Desarrollo Seguro de Aplicaciones Web Basado en OWASP

Código: OWA-101

Propuesta de Valor: DESARROLLO - PROGRAMACIÓN - METODOLOGÍAS

Duración: 30 Horas

Este curso está focalizado en las vulnerabilidades Web clasificadas por OWASP como de alto riesgo. Durante este curso se explicará teóricamente cada vulnerabilidad con prácticas hands-on, demostraciones y las contramedidas necesarias para mitigar dichas vulnerabilidades. El curso está desarrollado para que participantes de distintos niveles de conocimiento identifiquen las vulnerabilidades y puedan aplicar las contramedidas necesarias para aumentar la seguridad de las aplicaciones. El curso fue especialmente diseñado para satisfacer las necesidades esenciales sobre seguridad de QA testers, desarrolladores de Aplicaciones Web y expertos en Seguridad Informática.

AUDIENCIA

- Este curso está dirigido a: Líderes de Proyecto de desarrollo, Desarrolladores, Analistas de Calidad, Analistas Funcionales, Oficiales de Seguridad Informática, Auditores.

PRE REQUISITOS

- Conocimiento de programación en JAVA y nociones de seguridad.
- Experiencia en el desarrollo de componentes web.
- Familiarizado con el lenguaje SQL.
- Conocimientos básicos de Javascript.

OBJETIVOS

Al finalizar el curso los estudiantes serán capaces de:

- Describir los aspectos de seguridad en las diferentes etapas del desarrollo de software, alineadas a las buenas prácticas propuestas por OWASP.
- Señalar las debilidades más comunes de las aplicaciones y los fundamentos de una programación segura para defender la misma de ataques avanzados.

- Analizar, cuantificar y calificar los riesgos de seguridad de un proyecto de software.
- Utilizar los lineamientos y buenas prácticas de desarrollo seguro basándonos en normativas como, por ejemplo, SOX, PCI, BCRA/4609, ISO27002.

CERTIFICACIÓN DISPONIBLE

- Certificación emitida por **COGNOS**.

CONTENIDO

1.INTRODUCCIÓN A LA SEGURIDAD EN EL DESARROLLO DE SOFTWARE

1.1. CASOS REALES DE VULNERABILIDADES Y SU IMPACTO
1.2. PROBLEMÁTICA DE LAS APLICACIONES INSEGURAS. DERRIBANDO MITOS
1.3. DERRIBANDO MITOS
1.4. PARTICIPACIÓN DE SEGURIDAD INFORMÁTICA EN EL DESARROLLO DEL SOFTWARE

2.SOBRE EL PROYECTO OWASP

2.1. ¿QUÉ ES OWASP?
2.2. RECURSOS QUE OFRECE OWASP A LA COMUNIDAD
2.3. VULNERABILIDADES DEL TOP TEN OWASP

- 2.3.1. A1: INJECTION
- 2.3.2. A2: CROSS-SITE SCRIPTING (XSS)
- 2.3.3. A3: BROKEN AUTHENTICATION AND SESSION MANAGEMENT
- 2.3.4. A4: INSECURE DIRECT OBJECT REFERENCES
- 2.3.5. A5: CROSS-SITE REQUEST FORGERY (CSRF)
- 2.3.6. A6: SECURITY MISCONFIGURATION
- 2.3.7. A7: INSECURE CRYPTOGRAPHIC STORAGE
- 2.3.8. A8: FAILURE TO RESTRICT URL ACCESS
- 2.3.9. A9: INSUFFICIENT TRANSPORT LAYER PROTECTION
- 2.3.10. A10: UNVALIDATED REDIRECTS AND FORWARDS

3.SEGURIDAD EN LA ETAPA DE ANÁLISIS

3.1. PAUTAS DE SEGURIDAD EN EL ANÁLISIS DE REQUERIMIENTOS
3.2. DESARROLLO SEGURO Y COMPLIANCE

- 3.2.1. PCI, ISO27002

4.SEGURIDAD EN EL DISEÑO DE SOFTWARE

4.1. CRITERIOS BÁSICOS DE SEGURIDAD

- 4.1.1. PRINCIPIO DEL MENOR PRIVILEGIO
- 4.1.2. CRITERIO DE DEFENSA EN PROFUNDIDAD

4.2. MANEJO SEGURO DE ERRORES

- 4.2.1. CRITERIO DEL “FALLO SEGURO”
- 4.2.2. DEFINICIÓN DE MENSAJES DE ERROR
- 4.2.3. PREVENCIÓN DE DIVULGACIÓN DE INFORMACIÓN

4.3. MANEJO DE INFORMACIÓN SENSIBLE

- 4.3.1. ALMACENAMIENTO SEGURO
- 4.3.2. TRANSFERENCIA SEGURA
- 4.3.3. ENCRIPCIÓN Y HASHES

4.4. AUDITORÍA Y LOGGING

4.5. DISEÑO DE AUTENTICACIÓN Y AUTORIZACIÓN

- 4.5.1. SEGURIDAD EN WEB SERVICES

4.6. DISEÑO DE PROTECCIÓN CONTRA DENIAL OF SERVICE (D.O.S)

4.7. ERRORES DE LOGICA DE NEGOCIO

5.SEGURIDAD EN LA CODIFICACIÓN DE SOFTWARE

5.1. VULNERABILIDADES MÁS COMUNES. ¿CÓMO PREVENIRLAS?

- 5.1.1. SQL INJECTION & COMMAND INJECTION
- 5.1.2. XSS, CSRF

5.2. VULERABILIDADES DEL RANKING OWASP TOP 10 (2010)

5.3. OTRAS VULNERABILIDADES

- 5.3.1. ERRORES DE CANONIZACIÓN
- 5.3.2. INFORMATION DISCLOSURE
- 5.3.3. PHISHING VECTOR

5.4. RECURSOS DE OWASP PARA SEGURIDAD EN LA CODIFICACION

6.TESTING DE SEGURIDAD DE SOFTWARE

6.1. TÉCNICAS DE TESTING DE SEGURIDAD

- 6.1.1. TESTING DE SEGURIDAD VS TESTING FUNCIONAL
- 6.1.2. REVISIÓN DE CÓDIGO

6.2. RECURSOS DE OWASP PARA TESTING DE SEGURIDAD

- 6.2.1. OWASP TESTING PROJECT
- 6.2.2. OWASP CODE REVIEW GUIDE

6.3. TESTING DE SEGURIDAD EN EL CICLO DE VIDA DEL SOFTWARE

6.4. ESCALAMIENTO DE PRIVILEGIOS

6.5. HERRAMIENTAS DE TESTING DE SEGURIDAD

BENEFICIOS

- Al finalizar el participante conocerá los aspectos de seguridad en las diferentes etapas del desarrollo de software, alineadas a las buenas prácticas propuestas por OWASP, y señalará las debilidades más comunes de las aplicaciones y los fundamentos de una programación segura para defender la misma de ataques avanzados.