ABSOLUTE AppSec

Practical Secure-Code Review

Ready to take your bug hunting to a deeper level? Ever been tasked with reviewing source code for SQL Injection, XSS, Access Control and other security flaws? Does the idea of reviewing code leave you with heartburn? This course introduces the proven Absolute AppSec methodology and framework for performing a secure code review, as well as addressing common challenges in modern secure code review. Short circuit your development of a custom secure code review process by gleaning from Seth & Ken's 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 suss out security flaws, no matter the size of the code base, or the framework, or the language.

DEFCON Las Vegas, August 14-15

 Ken Johnson	Ken Johnson, has been hacking web applications professionally for 12 years and given security training for 9 of those years. Ken is both a breaker and builder and currently works on the GitHub application security team. Previously, Ken has spoken at RSA, You Sh0t the Sheriff, Insomnihack, CERN, DerbyCon, AppSec USA, AppSec DC, AppSec California, DevOpsDays DC, LASCON, RubyNation, and numerous Ruby, OWASP, and AWS events about appsec, devops security, and AWS security. Ken's current projects are WeirdAAL, OWASP Railsgoat, and the Absolute AppSec podcast with Seth Law.
 Seth Law	Seth Law is an experienced Application Security Professional with over 15 years of experience in the computer security industry. During this time, Seth has worked within multiple disciplines in the security field, from software development to network protection, both as a manager and individual contributor. Seth has honed his application security skills using offensive and defensive techniques, including tool development. Seth is employed as a security consultant, hosts the Absolute AppSec podcast with Ken Johnson, and is a regular speaker at developer meetups and security events, including Blackhat, Defcon, CactusCon, and other regional conferences.

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 overcoming obstacles and quickly distilling source code of an application, pull request, or feature to understand its functional and security aspects.

Students will be able to build personal secure code review techniques by learning 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.

Course Breakdown

Day One

Introduction & Theory

Topics Covered

- **Course Overview (Day 1)**
- Code Review Methodology
  - Overview
    - Application Overview & Risk Assessment
  - Information Gathering
    - Info Gathering Activities
    - Mapping
    - Authorization Functions
    - Authorization Review Checklist
  - Authentication
    - Authentication Review, Authn Review Vulnerabilities, Authn 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
    - Configuration Review Exercise
  - Reporting and Retesting

Day Two

Methodology Demonstration & Workshopping

Demo & Workshop

- Ken's Demo of Methodology in Practice against a codebase
- Workshop
  - Establishment of employee groups
  - Kickoff Secure Code Review activities for selected application
  - Ad-hoc Questions, Answers, and Direction for Review work and Presentation
  - Question/Answer Period
  - Presentation of Results

Requirements (Prerequisites)

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