COURSE OUTLINE

Application Security Foundations Level 1

This introductory course will answer all of your burning questions and define all of the technical terms right at the start. Then we will set goals for your AppSec program at work as an exercise. After this we dive in deep into every type of application security activity and tool on the market, while sprinkling you with quizzes and exercises. As a final project we make an AppSec program action plan for you to bring back to work with you.

Introduction

- Your Trainer: Tanya Janca
- History Lesson

Definitions and Burning Questions

- What is AppSec, What is DevSecOps, and Why Do They Matter?
- What is 'Cyber'?
- What is Application Security
- Computer Science VS Application Security
- What is DevOps?
- What is a Tech Stack?
- Can You Jump Right in an Application Security Position?
- Is Application Security Just Coding?
- Biggest Application Security Challenges
- Skillset Needed for Application Security
- How can I get into AppSec?
- Quiz

AppSec Program Goals

- What are Program Goals?
- Goal: Inventory
- Goal: Finding Vulnerabilities
- Goal: The Knowledge to Fix What You Have Found
- Goal: Giving Developers Security Tools
- Goal: Education and Reference Materials
- Goal: Secure SDLC
- Goal: Incident Response
- Goal: Continuous Improvement
- Quiz

Choosing Goals

- Choosing Your Program Goals
- Setting Goals

AppSec Activities – The Basics

- Interactive Exercise
- Interactive AppSec Activities Assignment
- Tactics Versus Strategy
- VA Scans and Security Assessments
- Threat Modelling
- Secure Code Review and SAST
- Software Composition Analysis (SCA)
- Penetration Testing
- Quiz

AppSec Activities – Intermediate

- Developer Education and Advocacy Programs
- Coordinated Disclosure
- Policies, Guidelines and Standards
- Giving Developers Security Tools
- Secure Coding Library/Templates
- Security Reference Materials
- 'The Partnership Model'
- Metrics and Measurement
- Security Regression Testing (with unit tests)
- Capture the Flag and Gamification
- Reviewing New Tech
- IDE Tools
- Adding a Shield in Front of Your App (WAF/RASP)
- Quiz

AppSec Activities – DevOps Flavoured

- Adding Security Tooling to a Pipeline
- Asynchronous Pipeline
- Chaos Engineering and Red Teaming
- Security Sprints
- Turning PenTest Results into Unit Tests
- Asking Directly for Feedback From Dev & Ops
- Quiz

AppSec Activities – Advanced

- Team-Specific Customized Security Training
- Creating Custom Tools
- Bug Bounties
- Red Teaming

- Targeting an Entire Bug Class
- Security Exercises and Simulations
- Interactive AppSec Activities Assignment
- Quiz

AppSec Tooling – The Basics

- Interactive Tooling Assignment
- Introduction to AppSec Tooling
- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)
- Software Composition Analysis Tools
- Web Proxy
- Fuzzing
- VM & Container VA scanners
- Quiz

AppSec Tooling – Intermediate

- API Tools that Speak Directly to the API
- Web Application Firewall (WAF)
- Vulnerability Management
- IDE Tools and Hooks
- Tooling Made for Pipelines Unit Test Creativity
- Quiz

AppSec Tooling – Modern Twist

- Interactive Application Security Testing (IAST)
- SIEM + App Integration
- RASP Runtime App Security Protection
- Service Mesh
- API Gateway
- Application and Web Asset Inventory
- Quiz

AppSec Adjacent Tooling

- Integrated Bug Tracker for Vulnerabilities
- Cloud native.mov
- Playbooks = Workflows + Serverless Apps
- VM/Container VA Scanners – Again
- File Integrity Monitoring
- Application Control Tooling
- AppSec Tooling Exercise – What to do
- Interactive Assignment
- Quiz

Updating Your Goals

- Final Project

Resources

- Open Web Application Security Project
- WoSEC
- #CyberMentoringMonday
- Tanya Janca: @SheHacksPurple

Conclusion

- Summary
- Thank You!