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

Duration: **1 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Understand how AI impacts web application security, identify emerging AI-related threats, and learn practical strategies for safer AI adoption in modern web environments.

The **AI & Web Application Security: A Practical Guide to Risks & Responses** course is designed for professionals who need a strong foundation in understanding how artificial intelligence is reshaping security risks in modern web applications.

As organizations increasingly adopt **chatbots**, **LLMs**, **generative AI tools**, and AI-powered automation systems, new categories of vulnerabilities and attack surfaces are emerging. This course helps teams understand these risks and develop practical approaches for secure AI integration.

Throughout the training, participants explore critical topics including:

- **Prompt injection**
- **Model manipulation**
- **Unsafe AI-generated output**
- **AI-powered cyber attacks**
- **Secure coding for AI systems**
- **AI API security**
- **OWASP AI and LLM security guidance**
- Enterprise AI governance and risk management

Through expert instruction, real-world demos, and technical discussions, attendees gain practical insights into how AI-related threats impact modern web applications and how organizations can reduce exposure through secure development practices and governance frameworks.

This course is an ideal starting point for organizations seeking to improve **AI security awareness**, support secure AI adoption, and strengthen protection strategies for AI-enabled web applications.

Prerequisites

Although this is not a hands-on lab course, participants should ideally have:

- Basic understanding of web application architecture
- Familiarity with input validation and API security
- Awareness of common application security concerns
- Comfort reviewing technical diagrams and workflows

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

Duration: **1 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Who Should Attend

This course is ideal for:

- **Security professionals**
- **Technical leads**
- **Web developers**
- **DevSecOps teams**
- **Application security specialists**
- **IT managers**
- **Security analysts**
- Decision-makers involved in AI security initiatives

This program is especially valuable for teams working with**AI-powered web applications**, **LLM security**, **AI governance**, and **secure AI adoption strategies**.

What You Will Learn

Participants will learn how to:

- Understand AI-related security risks in web applications
- Identify **prompt injection** and **model manipulation** attacks
- Evaluate vulnerabilities in AI-powered systems
- Apply **secure AI coding principles**
- Improve AI API security
- Use OWASP AI and LLM guidance effectively
- Build secure AI deployment strategies
- Develop AI risk management processes
- Create enterprise AI security policies and governance frameworks

Training Outline

1. Foundations of AI and Secure Coding for Web Applications

- The evolving AI threat landscape
- Why AI awareness matters
- Machine Learning and Deep Learning basics
- LLMs and Generative AI concepts
- AI in software development workflows
- Demo: AI integration in modern applications

2. Secure Coding Principles in the Age of AI

- AI-specific vulnerabilities
- Risks introduced by AI/ML integration
- Traditional secure coding vs AI secure development
- Insecure AI coding examples

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

- OWASP AI guidance
- Secure vs insecure AI-infused code

3. AI-Powered Attacks and Threats

- **Prompt injection attacks**
- **Data poisoning**
- **Model manipulation**
- AI backdoors
- Risks of AI-generated code
- Social engineering with AI
- Demo: Adversarial AI attacks

4. Defending Against AI-Powered Attacks

- Enterprise AI defense strategies
- AI threat modeling
- Governance and audit processes
- AI model monitoring
- Verifying AI components
- Mitigating model poisoning
- Secure AI frameworks
- Securing the software supply chain

5. Secure AI Integration in Web Applications

- Integrating AI into production systems
- Input/output validation
- Preventing injection attacks
- Secure API design
- Protecting user data in AI workflows
- Demo: Python AI model integration

6. NLP and AI Security Risks

- NLP security challenges
- Data leakage risks
- NLP-based attacks
- Vulnerability detection
- Prompt injection mitigation strategies

7. AI Risk Management and Security Leadership

- **NIST AI RMF**
- ISO/IEC AI standards
- AI governance frameworks
- Enterprise AI guardrails
- Secure AI deployment checklists
- Evaluating tools like GitHub Copilot and ChatGPT
- Guiding development teams securely

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

8. Safe Use of AI Tools in the Workplace

- AI tool usage across departments
- Safe data-sharing practices
- Building internal AI policies
- Reducing shadow AI risks
- Leadership strategies for AI security