C)SWAE™
CERTIFIED SECURE WEB APPLICATION ENGINEER

mile2®
CYBER SECURITY CERTIFICATIONS

Certified Secure Web Application Engineer

DATOS CLAVE

Nombre del curso:

C)SWAE

Duración: 4 días

Pre-requisitos:

- Un mínimo de 12 meses de experiencia en redes
- Conocimientos técnicos de TCP/IP
- Conocimiento de software de Microsoft
- Network+, Microsoft, Security+
- Conocimiento básico de Linux es esencial

Materiales:

- Manual de Estudiante
- Manual de Lab de Estudiante
- Software y Herramientas

Examen de Certificación:

- CSWAE –Certified Secure Web App Engineer

Track de Certificaciones:

- CPTE - Certified Pen Testing Engineer™
- CEH - Certified Ethical Hacker™
- CPEH - Certified Professional hacker™
- CSWAE –Certified Secure Web App Engineer

Puntaje de aprobación: 70%

OBJETIVO DEL CURSO

Internet es uno de los sitios más peligrosos para hacer negocios hoy en día. Todos los días compañías y gobierno son víctimas de ataques vía internet. En muchos casos, los ataques pudieran ser fácilmente frustrados pero hackers, bandas criminales organizadas y agentes extranjeros son capaces de explotar las debilidades de las aplicaciones web y la arquitectura. El programador Web Secure sabe cómo identificar, mitigar y defender contra todos los ataques, a través del diseño y la construcción de sistemas resistentes al fracaso. El desarrollador de aplicaciones web seguro, sabe cómo desarrollar aplicaciones web que no sean blanco de las vulnerabilidades comunes, y cómo probar y validar que sus aplicaciones sean seguras, fiables y resistentes al ataque. El curso Secure Web Application Engineer provee al desarrollador comprensión profunda y amplia de los conceptos de aplicaciones seguras, principios y normas. El desarrollador será capaz de diseñar, desarrollar y probar aplicaciones web que ofrezcan servicios web confiables que cumplan con los requisitos funcionales del negocio y satisfacer las necesidades de cumplimiento y garantía.

BENEFICIOS DEL CURSO

Los graduados del curso Certified Secure Web Application Engineer obtendrán conocimiento real de la seguridad mundial que les permita reconocer las vulnerabilidades, explotar las debilidades del sistema y ayudar a proteger contra las amenazas.

BENEFICIOS DEL CURSO

Las aplicaciones web son cada vez más sofisticadas y, como tal, son críticas para casi todas las grandes empresas en línea. Conforme más aplicaciones web aparezcan, el número de problemas de seguridad crecerá, las vulnerabilidades locales tradicionales, etc. La responsabilidad de la seguridad de los sistemas sensibles dependerá del desarrollador web, más que del vendedor o el administrador del sistema. Al igual que con la mayoría de los problemas de seguridad relacionados con cliente / servidor de comunicaciones, las vulnerabilidades de aplicaciones web en general se derivan del manejo inadecuado de las solicitudes de cliente y / o la falta de validación de entrada por parte del desarrollador .El curso Certified Secure Web Application Engineer enseña a los estudiantes a detectar varios problemas de seguridad en aplicaciones web e identificar las vulnerabilidades y riesgos.

Certified Secure Web Application Engineer

AL CONCLUIR

Al finalizar los estudiantes de CSWAE podrán realizar con seguridad el examen de certificación CSWAE (recomendado). Los estudiantes disfrutarán de un curso en profundidad que se actualiza continuamente para mantener e incorporar la aplicación web en constante cambio y las tecnologías de código seguro.

MÓDULOS DEL CURSO

Module 1 : Web Application Security

- **Lab**: Environment Setup - Lab

Module 2 : OWASP TOP 10

- **Lab**: Environment Setup - Lab

Module 3 : Theat Modeling & Risk Management

- **Lab**: Threat Modeling and Architecture Risk Analysis
- **Lab:** Quick Threat Modeling (the Doctor use case)

Module 4 : Application Mapping

- **Lab**: Web Application Mapping using Ethical Hacking Tools

Module 5 : Authentication and Authorisation attacks

- **Lab**: Client Side, Authentication and Authorization Attacks

Module 6 : Session Management attacks

- **Lab**: Session Management, Access Controls and Configuration Attacks

Module 7 : Application Logic attacks

- **Lab**: Application Logic, Information Disclosure and Data Transmission Attacks

Module 8 : Data Validation

- **Lab: Cert Java Oracle Secure Coding IDS**

Module 9 : AJAX attacks

- **Lab**: AJAX, Web Services and Server Attacks

Module 10 : Code Review and Security Testing

- **Lab**: Performing Code review and Building Security Test Scripts

Module 11 : Web Application Penetration Testing

- **Lab**: Performing Web Application PenTesting steps

Module 12 : Secure SDLC

- **Lab**: Case Study and Web Penetration Testing Assignment

Module 13 : Cryptography

- **Lab**: Encryption in Secure Coding (Example for Java, PHP and .NET)

Los cursos de Mile2 están acreditados por NSA CNSS 4011-4016, en Homeland's Security National, NICCS training schedule, preferido por el FBI Nivel 1-3.