C)SWAE™
CERTIFIED SECURE WEB APPLICATION ENGINEER

Certified Secure Web Application Engineer™

DATOS CLAVE

Nombre del curso
CSWAE™

Duración: 32 horas

Pre-requisitos:

- Un mínimo de 12 meses de experiencia en redes
- Sólidos conocimientos de TCP/IP
- Conocimiento de paquetería Microsoft
- Network+, Microsoft, Security+
- Coocimiento básico de Linux (esencial)

Materiales digitales:

- Manual de Referencia

Examen de Certificación:

- CSWAE - Certified Secure Web Application Engineer™

OBJETIVOS 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.

DESCRIPCIÓN 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.

CNSS

SC 0010 1001 0101 TM
SECURE CODING

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

Módulo 1
Web Application Security
Web Application Technologies and Architecture
Application Flaws and Defense Mechanisms
The Open Web Application Security Project (OWASP)

Módulo 2
Application Mapping
Threat Modeling
Architecture Risk Analysis
Lab: Threat Modeling and Architecture Risk Analysis

Módulo 4
Application Security Toolbox
Setting up a Testing Environment
Lab: Setting up a Security Testing Environment

Módulo 5
Client Side Attacks
Authentication Attacks
Authorization Attacks
Lab: Client Side, Authentication and Authorization Attacks

Módulo 6
Session Management Attacks
Access Control Attacks
Environment Configuration Attacks
Lab: Session Management, Access Controls and Configuration Attacks

Módulo 7
Application Logic Attacks
Information Disclosure Exploits
Data Transmission Attacks
Lab: Application Logic, Information Disclosure and Data Transmission Attacks

Módulo 8
AJAX Attacks
Web Services Attacks
Application Server Attacks
Lab: AJAX, Web Services and Server Attacks

Módulo 9
Insecure Code Discovery and Mitigation
Developing Security Testing Scripts
Lab: Performing Code review and Building Security Test Scripts

Módulo 10
Secure-Software Development Lifecycle (SDLC) Methodology
Web Hacking Methodology
Laboratorio: Estudio de caso y asignación de prueba de penetración web

5584215929
www.bitnueve.mx
@bitnuevemx
cursos@bitnueve.mx
Bitnuevemx