

Secure Web Applications | OWASP 2021 Top Ten 2021, Web Services, Rich Interfaces & More

Duration: 2 Day(s)

Course Overview

Securing Web Applications: A Technical Overview gives you a practical and eye-opening look at what really makes modern applications vulnerable. Whether you are on a security team, leading development efforts, or managing risk for web-based systems, this course will help you think more clearly about what threats actually look like in today's environment and how to recognize and respond to them with confidence. You will explore how bugs show up in working systems, what makes them dangerous, and how to plan effective defenses without needing to write code.

Through expert-led lectures and live demonstrations, you will work through realistic scenarios that show how common application flaws go unnoticed. You will examine where security breaks down in areas like user input handling, broken access rules, insecure design, and cryptographic errors. From authentication failures to outdated components and misconfigured systems, you will see how attackers find their way in and what it takes to stop them. This course walks through each category in the OWASP Top Ten using clear examples and connects them to patterns you can watch for in your own organization.

The course emphasizes technical understanding, strong evaluation habits, and better decision-making across teams. You will gain a deeper awareness of how poor security practices appear in web environments and how to identify bugs before they become problems. Whether you are reviewing architecture, leading planning meetings, or supporting a security function, this course gives you clear strategies, reference points, and practical takeaways that you can apply immediately to strengthen your organization's web security posture.

Review this course online at <https://www.alta3.com/courses/TT8120>

Objectives

- Understand key web application security risks and how to evaluate systems.
- Recognize and respond to OWASP Top Ten vulnerabilities effectively.
- Apply secure practices in evaluating authentication, encryption, and logging.
- Develop strong technical habits for secure web app planning and review.

Who Should Attend

- Security analysts
- DevSecOps team members
- Web developers
- Project leads
- Application stakeholders

Prerequisites

Although this course is not hands-on, it is helpful if you have the following incoming skills:

Recommended Prerequisites:

```
Basic knowledge of how web applications are
structured and delivered
Familiarity with general application security
goals and threats
Interest in learning how bugs are introduced,
found, and removed across a system
```

NOTE: If your class is hands-on, the demos can be done as labs designed to give light, hands-on exposure to core secure coding practices. While we're using ASP.NET as the base language for the examples, no prior experience with ASP.NET is needed—just follow along. The focus is on learning key web application security skills, not on mastering the language itself. TT4154 Introduction to TypeScript: Clean Code and Strong Skills for Web Developers TT8700 Securing Databases: Practical Database Security Skills for Safer Systems

Course Outline

Bug Hunting Foundation

1. Why Hunt Bugs?
2. Safe and Appropriate Bug Hunting/Hacking

Exploring the OWASP Top Ten & Removing Bugs

3. OWASP Top Ten Deep Dive (latest edition)
4. Removing Bugs

Bug Stomping 101: What Makes Applications Break: The Essentials

5. Unvalidated Data
6. Validation Analysis
7. Broken Access Control
8. Cryptographic Failures
9. Injection
10. Insecure Design
11. Security Misconfiguration

Bug Stomping 102: Advanced Vulnerabilities and Harder-to-See Threats

- 12. Identification and Authentication Failures
- 13. Vulnerable and Outdated Components
- 14. Software and Data Integrity Failures
- 15. Security Logging and Monitoring Failures
- 16. Server-Side Request Forgeries (SSRF)

Best Practices & What's Next

- 17. Quick Review of Best Practices
- 18. AI and Web Application Security Bonus: Web App Security Playbook Tip Guides, Cheat Sheets and other helpful resources