Introducción a OWASP

Ing. Camilo Fernandez
Consultor en Seguridad Informática
Octubre, 2010
cfernandez@develsecurity.com

OWASP

The OWASP Foundation
http://www.owasp.org

¿Que es OWASP?

- Open Web Application Security Project
  - Sin fines de lucro, organización de voluntarios
    - Todos los miembros son voluntarios
    - Todo el trabajo es donado por los patrocinadores
  - Proporcionar recursos gratuitos para la comunidad
    - Publicaciones, artículos, normas
    - Software de Testeo y Capacitación
    - Capítulos locales & Listas de correo
  - Soportada a través de patrocinios
    - Apoyo financiero a través de empresas o patrocinadores
    - Patrocinios personales de los miembros

¿Que es OWASP?

- Open Web Application Security Project
  - Promueve el desarrollo de software seguro
  - Orientada a la prestación de servicios orientados a la Web
  - Se centra principalmente en el "back-end" mas que en cuestiones de diseño Web
  - Un foro abierto para el debate
  - Un recurso gratuito para cualquier equipo de desarrollo de software

¿Que ofrece OWASP?

- Materiales de Educación
  - OWASP Top 10
  - Guía de Desarrollo OWASP
  - Guía de Testing OWASP
  - Guía OWASP para aplicaciones Web Seguras
  - Muchos mas
- Software
  - WebGoat
  - WebScarab
  - ESAPI
  - Muchos mas
- Capítulos Locales
  - Comunidades interesadas en Seguridad de Aplicaciones

¿Que ofrece OWASP?

- Desarrollo de nuevos proyectos
  - Posibilidad de utilizar las herramientas y colaboradores disponibles para generar nuevos proyectos

- Becas de Investigación
  - OWASP otorga becas a investigadores de la seguridad en aplicaciones para desarrollar herramientas, guías, publicaciones, etc.

Mas de $100,000 USD han sido otorgados al día de hoy en becas de investigación

Publicaciones OWASP

Mayores Publicaciones

TOP 10 vulnerabilidades de aplicaciones Web

Guía de desarrollo Seguro de aplicaciones Web

Guía de testeo de aplicaciones Web

Proyecto legal

Proyecto de métricas y medidas

AppSec FAQ

Publicaciones OWASP

- Características comunes
  - Todas las publicaciones están disponibles gratuitamente en http://www.owasp.org
  - Son liberadas bajo las licencias de "Lesser" GNU Public License agreement, o la GNU Free Documentation License (GFDL)
  - Documentos Vivos
    - Actualizados según sea necesario
    - Proyectos consecutivos

Publicaciones OWASP – TOP 10

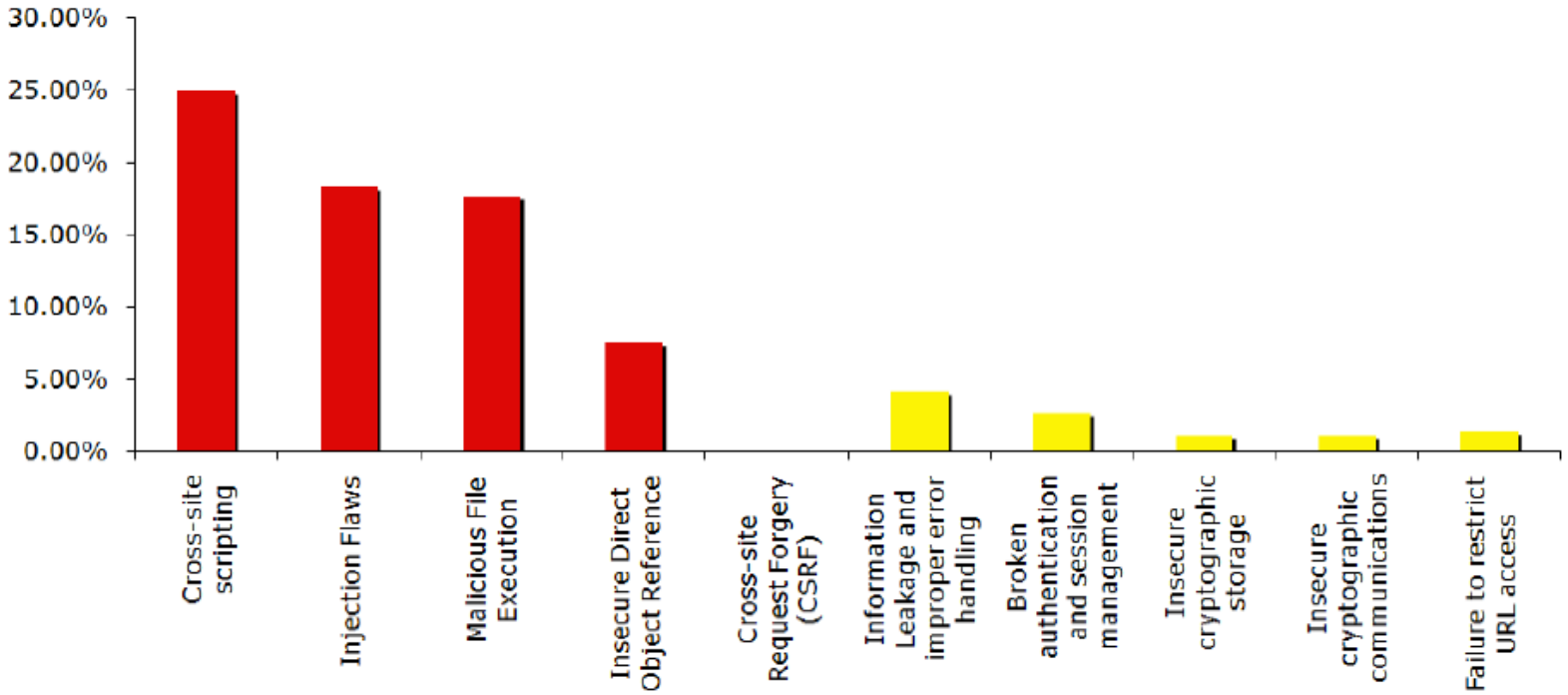
- Top 10 Web Application Security Vulnerabilities
  - Lista del TOP 10 de fallas de seguridad
  - Actualizada cada año
  - Dirigida a fallos de aplicaciones en el perímetro externo (Web)
  - Ampliamente aceptada por la industria
    - Federal Trade Commission (US Gov)
    - US Defense Information Systems Agency
    - VISA (Cardholder Information Security Program)
  - Fuerte presentación como Estándar (SANS)

Publicaciones OWASP – TOP 10

- Fallos de Seguridad Actuales
  - A1. Cross Site Scripting (XSS)
  - A2. Fallas de Infección (SQL)
  - A3. Ejecución de Archivos (RFI)
  - A4. Referencia Directa a Objetos (DOR)
  - A5. Falsificación de Petición (CSRF)
  - A6. Gestión Incorrecta de Errores (php, db, aspx, asp)
  - A7. Autentificación y Gestión de Sesiones (cookies)
  - A8. Almacenamiento inseguro (Texto Claro)
  - A9. Comunicaciones inseguras (HTTP)
  - A10. Restricción de acceso a URL ´ s

Publicaciones OWASP – TOP 10

- Convalidado con MITRE



Publicaciones OWASP – Guía de desarrollo

- Guía para el desarrollo Web seguro
  - Provee una guía **BASE** para el desarrollo Web
    - Introducción general a la seguridad
    - Introducción a seguridad a nivel de aplicación
    - Discute varias áreas clave de implementación
      - Arquitectura
      - Autenticación
      - Manejo de Sesión
      - Controles de Acceso y Autorización
      - Registro de Eventos
      - Validación de Datos

Publicaciones OWASP – Guía de Testeo

- Guía para el Testeo de Aplicaciones Web
  - Provee una guía de mejores practicas para la auditoria (PenTesting) de aplicaciones Web
    - Describe los ataques mas comunes (con ejemplos)
    - Define las fases de una auditoria
    - Discute varias áreas como lo son:
      - Footprinting
      - Fingerprinting (Sistemas Operativos)
      - Descubrimientos de Puertos
      - Descubrimiento de Aplicaciones
      - Identificación de Puntos de Entrada
      - Enumeración de Usuarios

OWASP Software

Mayores Aplicaciones

WebGoat

WebScarab

.Net Projects

oLab Projects

OWASP Software - WebGoat

- WebGoat
  - Principalmente una aplicación Educativa
  - Provee
    - Una base de prueba para encontrar fallos de seguridad.
    - Un conjunto de fallos de aplicación en una misma aplicación.
  - Que es?
    - Una aplicación en J2EE organizada en Lecciones de Seguridad
    - Basada en Tomcat y JDK 1.5
    - Orientada al aprendizaje
      - Fácil de Utilizar
      - Ilustra escenarios reales
      - Enseña ataques y soluciones viables

OWASP Software - WebGoat

- WebGoat – Que puedes aprender?
  - Un numero constante de ataques y soluciones
    - Cross Site Scripting
    - Inyección SQL
    - Inyección XPath
    - Manipulación de Parámetros
    - Robo de Sesión
    - Mecanismos de autentificación débil
  - En donde lo adquiero
    - http://www.owasp.org/software/webgoat.html
    - Descarga, Descomprime, Ejecuta!

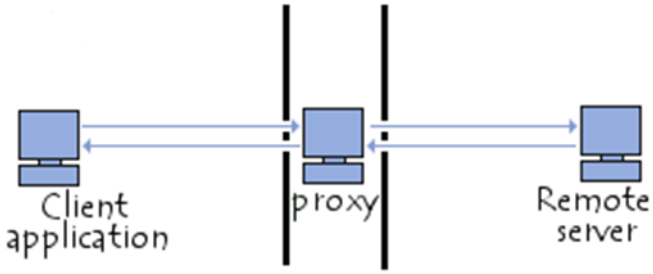
OWASP Software - WebScarab

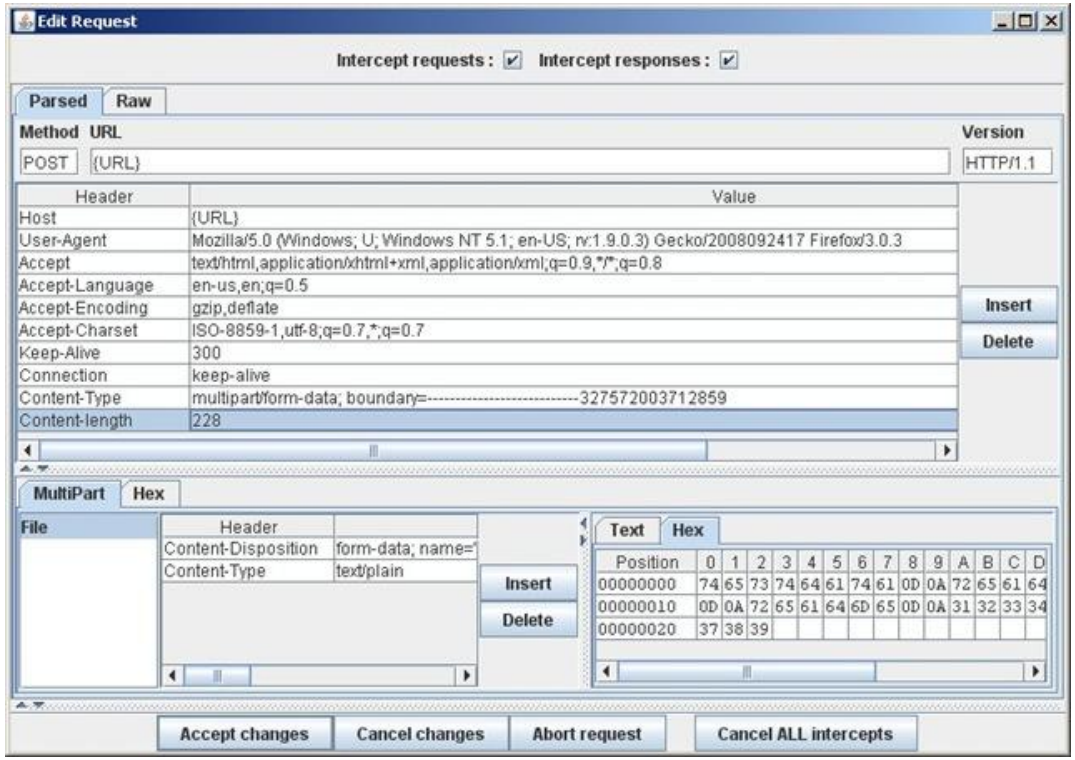
- WebScarab
  - Un Framework para analizar trafico HTTP/HTTPS
  - Desarrollado en Java
  - Usos Múltiples
    - Desarrollador: Debug entre el cliente y el servidor
    - Analista de Seguridad: Analizar trafico para identificar vulnerabilidades
  - Herramienta Técnica
    - Orientada a Desarrolladores
    - Extendible mediante plugins
    - Open Source
    - Bastante potente
  - En donde la consigo ?
    - http://www.owasp.org/software/webscarab.html

OWASP Software - WebScarab

- Que puede hacer?
  - Características
    - Análisis de Fragmentos – extrae scripts y HTML como lo obtiene el navegador, antes de ser renderizado por el mismo
    - Proxy – Observa el trafico entre el navegador y el servidor, Habilidad de modificar la información en transito, expone campos escondidos
    - Spider – identifica nuevos URL´s dentro de la pagina Web
    - Análisis de SessionID – Análisis y recopilación de Cookies

OWASP Software - WebScarab





OWASP Chapters Locales

- Creando Comunidades
  - Proveen oportunidades para compartir ideas y aprender sobre seguridad informática
  - Abiertos para cualquiera:
    - (Neewbie – Master Hax0r)
  - Provee un foro para discusiones
  - Oportunidad de presentar nuevas ideas y proyectos
  - Reuniones Periódicas
  - Listas de Correo
  - Ambientes Neutrales de Vendedores
  - Café Gratis!!!

OWASP Chapters Locales

- Un par de Reglas!

Lets keep it professional!

  - Nada de preguntas de
    - "Como hackeo una cuenta de Hotmail"
    - "Como entro a la computadora de mi exnovia"
    - "Como crackeo la WEP de mi vecino"

  - Nada de ventas o marketing en las listas de correos

Preguntas

- Alguna pregunta?

- Presentación estará disponible en:
  http://www.owasp.org/index.php/Guatemala

- Mailing List:
  https://lists.owasp.org/mailman/listinfo/owasp-spain

Gracias por su atención!
Visiten www.owasp.org