MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

Accredited by:

GLOBAL ACE CERTIFICATION

Certified Secure Web Application Developer (CSWAD)

Certification

This course explores on the application of secure software development life cycle framework focusing in PHP programming specifically in developing, testing, managing, or securing PHP based applications. Participants will be able to identify possible security issues, perform code reviews, and review application logs.

Terminal Objectives

- To define the framework of Secure Software Development Life Cycle (SSDLC).
- To identify application security component required in each phase of Software Development Life Cycle (SDLC), Requirement, Design, Development, Testing, Deployment and Maintenance.
- To conduct the hands-on for threat modelling and the interpretations of the result.
- To conduct hands-on for PHP source code review to ensure that methodologies are covered, and recommended solutions are implemented based on industry's best practice.
- To conduct hands-on for application development self-validation.
- To define the secure deployment mechanisms, process that includes using relevant tools, standard or best practices (e.g. OWASP, CWE, CIS, & etc).
- To determine countermeasures and mitigations against potential exploitations of application frameworks and software vulnerabilities based on threat modelling results.
- To identify and plan the application patches or the extent of releases that are compatible to the application to sustain application's integrity and availability.

Target Participants

- Developer, security architects, software engineer/designer.

Certified Examination

The CSWAD examination is certified by the Global ACE Certification. The examination framework is designed to align with a set of relevant Knowledge, Skills and Attitudes (KSA) that are necessary for a Secure Application Professional. Candidates will be tested via a combination of either continual assessment (CA), multiple choice (MC), theory/ underpinning knowledge assessment (UK), practical assessment (PA), assignments (AS) and case studies (CS) as required.

Candidates can take the examination at authorized examination centres in participating member countries. Candidates who have successfully passed the CSWAD examination will be eligible to apply as an associate or professional member by fulfilling the membership criteria defined under the Global ACE Certification.

Program Outline

Module 1: The need for S.S.D.L.C

1. The concept of Secure Software Development Life Cycle (S.S.D.L.C)
2. Software Development Life Cycle (SDLC) as of today and its frameworks
3. The difference between SDLC and S.S.D.L.C
4. The phases of S.S.D.L.C and security activities
5. Run PoC
6. The concept of Web Application Vulnerabilities (OWASP Top 10 vs. ASVS)

Module 2: Security Requirement & Design

1. The Concept of Security Requirement
2. Define Security Requirement
3. Use Case: Misuse Case & Security Use Case
4. Tools & Hands-on Exercises
5. Concept of Secure Design
6. Common Security Activities in Secure Design (Design Principles, Architecture Review, Threat Modelling)
7. Tools & Hands-on Exercises

Module 3: Securing the PHP Source Code

1. Secure Coding Implementation based on OWASP Top 10 and ASVS v4.0
2. Tools & Hands-on Exercises based on
   - A1: Injection
   - A2: Broken Authentication
   - A3: Sensitive Data Exposure
   - A4: XML External Entities (XXE)
   - A5: Broken Access Control
   - A6: Security Misconfiguration
   - A7: Cross-Site Scripting (XSS)
   - A8: Insecure Deserialization
   - A9: Using Components with Known Vulnerabilities
   - A10: Insufficient Logging & Monitoring

Program Outline

Module 4: Self-Secure Validation

1. Testing Framework
2. Identified Attack Vectors
3. Security Testing Component
4. Self-Secure Validation Test
5. Tools & Hands-on Exercises based on
   - A1: Injection
   - A2: Broken Authentication
   - A3: Sensitive Data Exposure
   - A4: XML External Entities (XXE)
   - A5: Broken Access Control
   - A6: Security Misconfiguration
   - A7: Cross-Site Scripting (XSS)
   - A8: Insecure Deserialization
   - A9: Using Components with Known Vulnerabilities
   - A10: Insufficient Logging & Monitoring

For additional information, please visit www.cybereducationscheme.org. You can also contact us at training@cybersecurity.my or call at 03 8800 7999

CyberSecurity Malaysia,
Level 7, Tower 1, Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor Darul Ehsan, Malaysia

Tel: +603 8800 7999 **Fax:** +603 8008 7000
Email : info@cybersecurity.my
Customer Service Hotline: 1 300 88 2999
Website: www.cybersecurity.my