPI)
OWASP AntiSamy Java & .NET Projects

Detectar:

OWASP Top 10
OWASP Application Security Verification Standard Project
OWASP Live CD
OWASP WebScarb
OWASP Code Review Guide
OWASP Testing Guide
Ciclo de Vida del SW:

OWASP Web Goat
OWASP AppSec FAQ Project
OWASP Legal Project

Te hacemos la más cordial invitación para que colabores en el contenido del **Newsletter**. Mándanos tu artículo A manuel.lopez@owasp.com, en español o en inglés.



Contenido:

Taller en el DivecFest—
"Universidad de Guadalajara" 2

OWASP Guadalajara—
Primera Reunión de
Capítulo 2

Proyecto OWASP del
Mes 3

OWASP-Google Summer of Code 3

OWASP Alrededor del
Mundo 4

Libro del Mes 4

Every Major Credit
Card Provider Is Potentially Hacked Right
Now 5

Taller en el DivecFest—"Universidad de Guadalajara"

Por Manuel López Arredondo
OWASP Leader

La Universidad de Guadalajara por medio del Centro Universitario de Ciencias Exactas e Ingenieras (CUCEI) invitó a OWASP Guadalajara para participar en el DivecFest 2012 realizado el 20 de Marzo de 2012.

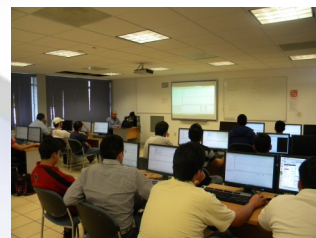
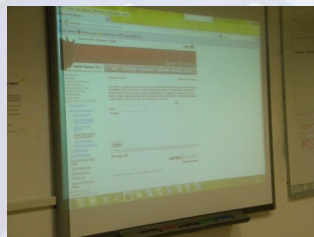
Tuvimos la oportunidad de conocer estudiantes de la Licenciatura en Informática así como de la Ingeniería en Sistemas.

Como en cada reunión, les comentamos a los estudiantes qué es OWASP y cuál es nuestra misión como organización global.

Posteriormente, comenzamos con el tema central del taller basándonos en el OWASP Top Ten y explicando los conceptos principales de los ataques de SQL injection y Cross-Site Scripting (XSS).

Inmediatamente después comenzamos la sesión práctica utilizando

WebGoat, PAROS Proxy y las OWASP Cheat Sheets. Con la ayuda de las herramientas los estudiantes aprendieron no sólo cómo se llevan a cabo estos ataques sino también, y más importante, cómo protegerse de ellos.



Fue una gran sesión! Esperemos ver de nuevo a muchos de esos estudiantes en nuestras siguientes sesiones.

OWASP Guadalajara—Primera Sesión de Capítulo

Por Manuel López Arredondo
OWASP Leader

El pasado 2 de Marzo de 2012, OWASP Guadalajara llevó a cabo su primera reunión de capítulo, la cual tuvo como casa a la American Society of Jalisco. Tuvimos oportunidad de conocer colegas de la industria de Seguridad Informática con deseos de incrementar su conocimiento y de aportar su experiencia.

Durante la primera parte de la reunión discutimos acerca de OWASP y de las actividades que estamos realizando en el capítulo Guadalajara; para después dar paso al tema principal de la sesión que fue el discutir acerca de los

recientes ataques de Anonymous. Principalmente de Lulzsec.

Este grupo hacktivista explotó vulnerabilidades de SQL Injection en sitios web de TELCEL (La compañía de teléfonos celulares más grande de México) y la Secretaría de Educación Pública (Departamento dependiente del Gobierno Mexicano), para ganar acceso a información confidencial de sus empleados y después publicarla en la Web.

Comentamos acerca de las técnicas utilizadas y realizamos una demostración de éste ataque por medio de WebGoat y Paros; del mismo modo analizamos la herramienta utilizado por Anonymous-

Lulzsec para explotar la vulnerabilidad de SQL Injection.

Al final de la sesión recibimos varios comentarios valiosos por parte de los asistentes que enriquecieron la reunión y también nos ayudarán para realizar con mayor éxito nuestras siguientes juntas de capítulo.

Gracias a todos los asistentes y mantente al tanto de nuestras siguientes sesiones.



Contenido:

Taller en el DivecFest—
"Universidad de Gua-
dalajara" 2

OWASP Guadalajara—
Primera Reunión de
Capítulo 2

Proyecto OWASP del
Mes 3

OWASP-Google Sum-
mer of Code 3

OWASP Alrededor del
Mundo 4

Libro del Mes 4

Every Major Credit
Card Provider Is Poten-
tially Hacked Right
Now 5

Proyecto OWASP del Mes—WebGoat

Por Manuel López Arredondo
OWASP Leader

Con el objetivo de dar a conocer a nuestra comunidad los diferentes Proyectos OWASP, éste espacio lo estaremos dedicando para describir un proyecto cada mes. Hoy es la oportunidad de WebGoat!

Dentro de las categorías de proyecto de OWASP, WebGoat está catalogado dentro de "Life Cycle". Es una aplicación desarrollada en J2EE y se hizo con la intención de que sea insegura con la finalidad de dar lecciones de Seguridad en Aplicaciones Web.

En cada lección los usuarios deben de demostrar su entendimiento del tema explotando una vulnerabilidad dentro de la aplicación. Por ejemplo, en el tema de SQL Injection, el usuario debe de explotar ésta vulnerabilidad con las técnicas aprendidas para robar números de tarjetas de crédito ficticios.

Dado que la seguridad en aplica-

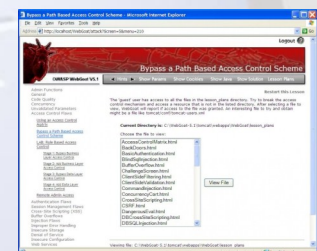
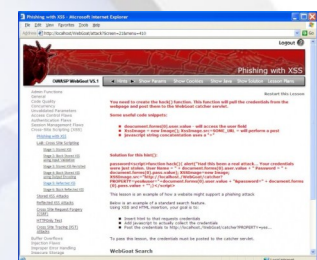
ciones Web es complicada de aprender sin la práctica y tomando en cuenta que muchos profesionales de Seguridad requieren realizar sus prácticas en ambientes legales antes de hacerlos en algún ambiente productivo, WebGoat cubre todas éstas necesidades dentro de un ambiente totalmente legal.

Actualmente hay más de 30 lecciones en WebGoat que cubren los siguientes temas:

- Cross-site Scripting (XSS)
- Access Control
- Thread Safety
- Hidden Form Field Manipulation
- Parameter Manipulation
- Weak Session Cookies
- Blind SQL Injection
- Numeric SQL Injection
- String SQL Injection
- Web Services
- Fail Open Authentication
- Dangers of HTML Comments
- Y muchas más ...

Baja la aplicación y comienza a

practicar desde ahora; también puedes bajar el código y modificarlo, mejorarlo, adecuarlo; **SIN COSTO!** La liga es: https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project



OWAP-Google Summer of Code

Hace unos días se envió a nuestra lista de distribución el comunicado para participar en el Google Summer of Code en donde OWASP fue invitado a participar como organización para ofrecer mentoría.

Si eres estudiante Universitario, te invitamos a participar de ésta iniciativa en alguno de los siguientes proyectos de OWASP:

- OWASP Enterprise Security API (ESAPI) Project
- OWASP AntiSamy.Net Project
- OWASP Zed Attack Proxy Project

- OWASP AppSensor Project

Las propuestas deben de ser enviadas antes del 6 de abril al buzón gsoc@lists.owasp.org.

Los beneficios que puedes tener al ser estudiante:

- Experiencia internacional al trabajar directamente con los líderes de proyecto de OWASP alrededor del mundo.
- Armar tu Curriculum Vitae con miras a enrolarte en el mercado laboral.

- Reconocimiento Internacional al haber aportado mejoras a un proyecto OWASP.

Visita la página:
https://www.owasp.org/index.php/Category:OWASP_Project

Evalúa los proyectos y participa en el que más te guste! No dejes pasar ésta gran oportunidad!

En caso de dudas acércate a los líderes del Capítulo Guadalajara quienes te orientaremos.



Contenido:

Taller en el DivecFest—
"Universidad de Gua-
dalajara" 2

OWASP Guadalajara—
Primera Reunión de
Capítulo 2

Proyecto OWASP del
Mes 3

OWASP-Google Sum-
mer of Code 3

OWASP Alrededor del
Mundo 4

Libro del Mes 4

Every Major Credit
Card Provider Is Poten-
tially Hacked Right
Now 5

OWASP Alrededor del Mundo

OWASP en el PenTesting Magazi- ne

Tom Brennan, miembro del conse-
jo de dirección internacional de
OWASP, fue entrevistado para la
revista PenTest; se tocaron temas
referentes a la participación de
OWASP con otras organizaciones
de Seguridad a nivel internacional,
recursos de aprendizaje en temas
de seguridad en aplicaciones desa-
rrollados por OWASP, Proyectos
OWASP y muchos temas más; el
número de la revista lo puedes
encontrar en la siguiente liga:

[https://www.owasp.org/
images/9/9f/
WEB_APPC_PENTESTING_03_2012.
pdf](https://www.owasp.org/images/9/9f/WEB_APPC_PENTESTING_03_2012.pdf)

Únete a las reuniones del capítu- lo OWASP Austin por GoToMee- ting

El capítulo de OWASP Austin se
reúne cada último Viernes de mes
de 11:30 AM a 1:00 PM CST. Los
datos para que te unas a sus sesio-
nes son:

[https://www3.gotomeeting.com/
join/730456806](https://www3.gotomeeting.com/join/730456806)

"Use your microphone and
speakers (VoIP) - a headset is re-
commended. Or, call in using your
telephone"

Access Code: 730-456-806

Audio PIN: Shown after joining the
meeting

Meeting ID: 730-456-806

Buscando Teachers para el pro- yecto OWASP HackingLabs

El Hacking Lab es un Proyecto que
tiene como objetivo ofrecer un
ambiente real para realizar prue-
bas de penetración a la aplicación;
hay un sistema de puntos y cada
usuario va ganando puntos de
acuerdo a: 1) la vulnerabilidad que
explotaron; 2) la explicación pro-
porcionada para explotar dicha
vulnerabilidad; 3) los controles
sugeridos para que ésta vulnerabi-
lidad no aparezca en sitios web.

El Proyecto OWASP HackingLabs

está en búsqueda de "Teachers"
para validar los resultados que
envían los usuarios del sitio.

Si estás interesado en participar
acércate a los líderes del Capítulo
Guadalajara y con gusto te apoya-
remos.

Reuniones de OWASP alrededor del Mundo

Global AppSec AsiaPac 2012— Abril
11 a Abril 14— Sydney, Australia

Global AppSec Research 2012—
Julio 10 a Julio 13—Atenas, Grecia

Global AppSec North America 2012
Oct 22 a Oct 26—Austin, Texas

Global AppSec Latin America
2012—Nov 14 a Nov 16—Buenos
Aires, Argentina

Detalles en:

[https://www.owasp.org/
index.php/
Cate-
gory:OWASP_AppSec_Conference](https://www.owasp.org/index.php/Cate-gory:OWASP_AppSec_Conference)

Libro del Mes—OWASP AppSensor

Te invitamos a que leas un libro al
mes con el objeto de ir incremen-
tando el conocimiento en materia
de Seguridad Informática.

El libro OWASP AppSensor es un
marco conceptual que ofrece una
guía para implementar capacida-
des de detección de intrusiones en
la capa de aplicación utilizando
controles estándares de seguridad
y recomendaciones para respuesta
automática basado en políticas
que diseñan con base a un patrón

particular. Al utilizar AppSensor,
la aplicación será capaz de identi-
ficar usuarios maliciosos dentro de
la aplicación y eliminar la amena-
za respondiendo con una acción
predeterminada como: terminar la
sesión del usuario, bloquear la
cuenta o notificar al administra-
dor.

En muchas ocasiones un atacante
requiere numerosas pruebas e
intentos de ataques antes de ex-
plotar una vulnerabilidad dentro

de la aplicación; con AppSensor es
posible identificar y eliminar la
amenaza del atacante antes de
que éste pueda comprometer el
sitio de forma exitosa.

Te invitamos a descargar el libro
de forma gratuita en:

[http://www.lulu.com/shop/owasp-
foundation/owasp-appsensor/
ebook/product-17489823.html](http://www.lulu.com/shop/owasp-foundation/owasp-appsensor/ebook/product-17489823.html)



Contenido:

Taller en el DivecFest—
"Universidad de Gua-
dalajara" 2

OWASP Guadalajara—
Primera Reunión de
Capítulo 2

Proyecto OWASP del
Mes 3

OWASP-Google Sum-
mer of Code 3

OWASP Alrededor del
Mundo 4

Libro del Mes 4

Every Major Credit
Card Provider Is Potentially Hacked Right
Now 5

Every Major Credit Card Provider Is Potentially Hacked Right Now

I would like to share with you the recent attack suffered by Global Payments.
By Eduardo Cerna
OWASP Leader

Recently, Global Payments, a major credit card processing company, has reportedly been hacked. That means each of the four major credit card companies, and according to reports, as many as 10 million customers are at risk.

The story has been developing throughout the morning. Right now, it goes like this: Hackers gained access to an administrative-privileged account at a New York City taxi company and, over the course of several months, stole 10 million credit card numbers. They've been sitting on them, waiting to spend all at once to maximize the time before they're shut down.

The Wall Street Journal puts the number of compromised accounts around 50,000, which is a far cry from 10 million. The massive number had originally been sourced to a post from a Gartner analyst, and while it seems a little far fetched that a cab company would have millions of numbers, we'd still err to caution.

"Visa has recently been notified by a third-party processor that they have detected a security breach within their payment-processing network," Visa said in a memo to banks.

MasterCard and Visa both stressed that their networks weren't compromised in the breach.

"The investigation is still in the early stages and if additional accounts are determined to be at risk" additional alerts will be distributed, Visa said.

Hack Attack

Some recent and large examples of data breaches

COMPANY	DATE	INCIDENT
Global Payments	January - February 2012	Details unknown, estimated 50,000 card accounts at risk
Citigroup	May 2011	Card numbers, names, email addresses from 360,000 accounts
*Epsilon Data Management	April 2011	Customer names, email addresses accessed
Heartland Payment Systems.	January 2009	Card numbers, expiration dates, internal bank codes stolenn
TJX Cos.	January 2007	Up to 90 million credit, debit card numbers stolen
CardSystems Solutions	June 2005	40 million cards exposed

*unit of Alliance Data Systems Corp.



Para mayor información
contacta a los Líderes del
Capítulo Guadalajara

Eduardo Cerna
eduardo.cerna@owasp.org

Manuel López Arredondo
manuel.lopez@owasp.org

Membresías


Sé parte de OWASP, hazte miembro HOY!

Individual:

50 USD anuales

<http://www.regonline.com/Register/Checkin.aspx?EventID=919827>

Beneficios:

- Kit de Bienvenida:
 - Un Sticker de OWASP
 - Maleta de OWASP 
- Una cuenta de email con el dominio @owasp.org
- Participación directa en alguno(s) de los 140+ proyectos de OWASP
- Incrementar tu red de contactos
- Descuentos en Conferencias “OWASP Day” y “AppSec” alrededor del mundo
- Obtén experiencia profesional reconocida internacionalmente al participar en OWASP.

OWASP Guadalajara—Beneficios

- Reuniones Trimestrales
- Lista de Distribución
- Foro abierto de Discusión
- Conocer Colegas de la Industria de InfoSec
- Concientización en la seguridad de WebApp en Guadalajara
- Proyectos Locales de OWASP?
- Libre y Abierto para cualquiera
- No presentaciones de ventas
- Hackfests y Docsfests
- OWASP Training Days vía GoToMeeting y presenciales (https://www.owasp.org/index.php/OWASP_Training)
- 1 crédito para CISSP, CISA, CEH, etc por cada reunión