Over 35 Years Of Technology Training

Document Generated: 12/16/2025

Learning Style: Virtual Classroom

Technology:

Difficulty: Beginner

Course Duration: 1 Day

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

About This Course:

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.

Course Objectives:

- 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.

Prerequisites:

- 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 Outline:

1: Foundations of AI and Secure Coding for Web Applications

- The evolving AI threat landscape: Risks and opportunities
- Why AI awareness matters for secure coding and enterprise security
- Core AI concepts: Machine learning, deep learning, LLMs, and generative AI
- Common ways AI intersects with software development and security
- Demo: How AI models can be embedded in modern applications

2: Secure Coding Principles in the Age of AI

- AI-specific coding vulnerabilities
- Threats introduced by integrating AI/ML into apps
- Key differences between traditional secure coding and AI/ML secure development
- Case study: Attack scenarios involving poor secure coding in AI models
- OWASP guidance
- Secure vs. insecure AI-infused code

3: How AI Attacks Your Code, Systems, and Teams

- Real-world AI-driven attack techniques: prompt injection, data poisoning, evasion
- AI-generated code: new risks and review challenges
- Model manipulation and AI backdoors
- Common AI-related vulnerabilities in web apps and APIs
- Human-in-the-loop risks: trust, overreliance, and social engineering
- Demo: Adversarial Attacks on AI

4: Defending Against AI-Powered Attacks

- Building an enterprise AI defense strategy
- Threat modeling with AI/ML in mind
- Establishing governance, model monitoring, and audit trails
- How to assess and verify AI components in your stack
- Best practices for mitigating model poisoning, backdoors, and misuse
- Tools and frameworks for secure AI development
- Securing the software supply chain for AI-integrated apps
- Policies to reduce exposure to AI-generated vulnerabilities
- Reviewing code with AI threat awareness

5: Secure AI Integration in Web Applications

- Integrating AI responsibly into production web systems
- Validating input/output of models and preventing injection
- Secure API design for AI services
- Handling user data securely in AI workflows
- Demo: Using a Python AI Model from a Web Application

6: Natural Language Processing (NLP) and AI Security Risks

- NLP systems and their security challenges (e.g., prompt injection, data leakage)
- How attackers use NLP to trick AI-powered systems
- Using NLP for vulnerability detection and monitoring
- Review prompt injection and mitigation techniques

7: AI Risk Management and Security Leadership

- Governance frameworks for AI (NIST AI RMF, ISO/IEC standards)

- Managing AI risk across the SDLC
- Setting up enterprise-wide guardrails for secure AI use
- Secure AI deployment checklists
- Evaluating tools like GitHub Copilot, ChatGPT, and internal LLMs
- Guiding development teams in secure AI usage

8: Staying Safe with AI Tools at Work

- Where AI tools are commonly used across roles and departments
- Safe data sharing practices for employees using AI (what's OK vs. what's risky)
- How to create and share clear internal guidelines and review processes
- Role of security leaders in managing workplace AI usage and reducing shadow AI

AI Playbook / Addendum