# *WAP: Web Application Penetration Testing*

**Objective:** หลักสูตร Web Application Penetration Testing (WAP) ออกแบบมาเพื่อเพิ่มความรู้และทักษะในด้านการค้นหาช่องโหว่ของ Web Application และเรียนรู้เทคนิคในการโจมตีระบบ หรือการทำให้ระบบหยุดให้บริการระบบ รวมถึงเพื่อเพิ่มความรู้ในการรักษาความปลอดภัยให้ Web Application โดยอ้างอิงตามมาตรฐาน Open Web Application Security Project (OWASP) ให้กับผู้เข้าอบรม ทั้งในภาคทฤษฎีและปฏิบัติ ผ่านวิธีการบรรยาย และทดลองปฏิบัติ (Lab & Workshop) จากสถานการณ์จำลอง ผู้เข้าอบรมให้สามารถตรวจสอบช่องโหว่ของ Web Site ที่ดูแลได้ด้วยตนเอง ตลอดจนการออกรายงานเพื่อแจ้งประเด็นช่องโหว่ที่ตรวจพบ แก่บุคคลที่เกี่ยวข้องและผู้บริหาร เพื่อรับทราบปัญหาของช่องโหว่ที่ตรวจพบ รวมถึงแนวปฏิบัติที่ดีในการกำกับเพื่อปิดประเด็นช่องโหว่

**Who should attend:** Security Penetration Tester (Beginner to Intermediate Level)

Information Security Consultant

Web application programmer

**Duration:** 3 Days (09:00 – 16:00)

**Method:** Lecture, workshops and Lab

**Venue:** Jasmine City Hotel, Soi Sukhumvit 23, Klongtoey-Nua, Wattana, Bangkok

**Fee:** 14,500 Baht (Early Bird 13,500 Baht - to be paid 2 weeks prior to training)

This price does not include 7% VAT.

**Language:** Thai

**Instructor:** Prart Jintana OSCP, C | EH, OSSA

**Course Outline:**

1. **Generation of Hacker/Ethical Hacker**
    - Hacker (Black and White)
    - Cracker
    - Hacktivist
    - Cyberterorism
    - Cyber Warfare
    - Motivation and Ethical
    - Hacking vs. Penetration Testing
    - Rule of Thumb in Hacking and Penetration Testing
    - Laws and Due Diligence and Contract
    - NEWS (update)



***Knowledger Co, Ltd.***
*164/74 Rama 4 Road, Chong Nonsri,*
*Yannawa, Bangkok 10120 Thailand*

***www.knowledgertraining.com***
*Tel: 081-583-8805, 0 81-643-2564*
*Email: info@knowledgertraining.com*

## 2. Fundamental of Web Application (Recap)

- Web Application Technology (Web 1.0, Web 2.0 and Web 3.0)
- Web Technology (HTML5 and CSS 3)
- Architecture of Client/Server
- OSI Layer
- Transmission Control Protocol and Internet Protocol (TCP/IP)
- HTTP Method and Version
- Web Application vs. Web Service
- Infrastructure Perimeter vs. Web Application Firewall
- Attack Vector and Attack Pattern

## 3. Fundamental of Web Application Penetration Testing

- Web Application Penetration Testing Engagement
- Web Application Penetration Testing Goal, Strategy and Approach
- Web Application Penetration Testing Methodology and Framework
  (Web Application Hacking Anatomy: Estimate and Evaluation theTarget, Exploring the Information, Enumeration, Exploitation, Embedding, Evasion and Evanescence)
- Web Application Penetration Testing Technique and Sense
- Web Application Scanning Tools/Assessment Tools and Exploit Tools
- OWASP Top 10 Vulnerability of the World Cyber Risk over Web Application

## 4. Web Application Penetration Testing and Countermeasure

- Exploring The Information
  (Google Hacking, Server Fingerprint, Whois, Web Spider, Hidden File, Default Configuration, Directory Listing, Disclose from Error Handing and etc)
- Server Side Attacked
  (Flaw of SQL Injection, Xpath Injection, LDAP Injection, HTML Injection and etc)
- Client Side Client Attacked
  (Malicious Execution by Cross-site Scripting (XSS), Click jacking, Cross-Site Request Forgery (CSRF/XSRF), Side Jacking and Surf Jacking
- Authentication (Bypass and Brute-Forcing)
- Authorization (Insecure Direct Object References and Failure to Restrict URL Access)
- Session Management Flaw and Prediction (Session Fixation, and Session Hijacking)
- Insecure Transportation Cryptography and Storage Cryptography (Heart Bleed Attack)
- Business Work Flow Flaws
- Denial of Services and DDOS

## 5. Fundamental Web Application Penetration Testing Report and Risk Assignment

- IT Security Governance, Regulation and Standards
- IT Security Risk Assessment
- Web Application Penetration Scanning vs. Assessment vs. Audit vs. Penetration Testing
- Penetration Report Development and Submit Period



***Knowledger Co, Ltd.***
*164/74 Rama 4 Road, Chong Nonsri,*
*Yannawa, Bangkok 10120 Thailand*

***www.knowledgertraining.com***
*Tel: 081-583-8805, 0 81-643-2564*
*Email: info@knowledgertraining.com*