Contents at a Glance

PART I Primer

1 Welcome to the Wide World of Web Application Security 3

2 Security Fundamentals 23

PART II Web Application Security Principles

3 Authentication 53

4 Authorization 91

5 Browser Security Principles: The Same-Origin Policy 149

6 Browser Security Principles: Cross-Site Scripting and Cross-Site Request Forgery 169

7 Database Security Principles 213

8 File Security Principles 253

PART III Secure Development and Deployment

9 Secure Development Methodologies 287

Epilogue The Wizard, the Giant, and the Magic Fruit Trees: A Happy Ending 319

Index 321