MAYASEVEN
HACK THINGS

SECURE APPLICATION DEVELOPMENT WORKSHOP

เขียนโค้ดให้ปลอดภัย เพิ่มความมั่นใจให้ธุรกิจของคุณ

เริ่มเรียน 3-4 ตุลาคม 2567

Early Bird
19,990.-
จากปกติ ~~29,990.-~~

จำกัดเฉพาะ
20
ที่นั่งแรกเท่านั้น!

ธรรศ แสงสมเรือง
นักเจาะระบบและ
นักแข่งเจาะระบบระดับประเทศ

นพ ภูมิไธสง
ผู้เชี่ยวชาญด้าน Cybersecurity
และอาจารย์ผู้สอนคอร์สของ
MAYASEVEN มากกว่า 10 ปี

วัตถุประสงค์

ปัจจุบันในโลกดิจิทัล ความปลอดภัยของแอปพลิเคชันเป็นสิ่งที่สำคัญอย่างยิ่ง การพัฒนาแอปพลิเคชันให้ปลอดภัยจึงเป็นทักษะที่จำเป็นสำหรับโปรแกรมเมอร์ทุกคน หลักสูตร **Secure Application Development Workshop** มุ่งเน้นให้ผู้เข้าอบรมเข้าใจหลักการสำคัญของการพัฒนาแอปพลิเคชันให้ปลอดภัย ครอบคลุมตั้งแต่การออกแบบ การเขียนโค้ด ไปจนถึงการทดสอบและการนำไปใช้งานจริง

การเรียนรู้และประยุกต์ใช้หลักการ Secure Coding ไม่เพียงแต่จะช่วยเพิ่มความปลอดภัยให้กับแอปพลิเคชันเท่านั้น แต่ยังช่วยลดต้นทุนและเวลาในการแก้ไขช่องโหว่ที่อาจเกิดขึ้นในภายหลังอีกด้วย อีกทั้งยังช่วยสร้างความเชื่อมั่นให้กับผู้บริหาร ลดความเสี่ยงจากการถูกแฮก การสูญเสียชื่อเสียงของบริษัท และการรั่วไหลของข้อมูลลูกค้า ซึ่งเป็นปัจจัยสำคัญในการแข่งขันทางธุรกิจ ดังนั้นการลงทุนพัฒนาทักษะด้าน Secure Coding จึงเป็นสิ่งที่คุ้มค่าและจำเป็นอย่างยิ่งสำหรับโปรแกรมเมอร์และองค์กรที่ต้องการสร้างแอปพลิเคชันที่มีคุณภาพและปลอดภัย หลักสูตรนี้จะช่วยให้ผู้เข้าอบรมก้าวทันภัยคุกคามที่เปลี่ยนแปลงอยู่ตลอดเวลา และพร้อมรับมือกับความท้าทายด้านความปลอดภัยในโลกไซเบอร์ได้อย่างมั่นใจ

เตรียมตัวก่อนเรียน

ผู้เรียนควร**มีพื้นฐานการเขียนโปรแกรมภาษาใดภาษาหนึ่ง** เพื่อที่จะอ่านทำความเข้าใจคอนเซ็ปต์หรือไอเดียในการหาช่องโหว่ภายในโค้ด

ผู้เรียนจำเป็น**จะต้องมี Notebook** สำหรับทำโจทย์โดยสเปคที่แนะนำคือ
1. RAM ไม่น้อยกว่า 8 GB
2. Harddisk มีพื้นที่ว่างอย่างน้อย 50 GB
3. ติดตั้งโปรแกรม Vmware Workstation (เวอร์ชั่นล่าสุด)

คอร์สนี้เหมาะกับใคร ?

ระดับปฏิบัติการ

- Software Developer
- Application Developer
- Quality Assurance/Tester
- Penetration Tester
- Vulnerability Tester
- Security Engineer
- Cloud Security
- DevOps Engineer
- DevSecOps Engineer
- Software Engineer
- Network Security
- Compliance Officer
- Information Security Professional
- System Engineer
- Network Engineer
- Test Engineer

ระดับบริหาร

- Software Security Manager
- Application Security Manager
- IT Project Manager
- Product Manager
- DevSecOps Manager
- IT Manager
- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)
- Chief Technology Officer (CTO)
- IT Director

Contact Us
LINE @MAYASEVEN
training@mayaseven.com

MAYASEVEN
HACK THINGS

โครงสร้างหลักสูตร (Course Outline)

Day 1

1. Foundations of Information Security

หัวข้อนี้เริ่มต้นด้วยการสำรวจแนวคิดพื้นฐานที่สำคัญของความปลอดภัยทางไซเบอร์ ได้แก่ การรักษาความลับ (Confidentiality) ความสมบูรณ์ของข้อมูล (Integrity) และความพร้อมใช้งาน (Availability) ผู้เรียนจะได้ศึกษาและเข้าใจหลักการสำคัญในการปกป้องข้อมูลและสินทรัพย์ดิจิทัลขององค์กร ความรู้พื้นฐานเหล่านี้จะเป็นรากฐานสำคัญในการสร้างกลยุทธ์และแนวปฏิบัติด้านความปลอดภัยที่มีประสิทธิภาพและยั่งยืน

2. Determining the Right Level of Security

ผู้เรียนจะได้เรียนรู้การประเมินและกำหนดระดับความปลอดภัยที่เหมาะสมสำหรับองค์กรหรือแอปพลิเคชัน โดยพิจารณาจากความเสี่ยง มูลค่าของข้อมูล ข้อกำหนดทางกฎหมาย และผลกระทบที่อาจเกิดขึ้น เพื่อให้แอปพลิเคชันมีความปลอดภัยในระดับที่เพียงพอและเหมาะสมกับบริบทการใช้งาน

3. Secure Design Principles and Concepts

ผู้เรียนจะได้เรียนรู้หลักการออกแบบที่ปลอดภัย เช่น แนวคิดการให้สิทธิ์น้อยที่สุด (Least Privilege) การป้องกันหลายชั้น (Defense in Depth) และการออกแบบให้ปลอดภัยตั้งแต่เริ่มต้น (Secure by Design) หลักการเหล่านี้ช่วยให้ผู้เรียนสามารถพัฒนาแอปพลิเคชันที่มีความปลอดภัยตั้งแต่การออกแบบจนถึงการใช้งานจริง ลดความเสี่ยงจากช่องโหว่และภัยคุกคามทางไซเบอร์

4. Security Development Lifecycle

ผู้เรียนจะได้เรียนรู้ขั้นตอนและกระบวนการในการนำความปลอดภัยเข้าไปในทุกช่วงของการพัฒนาแอปพลิเคชัน ตั้งแต่การวางแผน การออกแบบ การพัฒนา การทดสอบ จนถึงการบำรุงรักษา โดยมุ่งเน้นการตรวจสอบและลดความเสี่ยงด้านความปลอดภัยในแต่ละขั้นตอน เพื่อให้แน่ใจว่าแอปพลิเคชันมีความปลอดภัยเพียงพอและเป็นไปตามมาตรฐานสากล

5. Secure Coding Practices

ผู้เรียนจะได้เรียนรู้วิธีการเขียนโค้ดให้ปลอดภัยตามมาตรฐานสากล โดยมุ่งเน้นเทคนิคและแนวทางที่ช่วยลดความเสี่ยงการเกิดช่องโหว่ ผู้เรียนสามารถนำความรู้ที่ได้ไปใช้ในการตรวจสอบโค้ด (Code Review) เพื่อเพิ่มประสิทธิภาพและความปลอดภัยของโค้ดในกระบวนการพัฒนาได้อย่างทันที

6. Effective Threat Modeling Techniques

ผู้เรียนจะได้ศึกษาเกี่ยวกับการออกแบบ Threat Modeling เพื่อระบุและจัดการภัยคุกคามที่อาจเกิดขึ้น เรียนรู้วิธีการสร้างแบบจำลองภัยคุกคามอย่างมีประสิทธิภาพ พร้อมทั้งการใช้เครื่องมือที่เชื่อถือได้ ในการวิเคราะห์และประเมินความเสี่ยง ทำให้สามารถปกป้องระบบจากภัยคุกคามได้อย่างเป็นระบบ

7. Integrating Security into Development with DevSecOps

ผู้เรียนจะได้เรียนรู้เกี่ยวกับ DevSecOps ซึ่งเป็นแนวทางในการรวมความปลอดภัยเข้ากับกระบวนการพัฒนาและการดำเนินการ รวมถึงการใช้เครื่องมือต่าง ๆ และการตรวจสอบความปลอดภัยอัตโนมัติผ่าน CI/CD เพื่อเพิ่มประสิทธิภาพในการทดสอบและการตรวจจับช่องโหว่ ทำให้การพัฒนาแอปพลิเคชันมีความปลอดภัยยิ่งขึ้นตั้งแต่ต้นจนจบ

8. Application Security Myths

ผู้เรียนจะได้เรียนรู้และทำความเข้าใจในส่วนของความเชื่อผิด ๆ ที่เกี่ยวกับความปลอดภัยของแอปพลิเคชัน รวมถึงการเปิดเผยความเข้าใจที่ไม่ถูกต้องและวิธีการที่แท้จริงในการจัดการกับปัญหาด้านความปลอดภัย เพื่อเสริมสร้างการรับรู้และปรับปรุงแนวทางในการปกป้องแอปพลิเคชันจากภัยคุกคามอย่างมีประสิทธิภาพ

9. Top Application Vulnerabilities in Thailand

ในหัวข้อนี้ ผู้เรียนจะได้ศึกษาช่องโหว่ที่พบบ่อยในแอปพลิเคชันที่เกิดขึ้นจริงในประเทศไทย พร้อมตัวอย่างโค้ดที่มีช่องโหว่ ซึ่งได้รับการคัดเลือกจาก OWASP Top 10 และ CWE Top 25 เพื่อให้ครอบคลุมช่องโหว่และรูปแบบการโจมตีที่หลากหลาย ผู้เรียนจะได้วิเคราะห์และเรียนรู้วิธีการแก้ไขปัญหาอย่างเป็นระบบ โดยใช้กรณีศึกษาจริงเพื่อเสริมสร้างความเข้าใจในการจัดการและป้องกันช่องโหว่ในแอปพลิเคชัน

1. Broken Access Control ช่องโหว่ที่เกิดจากการควบคุมการเข้าถึงที่ไม่ดีพอ ซึ่งอาจทำให้ผู้ใช้ที่ไม่ได้รับอนุญาตเข้าถึงข้อมูลหรือฟังก์ชันสำคัญได้ ผู้เรียนจะได้วิเคราะห์ตัวอย่างโค้ดและเรียนรู้วิธีการป้องกันการเข้าถึงที่ไม่เหมาะสม

2. Cryptographic Failures ช่องโหว่ที่เกิดจากการใช้การเข้ารหัสที่ไม่ปลอดภัย เช่น การฝังคีย์ในโค้ดหรือการเข้ารหัสที่ไม่แข็งแรง ซึ่งอาจทำให้ข้อมูลสำคัญรั่วไหล ผู้เรียนจะวิเคราะห์ตัวอย่างโค้ดและเรียนรู้วิธีการใช้การเข้ารหัสอย่างถูกต้อง

3. Injection ช่องโหว่ที่เกิดจากการส่งข้อมูลที่เป็นอันตรายเข้าไปในแอปพลิเคชัน เช่น SQL Injection หรือ Cross-site Scripting ซึ่งอาจทำให้ข้อมูลถูกเปลี่ยนแปลงหรือถูกขโมยข้อมูล ผู้เรียนจะได้เรียนรู้วิธีการป้องกันผ่านการตรวจสอบและการกรองข้อมูล

MAYASEVEN
HACK THINGS

โครงสร้างหลักสูตร (Course Outline)

Day 2

4. Insecure Design ช่องโหว่ที่เกิดจากการออกแบบระบบที่ไม่ปลอดภัย เช่น การอัปโหลดไฟล์ที่เป็นอันตราย ผู้เรียนจะวิเคราะห์ตัวอย่างโค้ดและเรียนรู้วิธีการออกแบบระบบให้ปลอดภัย

5. Security Misconfiguration ช่องโหว่ที่เกิดจากการตั้งค่าที่ไม่เหมาะสม เช่น การตั้งค่าเซิร์ฟเวอร์ผิดพลาดหรือการเปิดเผยข้อมูลที่ไม่จำเป็น ผู้เรียนจะเรียนรู้วิธีการปรับแต่งการตั้งค่าเพื่อเพิ่มความปลอดภัย

6. Vulnerable and Outdated Components ช่องโหว่ที่เกิดจากการใช้ส่วนประกอบหรือแพ็กเกจที่มีความเสี่ยงเนื่องจากไม่ใช่เวอร์ชันล่าสุด ผู้เรียนจะเรียนรู้วิธีการตรวจสอบและอัปเดตส่วนประกอบเพื่อหลีกเลี่ยงความเสี่ยง

7. Identification and Authentication Failures ช่องโหว่ที่เกิดจากปัญหาการระบุตัวตนและการพิสูจน์ตัวตนที่ไม่ดีพอ ซึ่งอาจทำให้ผู้โจมตีเข้าถึงระบบได้โดยไม่ได้รับอนุญาต ผู้เรียนจะเรียนรู้ตัวอย่างโค้ดที่มีช่องโหว่และเรียนรู้วิธีป้องกันที่มีประสิทธิภาพ

8. Software and Data Integrity Failures ช่องโหว่ที่เกิดจากข้อผิดพลาดในการรักษาความสมบูรณ์ของแอปพลิเคชันหรือข้อมูลที่ไม่ดีพอ ซึ่งอาจทำให้ข้อมูลถูกเปลี่ยนแปลงหรือบุกรุกโดยไม่ได้รับอนุญาต ผู้เรียนจะวิเคราะห์ตัวอย่างโค้ดและเรียนรู้วิธีแก้ไขเพื่อเพิ่มความปลอดภัยให้กับแอปพลิเคชัน

9. Security Logging and Monitoring Failures ผู้เรียนจะได้ศึกษาเกี่ยวกับปัญหาที่เกิดจากการตั้งค่าการบันทึกและการตรวจสอบความปลอดภัยที่ไม่เพียงพอ ซึ่งอาจทำให้ไม่สามารถตรวจจับและตอบสนองต่อการละเมิดได้อย่างมีประสิทธิภาพ ผู้เรียนจะเรียนรู้วิธีการปรับปรุงการบันทึกข้อมูลและการตรวจสอบเพื่อเพิ่มความสามารถในการตรวจจับและตอบสนองต่อเหตุการณ์ได้อย่างทันท่วงที

10. Server-Side Request Forgery (SSRF) ช่องโหว่ที่ทำให้ผู้โจมตีสามารถส่งคำร้องขอของเซิร์ฟเวอร์ไปยังระบบภายในหรือภายนอกได้โดยไม่ได้รับการควบคุมอย่างเหมาะสม ผู้เรียนจะเรียนรู้ตัวอย่างโค้ดที่มีช่องโหว่และเรียนรู้วิธีป้องกันที่มีประสิทธิภาพ

11. Memory Related Vulnerabilities (Bonus) ช่องโหว่ที่เกี่ยวข้องกับการจัดการหน่วยความจำของเครื่อง เช่น การเข้าถึงหน่วยความจำที่ไม่ได้รับอนุญาตหรือการจัดการหน่วยความจำผิดพลาด ซึ่งอาจทำให้เกิดปัญหาด้านความปลอดภัย ผู้เรียนจะเรียนรู้ตัวอย่างโค้ดที่มีช่องโหว่และวิธีการป้องกันและแก้ไขปัญหาเกี่ยวกับการจัดการหน่วยความจำ

สำหรับผู้เรียน

- เพิ่มทักษะในการ **เขียนโค้ด**ที่ปลอดภัย
- เพิ่มโอกาสใน การ**เติบโต**ในสายอาชีพ
- **ระบุ**และ**แก้ไข**ช่องโหว่ได้รวดเร็ว
- ฝึกปฏิบัติการ**แก้ไขโค้ด**ในสถานการณ์จริง

สำหรับองค์กร

- **ลด**ความเสี่ยงและยกระดับความปลอดภัย
- **สร้าง**วัฒนธรรมความปลอดภัยในองค์กร
- **ประหยัด**ค่าใช้จ่ายจากความเสียหายที่อาจจะเกิดขึ้นในภายหลัง
- นำ **Framework** และกระบวนการไปใช้งานได้ทันที