



# CONTENTS

|                                                   |      |
|---------------------------------------------------|------|
| Foreword .....                                    | xvii |
| Acknowledgments .....                             | xix  |
| Introduction .....                                | xxi  |
| ▼ 1 Hacking Web Apps 101 .....                    | 1    |
| What Is Web Application Hacking? .....            | 2    |
| GUI Web Hacking .....                             | 2    |
| URI Hacking .....                                 | 3    |
| Methods, Headers, and Body .....                  | 4    |
| Resources .....                                   | 6    |
| Authentication, Sessions, and Authorization ..... | 6    |
| The Web Client and HTML .....                     | 7    |
| Other Protocols .....                             | 8    |
| Why Attack Web Applications? .....                | 9    |
| Who, When, and Where? .....                       | 11   |
| Weak Spots .....                                  | 11   |
| How Are Web Apps Attacked? .....                  | 12   |
| The Web Browser .....                             | 13   |
| Browser Extensions .....                          | 14   |
| HTTP Proxies .....                                | 18   |
| Command-line Tools .....                          | 25   |
| Older Tools .....                                 | 26   |
| Summary .....                                     | 26   |
| References & Further Reading .....                | 27   |
| ▼ 2 Profiling .....                               | 31   |
| Infrastructure Profiling .....                    | 32   |
| Footprinting and Scanning: Defining Scope .....   | 32   |
| Basic Banner Grabbing .....                       | 33   |
| Advanced HTTP Fingerprinting .....                | 34   |
| Infrastructure Intermediaries .....               | 38   |

|                                                     |     |
|-----------------------------------------------------|-----|
| Application Profiling .....                         | 45  |
| Manual Inspection .....                             | 46  |
| Search Tools for Profiling .....                    | 66  |
| Automated Web Crawling .....                        | 72  |
| Common Web Application Profiles .....               | 77  |
| General Countermeasures .....                       | 82  |
| A Cautionary Note .....                             | 83  |
| Protecting Directories .....                        | 83  |
| Protecting include Files .....                      | 84  |
| Miscellaneous Tips .....                            | 84  |
| Summary .....                                       | 85  |
| References & Further Reading .....                  | 85  |
| ▼ 3 Hacking Web Platforms .....                     | 87  |
| Point-and-Click Exploitation Using Metasploit ..... | 89  |
| Manual Exploitation .....                           | 92  |
| Evading Detection .....                             | 104 |
| Web Platform Security Best Practices .....          | 107 |
| Common Best Practices .....                         | 107 |
| IIS Hardening .....                                 | 110 |
| Apache Hardening .....                              | 113 |
| PHP Best Practices .....                            | 118 |
| Summary .....                                       | 119 |
| References & Further Reading .....                  | 119 |
| ▼ 4 Attacking Web Authentication .....              | 123 |
| Web Authentication Threats .....                    | 124 |
| Username/Password Threats .....                     | 124 |
| Strong(er) Web Authentication .....                 | 144 |
| Web Authentication Services .....                   | 147 |
| Bypassing Authentication .....                      | 151 |
| Token Replay .....                                  | 151 |
| Cross-site Request Forgery .....                    | 153 |
| Identity Management .....                           | 157 |
| Client-side Piggybacking .....                      | 161 |
| Some Final Thoughts: Identity Theft .....           | 161 |
| Summary .....                                       | 162 |
| References & Further Reading .....                  | 164 |
| ▼ 5 Attacking Web Authorization .....               | 167 |
| Fingerprinting Authz .....                          | 169 |
| Crawling ACLs .....                                 | 169 |
| Identifying Access Tokens .....                     | 170 |
| Analyzing Session Tokens .....                      | 172 |

|                                                |     |
|------------------------------------------------|-----|
| Differential Analysis .....                    | 174 |
| Role Matrix .....                              | 175 |
| Attacking ACLS .....                           | 177 |
| Attacking Tokens .....                         | 178 |
| Manual Prediction .....                        | 179 |
| Automated Prediction .....                     | 187 |
| Capture/Replay .....                           | 194 |
| Session Fixation .....                         | 195 |
| Authorization Attack Case Studies .....        | 196 |
| Horizontal Privilege Escalation .....          | 196 |
| Vertical Privilege Escalation .....            | 201 |
| Differential Analysis .....                    | 204 |
| When Encryption Fails .....                    | 206 |
| Using cURL to Map Permissions .....            | 207 |
| Authorization Best Practices .....             | 210 |
| Web ACL Best Practices .....                   | 211 |
| Web Authorization/Session Token Security ..... | 214 |
| Security Logs .....                            | 216 |
| Summary .....                                  | 217 |
| References & Further Reading .....             | 218 |
| ▼ 6 Input Injection Attacks .....              | 221 |
| Expect the Unexpected .....                    | 222 |
| Where to Find Attack Vectors .....             | 224 |
| Bypass Client-Side Validation Routines .....   | 225 |
| Common Input Injection Attacks .....           | 225 |
| Buffer Overflow .....                          | 226 |
| Canonicalization (dot-dot-slash) .....         | 227 |
| HTML Injection .....                           | 233 |
| Boundary Checks .....                          | 236 |
| Manipulate Application Behavior .....          | 237 |
| SQL Injection .....                            | 238 |
| XPath Injection .....                          | 251 |
| LDAP Injection .....                           | 254 |
| Custom Parameter Injection .....               | 255 |
| Log Injection .....                            | 256 |
| Command Execution .....                        | 257 |
| Encoding Abuse .....                           | 259 |
| PHP Global Variables .....                     | 259 |
| Common Side-effects .....                      | 260 |
| Common Countermeasures .....                   | 261 |
| Summary .....                                  | 262 |
| References & Further Reading .....             | 264 |

|      |                                                 |     |
|------|-------------------------------------------------|-----|
| ▼ 7  | Attacking XML Web Services                      | 267 |
|      | What Is a Web Service?                          | 268 |
|      | Transport: SOAP over HTTP(S)                    | 269 |
|      | WSDL                                            | 273 |
|      | Directory Services: UDDI and DISCO              | 275 |
|      | Similarities to Web Application Security        | 279 |
|      | Attacking Web Services                          | 279 |
|      | Web Service Security Basics                     | 288 |
|      | Summary                                         | 291 |
|      | References & Further Reading                    | 292 |
| ▼ 8  | Attacking Web Application Management            | 295 |
|      | Remote Server Management                        | 296 |
|      | Telnet                                          | 296 |
|      | SSH                                             | 297 |
|      | Proprietary Management Ports                    | 298 |
|      | Other Administration Services                   | 299 |
|      | Web Content Management                          | 299 |
|      | FTP                                             | 299 |
|      | SSH/scp                                         | 300 |
|      | FrontPage                                       | 300 |
|      | WebDAV                                          | 302 |
|      | Misconfigurations                               | 309 |
|      | Unnecessary Web Server Extensions               | 309 |
|      | Information Leakage Misconfigurations           | 312 |
|      | State Management Misconfiguration               | 327 |
|      | Summary                                         | 332 |
|      | References & Further Reading                    | 333 |
| ▼ 9  | Hacking Web Clients                             | 335 |
|      | Exploits                                        | 336 |
|      | Web Client Implementation Vulnerabilities       | 337 |
|      | Trickery                                        | 352 |
|      | General Countermeasures                         | 358 |
|      | Low-privilege Browsing                          | 359 |
|      | Firefox Security Extensions                     | 361 |
|      | ActiveX Countermeasures                         | 361 |
|      | Server-side Countermeasures                     | 363 |
|      | Summary                                         | 364 |
|      | References & Further Reading                    | 364 |
| ▼ 10 | The Enterprise Web Application Security Program | 371 |
|      | Threat Modeling                                 | 372 |
|      | Clarify Security Objectives                     | 374 |
|      | Identify Assets                                 | 374 |

|                                                      |     |
|------------------------------------------------------|-----|
| Architecture Overview .....                          | 375 |
| Decompose the Application .....                      | 377 |
| Identify and Document Threats .....                  | 377 |
| Rank the Threats .....                               | 379 |
| Develop Threat Mitigation Strategies .....           | 380 |
| Code Review .....                                    | 382 |
| Manual Source Code Review .....                      | 382 |
| Automated Source Code Review .....                   | 387 |
| Binary Analysis .....                                | 387 |
| Security Testing of Web App Code .....               | 397 |
| Fuzzing .....                                        | 397 |
| Test Tools, Utilities, and Harnesses .....           | 399 |
| Pen-testing .....                                    | 400 |
| Security in the Web Development Process .....        | 401 |
| People .....                                         | 401 |
| Process .....                                        | 404 |
| Technology .....                                     | 406 |
| Summary .....                                        | 409 |
| References & Further Reading .....                   | 410 |
| ▼ A Web Application Security Checklist .....         | 413 |
| ▼ B Web Hacking Tools and Techniques Cribsheet ..... | 419 |
| ▼ Index .....                                        | 429 |