Certified OWASP Security Fundamentals Training

Duration: **1 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Overview

This course aims to teach learners about the OWASP top 10 in bite size modules; we will look at the OWASP top 10 vulnerabilities and mitigations available to any development environment. Learners will be able to challenge for the Certified OWASP Security Fundamentals Exam, post course. It is important to understand that this is the baseline set of security standards. Remembering that this knowledge can be reused across technology stacks.

The course introduces AI security threats, OWASP LLMs, and OWASP for agentic systems, models, data, and prompts.

Prerequisites

There are no prerequisites for this course.

Note: This course does not cover hands-on coding. Additional courses, such as Secure by Design, can be found in our Secure Engineering pathway.

What You Will Learn

- Explain the purpose of the OWASP Top 10
- Explain how these vulnerabilities could be exploited
- Outline potential impact and consequences of web-based attacks
- Describe baseline mitigation steps and techniques to prevent common web and application-based attacks
- Recognise causes and impacts of major web application risks
- Learn from case studies of real-world vulnerabilities
- Recommend preventive and detective security controls
- Apply secure configuration and cloud audit practices
- Understand SBOMs and software supply chain risk
- Identify risks in AI-generated code and AI systems
- Recognise vulnerabilities in LLM’s, MCP, and agentic AI applications
- Identify ways to protect AI models, data, prompts, and infrastructure