

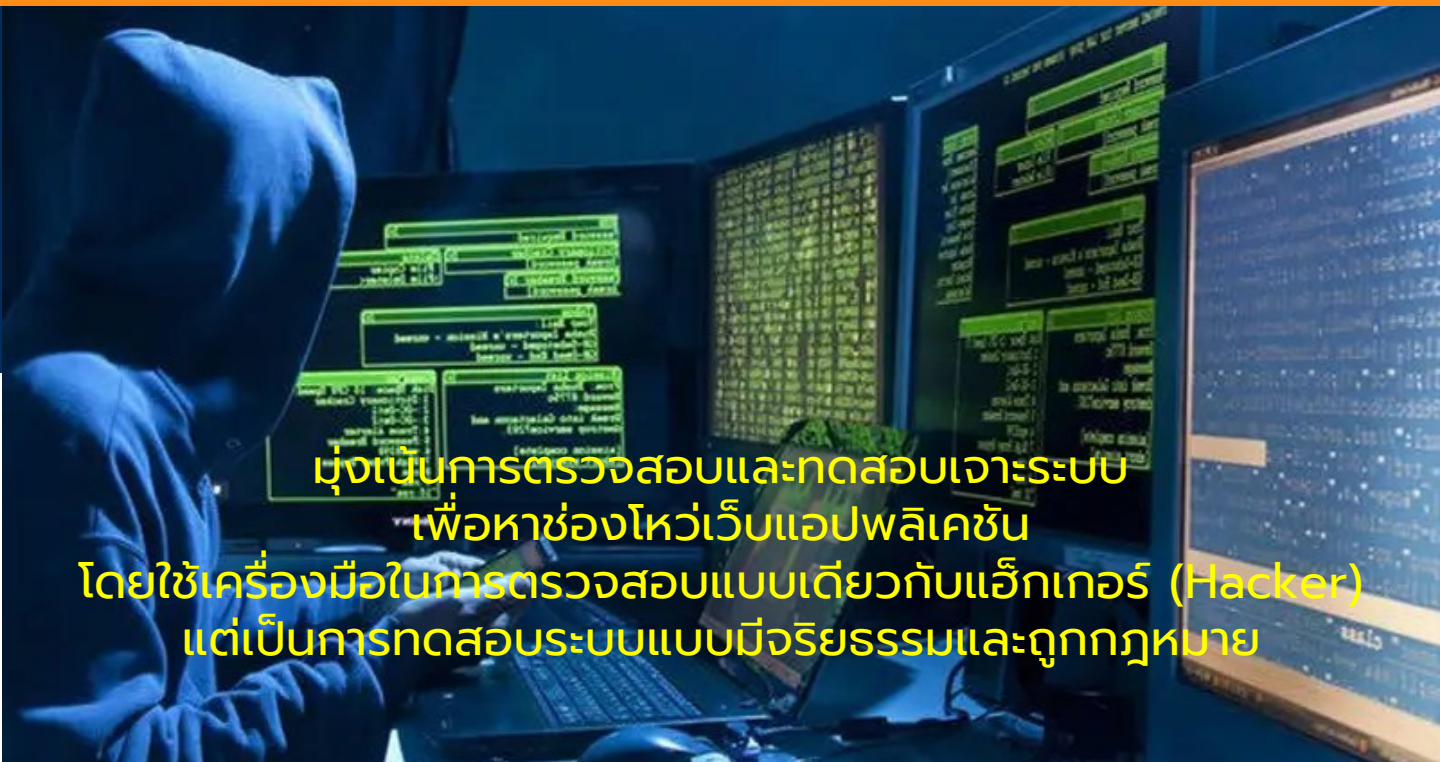


WAHS

Web Application Hacking and Security



หลักสูตรฝึกอบรมเชิงปฏิบัติการ
การทดสอบเจาะระบบและความมั่นคงปลอดภัยด้านเว็บแอปพลิเคชัน



มุ่งเน้นการตรวจสอบและทดสอบเจาะระบบ
เพื่อหาช่องโหว่เว็บแอปพลิเคชัน

โดยใช้เครื่องมือในการตรวจสอบแบบเดียวกับแฮ็กเกอร์ (Hacker)
แต่เป็นการทดสอบระบบแบบมีจริยธรรมและถูกกฎหมาย

Key Highlights

- ♥ เรียนรู้และเข้าใจสาระสำคัญด้านความปลอดภัยจากการโจมตีเว็บแอปพลิเคชัน
- ♥ เรียนรู้มาตรการความมั่นคงปลอดภัยบน HTTP Security Header
- ♥ เรียนรู้แนวทางและวิธีการทดสอบเจาะระบบ Penetration Testing Methodologies
- ♥ เรียนรู้การทดสอบเจาะระบบ และแนวทางป้องกันรูปแบบการโจมตี บน 10 อันดับความเสี่ยงจาก OWASP
- ♥ เข้าใจการทดสอบเจาะระบบในรูปแบบต่าง ๆ พร้อมการทำรายงานที่ถูกต้อง
- ♥ ฝึกปฏิบัติเข้มข้นในการทดสอบเจาะระบบในรูปแบบที่หลากหลาย



หลักสูตรฝึกอบรมเชิงปฏิบัติการ การทดสอบเจาะระบบและความมั่นคงปลอดภัยด้านเว็บแอปพลิเคชัน

Web Application Hacking and Security

ในปัจจุบันภัยคุกคามทางไซเบอร์จากแฮกเกอร์ (Hacker) หรือผู้ไม่ประสงค์ดียังทวีความรุนแรงมากขึ้นเรื่อย ๆ โดยเฉพาะการโจมตีเว็บแอปพลิเคชัน ซึ่งเป็นช่องทางสำคัญในการเข้าถึงข้อมูลขององค์กร เป้าหมายของแฮกเกอร์อาจเป็นการขโมยข้อมูลสำคัญ ทำลายชื่อเสียงขององค์กร หรือเรียกร้องผลประโยชน์ในรูปแบบต่าง ๆ ส่งผลให้หน่วยงานภาครัฐและเอกชนได้รับความเสียหายอย่างมาก หลักสูตรนี้ถูกออกแบบมาเพื่อสร้างความเข้าใจและความเชี่ยวชาญด้านความมั่นคงปลอดภัยของระบบ รวมถึงสร้างความรู้ความสามารถในการตรวจสอบความมั่นคงปลอดภัยของเว็บแอปพลิเคชัน โดยมุ่งเน้นการตรวจสอบและทดสอบเจาะระบบเพื่อหาช่องโหว่โดยใช้เครื่องมือในการตรวจสอบแบบเดียวกับที่แฮกเกอร์ (Hacker) ใช้ แต่เป็นการทดสอบระบบแบบมีจริยธรรมและถูกกฎหมาย ผู้เข้าอบรมจะได้พัฒนากะในการป้องกันภัยทางไซเบอร์และช่วยให้องค์กรสามารถรับมือกับการโจมตีได้อย่างมีประสิทธิภาพ

โครงสร้างหลักสูตร

หลักสูตรนี้เป็นหลักสูตรที่สร้างความรู้ความเข้าใจเกี่ยวกับการทดสอบเจาะระบบและความมั่นคงปลอดภัยด้านเว็บแอปพลิเคชัน ตลอดจนฝึกปฏิบัติเพื่อพัฒนากะที่จำเป็นอย่างเข้มข้น รวมจำนวน 18 ชั่วโมง / 3 วันทำการ

หัวข้อ	ชั่วโมง	ครั้ง (วัน)
บรรยาย และกรณีศึกษา	9	1.5
ฝึกปฏิบัติการ (Workshop)	9	1.5
รวม	18	3

เนื้อหาหลักสูตร ประกอบด้วย

- Introduction to Web Application
- HTTP Security Headers
- Introduction to Web Application Security
- Penetration Testing Methodology
- Penetration Testing Framework
- Types of Web Penetration Testing
- Web Application Penetration Testing Tools
- Web Application Penetration Testing Checklist
- Web Application Penetration Testing Certifications
- The Penetration Testing Process
- Web Application Proxies
- Using Hacking Tools
- Open Web Application Security Project (OWASP)
 - OWASP TOP 10 2013: SQL Injection
 - OWASP TOP 10 2013: Broken Authentication and Session Management
 - OWASP TOP 10 2013: Cross-site Scripting
 - OWASP TOP 10 2013: Security Misconfiguration
 - OWASP TOP 10 2017: XML External Entities (XXE)
 - OWASP TOP 10 2017: Insecure Deserialization
 - OWASP TOP 10 2021: Insecure Design
 - OWASP TOP 10 2021: Software and Data Integrity Failures
 - OWASP TOP 10 2021: Server-Side Request Forgery

ระยะเวลาหลักสูตร

อบรมระหว่างวันที่ 28 - 30 มกราคม 2569
เวลา 9.00 - 16.00 น. (รวมระยะเวลา 3 วัน)

หลักสูตรนี้เหมาะสำหรับ

- นักพัฒนาโปรแกรมด้านเว็บแอปพลิเคชัน
- ผู้ดูแลระบบ (System Administrator)
- นักทดสอบเจาะระบบ (Penetration Tester)
- ปรึกษาด้านความมั่นคงปลอดภัยสารสนเทศ (IT Security Consultant)

วิทยากรประจำหลักสูตร



อาจารย์ เจษฎา กองกันเหลือง

กรรมการผู้จัดการ

บริษัท ที-เน็ต ไอที โซลูชัน จำกัด

- Certified Ethical Hacker (CEH)
- Certified Hacking Forensic Investigator (CHFI)
- Certified Security Analyst (E|CSA)
- IT Specialist Certification (ITS): Cyber Security

ค่าลงทะเบียน

ท่านละ 24,500 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)

- เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐที่ไม่ใช่รัฐกิจและไม่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม
- โปรโมชันพิเศษ!!! ลงทะเบียนหน่วยงานเดียวกันตั้งแต่ 2 ท่านขึ้นไปรับส่วนลดทันที 10%

สถานที่อบรม



โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพฯ
เลขที่ 9 ถนนราชปรารภ เขตราชเทวี
กรุงเทพมหานคร

หมายเหตุ

- หากท่านต้องการยกเลิกการลงทะเบียน กรุณาแจ้งยืนยันการยกเลิกเป็นลายลักษณ์อักษร อย่างน้อย 7 วันทำการก่อนวันจัดงาน หากการแจ้งยกเลิกล่าช้ากว่าเวลาที่กำหนดดังกล่าว ทางสถาบันฯ ขอสงวนสิทธิ์หักค่าดำเนินการ คิดเป็นจำนวนเงิน 30% จากค่าลงทะเบียนจำนวนเต็ม
- สถาบันพัฒนาบุคลากรแห่งอนาคต ขอสงวนสิทธิ์ในการเปลี่ยนแปลงเนื้อหาหลักสูตร วิทยากร ตามความเหมาะสมและความจำเป็น เพื่อประโยชน์สูงสุดของผู้เข้ารับการอบรม
- ผู้เข้าอบรมต้องใช้เวลาเรียนไม่ต่ำกว่า 80% และทำกิจกรรมทุกหัวข้อของหลักสูตร จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

ศึกษารายละเอียดเพิ่มเติมได้ที่ <https://www.career4future.com/wahs>

สอบถามรายละเอียดเพิ่มเติมได้ที่ 0 2644 8150 ต่อ 81891 E-mail: npd@nstda.or.th

ใบลงทะเบียน

หลักสูตรฝึกอบรมเชิงปฏิบัติการการทดสอบเจาะระบบและความมั่นคงปลอดภัย ด้านเว็บแอปพลิเคชัน (Web Application Hacking and Security)

รายละเอียดผู้เข้ารับการอบรม (กรุณาเขียนตัวบรรจง ครบถ้วน และถูกต้อง เพื่อใช้ในการออกวุฒิบัตร)

ประเภทหน่วยงาน

- ☐ ราชการ
☐ รัฐวิสาหกิจ
☐ เอกชน
☐ ส่วนตัว

ต้องการออกใบเสร็จในนาม

- ☐ องค์กร
☐ ส่วนบุคคล
(โปรดระบุเลขบัตรประชาชน)

ต้องการระบุชื่อผู้เข้าอบรมในใบเสร็จหรือไม่

- ☐ ต้องการ
☐ ไม่ต้องการ

1
คำนำหน้า (ไทย) นาย/นาง/นางสาว/อื่นๆ
ชื่อ-สกุล (ไทย)
ชื่อ-สกุล (อังกฤษ)
ตำแหน่งงาน โทรศัพท์/มือถือ
E-mail (ใช้เป็น Log in เข้าสู่ระบบ)

2
คำนำหน้า (ไทย) นาย/นาง/นางสาว/อื่นๆ
ชื่อ-สกุล (ไทย)
ชื่อ-สกุล (อังกฤษ)
ตำแหน่งงาน โทรศัพท์/มือถือ
E-mail (ใช้เป็น Log in เข้าสู่ระบบ)

3
คำนำหน้า (ไทย) นาย/นาง/นางสาว/อื่นๆ
ชื่อ-สกุล (ไทย)
ชื่อ-สกุล (อังกฤษ)
ตำแหน่งงาน โทรศัพท์/มือถือ
E-mail (ใช้เป็น Log in เข้าสู่ระบบ)

ที่อยู่สำหรับออกใบกำกับภาษี/ใบเสร็จรับเงิน

ชื่อองค์กร (ไทย)
ชื่อองค์กร (อังกฤษ)
หมายเลขประจำตัวผู้เสียภาษี ☐ สำนักงานใหญ่ ☐ สาขา (โปรดระบุ)
ห้อง ชั้น อาคาร/หมู่บ้าน เลขที่ หมู่ที่ ซอย
ถนน แขวง/ตำบล เขต/อำเภอ
จังหวัด รหัสไปรษณีย์ โทรศัพท์ ต่อ โทรสาร
ชื่อ-สกุล ผู้ประสานงาน โทรศัพท์ ต่อ E-mail

ท่านได้รับข่าวสารการจัดงานนี้จาก

☐ จดหมายเชิญ ☐ เว็บไซต์ career4future.com ☐ Facebook/Twitter ☐ Line
☐ เพื่อนหรือคนรู้จักแนะนำ ☐ ช่องทางอื่น (โปรดระบุ)

รายละเอียดค่าลงทะเบียน (รวมภาษีมูลค่าเพิ่มแล้ว)

หลักสูตร	ค่าลงทะเบียน (บาท)
หลักสูตรฝึกอบรมเชิงปฏิบัติการการทดสอบเจาะระบบและความมั่นคงปลอดภัย ด้านเว็บแอปพลิเคชัน (Web Application Hacking and Security) วันที่ 28 - 30 มกราคม 2569 ณ โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพฯ	24,500

เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐ ที่ไม่ใช่ธุรกิจและไม่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม
โปรดบันทึกผล! ลงทะเบียนหน่วยงานเดียวกันตั้งแต่ 2 ท่านขึ้นไป รับส่วนลดทันที 10%

4 ช่องทางการลงทะเบียน

-  Website: www.career4future.com/wahs
 Call Center: 0 2644 8150
ต่อ 81891 (คุณนิพนธ์)
 Fax: 0 2644 8150
 E-mail: npd@nstda.or.th

วิธีการชำระเงิน

ท่านสามารถชำระเงินโดย การโอนเงินหรือนำฝากเช็คธนาคาร ได้ทั้ง 2 ธนาคารดังนี้

ชื่อบัญชี (ภาษาไทย): สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

ชื่อบัญชี (ภาษาอังกฤษ): National Science and Technology Development Agency

 ธนาคารกรุงเทพ สาขา: อุทยานวิทยาศาสตร์ เลขที่บัญชี: 080-0-00001-0 ประเภทบัญชี: เงินฝากสะสมทรัพย์

 ธนาคารกรุงไทย สาขา: ตลาดไท เลขที่บัญชี: 152-1-32668-1 ประเภทบัญชี: ออมทรัพย์

แล้วส่งหลักฐานการโอนเงินมาที่ e-mail: npd@nstda.or.th

หมายเหตุ

- กรุณาชำระเงินภายใน วันที่ 21 มกราคม 2569
- ค่าลงทะเบียนรวม อาหารกลางวัน และอาหารว่าง 2 มื้อต่อวัน เอกสารประกอบการอบรม และภาษีมูลค่าเพิ่ม
- ขอสงวนสิทธิ์ในการเปลี่ยนแปลงกำหนดการตามความเหมาะสม
- สถาบันฯ เป็นหน่วยงานราชการ ได้รับการยกเว้นไม่ต้องหักภาษี ณ ที่จ่าย 3%
- ข้าราชการมีสิทธิเบิกค่าลงทะเบียนได้ตามระเบียบกระทรวงการคลัง และเข้าร่วมอบรมสัมมนาได้ โดยไม่ต้องเป็นวันลา
- ค่าใช้จ่ายในการส่งบุคลากรเข้าอบรมทางวิชาชีพของบริษัทหรือห้างหุ้นส่วนนิติบุคคล สามารถนำไปลดหย่อนภาษีได้ 200%
- หากท่านต้องการยกเลิกการลงทะเบียน กรุณาแจ้งยืนยันการยกเลิกเป็นลายลักษณ์อักษร อย่างน้อย 7 วันทำการ ก่อนวันจัดงาน หากการแจ้งยกเลิกล่าช้ากว่าเวลาที่กำหนดดังกล่าว ทางสถาบันฯ ขอสงวนสิทธิ์ในการหักค่าดำเนินการ คิดเป็นจำนวนเงิน 30% จากค่าลงทะเบียนเต็มจำนวน

สถานที่อบรม

โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพฯ
เลขที่ 9 ถนนราชปรารภ เขตราชเทวี
กรุงเทพมหานคร

สวทช.
NSTDA

สถาบันพัฒนาบุคลากรแห่งอนาคต (Career for the Future Academy)
73/1 อาคารสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) ชั้น 6
ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400
โทรศัพท์ 0 2644 8150 โทรสาร 0 2644 8110

Follow Us: <https://www.facebook.com/Career4FutureAcademy>

