

Building Security into your PHP Applications (SEC)

Days of Training: 1

Overview

Security is one of the most important things to keep in mind when developing web applications. Unfortunately, it is also one of the things often overlooked. Reviewing hundreds or thousands of lines of code is a daunting task, one that can be avoided if an application is developed with security in mind. This PHP class presents a comprehensive overview of security and has been designed to equip PHP developers with the knowledge they need to build more secure web applications. Participants apply what they have learned by identifying and correcting security flaws within a practice application.

Audience

This course is designed for experienced PHP application developers who want to learn or be reminded of security best practices. New PHP developers can also benefit from taking this course, to learn best practices for building security into the applications they are learning to create, although some of the material may seem a little advanced.

Pre-requisite(s)

Basic knowledge of PHP 5

Price

SG\$800 before GST

Objectives

Upon completing the course, participants will be prepared to:

- Incorporate standard, best practice security measures into their PHP applications
- Identify the most common types of vector attacks and how best to monitor and guard against them

Topics Include

What is Security
The Defense in Depth Concept
Security's Basic Rules
Guidelines for Building Secure Web Applications
Injection Attacks (SQL, XSS, Command, Remote Code)
XSRF Attacks
Session Security
Secure File Uploads
Creating Secure Configurations
Password Security
Sandboxes & Tarpits
Security through Obscurity
Security Implications for AJAX
Filtering for Charsets

MSM6427-ILT