



กำหนดการอบรม

หลักสูตรฝึกอบรมเชิงปฏิบัติการ
การทดสอบเจาะระบบและความมั่นคงปลอดภัยด้านเว็บแอปพลิเคชัน
(Web Application Hacking and Security: WAHS)

ระหว่างวันที่ 1-3 เมษายน 2569
ณ โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพฯ

วิทยากร : นายเจษฎา ทองก้านเหลือง
ผู้ช่วยวิทยากร : นายธนพล กระจ่างธร

กำหนดการอบรม (ระยะเวลา 3 วัน)

วันพุธที่ 1 เมษายน 2569		หมายเหตุ
09:00 – 10:30 น.	Introduction to Web Application <ul style="list-style-type: none"> ○ Web Application Attack Statistics ○ Terminology ○ Web Application History ○ Web Application Architecture ○ Web application components ○ Web application Languages ○ Web Server ○ HTTP Protocol ○ Encoding ○ User Agent ○ Session & Cookie ○ HTTP Security Header 	
10:30 – 12:00 น.	HTTP Security Headers <ul style="list-style-type: none"> ○ Content-Security-Policy (CSP) ○ Strict-Transport-Security Header (HSTS) ○ X-Content-Type-Options ○ X-Frame-Options ○ Referrer-Policy Introduction to Web Application Security <ul style="list-style-type: none"> ○ Vulnerability Stack ○ Defense in depth 	
12:00 – 13:00 น.	พักรับประทานอาหารกลางวัน	
13:00 – 14:30 น.	Penetration Testing Methodology <ul style="list-style-type: none"> ○ OWASP (Open Web Application Security Project) ○ OSSTMM (Open Source Security Testing Methodology Manual) ○ PTF (Penetration Testing Framework) ○ ISSAF (Information Systems Security Assessment Framework) ○ PCI DSS (Payment Card Industry Data Security Standard) Penetration Testing Framework <ul style="list-style-type: none"> ○ Cyber Kill Chain Framework ○ MITRE ATT&CK ○ NIST Penetration Testing Framework 	
14:30 – 16:00 น.	Types of Web Penetration Testing <ul style="list-style-type: none"> ○ Internal Penetration Testing ○ External Penetration Testing Web Application Penetration Testing Tools (Kali Linux Example) <ul style="list-style-type: none"> ○ Zed Attack Proxy (ZAP) ○ Wfuzz ○ Wapiti ○ W3af 	

	<ul style="list-style-type: none"> ○ SQLMap <p>Web Application Penetration Testing Checklist</p> <ul style="list-style-type: none"> ○ OWASP Web Application Security Testing Checklist ○ SANS Securing Web Application Technologies Checklist <p>Web Application Penetration Testing Certifications</p> <ul style="list-style-type: none"> ○ OSWE (Offensive Security Web Expert) ○ GWAPT (GIAC Web Application Penetration Tester) ○ CWAPT (Certified Web App Penetration Tester) ○ eWPT (elearnSecurity Web Application Penetration Tester) 	
วันพฤหัสบดีที่ 2 เมษายน 2569		หมายเหตุ
09:00 – 10:30 น.	<p>The Penetration Testing Process</p> <ul style="list-style-type: none"> ○ Reconnaissance (Active/Passive) ○ Scanning/Enumeration ○ Exploitation ○ Privilege Escalation/Maintaining Access ○ Reporting <p>Web Application Proxies</p> <ul style="list-style-type: none"> ○ Example: Burp Proxy, OWASP ZAP <p>Using Hacking Tools</p> <ul style="list-style-type: none"> ○ Example: Kali Linux 	
10:30 – 12:00 น.	<p>Open Web Application Security Project (OWASP)</p> <ul style="list-style-type: none"> ○ OWASP Web Security Testing Guide ○ OWASP Application Security Verification Standard Project (ASVS) ○ OWASP Cheat Sheet Series ○ OWASP TOP Ten ○ OWASP Web Application Security Testing Checklist <p>OWASP TOP 10 2013: SQL Injection</p> <ul style="list-style-type: none"> ○ Explanations ○ SQL Injection Demo ○ Command Injection Demo ○ Defense ○ LAB Demo 	
12:00 – 13:00 น.	พักรับประทานอาหารกลางวัน	
13:00 – 16:00 น.	<p>OWASP TOP 10 2013: Broken Authentication and Session Management</p> <ul style="list-style-type: none"> ○ Explanations ○ Hijack a Session Demo ○ Brute Force Demo ○ Defense ○ LAB Demo <p>OWASP TOP 10 2013: Cross-site Scripting</p> <ul style="list-style-type: none"> ○ Explanations ○ Reflected XSS HTML context Demo. ○ Stored Demo ○ Defense ○ LAB <p>OWASP TOP 10 2013: Security Misconfiguration</p> <ul style="list-style-type: none"> ○ Explanations ○ Directory Browsing Demo ○ Web Server Banner Disclosure Demo ○ Defense ○ LAB Demo 	
วันศุกร์ที่ 3 เมษายน 2569		หมายเหตุ
09:00 – 12:00 น.	<p>OWASP TOP 10 2017: XML External Entities (XXE)</p> <ul style="list-style-type: none"> ○ Explanations ○ XML External Entities (XXE) Demo ○ Defense ○ LAB <p>OWASP TOP 10 2017: Insecure Deserialization</p> <ul style="list-style-type: none"> ○ Explanations ○ Insecure Deserialization Demo 	

	<ul style="list-style-type: none"> ○ Defenses ○ LAB 	
12:00 – 13:00 น	พักรับประทานอาหารกลางวัน	
13:00 – 16:00 น.	OWASP TOP 10 2021: Insecure Design <ul style="list-style-type: none"> ○ Explanations OWASP TOP 10 2021: Software and Data Integrity Failures <ul style="list-style-type: none"> ○ Explanations OWASP TOP 10 2021: Server-Side Request Forgery <ul style="list-style-type: none"> ○ Explanations ○ Server-Side Request Forgery Demo ○ Defense ○ LAB 	

หมายเหตุ:

- สถาบันพัฒนาบุคลากรแห่งอนาคต ขอสงวนสิทธิ์ในการเปลี่ยนแปลงกำหนดการตามความเหมาะสม โดยยังคงเนื้อหาและสาระสำคัญของการอบรมไว้
- พักรับประทานอาหารว่าง เวลา 10.30 – 10.45 น. และ 14:30 – 14:45 น. และพักรับประทานอาหารกลางวัน เวลา 12.00-13.00 น.
- ผู้เข้าร่วมอบรมต้องมีเวลาเข้าเรียนไม่ต่ำกว่า 80% จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

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