sedian

Seguridad Digital
de Andalucía

Ficha técnica

Desarrollo web seguro

Curso elearning 40h.

JUNTA DE ANDALUCIA
CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

© 2018 Junta de Andalucía. Consejería de Empleo, Empresa y Comercio. Este documento y, en su caso, cualquier documento anexo al mismo, contiene información de carácter confidencial exclusivamente dirigida a su destinatario o destinatarios. Queda prohibida su divulgación, copia o distribución a terceros sin la previa autorización escrita de "Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.". Si no es Ud. el destinatario del documento le ruego lo destruya sin hacer copia digital o física, comunicando a "Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A." vía e-mail o fax la recepción del presente documento. Toda declaración de voluntad contenida deberá ser tenida por no producida.

ÍNDICE

1.Datos básicos

A continuación se detallan las características, metodología y toda la información relevante para el desarrollo del curso elearning de 40h sobre "Desarrollo Web Seguro".

- **Título**: Desarrollo Web Seguro
- **Modalidad**: e-learning
- **Público objetivo**: Responsables de seguridad TIC y personal TIC de la Junta de Andalucía y entidades vinculadas
- **Duración**: 40 horas
- **Fecha**: 21 de mayo al 29 junio de 2018

2.Tutor

CARLOS GARCÍA SÁNCHEZ.

Carlos García Sánchez posee una amplia experiencia en el ámbito tecnológico donde ha trabajado y colaborado para compañías influyentes con excelentes resultados dentro del marco de la ciberseguridad.

Ha participado en proyectos de desarrollo seguro para clientes / empresas como: Fifteen Digital, Lesniak Swann, Buleboo Studio, LG Electronics y otros perfiles de clientes.

Actualmente trabaja en la linea de servicio de IT Risk Advisory de Deloitte para clientes de EMEA realizando proyectos SAST con algunos de

los fabricantes líderes en el cuadrante Gartner como Fortify, Checkmarx, Veracode o Buguroo bugscout.

Además de esto, posee un amplio conocimiento en el campo de la cyber seguridad, en temas como el pentesting, desarrollo seguro de software, sistemas de control industrial (ICS-SCADA) y otras técnicas y herramientas.

Su experiencia como ponente en importantes conferencias de seguridad y reportando vulnerabilidades a empresas aporta un gran valor humano.

3.Objetivos

Entre los objetivos de este curso online, están el formar desarrolladores en programación segura y mejorar las habilidades de los auditores de seguridad en el análisis y evaluación del código fuente de las aplicaciones.

El curso expone al alumno a diferentes lenguajes de programación y entornos de desarrollo. El temario engloba un análisis en profundidad de los riesgos presentes en cada uno de los diferentes entornos, así como las mejores prácticas seguidas por los desarrolladores más expertos para el desarrollo de aplicaciones seguras y estables.

Adicionalmente, el programa abarca técnicas específicas para la identificación de vulnerabilidades en código fuente y para la ejecución continuada de acciones que minen una aplicación inicialmente comprometida.

4.Contenidos

1.- Protocolo HTTP

Objetivo

- Introducir el protocolo HTTP en la capa de aplicación del modelo OSI.
- Analizar las cabeceras del protocolo HTTP.
- Conocer los principales métodos del protocolo HTTP.
- Interpretar los códigos de respuesta del protocolo HTTP.
- Ofrecer una visión general sobre las vulnerabilidades de las aplicaciones web.
- Interceptar y modificar el protocolo HTTP.

Contenido

1. Protocolo HTTP
    1. Introducción
    2. Objetivos
    3. Introducción al protocolo HTTP
    4. Métodos HTTP
    5. Codificación de la información
    6. Introducción a las vulnerabilidades en aplicaciones web
    7. El proyecto OWASP y las vulnerabilidades en aplicaciones web
    8. Esnifado y codificación de cabeceras
    9. Resumen

10. Referencias

2.- Ciclo de vida de desarrollo seguro de software (SDLC)

Objetivo

- Conocer la importancia del ciclo de vida de desarrollo seguro
- Conocer las fases del SDLC y su aplicación en las tecnologías de información
- Analizar las vulnerabilidades que afectan a los SDLC

Contenido

1. Ciclo de vida de desarrollo seguro de software (SDLC)
    1. Introducción a la unidad
    2. Objetivos
    3. Introducción al SDLC
    4. Fases del SDLC
    5. SDLC-IT (Systems Development Life Cycle for Information Tecnologies)
    6. Aplicación del SDLC
    7. Otras vulnerabilidades que afectan a los SDLC

3.- OWASP general

Objetivo

- Dar a conocer el proyecto abierto de seguridad de aplicaciones web (OWASP-Open Web Security Project).
- Conocer los principales riesgos de seguridad en aplicaciones web según OWASP.
- Adquirir una visión general de cada uno de los diez principales riesgos de seguridad en aplicaciones web según OWASP.

Contenido

1. OWASP general
    1. Introducción

2. Objetivos
3. Riesgos de seguridad en aplicaciones web
4. Visión general OWASP 2013 “TOP TEN”
5. Cambios con respecto a OWASP 2013
6. Resumen de los factores de riesgo
7. Verificación de pruebas OWASP
8. Otros recursos OWASP
9. Resumen
10. Referencias

4.- OWASP Top Ten

Objetivo

- Adquirir los conocimientos necesarios para comprender cada uno de los principales riesgos de una aplicación web según OWASP.
- Tener una visión en profundidad de cada uno de los riesgos “Top Ten” del proyecto OWASP.
- Conocer las contramedidas generales de seguridad para reducir los riesgos más críticos en aplicaciones web.

Contenido

1. OWASP Top Ten
    1. Introducción
    2. Objetivos
    3. Inyección
    4. Pérdida de autenticación
    5. Exposición de datos sensibles
    6. Entidades externas XML (XXE)
    7. Pérdida de control de acceso
    8. Configuración de seguridad incorrecta
    9. Secuencias de comandos en sitios cruzados (XSS)
    10. Deserialización insegura
    11. Uso de componentes con vulnerabilidades conocidas
    12. Registro y monitoreo insuficiente
    13. Referencias

5.- OWASP Java Top Ten

Objetivo

- Conocer las diferentes técnicas de defensa disponibles en JAVA para prevenir cada uno de los riesgos “top ten” del proyecto OWASP.
- Aplicar código seguro a nuestros desarrollos de aplicaciones web.
- Ofrecer una visión general para no cometer errores básicos en el diseño de aplicaciones seguras en JAVA.

Contenido

1. OWASP Java Top Ten
    1. Introducción
    2. Objetivos
    3. Inyección
    4. Pérdida de autenticación y gestión de sesiones
    5. Autenticación
    6. Autorización
    7. Referencias inseguras
    8. Gestión de errores
    9. Denegación de servicio
    10. Prácticas específicas de Java
    11. Referencias

6.- Seguridad PHP

Objetivo

- Comprender la importancia de los filtros en las funciones de entrada y salida.
- Establecer una relación entre OWASP “Top Ten” y el lenguaje de desarrollo PHP.
- · Establecer medidas de seguridad para vulnerabilidades comunes en código PHP.
- Conocer cómo almacena PHP las sesiones en alojamientos compartidos.

- Deshabilitar e investigar funciones “maliciosas” de PHP.
- Desarrollar aplicaciones web de forma segura en PHP.

Contenido

1. Seguridad PHP
    1. Introducción
    2. Objetivos
    3. Consideraciones previas
    4. Register globals
    5. Filtrado de datos
    6. Error reporting
    7. Proceso de formularios
    8. Credenciales y bases de datos
    9. Sesiones
    10. Alojamientos compartidos
    11. Funciones “maliciosas” de PHP
    12. Resumen
    13. Referencias

7.- Seguridad en aplicaciones .NET

Objetivo

- Conocer los principales ataques realizados sobre aplicaciones .NET.
- Conocer el modelo de amenazas definido por Microsoft en sus distintas categorías, centrándose en cómo afecta a las aplicaciones web.
- Comprender los principios generales de seguridad en aplicaciones web bajo entornos Microsoft.

Contenido

1. Seguridad en aplicaciones .NET
    1. INTRODUCCIÓN
    2. OBJETIVOS
    3. Principales ataques en aplicaciones web desarrolladas en .NET
    4. Amenazas de seguridad para las aplicaciones web

5. Procedimientos generales de seguridad
6. OWASP A1-Inyección SQL en .NET
7. Inyección SQL en cabeceras de solicitud del protocolo HTTP
8. Contramedidas en .NET para inyección SQL
9. OWASP A2–Pérdida de autenticación en .NET
10. Contramedidas para la pérdida de autenticación y gestión de sesiones en .NET
11. Seguridad en Web.config
12. Resumen
13. Referencias

8.- Buenas prácticas de seguridad

Objetivo

- Conocer las recomendaciones de seguridad del proyecto OWASP para aplicaciones web.
- Reforzar la visión general de seguridad en el desarrollo del software.
- Ofrecer diferentes listas de verificación y comprobación para mitigar los riesgos de seguridad en las aplicaciones web.

Contenido

1. Buenas prácticas de seguridad
    1. Introducción
    2. Objetivos
    3. Integración con el ciclo de desarrollo seguro
    4. Visión general de la seguridad en el desarrollo de software
    5. Buenas prácticas de seguridad en el desarrollo de aplicaciones web
    6. Resumen
    7. Referencias

5.Metodología de evaluación

Los alumnos asistentes dispondrán de dos sistemas de evaluación para este curso online. Dentro del paquete SCORM y fuera del mismo.

Dentro del paquete SCORM y al finalizar cada unidad del curso, el alumno realizará una evaluación con el objetivo de validar y comprobar los conocimientos adquiridos. Esta evaluación está compuesta por 10 preguntas.

Evaluación final del curso. Una vez completada todas las unidades, el alumno deberá realizar una evaluación final del curso y que sumará a la puntuación total del curso. Para esta evaluación final, el alumno dispondrá de 2 intentos y debiendo alcanzar al menos el 65% de preguntas o pruebas superadas para poder obtener una calificación de aprobado. En caso contrario, el alumno podría no aprobar dicho curso.

El alumno no necesariamente deberá recorrer todas las pantallas para poder obtener una calificación, pudiendo ir directamente a cada evaluación de las diferentes secciones de cada unidad dentro del paquete SCORM.

5.1.Calificaciones

Evaluación y prácticas de unidades del paquete SCORM. Supone el 35% de la calificación final.

Evaluación final del curso fuera del paquete SCORM. Supone el 65% de la calificación final.

Calificación mínima para obtener el certificado de aprobado, 65%

Número máximo de intentos, 2

5.2.Metodología de seguimiento

Para realizar un correcto seguimiento del curso y disponer de los medios necesarios para que los alumnos puedan elevar sus dudas al tutor, se dispondrán de los siguientes canales para tal fin.

1. Mail del tutor. Los alumnos podrán mantener contacto con el tutor del curso mediante la dirección de mail formacion.sedian@juntadeandalucia.es , donde el tutor dispondrá de un plazo máximo de 48h para responder al alumno.

2. Teléfono de asistencia técnica al alumno. Los participantes a este curso dispondrán del teléfono de asistencia 665 36 76 70 donde podrán elevar dudas referentes a la gestión, aspectos técnicos y usabilidad de la plataforma y administración del curso. Este teléfono estará operativo de lunes a jueves de 9:00h a 13:00h y de 16:00h a 18:00h.

3. Videoconferencia Skype. Todos los jueves y hasta la finalización del curso, estará disponible el canal de Skype para que los alumnos puedan mantener una videoconferencia con el tutor y así poder resolver las dudas o profundizar en contenidos que requieren una asistencia técnica.

4. Foro de discusión. Los alumnos disponen de un foro de discusión donde mantendrán una relación colaborativa y podrán mantener contacto con el tutor.