Curso

Desarrollo Seguro ante Ciberataques para Java, .NET, JavaScript, Angular, React, IOS y Android

(OWASP - PCI-DSS)

20 Horas

Vigo, 3, 4, 5 y 6 de Junio de 2019

www.vitaedigital.com

Vitae

Introducción:

A medida que cambian las prácticas de codificación segura aceptadas por la industria, las prácticas de codificación de las organizaciones y la capacitación de los desarrolladores se deben actualizar para abordar nuevas amenazas, por ejemplo, ataques para extraer la memoria o ataques del tipo side-channel derivados del empleo de microprocesadores con vulnerabilidades en su microcódigo.

Las vulnerabilidades identificadas en los Requisitos en OWASP y PCI-DSS proporcionan un punto de partida. Es responsabilidad de la organización informarse sobre las últimas tendencias en vulnerabilidades e incorporar las medidas apropiadas, -como los nuevos riesgos identificados y no tratados de forma específica en OWASP y PCI -DSS- en cuanto a las prácticas de codificación segura que cubrirá adecuadamente la presente formación.

Se desarrollarán numerosos ejercicios de código para la búsqueda activa de vulnerabilidades y su correspondiente mitigación en el lenguaje de desarrollo más empleado en la industria.

Objetivos del curso:

Actualización de nuevas prácticas de codificación segura adaptada al framework y lenguaje de desarrollo más empleados por la Industria cubriendo la actualización a las nuevas amenazas detectadas hasta el momento de la realización del curso.

Dirigido :

Programadores, Analista Programadores, Ingenieros de Software, Responsables de Seguridad TI y todo profesional que tenga responsabilidades en Seguridad TI.

Duración:

20 horas en 4 sesiones de 5 horas

TEMARIO

Módulo Formativo I: Conceptos Generales de Desarrollo Seguro

1.- Secure Software Development Life Cycle (S-SDLC)

- 1.1.- Introducción
- 1.2.- S-SDLC
- 1.3.- Open SAMM
- 1.4.- Métodos de detección de vulnerabilidades en código

2.- Vulnerabilidades en las aplicaciones

- 2.1.- Introducción
- 2.2.- Enumeración de vulnerabilidades (Organismos)
- 2.3.- Enumeración de vulnerabilidades (CWE – Common Weakness Enumeration)
  - 2.3.1.- Tipo de vulnerabilidad (CWE)
  - 2.3.2.- Mediciones y sistema de puntuación
  - 2.3.3.- Priorización de vulnerabilidades
  - 2.3.4.- CWSS (Common Weakness Scoring System)
  - 2.3.5.- CWRAF (Common Weakness Risk Analysis Framework)
- 2.4.- CVE y CVSS
  - 2.4.1.- CVE (Common Vulnerabilites and Exposures)
  - 2.4.2.- CVSS (Common Vulnerabilites Scoring System)
  - 2.4.3.- CVE Details

Módulo Formativo II: OWASP y PCI-DSS

1.- OWASP Top Ten 2017

- 1.1.- OWASP: Introducción
- 1.2.- OWASP: Proyecto Top Ten
- 1.3.- OWASP: Riesgos de seguridad de las Aplicaciones Web
  - 1.3.1.- Inyección
  - 1.3.2.- Pérdida de Autenticación
  - 1.3.3.- Exposición de Datos Sensibles
  - 1.3.4.- Entidades Externas XML (XXE)
  - 1.3.5.- Pérdida de Control de Acceso
  - 1.3.6.- Configuración de Seguridad Incorrecta
  - 1.3.7.- Cross-Site Scripting (XSS)
  - 1.3.8.- Deserialización Insegura
  - 1.3.9.- Uso de Componentes con vulnerabilidades Conocidas
  - 1.3.10.- Registro y Monitoreo Insuficientes
- 1.4.- OWASP: Consejos a desarrolladores
- 1.5.- OWASP: Consejos a (pen)testers
- 1.6.- OWASP: Consejos a administradores de aplicaciones
- 1.7.- OWASP: Consejos a Organizaciones

2.- OWASP Top Ten Mobile 2016

- 2.1.- Introducción
- 2.2.- OWASP Top Ten Mobile 2016 (Final Release)
  - 2.2.1.- Uso incorrecto de la plataforma
  - 2.2.2.- Almacenamiento inseguro de datos

3.3.8.- Req. no contemplado y A8:2017 - Deserialización Insegura

3.3.9.- Req. 6.5.6 y A9:2017 - Uso de Componentes con Vulnerabilidades Conocidas

3.3.10.- Req. no contemplado y A10:2017 - Registro y Monitoreo Insuficientes

3.4.- Requisitos no contemplados en OWASP Top Ten 2017

3.5.- Cumplimiento normativo de PCI-DSS v3.2.1

3.5.1.- Actualización de la documentación vinculada con el SSDLC (Secure Software Development Life Cycle) para que contemplen la totalidad de los riesgos del Top Ten de la OWASP 2017 – Req. 6.3

3.5.2.- Actualización de los criterios empleados en la revisión de código (ya sea si se realiza manualmente o empleando herramientas automatizadas) antes de enviarlo a Producción para que cubran estos nuevos riesgos – Req. 6.3.2

3.5.3.- Actualización del material de formación en desarrollo seguro incluyendo estos nuevos riesgos y describir sus contramedidas – Req. 6.5

3.5.4.- Formación de los empleados en desarrollo seguro incluyendo estos nuevos riesgos - Req. 6.5

Módulo Formativo III: OWASP Best Practices

1.- OWASP Secure Coding

1.1.- Best Practices

1.1.1.- Validación de entradas

1.1.2.- Codificación de salidas

1.1.3.- Administración de autenticación y contraseñas

1.1.4.- Administración de sesiones

1.1.5.- Control de acceso

1.1.6.- Prácticas criptográficas

1.1.7.- Manejo de errores y logs

1.1.8.- Protección de datos

1.1.9.- Seguridad en comunicaciones

1.1.10.- Configuración de los sistemas

1.1.11.- Seguridad de bases de datos

1.1.12.- Manejo de ficheros

1.1.13.- Manejo de memoria

1.1.14.- Prácticas generales

1.2.- OWASP Development Guide (v3.0 dev vs 2.0.1 stable)

1.3.- OWASP ASVS (Application Security Verification Standard) v3.0.1

1.4.- OWASP Code Review v2.0

1.5.- OWASP Testing Project

1.6.- OWASP Proactive Controls

1.7.- OWASP Cheat Sheet

Módulo Formativo IV: Language General Secure Coding

Nota.- El módulo formativo será llevado a cabo mediante la explicación detallada de cada entrada mediante un ejemplo de código no securizado y su implementación mitigando la vulnerabilidad descrita por lo que requiere conocimientos específicos sobre el lenguaje de desarrollo empleado.

1.- General Language Specific Secure Coding

- 1.1.- JAVA
- 1.2.- .Net
- 1.3.- Mobile (Android & iOS)
- 1.4.- Angular/Node/React

Módulo Formativo V: Análisis Estático de Código con herramientas Open Source

1.- SonarQube

- 1.1.- Instalación
- 1.2.- Configuración y plugins
- 1.3.- Detección de vulnerabilidades en el código fuente

INFORMACIÓN DEL CURSO

Duración	20 Horas Lectivas
Lugar	Vigo
Fechas	3, 4, 5 y 6 de Junio de 2019
Horario	De Lunes a Jueves de 16:00 a 21:00
Donde	Centro Social Fundación AFundacion ABANCA C/ Policarpo Sanz, 24 - 26 36202 Vigo

Pedro Candel

Pedro Candel es uno de los mayores expertos en cibeseguridad a nivel nacional. Ha sido docente en varios Máster de Seguridad en diferentes Universidades.

Es especialista en seguridad ofensiva, descubrimiento de vulnerabilidades, análisis de malware e ingeniería inversa. Es ponente habitual en las principales conferencias de ciberseguridad de España y también a nivel internacional en Europa y Latinoamérica. Ha presentado trabajos de investigación en todo el mundo y realizado auditorías de hacking ético.

Ponente habitual en congresos, conferencias, eventos y otras instituciones nacionales e internacionales en materia de ciberseguridad presentando trabajos de investigación en todo el mundo.

Ha trabajado en Deloitte CyberSOC Academy, Buguroo Offensive Security, para el Servicio de Formación y Empleo de la Junta de Comunidades de Castilla-La Mancha y varias consultoras privadas de Telecomunicaciones y Seguridad TIC formando a cientos de grandes empresas de todo de sectores entre los que destaca el financiero, logístico, farmacéutico, TIC, etc. y formación a Fuerzas y Cuerpos de Seguridad del Estado.

También, como auditor de seguridad especializado, ha realizado auditorías de hacking ético para clientes del IBEX35, NASDAQ y todo tipo de empresas privadas.

CONDICIONES ECONÓMICAS

Tarifa por Asistente	**290 €** **(Cuota Bonificable por la Fundación Tripartita)**
Tarifa por asistente a partir de dos personas de la misma empresa u organización	**250 €** **(Cuota Bonificable por la Fundación Tripartita)**

Forma de Pago:
Por transferencia al finalizar el curso a la recepción de la factura

Se añadirá el 21 % de IVA

Inscripción:
Marcos Carbonell
marcos@vitaedigital.com
Tlf : 986 47 21 01
637 82 02 57

Plazas limitadas, reserva de plazas por riguroso orden de inscripción