# Web Application Penetration testing: A Beginner is Guide

## Course Introduction

This 2-day intensive course is designed for beginners, providing a thorough introduction to the core principles of web security and penetration testing methods. Participants will acquire crucial theoretical understanding and practical skills necessary for conducting penetration testing on web applications. During the course, participants will fully engage in the field of web security, exploring vulnerabilities and learning how to secure web applications against potential cyber threats.

## Course Objectives

- To understand the fundamental principles of web application security, with a focus on the OWASP Top 10 vulnerabilities.
- To learn how to use various penetration testing tools and techniques essential for assessing web application security.
- To gain the knowledge of web application vulnerabilities such as SQL injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and other related security threats.
- To acquire practical skills by conducting hands-on penetration testing on web applications, identifying security flaws, and exploiting vulnerabilities, including those found in the OWASP Top 10.

## Learning Level

- Fundamental

## Course Duration

- 2 Days

## Target Group

- Junior penetration tester
- IT auditor
- Developer
- IT operation
- General attendees (ผู้สนใจทั่วไป)

**For More Information & Registration, Please Contact Training Division**
Tel:(66) 2253-4736, Fax:(66) 2253-4737, Hotline:(66) 86-325-7129, E-mail: registration@acisonline.net

© Copyright 2001-2026: ACIS Professional Center Co., Ltd. All rights reserved. All contents of this form constitute the property of ACIS Professional Center Co., Ltd. and may not be copied, reproduced or distributed without prior written permission

# Course Outline

Day 1

- Introduction to Web Application Penetration Testing
- What is Web PenTest and Type of PenTest
- Writing Pentest Report
- OWASP Web Top 10
  - Broken Access Control
  - Cryptographic Failures
  - Injection
  - Insecure Design
  - Security Misconfiguration
  - Vulnerable and Outdated Components
  - Identification and Authentication Failures
  - Software and Data Integrity Failures
  - Security Logging and Monitoring Failures
  - Server-Side Request Forgery
- Web Application PenTest Tools
- BurpSuite Basics
- Setting Up the PenTest Environment

Day 2

- SQL Injection
- Cross Site Scripting
- Cross Site Request Forgery
- File upload Vulnerabilities
- Security Header
- Broken Authentication
- Broken Access Control Vulnerability
- File Inclusion
- Business logic vulnerabilities
- Capture The Flag (CTF)

**For More Information & Registration, Please Contact Training Division**
Tel:(66) 2253-4736, Fax:(66) 2253-4737, Hotline:(66) 86-325-7129, E-mail: registration@acisonline.net

© Copyright 2001-2026: ACIS Professional Center Co., Ltd. All rights reserved. All contents of this form constitute the property of ACIS Professional Center Co., Ltd. and may not be copied, reproduced or distributed without prior written permission

Official Training Partner



**© Copyright 2001-2026: ACIS Professional Center Co., Ltd. All rights reserved. All contents of this form constitute the property of ACIS Professional Center Co., Ltd. and may not be copied, reproduced or distributed without prior written permission**