MINISTRY OF DIGITAL

CyberSecurity MALAYSIA

Accredited by:

GLOBAL ACE CERTIFICATION

Certified Secure Application Professional (CSAP)

Certification

Certified Secure Application Professional (CSAP) is a 4 days hands-on training and certification programme that designed specifically to understand the basics of cryptography; presenting the main ideas in simple language. Important areas are highlighted, such as Stream Cipher, block ciphers, public key algorithms, digital signatures, and applications as well as a historical look at the field.

Terminal Objectives

- Understand the basic concepts of secure coding
- Learn the Open Web Application Security Project (OWASP) and Common Weakness Enumeration (CWE) secure coding standards on security vulnerabilities
- Learn the detail of the Open Web Application Security Project (OWASP) Top Ten secure coding practices and examples of application source code security vulnerabilities
- To identify and to avoid the common coding mistakes
- To examine application source code vulnerabilities and demonstrate how the issues are exploited by attackers
- To ensure the participants have understand the course and apply the knowledge into software development

Target Participants

- Cyber Security Professionals
- Information Security officers/ ISMS Manager
- ICTSOs/CIOs/CISOs/CSOs/CTOs
- Security auditors, governance and compliance officers
- Application Developers, Software Engineers and Programmers

Certified Examination

The CSAP 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 an Information Security Awareness Manager. 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 scheme member countries. Candidates who have successfully passed the CSAP examination will be eligible to apply as an associate or professional member by fulfilling the membership criteria defined under the Global ACE Scheme.

Program Outline

Day 1

Session 1 : The Concept of Secure Coding
Session 2 : Introduction of Web Security and Secure Coding organizations
Session 3 : Classification of security flaws
3.1 OWASP TOP 10
3.2 CWE/SANS TOP 25
3.3 Secure Coding Guide in South Korea
Session 4 : Configuration of test application for exercise

Day 2

Session 5 : Software weakness

5.1 SQL Injection
a) Security Breach Examples
b) SQL Injection Definition
c) Exercise - How to test application for SQL Injection
d) Exercise - How to write secure code

5.2 Directory Path Traversal
a) Security Breach Examples
b) Directory Path Travesal Definition
c) Exercise - How to test application for Directory Path Tranversal
d) Exercise - How to write secure code

5.3 Cross-Site Scripting (XSS)
a) Security Breach Examples
b) XSS Definition
c) Exercise - How to test application for XSS
d) Exercise - How to write secure code

- 5.4 OS Command Injection
  - a) Security Breach Examples
  - b) OS Command Injection Definition
  - c) Exercise - How to test application for OS Command Injection
  - d) Exercise - How to write secure code
- 5.5 URL Redirection to Untrusted Site
  - a) Security Breach Examples
  - b) URL Redirection to Untrusted Site Definition
  - c) Exercise - How to test application for URL Redirection to Untrusted Site
  - d) Exercise - How to write secure code
- 5.6 Xpath Injection
  - a) Security Breach Examples
  - b) Xpath Injection Definition
  - c) Exercise - How to test application for Xpath Injection
  - d) Exercise - How to write secure code
- 5.7 HTTP Response Splitting
  - a) Security Breach Examples
  - b) HTTP Response Splitting Definition
  - c) Exercise - How to test application for HTTP Response Splitting
  - d) Exercise - How to write secure code
- 5.8 Reliance on Untrusted Inputs in a Security Decision
  - a) Security Breach Examples
  - b) Reliance on Untrusted Inputs in a Security Decision Definition
  - c) Exercise - How to test application for Reliance on Untrusted Inputs in a Security Decision
  - d) Exercise - How to write secure code
- 5.9 Use of a Broken or Risky Cryptographic Algorithm
  - a) Security Breach Examples
  - b) Use of a Broken or Risky Cryptographic Algorithm
  - c) Exercise - How to test application for Use of a Broken or Risky Cryptographic Algorithm
  - d) Exercise - How to write secure cod

Day 3

Session 5: Software weakness (continued)

- 5.10 Cleartext Transmission of Sensitive Information
  - a) Security Breach Examples
  - b) Cleartext Transmission of Sensitive Information Definition
  - c) Exercise - How to test application for Cleartext Transmission of Sensitive Information
  - d) Exercise - How to write secure code
- 5.11 Cleartext Storage of Sensitive Information
  - a) Security Breach Examples
  - b) Cleartext Storage of Sensitive Information Definition
  - c) Exercise - How to test application for Cleartext Storage of Sensitive Information
  - d) Exercise - How to write secure code
- 5.12 Hard-Coded Credentials
  - a) Security Breach Examples
  - b) Hard-Coded Credentials Definition
  - c) Exercise - How to test application for Hard-Coded Credentials
  - d) Exercise - How to write secure code
- 5.13 Use of Hard-Coded Cryptographic Key
  - a) Security Breach Examples
  - b) Use of Hard-Coded Cryptographic Key Definition
  - c) Exercise - How to test application for Use of Hard-Coded Cryptographic Key
  - d) Exercise - How to write secure code
- 5.14 Information Exposure Through Persistent Cookies
  - a) Security Breach Examples
  - b) Information Exposure Through Persistent Cookies Definition
  - c) Exercise - How to test application for Information Exposure Through Persistent Cookies
  - d) Exercise - How to write secure code
- 5.15 Information Exposure Through Comments
  - a) Security Breach Examples
  - b) Information Exposure Through Comments Definition
  - c) Exercise - How to test application for Information Exposure Through Comments
  - d) Exercise - How to write secure code
- 5.16 Error Handling
  - a) Security Breach Examples
  - b) Error Handling Definition
  - c) Exercise - How to test application for Error Handling
  - d) Exercise - How to write secure code
- 5.17 Null Pointer Dereference
  - a) Security Breach Examples
  - b) Null Pointer Dereference Definition
  - c) Exercise - How to test application for Null Pointer Dereference
  - d) Exercise - How to write secure code
- 5.18 Improper Resource Shutdown or Release
  - a) Security Breach Examples
  - b) Improper Resource Shutdown or Release Definition
  - c) Exercise - How to test application for Improper Resource Shutdown or Release
  - d) Exercise - How to write secure code
- 5.19 Reliance on Reverse DNS Resolution for a Security-Critical Action
  - a) Security Breach Examples
  - b) Reliance on Reverse DNS Resolution for a Security-Critical Action Definition
  - c) Exercise - How to test application for Reliance on Reverse DNS Resolution for a Security-Critical Action
  - d) Exercise - How to write secure code

Day 4

Workshop