หลักสูตรความมั่นคงปลอดภัยด้านเว็บแอพพลิเคชัน

(Web Application Hacking&Security)

Key Highlights

1.เรียนรู้วิธีการตั้งค่าความปลอดภัยบนเว็บเซิร์ฟเวอร์ เช่น apache,nginx, IIS เป็นต้น
2.เรียนรู้ฟังก์ชันการใช้งานความมั่นคงปลอดภัยในการพัฒนา Software อย่างปลอดภัย
3.เรียนรู้การรับส่งข้อมูลผ่านโปรโตคอล HTTP และ Websockets อย่างปลอดภัย
4.เรียนรู้การทดสอบเจาะระบบบน 10 อันดับความเสี่ยงจาก OWASP
5.เรียนรู้มาตราการความปลอดภัย HTTP Security Header (Protection For Browsers)
6.เรียนรู้การออกแบบ Web Application อย่างปลอดภัย

หลักการและเหตุผล

ในปัจจุบันภัยคุกคามที่เกิดขึ้นจากผู้ไม่ประสงค์ดี (Hacker) ได้ทวีความรุนแรงขึ้นทุกวันโดยมุ่งเน้นการโจมตีหน่วยงานภาครัฐ เอกชน และมหาวิทยาลัย และร่วมไปถึงเว็บไซต์ขายของ (E-Commerce) จากทั้งภายใน และภายนอกประเทศ เพื่อทำลายชื่อเสียงและเรียกร้องสิทธิต่าง ๆ ตามที่ต้องการ ซึ่งสาเหตุที่เว็บไซต์ตกเป็นเป้าหมายหลักที่โดนบุกรุกเนื่องจากผู้ไม่ประสงค์ดีสามารถเข้าถึงจากที่ใดก็ได้บนโลกผ่านระบบเครือข่ายอินเทอร์เน็ตทำให้ง่ายต่อการบุกรุก ดังนั้นเพื่อให้นักพัฒนาโปรแกรมด้านเว็บแอพพลิเคชัน (Web Application Programmer) ต่าง ๆ เช่น PHP, JAVA, C# เป็นต้น หรือผู้ดูแลระบบ (System Administrator) หรือ นักทดสอบเจาะระบบ (Penetration Tester) หรือสายงานด้านความมั่นคงปลอดภัยสารสนเทศทั้งหมดให้มีความรู้ความเข้าใจเกี่ยวกับภัยคุกคามหรือช่องโหว่ต่าง ๆ ที่เกิดขึ้นจริงในปัจจุบันด้วยวิธีการเจาะเว็บแอพพลิเคชันแบบผู้ไม่ประสงค์ดี จนทำให้ผู้เข้าร่วมอบรมมีความตระหนักถึงความเสี่ยงและเข้าใจถึงปัญหาที่เกิดขึ้นพร้อมทั้งสามารถนำแนวทางไปใช้ในการปรับปรุงและแก้ไขช่องโหว่บนเว็บแอพพลิเคชันได้สำเร็จ

วัตถุประสงค์

1.เพื่อให้ผู้เข้าร่วมอบรมเรียนรู้และเข้าใจพื้นฐานความมั่นคงปลอดภัยทางสารสนเทศ
2.เพื่อให้ผู้เข้าร่วมอบรมเรียนรู้และเข้าใจแนวทางการการออกแบบแอปพลิเคชัน
3.เพื่อให้ผู้เข้าร่วมอบรมเรียนรู้และเข้าใจขั้นตอน และวิธีการป้องกันและแนวทางการเข้ารหัสเพื่อหลีกเลี่ยงช่องโหว่ด้านความปลอดภัย
4.เพื่อให้ผู้เข้าร่วมอบรมเรียนรู้และเข้าใจจุดอ่อนหรือช่องโหว่ที่เกิดขึ้นบนเว็บแอปพลิเคชัน
5.เพื่อให้ผู้เข้าร่วมอบรมเรียนรู้และเข้าใจวิธีการทดสอบเจาะระบบบนช่องโหว่ต่างๆ ที่เกิดขึ้นบนเว็บแอปพลิเคชัน

ประโยชน์ที่ได้รับ

1. ผู้เข้าร่วมอบรมสามารถนำรู้พื้นฐานความมั่นคงปลอดภัยทางสารสนเทศไปประยุกต์ใช้งานได้จริงภายในองค์กร
2. ผู้เข้าร่วมอบรมสามารถนำแนวทางการป้องกันความมั่นคงปลอดภัยทางสารสนเทศไปประยุกต์ใช้งานได้จริงภายในองค์กร
3. ผู้เข้าร่วมอบรมสามารถนำขั้นตอน และวิธีการทดสอบเจาะระบบบนช่องโหว่ต่างๆ ไปประยุกต์ใช้งานได้จริงภายในองค์กร
4. ผู้เข้าร่วมอบรมสามารถนำความรู้และเข้าใจจุดอ่อนหรือช่องโหว่ที่เกิดขึ้นบนระบบสารสนเทศไปประยุกต์ใช้งานได้จริงภายในองค์กร

ผู้ที่เหมาะสมในการอบรมหลักสูตรนี้

1.นักพัฒนาโปรแกรมด้านเว็บแอพพลิเคชัน (Web Application Programmer)
2.ผู้ดูแลระบบ (System Administrator)
3.นักทดสอบเจาะระบบ (Penetration Tester)
4.ที่ปรึกษาด้านความมั่นคงปลอดภัยสารสนเทศ (IT Security Consultant)
5.ผู้สนใจอื่น ๆ ด้านความมั่นคงปลอดภัยสารสนเทศ

ราคาค่าเข้าอบรม

ค่าลงทะเบียนอบรม 1 ท่าน 15,900 บาท (รวม VAT แล้ว)
จำนวนผู้เข้าร่วมอบรมไม่เกิน 10 ท่าน

สิ่งที่ผู้เข้าร่วมต้องเตรียม

Notebook ส่วนตัว

ระยะเวลาการอบรมจำนวน 2 วัน

รอบที่ 1 วันที่ 28-29 เมษายน 2565
รอบที่ 2 วันที่ 30-31 พฤษาคม 2565
รอบที่ 3 วันที่ 29-30 มิถุนายน 2565

เวลา วันที่ *1*	เนื้อหา
9.00-10.30	Introduction to Web Application • ภัยคุกคาม ช่องโหว่ ที่เกิดขึ้นในปัจจุบัน • เรียนรู้คำศัพท์ที่เกี่ยวข้อง • ประวัติการพัฒนาเว็บแอพพลิเคชัน • โครงสร้างระบบเว็บแอพพลิเคชัน • เว็บไซต์และเว็บแอพพลิเคชัน • เว็บเซิร์ฟเวอร์ • ทำความรู้จัก HTTP Protocol
10.30-10.45	อาหารว่าง
10.45-12.00	Introduction to Web Application Security • Defense in depth Using a Web Proxy • Example: Burp Proxy Using a Hacking Tools • Example: Kali Linux
12.00-13.00	รับประทานอาหารกลางวันร่วมกัน
13.00-14.30	Web Application Penetration Testing Methodology • ทำความรู้จัก Open Web Application Security Project (OWASP) • OWASP Testing Guide • เรียนรู้ 10 อันดับช่องโหว่ที่เกิดขึ้นในปัจจุบันบนเว็บแอพพลิเคชัน • A1-Injection • Explanations • SQL Injection Demo • Command Injection Demo • Defense • LAB
14.30-14.45	อาหารว่าง
14.45-17.00	• A3-Cross-site Scripting • Explanations • Reflected XSS HTML context Demo • Stored Demo • Defense • LAB • A4-Insecure Direct Object Reference • Explanations • IDO URLs tokens Demo • Defense • LAB • A5-Security Misconfiguration • Explanations • Directory Browsing • User Agent Manipulation • Defense • LAB

เวลา วันที่ 2	เนื้อหา
9.00-10.30	• A6 Sensitive Data Exposure • Explanations • Hidden Pages Demo • Defenses • LAB • A7 Missing Function Level Access Control • Explanations • Role Demo • Defenses • LAB
10.30-10.45	อาหารว่าง
10.45-12.00	• A8 Cross-site Request Forgery • Explanations • CSRF JS Demo • Defenses • LAB • A9 Using Components with Known Vulns • Explanations • Libraries & CVE Demo • Defenses • LAB
12.00-13.00	รับประทานอาหารกลางวันร่วมกัน
13.00-14.30	• A10 Unvalidated Redirects and Forwards • Explanations • Redirect to malicious URL • Defenses • LAB
14.30-14.45	อาหารว่าง
14.45-17.00	• สรุปผลกระทบที่เกิดขึ้นบน OWASP TOP 10 2013 • รายละเอียดเพิ่มเติม OWASP TOP 10 2017 • A4:2017-XML External Entities (XXE) • A8:2017-Insecure Deserialization • A10:2017-Insufficient Logging&Monitoring S

หมายเหตุ : เนื้อหาอาจมีการปรับเปลี่ยนแก้ไขตามความเหมาะสม

โปรโมชันส่วนลด

- ชำระล่วงหน้าก่อน 2 อาทิตย์ ส่วนลด 1,000 บาท
- มาคู่บริษัทเดียวกัน 3,000 บาท
- นักศึกษาส่วนลด 3,000 บาท
- ลงต่อเนื่องคอร์สลด 10%