Document Generated: 12/11/2025

Learning Style: Virtual Classroom

Technology:

Difficulty: Beginner

Course Duration: 2 Days

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

About This Course:

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 From authentication failures to outdated components and misconfigured systems, you will see how attackers find their way in and what it takes to stop them.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

Course Objectives:

- 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- Spot vulnerable and outdated components and explain the risks they introduce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

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.

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

Course Outline:

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