HYW Hacking and Auditing Web Application Security

Course Introduction

This three-days course provides in-depth knowledge about Web application security explains common security terminology and presents a set of proven security principles upon which many of the recommendations throughout this guide are based. It presents an overview of the security process and explains why a holistic approach to security that covers multiple layers including the network, host and application, is required to achieve the goal of hack-resilient Web applications.

Also, the course introduces and defines host configuration categories and application vulnerability categories.

Course Objectives

- This course focuses on the latest tools and techniques used in designing applications which provide data to those who need it while keeping the bad guys out.
- The candidate will have hands on experience using current tools to detect and prevent Cross-site scripting (XSS), and SQL Injection as well as an in-depth understanding of authentication, and session management systems and their weaknesses and how they are best defended.
- This course will focus on OWASP top 10 web application security guide.

Course Highlights

- Windows and Linux Web Penetration testing tools include audit checklists provided
- Free membership for ACIS Alumni
    - Access to the latest information related to the course subjects
    - A life-time class re-sit

Learning Level

- Advanced

Course Duration

- 3 Days (18 Hours)

Prerequisites

- Knowledge about basic networking
- Knowledge about Information Security
- Knowledge about Web Application Technologies

Target Group

- Web Application Programmers
- Systems/Network Administrators

- IT Auditors
- Anyone interested in learning the concepts of secure Web application design
- Information Security Professional

Course Outline

Module 1: Introduction to Web Application Security

- The Evolution of Web Applications
- Components used in Enterprise Web Environments
- Web Application Technologies
- Web Application Security

Module 2: OWASP Projects

- OWASP TOP 10 Project
- OWASP Testing Guide Project
- OWASP Code Review Project
- Other OWASP Projects

Module 3: Discovery and Identifying the Web Server, Web Application and Subsystem

- Internet Host and Network Information Gathering
- OS Fingerprinting
- Web Server Fingerprinting
- Application Fingerprinting
- Investigating Web Service Vulnerabilities
- Web harvesting
- LAB: Information Gathering for Web Application

Module 4: Attack: Bypassing Client-Side Controls

- Transmitting (sensitive) Data via the Client
- Bypass Client-Side Script Validation
- LAB: Sensitive Data Tampering Attack
- Countermeasures

Module 5: Attack: Access Controls

- Common Vulnerabilities
- Attacking Access Controls
- LAB: Broken Access Control Attack
- Exploiting Path Traversal
- LAB: Path Traversal Attack

- Countermeasures

Module 6: Attack: Authentication and Session Management

- Authentication Technologies
- Design Flaws in Authentication Mechanisms
- Implementation Flaws in Authentication
- Weaknesses in Session Token Generation
- Weaknesses in Session Token Handling
- LAB: Session Brute-Force
- LAB: Session Hijack
- Countermeasures

Module 7: Attack: Injecting Code

- Command Injection
- Web Scripting Languages Injection
- SOAP Injection
- SQL Injection
- LDAP Injection
- SMTP Injection
- LAB: Injection Attacks
- Countermeasures

Module 8: Attack: Cross-Site Scripting

- Reflected XSS
- Stored XSS
- DOM-Based XSS
- Request Forgery XSS
- Exploitation Techniques
- LAB: XSS Attacks
- Countermeasures

Module 9: Attack: Application Logic

- The Nature of Logic Flaws
- Example: Real-World Logic Flaws
- Avoiding Logic Flaws

Module 10: Attack: Exploiting Information Disclosure

- Exploiting Error Messages
- GHDB (Google Hack Database)

- LAB: GHDB Scanners
- Countermeasures

Module 11: Attack: Buffer Overflow

- Buffer Overflow Vulnerabilities
- Countermeasures

Module 12: Attack: Web Server

- Vulnerable Web Server Configuration
- Vulnerable Web Server Software
- Countermeasures

Module 13: Finding Vulnerabilities in Source Code

- Approaches to Code Review
- Signatures of Common Vulnerabilities
- LAB: Web Vulnerability Scanners
- LAB: Tools for Code Browsing

Recommended Course tracks

- PEN : Professional Penetration Testing Techniques and Vulnerability Assessment
- HDB : Hacking and Auditing Databases Security
- HDW : Hacking and Auditing Microsoft Windows Server Security

สำรองที่นั่งและขอรับรายละเอียดเพิ่มเติมกรุณาติดต่อ (FOR MORE INFORMATION & REGISTRATION PLEASE CONTACT)	
คุณธนภัทร ไชยพิมล Mr. Tanapat Chaipimol Tel:(66) 2-650-5771 Ext.105 Fax: (66) 2-650 5776 Mobile: (66) 86-330-8532 Email: tanapat.ch@acisonline.net	คุณกิตมณี นิยมญาติ Ms. Kitmanee Niyomyat Tel:(66) 2-650-5771 ext. 108 Fax: (66) 2-650 5776 Mobile: (66) 86-325-7129 Email: kitmanee.ni@acisonline.net

ACIS Professional Center Co.Ltd.

2101, 21 Fl., 62 The Millennia Building, Lungsuan Rd., Lumpini, Pathumwan, Bangkok 10330
Tel: +(66)2-650-5771 Fax: +(66)2-650-5776 Hotline: +(66)86-352-7129 Email: registration@acisonline.net
Website: www.acisonline.net