



conetic

Confederación Española de Empresas de Tecnologías
de la Información, Comunicaciones y Electrónica.

Programación segura



Introducción

Se propone esta formación en ciberseguridad desde el punto de vista del desarrollo de software (**Programación Segura**), con especial atención a las tecnologías **JAVA**.

El seminario está orientado a jefes de proyecto, desarrolladores de **aplicaciones web** con tecnología Java, con el fin de mejorar la capacidad de los equipos de pruebas y los de desarrollo, ayudando a diseñar las pruebas y a implementar mecanismos de seguridad en sus aplicativos.

La idea principal es instruirse en la realización de pruebas de **Pentesting** y **remediación de vulnerabilidades**.

En la actualidad existe una creciente necesidad, tanto operativa como legal, de disponer de herramientas de supervisión y monitorización de la ciberseguridad con el fin de proteger los activos digitales y/o procesos productivos, por ello, para las empresas de nuestro sector **desarrollar software seguro es una necesidad, no una opción.**

Objetivos

El objetivo es doble, por un lado, con la realización de este seminario se obtendrán conocimientos sobre las formas más habituales de ataques en cada uno de los entornos web y se diseccionará la forma de llevar a cabo dichos ataques, mediante ejercicios prácticos de *Pentesting*. Por otro lado, y una vez conocido el problema, se le pondrá solución, mediante técnicas de remediación de vulnerabilidades, y se automatizará la ejecución de los planes de prueba.

Para la estructuración del seminario se tendrá como referencia las guías, documentos y ejemplos editados por la [OWASP Foundation](#), referente internacional en esta materia.

El taller de *pentesting* consiste en una formación eminentemente práctica, durante la misma, el instructor mostrará en tiempo real cómo explotar vulnerabilidades, así como el diseño y ejecución de casos de prueba. Adicionalmente, planteará ejercicios que los asistentes tendrán que resolver individualmente, para posteriormente ser corregidos durante el curso.

Para el taller se empleará los estándares de OWASP como documentación técnica de base se usará:

[OWASP Application Security Verification Standard](#) y [OWASP Testing Guide](#) para entornos web.

Plan de trabajo y contenido

El seminario está estructurado de manera que pueda ser realizado en **diferentes bloques**, en base al interés de cada uno de los asistentes. Cada participante deberá construir un itinerario personalizado en base a sus intereses y el papel que juegue dentro de su organización; así un desarrollador interesado en aplicaciones web podrá asistir a ambos bloques, mientras que una persona interesada en conocer los conceptos básicos podrá asistir únicamente a la introducción. Para asistir al taller exclusivamente, se recomienda disponer de conocimientos previos en programación segura y conocer las vulnerabilidad de OWASP.

A continuación, se presentan el calendario programado, así como el detalle de contenido de cada uno de los bloques.

Precio

El precio de la formación será de 14 €/hora y alumno.

Calendario:

Las sesiones serán todas de 3 horas, y se realizarán de 8.00h horas a 11.00 horas, impartidas de forma telemática

Fechas:

Introducción al desarrollo Seguro, días 13, 14, 15 y 16 de diciembre.

Taller de mitigación y pruebas web con java, días 20, 21 y 22 de diciembre.

Detalle del contenido:

Introducción al Desarrollo Seguro (4 jornadas x 3horas - 12 horas total)

1. Introducción: atacantes y amenazas
2. Seguridad en el desarrollo: competencias, *roles* y equipos
3. OWASP TOP 10
4. Ciclo de Vida de Desarrollo SW seguro (tradicional y ágil)
5. Herramientas para el desarrollo SW seguro: SAST, DAST
6. Taller de *pentesting*
 - a. Una aplicación insegura
 - b. Herramientas de *pentesting*
 - c. Ejecución de diferentes ataques

Bloque III - Taller mitigación y pruebas Web con Java (3 jornadas x 3 horas – 9 horas total)

1. Arquitecturas servidor java, transiciones de páginas, SPAs y apis REST
2. Spring MVC y Spring Boot: especificaciones vs frameworks
3. Estándares OWASP y OWASP Testing Guide
4. Verificación de la gestión de sesiones
5. Verificación del control de acceso
6. Verificación de entrada maliciosa
7. Verificación de la criptografía
8. Verificación del logging y manejo de errores
9. Verificación de la protección de datos
10. Verificación de la seguridad en las comunicaciones
11. Verificación de la configuración de seguridad HTTP
12. Verificación de los controles maliciosos
13. Verificación de la lógica de negocio
14. Verificación de los recursos y ficheros

Requisitos de los asistentes:

Al ser una formación técnica asociada al desarrollo de **aplicaciones**, los asistentes deberán:

- Poseer nociones en programación en Java, y javascript.
- Poseer nociones básicas del funcionamiento de redes y comunicaciones.
- Disponer de un equipo en el que realizar los ejercicios propuestos.
- Disponer de todo lo necesario para hacer el seguimiento de las sesiones por TEAMS de Microsoft.
- Disponer de [VAGRANT](#) instalado en su máquina