APP101 - APPSEC FUNDAMENTALS

Course Learning Objectives

This course is designed for those who would like to build a solid understanding of the core concepts and essential principles at the heart of application security today. By the end of this course, you'll discover the fundamental concepts and key trends that shaped the industry as it exists today and how AppSec fits into the bigger picture of information security as a whole.

Description

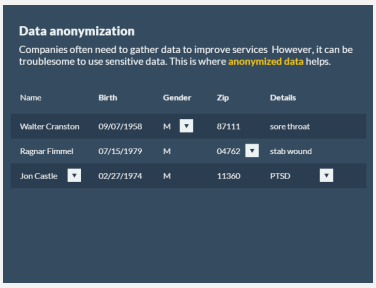
AppSec Fundamentals has been designed to provide insight into application security. Starting with key terminology and concepts, the course then provides an overview of the necessity of holistic security from the outset, the importance of protecting customer information, the requirements for managing risk at a business level, and incorporating security best practices into your software life cycle. Understanding these ideas will help you to better appreciate the challenges — and opportunities — in application security today.

Audience

General Staff

Time Required

Tailored learning - 75 minutes total



SecurityCompass
COPYRIGHT 2020

APP101 - APPSEC FUNDAMENTALS

Course Outline

1. Application security, threats, and attacks

- CIA - Confidentiality, Integrity, Availability
- Application security
- The importance of AppSec
- Terminology
- Types of applications
- Exercise: Types of applications
- Instant App
- AppSec roles and responsibilities
- Hacking: past and present
- "Trustworthy computing" memo
- Threat actors
- Types of hackers
- A common vulnerability
- Example: Buffer overflows
- AppSec education

2. Secure software

- General principles
- Holistic security
- Attacking vs defending
- Project management concerns
- Security from the start
- Usability vs security
- Secure software principles
- Core security principles
- General security principles
- Exercise: General security principles
- Design security principles

3. Data security and privacy

- The data life cycle
- About data privacy
- Data collection
- Stages of data collection
- Privacy best practices
- Data anonymization
- Data disposal
- Data security
- Storage in the cloud
- Cryptography
- Goals of cryptography
- Symmetric encryption
- Asymmetric encryption
- Crypto handshake
- Communication and network security
- Security concerns
- Securing data
- Patching applications
- Patch and vulnerability management
- Patch and vulnerability management process
- End point security

4. Governance, risk management, and compliance

- Introduction
- Organizational standards
- Internal standards
- External standards
- Regulations
- Challenges
- Risk management
- Threats, assets, and vulnerability
- Example: Threats, assets, and vulnerability
- Attack, likelihood, and impact
- Types of risks
- Due diligence and due care
- Factoring risk
- Exercise: Factoring risk
- Residual risk
- Strategies for handling risk
- Business vs. technical risks
- Compliance and auditing
- Standards, acts, and regulations

5. Secure software development, acquisition, and testing

- Identify risk
- Identify risk at all phases
- Development process
- Software development methodologies
- Waterfall
- Agile
- DevOps
- Other methodologies
- Security methodologies
- Threat modeling
- Application security services
- Penetration testing
- Types of pen tests
- Source code testing
- DAST vs SAST vs IAST
- Fuzzing
- Web Application Firewall (WAF)
- Third-party software security

SecurityCompass

COPYRIGHT 2020