AI & Web Application Security A Practical Guide to Risks & Responses (TTAI2835) Eğitimi

Süre: **1 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

Overview

Yapay zekânın web uygulama güvenliği üzerindeki etkilerini öğrenin, AI tabanlı güvenlik risklerini analiz edin ve modern web ortamlarında güvenli AI kullanım stratejileri geliştirin.

AI & Web Application Security: A Practical Guide to Risks & Responses eğitimi, yapay zekâ destekli web uygulamalarında ortaya çıkan güvenlik risklerini anlamak ve güvenli AI entegrasyonu sağlamak isteyen profesyoneller için hazırlanmış kapsamlı bir teknik farkındalık programıdır.

Modern web uygulamalarında kullanılan **chatbotlar**, **LLM sistemleri**, **generative AI çözümleri** ve AI destekli otomasyon araçları yeni nesil güvenlik açıklarını da beraberinde getirmektedir. Bu eğitim, ekiplerin henüz tam olarak hazırlıklı olmadığı bu yeni tehdit ortamını anlamasına yardımcı olur.

Program boyunca katılımcılar; **prompt injection**, **model manipulation**, **unsafe AI output**, **AI-powered attacks**, **secure coding for AI**, **AI API security**, **OWASP AI güvenlik standartları** ve güvenli AI deployment stratejileri gibi kritik konuları inceleyecektir.

Gerçek dünya senaryoları, teknik demolar ve uygulamalı örnekler sayesinde katılımcılar; AI destekli sistemlerde güvenlik açıklarını tanımlamayı, riskleri değerlendirmeyi ve organizasyonlarında güvenli AI kullanım politikaları geliştirmeyi öğrenecektir.

Bu eğitim; AI güvenlik farkındalığını artırmak, güvenli web uygulama geliştirme süreçlerini desteklemek ve modern AI tehditlerine karşı hazırlıklı olmak isteyen ekipler için güçlü bir başlangıç sunmaktadır.

Prerequisites

Bu eğitim teknik seviyede olsa da uygulamalı laboratuvar içermez. Katılımcıların aşağıdaki konularda temel bilgi sahibi olması önerilir:

- Web uygulama mimarileri
- Input validation
- API güvenliği
- Temel application security kavramları
- Teknik workflow ve diyagram okuma becerisi

AI & Web Application Security A Practical Guide to Risks & Responses (TTAI2835) Eğitimi

Süre: **1 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

Who Should Attend

Bu eğitim aşağıdaki profesyoneller için idealdir:

- **Security professionals**
- **Technical leads**
- **Web developers**
- **DevSecOps ekipleri**
- **Application security uzmanları**
- **IT yöneticileri**
- **Security analysts**
- AI güvenliği konusunda farkındalık kazanmak isteyen karar vericiler

Bu program özellikle **AI destekli web uygulamaları**, **LLM güvenliği**, **AI risk yönetimi** ve **secure AI adoption** süreçlerinde görev alan ekipler için uygundur.

What You Will Learn

Eğitim sonunda katılımcılar şunları öğrenir:

- Yapay zekânın web uygulamalarına getirdiği güvenlik risklerini anlamak
- **Prompt injection** ve **model manipulation** saldırılarını tanımak
- AI destekli sistemlerde güvenlik açıklarını değerlendirmek
- **Secure AI coding** prensiplerini uygulamak
- AI API güvenliğini sağlamak
- OWASP AI ve LLM güvenlik rehberlerini kullanmak
- Güvenli AI deployment stratejileri geliştirmek
- AI risk yönetimi süreçleri oluşturmak
- Organizasyon genelinde güvenli AI kullanım politikaları hazırlamak

Outline

1. Web Uygulamalarında AI ve Güvenli Kodlama Temelleri

- Yapay zekâ tehdit ortamı
- AI farkındalığının önemi
- Machine Learning ve Deep Learning temelleri
- LLM ve Generative AI kavramları
- AI'nin yazılım geliştirme süreçlerine etkisi
- Demo: Modern uygulamalarda AI entegrasyonu

2. AI Çağında Secure Coding Prensipleri

- AI'ye özel güvenlik açıkları
- AI/ML entegrasyon riskleri
- Geleneksel secure coding vs AI secure development
- Güvensiz AI kod örnekleri

BİLGİNÇ IT Academy

info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

- OWASP AI güvenlik rehberleri
- Secure vs insecure AI-infused code

3. AI Destekli Saldırılar ve Riskler

- **Prompt injection saldırıları**
- **Data poisoning**
- **Model manipulation**
- AI backdoor saldırıları
- AI-generated code riskleri
- Social engineering ve AI
- Demo: Adversarial AI attacks

4. AI Tabanlı Saldırılara Karşı Savunma

- Enterprise AI defense strategy
- AI threat modeling
- Governance ve audit süreçleri
- AI model monitoring
- AI component verification
- Model poisoning mitigation
- Secure AI frameworks
- Software supply chain security

5. Web Uygulamalarında Güvenli AI Entegrasyonu

- Production ortamında AI kullanımı
- Input / output validation
- Injection prevention teknikleri
- Secure API design
- AI workflows içinde veri güvenliği
- Demo: Python AI model entegrasyonu

6. NLP ve AI Güvenlik Riskleri

- NLP sistem güvenliği
- Data leakage riskleri
- NLP tabanlı saldırılar
- Vulnerability detection
- Prompt injection mitigation yöntemleri

7. AI Risk Yönetimi ve Security Leadership

- **NIST AI RMF**
- ISO/IEC AI standartları
- AI governance frameworkleri
- Enterprise AI guardrails
- Secure AI deployment checklist
- GitHub Copilot ve ChatGPT güvenliği
- Development team guidance

BİLGİNÇ IT Academy

info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

8. İş Yerinde Güvenli AI Kullanımı

- Departmanlarda AI araç kullanımı
- Güvenli veri paylaşımı
- Internal AI policies oluşturma
- Shadow AI risklerini azaltma
- Security leadership stratejileri