AI Security Laboratory Hands-On + Full-Stack Eğitimi

Süre: **2 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Yapay zeka sistemlerine yönelik saldırı yöntemlerini, savunma yaklaşımlarını ve güvenlik operasyonlarında AI kullanımını uygulamalı olarak öğrenin.

AI Security Laboratory Hands-On + Full-Stack, modern yapay zeka sistemlerinin ortaya çıkardığı yeni güvenlik risklerini hem saldırgan hem de geliştirici perspektifinden ele alan, iki günlük yoğun ve uygulamalı bir eğitim programıdır.

Eğitimde katılımcılar, AI ve Large Language Model tabanlı uygulamalara yönelik saldırıları analiz ederken aynı zamanda güvenli AI sistemlerinin nasıl geliştirilebileceğini ve yapay zekanın günlük security operations süreçlerinde nasıl kullanılabileceğini öğrenir.

Programın offensive security bölümünde **prompt injection, LLM jailbreaking ve LLM application fuzzing** gibi güncel saldırı teknikleri ele alınır. Katılımcılar AI sistemlerinin geleneksel uygulamalardan farklı saldırı yüzeylerini keşfeder ve non-deterministic model davranışlarının security testing süreçlerini nasıl değiştirdiğini inceler.

Eğitimin savunma ve engineering tarafında ise local LLM'ler, private AI mimarileri, data anonymization süreçleri, LLM Guard gibi open-source güvenlik araçları ve AI attack detection yaklaşımları üzerinde çalışılır.

Program ilerledikçe katılımcılar agentic AI sistemleri oluşturarak gerçek zamanlı güvenlik operasyonları ve automated threat hunting senaryoları geliştirir. Ayrıca AI'ın vulnerability research, CVE analizi ve proof-of-concept geliştirme süreçlerinde nasıl kullanılabileceği incelenir.

Eğitim, uygulamalı laboratuvar çalışmalarının yanı sıra yeniden kullanılabilir Python script'leri ve eğitim sonrasında da kullanılabilecek lifetime lab access içerir.

Eğitim Süresi ve Yaklaşımı

Bu eğitim **iki günlük hands-on ve full-stack bir security laboratory** formatında yürütülür.

Katılımcılar yalnızca teorik bilgi edinmekle kalmaz; saldırı, savunma, otomasyon ve AI development senaryolarını doğrudan laboratuvar ortamında uygular.

Kurumlara Sağladığı Katkılar

AI sistemlerinin production ortamlarında yaygınlaşmasıyla birlikte kurumlar klasik application security kontrollerinin ötesinde yeni risklerle karşılaşmaktadır.

Bu eğitim, teknik ekiplerin:

- AI-specific attack surface'leri daha iyi anlamasına,
- Prompt injection ve jailbreaking gibi yeni saldırıları analiz etmesine,
- AI security guardrail ve defence mekanizmaları geliştirmesine,
- Hassas verileri AI workflow'larında daha kontrollü kullanmasına,
- AI'ı SOC ve security engineering operasyonlarında otomasyon amacıyla kullanmasına,
- AI sistemlerini production ortamına daha güvenli şekilde entegre etmesine

yardımcı olur.

Katılımcılara Sağladığı Kazanımlar

AI Security Laboratory Hands-On + Full-Stack Eğitimi

Süre: **2 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Eğitim sonunda katılımcılar AI security alanını yalnızca teorik bir perspektiften değil, saldırıdan savunmaya ve uygulama geliştirmeden security operations'a kadar full-stack bir yaklaşımla değerlendirebilir.

Katılımcılar:

- LLM tabanlı uygulamalara yönelik saldırıları test edebilir.
- AI-specific vulnerability türlerini daha iyi tanımlayabilir.
- Local ve cloud LLM tabanlı security workflow'ları oluşturabilir.
- AI savunma katmanları ve guardrail'ler uygulayabilir.
- Güvenlik görevleri için yeniden kullanılabilir Python otomasyonları geliştirebilir.
- AI destekli vulnerability research gerçekleştirebilir.
- Agentic AI sistemlerini security operations senaryolarına uyarlayabilir.
- Eğitim sonrasında lifetime lab access üzerinden uygulamalarını geliştirmeye devam edebilir.

Önkoşullar

Katılımcıların application security konusunda genel bir anlayışa ve web teknolojileri ile API'ler hakkında temel deneyime sahip olması önerilir.

Ayrıca aşağıdaki bilgiler faydalıdır:

- Temel programming veya scripting deneyimi,
- Security testing süreçlerine aşinalık,
- Command-line kullanımı konusunda temel yetkinlik.

Tüm laboratuvar aktivitelerine katılabilmek için bir **OpenAI API key** gereklidir.

AI teknolojilerinin hızlı gelişen yapısı nedeniyle eğitim öncesinde ihtiyaç duyulması halinde ek teknik gereksinimler paylaşılabilir.

AI Security Laboratory Hands-On + Full-Stack Eğitimi

Süre: **2 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Kimler Katılmalı

Eğitim, AI teknolojilerinin güvenlik boyutunu uygulamalı olarak öğrenmek isteyen farklı security ve development profillerine yöneliktir.

Özellikle:

- **Penetration tester ve offensive security uzmanları:** Prompt injection, non-deterministic application fuzzing ve LLM jailbreaking gibi yeni AI exploitation tekniklerini öğrenmek isteyenler,
- **Security engineer ve security architect'ler:** Open-source AI defence framework'leri, data anonymization flow'ları ve LLM Guard gibi guardrail çözümlerini uygulamak isteyenler,
- **SOC analyst ve incident responder'lar:** Real-time security operations ve automated threat hunting için agentic AI sistemleri geliştirmek isteyenler,
- **AI ve software developer'lar:** OpenAI gibi cloud tabanlı veya private LLM API'lerini production sistemlere entegre ederken AI-specific vulnerability'leri azaltmak isteyenler,
- **Security practitioner'lar:** Advanced prompting, AI-powered shell ve özel Python automation script'leriyle günlük operasyonlarını otomatikleştirmek isteyenler

için uygundur.

Neler Öğreneceksiniz

Eğitim sonunda katılımcılar aşağıdaki konularda uygulamalı deneyim kazanır:

- Direct ve indirect prompt injection,
- LLM jailbreaking,
- LLM application fuzzing,
- AI-powered shell kullanımı,
- Advanced prompting,
- Local LLM ve private AI mimarileri,
- AI programming,
- AI attack detection,
- OpenAI modelleri ve API kullanımı,
- Embeddings,
- Quantization,
- LLM Guard,
- Agentic AI geliştirme,
- Kendi prediction model'ini oluşturma,
- AI destekli CVE research ve PoC geliştirme,
- Daha gelişmiş AI sistemlerinin diğer AI sistemlerini değerlendirmesi,
- Specialized AI security tools kullanımı.

Eğitim İçeriği

AI ve LLM Saldırı Vektörleri

Modern LLM uygulamalarında ortaya çıkan başlıca saldırı yüzeylerini inceleyin.

AI Security Laboratory Hands-On + Full-Stack Eğitimi

Süre: **2 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Direct ve indirect prompt injection yöntemlerini, LLM jailbreaking tekniklerini ve AI uygulamalarının instruction hierarchy veya context yapılarının saldırılar tarafından nasıl hedeflenebileceğini öğrenin.

Security Practitioner'lar için AI Programming

AI tabanlı security workflow'ları geliştirmek için temel programlama yaklaşımlarını uygulayın.

Local LLM ve private AI sistemleriyle çalışın, OpenAI gibi cloud model API'lerini kullanın ve security use case'lerine uygun AI workflow'ları oluşturun.

Tamamen private AI setup'larının nasıl kurgulanabileceğini inceleyin.

AI Attack Detection ve Savunma

AI uygulamalarına yönelik saldırıları tespit etmek için kullanılabilecek yöntemleri keşfedin.

Local LLM'lerden faydalanın, hassas verilerin cloud LLM sağlayıcılarına gönderilmeden önce anonymize edilmesini sağlayan akışlar oluşturun ve **LLM Guard** gibi open-source defence çözümlerini kullanın.

LLM Uygulamalarını Fuzzing ile Test Etme

LLM uygulamalarında fuzzing yaklaşımının geleneksel application fuzzing'den neden farklı olduğunu öğrenin.

Modern LLM'lerin non-deterministic davranışlarını dikkate alarak AI uygulamalarında güvenlik testi için uygun fuzzing yaklaşımları geliştirin.

Günlük Güvenlik Operasyonlarında AI Kullanımı

AI'ı security practitioner'ların günlük görevlerine dahil edin.

AI-powered shell, advanced prompting ve özel AI security tool'ları kullanarak analiz, otomasyon ve operasyon süreçlerini hızlandırın.

Hazır ve Yeniden Kullanılabilir Python Script'leri

Günlük güvenlik çalışmalarında kullanılabilecek hazır Python script'leri üzerinde çalışın.

Bu script'leri farklı security task'lerine uyarlayarak tekrar kullanılabilir AI automation building block'ları oluşturun.

Daha Akıllı AI ile Diğer AI Sistemlerini Değerlendirme

Bir AI sisteminin başka bir AI sistemini analiz etmek veya değerlendirmek için nasıl kullanılabileceğini keşfedin.

Security practitioner'ların yararlanabileceği daha ileri AI tekniklerini ve deneysel projeleri inceleyin.

AI ile CVE Araştırması ve PoC Geliştirme

AI'ın vulnerability research süreçlerini nasıl destekleyebileceğini öğrenin.

AI Security Laboratory Hands-On + Full-Stack Eğitimi

Süre: **2 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

CVE araştırmalarında AI'dan yararlanma, teknik bilgileri analiz etme ve proof-of-concept geliştirme süreçlerinin hızlandırılması üzerine çalışın.

Real-Time Security Operations için Agentic AI

Gerçek zamanlı güvenlik operasyonlarında görev alabilecek agentic AI sistemleri oluşturun.

Olayları analiz eden, farklı tool'ları kullanabilen ve önceden tanımlanmış güvenlik workflow'larını uygulayabilen AI agent yapıları geliştirin.