



Desarrollo de Aplicaciones Web Seguras Basado en la Guía OWASP 2.0

• Descripción del Curso

Este curso de 24 horas brinda guías para el desarrollo de aplicaciones web de modo seguro. Durante el curso se presentarán ejemplos de fallas comunes en las aplicaciones, su mecanismo de explotación y remediación.

• Justificación

En la formación que reciben de los desarrolladores de aplicaciones no es común encontrar los temas relacionados con la seguridad de la información, al unir esta falencia con la necesidad de producir aplicaciones que respondan rápidamente a las necesidades del mercado se crea un espacio donde hay poco tiempo para investigar y hacer las pruebas necesarias para involucrar los elementos de seguridad necesario para la protección de la información que manejan las aplicaciones desarrolladas.

El proceso de certificación de la norma PCI V1.2 y V2.0 exigen evidencia que los desarrolladores de las aplicaciones involucradas en el alcance de la norma, tengan un entrenamiento para desarrollo de aplicaciones seguras.

El contenido de este curso incluye las guías necesarias para el desarrollo de aplicaciones seguras con la información más actualizada a la que se tiene alcance.

Perfil de la Audiencia

El contenido de este curso está orientado a desarrolladores de aplicaciones web que manejen información considerada como restringida o confidencial para la compañía.

Prerrequisitos

Antes de atender a este curso el estudiante debe tener:

- Experiencia en el desarrollo de aplicaciones Web
- Experiencia en el desarrollo de aplicaciones con bases de datos
- Se recomienda tener conocimientos de alguno de estos lenguajes: Perl, PHP, C, C++ o Java.
- Alto nivel de comprensión en la lectura en inglés.



• Objetivos

Después de completar el curso el estudiante estará en capacidad de:

- Hacer una valoración de las amenazas que tienen las aplicaciones
- Identificar las normas o estándares del mercado para comercio electrónico
- Conocer algunos mecanismos de autenticación y sus problemas asociados
- Identificar los requerimientos necesarios para dar autorización en las aplicaciones
- Reconocer las principales fallas de seguridad asociadas a la validación de datos
- Realizar pruebas sobre las aplicaciones para la explotación de la inyección de código SQL y aplicar los mecanismos de remediación
- Identificar los requerimientos para el manejo de los errores y los registros de auditoría
- Entender cómo funcionan las diferentes técnicas de cifrado
- Conocer las buenas prácticas para el manejo de interfaces de administración y/o configuración de las aplicaciones
- Conocer los mecanismos usados para lograr una denegación de servicio y las técnicas para protegerse

Materiales Entregados

- CD con las presentaciones, documentos y herramientas relevantes
- Guía OWASP 2.0 impresa
- Certificado de Asistencia (para aquellos que asistan al 80% del curso)

Contacto

IQ Information Quality

Calle 109 # 18B - 31 oficina 205

Teléfono: 571 - 6 19 63 92

Andrés Herrera

andres.herrera@iqcol.com

www.iqcol.com

Bogotá, Colombia