OWASP

Desarrollo Seguro: práctica orientada a prevención de OWASP Top 10

OWASP Top 10 es una lista de las 10 vulnerabilidades más comunes encontradas en aplicaciones web y los errores de programación que generan dichas vulnerabilidades.

El curso se basa en la última edición oficial de OWASP Top 10 v2017.

Objetivos generales

Este curso está orientado a conocer las 10 vulnerabilidades consideradas críticas por OWASP así como la forma de analizarlas, explotarlas y solucionarlas desde el inicio hasta la implementación de cualquier proyecto de desarrollo de aplicaciones.

Requisitos previos

Conocimiento básico sobre análisis de sistemas y programación.

Público Objetivo

El curso está orientado a desarrolladores, administradores de bases de datos, líderes de proyecto, analistas de sistemas y personas vinculadas al análisis, diseño, arquitectura y desarrollo de aplicaciones, así como a los responsables de seguridad de la información de la organización.

Finalizado el curso, el asistente será capaz de:

- Conocer y entender las 10 vulnerabilidades consideradas críticas por OWASP
- Entender las amenazas y vulnerabilidades a las que está expuesta cualquier aplicación
- Reconocer y detectar de manera proactiva las falencias del desarrollo de las aplicaciones
- Identificar vulnerabilidades en aplicaciones en forma manual y con herramientas
- Aplicar las contramedidas necesarias para aumentar la seguridad de las aplicaciones

Este curso complementa el otro curso **"SDLC, Desarrollo Seguro y Modelado de Amenazas aplicado al Ciclo de Vida del Desarrollo del Software"** dictado por **Segu-Info**.

Material a entregar

Presentaciones utilizadas durante el curso en formato digital.

Duración y Modalidad

Este curso teórico/práctico tiene una duración de **16 horas** y la modalidad de cursada es presencial. También puede ser desarrollado ***in-company***.

Instructor

Cristian Borghello es Licenciado en Sistemas (UTN), desarrollador, Certified Information Systems Security Professional (CISSP), Certificate of Cloud Security Knowledge (CCSK), Microsoft MVP (Most Valuable Professional) Security.
Actualmente es Director de **Segu-Info** y **Segu-Kids** y se desempeña como consultor independiente en Seguridad de la Información.
Escribe para diversos medios especializados e investiga en forma independiente sobre Seguridad Informática y de la Información.
Ha brindado cursos y dictado congresos y seminarios nacionales e internacionales sobre la temática.

Temario

Estado en la seguridad del software - Teórico

- Principios del diseño de software seguro
- Modelado de Amenazas, DREAD y STRIDE
- Conceptos generales sobre el desarrollo de aplicaciones web
- OWASP Top 10, CWE, SANS Top 20 y OWASP Mobile Security Project
- Revisión de Guías de desarrollo y Testing de OWASP
- Desarrollo Agile Seguro, *DevOps* y *DevSecOps*
- Caso de Uso, Casos de Abuso y *Test Cases*

Análisis de vulnerabilidades del Top 10 de OWASP 2017 – Teórico - Práctico

- *Testing Black y White Box*
- Tipos de validaciones
- A1. Ataques de inyección
    - Comandos de sistema operativo
    - *SQL Injection y Blind SQL Injection*
    - LDAP
    - Xpath y JSON
- Prevención de inyecciones
- A2. Pérdida de autenticación y gestión de sesiones
    - Cookies inseguras
    - Validación de sesión y pérdida de autenticación
- A3. Exposición de datos sensibles
    - Validación de capa de transporte
    - Almacenamiento criptográfico inseguro
    - Protección insuficiente en la capa de transporte
    - Riesgos de exposición de datos sensibles en el navegador
- A4. Entidades Externas XML (XXE)
- A5. Pérdida de Control de Acceso
    - Redirecciones y restricciones de acceso

    - Rutas por defecto e inseguras
    - *Path traversal*
- A6. Configuración de Seguridad Incorrecta
    - Configuración insegura de servidores y componentes
    - Redirecciones y reenvíos no validados
    - Directorios por defecto
    - Archivos de configuración
    - Backups
    - Hardening de aplicaciones
- A7. *Cross-site Scripting (XSS)*
    - Tipos y definiciones
    - Técnicas de inyección de script
    - Codificación y ofuscamiento
- A8. Deserialización Insegura
- A9. Componentes con vulnerabilidades conocidas
- A10. Registro y Monitoreo Insuficientes
- Otras vulnerabilidades conocidas
    - *Cross_Site_Request_Forgery (CSRF)*
    - Uso inseguro de Certificados Digitales y Protocolo HTTPS