

The Open Web Application Security Project

Aplicación práctica y perspectivas educativas

Msc. Helios Mier Castillo
helios@seguridadyprivacidad.org





Agenda

- Breve presentación
- Necesidad y Justificación
- ¿Cómo participar?
- Publicaciones y Proyectos
- Organización del conocimiento
- En la práctica profesional
- White hats vs Black hats
- Conclusiones



Acerca de OWASP

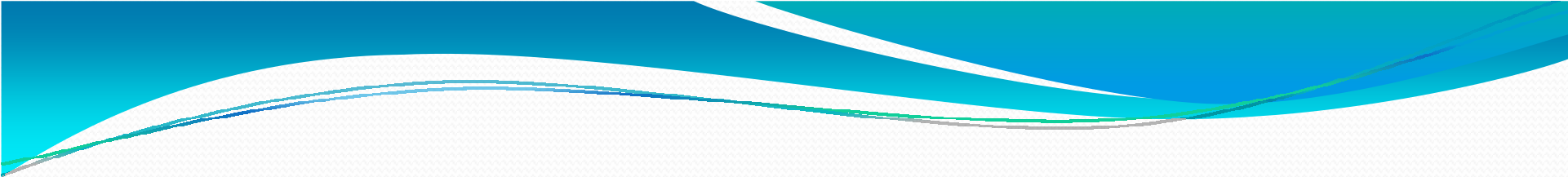
- Creada en Septiembre de 2001 en USA.
- Agrupa más de 100 capítulos locales en todo el mundo y miles de profesionistas a través de foros en internet.
- Desde 2008 se reconoce como una referencia estándar de facto en la industria del desarrollo de software.
- Es un proyecto muy joven comparado con otros del ramo, pero se ha convertido en uno muy importante que debe de tomarse en cuenta.



Necesidad

- Las aplicaciones basadas en Web se conforman de varias tecnologías y de distintos proveedores.
- Cada tecnología en particular tiene sus propias vulnerabilidades y fortalezas.
- Por la filosofía de crear sistemas basados en capas, una sola aplicación contiene los riesgos de todos sus componentes.
- Un solo sistema será muy fuerte en un punto, pero puede ser frágil en otro.
- Siempre se están descubriendo nuevas vulnerabilidades.

9 USUARIO	6 USUARIO	Todo el factor de la naturaleza humana
8 POLITICA	5 POLITICA	Regulaciones, políticas, reglamentos, Procesos, modelos, estándares, etc..
7 APLICACION	4 APLICACION	Aplicación y reglas de negocio. Todos los Programas que usamos o hacemos
6 PRESENTACION		Transporte y representación de datos: ej. Protocolo HTTP, SQL, etc.
5 SESION		Comunicaciones entre cliente-servidor: Ej. NETBIOS, SOAP, ORB, RPC, etc.
4 TRANSPORTE	3 TRANSPORTE	Enlace punto a punto y confiabilidad en Los mensajes: Protocolo TCP/UDP
3 RED	2 INTERNET	Identificación y localización: Protocolo IP
2 ENLACE	1 RED	Conexión entre dispositivos: Ethernet, 802.11x, Bluetooth
1 FISICA		Movimiento de bits: Señales eléctricas, Señales de radio, señales de luz.

- 
- Un sistema expuesto en el internet se enfrenta a numerosos atacantes.
 - Si el sistema tiene una vulnerabilidad, es una cuestión de tiempo antes de que alguien la encuentre.
 - Los atacantes van desde adolescentes inmaduros sin nada mejor que hacer, criminales con o sin experiencia, hasta espionaje corporativo o político.
 - Siempre habrá una razón por la que alguien quiera atacar un sitio.



La amenaza y los intrusos

- Es un rol que siempre existe a considerar:
 - Factor accidental o incidental.
 - Factor humano o tecnológico,
 - Factor Interno o externo.
 - Factor inocente o malicioso.
 - Factor directo o indirecto.
 - Factor visible o invisible.
- No es cuestión de cuándo, sino de cómo.
- Siempre será por el punto más débil.

9 USUARIO	Actividades en lugares prohibidos, abuso de privilegios, fuga de Información. Ingeniería Social.
8 POLITICA	Actividad en lugares prohibidos, abuso de cuentas y contraseñas, Abuso y explotación de la falta de preparativos de seguridad.
7 APLICACION	Manipulación de protocolo stateless, Inyección de SQL, Manipulación De funciones de aplicación, explotación de errores de diseño
6 PRESENTACION	Analizadores de vulnerabilidades, explotación de errores de Configuración de servicios.
5 SESION	Analizadores de vulnerabilidades, ataques de adivinación de cuentas Y contraseñas, errores de configuración de servidores.
4 TRANSPORTE	Barrido de puertos, Session hijacking, abuso y explotación de Servicios y protocolos obsoletos. BandwidthRaep
3 RED	Ataques conocidos a las vulnerabilidades de TCP/IP, Negación de servicio, IP address abuse. Man in the Middle.
2 ENLACE	Acceso personal a dispositivos, ataques conocidos basicos (ARP Spoofing, Blue Smack), Ataques pasivos (Sniffers)
1 FISICA	Intrusión personal, acoplamiento de equipo renegado, accesos A deshoras, actividad en lugares prohibidos. TEMPEST



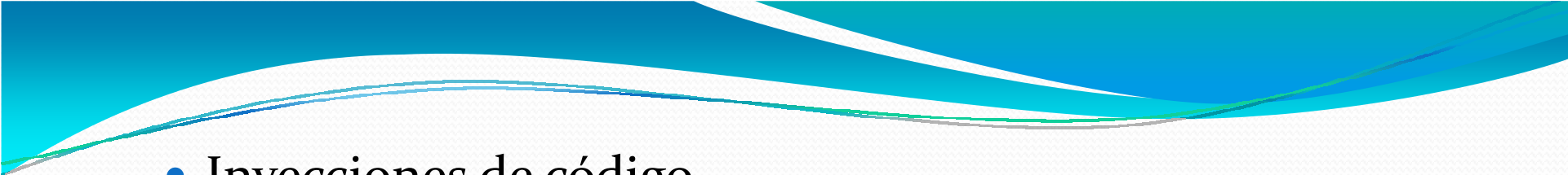
La educación de los ingenieros

- ¿Cuántos planes de estudio integran una temática completa de lo que necesitan saber de seguridad?
 - Administración de servicios de red
 - Administración de bases de datos
 - Arquitectos de software y programadores
- En la escuela no alcanza el tiempo para enseñar todo lo que se necesita saber.
- Obliga a que el profesionalista busque capacitación por su cuenta, pero ¿Dónde? Y ¿de qué?



Base de Conocimiento OWASP

- Tópicos específicos:
 - Principios de codificación segura
 - Modelado de amenazas
 - Manejo de dinero electrónico y transferencias bancarias.
 - Phishing
 - Seguridad de Servicios Web
 - Mecanismos de Autenticación y pruebas de identidad.
 - Manejo de sesiones de usuario
 - Autorización y mecanismos de control.
 - Validación de datos de entrada.

- 
- Inyecciones de código
 - Canonicalización y codificación de caracteres.
 - Administración y auditoría de bitácoras (log)
 - Administración de errores y fail-safes.
 - Control de archivos y material subido por el visitante.
 - Buffer overflow, administración de memoria, bandwidth
 - Control de acceso a subsistemas de administración.
 - Cifrado de llave pública y privada, PKI.
 - Administración de la configuración.
 - Mantenimiento de hardware y software.
 - Ataques de Negación de Servicio (Local, de red, remota, distribuida, voluntaria, slashdoteo)

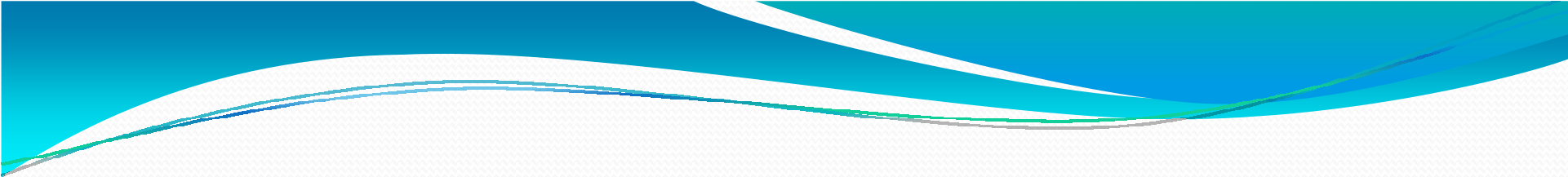
Aprendiendo

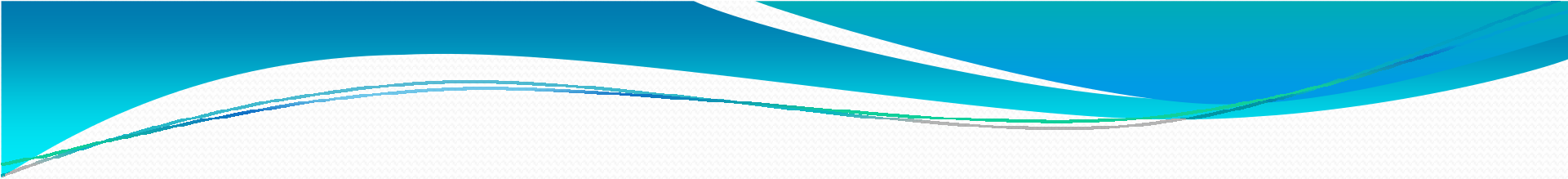
- Los tópicos que abarca OWASP cubren cientos de horas de teoría. Y ponerlos en práctica y dominarlos mucho más.
- Prácticamente hay una carrera completa en cuanto a tiempo de estudio necesario.
- El contenido se puede considerar de nivel intermedio a avanzado.
- Cambia constantemente en su aplicación debido a la aparición de nuevas tecnologías y productos.
- Debate: ¿Enseñar a los alumnos los patrones desde inicio o corregir estilos después?



Publicaciones y proyectos

- OWASP Guide
 - Todo el compendio de conocimiento
- OWASP Code Review Project
 - Guías para a inspección de código
- OWASP Top 10
 - Análisis detallado de las 10 principales amenazas vigentes observadas “in the wild”.
- OWASP Application Security Verification Standard
 - Realización de inspecciones de las aplicaciones.
- OWASP Testing Guide & Metrics
 - Guías para procesos de pruebas de calidad.

- 
- WebGoat
 - Una aplicación de entrenamiento para probar y entender las vulnerabilidades y los ataques a nivel de aplicación.
 - Validation filters
 - Colección de códigos y scripts para realizar validaciones de entradas contra ataques conocidos.
 - WebScarab
 - Herramienta de apoyo para localizar y analizar vulnerabilidades.
 - AntiSamy
 - API para validar contra ataques de Cross Site Scripting.

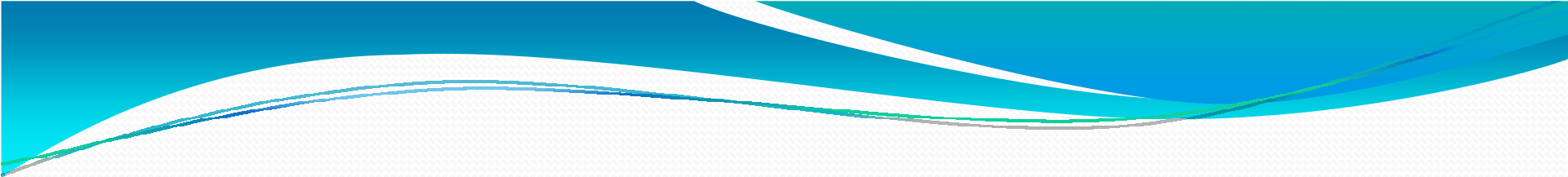
- 
- Mod_Security & Core Rule Set
 - Un firewall/IPS a nivel de aplicación, para reforzar a nivel de capa 6 las reglas de seguridad en comunicaciones que una aplicación envía al servidor.
 - OWASP Live CD
 - Herramientas de análisis.
 - OWASP Enterprise Security API (ESAPI)
 - Una librería completa de código listo para ser usado en backends y frontends.

OWASP Top 10 – revisión 2010

- A1 – Inyección de código
 - Introducir maliciosamente en una aplicación texto malformado que el motor del sistema interpretará como instrucciones válidas.
- A2 – Cross Site Scripting (XSS)
 - Introducción de texto malformado que se hace llegar hasta la víctima para que sea interpretado como código.
- A3 – Mala administración de autenticación y sesiones
 - Aprovecharse maliciosamente de errores de control de identidad derivados de un mal manejo de una sesión del usuario. Recordar que HTTP es un protocolo sin estado.

A4 – Acceso directo a objetos y referencias

- Manipular el request que se le envía al servidor y la aplicación para obtener comportamiento que no estaba originalmente a nuestro alcance.
- A5 – Cross Site Request Forgery (CSRF)
 - Un sitio malicioso que puede enviar peticiones a otro sitio aprovechándose de no validar una sesión por ventana de navegador abierta.
- A6 – Errores de configuración de infraestructura.
 - Vulnerabilidades de sistema desde la red hasta el servidor del sistema de aplicaciones.
- A7 – Errores de almacenamiento criptográfico.
 - Error en el diseño de la estructura de datos para ocultar la verdadera información sensible ala vista de extraños.
 - *Tomar nota de la existencia de la Ley de Protección de Datos

- 
- A8 – Error de restricción de acceso por URL.
 - Manipular las peticiones al servidor para obtener acceso a archivos o comandos que no le pertenecen al visitante.
 - A9 – Protección de datos insuficiente de TLS/SSL
 - Transmisión incompleta de datos sensibles por canales cifrados. Mal aplicación de SSL.
 - A10 – Redirecciones sin validación.
 - Falta de control entre los orígenes y destinos del flujo de trabajo de un usuario, o la manipulación de parámetros para engañar a un usuario que vaya a un sitio erróneo.

¿cómo participar?

- Cualquiera puede acceder a los materiales y proyectos, ¡son open source! . www.owasp.org
 - En múltiples idiomas, los pueden difundir.
- Asistan a eventos y reuniones locales.
 - Próximo: OWASP Day México Nov/2011 en Ags.
- Voluntariado organizando grupos de estudio.
- Unirse a los foros y listas de distribución.
- Apoyando económicamente:
 - Membresía voluntaria anual US\$50.00 dls y donativos
- Colaborar en un proyecto.



Black Hat vs White Hat

- La seguridad informática es una carrera de conocimiento y de aplicación.
 - Realmente deberías de estar preocupado si no sabes que hacer, y más cuando sabes y no lo haces.
- OWASP lista los ataques y mecanismos de protección más comunes que todo profesional de tecnología de información debe de conocer.
- Existen disponibles mucha información para atacar y herramientas, black hats tienen la ventaja.



The Low Hanging Fruit

- Revisar las noticias de hacks notables: grandes y pequeñas empresas han caído.
- Defender un sistema realmente es más difícil que atacarlo.
- Hay una gran cantidad de sistemas que tienen al menos una falla. Ninguno es perfecto.
- Sistemas bajo medida son los que tienen una mayor probabilidad de tener una vulnerabilidad.
- Todos pueden llegar a caer, pero vemos que muchos se caen de un estornudo.

Conclusiones

- OWASP prácticamente es toda una profesión. Es la base de conocimientos mas sólidos que hay de una forma práctica.
- Todos los conceptos se deben incluir en un proyecto desde su fase de planeación, sin que te los pida el cliente.
- La meta es una: que un sistema pueda sobrevivir las condiciones adversas de estar en el internet público.
- Si no se puede aplicar todo, cuando menos se debe cubrir lo que considera el Top 10.



¡GRACIAS!

- Msc. Helios Mier Castillo
- helios@seguridadyprivacidad.org