DESSEG | Desarrollo Seguro

Duración: 3 días

DESSEG

Objetivos del curso

- Entender los aspectos relacionados con la seguridad en aplicaciones en producción, desarrollo, y las metodologías y herramientas para analizar, diseñar, e implementar controles en el ciclo de vida del desarrollo de aplicaciones.
- Aplicar las mejores prácticas de codificación para el desarrollo de aplicaciones seguras, independientemente del lenguaje de programación.
- Conocer técnicas de detección, validación y mitigación de los riesgos potenciales existentes en las aplicaciones web, las cuales permitirán desarrollar aplicaciones Web seguras. Comprender e identificar las vulnerabilidades de OWASP top 10 e incorporar ese conocimiento en el esquema de protección de aplicaciones web.
- Entender las principales amenazas a las que están expuestas las aplicaciones móviles y conocer los controles especificados en el estándar de seguridad de aplicaciones móviles de la OWASP.
- Conocer las mejores prácticas en materia de desarrollo de APIs, para implementar los controles necesarios para aumentar la seguridad de estas.
- Conocer los beneficios, conceptos de DevSecOps e incorporar las prácticas de seguridad de DevOps en el desarrollo de las aplicaciones de la organización.

Perfil de la audiencia

- Este curso es ideal para desarrolladores de software, responsables de aplicar las mejores prácticas en cada fase del ciclo de vida del desarrollo de software.
- Así mismo, es de gran ayuda para toda persona involucrada en cualquiera de las etapas del desarrollo de un proyecto de software.

Prerequisitos

Para tomar este curso se recomienda tener por lo menos dos años de experiencia como profesional en el ciclo de vida de desarrollo de software.

DESSEG | Desarrollo Seguro

Duración: 3 días

Esquema del curso

Capítulo 1: Seguridad en el Ciclo de Vida de Desarrollo de Software

- Objetivos
- 1.1 El Ciclo de Vida de Desarrollo de Software
- 1.2 Entendiendo la Seguridad en Aplicaciones, Amenazas y Ataques
- 1.3 Recopilación de Requerimientos de Seguridad
- 1.4 Diseño y Arquitectura de Aplicaciones Seguras
- 1.5 Controles de Seguridad
- 1.6 Estrategias para el Desarrollo de Aplicaciones
- 1.7 Metodología de Seguridad para el Desarrollo de Aplicaciones
- 1.8 El rol del Especialista de Seguridad en el Desarrollo de Aplicaciones
- 1.9 Determinación del Nivel de Riesgo Aceptable en las Aplicaciones
- 1.10 Administración de Cambios
- 1.11 Administración de Configuraciones

Capítulo 2: Fundamentos de la programación segura

- Objetivos
- 2.1 Modelo de seguridad
- 2.2 Modelado de amenazas
- 2.3 Escenarios de ataque
- 2.4 Prácticas de codificación segura
- 2.5 Prácticas de uso seguro de bases de datos
- 2.6 Pruebas estáticas y dinámicas de aplicaciones seguras (SAST & DAST)
- Laboratorio
- Caso de Estudio: Real time vehicle tracking system

Capítulo 3: Seguridad en aplicaciones Web

- Objetivos
- 3.1 Introducción a desarrollo de aplicaciones WEB
- 3.2 Seguridad en aplicaciones Web

- 3.3 OWASP Top 10
- Laboratorio
- 3.4 Ataques de autenticación y autorización
- 3.5 Ataques de administración de sesiones
- 3.6 Ataques lógica de aplicaciones
- 3.7 Validación de datos
- 3.8 Ataques AJAX
- 3.9 Revisión de código y pruebas de seguridad de aplicaciones web
- Laboratorio

Capítulo 4: Desarrollo Seguro de Aplicaciones Móviles

- Objetivos
- 4.1 Introducción a las aplicaciones móviles
- 4.2 Amenazas y ataques de aplicaciones móviles
- 4.3 El estándar de seguridad de aplicaciones móviles de la OWASP
- 4.4 MASVS-STORAGE: Almacenamiento
- 4.5 MASVS-CRYPTO: Criptografía
- 4.6 MASVS-AUTH: Autenticación y autorización
- 4.7 MASVS-NETWORK: Comunicación de red
- 4.8 MASVS-PLATFORM: Interacción de plataforma
- 4.9 MASVS-CODE: Calidad del código
- 4.10 MASVS-RESILIENCE: Resiliencia contra la ingeniería inversa y la manipulación
- 4.11 Pruebas de aplicaciones móviles
- Laboratorio

Capítulo 5: Desarrollo Seguro de APIs

- Objetivos
- 5.1 Introducción a las APIs
- 5.2 API REST y API SOAP
- 5.3 Amenazas y ataques en el uso de APIs
- 5.4 OWASP API Security Top 10
- 5.5 Mecanismos de Seguridad para APIs
- 5.6 API Gateways
- Caso de Estudio: Azure API Management Service
- Laboratorio

DESSEG | Desarrollo Seguro

Duración: 3 días

Capítulo 6: DevSecOps- Desarrollo Seguridad y Operaciones

- Objetivos
- 6.1 Introducción a DevOps
- 6.2 Conceptos Base
- 6.3 Everything as Code
- 6.4 lnfrastructure as Code
- 6.5 Integrando Seguridad en CI/CD (Continuous lntegration and Delivery)
- 6.6 Administración de Vulnerabilidades en DevOps
- 6.7 Administración de Artefactos
- 6.8 Administración de Secretos usando Vault, Jenkins y Docker Secrets
- 6.9 Herramientas Básicas
- 6.10 Seguridad en Contenedores
- 6.11 Seguridad en Máquinas Virtuales
- 6.12 Seguridad en la Nube
- Caso de Estudio: Banking platform in the cloud