Certified C# and Web application security Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

This training equips developers with the knowledge and hands-on experience to**secure C# and ASP.NET web applications**.
It focuses on **OWASP Top 10**, **.NET security features**, and **industry standards (SEI CERT, Saltzer & Schroeder)**.

Key topics include:

- SQL Injection
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Authentication and Session Management
- Cryptography and Secure Framework APIs

Participants engage in hands-on labs to identify, exploit, and remediate vulnerabilities in real-world scenarios.

Regulatory Compliance (BDDK)

Fully aligned with the
Regulation on Banks' Information Systems and Electronic Banking Services (Articles 20, 22, 23, 25).

This ensures the course meets **secure software development and testing obligations** required for banks and financial institutions.

Who Should Attend

C# developers, software engineers, and IT professionals
responsible for **developing or maintaining secure .NET web applications**, especially in **regulated industries**.

Certified C# and Web application security Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

By the end of this training, you will have gained knowledge and skills in the following areas:

- Identify and fix OWASP Top 10 vulnerabilities in .NET applications.
- Apply secure C# coding techniques to mitigate injection, XSS, and deserialization flaws.
- Implement secure authentication, session, and access control.
- Utilize .NET cryptographic APIs for encryption and key management.
- Perform security testing with OWASP ZAP, SQLMap, and Burp Suite.
- Apply SEI CERT and secure coding standards.

Graduates will be able to:

- Build **secure ASP.NET applications** following OWASP and SEI CERT standards.
- Conduct code-level vulnerability testing.
- Ensure **BDDK-compliant secure software development practices**.

Outline

Day 1: Introduction to IT security and secure coding

- Fundamentals of IT security and risk management.
- Understanding security flaws and their exploitation in cybercrime.
- Overview of OWASP Top Ten vulnerabilities and secure coding principles.
- Injections:
  - SQL Injection: Attack methods, blind SQL injection, and prevention using parameterized queries.
  - Command Injection: Detection, prevention techniques, and hands-on exercises.
  - XML Injection: Addressing and mitigating injection risks.
- Cross-Site Scripting (XSS): Persistent, reflected, and DOM-based XSS attacks with prevention strategies and exercises.

Day 2: Advanced web vulnerabilities and secure coding

- Authentication and Session Management:
  - Best practices for secure authentication.
  - Common vulnerabilities in session handling, including cookies and JWT tokens.
  - Exercises on securing authentication and sessions.

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Business Logic Vulnerabilities:
- Identifying and preventing issues like privilege escalation and payment manipulation.
- Practical exercises on mitigating business logic flaws.
- Securing forms and session tokens against CSRF attacks.
- Prevention techniques with ASP.NET.
- Addressing path traversal and insecure file upload vulnerabilities.
- Exercises on secure coding practices.
- Understanding and mitigating race conditions in multi-threaded environments.
- Cross-Site Request Forgery (CSRF):
- File and Path Vulnerabilities:
- Race Conditions:

Day 3: .NET security and advanced topics

- .NET Security Architecture:
  - Core security features, including role-based access control and secure error handling.
  - Serialization and deserialization vulnerabilities and their mitigation.
- Practical Cryptography:
- Symmetric and asymmetric encryption techniques.
- Cryptographic APIs in .NET and best practices for key management.
- In-depth analysis of new vulnerabilities such as insecure deserialization and cookie injection.
- Tools and techniques for static code analysis, penetration testing, and vulnerability management.
- Exercises using tools like OWASP ZAP and SQLMap.
- Applying robust programming principles from Saltzer and Schroeder.
- Recommended resources and further reading for secure coding practices.
- Emerging Threats:
- Security Testing and Vulnerability Management:
- Principles of Secure Coding:

Exams and Assessments

- Multiple-choice exam (60 questions, 50% pass mark).
- The APMG Proctor-U exam is taken online after course completion.
- Delegates receive individual access to the APMG candidate portal (available two weeks post-exam).