

SOFTWARE SECURED

SS - 203

# Writing Secure .NET Code

---

Developer Training  
Course Outline



# Writing Secure .NET Code

## 2 DAY COURSE

*"My entire development had taken software security training from Software Secured. The training provided very practical guidance on how to write secured software catered in the programming language we requested.*

*We had already made some changes based on what we learned."*

*- Tongfeng Zhang, CIRA*

## COURSE SUMMARY

This technical course focuses on **OWASP Top 10 – 2021** edition. It covers a wide range of application security topics in applications built with the .NET Framework. During this hands-on course, students will examine actual code, tools, and other resources that help them understand how hackers think, the techniques they use to attack their applications and the best countermeasures they can use to mitigate the risk of those attacks.

## TARGET AUDIENCE

- .NET Software Developers
- Technical Leads
- Software Architects

## REQUIREMENTS & PREREQUISITES

- Understanding of the web as well as the HTTP protocol.
- Understanding of web development technologies such as HTML, CSS, JavaScript, SQL, etc
- Understanding of basic principles of the .NET framework
- Students are required to bring their own laptops with a minimum of 8 GB RAM installed.
- Microsoft Remote Desktop Installed

# COURSE CONTENTS

- **Introduction**
- **A1. Attacking & Securing Access Control (OWASP Top 10)**
  - Vertical Access Control Issues
  - Horizontal Access Control Issues
  - Resource-based Access Control Issues
  - Introduction to .NET Authorization framework
- **A2. Attacking and Remediating Cryptographic Failures (OWASP Top 10)**
  - Security of data in transit
  - Security of data at rest
  - Best use of Encryption, Hashing and Encoding
  - Introduction to the .NET Cryptography Model
- **A3. Attacking & Securing Data Storages (OWASP Top 10)**
  - Attacking and mitigating SQL Injection
  - Attacking and mitigating Cross-site Scripting
  - Core .NET mitigations against injection attacks
- **A4. Insecure Design (OWASP Top 10)**
  - Attacking insecure design patterns
  - Integrating security throughout the development lifecycle
  - Leveraging .NET Core as a secure design pattern
- **A5. Security Misconfiguration (OWASP Top 10)**
  - Most common application misconfiguration issues.
  - Most common platforms misconfiguration issues.
  - Most common HTTP headers misconfiguration issues.
- **A6. Vulnerable and Outdated Components (OWASP Top 10)**
  - The risk of using outdated components
  - Creating a plan to mitigate the risk of 3rd party components

## COURSE CONTENTS

- **A7. Identification and Authentication Failures (OWASP Top 10)**
  - An overview of authentication-based failure and their mitigation techniques
  - How to implement multi-factor authentication properly
  - Single-sign-on issues and mitigation techniques.
  - Introduction to .NET Authentication framework
- **A8. Software and Data Integrity Failures**
  - An overview of attacks resulting from the lack of software and data integrity
  - Case Study: SolarWinds attack
  - Insecure deserialization attacks and mitigations.
- **A9. Security Logging and Monitoring Failures**
  - Most common logging failures
  - An overview for creating a solid logging framework
- **A10. Server-Side Request Forgery (SSRF) (OWASP Top 10)**
  - An overview of SSRF attacks and consequences
  - Mitigation strategies to avoid SSRF issues
- **Conclusion and closeout remarks**

## INTERESTED?

BOOK A TRAINING

VISIT US ONLINE

[www.softwaresecured.com](http://www.softwaresecured.com)

1-800-611-5741

[info@softwaresecured.com](mailto:info@softwaresecured.com)

301 Moodie Dr. Unit 108, Ottawa, ON, K2H 9C4