Web Application Security Essentials: Understanding OWASP Risks and Fixes That Really Work - TT8120

Get practical insight into modern web app threats and what it takes to plan, review, and secure applications effectively.

Duration: 2 Days
Skill Level: Introductory
Available Format: Instructor-Led Online; Instructor-Led, Onsite In Person ; Blended; On Public Schedule

Learn how to recognize what makes real web applications vulnerable and what to do about it, even if you are not writing code. This course walks you through the most common security flaws found in working systems using live demos, simple explanations, and real-world examples you can actually relate to. You will explore patterns from the OWASP Top Ten, see how bugs like broken access control, injection, and misconfigurations show up, and understand how to reduce risk in your own environment. Whether you are part of a security team, a development group, or leading projects that rely on web technologies, this is a clear and useful place to start.

What You'll Learn

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 From authentication failures to outdated components and misconfigured systems, you will see how attackers find their way in and what it takes to stop them.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.

Objectives

This course is designed to help you understand and address key web application security risks, so you can better evaluate your systems, contribute to safer practices, and guide your team in avoiding costly mistakes.

By the end of this course, you will be able to:

- Identify common reasons teams overlook security flaws in web applications
- Explain why security tools and policies are not always enough to prevent risk
- Recognize the structure and purpose of the OWASP Top Ten vulnerabilities
- Understand how unvalidated data and broken access control open systems to attack
- Evaluate real-world demonstrations of input validation, injection, and misconfiguration issues
- Apply secure thinking when reviewing authentication, encryption, and logging practices
- Spot vulnerable and outdated components and explain the risks they introduce
- Build stronger habits and technical practices for secure web application planning and review

If your team requires different topics, additional skills or a custom approach, our team will collaborate with you to adjust the course to focus on your specific learning objectives and goals.

Audience

This **technical overview** course is intended for security analysts, DevSecOps team members, web developers, project leads, and application stakeholders who are involved in web application planning, architecture, review, or oversight. It is particularly useful for team members who do not specialize in secure coding but need to understand the risks that exist in real applications and how to mitigate them. No hands-on coding is required, but a comfort level with web system design, workflows, and technical discussion is recommended.

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.

Pre-Requisites

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.

TT8700	Securing Databases: Practical Database Security Skills for Safer Systems
TT4154	Introduction to TypeScript: Clean Code and Strong Skills for Web Developers

Agenda

Please note that this list of topics is based on our standard course offering, evolved from typical industry uses and trends. We'll work with you to tune this course and level of coverage to target the skills you need most. Topics, agenda and labs are subject to change, and may adjust during live delivery based on audience skill level, interests and participation.

1. Bug Hunting Foundation

Start with a clear understanding of what bug hunting is, why it matters, and how to approach it responsibly in real-world environments.

- Why Hunt Bugs?
- Safe and Appropriate Bug Hunting/Hacking

2. Exploring the OWASP Top Ten & Removing Bugs

Learn how to spot and respond to the most common and dangerous web application risks using the OWASP Top Ten as your guide.

- OWASP Top Ten Deep Dive (latest edition)
- Removing Bugs

3. Bug Stomping 101: What Makes Applications Break: The Essentials

Explore the most frequent application-level flaws and how to recognize unsafe patterns that lead to real vulnerabilities.

- Unvalidated Data
- Validation Analysis
- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design
- Security Misconfiguration

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

Dig deeper into system-wide risks like authentication failures, outdated components, and logging gaps that attackers love to exploit.

- Identification and Authentication Failures
- Vulnerable and Outdated Components

- Software and Data Integrity Failures
- Security Logging and Monitoring Failures
- Server-Side Request Forgeries (SSRF)

5. Best Practices & What's Next

Wrap up with practical, team-ready strategies you can use right away to improve security awareness and reduce risk in your web environment.

- Quick Review of Best Practices
- AI and Web Application Security

Bonus: Web App Security Playbook

- Tip Guides, Cheat Sheets and other helpful resources

Follow On Courses

TT8320-J	Java Secure Coding Camp | Attacking and Securing Java Web Applications
TT8320-N	.Net Secure Coding Camp | Attacking and Securing C# / ASP.Net Core Web Applications
TTAI2820	Mastering AI Security Boot Camp
TTAI2832	Applying AI to the 2021 OWASP Top Ten

Related Courses

TT8320-J	Java Secure Coding Camp | Attacking and Securing Java Web Applications
TT8700	Securing Databases: Practical Database Security Skills for Safer Systems
TT8800	Information Assurance (STIG) Overview
TTAI2810	Mastering Machine Learning Operations (MLOps) and AI Security Boot Camp
TTAI2820	Mastering AI Security Boot Camp
TTAI2832	Applying AI to the 2021 OWASP Top Ten
TTAI2835	AI & Web Application Security: A Practical Guide to Risks & Responses
TTPS4894	Python Security | Introduction to Python Programming for Security Analysts & Professionals

TT4154	Introduction to TypeScript: Clean Code and Strong Skills for Web Developers
TT8120	Web Application Security Essentials: Understanding OWASP Risks and Fixes That Really Work
TT8320-N	.Net Secure Coding Camp | Attacking and Securing C# / ASP.Net Core Web Applications
TT8160	QuickStart to PCI Compliance for Developers
TT8161	PCI Compliance Refresher for Developers
TT8810	STIG Series | Application Security and Development (STIG)

Setup Made Simple! All of our AI for Business course software, digital course files or course notes, labs, data sets and solutions, live coaching support channels and rich extended learning and post training resources are provided for you in our easy access, single source, no install required online Learning Experience Platform (LXP), remote lab and content environment. Or we can provide a local installation (trial edition) to setup and use on your machine. Access periods and versions vary by course. Please inquire about set up details and options for your specific course of interest. Regardless of setup option, we will collaborate with you to ensure your team is set up and ready to go well in advance of the class.

Ways to Learn: At Trivera, we believe that Experience is Everything. Our customizable, hands-on courses are delivered live online, onsite, or in a blended format for maximum flexibility. We provide real-time expert-led training and coaching for all skill levels, from small groups to enterprise-wide programs, ensuring every learner gains the latest, most relevant job-ready skills they can apply with confidence. This course is also available for individuals or small groups on our extensive Public Schedule (see current dates below). We look forward to helping you take the next steps in your modern web developer learning journey.

For More Information

Please contact us or call 844-475-4559 toll free for more information about our training services (instructor-led, self-paced or blended), coaching and mentoring services, public course enrollment or questions, partner programs, courseware licensing options and more.