EC-COUNCIL



EC-COUNCIL · PROGRAMA DE SEGURIDAD DE APLICACIONES

Certified Application Security Engineer (C|ASE) .NET

Construya aplicaciones .NET seguras en todas las fases del ciclo de desarrollo: requisitos, diseño, codificación, pruebas y despliegue

¿Por qué debería asistir?

El Certified Application Security Engineer (C|ASE) de EC-Council se enfoca en los procesos de desarrollo seguro de software. Es un curso práctico e integral que cubre las actividades de seguridad de todas las fases del ciclo de vida de desarrollo seguro (SDLC): planificar, crear, probar y desplegar una aplicación.

A diferencia de otras formaciones, va más allá de la codificación segura e incluye los requisitos de seguridad, el diseño robusto y la seguridad después del desarrollo. La versión .NET cierra una brecha real: pocos programas enseñan a los desarrolladores .NET a escribir código que, además de correcto, sea seguro. C|ASE prepara a ingenieros, analistas y testers de aplicaciones para construir software robusto frente a los desafíos operativos actuales.

3 días	24 h	10	6 fases	.NET
DURACIÓN	FORMACIÓN	MÓDULOS	SDLC SEGURO	PLATAFORMA



¿Quién debería participar?

Desarrolladores .NET
Desarrolladores .NET con un mínimo de dos años de experiencia que quieren escribir código seguro desde el inicio.

Futuros especialistas en AppSec
Personas que desean convertirse en ingenieros, analistas o testers de seguridad de aplicaciones.

Pruebas y calidad
Profesionales de pruebas y QA que evalúan vulnerabilidades en aplicaciones web y en el código fuente.

Gestión y protección de aplicaciones
Personas que participan en el desarrollo, las pruebas, la gestión o la protección de aplicaciones.

Objetivos de aprendizaje

- Comprender a fondo el SDLC seguro y sus modelos
- Conocer el OWASP Top 10, el modelado de amenazas y las pruebas SAST y DAST
- Capturar los requisitos de seguridad de una aplicación en desarrollo
- Definir, mantener y hacer cumplir las mejores prácticas de seguridad de aplicaciones
- Realizar revisiones de código manuales y automatizadas, y pruebas de seguridad de aplicaciones web
- Aplicar estándares de codificación segura basados en la guía OWASP o CERT Secure Coding
- Usar tecnologías de escaneo como AppScan, Fortify y WebInspect, inicio de sesión único y cifrado
- Calificar la severidad de los defectos y publicar reportes con los riesgos y sus mitigaciones

Seguridad en todas las fases del SDLC

Requisitos | Diseño | Desarrollo | Pruebas | Despliegue | Mantenimiento | OWASP Top 10 | SAST y DAST

Programa del curso

Duración: 3 días (24 horas)

Módulo	Contenido
Módulos 1–4 Día 1	01 **Seguridad de aplicaciones, amenazas y ataques:** necesidad de la seguridad de aplicaciones, amenazas y ataques comunes, OWASP Top 10 y SDLC seguro. 02 **Obtención de requisitos de seguridad:** definición de requisitos de seguridad, casos de abuso y de uso indebido, y casos de uso de seguridad. 03 **Diseño y arquitectura seguros de aplicaciones:** principios de diseño seguro, modelado de amenazas y arquitectura de seguridad. 04 **Prácticas de codificación segura para la validación de entradas:** validación de entradas en ASP.NET, ataques de inyección y XSS, y codificación de salida.
Módulos 5–7 Día 2	05 **Prácticas de codificación segura para autenticación y autorización:** mecanismos de autenticación en ASP.NET, gestión de contraseñas y autorización por roles. 06 **Prácticas de codificación segura para criptografía:** cifrado simétrico y asimétrico, hashing, firmas digitales y protección de datos en .NET. 07 **Prácticas de codificación segura para la gestión de sesiones:** ataques a la sesión (secuestro y fijación) y configuración segura de sesiones y cookies.
Módulos 8–10 Día 3	08 **Prácticas de codificación segura para el manejo de errores:** manejo de excepciones, páginas de error personalizadas, y registro y auditoría seguros. 09 **Pruebas estáticas y dinámicas de seguridad de aplicaciones (SAST y DAST):** revisión de código manual y automatizada, y escaneo de aplicaciones en ejecución. 10 **Despliegue y mantenimiento seguros:** configuración y endurecimiento del entorno de despliegue, actualizaciones de seguridad y evaluación de vulnerabilidades.



Examen

Duración: 2 horas

Título	Certified Application Security Engineer (C|ASE) .NET		
Código	312-95	**N.º de preguntas**	50
Formato	Opción múltiple	**Duración**	2 horas
Aprobación	70 %	**Plataforma**	EC-Council Exam Portal

Requisitos de elegibilidad

- **Capacitación oficial:** completar la formación oficial C|ASE con un partner acreditado de EC-Council (centro de formación acreditado, iWeek o iLearn). La cuota de solicitud de US$100 aplica salvo que esté incluida en la formación.
- **Miembros ECSP (.NET/Java):** miembros activos y al día no pagan una cuota de solicitud adicional.
- **Experiencia:** al menos dos años de experiencia en seguridad de la información o desarrollo de software, con una cuota de solicitud no reembolsable de US$100.
- **Certificaciones equivalentes:** por ejemplo GSSP .NET/Java, con una cuota de solicitud no reembolsable de US$100.

Certificación C|ASE

El examen C|ASE puede presentarse al completar la formación oficial. Quienes lo aprueban reciben su certificado C|ASE y los beneficios de membresía de EC-Council, y deben cumplir las políticas de educación continua de EC-Council. La certificación demuestra el dominio de los conocimientos y habilidades necesarios para manejar las vulnerabilidades comunes del software de aplicación.

Información general

- 24 horas de formación oficial, práctica y centrada en el SDLC seguro
- Revisión de código y pruebas con herramientas de escaneo como AppScan, Fortify y WebInspect
- EC-Council es una organización acreditada bajo la norma ISO/IEC 17024 y reconocida por la Directiva 8140/8570 del DoD