Cybersecurity Series

AI Secure Programming for Web Applications / Technical Overview (TTAI2835)

Boost Web Application Security! Leverage AI to Mitigate OWASP Vulnerabilities, Anticipate Breaches, Debug Applications & More

- **Course: AI Secure Programming for Web Applications / Technical Overview (TTAI2835)**
- **Duration:** 2 days
- **Audience:** This is an **intermediate level lecture / demo style** course ideally suited for software developers, IT professionals, and cybersecurity enthusiasts who are keen to enhance their understanding of AI in web application security.
- **Format / Engaging Seminar:** This course is a seminar / workshop style event that combines engaging instructor-led presentations with use case exploration and engaging group activities. Labs are not machine based. Hands-on can be added upon request, tailored to your tools and topics of choice.
- **Flexible Delivery Options**: This course can be delivered for your team or organization **online-live (virtual)**, **onsite in-person, self-paced** or across our immersive **blended learning experience platform (LXP).**
- **Public Schedule**: This course is currently available on our Public Open Enrollment Schedule.
- **Customizable**: We're flexible! This course agenda, topics, labs, hours and delivery modalities can be adjusted to target your specific training skills objectives, tools and learning goals. Please ask for details.

Overview

AI Secure Programming for Web Applications / Technical Overview is a one-day, technical primer geared for developers and tech-enthusiasts eager to explore AI's potential to boost security in their web development projects. The value of applying AI to web security is vast. By leveraging AI techniques, you can devise proactive defenses, anticipate potential security breaches, and ensure a more robust digital framework. The skills acquired will allow you to build secure AI-driven web applications that are less prone to breaches and hacks—an asset to any organization. You can apply your newfound knowledge to a wide array of projects, from designing resilient web applications to improving the security of existing digital infrastructures.

The course begins with an introduction to AI and secure coding, offering a solid foundation to build upon. It then delves into the OWASP Top Ten 2021, giving you insight into the most critical security risks for web applications and how AI can mitigate them. The subsequent sections focus on secure AI programming and web application integration, empowering you to combine AI models with web applications seamlessly. You'll also explore deploying and debugging AI applications and understand how to troubleshoot real-world challenges. Lastly, you'll delve into the fascinating domain of Natural Language Processing (NLP) and its implications for AI security, gaining a unique skill set that combines linguistic knowledge with technical acumen.

By the end of this course, you'll be equipped with the knowledge to apply AI to enhance web application security in your projects. You'll have a solid understanding of secure AI programming, how to deploy and debug AI applications, and how to leverage NLP to identify vulnerabilities in web applications. This course not only empowers you with an important skill set but also contributes to shaping a more secure, AI-enhanced digital landscape.

Learning Objectives

Throughout the course you'll learn to:

- Master the basics of artificial intelligence and secure coding: Get familiar with the foundational aspects of AI and the significance of secure coding, setting a strong base to build your knowledge on.
- Understand the OWASP Top Ten 2021: Dive into the major web application security risks and explore how AI can play a significant role in their mitigation.
- Grasp the concept of secure AI programming: Learn about the key principles of secure AI programming and how to implement them effectively in your projects.
- Get hands-on with web application integration: Acquire the know-how to integrate AI models seamlessly with web applications, taking your programming skills to the next level.
- Get the hang of deploying and debugging AI applications: Familiarize yourself with the process of deploying AI applications

and learn how to troubleshoot common issues that might pop up.
- Explore the fascinating world of Natural Language Processing: Delve into the intersection of language and AI, understanding how NLP can be used to identify vulnerabilities in web applications.

Audience

This introductory level course is geared for tech enthusiasts, software developers, web application developers, and AI aspirants seeking to harness the power of AI to enhance web security. It's also ideal for IT professionals responsible for web security in their organizations who are eager to innovate with AI-driven solutions. Roles might include Web Application Developers, Software Engineers, Information Security Analysts, AI/Machine Learning Enthusiasts, IT Managers focused on Web Security, Data Scientists interested in Web Security or others

Pre-Requisites

This is not a hands-on course, however its helpful if you have:
- Basic Understanding of Web Applications
- Basic understanding of programming concepts
- Basic cybersecurity concepts

Take Before:
- TT8120 Securing Web Applications Overview | OWASP Top Ten and Beyond (2 days)

NOTE: This course is lecture / demo based, but labs can be added upon request for private courses. For a hands-on edition of the course, attendee pre-requisites would realign depending on the tools selected and audience. Please inquire for details.

Related Courses
The following is a small subset of our related courses. Please see our full catalog for a complete list.
- TT8120 Securing Web Applications Overview | OWASP Top Ten and Beyond (2 days)
- TT8150 OWASP Top Ten Deep Dive (2 days)
- TTAI2810 Mastering Machine Learning Operations (MLOps) and AI Security Boot Camp (3 days)
- TTAI2820 Mastering AI Security Boot Camp (3 days)
- TTAI2832 AI Security: Applying AI to the OWASP Top Ten (2 days)
- TTAI2835 AI Secure Programming for Web Applications / Technical Overview (1 day)

Course Topics / Agenda

Please note that topics, agenda and labs are subject to change, and may adjust during live delivery based on audience skill level, interests and participation.

1. **Introduction to AI and Secure Coding**
- Understand the basics of AI and the importance of secure coding
- Understanding AI: An overview
- Secure Coding in AI
- Intro to machine learning
- Demo: Demonstrate a basic AI model

2. **Understanding OWASP Top Ten 2021 and AI Implications**
- Understand the OWASP Top Ten 2021 and how AI can mitigate risks
- Brief overview of the OWASP Top Ten 2021
- Discussing security risks in AI applications
- Demo: Show how AI can be used to identify potential security threats using

3. **Secure AI Programming and Web Application Integration**
- Understand the concept of secure AI programming and web application integration
- Security in AI: An Overview
- Secure data handling in AI
- Connecting AI models with Web applications
- Demo: Demonstrate connecting an AI model to a web application

4. **Deploying and Debugging AI Applications**
- Understand how to deploy and debug AI applications
- The fundamentals of AI application deployment
- Troubleshooting common issues in AI applications

- Demo: Demonstrate deploying a simple AI model

5. **Natural Language Processing and AI Security**
- Understand the basics of Natural Language Processing (NLP) and AI security
- Overview of NLP in AI
- AI in identifying vulnerabilities in web applications
- Demo: Showcase text processing and analysis

Setup Made Simple! Learning Experience Platform (LXP)

All applicable course software, digital courseware files or course notes, labs, data sets and solutions, live coaching support channels and rich extended learning and post training resources are provided for you in our "easy access, no install required" online **Learning Experience Platform (LXP),** remote lab and content environment. Access periods vary by course. We'll collaborate with you to ensure your team is set up and ready to go well in advance of the class. Please inquire about set up details and options for your specific course of interest.

For More Information

For more information about our training services (instructor-led, self-paced or blended), collaborative coaching services, robust Learning Experience Platform (LXP), Career Experiences, public course schedule, partner programs, courseware licensing options or to see our complete list of course offerings, solutions and special offers, please visit us at **www.triveratech.com**, email **Info@triveratech.com** or call us toll free at **844-475-4559.** Our pricing and services are always satisfaction guaranteed.