Course Name : PHP Security – Attacks & Fixes
Duration : 2 Days
Skill Level : Intermediate

Course Description :
This Web security training is designed for PHP application developers who are looking to enhance their skills and be able to learn and implement security best practices in their PHP projects. After completing this course, the candidates will be able to identify the most common types of vector attacks and industry experienced vulnerabilities allowing to monitor and fortify your application code against them.

MODULE 1: INTRODUCTION
- Welcome
- What you need to know?
- Introduction to Web Application Security
- What is Security
- Defense in Depth
- Basic Security Rules
- Building Secure Web Applications Guidelines

MODULE 2: SECURITY CONCEPTS & PRACTICES
- All Input is Tainted
- Whitelist and Blacklist Filtering
- Filtering the Input
- Escaping the Output
- Filtering and Validation
- Register Globals and Security Vulnerability

MODULE 3: SECURITY ATTACKS & PREVENTIONS
- All Input is Tainted
- SQL Injection
- Cross SiteScripting (XSS)
- Cross Site Request Forgery (CSRF)
- Include/Require FileExtensions
- Password Hashing
- Directory Listing
- HttpOnly Cookies
- What you Shouldn’t Store in Cookies
- Session Hijacking
- User Defined File Includes
- Error Reporting

MODULE 4: CONCLUSION
- QA
- Useful PHP Resources
- Feedback

Rynet Malaysia Sdn. Bhd. (899837-K)
95-2, Block H, The Suites, Jaya One, 72A, Jalan Universiti, 46200 Petaling Jaya,Selangor, Malaysia.
Phone: +603-7623-1088 | Fax: +603-7660-9393