Table of Contents

Preface xiii

1. The History of Software Security 1
The Origins of Hacking 1
The Enigma Machine, Circa 1930 2
Automated Enigma Code Cracking, Circa 1940 5
Introducing the "Bombe" 7
Telephone "Phreaking," Circa 1950 8
Anti-Phreaking Technology, Circa 1960 10
The Origins of Computer Hacking, Circa 1980 11
The Rise of the World Wide Web, Circa 2000 12
Hackers in the Modern Era, Circa 2015+ 15
Summary 18

Part I. Recon

2. Introduction to Web Application Reconnaissance 21
Information Gathering 21
Web Application Mapping 23
Summary 25

3. The Structure of a Modern Web Application 27
Modern Versus Legacy Web Applications 27
REST APIs 29
JavaScript Object Notation 32
JavaScript 33
Variables and Scope 34

Functions 36
Context 37
Prototypal Inheritance 38
Asynchrony 41
Browser DOM 44
SPA Frameworks 45
Authentication and Authorization Systems 46
Authentication 47
Authorization 47
Web Servers 48
Server-Side Databases 49
Client-Side Data Stores 50
Summary 51

4. Finding Subdomains. 53
Multiple Applications per Domain 53
The Browser's Built-In Network Analysis Tools 54
Taking Advantage of Public Records 57
Search Engine Caches 58
Accidental Archives 60
Social Snapshots 62
Zone Transfer Attacks 65
Brute Forcing Subdomains 67
Dictionary Attacks 72
Summary 75

5. API Analysis. 77
Endpoint Discovery 77
Authentication Mechanisms 81
Endpoint Shapes 82
Common Shapes 82
Application-Specific Shapes 83
Summary 84

6. Identifying Third-Party Dependencies. 87
Detecting Client-Side Frameworks 87
Detecting SPA Frameworks 88
Detecting JavaScript Libraries 90
Detecting CSS Libraries 91
Detecting Server-Side Frameworks 92
Header Detection 92
Default Error Messages and 404 Pages 92

Database Detection 95
Summary 96

7. Identifying Weak Points in Application Architecture. 99
Secure Versus Insecure Architecture Signals 100
Multiple Layers of Security 104
Adoption and Reinvention 105
Summary 107

8. Part I Summary. 109

Part II. Offense

9. Introduction to Hacking Web Applications. 113
The Hacker's Mindset 113
Applied Recon 114

10. Cross-Site Scripting (XSS). 117
XSS Discovery and Exploitation 118
Stored XSS 121
Reflected XSS 123
DOM-Based XSS 126
Mutation-Based XSS 128
Summary 130

11. Cross-Site Request Forgery (CSRF). 131
Query Parameter Tampering 131
Alternate GET Payloads 136
CSRF Against POST Endpoints 137
Summary 139

12. XML External Entity (XXE). 141
Direct XXE 141
Indirect XXE 145
Summary 146

13. Injection. 147
SQL Injection 147
Code Injection 151
Command Injection 155
Summary 158

14. Denial of Service (DoS)..... 161
regex DoS (ReDoS) 162
Logical DoS Vulnerabilities 164
Distributed DoS 167
Summary 169

15. Exploiting Third-Party Dependencies..... 171
Methods of Integration 173
Branches and Forks 174
Self-Hosted Application Integrations 174
Source Code Integration 175
Package Managers 176
JavaScript 176
Java 178
Other Languages 179
Common Vulnerabilities and Exposures Database 180
Summary 181

16. Part II Summary..... 183

Part III. Defense

17. Securing Modern Web Applications..... 187
Defensive Software Architecture 188
Comprehensive Code Reviews 188
Vulnerability Discovery 189
Vulnerability Analysis 190
Vulnerability Management 190
Regression Testing 191
Mitigation Strategies 191
Applied Recon and Offense Techniques 192

18. Secure Application Architecture..... 193
Analyzing Feature Requirements 193
Authentication and Authorization 195
Secure Sockets Layer and Transport Layer Security 195
Secure Credentials 197
Hashing Credentials 197
2FA 200
PII and Financial Data 201
Searching 201

Summary 203

19. Reviewing Code for Security..... 205
How to Start a Code Review 206
Archetypical Vulnerabilities Versus Custom Logic Bugs 207
Where to Start a Security Review 209
Secure-Coding Anti-Patterns 211
Blacklists 211
Boilerplate Code 212
Trust-By-Default Anti-Pattern 213
Client/Server Separation 213
Summary 214

20. Vulnerability Discovery..... 215
Security Automation 215
Static Analysis 216
Dynamic Analysis 217
Vulnerability Regression Testing 218
Responsible Disclosure Programs 221
Bug Bounty Programs 222
Third-Party Penetration Testing 223
Summary 224

21. Vulnerability Management..... 225
Reproducing Vulnerabilities 225
Ranking Vulnerability Severity 226
Common Vulnerability Scoring System 226
CVSS: Base Scoring 228
CVSS: Temporal Scoring 230
CVSS: Environmental Scoring 231
Advanced Vulnerability Scoring 232
Beyond Triage and Scoring 232
Summary 233

22. Defending Against XSS Attacks..... 235
Anti-XSS Coding Best Practices 235
Sanitizing User Input 237
DOMParser Sink 238
SVG Sink 238
Blob Sink 239
Sanitizing Hyperlinks 239
HTML Entity Encoding 240

CSS 241
Content Security Policy for XSS Prevention 242
Script Source 242
Unsafe Eval and Unsafe Inline 243
Implementing a CSP 244
Summary 245

23. Defending Against CSRF Attacks. 247
Header Verification 247
CSRF Tokens 249
Stateless CSRF Tokens 250
Anti-CRSF Coding Best Practices 250
Stateless GET Requests 251
Application-Wide CSRF Mitigation 252
Summary 253

24. Defending Against XXE. 255
Evaluating Other Data Formats 256
Advanced XXE Risks 257
Summary 257

25. Defending Against Injection. 259
Mitigating SQL Injection 259
Detecting SQL Injection 260
Prepared Statements 261
Database-Specific Defenses 263
Generic Injection Defenses 263
Potential Injection Targets 263
Principle of Least Authority 264
Whitelisting Commands 265
Summary 266

26. Defending Against DoS. 269
Protecting Against Regex DoS 270
Protecting Against Logical DoS 270
Protecting Against DDoS 271
DDoS Mitigation 272
Summary 273

27. Securing Third-Party Dependencies. 275
Evaluating Dependency Trees 275
Modeling a Dependency Tree 276

Dependency Trees in the Real World 277
Automated Evaluation 277
Secure Integration Techniques 277
Separation of Concerns 278
Secure Package Management 278
Summary 279

28. Part III Summary..... 281
The History of Software Security 281
Web Application Reconnaissance 283
Offense 284
Defense 285

29. Conclusion..... 289

Index..... 291