Securing Web Applications | 2021 OWASP Top Ten and Beyond (Language Neutral)

Code: TT8120
Length: 2 days
URL: View Online

Security experts agree that the least effective approach to security is "penetrate and patch". It is far more effective to "bake" security into an application throughout its lifecycle. After spending significant time examining a poorly designed (from a security perspective) web application, developers are ready to learn how to build secure web applications starting at project inception. The final portion of this course builds on the previously learned mechanics for building defenses by exploring how design and analysis can be used to build stronger applications from the beginning of the software lifecycle.

Securing Web Applications is a seminar style course designed for web developers and technical stakeholders who need to produce secure web applications. They will thoroughly examine best practices for defensively coding web applications, covering all the 2021 OWASP Top Ten as well as several additional prominent vulnerabilities (such as file uploads and handling untrusted free-form text). Our web app security expert will share how to integrate security measures into the development process. You will also explore core concepts and challenges in web application security showcasing real world examples that illustrate the potential consequences of not following these best practices.

This course is also PCI Compliant.

Skills Gained

- Understand the concepts and terminology behind defensive, secure coding including the phases and goals of a typical exploit
- Establish the first axiom in security analysis of ALL web applications for this course and beyond
- Establish the first axiom in addressing ALL security concerns for this course and beyond
- Ensure that any hacking and bug hunting is performed in a safe and appropriate manner
- Identify defect/bug reporting mechanisms within their organizations
- Avoid common mistakes that are made in bug hunting and vulnerability testing
- Develop an appreciation for the need and value of a multilayered defense in depth
- Understand potential sources for untrusted data
- Understand the consequences for not properly handling untrusted data such as denial of service, cross-site scripting, and injections
- Understand the vulnerabilities of associated with authentication and authorization
- Detect, attack, and implement defenses for authentication and authorization functionality and services
- Understand the dangers and mechanisms behind Cross-Site Scripting (XSS) and Injection attacks
- Detect, attack, and implement defenses against XSS and Injection attacks
- Understand the risks associated with XML processing, software uploads, and deserialization and how to best eliminate or mitigate those risks

- Learn the strengths, limitations, and use for tools such as code scanners, dynamic scanners, and web application firewalls (WAFs)
- Understand techniques and measures that can used to harden web and application servers as well as other components in your infrastructure
- Identify resources to use for ongoing threat intelligence
- Plan next steps after completion of this training

Who Can Benefit

This is an overview-level , lecture and demonstration style course, designed to provide technical application project stakeholders with a first-look or baseline understanding of how to develop well defended web applications.

Prerequisites

Real-world programming experience is highly recommended for code reviews, but not required.

Course Details

Session: Bug Hunting Foundation

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

Session: Moving Forward From Hunting Bugs

- Lesson: Removing Bugs

Session: Foundation for Securing Web Applications

- Lesson: Principles of Information Security

Session: Bug Stomping 101

- Lesson: Unvalidated Data
- Lesson: A01: Broken Access Control
- Lesson: A02: Cryptographic Failures
- Lesson: A03: Injection
- Lesson: A04: Insecure Design
- Lesson: A05: Security Misconfiguration

Session: Bug Stomping 102

- Lesson: A06: Vulnerable and Outdated Components
- Lesson: A07: Identification and Authentication Failures
- Lesson: A08: Software and Data Integrity Failures
- Lesson: A09: Security Logging and Monitoring Failures
- Lesson: A10: Server-Side Request Forgery (SSRF)

Session: Moving Forward

- Lesson: Applications: What Next?
- Lesson: SDL Overview
- Lesson: SDL in Action

Schedule (as of 3)

Date	Location	
May 13, 2024 – May 14, 2024	Virtual	Enroll
Jul 8, 2024 – Jul 9, 2024	Virtual	Enroll
Sep 3, 2024 – Sep 4, 2024	Virtual	Enroll
Oct 28, 2024 – Oct 29, 2024	Virtual	Enroll
Dec 16, 2024 – Dec 17, 2024	Virtual	Enroll
