

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 - 90 minutes total

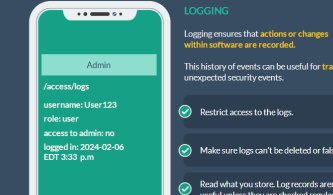
An AppSec toolkit

 Authentication user proves who they are	 Authorization what the user is allowed to do	 Encryption keep data confidential, both at rest and in transit	 Logging get visibility into what's happened in your application
---	--	--	---

Digital signatures



AppSec toolkit - Logging



LOGGING

Logging ensures that actions or changes within software are recorded. This history of events can be useful for tracking unexpected security events.

- Restrict access to the logs.
- Make sure logs can't be deleted or falsified
- Read what you store. Log records aren't useful unless they are checked regularly.

APP101 - APPSEC FUNDAMENTALS

Course Outline

1. Introducing Application Security

- What are InfoSec and AppSec?
- Threat, vulnerability, and risk
- Skydiving exercise
- CIA triad
- CIA in practice
- Threat actors
- Types of threat actors
- Attack types
- Attack types exercise

2. Secure Software Architecture

- Secure software principles
- Practicing security principles
- Application architecture
- Server-side and client-side applications
- An AppSec toolkit
- Authentication
- Authorization
- Logging
- Secure sessions
- Exception management

3. Data Security and Privacy

- Protecting data
- The data life cycle
- Data privacy
- Data collection
- Stages of data collection
- Privacy best practices
- Data disposal
- Understanding cryptography
- Cryptography
- Encryption
- Symmetric encryption
- Asymmetric encryption
- TLS handshakes
- Hashing
- Digital signatures
- Use of digital signatures
- Password hashing
- Overconfidence
- Countermeasures best practices

4. Secure Software Development

- Security as a process
- Physical security
- The secure SDLC
- Your AppSec Team
- Stages of the SDLC
- Requirements
- Design
- Development
- Testing
- Deployment
- Maintenance
- Security from the start

5. Governance, Risk Management, and Compliance

- Security posture
- GRC
- GRC improvements
- Governance
- The governance report
- Risk management
- Risk assessment
- Risk value
- Business vs. technical risks
- Residual risk
- RMM ranking system
- The risk report
- Compliance
- Compliance requirements
- Standards
- Compliance report