Practical Secure-Code Review

Secure-Code Review Practical Bug-Hunting (SCR-301) 2 Days

Overview

The Practical Secure Code Review training course is designed to teach developers and security professionals a repeatable process for reviewing source code for security flaws. It addresses multiple common challenges in modern secure code review, including quickly distilling an application, pull request, or feature into functional and security aspects. Students will be able to build personal secure code review techniques by gleaning from our past adventures in performing hundreds of code reviews and the lessons we've learned along the way. We will share a proven methodology to perform security analysis of any source code repository and identify security flaws, no matter the size of the code base, or the framework, or the language.

Requirements

Laptop with wireless and virtual machine (VMWare/Virtual Box) capabilities.

Attendees should be familiar with the development process (SDLC) and where security code reviews fit into the process. Attendees must have experience using an IDE, running command-line tools, and be able to read application source code. Attendee must have knowledge of the OWASP Top 10 and other common vulnerabilities.

Approach

Redpoint Security uses years of development experience to tailor training courses to developers. Each course features custom-developed intentionally vulnerable applications used to demonstrate the exploitation and mitigation of vulnerabilities. This course takes a hands-on approach and requires students to interact with the vulnerable applications to better understand the topics.

Outline

Day 1 - Theory

- Overview
- Code Review Methodology
    - Overview
        - Application Overview & Risk Assessment
    - Information Gathering
        - Info Gathering Activities
        - Mapping
        - Authorization Functions
        - Authorization Review Checklist
    - Authentication
        - Authentication Review

  - Authentication Review Vulnerabilities
  - Authentication Review Checklist
  - Authentication Exercise
- Auditing
    - Auditing Review
    - Auditing Review Vulnerabilities
    - Auditing Review Checklist
    - Auditing Review Exercise
- Injection
    - Injection Review
    - Injection Review Vulnerabilities
    - Injection Review Checklist
    - Injection Review Exercise
- Cryptographic Analysis
    - Cryptographic Analysis Review
    - Cryptographic Analysis Vulnerabilities
    - Cryptographic Analysis Checklist
    - Cryptographic Analysis Exercise
- Configuration Review
    - Configuration Review
    - Configuration Review Vulnerabilities
    - Configuration Review Checklist
- Reporting and Retesting

Day 2: Workshop

- Establishment of employee groups
- Kickoff Secure Code Review activities for Client Applications
- Ad-hoc Questions, Answers, and Effort Presentations
- Question/Answer Period
- Presentation of Results