Hacking and Auditing Web Application Security (HWS)

Duration 3 Days

COURSE DESCRIPTION

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.

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 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

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th

- **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

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th

- **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

PREREQUISITE

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

WHO SHOULD ATTEND

- Web Application Programmers
- Systems/Network Administrators
- IT Auditors
- Anyone interested in learning the concepts of secure Web application design
- Information Security Professional

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th