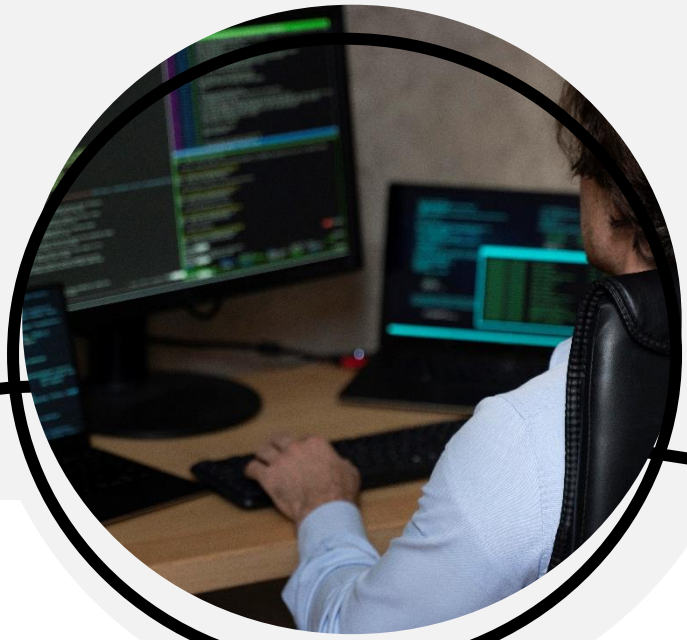
vuela | Junta de Andalucía

Secure Programming Foundation



Curso Blended | *Nivel Avanzado* | *40h* | *31/10 al 24/11* | *De 25 a 45 plazas*

¿QUÉ VAS A APRENDER?

Este curso de tiene como objetivo enseñar a los estudiantes técnicas avanzadas de hacking ético, con el fin de identificar y mitigar vulnerabilidades de seguridad en sistemas, redes, aplicaciones y dispositivos.

Es importante que los profesionales de seguridad de la información adquieran estas habilidades avanzadas en ethical hacking, ya que la industria necesita cada vez más expertos capaces de identificar, prevenir y mitigar ataques de hackers malintencionados. También es importante que los profesionales de seguridad de la información puedan poner en práctica estas técnicas en su organización, con el fin de garantizar la seguridad y protección de los datos confidenciales de la empresa.

Parte eLearning → 20 horas

OBJETIVOS:

Comprender los principios fundamentales de las aplicaciones web. Para ello es necesario tener un conocimiento profundo del funcionamiento del protocolo de transferencia de hipertexto (HTTP), además de cómo implementan la seguridad los navegadores modernos.

CONTENIDOS:

Módulo 1. Introducción a la programación segura (4 horas)

1. El acrónimo STRIDE y la seguridad web.
2. ¿Por qué el software es inseguro?
3. ¿Qué debes conocer de http relativo al hackeo de las aplicaciones?
4. El modelo de seguridad del navegador web.

Actividad → El alumno deberá desarrollar un resumen que explique las etiquetas HTML más importante.

OBJETIVOS:

Conocer la función de la autenticación de los usuarios y cómo almacenar los passwords de forma segura en el servidor.

Entender el concepto de sesión http y las técnicas y trucos que emplean los actores de la amenaza para secuestrar sesiones.

Comprender que es necesario filtrar la entrada para evitar ataques.

CONTENIDOS:

Módulo 2. Autenticación, gestión de sesiones, administración de la entrada de usuario y autorización (4horas)

1. Autenticación, contraseñas y su almacenamiento en el servidor.
2. Hashing de contraseñas y tablas Rainbow.
3. Procedimientos para el cambio del password.
4. Administración de la sesión.
5. Cross Site Request Forgery y otros ataques.
6. Consultas directas y parametrizadas. Otros tipos de inyección. La importancia de la codificación y la normalización.
7. Desbordamiento de búfer y Cross Site Scripting (XSS).

Actividad → El alumno deberá desarrollar un resumen que indique la mejor práctica para defenderse del ataque XSRF.

OBJETIVOS:

Conocer que la importancia de realizar una autorización correcta es la clave para que la aplicación no sea hackeada.

Entender la criptográfica asimétrica y cómo se emplea en las aplicaciones web.

Aprender a diseñar sistemas seguros y expresar la arquitectura mediante diagramas DFD.

CONTENIDOS:

Módulo 3. Autorización, hardening de sistemas, criptografía y diseño seguro de aplicaciones (4 horas)

1. Autorización y condiciones de carrera.
2. Hardening de servicios y servidores.
3. Criptografía asimétrica de clave pública.
4. Requisitos de seguridad y diseño seguro de aplicaciones.

Actividad → Crear un documento que incluya un diagrama de flujo de datos (DFD) de una arquitectura segura de una aplicación de tres capas.

OBJETIVOS:

Conocer que las vulnerabilidades están presentes a nivel de sistema operativo, servidor o aplicación. Estudiar las debilidades más frecuentes encontradas en el desarrollo web y determinar los tipos de inyección más habituales hoy en día.

CONTENIDOS:

Módulo 4. OWASP y el desarrollo seguro de aplicaciones (Parte I) (4 horas)

1. OWASP y las debilidades en las aplicaciones.
2. OWASP Top Ten.
3. A01:2021-Broken Access Control.
4. A02:2021-Cryptographic Failures.
5. A03:2021-Injection.
6. A04:2021-Insecure Design.

Actividad: →El alumno deberá desarrollar un fragmento de código que contenga una debilidad de inyección. Puede usar el lenguaje de programación de su interés.

OBJETIVOS:

Comprender los ataques a los que se enfrentan los protocolos inalámbricos comunes, y extender este conocimiento a redes bluetooth.

Entender las amenazas a las que se enfrenta la telefonía móvil.

CONTENIDOS:

Módulo 5. OWASP y el desarrollo seguro de aplicaciones (Parte II) (4 horas)

1. A05:2021-Security Misconfiguration.
2. A06:2021-Vulnerable and Outdated Components.
3. A07:2021-Identification and Authentication Failures.
4. A08:2021-Software and Data Integrity Failures.
5. A09:2021-Security Logging and Monitoring Failures.
6. A10:2021-Server-Side Request Forgery.

Actividad → El alumno deberá desarrollar un fragmento de código que inserte información sensible en el log de una aplicación. Puede usar el lenguaje de programación de su interés.

Sesiones online en directo → 20 horas

OBJETIVOS:

El principal objetivo de estas sesiones es que apliquen la parte elearning mediante ejercicios prácticos. Por ello, se usará la metodología flipped clasroom.

CONTENIDOS:

Sesión 1 Despliegue del laboratorio. OWASP ZAP, Burp suite, Nikto, → 4 horas.
(Relacionado con todos los módulos de elearning)

- **Temática a tratar**: Despliegue del laboratorio para hacer las prácticas. Despliegue de OWASP ZAP y tutorial de uso. Despliegue de Burp Suite y tutorial de uso. Despliegue de Nitko y tutorial de uso.

Sesión 2 Evaluación de vulnerabilidades en aplicaciones web. Parte I → 4 horas.
(Relacionado con todos los módulos de elearning)

- **Temática a tratar:**
  - Ataques de Inyección: Exfiltrar el esquema de la base de datos. Iniciar sesión con una cuenta que no existe. Iniciar sesión con la cuenta del administrador. Iniciar sesión con otro usuario. Realizar un ataque DoS NoSQL.
  - Romper la autenticación: Resetear la contraseña de un usuario por medio del procedimiento de restablecer contraseña olvidada. Cambiar la contraseña de un usuario. Iniciar sesión con una cuenta de usuario que ja sido borrada. Resolver el reto 2FA.
  - Exposición de datos sensibles: Ganar acceso a cualquier archivo log del servidor. Acceder a un archivo de backup olvidado por el programador. Robas datos personales sin usar inyección.

Sesión 3 Evaluación de vulnerabilidades en aplicaciones web. Parte II → 4 horas.
(Relacionado con todos los módulos de elearning)

- **Temática a tratar:**
  - Entidades externas XML: Recuperar el contenido de system.ini o /etc/passwd.
  - Validación de entrada inapropiada: Registrar un usuario con privilegios de administrador. obtener la membresía DeLuxe sin pagar por ello. Usar un cupón de una campaña finalizada. Hacer un pedido que te hará rico. Saltar un control de seguridad usando Poison Null Byte. Subir un archivo que no tiene extensión pdf ni zip.
  - Control de acceso inadecuado: Cambiar el nombre de un usuario mediante CSRF. Poner una valoración en nombre de otro usuario. Poner un producto en el carrito de otro cliente.

Sesión 4 Evaluación de vulnerabilidades en aplicaciones web. Parte III → 4 horas.
(Relacionado con todos los módulos de elearning)

- **Temática a tratar:**
  - Cross Site Scripting: Realizar un ataque XSS persistente. Saltar la política de Seguridad de Contenido y realizar un ataque XSS. Realizar un ataque XSS contra el DOM. Realizar un ataque XSS reflejado.
  - Deserialización insegura: Realizar una ejecución de código remoto. Deshabilitar permanentemente al chatbot. Ataque a la cadena de suministro. Detectar una biblioteca vulnerable que se usa en la app.

Sesión 5 Evaluación de vulnerabilidades en aplicaciones web. Parte IV → 4 horas.
(Relacionado con todos los módulos de elearning)

- **Temática a tratar:**
  - Seguridad a través de la ocultación: Delatar a un personaje notorio (Esteganografía)
  - Redirecciones: Forzar una redirección que no debería ocurrir.
  - Anti-automatización: Saltar el CAPTCHA.
  - Criptografía: Crear un cupón que otorgue un descuento del 80%. Detectar un algoritmo o biblioteca que no debería usarse.

La impartición de esta acción formativa se realizará mediante la modalidad flipped classroom más online en directo de la siguiente forma:

- El **contenido interactivo** estará **disponible** en la **plataforma** online, de manera que será de **libre consulta** para el alumnado y este deberá haberse organizado de manera autónoma bajo las recomendaciones que se le marquen para haber consultado la lección o módulo correspondiente.
    - Con ello lo que se busca es un mayor protagonismo en el proceso de E-A y que el alumnado se involucre más en el mismo, mejorando su trabajo individual.
- Posteriormente, en la **sesión online**, se tratará el caso de uso de lo que ya el estudiante ha visto y leído, por lo que su participación y motivación será mucho más activa.
    - El objetivo de esto es fomentar un aprendizaje más profundo y significativo de manera que son ellos los que buscan construir sus conocimientos, a la par que esto permitirá mejorar el trabajo colectivo mediante los proyectos que compartan.

Valor añadido → Permite atender a la diversidad del aula

Los alumnos visionan los contenidos tantas veces como quieran y tienen las tutorías del profesor para resolver sus dudas de manera individualizada.

¿A QUIÉN ESTÁ DIRIGIDO?

- Profesionales del sector TIC en Andalucía.
- Perfiles TIC de empresas de Andalucía.

CRITERIOS DE SELECCIÓN

Para la selección del público participante de esta acción formativa, se tendrá en cuenta por estricto orden de llegada de la solicitud:

- Que tenga estudios universitarios o de Formación Superior relacionada con la materia a impartir, como ingeniería, informática, matemáticas, estadística, física o asimiladas.
- Que sea trabajador del sector TIC andaluz, o que tenga perfil TIC y que trabaje en una empresa andaluza de cualquier otro sector.

En caso de que no se llenen las plazas totales del curso (45) se dará paso a otro tipo de perfiles.

CONOCIMIENTOS MÍNIMOS REQUERIDOS POR PARTE DEL ALUMNADO:

- Acceso a Internet
- Conocer algún lenguaje de programación.
- Conocimientos de ciberseguridad a nivel básico/medio.

REQUISITOS PARA REALIZAR LA PARTE DE LAS CLASES EN DIRECTO DE MANERA ÓPTIMA

- El alumno deberá disponer de un equipo con VirtualBox instalado. con un mínimo de 16GB de RAM y 4 cores.
- Previo al inicio de la parte online en directo, que se descarguen las VMs.
- La configuración del laboratorio se hará el primer día del online en directo.

EQUIPO DOCENTE

Antonio Salazar Graván

Ingeniero Técnico Informático por la Universidad de Cádiz, MCT de Microsoft desde 2012.

Especialista en Ciberseguridad e infraestructuras con más de 20 años de experiencia en formación y consultoría

https://www.linkedin.com/in/antonio-salazar-gravan/

CALENDARIO:

- **Fecha inicio del curso:**
  31/10/2023
- **Fecha impartición sesiones online en directo:**
- 13 al 17 de noviembre de 9 a 13 horas.
- **Fecha fin del curso:**
  24/11/2023

EVALUACIÓN:

Obligatorio para obtener el certificado:

- **[20%] La asistencia a las clases** o su visionado posterior. Estos vídeos se subirán a la plataforma y se establecerán los mecanismos para verificar que el alumnado que no asistió sí que visualizó el vídeo de manera asíncrona.
  - El mínimo de vídeos o asistencia a las clases para la titulación es de 4.
- **[30%] Visualización de contenido formativo.** Por medio de la lectura del SCORM.
  - Deberán ver al menos el 75% del contenido o lo que equivale a 4 módulos.
- **[30%] Realización de pruebas de conocimientos.** Que se colgarán mediante una batería de preguntas en la plataforma con orden aleatorio.
  - Deberán sacar un mínimo de un 5 al menos en 4 de los 5 módulos.

No es obligatorio, pero sí muy recomendable:

- **[20%] Actividades.** Serán de carácter no evaluable, pero servirá de preparación para las sesiones online en directo y además se ofrecerá retroalimentación.

CERTIFICADO

Una vez superadas todas las evaluaciones de los módulos del curso y habiendo asistido al número mínimo de clases exigido, podrás obtener la certificación.

El certificado se emitirá digitalmente en formato pdf incluyendo la siguiente información:

- Datos del alumno.
- Datos del curso: título, fecha de impartición, duración, contenidos impartidos.
- Sello y firma digitalizada de la empresa impartidora del curso. El certificado no lleva firma digital ni sello/firma de la Junta de Andalucía

Ten en cuenta que estos cursos no tienen validez académica ni acreditación de créditos universitarios.

OTRAS CUESTIONES DE INTERÉS DE ESTA ACCIÓN FORMATIVA:

Una posible orientación al tiempo dedicado al estudio, lectura y visualización del contenido sería la siguiente:

- Tiempo de consulta de contenidos y vídeos: 15 horas.
- Tiempo de realización de actividades: 1,5 horas.
- Tiempo de realización de exámenes: 2 horas.
- Tiempo de consulta en foros e interacción con los compañeros: 1,5 horas.
- Asistencia a las sesiones online en directo: 20 horas.

De todas formas y al tratarse de un curso abierto y parcialmente en línea, cada alumno podrá seguir su propio ritmo de aprendizaje siempre y cuando cumpla con los criterios mínimos de evaluación para la obtención del certificado de formación.