# Contents

- **Foreword** ........................................... .xix
- **Introduction** ........................................... .xxiii

## I Preparing the Battle Space ..................... 1

1 Application Fortification ............................. 7  
   *Recipe 1-1: Real-time Application Profiling* .......................... 7  
   *Recipe 1-2: Preventing Data Manipulation with Cryptographic Hash Tokens* ........................................... 15  
   *Recipe 1-3: Installing the OWASP ModSecurity Core Rule Set (CRS)* .......................... 19  
   *Recipe 1-4: Integrating Intrusion Detection System Signatures* ........................................... 33  
   *Recipe 1-5: Using Bayesian Attack Payload Detection* ........................................... 38  
   *Recipe 1-6: Enable Full HTTP Audit Logging* ........................................... 48  
   *Recipe 1-7: Logging Only Relevant Transactions* ........................................... 52  
   *Recipe 1-8: Ignoring Requests for Static Content* ........................................... 53  
   *Recipe 1-9: Obscuring Sensitive Data in Logs* ........................................... 54  
   *Recipe 1-10: Sending Alerts to a Central Log Host Using Syslog* ........................................... 58  
   *Recipe 1-11: Using the ModSecurity AuditConsole* ........................................... 60

2 Vulnerability Identification and Remediation ....... 67  
   *Recipe 2-1: Passive Vulnerability Identification* ........................................... 70  
   *Recipe 2-2: Active Vulnerability Identification* ........................................... 79  
   *Recipe 2-3: Manual Scan Result Conversion* ........................................... 88  
   *Recipe 2-4: Automated Scan Result Conversion* ........................................... 92  
   *Recipe 2-5: Real-time Resource Assessments and Virtual Patching* ........................................... 99

3 Poisoned Pawns (Hacker Traps) ...................... 115  
   *Recipe 3-1: Adding Honeypot Ports* ........................................... 116  
   *Recipe 3-2: Adding Fake robots.txt Disallow Entries* ........................................... 118  
   *Recipe 3-3: Adding Fake HTML Comments* ........................................... 123  
   *Recipe 3-4: Adding Fake Hidden Form Fields* ........................................... 128  
   *Recipe 3-5: Adding Fake Cookies* ........................................... 131
Asymmetric Warfare

4 Reputation and Third-Party Correlation

Recipe 4-1: Analyzing the Client’s Geographic Location Data
Recipe 4-2: Identifying Suspicious Open Proxy Usage.
Recipe 4-3: Utilizing Real-time Blacklist Lookups (RBL)
Recipe 4-4: Running Your Own RBL
Recipe 4-5: Detecting Malicious Links

5 Request Data Analysis

Recipe 5-1: Request Body Access
Recipe 5-2: Identifying Malformed Request Bodies
Recipe 5-3: Normalizing Unicode
Recipe 5-4: Identifying Use of Multiple Encodings
Recipe 5-5: Identifying Encoding Anomalies
Recipe 5-6: Detecting Request Method Anomalies
Recipe 5-7: Detecting Invalid URI Data
Recipe 5-8: Detecting Request Header Anomalies
Recipe 5-9: Detecting Additional Parameters
Recipe 5-10: Detecting Missing Parameters
Recipe 5-11: Detecting Duplicate Parameter Names
Recipe 5-12: Detecting Parameter Payload Size Anomalies
Recipe 5-13: Detecting Parameter Character Class Anomalies

6 Response Data Analysis

Recipe 6-1: Detecting Response Header Anomalies
Recipe 6-2: Detecting Response Header Information Leakages
Recipe 6-3: Response Body Access
Recipe 6-4: Detecting Page Title Changes
Recipe 6-5: Detecting Page Size Deviations
Recipe 6-6: Detecting Dynamic Content Changes
Recipe 6-7: Detecting Source Code Leakages
Recipe 6-8: Detecting Technical Data Leakages
Recipe 6-9: Detecting Abnormal Response Time Intervals
Recipe 6-10: Detecting Sensitive User Data Leakages
Recipe 6-11: Detecting Trojan, Backdoor, and Webshell Access Attempts
7 Defending Authentication ........................................ 265
   Recipe 7-1: Detecting the Submission of Common/Default Usernames .... 266
   Recipe 7-2: Detecting the Submission of Multiple Usernames .......... 269
   Recipe 7-3: Detecting Failed Authentication Attempts ................. 272
   Recipe 7-4: Detecting a High Rate of Authentication Attempts ....... 274
   Recipe 7-5: Normalizing Authentication Failure Details ............. 280
   Recipe 7-6: Enforcing Password Complexity ....................... 283
   Recipe 7-7: Correlating Usernames with SessionIDs ............... 286

8 Defending Session State ........................................ 291
   Recipe 8-1: Detecting Invalid Cookies ................................ 291
   Recipe 8-2: Detecting Cookie Tampering .............................. 297
   Recipe 8-3: Enforcing Session Timeouts ............................... 302
   Recipe 8-4: Detecting Client Source Location Changes
                During Session Lifetime ................................ 307
   Recipe 8-5: Detecting Browser Fingerprint Changes During Sessions .... 314

9 Preventing Application Attacks ................................. 323
   Recipe 9-1: Blocking Non-ASCII Characters ......................... 323
   Recipe 9-2: Preventing Path-Traversal Attacks ..................... 327
   Recipe 9-3: Preventing Forceful Browsing Attacks .................. 330
   Recipe 9-4: Preventing SQL Injection Attacks ...................... 332
   Recipe 9-5: Preventing Remote File Inclusion (RFI) Attacks ..... 336
   Recipe 9-6: Preventing OS Commanding Attacks .................... 340
   Recipe 9-7: Preventing HTTP Request Smuggling Attacks ........ 342
   Recipe 9-8: Preventing HTTP Response Splitting Attacks ......... 345
   Recipe 9-9: Preventing XML Attacks ................................. 347

10 Preventing Client Attacks .................................... 353
   Recipe 10-1: Implementing Content Security Policy (CSP) ............ 353
   Recipe 10-2: Preventing Cross-Site Scripting (XSS) Attacks ....... 362
   Recipe 10-3: Preventing Cross-Site Request Forgery (CSRF) Attacks . 371
   Recipe 10-4: Preventing UI Redressing (Clickjacking) Attacks .... 377
   Recipe 10-5: Detecting Banking Trojan (Man-in-the-Browser) Attacks . 381

11 Defending File Uploads ....................................... 387
   Recipe 11-1: Detecting Large File Sizes ............................. 387
   Recipe 11-2: Detecting a Large Number of Files .................... 389
   Recipe 11-3: Inspecting File Attachments for Malware .............. 390
Contents

12 Enforcing Access Rate and Application Flows .......... 395
   Recipe 12-1: Detecting High Application Access Rates ........ 395
   Recipe 12-2: Detecting Request/Response Delay Attacks ....... 405
   Recipe 12-3: Identifying Inter-Request Time Delay Anomalies .... 411
   Recipe 12-4: Identifying Request Flow Anomalies .......... 413
   Recipe 12-5: Identifying a Significant Increase in Resource Usage .... 414

III Tactical Response ........................................... 419

13 Passive Response Actions .............................. 421
   Recipe 13-1: Tracking Anomaly Scores ....... 421
   Recipe 13-2: Trap and Trace Audit Logging .......... 427
   Recipe 13-3: Issuing E-mail Alerts .......... 428
   Recipe 13-4: Data Sharing with Request Header Tagging .... 436

14 Active Response Actions ............................... 441
   Recipe 14-1: Using Redirection to Error Pages .......... 442
   Recipe 14-2: Dropping Connections ........ 445
   Recipe 14-3: Blocking the Client Source Address .......... 447
   Recipe 14-4: Restricting Geolocation Access Through Defense Condition (DefCon) Level Changes ........ 452
   Recipe 14-5: Forcing Transaction Delays .......... 455
   Recipe 14-6: Spoofing Successful Attacks .......... 462
   Recipe 14-7: Proxying Traffic to Honeypots .......... 468
   Recipe 14-8: Forcing an Application Logout .......... 471
   Recipe 14-9: Temporarily Locking Account Access .......... 476

15 Intrusive Response Actions ............................. 479
   Recipe 15-1: JavaScript Cookie Testing .......... 479
   Recipe 15-2: Validating Users with CAPTCHA Testing .......... 481
   Recipe 15-3: Hooking Malicious Clients with BeEF .......... 485

Index .......................................................... 495