Module Title : Certified Secure Application Professional (CSAP)

Duration : 4 days

Overview

Everyday cybercriminals are looking for ways to penetrate the systems for their evil intentions. The recent rising trend of ransomware is also exploiting the unsecured systems to infect many other users or organizations. Therefore, the need for Malaysia to develop secure coding has become an important and urgent issue to protect organizations in Malaysia.

Objective

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

Target Participants

1. Cyber Security Professionals
2. Information Security officers/ ISMS Manager
3. ICTSOs/CIOs/CISOs/CSOs/CTOs
4. Security auditors, governance and compliance officers
5. Application Developers, Software Engineers and Programmers

Agenda

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

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

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