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

Understand how AI impacts web app security and learn practical ways to spot risks, guide safe use, and reduce exposure.

Duration: 1 Day
Skill Level: Introductory
Available Format: Instructor-Led Online; Instructor-Led, Onsite In Person ; On Public Schedule

Learn how AI is changing the way web applications are built, secured, and attacked in this practical, expert-led session designed for security professionals and technical team members who are new to AI tools and risks. Through engaging lectures, live demonstrations, and real-world examples, you will explore how threats like prompt injection, model manipulation, and unsafe output can affect your systems, and what you can do to reduce exposure. Whether you work in application security, DevSecOps, or lead technical planning, this course gives you the clarity, patterns, and guidance you need to start making smarter decisions around AI in your web stack - no coding required.

What You'll Learn

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.

If your team requires different topics, additional skills or a custom approach, our team will collaborate with you to adjust the course to focus on your specific learning objectives and goals.

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-Requisites

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

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.

TTAI2810	Mastering Machine Learning Operations (MLOps) and AI Security Boot Camp

Agenda

Please note that this list of topics is based on our standard course offering, evolved from current industry uses and trends. We will work with you to tune this course and level of coverage to target the skills you need most. Course agenda, topics and labs are subject to adjust during live delivery in response to student skill level, interests and participation.

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

Related Courses

TT8120	Web Application Security Essentials
TT8320-J	Java Secure Coding Camp | Attacking and Securing Java Web Applications
TT8320-N	.Net Secure Coding Camp | Attacking and Securing C# / ASP.Net Core Web Applications
TTAI2800	AI Security Deep Dive

Setup Made Simple! All of our AI for Business course software, digital course 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, single source, no install required online Learning Experience Platform (LXP), remote lab and content environment. Or we can provide a local installation (trial edition) to setup and use on your machine. Access periods and versions vary by course. Please inquire about set up details and options for your specific course of interest. Regardless of setup option, we will collaborate with you to ensure your team is set up and ready to go well in advance of the class.

Ways to Learn: At Trivera, we believe that Experience is Everything. Our customizable, hands-on courses are delivered live online, onsite, or in a blended format for maximum flexibility. We provide real-time expert-led training and coaching for all skill levels, from small groups to enterprise-wide programs, ensuring every learner gains the latest, most relevant job-ready skills they can apply with confidence. This course is also available for individuals or small groups on our extensive Public Schedule (see current dates below). We look forward to helping you take the next steps in your modern web developer learning journey.

For More Information

Please contact us or call 844-475-4559 toll free for more information about our training services (instructor-led, self-paced or blended), coaching and mentoring services, public course enrollment or questions, partner programs, courseware licensing options and more.