API Security Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

API Security Training introduces the essential security principles and defensive approaches used to protect **Application Programming Interfaces (APIs)**, which enable communication and data exchange between modern software systems.

APIs play a central role in connecting digital applications and services, but they also represent important targets for cyberattacks. As a result, **authentication**, **authorization**, **data confidentiality**, and **vulnerability identification** are critical considerations when developing and operating secure API-based systems.

The course explores authentication technologies such as **OAuth 2.0** and **OpenID Connect**, along with **API Gateway** management, **authorization security**, **input validation**, **injection attacks**, and techniques for protecting API services.

Participants also examine **rate limiting**, protection against **DoS/DDoS attacks**, **TLS/SSL**, **logging**, **monitoring**, and **API penetration testing methodologies**. The training aims to strengthen their ability to assess and improve the security of modern API infrastructures.

Prerequisites

There are **no prerequisites** for attending this training.

Who Should Attend

- **Software Professionals**
- **Cybersecurity Specialists and Analysts**
- **System and Security Architects**
- **DevOps and DevSecOps Engineers**
- **IT Auditors**

API Security Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

Upon completing this training, you will be able to:

- Explain fundamental **API security** concepts and their importance in modern applications.
- Understand **OAuth 2.0** and **OpenID Connect** flows and evaluate suitable authentication methods.
- Establish secure authorization structures using **RBAC and ABAC**.
- Reduce risks associated with **Injection Attacks** through effective **Input Validation**.
- Improve API resilience against **DoS/DDoS attacks** using **Rate Limiting** and resource management.
- Apply approaches for protecting data transmission with**TLS/SSL**.
- Support security event tracking through **Logging and Monitoring**.
- Identify vulnerabilities using **API penetration testing methodologies** and prepare **security assessment reports**.

Outline

1. Introduction to API Security and Fundamental Concepts

- Understanding **Application Programming Interfaces (APIs)**
- The role of APIs in modern software architectures
- Why API security is important
- Evaluating security requirements for API-based systems

2. Authentication Mechanisms

- Understanding **Authentication**
- The role of authentication in API access
- Evaluating secure authentication approaches

3. OAuth 2.0 and OpenID Connect

- Exploring **OAuth 2.0** flows
- Understanding **OpenID Connect (OIDC)**
- Selecting appropriate secure sign-in and access models for different system requirements

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Integrating authentication mechanisms into API-based systems

4. Authorization Security

- Introduction to **Authorization**
- Managing role-based access with **RBAC (Role-Based Access Control)**
- Applying attribute-based authorization with **ABAC (Attribute-Based Access Control)**
- Establishing secure authorization hierarchies

5. Input Validation and Injection Attacks

- Understanding **Input Validation**
- Evaluating the security of incoming API data
- Risks associated with **Injection Attacks**
- Reducing attack risks through secure input validation techniques

6. API Gateway and Service Protection

- The role of **API Gateway** management in API security
- Controlling request traffic with **Rate Limiting**
- Resource management strategies
- Improving service resilience against **DoS and DDoS attacks**

7. Secure Data Communication, Logging, and Monitoring

- Protecting data transmission with **TLS/SSL**
- Fundamental approaches to maintaining data confidentiality
- **Logging** practices
- **Monitoring** techniques
- Supporting security event tracking and **incident response processes**

8. API Security Testing and Penetration Testing Methodologies

- Introduction to **API Penetration Testing**
- Identifying API security vulnerabilities
- Evaluating security findings
- Preparing **security assessment reports** aligned with international standards

API Security Training

Duration: **3 Day**

BİLGİNÇ
IT Academy
info@bilginc.com
bilginc.com