Hands-on DevSecOps and AppSec Automation

Training Course

15th & 16th 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 buy going to the website https://appsecday.io/.

Course Abstract

Scalable and comprehensive application security is an essential requirement for any product, especially within mature software delivery environments utilising DevOps practices and principles allowing you to move faster. However, incorporating robust and resilient application security practices within a continuous delivery pipeline can be challenging.

To compound these challenges, application security and engineering teams grapple with a host of capacity issues. From a more reactive model, where security assurance was done periodically, and in bursts, we now have to embed application security practices throughout an organization's product development life cycle. This has resulted in teams being stretched in multiple directions, and unable to cope with the ever increasing demands. While your product may be delivered to your customers faster, application security still remains difficult to integrate within your continuous delivery environment.

What attendees will learn?

This training addresses these challenges and more, and is focused towards enabling and delivering application security at scale to organizations. This is a largely hands-on program, with a plethora of anecdotes, examples and real-world case studies. This gives the participants a comprehensive view of implementing practical DevSecOps and application security automation practices within their organizations. In fact, most of the participants have reported that they were able to use learnings from this training almost immediately.

What attendees will be provided?

- Slides for the training course.
- Virtual Machine with all the required software and reference material.

What attendees should bring?

- A laptop that is capable of running a VirtualBox virtual machine.
- Must have access to copy from a USB flash drive to install the virtual machine image.
- Please download and install the latest installation of Oracle VM VirtualBox.
- On some Windows machines you will need to enable Virtualization in the BIOS options.

Pre-requisites

Basic knowledge of application security concepts and web application testing techniques preferred but not required.

Detailed Outline

Day 1

- The Problem with the old models of Application Delivery
- A Quick History of Agile and DevOps
- The Coming of DevOps
- The Need for Security in DevOps
- Security in Continuous Integration
- Security Integrations for Jenkins and other CI Tools
- Introduction to Static Application Security Testing (SAST) for Continuous Integration
    - Success Factors for SAST - Tool Focus
        - FindSecBugs
        - NodeJSScan
        - Bandit
        - Brakeman
        - MobSF (Mobile SAST)
    - Hands-on Labs - SAST Framework for CI Tools like Jenkins
    - Rolling out custom SAST Workflows – using Abstract Syntax Trees and Regular Expressions
    - Hands-on SAST - Write your own AST checks for SAST
- Dynamic Application Security Testing with Continuous Integration
- Concepts of DAST with Security Testing
    - Security Automation Testing using BurpSuite Professional, OWASP ZAP, w3af, Selenium, OpenAPI (Swagger)
    - Security Regression Tests - How to design and write them
    - Hands on Labs - Creating Parameterized Security Automation Testing Scripts for w3af, OWASP ZAP, BurpSuite Pro and Selenium
    - Hands-on Labs: Leveraging Functional Test Automation with multiple frameworks for Security Testing
        - Robot Framework
        - NighwatchJS
        - Tavern - REST API Testing
        - Puppeteer
    - Hands on labs - Integrating Custom Security Automation with Jenkins and other CI Tools
- Hands-on Automation for Security Regressions
- Application Security Automation – Deep-Dive:
    - Hands-on:
        - OWASP ZAP Deep-Dive

            - Scan Policy
            - Extensions
            - Certificate Management
        - OWASP ZAP API Deep-Dive
        - OWASP ZAP Scripting Workshop
            - Create Active Scan Scripts for Custom Application Vulnerabilities
            - Create Zest Scripts for Authentication
        - OWASP ZAP API Testing with OpenAPI Specification
- Introduction to Robot Framework:
    - Introduction to BDD and ATDD Frameworks
    - Introduction to Robot Framework and its Declarative Syntax
    - Writing Application Security Test Recipes using Robot Framework
        - Hands-on: OWASP ZAP - Robot Framework Integration
        - Creating Parameterized AppSec Automation with Robot Framework, Selenium, OWASP ZAP and BurpSuite Pro
- Identifying Insecure Software Libraries in Continuous Integration
    - Hands-on Labs: OWASP Dependency Check and Dependency Track
    - Hands-on labs: RetireJS
    - Hands-on Labs: RoboNPMAudit
- Hands-on: Using these techniques to create an "Continuous Application Security Test Pipeline”
- Introduction to Application Vulnerability Correlation
    - Key Application Security Testing Metrics
    - Visualizing Results from AppSec Testing
    - Hands-on: Correlating and Aggregating across tools with CWE
-

Day 2

- Securing Containerized Deployments:
    - Container Security Threat Model:
        - Container - Host Attacks
        - Container - Container Attacks
        - Container Sprawl
        - Container Secrets Exposure
        - Insecure Libraries and Applications in Containerized Deployments
        - Container Daemon Threats
        - Hands-on Labs: Container Threat Models (real-world examples)
        - Hands-on Labs: Privilege-Escalation on Container Deployment
    - Securing Containers:

        - Secrets Management for Containers
        - Hardening Host Machines for Dockerized Deployments
        - Application Whitelisting for Containerized Deployments
        - Hands-on Labs: Container Vulnerability Scanning - DevOps Pipeline
        - Hands-on Labs: Hardening Host for Docker deployment
        - Hands-on Labs: Profiling Containerized Applications for security
        - Hands-on Labs: AppArmor and SECCOMP Profiles for Application Whitelisting
- Agile Threat Modeling
    - Integrating Threat Models into Requirements and Design Specs
        - Abuser Stories
        - Refutation Criteria
        - Integrating Abuser Stories into the Agile SDLC
- Automating Application Security Pentesting with the “ThreatPlaybook” Framework (Application Security as Code)
    - Generating “Threat Models as Code”
        - Threat Model Process Flow Diagrams with MermaidJS and Robot Framework
        - Documenting Security Test Cases for Threat Models
- Creating Application Pentest Pipelines
    - Creating a “Threat Model to Pentest Pipeline” with the Automaton Framework:
    - Hands-on Labs: ThreatPlaybook Threat Modeling Library
    - Hands-on Labs: Automating Reconnaissance with RoboNmap, RoboSublist3r and RoboDirBuster
    - Hands-on: Parameterized Application Vulnerability Assessment with OWASP ZAP
    - Hands-on: Automated Fuzzing with the WFuzz Framework and SecLists
    - Creating Recipes for Automated Pentesting of Apps, combined with Functional Automation Scripts
    - Hands-on: Write an Automated Pentest Pipeline recipe from Threat Model to Pentest for an Intentionally Vulnerable Web Service
-

Trainer Biography

Abhay Bhargav

https://www.linkedin.com/in/abhaybhargav/

Abhay Bhargav is the CTO of we45, an Application Security focused company. Abhay is the author of two international publications. "Secure Java for Web Application Development" and "PCI Compliance: A Definitive Guide". Abhay is a builder and breaker of applications, and has authored multiple applications in Django and NodeJS.

He is the Chief Architect of Orchestron at a leading Application Vulnerability Correlation and Orchestration Framework. He is a passionate Pythonista and loves the idea of automating security. This passion prompted him to author a now world renown DevSecOps training course that has been delivered in multiple locations, recently at OWASP AppSec USA 2016, OWASP AppSec EU and USA 2017.

Abhay has also delivered a workshop on DevSecOps at DEFCON 25 and speaks regularly at industry events including OWASP, ISACA, Oracle OpenWorld, JavaOne, and others. He will also be showcasing Threat-Modeling-as-Code and AppSec Automation Framework "ThreatPlaybook" at BlackHat USA 2018 as well as delivering a workshop at DEFCON 26 (2018).