TEC012: Hacking and Auditing Web Application Security

COURSE DESCRIPTION:

This 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.

PREREQUISITES:

- 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.

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

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

- **Module 4:** Attack: Bypassing Client-Side Controls
  - Transmitting (sensitive) Data via the Client
  - Bypass Client-Side Script Validation

- **Module 5:** Attack: Access Controls
  - Common vulnerabilities
  - Attacking Access Controls
  - Exploiting Path Traversal

- **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

- **Module 7:** Attack: Injecting Code
  - Command injection
  - Web Scripting Languages Injection
  - SOAP Injection
  - SQL Injection
  - LDAP Injection
  - SMTP Injection

- **Module 8:** Attack: Cross-Site Scripting
  - Reflected XSS
  - Stored XSS
  - DOM-Based XSS
  - Request Forgery XSS
  - Exploitation Techniques

- **Module 9:** Attack: Application Logic
  - The Nature of Logic Flaws
  - Avoiding Logic Flaws

- **Module 10:** Attack: Exploiting Information Disclosure
  - Exploiting Error Messages
  - GHDB (Google Hack Database)

- **Module 11:** Attack: Buffer Overflow
  - Buffer Overflow Vulnerabilities

- **Module 12:** Attack: Web Server
  - Vulnerable Web Server Configuration
  - Vulnerable Web Server Software

- **Module 13:** Finding Vulnerabilities in Source Code
  - Approaches to Code Review
  - Signature of Common Vulnerabilities

วิทยากร: อ.เอกฤทธิ์ ธรรมสถิต

- MASTER OF BUSINESS ADMINISTRATION (EXECUTIVE) DEGREE
  SASIN GRADUATE INSTITUTE OF BUSINESS ADMINISTRATION OF
  CHULALONGKORN UNIVERSITY
- MASTER OF SCIENCE, MAJOR IN INFORMATION
  Technology Faculty of Information Technology
  KING'S MONGKUT INSTITUTE OF TECHNOLOGY LADKRABANG
- BACHELOR OF SCIENCE
  KING'S MONGKUT INSTITUTE OF TECHNOLOGY NORTH BANGKOK
- DIPLOMA PROGRAM FOR MANAGEMENT
  KELLOGG – NORTHWESTERN UNIVERSITY, UNITED STATE OF AMERICA
  Certificate:
  - Microsoft Certified professional (MCP)
  - Microsoft Certified Systems Administrator (MSCA)
  - Microsoft Certified Systems Engineer (MSCE)
  - Cisco Certified Network Associate (CCNA)
  - Certificate of CompTIA Security+
  - Certified Technical training CTT+
  - Certified Ethical Hacker
  - Certified Hacking Forensic Investigator
  - Certified Wireless Network Administrator
  - Certified Wireless Security Professional

จำนวนชั่วโมงในการฝึกอบรม: 5 วัน (30 ชั่วโมง)

กำหนดการอบรม: ตามตารางปฏิทินอบรมประจำปี https://www.career4future.com/trainingprogram

ช่วงเวลาฝึกอบรม: 9.00 - 16.00 น.

ค่าลงทะเบียนอบรม: ท่านละ 25,500 บาท (ราคารวมภาษีมูลค่าเพิ่มแล้ว)
** สถาบันฯ เป็นหน่วยงานราชการ จึงไม่อยู่ในเกณฑ์ที่ต้องถูกหักภาษี ณ ที่จ่าย

สถานที่ฝึกอบรม :

สถาบันพัฒนาบุคลากรแห่งอนาคต
เลขที่ 73/1 อาคารสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) ชั้น 6
ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400

วิธีการการสำรองที่นั่ง:

ติดต่อสำรองที่นั่งล่วงหน้า ในวัน-เวลาราชการ
โทรศัพท์: 0 2644 8150 ต่อ 81886, 81887
โทรสาร: 0 2644 8110
Website: www.career4future.com
E-mail: training@nstda.or.th