CSWAE
Certified Secure Web Application Engineer

Overview

Organizations and governments fall victim to internet-based attacks every day. In many cases, web attacks could be thwarted but hackers, organized criminal gangs, and foreign agents are able to exploit weaknesses in web applications. The Secure Web programmer knows how to identify, mitigate and defend against all attacks through designing and building systems that are resistant to failure. The secure web application developer knows how to develop web applications that aren't subject to common vulnerabilities, and how to test and validate that their applications are secure, reliable and resistant to attack.

Upon Completion

Upon completion, Certified Secure Web Application Engineer students will be able to establish industry acceptable auditing standards with current best practices and policies. Students will also be prepared to competently take the C)SWAE exam.

Course Length

5 days

Format

- Instructor-led classroom
- Live Online Training

Prerequisites

- A minimum of 24 months' experience in software technologies & security
- Sound knowledge of networking
- At least one coding Language
- Linux understanding
- Open shell

Student Materials

- Student Workbook
- Student Lab Guide
- Exam Prep Guide

Certification Exam

Mile2's CSWAE- Certified Secure Web Application Engineer.

Who Should Attend?

- Coders
- Web Application Engineers
- IS Managers
- Application Engineers
- Developers
- Programmers

Course Outline

- Module 1: Web Application Security
- Module 2: OWASP Top 10
- Module 3: Threat Modeling & Risk Management
- Module 4: Application Mapping
- Module 5: Authentication and Authorization Attacks
- Module 6: Session Management Attacks
- Module 7: Application Logic Attacks
- Module 8: Data Validation
- Module 9: AJAX Attacks
- Module 10: Code Review And Security Testing
- Module 11: Web Application Penetration Testing
- Module 12: Secure SDLC
- Module 13: Cryptography

Lab Outline

- Module 1: Environment Setup and Architecture
- Module 2: OWASP TOP 2013: Session Management Attacks
- Module 3: Threat Modeling
- Module 4: Application Modeling and Analysis
- Module 5: Authentication and Authorization Attacks
- Module 6: Session Management Attacks
- Module 9: AJAX Security
- Module 10-1: Code Review
- Module 10-2: Security Test Scripts
- Module 10-3: Writing Java Secure Code
- Annex 11: Alternatives Labs
- Lab 11-1 4: WebGoat & WebScarab
- Lab 11-2: WebGoat - Cross-Site Request Forgery (CSRF)
- Lab 11-3 Missing Function Level Access Control
- Lab 11-4: Perform Forced Browsing Attacks