OWASP

Desarrollo Seguro de API y Microservicios basado en OWASP Top 10

Tanto el uso de API, como el modelo de ejecución *Serverless* son características fundamentales de las aplicaciones actuales. Las API exponen la lógica de la aplicación y datos confidenciales y, por esto, se han convertido en un objetivo importante para los atacantes.

En este curso se analizan los riesgos de seguridad de una aplicación, particularmente el Top 10 de vulnerabilidades de APIs y *Serverless* publicados en 2019.

SEGU.INFO
SEGURIDAD DE LA INFORMACION

Objetivos generales

En este curso se analizan los riesgos de seguridad de una app, particularmente el Top 10 de vulnerabilidades específicas de APIs y Serverless, y se muestran soluciones para entenderlas y mitigarlas.

Requisitos previos

Conocimiento básico sobre análisis de sistemas y programación web y móvil.

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 web, microservicios y móviles, 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 de OWASP para las API
- Conocer y entender las 10 vulnerabilidades de OWASP para los microservicios
- Entender las amenazas y vulnerabilidades a las que está expuesta cualquier aplicación que utiliza API
- 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"** y **"Desarrollo Seguro: práctica orientada a prevención de OWASP Top 10"** dictados 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 **8 o 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 y mobile
- OWASP Top 10, CWE, SANS Top 20, OWASP Mobile Security Project
- OWASP Top 10 API y Serverless
- 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 de OWASP API Security Top 10 (2019) – Teórico - Práctico

- *Testing Black y White Box*
- Tipos de validaciones
- Introducción al Top 10 de OWASP
- OWASP Serverless Top 10 (2017)
- OWASP API Security Top 10 (2019)
- Injection
- Broken object and function level authorization
- Broken authentication and access control
- Excessive sensitive data exposure
- Lack of resources and rate limiting
- Mass assignment
- Security misconfiguration
- Improper assets management
- Insufficient logging and monitoring

- XML External Entities (XXE)
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- OWASP API Security Top 10 cheat sheet
- Recomendaciones y buenas prácticas