Course Introduction

หลักสูตรนี้จะเน้นการสร้างความปลอดภัยให้กับ Web API โดยจะเริ่มตั้งแต่การทำความเข้าใจการทำงานของ API ในรูปแบบต่างๆ ทั้ง REST, GraphQL และ gRPC ซึ่งในหลักสูตรนี้เราจะเน้นที่ความปลอดภัยของ REST API เป็นหลักเนื่องจากเป็น Common practices ของการทำ Web API และปัญหาใหญ่ที่สุดของ API คือเรื่องของ Authorization
เราจึงต้องทำความเข้าใจการทำงานของ OAuth2(Authorization Framework ที่ถูก Implement มากที่สุด) เพื่อที่จะได้เลือก Flow การทำงานได้อย่างถูกต้อง

Course Objectives

- เข้าใจการทำงานพื้นฐานของ REST API
- รู้จัก Technology ที่ใช้ในการทำ Web API
- เข้าใจธรรมชาติและปัญหาของ Web API
- เข้าใจการทำงานของ JWT และ OAuth2
- รู้ว่าต้องทำอย่างไรเพื่อให้ Web API ของเราปลอดภัย

Learning Level

- Intermediate

Course Duration

- 3 Days

Target Group

- Software Engineer
- Software Developer
- Software Tester

Course Outline

Day 1

1. Overview of the security threats
    a. Introduction to OWASP Project
    b. OWASP Top 10
    c. OWASP API Top 10
    d. OWASP REST Security
    e. OWASP REST Cheatsheet

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

API Best practices

a. What is REST API
b. What is GraphQL
c. What is gRPC
d. REST vs RPC
e. HTTP Method
f. HTTP Request and Response
g. Manipulate resources
h. Using API Gateway

Day 2

API Testing

a. Open API Specification (OAS)
b. Automated Testing with Postman
c. Automated Testing with SoapUI
d. Performance Testing with jMeter

Same-origin policy

a. Defining origin
b. Cross-site scripting attack (XSS)
c. Cross-site request forgery attack (CSRF)
d. Enable Cross Origin Resource Sharing (CORS)

Day 3

SSL Encrypted API Traffic

a. Man in the Middle attack
b. Rejecting invalid certificates
c. Identifying Invalid Certificates
d. Certificate Pinning

Secure RESTful API

a. Require Https
b. How to CORS work
c. Middleware concepts
d. Add CORS middleware
e. Versioning your API
f. Secure API endpoints
g. API Rate Limiting
h. Self-documentation and HATEOAS
i. Logging and Monitoring services
j. HTTP Exception handling
k. Defence in Depth with Microservices

Official Training Partner