API Security Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

API Güvenliği Eğitimi, modern yazılım sistemlerinde uygulamalar arasında veri alışverişini sağlayan **API'ların (Application Programming Interfaces)** güvenliğini korumaya yönelik temel yaklaşımları ve savunma yöntemlerini ele alır.

Dijital sistemlerin birbirine bağlı çalışmasında önemli bir rol üstlenen API'lar, aynı zamanda siber saldırılar açısından kritik hedefler arasında yer alır. Bu nedenle **kimlik doğrulama**, **yetkilendirme**, **veri gizliliği** ve **güvenlik açıklarının tespit edilmesi**, API tabanlı uygulamaların güvenli biçimde geliştirilmesi ve işletilmesi için önem taşır.

Eğitim kapsamında **OAuth 2.0** ve **OpenID Connect** gibi kimlik doğrulama teknolojileri, **API Gateway** yönetimi, **yetkilendirme güvenliği**, **Input Validation**, **Injection saldırıları** ve API sistemlerini korumaya yönelik yöntemler incelenir.

Katılımcılar ayrıca **Rate Limiting**, **DoS/DDoS saldırılarına karşı dayanıklılık**, **TLS/SSL**, **loglama**, **izleme** ve **API sızma testi metodolojileri** hakkında bilgi edinerek modern API altyapılarının güvenliğini değerlendirme ve geliştirme becerilerini ilerletir.

Prerequisites

Bu eğitime katılım için herhangi bir **ön koşul bulunmamaktadır**.

Who Should Attend

- **Yazılım uzmanları**
- **Siber güvenlik uzmanları ve analistleri**
- **Sistem ve güvenlik mimarları**
- **DevOps ve DevSecOps mühendisleri**
- **BT denetçileri**

API Security Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

Eğitimi tamamladığınızda:

- **API güvenliği** kavramlarını ve modern uygulamalardaki önemini açıklayabileceksiniz.
- **OAuth 2.0** ve **OpenID Connect** akışlarını anlayarak uygun kimlik doğrulama yöntemlerini değerlendirebileceksiniz.
- **RBAC ve ABAC** modelleriyle güvenli yetkilendirme yapıları oluşturabileceksiniz.
- **Input Validation** teknikleriyle **Injection saldırılarının** oluşturduğu riskleri azaltabileceksiniz.
- **Rate Limiting** ve kaynak yönetimi yaklaşımlarıyla API servislerinin **DoS/DDoS** saldırılarına karşı dayanıklılığını artırabileceksiniz.
- **TLS/SSL** ile veri iletişiminin korunmasına yönelik yöntemleri uygulayabileceksiniz.
- **Logging ve Monitoring** süreçlerini kullanarak güvenlik olaylarının izlenmesini destekleyebileceksiniz.
- **API sızma testi metodolojileri** ile güvenlik açıklarını belirleyebilecek ve **denetim raporları** hazırlayabileceksiniz.

Outline

1. API Güvenliğine Giriş ve Temel Kavramlar

- **API (Application Programming Interface)** kavramı
- API'ların modern yazılım mimarilerindeki rolü
- API güvenliğinin önemi
- API tabanlı sistemlerde güvenlik gereksinimlerinin değerlendirilmesi

2. Kimlik Doğrulama Mekanizmaları

- **Authentication (Kimlik Doğrulama)** kavramı
- API erişiminde kimlik doğrulamanın rolü
- Güvenli kimlik doğrulama yaklaşımlarının değerlendirilmesi

3. OAuth 2.0 ve OpenID Connect

- **OAuth 2.0** akışlarının incelenmesi
- **OpenID Connect (OIDC)** yapısının anlaşılması

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Farklı sistem gereksinimlerine uygun güvenli giriş ve erişim modellerinin seçilmesi
- Kimlik doğrulama mekanizmalarının API sistemlerine entegrasyonu

4. Yetkilendirme (Authorization) Güvenliği

- **Authorization (Yetkilendirme)** kavramı
- **RBAC (Role-Based Access Control)** ile rol tabanlı erişim yönetimi
- **ABAC (Attribute-Based Access Control)** ile nitelik tabanlı yetkilendirme
- Yetki hiyerarşilerinin güvenli biçimde yapılandırılması

5. Input Validation ve Injection Saldırıları

- **Input Validation (Girdi Doğrulama)** yaklaşımı
- API'larda giriş verilerinin güvenlik açısından değerlendirilmesi
- **Injection saldırılarının** oluşturduğu riskler
- Güvenli girdi doğrulama teknikleriyle saldırı risklerinin azaltılması

6. API Gateway ve Servis Koruma Yaklaşımları

- **API Gateway** yönetiminin API güvenliğindeki rolü
- **Rate Limiting** ile istek trafiğinin kontrol edilmesi
- Kaynak yönetimi stratejileri
- **DoS ve DDoS saldırılarına** karşı servis dayanıklılığının artırılması

7. Veri İletişimi Güvenliği, Loglama ve İzleme

- **TLS/SSL** kullanılarak veri iletişiminin korunması
- Veri gizliliğinin sağlanmasına yönelik temel yöntemler
- **Logging (Loglama)** süreçleri
- **Monitoring (İzleme)** uygulamaları
- Güvenlik olaylarının takip edilmesi ve **olay müdahale süreçlerinin** desteklenmesi

8. API Güvenlik Testleri ve Sızma Testi Metodolojileri

- **API sızma testi (API Penetration Testing)** yaklaşımları
- API güvenlik açıklarının tespit edilmesi
- Güvenlik bulgularının değerlendirilmesi

API Security Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

- Uluslararası standartlara uygun **güvenlik denetim raporlarının** hazırlanması