

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

**Price:** 995

**Duration:**

**Delivery Methods:** Virtual

## Overview

### Overview

**AI Secure Programming for Web Applications / Technical Overview** is built for security professionals, technical leaders, developers, and stakeholders who need a strong starting point to understand how AI is reshaping risks in modern web applications. As AI-powered features like chatbots, language models, and generative content become more common across systems, they bring new vulnerabilities that many teams are not yet prepared to address. This course helps you get up to speed with the key concepts, attack types, coding considerations, and design decisions that impact web security when AI is involved.

Through expert instruction, real-world demos, and focused discussion, you will explore how threats like prompt injection, model manipulation, and unsafe output can emerge in real applications, and what it looks like to mitigate them effectively. The course covers essential secure programming patterns for AI-enabled features, practical guidance for working with APIs and AI-generated content, and team-ready advice for managing risk from tools like ChatGPT or Copilot. This is a valuable first step for anyone looking to take on AI-related security more confidently, whether leading development projects, evaluating vendor tools, or beginning to build internal policies and protections. You will leave with a clearer understanding of where to start, what to look for, and how to support safer adoption of AI in your web environment.

### Objectives

This course is designed to help you build a strong foundation in understanding how AI impacts web application security, so you can recognize risks, support safer integration efforts, and guide next steps for your team or organization.

By the end of this course, you will be able to:

- **Explain the core risks AI introduces to web applications**, including how models behave differently than traditional code and why that matters for security.
- **Identify common attack methods used against AI-powered systems**, such as prompt injection, model manipulation, and unsafe AI-generated output.
- **Understand where AI shows up in modern web apps**, and begin recognizing how features like chatbots, AI-based search, and LLMs affect system behavior and risk.
- **Describe practical guardrails and coding patterns** that help reduce the risk of using or connecting AI in a web application, even if you are not writing code directly.
- **Know what to look for when evaluating AI tools and services**, and how to ask the right questions about privacy, input handling, and model behavior.
- **Use OWASP AI and LLM guidance as a starting point** to frame risk areas, support internal conversations, and align your organization with emerging AI security standards.

## Audience

This overview-level course is intended for security professionals, technical leads, developers, and decision-makers who are involved in web application planning, review, or protection and are new to AI-related tools and risks. It is ideal for roles such as security analysts, DevSecOps team members, web developers, application security leads, and IT managers who want to understand how to evaluate and support secure AI adoption in modern web environments. Attendees do not need to be programmers. Concepts are explained in both technical and non-coding terms.

## Pre-Reqs

This is not a hands-on course, however its helpful if you have:

- Basic understanding of how web applications are structured and delivered
- Familiarity with common application security concerns, such as input validation and API access
- Comfort reviewing technical diagrams, workflows, or simple code examples from a security perspective

## Course Schedule

Date	Time	Price	Options
06/26/2026	09:00 AM - 05:00 PM CT	995.00	<a href="#">Buy Now</a> <a href="#">Enroll</a>
09/25/2026	09:00 AM - 05:00 PM CT	995.00	<a href="#">Buy Now</a> <a href="#">Enroll</a>

## Why Professionals Choose TOPTALENT?

### Dedicated Texas-Based Support

Get assistance every step of the way from our **Texas-based team**, ensuring your training experience is hassle-free and aligned with your goals.

### 3000+ Curated Professional Courses

Access an extensive portfolio of over 3000 courses across IT, Business Application and Leadership – Designed to meet evolving Industry demands

### 95% Client Approval Rating

Trusted by professionals nationwide our 95% approval rating reflects consistent quality, measurable impact and exceptional service.

### Certified Industry Instructor

Learn from professionally certified experts with real world experience and a proven commitment to learner success.

For questions

call:

[\(469\) 721-6100](tel:(469)721-6100)

Email:

[info@toptalentlearning.com](mailto:info@toptalentlearning.com)

[Find More Training](#)

## **FAQ**

### **What if I have to reschedule my class due to conflict?**

Ten (10) business days' notice is required to reschedule a class with no additional fees. Notify TOPTALENT LEARNING as soon as possible at 469-721-6100 or by written notification to [info@toptalentlearning.com](mailto:info@toptalentlearning.com) to avoid rescheduling penalties.

### **How do I enroll for this class?**

Please contact our team at 469-721-6100; we will gladly guide you through the online purchasing process.

### **What happens once I purchase a class?**

You will receive a receipt and an enrollment confirmation sent to the email you submitted at purchase. Your enrollment email will have instructions on how to access the class. Any additional questions our team is here to support you. Please call us at 469-721-6100.

### **What is your late policy?**

If a student is 15 minutes late, they risk losing their seat to a standby student. If a student is 30 minutes late or more, they will need to reschedule. A no-show fee will apply. Retakes are enrolled on a stand-by basis. The student must supply previously issued courseware. Additional fees may apply.

### **What happens when I finish my class?**

You will receive a 'Certificate of Completion' once you complete the class. If you purchased an exam voucher for the class, a team member from TOPTALENT LEARNING will reach out to discuss your readiness for the voucher and make arrangements to send it.