BRIEF CONTENTS

Foreword xix
Introduction xxi

PART I: THE INDUSTRY 1

Chapter 1: Picking a Bug Bounty Program 3

Chapter 2: Sustaining Your Success 15

PART II: GETTING STARTED 31

Chapter 3: How the Internet Works 33

Chapter 4: Environmental Setup and Traffic Interception 45

Chapter 5: Web Hacking Reconnaissance 61

PART III: WEB VULNERABILITIES 109

Chapter 6: Cross-Site Scripting 111

Chapter 7: Open Redirects 131

Chapter 8: Clickjacking 143

Chapter 9: Cross-Site Request Forgery 155

Chapter 10: Insecure Direct Object References 175

Chapter 11: SQL Injection 187

Chapter 12: Race Conditions 205

Chapter 13: Server-Side Request Forgery 213

Chapter 14: Insecure Deserialization 231

Chapter 15: XML External Entity 247

Chapter 16: Template Injection 261

Chapter 17: Application Logic Errors and Broken Access Control 275

Chapter 18: Remote Code Execution 283
Chapter 19: Same-Origin Policy Vulnerabilities 295
Chapter 20: Single-Sign-On Security Issues 307
Chapter 21: Information Disclosure 323

PART IV: EXPERT TECHNIQUES 333

Chapter 22: Conducting Code Reviews 335
Chapter 23: Hacking Android Apps. 347
Chapter 24: API Hacking 355
Chapter 25: Automatic Vulnerability Discovery Using Fuzzers 369

Index 381