Course Introduction

หลักสูตรนี้จะเน้นการสร้างความปลอดภัยให้กับ Web API โดยจะเริ่มตั้งแต่ การทำความเข้าใจการทำงานของ API ในรูปแบบต่างๆ ทั้ง REST, GraphQL และ gRPC ซึ่ง ในหลักสูตรนี้เราจะเน้นที่ความปลอดภัยของ 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

<u>Day 1</u>

1. Overview of the API security
   a. OWASP REST Security
   b. OWASP REST Cheatsheet
   c. Generic Web Service Security
   d. RESTful web service

© Copyright 2001-2026: ACIS Professional Center Co., Ltd. All rights reserved. All contents of this form constitute the property of ACIS Professional Center Co., Ltd. and may not be copied, reproduced or distributed without prior written permission

e. GraphQL

2. OWASP API Top 10
   a. Broken Object Level Authorization
   b. Broken Authentication
   c. Broken Object Property Level Authorization
   d. Unrestricted Resource Consumption
   e. Broken Function Level Authorization

Day 2

3. OWASP API Top 10 (Cont.)
   a. Unrestricted Access to Sensitive Business Flows
   b. Server-Side Request Forgery
   c. Security Misconfiguration
   d. Improper Inventory Management
   e. Unsafe Consumption of APIs
4. Secure RESTful API
   a. Require https
   b. Middleware concepts
   c. Add CORS middleware
   d. Secure API endpoints
   e. API rate limiting
   f. Self-documentation and HATEOAS
   g. Logging and monitoring services
   h. HTTP exception handling
   i. Defence in depth with Microservices

Day 3

5. API Testing
   a. Open API specification (OAS)
   b. Automated testing with Postman
   c. Scanning API with OWASP ZAP
6. Securing API with OAuth 2.0
   a. Authentication and authorization
   b. What is OAuth

© Copyright 2001-2026: ACIS Professional Center Co., Ltd. All rights reserved. All contents of this form constitute the property of ACIS Professional Center Co., Ltd. and may not be copied, reproduced or distributed without prior written permission

c. What is Open ID Connect (OIDC)

d. How access token work

e. Add a token endpoints

f. OAuth grant types

g. Refresh token flow

h. Authorization server

i. Leveraging scopes

Official Training Partner

© Copyright 2001-2026: ACIS Professional Center Co., Ltd. All rights reserved. All contents of this form constitute the property of ACIS Professional Center Co., Ltd. and may not be copied, reproduced or distributed without prior written permission