AMBIENT-IT

+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 01/07/2024

Sign up

OWASP security training with ASP.NET

2 days (14 hours)

Presentation

Advanced training on Web application security in C# .NET Core 8 & ASP.NET MVC. Based on practical case studies, this course will show you the best practices to adopt in order to avoid most recent security flaws, with the famous OWASP 2021 TOP 10 as a guideline.

Learn about security best practices and software vulnerabilities. Secure your SaaS solution and ASP.NET Web applications. Instill a culture of security awareness in your engineering teams, so that they become autonomous in the right reflexes and best practices to implement.

Focus on OWASP principles (TOP 10 security flaws), such as: Cross-site Scripting (XSS), Injection flaws, Broken Auth&Acess, CSRF, API provider, Data Encoding, Signature & Encryption...

The aim is to be able to prevent potential vulnerabilities and correct them using the right methodology. Don't wait until it's too late to make your team aware of the best prevention techniques!

In this state-of-the-art application security training course, you'll of course be using the latest technologies: Visual Studio 2022 17, Core 8, C# 13.

Objectives

- Knowing and understanding the most common Web vulnerabilities
- Understanding .NET security mechanisms
- Learn how to develop secure applications
- Authenticate and authorize access to ASP.NET applications
- Encrypting data with the .NET Framework

Target audience

- Developers
- Architects
- Safety auditors

Prerequisites

- Knowledge of C# and .NET programming
- Test My Knowledge

Software requirements

Visual Studio Code installed with these extensions :

- ASP .NET
- Cross-platform .NET Core development
- .NET profiling tools
- IntelliCode
- Text Template Transformation
- Developer Analytics tools
- .NET Compilet Platform SDK

Further information

- We also offer training on the latest Core version of .NET on ASP.NET

OWASP .NET Security training program

The main security vulnerabilities

- Presentation of the biggest breaches and their respective costs (Aadhar, Cambridge Analytica, Exactis, Marriott Starwood...).
- OWASP Top 10 security vulnerabilities in 2021
- Exploiting vulnerabilities
- Notion and calculation of Risk Factor
- Visualizing user impact
- Implementing security mechanisms
- New for 2022: security risks in your supply chain, a major failure issue

Case studies

- SQL injection
- Broken Authentication
- Hashing & Salting
- Sensitive data exposure
- Security Misconfiguration
- Xml External Entities (XXE)
- Broken Access Control
- Cross Site Scripting (XSS)
- Insecure deserialization
- Insufficient Logging & Monitoring
- Using Components with Known Vulnerabilities
- CORS (Cross-origin resource sharing)
- CSRF (Cross Site Request Forgery)
  - SameSite Cookie
  - Unvalidated redirect

Everyday safety

- Presentation of analysis tools
- Create your own Roslyn analysis
  - Linq: query the syntax tree
  - Code Analyzer 101
  - Diagnostic Analyzer Class
  - Analysis Context Event
- Puma
- Supply chain vulnerabilities: Integrating security into the DevOps tool chain
- Safety culture

Certificates

- Why use server certificates and how they work
- Interest, operation and implementation of customer certificates
- Why pinning certificates is important, how it works and how to use it

Encryption

- Overview of different encryption types and algorithms
  - Symmetrical
  - Asymmetrical: HMAC, JWT, AES, PBKDF2, BASE64
  - Digital signature
  - TLS, SSL
  - Pinning
- Implementation in .NET

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.