Ensuring Code Quality and Security in AI assisted Software Engineering Eğitimi

BİLGİNÇ
IT Academy
info@bilginc.com
bilginc.com

Süre: **1 Gün**

Ensuring Code Quality and Security in AI Assisted Software Engineering eğitimi, yapay zeka destekli geliştirme araçlarından yararlanırken kod kalitesi, uygulama güvenliği ve uyumluluk sorumluluğunu korumak isteyen yazılım profesyonellerine yönelik uygulamalı bir programdır.

Üretken yapay zeka araçları yazılım geliştirme süreçlerini hızlandırabilir; ancak AI tarafından üretilen kodun doğrudan kabul edilmesi mantıksal hatalara, güvenlik açıklarına, gereksiz karmaşıklığa ve gözden kaçan edge case'lere yol açabilir. Eğitim, geliştiricilerin AI çıktısını eleştirel biçimde değerlendirmesine ve bu çıktıları sağlam yazılım mühendisliği uygulamalarıyla doğrulamasına odaklanır.

Katılımcılar; hallucinated API'ler, yanlış varsayımlar, eksik test senaryoları ve güvensiz kodlama kalıpları gibi yaygın AI kaynaklı sorunları inceler. Testing, static analysis, automated quality checks ve secure coding teknikleri gerçekçi senaryolar üzerinde uygulanır. OWASP Top 10 kapsamındaki riskler üzerinden AI tarafından oluşturulan kodun güvenlik açısından nasıl değerlendirileceği ve iyileştirileceği ele alınır.

Program ayrıca teknik kontrollerin ötesine geçerek code provenance, fikri mülkiyet, lisanslama, veri koruma ve kurumsal AI politikalarını kapsar. Böylece katılımcılar AI araçlarını yalnızca daha verimli değil, aynı zamanda kontrollü, güvenli ve kurumsal standartlarla uyumlu biçimde kullanmayı öğrenir.

Önkoşullar

Katılımcıların:

- En az bir programlama dilinde kod yazma deneyimine,
- Version control ve testing gibi temel yazılım geliştirme uygulamalarına aşinalığa,
- Uygulama güvenliği kavramları hakkında temel bilgiye,
- GitHub Copilot veya benzeri AI destekli geliştirme araçları hakkında genel farkındalığa

sahip olmaları önerilir.

Kimler Katılmalı

Bu eğitim özellikle:

- AI destekli kodlama araçlarını kullanan veya kullanmaya hazırlanan yazılım geliştiriciler ve mühendisler,
- Kod kalitesi ve güvenlik standartlarından sorumlu teknik liderler,
- Geliştirme süreçlerine otomasyon ve AI araçları entegre eden DevOps ve platform mühendisleri,
- Daha geniş bir dijital dönüşüm kapsamında yazılım geliştirme süreçlerinde AI kullanımını benimseyen kuruluşların teknik ekipleri

için tasarlanmıştır.

Ensuring Code Quality and Security in AI assisted Software Engineering Eğitimi

Süre: **1 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Neler Öğreneceksiniz

Eğitimin sonunda katılımcılar:

- Kod kalitesi ve güvenliğine ilişkin sorumluluğu koruyarak AI destekli geliştirme araçlarını kullanabilir,
- AI tarafından oluşturulan kod içerisindeki mantıksal hataları, güvensiz kalıpları ve diğer yaygın sorunları belirleyebilir,
- AI destekli geliştirme süreçlerine testing, static analysis ve automated quality checks dahil edebilir,
- OWASP Top 10 ile ilişkili güvenlik açıklarını tespit ederek uygun düzeltmeleri uygulayabilir,
- AI tarafından üretilen kodu maintainability, performance ve robustness açısından refactor edebilir,
- AI çıktılarının hangi durumlarda kullanılabileceğini ve ne zaman ek doğrulama gerektiğini değerlendirebilir,
- Sorumlu AI destekli yazılım geliştirmeye yönelik kurumsal governance çalışmalarına katkıda bulunabilir.

Eğitim İçeriği

AI Destekli Geliştirmeye Başlangıç

- AI destekli yazılım geliştirme araçları ve yeteneklerine genel bakış
- Model karşılaştırma araçları ve farklı prompting yaklaşımlarının gösterimi
- Üretkenlik kazanımları ile kalite ve güvenlik arasındaki trade-off'lar
- Mevcut geliştirme süreçlerinde AI kullanımına ilişkin grup tartışması
- **Lab:** AI tarafından oluşturulan kodun kalitesini değerlendirme
- AI çıktılarını yapılandırılmış bir kontrol listesiyle inceleme
- Correctness, maintainability ve security sorunlarını belirleme
- Bulguları risk seviyesine göre sınıflandırma ve önceliklendirme

Challenge: Task Management API

- Dependency ve scheduling logic içeren bir task manager oluşturma
- Circular dependency ve resource conflict sorunlarını tespit etme
- Uygulamayı iş gereksinimlerine göre değerlendirme
- Structured code review tekniklerini uygulama

AI Kaynaklı Kod Kalitesi Sorunlarını Anlamak

- AI-generated code içerisindeki yaygın hata kalıpları
- Hallucinated API'ler ve hatalı varsayımlar
- Gizli karmaşıklık ve over-engineering
- Eksik edge case'ler ve tutarsız mantık
- İnsan ve AI tarafından oluşturulan kodlarda ortak coding standards sağlama
- Linters, formatters ve automated code review araçlarını sürece dahil etme
- Pull request ve code review uygulamalarını değerlendirme

Lab: AI Kodunu Test Etme ve Refactoring

- AI tarafından oluşturulan unit test'leri üretme ve çalıştırma
- Test coverage içerisindeki boşlukları belirleme

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Invalid inputs ve concurrency gibi edge case'leri doğrulama
- Kodu clarity, modularity ve maintainability açısından refactor etme
- Logging ve error handling ekleme
- Performance iyileştirmeleri gerçekleştirme

Challenge: E-Commerce Pricing Engine

- İndirim, vergi ve promosyonları kapsayan fiyatlandırma mantığı geliştirme
- Yanlış hesaplamaları ve edge case problemlerini belirleme
- Test coverage'ı geliştirme ve deterministic sonuçlar sağlama
- Static analysis ve quality gates uygulama

AI Destekli Geliştirmede Güvenlik

- AI-generated code açısından OWASP Top 10 risklerine giriş
- Authentication, data handling ve API'lerde karşılaşılan yaygın güvenlik açıkları
- Security scanning ve dependency analysis araçları
- Secure coding uygulamalarının AI iş akışlarıyla bütünleştirilmesi

Lab: Güvenlik Açıklarını Bulma ve Düzeltme

AI tarafından oluşturulan bir user management sistemi üzerinde aşağıdaki riskler incelenir:

- Broken access control
- Zayıf cryptographic uygulamalar
- Injection açıkları
- Authentication zayıflıkları
- Manuel inceleme sonuçlarını automated security tools ile karşılaştırma
- Parameterised queries uygulama
- Güçlü password hashing kullanma
- Input validation ve sanitisation
- Secure token handling

Güvenlik Testleri ve Doğrulama

- Saldırı senaryolarını simüle eden test case'ler oluşturma
- Temel penetration testing senaryolarını uygulama
- Yapılan düzeltmeleri güvenlik gereksinimlerine göre doğrulama

İleri Seviye Uygulama: Multi-Factor Authentication

- Sistemi güvenli authentication mekanizmalarıyla genişletme
- Edge case'leri değerlendirme
- Timing attack risklerini ele alma
- Kullanılabilirlik ile güvenlik arasında uygun dengeyi kurma

Governance, Fikri Mülkiyet ve Uyumluluk

- Code provenance ve AI-generated content
- Lisanslama riskleri ve intellectual property konuları
- Veri koruma gereksinimleri
- Kurumsal AI politikaları
- Responsible AI development uygulamalarının oluşturulması

Ensuring Code Quality and Security in AI assisted Software Engineering Eğitimi

Süre: **1 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Grup Çalışması: Responsible AI Coding Policy

- AI araçlarının kullanımına yönelik kurumsal standartlar oluşturma
- Tool selection ve approval süreçleri
- Code attribution ve IP protection
- Quality ve security gates
- Developer training ve competency gereksinimleri
- Incident response ve audit süreçleri

Sektörel Senaryo Çalışmaları

- Finansal hizmetler
- Sağlık
- Kamu
- Perakende
- Sektöre özgü regulatory ve compliance gereksinimlerini belirleme
- Üretkenlik ile risk yönetimi arasında denge kurma

Politika Sunumu ve Değerlendirme

- Ekiplerin oluşturduğu politikaları sunması ve değerlendirmesi
- İyi uygulamaları ortak bir yapıda birleştirme
- Implementation roadmap ve success metrics belirleme

Kapanış

- AI-generated code'un eleştirel değerlendirilmesine ilişkin temel noktaların pekiştirilmesi
- Kazanımların gerçek geliştirme ortamlarına uyarlanması
- AI destekli yazılım geliştirme yolculuğundaki sonraki adımların belirlenmesi