Application Security Essentials

Training Course

17th & 18th 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

The course focuses on core application security principles aimed at the engineering community such as developers, architects and quality assurance testers. The course aims to equip the attendees with platform and technology agnostic remediation strategies against application security vulnerabilities.

In addition, it will also cover web vulnerabilities within the OWASP Top 10 - 2017, taught using real world case studies, demonstrations and hands on exercises. The modules are designed to drive home the concept of building applications securely, irrespective of the technology or platform.

What attendees will learn?

Attendees will come away with an in depth understanding of not only best practices involved in securing software but also knowledge of how to identify within code and test for security vulnerabilities from an attackers perspective.

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

Knowledge of programming will help, but not required.

Detailed Outline

Day 1

Need and Importance of Web Application Security

- Introduction to Information Security - Concept Deep-Dive
- Dissecting Major Web Security Incidents
- Case Study in Web Application Security - from we45
- Success/Failure Factors - Web Application Security

Vulnerability - Attacker Perspective - Deep Dive OWASP Top 10 - 2017

- Introduction to our Workshop Vulnerable Web App
- A1-Injection
    - Introduction to SQL Injection
    - SQL Injection Deep-Dive - Techniques and Attacker Practices + Case Studies
    - XML Injection - Overview and Attacker Techniques
    - Server-Side Template Injection - Overview and Attacker Techniques
    - Injection Attacks against SOAP and REST based Web Services
- A2-Broken Authentication
    - Session Hijacking Attacks
    - Session Fixation Attack
    - Authentication Bypass Attacks
    - Attacks against Stateless Authentication Implementations - JWT
- A3-Sensitive Data Exposure
    - Security Flaws - Data at Rest
        - Security Failures in Password Protection
        - Security failures - Cryptographic Implementations
        - Case Study - Adobe Password Breach (Encryption Failure)
    - Security Flaws - Data in Transit
        - Transport Layer Security Configuration Flaws
        - SSLStrip and Downgrade Attacks - POODLE, CRIME
        - Man in the Middle with SSL Attacks
- A4 – XML External Entities (XXE)

- Real-world applications for XXE Attacks
- Specific issues with XML Parsers and weak implementations
- XXE Detailed Explanation and Deep-Dive

- A5-Broken Access Control
  - Introduction to Authorization-driven Attacks and Direct Object Reference Attacks
  - Primary Key based Insecure Direct Object Reference Attacks
  - MVC Framework based Insecure Direct Object Reference Attacks
  - Other Authorization Attacks and Attacks against Access Control
- A6-Security Misconfiguration
  - Common Security Misconfiguration Flaws in the web circa 2017
  - Comprehensive Model for Application Security Component Hardening
- A7-Cross-Site Scripting (XSS)
  - Introduction to Same Origin Policy
  - Reflected Cross Site Scripting Attacks
  - Persistent Cross Site Scripting Attacks
  - DOM-Based XSS Attacks
- A8-Insecure Deserialization
  - Serialization Flaws in the Real World – Case Studies and Detailed Explanations
  - Examples of Serialization flaws against different platforms
- A9-Using Components with Known Vulnerabilities
  - Overview of Vulnerabilities in libraries and software components
  - Techniques to identify vulnerabilities in libraries and software components
  - Exit Strategies for Identified Vulnerabilities in Software Components
- A10-Insufficient Logging and Monitoring
  - Examples of Insufficient Attack Protection
  - Introduction to Application Security Testing
    - SAST
    - DAST
    - IAST
    - RASP

        - Application Security Monitoring Best Practices
            - Logging and Log Management Failures
- Other Key Application Security Flaws:
    - Server-Side Request Forgery
    - Cross-Site Request Forgery

Day 2

Best Practices - Defender's Perspective - Deep Dive

- Authentication, Authorization and Access Control - Concept Focus
    - Web Security Authentication Best Practices - Implementation
        - Authentication Process Management for Web Apps and Web Services
        - Authentication Best Practices:
            - Password Management
            - Session Management
            - Security Configuration
    - Request Authentication Best Practices
    - Protection against CSRF Attacks - Tokens and Postback calls
    - Web Services CSRF Protections
    - Authorization Best Practices
        - Best practices in creating a permissions management system
        - Best Practices for:
            - Primary Key Entropy and Token Generation
            - Permissions Management based on Authorization Matrix
    - Framework Best Practices - Authentication and Authorization
- When Parsers Attack – Security Pitfalls and Practices to protect against vulnerabilities with Parsers:
    - SSRF and URL Parsers
    - Protection Strategies for SSRF
    - Serialization Flaws and Dangerous Libraries
    - Protection Strategies for Deserialization – across multiple formats
- Cryptography
    - Introduction to Cryptography and Cryptographic Implementations
    - Deep-Dive - Cryptography:
        - Symmetric and Asymmetric Ciphers
        - Block and Stream Ciphers
        - Modes of Encryption - Best Practices
        - Key Management Essentials

    - Cryptography - Data in Transit
        - Deep-Dive - SSL and TLS Concepts
        - SSL and TLS Security Best Practices
        - Session and TLS Security Best Practices
    - One-way hashing
        - Hashing Concept Overview
        - Hashing Best Practices
        - Hashing vs. Password Based Key Generation - Engineering Choices and Trade-offs
- Logging and Log Management - Best Practices
    - Logging Overview - Security Need
    - Enterprise Logging and Log Management Practices
    - Failures in Logging and Log Management - Case Study
    - Logging Best Practices
- Introduction to Application Security Testing
    - Types of Application Security Testing
    - SAST – Static Application Security Testing
    - DAST – Dynamic Application Security Testing
    - Hands-On Exercises
- Secure Coding Practices
    - Input Validation
        - Input Validation - Need and Overview
        - Input Validation - Deep Dive
        - Input Validation - Best Practices - By frameworks
    - Output Encoding
        - Output Encoding - Need for Output Encoding
        - Output Encoding - Frameworks and Best practices
- Secure Database Access
    - Need for Parameterized SQL Statements
    - Parameterized vs. Dynamic SQL Statements
    - ORMs and security benefits

List of Hands-On Labs for Participants

- Hands-On SQL Injection Labs - Blind, Error Based SQL Injections
- Hands-on SQL Injection Remediation labs - Dynamic vs. Parameterized Queries
- Hands-on Authentication Bypass Labs - VERB Tampering Attack
- Hands-on Session Fixation Attack Labs
- Insecure Direct Object Reference Attack Labs
- Hands-on Password Brute Force Labs
- Hands-on Misconfiguration of Database Labs
- Hands-on Password Hash Cracking Labs
- Hands-on Insecure Cryptographic Implementations - ECB Mode

- Hands on Labs - Assessing Insecure SSL/TLS Implementations
- Hands-on Labs - Scanning for Insecure Software Libraries and Components
- Hands-on Labs - Session Management and Attribute Best Practices
- Hands-on Labs - Symmetric Cipher Comparison (Modes of Encryption)
- Hands-on Labs - Input Validation - Regular Expressions
- Hands-on Labs - Output Encoding - Escape using Templating Languages
- Insecure Deserialization Hands-on Labs
- XML External Entities and Protection Strategy Labs
- OWASP ZAP – Introduction to Application Security Testing

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).