CURSO

DESARROLLO SEGURO DEVSECOPS (SSDLC)

Plan de estudio

educación IT

Nuestro propósito

Transformar positivamente la vida de las personas.

Queremos que seas protagonista en la transformación que estamos viviendo. Por eso, nos comprometemos a capacitarte para que estés al día con las necesidades digitales actuales.

Te invitamos a trabajar en conjunto para que descubras tu mejor versión y la potencies. Anímate, toma las riendas de tu futuro.

Code your future!

Contenido del curso

Aprende a prevenir ataques reales desde el código. Domina OWASP, SAST, DAST y más en un curso 100% práctico.

Prácticas en clase

A lo largo del curso aplicarás los conceptos vistos mediante ejercicios prácticos y laboratorios técnicos.

- Analizarás código vulnerable en aplicaciones reales para identificar errores comunes en la validación de entradas, control de acceso y manejo de sesiones.
- Utilizarás herramientas de análisis estático como SonarQube y Semgrep para detectar vulnerabilidades en el código fuente, y las integrarás a pipelines de CI/CD para automatizar la revisión de seguridad.
- Realizarás escaneos dinámicos con OWASP ZAP, explorando cómo detectar fallas en aplicaciones web desde una perspectiva externa.
- Configurarás políticas de seguridad a nivel de cabeceras HTTP, gestión de sesiones y protección de datos sensibles.
- Simularás escenarios de implementación de controles como autenticación multifactor, control de acceso basado en roles y protección contra ataques como SSRF.
- Trabajarás con modelos de amenazas, reportes de hallazgos y recomendaciones de remediación aplicables al ciclo de desarrollo real.

¿Qué aprenderás?

- SSDLC y diferencia del SDLC clásico
- Estándares clave: CWE, CVSS, OWASP ASVS.
- OWASP Proactive Controls
- SAST y su rol en el SSDLC.
- Instalación y configuración de SonarQube.
- Uso de Semgrep con reglas OWASP.
- DAST en SDLC.
- Uso de OWASP ZAP para escaneo pasivo/activo.
- Incorporación de SAST en pipelines CI/CD.
- Implementación de control de acceso.
- JWT, OAuth2, scopes y claims.
- Gitleaks.

Plan de estudios

1 Fundamentos de Desarrollo Seguro

- Introducción al desarrollo seguro.
- Estadísticas de vulnerabilidades
- Estadísticas de ataques reales.
- SSDLC y diferencia del SDLC clásico.
- Proceso SSDLC
- Evaluación de riesgos.
- Modelado de amenazas (STRIDE vs DREAD).
- Escaneo de código
- Evaluación de seguridad.
- Estándares clave: CWE, CVSS, OWASP ASVS.
- OWASP Proactive Controls.
- OWASP Proactive Controls (2018 vs. 2024).
- IA en estándares de seguridad.
- Introducción al rol de AppSec en equipos.
- C4: abordaje de seguridad desde el inicio.
- Pipelines y metodologías SSDLC.
- OWASP S-SDLC y Microsoft SDL.

2 Análisis Estático de Seguridad (SAST)

- Revisión de Código.
- Revisión Manual.
- Buscar funciones inseguras.
- Análisis de contexto de funciones.
- Limitaciones revisión manual.

- Falsos positivos.
- Almacenamiento código fuente.
- Control de versiones.
- SAST y su rol en el SSDLC.
- Instalación y configuración de SonarQube.
- Uso de Semgrep con reglas OWASP.
- Escaneo de código.
- Revisión de findings.
- IA para snippets de corrección.
- C5: Configuraciones seguras por defecto.
- C6: Mantener seguros tus componentes.
- Incorporación de SAST en pipelines CI/CD.
- Ejercicio práctico con findings reales.

3 Validación de entradas seguras

- C3: Validación de entradas y excepciones.
- DVWA/VAPT.
- OWASP Juice Shop.
- IA Aplicada al desarrollo.
- Datos confiables vs no confiables.
- Sanitización de vulnerabilidades.
- Inyección de comandos.
- Control de datos del usuario en formularios.
- Control de datos del usuario en APIs.
- SQL Injection.
- XSS: errores comunes en output encoding.
- OS Command Injection/File Upload inseguro.
- Deserialización/XXE/LDAP injection.

- Manejo seguro de errores y excepciones.

4 Análisis Dinámico Automatizado (DAST)

- DAST como complemento de SAST.
- DAST en SDLC.
- Pros y Contras DAST.
- Spiders y Crawlers.
- Uso de OWASP ZAP para escaneo pasivo/activo.
- Escaneos Autenticados.
- APIs con ZAP.
- ZAP CLI.
- Automatización de escaneos.
- ZAP2docker.
- Integración en pipelines CI/CD.
- Comparación de hallazgos entre SAST y DAST.
- Prioridad de vulnerabilidades.
- Explotación limitada.
- Reportes Automáticos DAST.
- C10: Prevención de SSRF.
- Otras herramientas de mercado.
- Análisis DAST con IA.
- IA para priorización.
- Buenas prácticas de remediación.

5 Seguridad: autenticación, sesiones y accesos

- C1: Implementar control de acceso.
- C7: Protección de identidades digitales.
- Autenticación fuerte y MFA.

- ID de sesiones débiles.
- Fuerza Bruta.
- Captchas Inseguros.
- JWT, OAuth2, scopes y claims.
- Bypass de Autorización.
- Prevención de CSRF.
- Manejo seguro de sesiones y tokens
- Cookies seguras
- Enumeracion de usuarios
- Recuperación de cuentas.
- Tiempo de vida de sesiones/tokens.
- SSO y federación de identidades.
- LLM para cumplimiento.

6 Criptografía, manejo de errores y cierre

- C2: Uso de criptografía para proteger datos.
- Cifrado Débil.
- Manejo inseguro de contraseñas y hashing.
- Gitleaks.
- Criptografía moderna.
- AES, RSA, SHA-256, bcrypt.
- Validación Cifrado con LLM.
- Gestión de secretos y claves.
- Rotación y caducidad de llaves y secretos.
- Certificados digitales.
- protección de datos en tránsito TLS/HTTPS.
- C8: funciones de seguridad del navegador.
- Headers HTTP: CSP, HSTS, X-Frame-Options.

- Análisis encabezados online.
- Análisis encabezados offline.
- Redirecciones abiertas HTTP
- CSP Bypass.
- C9: Registros y monitoreo de seguridad.
- Eventos críticos y respuesta a incidentes.
- Checklist de seguridad.

Modalidad del Curso

Duración
5 semanas / 18 h

Frecuencia semanal
2 encuentros de 2 h

Modalidad
Online en vivo

Grupos reducidos
Promedio 20 personas

Nivel: Intermedio

- [ ] Principiante
- [x] Intermedio
- [ ] Avanzado
- [ ] Experto

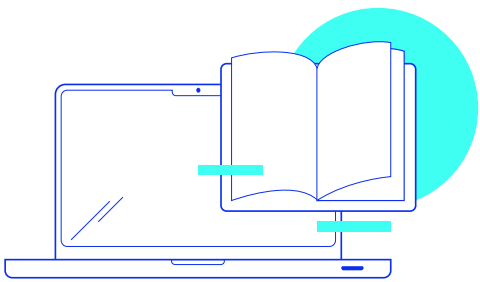
Requisitos

Es recomendable tener una base sobre:

Introducción a Python Introducción a Java Introducción a Bases de Datos y SQL

Dedicación fuera de clase

Además de las horas de clase, recomendamos que inviertas 4 h semanales extras para realizar los desafíos complementarios, estudiar el material de lectura y completar los exámenes del Alumni.



¿Cómo será tu experiencia?

Aprender haciendo

Ejercita y pon en práctica lo estudiado.

Trabajo en equipo

Une esfuerzos y potencia los resultados.

Clases grabadas

Consúltalas las veces que quieras.

Profesores expertos

Aprende de gigantes de la industria.

Asistente académico

Recibe soporte dentro y fuera de clase.

Plataforma Alumni

Encuentra recursos, materiales y clases.

¿Por qué Educación IT?

IT Créditos

Gana puntos al aprobar los exámenes de los cursos. Luego, podrás canjearlos por nuevos cursos sin costo alguno. Los IT Créditos que acumules no vencen ni se devalúan.

Garantía de aprendizaje

Si necesitas reforzar conceptos, recuperar clases o no estás satisfecho, ¡vuelve a tomar el curso sin ningún costo! Puede ser de forma total o parcial.

Comunidad en Discord

Mantente en contacto con la comunidad de EducaciónIT a través de nuestro servidor de Discord. Podrás hablar con tus compañeros, profesores, asistentes académicos y soporte.

Preguntas frecuentes

Si me pierdo una o más clases, ¿puedo recuperarlas?

Todas las clases quedan grabadas de por vida en tu plataforma Alumni. ¡Siempre podrás volver a verlas cada vez que lo necesites!

¿Cómo voy a aprender?

Te enfrentarás a situaciones de trabajo reales, en donde tendrás que aplicar lo aprendido de forma individual y en equipo. Por medio de la prueba y el error, irás superando desafíos y obteniendo nuevas habilidades que luego podrás aplicar en el ámbito laboral.

¿Cómo son las clases online en vivo?

Las clases duran entre 2 y 3 horas de lunes a viernes (sábados 3 o 4 hs) y se desarrollan de forma online en vivo en aulas virtuales, donde vas a poder interactuar con el instructor y tus compañeros.
Manejamos cupos reducidos para que puedas tener un seguimiento más personalizado durante tu aprendizaje.

Plan de estudio

Code your future

www.educacionit.com

@educacionit