Mejores Prácticas para Integración y Desarrollo de Software Seguro

Código: DES-120

Propuesta de Valor: DESARROLLO - PROGRAMACIÓN - METODOLOGÍAS

Duración: 21 Horas

Integrar la seguridad en el ciclo de desarrollo de software produce aplicaciones robustas y permite prevenir conflictos. El seminario, permitirá al participante reconocer los principios y conceptos claves para desarrollo seguro de software desde distintos aspectos, como proteger el software desarrollado; minimizar los riesgos en las aplicaciones empresariales que sustentan procesos de negocio; identificar las mejores prácticas del mercado para lograr software libre de riesgos; y contar con un proceso recomendado para desarrollo de software seguro. Su aplicación es genérica para cualquier lenguaje o framework de desarrollo, y se basa en las recomendaciones de estándares en seguridad de información. La metodología se basa en el trabajo en grupo, debate y análisis colectivo sobre los temas.

AUDIENCIA

- Gerentes de TI, personal de TI. Gerentes de seguridad de la información (CISO). Contralores. Auditores de seguridad, auditores internos. Responsables de procesos de gestión de seguridad. Gerentes de desarrollo, aplicaciones, proyectos y negocios. Consultores del área de seguridad de TI, desarrolladores de TI, analistas de TI, testers de TI, jefes de proyecto de TI. Profesionales independientes que busquen mejorar la seguridad de las aplicaciones informáticas de su empresa.

PRE REQUISITOS

- Se requiere conocimientos en desarrollo y programación.

OBJETIVOS

- Aprende técnicas y pautas para aplicar en el ciclo de desarrollo de software e identifica los puntos de validación de seguridad, que permitan integrar y construir software seguro.

CERTIFICACIÓN DISPONIBLE

- Certificado emitido por COGNOS.

CONTENIDO

1. ATAQUES BASADOS EN MEMORIA

1.1. SEGURIDAD DE BAJO NIVEL
1.2. LAYOUT DE MEMORIA
1.3. BUFFER OVERFLOW
1.4. INYECCIÓN DE CÓDIGO
1.5. OTRAS FORMAS DE EXPLOTAR LA MEMORIA
1.6. VULNERABILIDADES EN LOS STRING

2. DEFENSA CONTRA ATAQUES DE BAJO NIVEL

2.1. DEFENSA CONTRA ATAQUES DE BAJO NIVEL
2.2. MEMORIA SEGURA
2.3. TIPOS SEGUROS
2.4. EVITANDO LAS VULNERABILIDADES
2.5. PROGRAMACIÓN ORIENTADA AL RETORNO
2.6. INTEGRIDAD DE CONTROL DE FLUJO
2.7. CODIFICACIÓN SEGURA

3. SEGURIDAD WEB

3.1. SEGURIDAD EN LA WEB
3.2. TEMAS BÁSICOS EN WEB
3.3. INYECCIÓN SQL
3.4. CONTRAMEDIDAS PARA LA INYECCIÓN SQL
3.5. USO DE FIELDS Y COOKIES
3.6. HIJACK DE SESIÓN
3.7. CROSS SITE REQUEST FORGERY (CSRF)
3.8. CROSS-SITE SCRIPTING

4. CONSTRUYENDO SOFTWARE SEGURO

4.1. DISEÑO Y CONSTRUCCIÓN DE SOFTWARE SEGURO
4.2. ANÁLISIS DE ARQUITECTURA DE RIESGO
4.3. REQUERIMIENTOS DE SEGURIDAD
4.4. EVITANDO CAÍDAS
4.5. CATEGORÍA DE DISEÑO
4.6. DISEÑO ADECUADO

5. ANÁLISIS ESTÁTICO Y EJECUCIÓN SIMBÓLICA PARA SEGURIDAD

5.1. ANÁLISIS ESTÁTICO
5.2. ANÁLISIS DE FLUJO
5.3. ANÁLISIS SENSITIVO DE CONTEXTO

6. PRUEBAS DE PENETRACIÓN

6.1. PRUEBAS DE PENETRACIÓN
6.2. FUZZ TESTING

7. OWASP

7.1. OWASP

BENEFICIOS

- Al finalizar el curso, profundizarás conceptos y principios claves en seguridad de información, minimizando riesgos en aplicaciones empresariales.