Faysal Aziz

API Security Essentials

1-da course

FA-0105 · one-day

Cybersecurity

Introduction

This one-day intensive course is designed to equip participants with a comprehensive understanding of the critical aspects of API (Application Programming Interface) security. As APIs become the backbone of software communication and integration, securing them has never been more crucial. This course covers the foundational security principles, common vulnerabilities, and best practices for securing APIs. Through a blend of theoretical concepts and practical exercises, participants will learn how to design, implement, and manage secure APIs.

Learning outcomes

By the end of this course, participants will be able to:

- Understand the importance and principles of API security.
- Identify common security threats and vulnerabilities affecting APIs.
- Implement strategies for authenticating and authorizing API users.
- Apply best practices for securing data in transit and at rest.
- Use tools and techniques for testing and monitoring API security.
- Develop strategies to mitigate and respond to security incidents involving APIs.

Prerequisites

Participants should have:

1. Working understanding of web technologies (HTTP, HTTPS)
2. Deep understanding with structures such as JSON/XML.
3. Understanding of RESTful API and CRUD concepts.

4. Experience with programming.
5. Good understanding of client-server architecture.
6. Basic knowledge of cybersecurity fundamentals.

   Access to:

   1. Web browser
   2. Postman
   3. Terminal (Terminal / Command Prompt / PowerShell etc.)
   4. Unrestricted access to the internet

8. Willingness to learn.

Training outline

1. Introduction to API Security

1. Understanding APIs and their importance in modern software development.
2. Overview of API security and its significance.

2. Fundamental Security Principles for APIs

1. Confidentiality, Integrity, and Availability (CIA) Triad in APIs.
2. Least privilege and defense-in-depth strategies.

3. Common API Security Threats and Vulnerabilities

1. Injection Flaws: SQL, Command, and XXE (XML External Entity) Injection.
2. Broken Authentication and Session Management.
3. Sensitive Data Exposure.
4. XML and JSON Threats.
5. Insecure Direct Object References (IDOR).
6. Security Misconfiguration.
7. Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF).

4. Authentication and Authorization

1. Basics of API Authentication Mechanisms: API Keys, Basic Auth, Tokens.
2. OAuth 2.0 and JWT (JSON Web Tokens) for secure authorization.
3. Implementing Role-Based and Attribute-Based Access Control.

5. Securing Data in Transit and at Rest

1. SSL/TLS for Data in Transit.
2. Encryption and Hashing Techniques for Data at Rest.
3. Best Practices for API Keys and Credentials Management.

6. API Security Best Practices and Standards

1. Secure Coding Practices for APIs.
2. OpenAPI Specification (OAS) for API Security.
3. Utilizing API Gateways and Service Meshes for Enhancing Security.

7. Testing and Monitoring API Security

1. Penetration Testing and Vulnerability Assessment for APIs.
2. Tools and Techniques for API Security Testing.
3. Logging, Monitoring, and Anomaly Detection.

8. Incident Response and Recovery

1. Preparing for Security Incidents.
2. Responding to API Security Breaches.
3. Post-Incident Analysis and Recovery Processes.

9. Exercise and Case Study

1. Hands-on Exercise: Securing a Sample API.
2. Case Study: Analyzing and Mitigating an API Security Breach.

The course concludes with a comprehensive review of the covered topics, followed by a Q&A session where participants can discuss specific concerns or scenarios related to their work environment. Participants will leave the course with a solid foundation in API security, equipped with the knowledge and skills necessary to protect their APIs from potential threats and vulnerabilities.

© 2026 Faysal Aziz · Kuala Lumpur