



Alice & Bob learn
**APPLICATION
SECURITY**

Tanya Janca
@shehackspurple

WILEY

Table of Contents

[Cover](#)

[Introduction](#)

[Pushing Left](#)

[About This Book](#)

[Out-of-Scope Topics](#)

[The Answer Key](#)

[Part I: What You Must Know to Write Code Safe
Enough to Put on the Internet](#)

[CHAPTER 1: Security Fundamentals](#)

[The Security Mandate: CIA](#)

[Assume Breach](#)

[Insider Threats](#)

[Defense in Depth](#)

[Least Privilege](#)

[Supply Chain Security](#)

[Security by Obscurity](#)

[Attack Surface Reduction](#)

[Hard Coding](#)

[Never Trust, Always Verify](#)

[Usable Security](#)

[Factors of Authentication](#)

[Exercises](#)

[CHAPTER 2: Security Requirements](#)

[Requirements](#)

[Requirements Checklist](#)

[Exercises](#)

[CHAPTER 3: Secure Design](#)

[Design Flaw vs. Security Bug](#)

[Secure Design Concepts](#)

[Segregation of Production Data](#)

[Threat Modeling](#)

[Exercises](#)

[CHAPTER 4: Secure Code](#)

[Selecting Your Framework and](#)

[Programming Language](#)

[Untrusted Data](#)

[HTTP Verbs](#)

[Identity](#)

[Session Management](#)

[Bounds Checking](#)

[Authentication \(AuthN\)](#)

[Authorization \(AuthZ\)](#)

[Error Handling, Logging, and Monitoring](#)

[Exercises](#)

[CHAPTER 5: Common Pitfalls](#)

[OWASP](#)

[Defenses and Vulnerabilities Not](#)

[Previously Covered](#)

[Race Conditions](#)

[Closing Comments](#)

[Exercises](#)

[Part II: What You Should Do to Create Very Good Code](#)

[CHAPTER 6: Testing and Deployment](#)

[Testing Your Code](#)

[Testing Your Application](#)

[Testing Your Infrastructure](#)

[Testing Your Database](#)

[Testing Your APIs and Web Services](#)

[Testing Your Integrations](#)

[Testing Your Network](#)

[Deployment](#)

[Exercises](#)

CHAPTER 7: An AppSec Program

Application Security Program Goals

Application Security Activities

Application Security Tools

CHAPTER 8: Securing Modern Applications and Systems

APIs and Microservices

Online Storage

Containers and Orchestration

Serverless

Infrastructure as Code (IaC)

Security as Code (SaC)

Platform as a Service (PaaS)

Infrastructure as a Service (IaaS)

Continuous

Integration/Delivery/Deployment

Dev(Sec)Ops

The Cloud

Cloud Workflows

Modern Tooling

Modern Tactics

Summary

Exercises

Part III: Helpful Information on How to Continue to Create Very Good Code

CHAPTER 9: Good Habits

Password Management

Multi-Factor Authentication

Incident Response

Fire Drills

Continuous Scanning

Technical Debt

Inventory

[Other Good Habits](#)

[Summary](#)

[Exercises](#)

[CHAPTER 10: Continuous Learning](#)

[What to Learn](#)

[Take Action](#)

[Exercises](#)

[Learning Plan](#)

[CHAPTER 11: Closing Thoughts](#)

[Lingering Questions](#)

[Conclusion](#)

[APPENDIX A: Resources](#)

[Introduction](#)

[Chapter 1: Security Fundamentals](#)

[Chapter 2: Security Requirements](#)

[Chapter 3: Secure Design](#)

[Chapter 4: Secure Code](#)

[Chapter 5: Common Pitfalls](#)

[Chapter 6: Testing and Deployment](#)

[Chapter 7: An AppSec Program](#)

[Chapter 8: Securing Modern Applications and Systems](#)

[Chapter 9: Good Habits](#)

[Chapter 10: Continuous Learning](#)

[APPENDIX B: Answer Key](#)

[Chapter 1: Security Fundamentals](#)

[Chapter 2: Security Requirements](#)

[Chapter 3: Secure Design](#)

[Chapter 4: Secure Code](#)

[Chapter 5: Common Pitfalls](#)

[Chapter 6: Testing and Deployment](#)

[Chapter 7: An AppSec Program](#)