C)SWAE: Secure Web Application Engineer

Course ID #: 7000-781-ZZ-Z

Hours: 35

Course Content

Course Description:

In this course you will cover 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.

Course Objectives:

Upon successful completion of this course, students will be able to:

- Establish industry acceptable auditing standards with current best practices and policies
- Competently take the C)SWAE exam

Prerequisites:

- 24 months experience in software technologies and security
- Sound knowledge of networking
- At least one coding language
- Linux understanding
- Open shell

Target Audience:

- Pen Testers
- Security Officers
- Ethical Hackers
- Network Auditors
- Vulnerability assessors
- System Owners and Managers
- Cyber Security Engineers

Topics:

Module 1: Web Application Security

- Web Application Security
- Web Application Technologies and Architecture
- Secure Design Architecture
- Application Flaws and Defense Mechanisms
- Defense In-Depth
- Secure Coding Principles

Module 2: OWASP TOP 10

- The Open Web Application Security Project (OWASP)
- OWASP TOP 10 for 2017 & 2018

C)SWAE: Secure Web Application Engineer

Course ID #: 7000-781-ZZ-Z

Hours: 35

Module 3: Threat Modeling & Risk Management

- Threat Modeling Tools & Resources
- Identify Threats
- Identify Countermeasures
- Choosing a Methodology
- Post Threat Modeling
- Analyzing and Managing Risk Incremental Threat Modeling
- Identify Security Requirements
- Understand the System
- Root Cause Analysis

Module 4: Application Mapping

- Application Mapping
- Web Spiders
- Web Vulnerability Assessment
- Discovering other content
- Application Analysis
- Application Security Toolbox
- Setting up a Testing Environment

Module 5: Authentication and Authorization attacks

- Authentication
- Different Types of Authentication (HTTP, Form)
- Client Side Attacks
- Authentication Attacks
- Authorization
- Modeling Authorization
- Least Privilege
- Access Control
- Authorization Attacks
- Access Control Attacks
- User Management
- Password Storage
- User Names
- Account Lockout
- Passwords
- Password Reset
- Client-Side Security
- Anti-Tampering Measures
- Code Obfuscation
- Anti-Debugging

Module 6: Session Management attacks

- Session Management Attacks
- Session Hijacking
- Session Fixation
- Environment Configuration Attacks

Module 7: Application Logic attacks

- Application Logic Attacks
- Information Disclosure Exploits
- Data Transmission Attacks

Module 8: Data Validation

- Input and Output Validation
- Trust Boundaries
- Common Data Validation Attacks
- Data Validation Design
- Validating Non-Textual Data
-
-
- Validation Strategies & Tactics
- Errors & Exception Handling
- Structured Exception Handling
- Designing for Failure
- Designing Error Messages
- Failing Securely

Module 9: AJAX attacks

- AJAX Attacks
- Web Services Attacks
- Application Server Attacks

Module 10: Code Review and Security Testing

- Insecure Code Discovery and Mitigation
- Testing Methodology
- Client Side Testing
- Session Management Testing
- Developing Security Testing Scripts
- Pen testing a Web Application

C)SWAE: Secure Web Application Engineer

Course ID #: 7000-781-ZZ-Z

Hours: 35

Module 11: Web Application Penetration Testing

- Insecure Code Discovery and Mitigation
- Benefits of a Penetration Test
- Current Problems in WAPT
- Learning Attack Methods
- Methods of Obtaining Information
- Passive vs. Active Reconnaissance
- Footprinting Defined
- Introduction to Port Scanning
- OS Fingerprinting
- Web Application Penetration Methodologies
- The Anatomy of a Web Application Attack
- Fuzzers

Module 12: Secure SDLC

- Secure-Software Development Lifecycle (SDLC) Methodology
- Web Hacking Methodology

Module 13: Cryptography

- Overview of Cryptography
- Key Management
- Cryptography Application
- True Random Generators (TRNG)
- Symmetric/Asymmetric Cryptography
- Digital Signatures and Certificates
- Hashing Algorithms
- XML Encryption and Digital Signatures Authorization Attacks

NOTE: Student will use Kali Linux

Labs:

Lab 1 – Environment Setup and Architecture
Lab 2 – OWASP TOP 10 2013
Lab 3 – Threat Modeling
Lab 4 – Application Mapping & Analysis
Lab 5 – Authentication and Authorization attacks
Lab 06 - Session Management attacks
Lab 9 – AJAX Security
Lab 10 – Code Review and Security Testing
Lab 11: Alternatives Labs

Accreditations:

Register for this class by visiting us at:
www.tcworkshop.com or calling us at 800-639-3535