Course Introduction

Today is programming developer must be able to efficiently understand the concept of secure coding techniques to develop a secure application. In order to provide a total secure solutions from operating system level to application level. This course provides all those necessary skills for programming developer to understand how to write a secure PHP Application technique of major systems. In this course, you will learn current web application threats and how to add security to your PHP Web applications and PHP Open source CMS/Blog (Wordpress). It is assumed that you have been coding PHP Web applications for at least a year, so it won t cover the basics of the language (either conventions or syntax). The goal is to make you more aware of what you should be doing to secure the Web applications you are building.

Course Objectives

- Attendee of this program will have the knowledge and skills needed to meet the real-world challenges faced by programming developer. They can prevent suspicious activities that might compromise the system and application. A secure coding can provide an advance security on systems.

Learning Level

- Intermediate

Course Duration

- 3 Days

Course Prerequisite

- SDLCF

Target Group

- Web Application Developer

Software Quality Assuror

IT Manager

Course Outline

PHP Secure Coding

1. Introduction to Web Security

– Challenges

– Open Web Application Project (OWASP)

– Documents and Standard

– OWASP Top 10

2. Injection Flaw

– SQL Injection

– Common Defence

– Regular Expression

– Parameterized Query

– Case Study

3. Broken Authentication

– Attack Vector

– Session Hijack

– Common Defence

– Case Study

4. Sensitive Data Exposure

– Attack Vector

– Common Defence

– Case Study

5. XML External Entities (XXE)

– XXE Injection

– Common Defence

6. Broken Access Control

- – Horizontal Access Control
- – Vertical Access Control
- – Common Defence
- – Auth and Authorization Framework

7. Security Misconfiguration
   - – Common Defence
   - – Secure Header Project
   - – Case Study

8. Cross-Site Scripting(XSS)
   - – Understanding XSS
   - – Common Defence
   - – Case Study

9. Insecure Deserialization
   - – Serialization and Deserialization
   - – Common Defence
   - – Case Study

10. Using Components with known vulnerability
    - – Exploitation Database
    - – Common Defence
    - – OSS Bill of Material

11. Insufficience Logging and monitoring
    - – Common Defence
    - – Incident Response
    - – App Sensor