# 3 Days Course on
# PHP Secure Programming

## Course Overview

PHP as a programming language is easy to learn and easy to use. This is also the reason for its popularity. Unfortunately, PHP does not only make it easy to write applications, it also comes with certain features that make it easy to write insecure code. This course gives guidelines on how to avoid dangerous language constructs and features. Moreover, it gives instructions on how to perform proper security checks that help to defend against common attacks. Each section deals with a specific security problem or function group and is accompanied by a list of recommendations. These recommendations can be used as a checklist during the development phase and for security assessments.

## Prerequisites

Have knowledge and/or experience in HTML, SQL, and PHP programming.

## Course Settings

| | |
|---|---|
| Date | Refer to Training Calendar |
| Venue | Refer to Training Calendar |
| Fees | Contact Us at sales@2-sigma.com |
| Timings | 0900-1700 (3 Days) |
| Inclusive | Certificates and notes |
| Audience | IT Officer, Web Application Developer and Programmer |

# PHP Security -Schedule

| Day 1 | |
|---|---|
| 09.00am – 10.00am | **Overview**<br>• What is PHP security?<br>• Basic steps<br>• Register globals |
| 10.00am – 10.30am | Breakfast |
| 10.30am – 12.45pm | **Security Principles**<br>• Defense in depth<br>• Least privilege<br>• Simple is beautiful<br>• Minimum Exposure |
| 12.45pm – 02.15pm | Lunch |
| 02.15pm – 05.00pm | **Security Practices**<br>• Balance risk & usability<br>• Track data<br>• Filter input<br>• Escape output<br>**Forms & URLs**<br>• Forms & data<br>• Semantic URL attacks<br>• File upload attacks<br>• Cross-site scripting<br>• Cross-site Request Forgeries<br>• Spoofed form submissions<br>• Spoofed HTTP requests |
| **Day 2** | |
| 09.00am – 10.00am | **Database & SQL**<br>• Exposed access credentials<br>• SQL Injection<br>• Exposed data |
| 10.00am – 10.30am | Breakfast |
| 10.30am – 12.45pm | **Sessions and Cookies**<br>• Cookie theft<br>• Exposed Session data<br>• Session fixation<br>• Session hijacking |
| 12.45pm – 02.15pm | Lunch |
| 02.15pm – 05.00pm | **Include Files**<br>• Exposed source code<br>• Backdoor URLs<br>• Filename manipulation<br>• Code injection<br>**Files & Commands** |

| | |
|---|---|
| | • Travesing the filesystem<br>• Remote file risks<br>• Command injection |
| **Day 3** | |
| 09.00am – 10.00am | **Authentication and Authorization**<br>• Brute force attacks<br>• Password sniffing<br>• Reply attacks<br>• Persistent Logins |
| 10.00am – 10.30am | Breakfast |
| 10.30am – 12.45pm | **Secure operations**<br>• Captcha<br>• Input validations |
| 12.45pm – 02.15pm | Lunch |
| 02.15pm – 05.00pm | **Secure Environment**<br>• mod_security<br>• Suhosin<br>• Intrusion detection system |

## More Information

**Two Sigma Technologies**
19-2, Jalan PGN 1A/1, Pinggiran Batu Caves,
68100 Batu Caves, Selangor
Tel: 03-61880601/Fax: 03-61880602

To register, please email to sales@2-sigma.com or fax the registration form to 03-61880602, we will contact you for further action.

**Two Sigma Technologies**
Suite B, 19-2, Jalan PGN 1A/1, Pinggiran Batu Caves,
68100 Batu Caves, Selangor
Tel : 03-61880601/Fax :03-61880602
sales@2-sigma.com
www.2-sigma.com