

Hacking and Auditing Web Application Security

TEC012

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)

ช่วงเวลาฝึกอบรม: 9.00 - 16.00 น.

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

ค่าลงทะเบียนอบรม: ท่านละ 25,500 บาท

หมายเหตุ • ราคาค่าลงทะเบียนอบรม ไม่รวมภาษีมูลค่าเพิ่ม • เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐ ที่ไม่ใช่ธุรกิจ และไม่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม • สถาบันฯ เป็นหน่วยงานราชการ ได้รับการยกเว้นไม่ต้องหักภาษี ณ ที่จ่าย 3% • ค่าใช้จ่ายในการส่งบุคลากรเข้าอบรมทางวิชาชีพของ บริษัทหรือห้างหุ้นส่วนนิติบุคคล สามารถนำไปลดหย่อนภาษีได้ 200% • ข้าราชการมีสิทธิ์เบิกค่าลงทะเบียนได้ตามระเบียบกระทรวงการคลังและเข้าร่วมอบรมสัมมนาโดยไม่ถือเป็นวันลา	• สถาบันฯ ขอสงวนสิทธิ์ในการเปลี่ยนแปลงเนื้อหาหลักสูตร วิทยากร รูปแบบการอบรม ตามความเหมาะสมและความจำเป็น เพื่อประโยชน์สูงสุดของผู้เข้ารับการอบรม • สถาบันฯ ขอสงวนสิทธิ์ ไม่บันทึกภาพ วิดีโอ หรือบันทึกเสียง ตลอดระยะเวลาการอบรม เนื่องจากเป็นลิขสิทธิ์ร่วมระหว่างวิทยากรกับสถาบันฯ และเพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล • ผู้เข้าอบรมต้องมีเวลาเรียนไม่ต่ำกว่า 80% และทำกิจกรรมทุกหัวข้อของหลักสูตร จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)
หลักสูตรจัดอบรมรูปแบบ Onsite เท่านั้น • สถาบันฯ มีการจัดเตรียมเครื่องคอมพิวเตอร์ เอกสารการอบรม พร้อมอาหารว่าง และอาหารกลางวันให้กับผู้เข้าอบรม • มอบวุฒิบัตรภายหลังจบการอบรม สถานที่อบรม ห้องอบรม ณ สถาบันพัฒนาบุคลากรแห่งอนาคต อาคาร สวทช. ชั้น 6 ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400	

ติดต่อสอบถามรายละเอียด

สถาบันพัฒนาบุคลากรแห่งอนาคต (Career for the Future Academy)
73/1 อาคารสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) ชั้น 6
ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400
โทรศัพท์ 0 2644 8150 ต่อ 81886-7
โทรสาร 0 2644 8150
E-mail: training@nstda.or.th
www.career4future.com