Course Introduction

หลักสูตรนี้จะเป็นจุดเริ่มต้นสำหรับการทำความเข้าใจในเรื่องของ Web Application ในภาพกว้างโดยที่เราจะเริ่มต้นจากการเรียนรู้หลักการพื้นฐานของ Web application เป็นอย่างไรและมี Best practices อะไรบ้างที่เราควรจะปฏิบัติตาม รวมทั้งการวาง Architecture ที่ถูกต้องควรจะเป็นอย่างไร
หลักสูตรนี้จะเป็นพื้นฐานที่สำคัญสำหรับผู้ที่ทำงานเกี่ยวกับ Security ใน Application layer และ Developer ทั่วไป

Course Objectives

- เข้าใจการทำงานพื้นฐานของ Web application
- เข้าใจธรรมชาติและปัญหาของ Web application
- เข้าใจการออกแบบ Architecture แบบต่างๆ
- รู้ว่าสิ่งที่ต้องทำเพื่อให้ Web Application ของเราปลอดภัยมีอะไรบ้าง

Learning Level

- Intermediate

Course Duration

- 3 Days

Target Group

- Project Manager
- Business Analyst
- Software Developer
- Software Engineer
- ผู้สนใจทั่วไป

Course Outline

Day 1

1. Introduction to IT Security

- Why you have to secure?
- IT Security basic concept
- CIA Triad

- Cryptography 101
- Basic security control
- HTTP Request and Response
- Web Application Firewall (WAF)
- Rapid Application Self-Protection (RASP)
- Web application architecture
- Benefit of Micro services architecture

2. Threat and Vulnerability

- Find open ports and services
- Tools to spider website
- OWASP Top 10 (2017)
- CWE/SANS Top 25
- Buffer overflow
- Denial of Service (DoS)
- CSRF and Logic flaw
- Weak signature algorithm

Day 2

3. Intercepting message

- Man in the Middle Attack (MITM Attack)
- Proxy
- OWASP ZAP
- Manipulate request and response
- Problem of including external JavaScript

4. Know about Https

- How does SSL/TLS Work
- Grading Https Configuration
- Strict Transport Security (HSTS)
- Blocked mixed content
- Public Key Pinning (HPKP)
- SSL Certificates
- Intercept Https message

- SSL strip attack

Day 3

5. Securing your site

- Turn-off form autocomplete
- Properly configuring server MIME types
- Hiding banner
- Using sub resource integrity
- OWASP Secure header project
- Content Security Policy (CSP)
- Define unsafe functions
- White-listing input validation

Day 4

6. Securing uploaded files

- Setting file permissions
- Limiting upload file types
- Validate upload file type

7. Same-origin policy

- Defining origin
- Cross-site scripting attack (XSS)
- Cross-site request forgery attack (CSRF)
- Enable Cross Origin Resource Sharing (CORS)
- Securing cookies

8. Secure authentication

- Preventing account enumeration
- Brute forcing attack
- Throttling brute-force attack
- Anti-Automation (CAPTCHA)
- Multi-factor authentication
- Password requirements
- Secure password recovery

For More Information & Registration, Please Contact Training Division
Tel:(66) 2253-4736, Fax:(66) 2253-4737, Hotline:(66) 86-325-7129, E-mail: registration@acisonline.net

– Implementing password reset tokens

Day 5

9. Logging and Monitoring

– Logging, Monitoring and Alerting
– Should and should not log
– Improving quality of log file
– Applying an effective monitoring strategy

10. Automated security scanning

– Arachni
– OWASP ZAP

Official Training Partner