Seth & Ken's Excellent Adventures in Secure Code Review

Training Course

30th & 31st of October

Table of Contents

All training courses are two full days of intensive, hands-on learning and include complimentary morning tea, lunch and afternoon tea. Tickets can be secured by going to the website https://appsecday.io/.

Course Abstract

This course introduces security and technology professionals alike to the nitty-gritty details of performing secure code reviews.

Have you ever been asked to review code manually with the intention of finding security issues such as SQL Injection, XSS, and Access Control flaws? What about assessing the security reputation of a new framework or library? Or being asked to review a pull request from a sensitive part of the code base? This course addresses all of these common challenges in modern secure code review.

- Code Review Methodology used to cover security issues
- Practical methods for identifying OWASP Top 10 vulnerabilities in:
    - Go
    - Ruby/Rails
    - Django/Python
    - Node/Express
    - Java/Spring
    - .Net/MVC
- Open source code review tools available for different languages
- Hands-on experience identifying vulnerabilities in known-vulnerable code bases.

We have concentrated on taking our past adventures in code review, the lessons we've learned along the way, and made them applicable for others who perform code reviews. We will share our methodology to perform analysis of any source code and suss out security flaws, no matter the size of the code base, or the framework, or the language.

You as a student will learn the methodology, techniques, approach, and tools used by Seth Law and Ken Johnson to understand code flows, trace user input, identify vulnerabilities, and effectively secure an application code base.

What attendees will learn?

Students will take away knowledge and experience in approaching numerous code languages and frameworks to complete a security source code review. In addition, the

learned methodology can be customized by the attendee to fit into any organization's security SDLC. Finally, the attendee will have the tools to review source code for any web, mobile, or modern application, whether or not the targeted language is specifically covered during the course.

What attendees will be provided?

- Presentation materials.
- Source code to be analyzed during the course (VM provided, if desired).

What attendees should bring?

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

Pre-requisites

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

Detailed Outline

Day 1

- Overview
  - Introduction
  - Philosophy
  - What to Expect
  - The Circle-K Framework
  - What we're doing
  - What we're NOT doing
  - Tools/Lab Setup
- Code Review Methodology
  - Intro to Methodology
  - Application Overview & Risk Assessment
    - Napolean Exercise
    - Napolean Exercise Post-Mortem
  - Information Gathering
    - Mapping
      - Rufus Exercise
      - Rufus Exercise Post-Mortem
      - Authorization Functions
      - Identify in several frameworks
      - Discuss Caveats (IDOR, Framework Nuances, and more.)
      - Sigmund Exercise
      - Sigmund Exercise Post-Mortem
  - Authorization Review
    - Review how roles are enforced
    - Logic Flaws
    - Mass Assignment
    - Missing Function Level Access Control

        - Privilege Escalation
        - Genghis Khan Exercise
    - Authentication Review
        - Define/review user identity process
        - Broken Authentication
        - User Enumeration
        - Session Management Issues
        - Authentication Bypass
        - Brute-Force Attacks
        - Socrates Exercise
        - Auditing Review
    - Cover checklist
        - Insufficient logging
        - Sensitive Data Exposure
        - Debug Messages
        - Error Handling
        - Information Leakage
        - Java Example
        - Auditing Checklist Review
        - Abraham Lincoln Exercise
        - Abraham Lincoln Exercise Post Mortem
    - Injection Review
        - Cause
        - Types (SQLi, NoSQLi, XSS, XXE, SSRF)
        - Checklist
        - Where to most commonly identify
            - Examples in various frameworks
        - Billy The Kid Exercise
        - Billy The Kid Exercise Post-Mortem

Day 2

- Cryptographic Review
    - Types of Flaws
    - Locations to review
    - Checklist review
    - Beethoven Exercise
    - Beethoven Exercise Post-Mortem
- Configuration Review
    - How to identify (for a given framework)
    - Examples walk-thru
    - Dependencies
    - Insecure Defaults
    - Checklist Review
- Reporting
    - Overview
    - Relevant data points
- Final Exercise... pair with partners and use the methodology against real open source applications
- Walk-thru results with the class (every group does a short 5 minute presentation of their notes)

Trainer Biography

Ken Johnson

https://www.linkedin.com/in/ken-johnson-a180a042/

Ken Johnson has been hacking web applications professionally for 11 years and given security training for 8 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

https://www.linkedin.com/in/seth-law-b01ba618/

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 currently 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.