Web Security Testing Cookbook*

Systematic Techniques to Find Problems Fast

Paco Hope and Ben Walther

O'REILLY'
Beijing • Cambridge • Farnham • Koln • Sebastopol • Tokyo

Table of Contents

Foreword xiii

Preface xv

1. Introduction 1

1.1 What Is Security Testing? 1
1.2 What Are Web Applications? 5
1.3 Web Application Fundamentals 9
1.4 Web App Security Testing 14
1.5 It's About the How 14

2. Installing Some Free Tools 17

2.1 Installing Firefox 17
2.2 Installing Firefox Extensions 18
2.3 Installing Firebug 19
2.4 Installing OWASP's WebScarab 20
2.5 Installing Perl and Packages on Windows 21
2.6 Installing Perl and Using CPAN on Linux, Unix, or OS X 22
2.7 Installing CAL9000 22
2.8 Installing the ViewState Decoder 23
2.9 Installing cURL 24
2.10 Installing Pornzilla 24
2.11 Installing Cygwin 25
2.12 Installing Nikto 2 27
2.13 Installing Burp Suite 28
2.14 Installing Apache HTTP Server 28

3. Basic Observation 31

3.1 Viewing a Page's HTML Source 32
3.2 Viewing the Source, Advanced 33
3.3 Observing Live Request Headers with Firebug 36
3.4 Observing Live Post Data with WebScarab 40

3.5 Seeing Hidden Form Fields 43
3.6 Observing Live Response Headers with TamperData 44
3.7 Highlighting JavaScript and Comments 47
3.8 Detecting JavaScript Events 48
3.9 Modifying Specific Element Attributes 49
3.10 Track Element Attributes Dynamically 51
3.11 Conclusion 53

4. **Web-Oriented Data Encoding. 55**
4.1 Recognizing Binary Data Representations 56
4.2 Working with Base 64 58
4.3 Converting Base-36 Numbers in a Web Page 60
4.4 Working with Base 36 in Perl 60
4.5 Working with URL-Encoded Data 61
4.6 Working with HTML Entity Data 63
4.7 Calculating Hashes 65
4.8 Recognizing Time Formats 67
4.9 Encoding Time Values Programmatically 68
4.10 Decoding ASP.NET's ViewState 70
4.11 Decoding Multiple Encodings 71

5. **Tampering with Input. 73**
5.1 Intercepting and Modifying POST Requests 74
5.2 Bypassing Input Limits 77
5.3 Tampering with the URL 78
5.4 Automating URL Tampering 80
5.5 Testing URL-Length Handling 81
5.6 Editing Cookies 84
5.7 Falsifying Browser Header Information 86
5.8 Uploading Files with Malicious Names 88
5.9 Uploading Large Files 91
5.10 Uploading Malicious XML Entity Files 92
5.11 Uploading Malicious XML Structure 94
5.12 Uploading Malicious ZIP Files 96
5.13 Uploading Sample Virus Files 96
5.14 Bypassing User-Interface Restrictions 98

6. **Automated Bulk Scanning. 101**
6.1 Spidering a Website with WebScarab 102
6.2 Turning Spider Results into an Inventory 104
6.3 Reducing the URLs to Test 107
6.4 Using a Spreadsheet to Pare Down the List 107
6.5 Mirroring a Website with LWP 108

6.6 Mirroring a Website with wget 110
6.7 Mirroring a Specific Inventory with wget 111
6.8 Scanning a Website with Nikto 112
6.9 Interpretting Nikto's Results 114
6.10 Scan an HTTPS Site with Nikto 115
6.11 Using Nikto with Authentication 116
6.12 Start Nikto at a Specific Starting Point 117
6.13 Using a Specific Session Cookie with Nikto 118
6.14 Testing Web Services with WSFuzzer 119
6.15 Interpreting WSFuzzer's Results 121

7. Automating Specific Tasks with cURL. 125
7.1 Fetching a Page with cURL 126
7.2 Fetching Many Variations on a URL 127
7.3 Following Redirects Automatically 128
7.4 Checking for Cross-Site Scripting with cURL 128
7.5 Checking for Directory Traversal with cURL 132
7.6 Impersonating a Specific Kind of Web Browser or Device 135
7.7 Interactively Impersonating Another Device 136
7.8 Imitating a Search Engine with cURL 139
7.9 Faking Workflow by Forging Referer Headers 140
7.10 Fetching Only the HTTP Headers 141
7.11 POSTing with cURL 142
7.12 Maintaining Session State 144
7.13 Manipulating Cookies 145
7.14 Uploading a File with cURL 146
7.15 Building a Multistage Test Case 147
7.16 Conclusion 152

8. Automating with LibWWWPerl. 153
8.1 Writing a Basic Perl Script to Fetch a Page 154
8.2 Programmatically Changing Parameters 156
8.3 Simulating Form Input with POST 157
8.4 Capturing and Storing Cookies 158
8.5 Checking Session Expiration 159
8.6 Testing Session Fixation 162
8.7 Sending Malicious Cookie Values 164
8.8 Uploading Malicious File Contents 166
8.9 Uploading Files with Malicious Names 167
8.10 Uploading Viruses to Applications 169
8.11 Parsing for a Received Value with Perl 171
8.12 Editing a Page Programmatically 172
8.13 Using Threading for Performance 175

9. Seeking Design Flaws 177
9.1 Bypassing Required Navigation 178
9.2 Attempting Privileged Operations 180
9.3 Abusing Password Recovery 181
9.4 Abusing Predictable Identifiers 183
9.5 Predicting Credentials 184
9.6 Finding Random Numbers in Your Application 186
9.7 Testing Random Numbers 188
9.8 Abusing Repeatability 190
9.9 Abusing High-Load Actions 192
9.10 Abusing Restrictive Functionality 194
9.11 Abusing Race Conditions 195

10. Attacking AJAX 197
10.1 Observing Live AJAX Requests 199
10.2 Identifying JavaScript in Applications 200
10.3 Tracing AJAX Activity Back to Its Source 201
10.4 Intercepting and Modifying AJAX Requests 202
10.5 Intercepting and Modifying Server Responses 204
10.6 Subverting AJAX with Injected Data 206
10.7 Subverting AJAX with Injected XML 208
10.8 Subverting AJAX with Injected JSON 209
10.9 Disrupting Client State 211
10.10 Checking for Cross-Domain Access 212
10.11 Reading Private Data via JSON Hijacking 213

11. Manipulating Sessions 215
11.1 Finding Session Identifiers in Cookies 216
11.2 Finding Session Identifiers in Requests 218
11.3 Finding Authorization Headers 219
11.4 Analyzing Session ID Expiration 221
11.5 Analyzing Session Identifiers with Burp 225
11.6 Analyzing Session Randomness with WebScarab 227
11.7 Changing Sessions to Evade Restrictions 232
11.8 Impersonating Another User 233
11.9 Fixing Sessions 234
11.10 Testing for Cross-Site Request Forgery 235

12. Multifaceted Tests 237
12.1 Stealing Cookies Using XSS 237
12.2 Creating Overlays Using XSS 239
12.3 Making HTTP Requests Using XSS 240
12.4 Attempting DOM-Based XSS Interactively 242

12.5 Bypassing Field Length Restrictions (XSS) 244
12.6 Attempting Cross-Site Tracing Interactively 245
12.7 Modifying Host Headers 247
12.8 Brute-Force Guessing Usernames and Passwords 248
12.9 Attempting PHP Include File Injection Interactively 251
12.10 Creating Decompression Bombs 252
12.11 Attempting Command Injection Interactively 254
12.12 Attempting Command Injection Systematically 256
12.13 Attempting XPath Injection Interactively 258
12.14 Attempting Server-Side Includes (SSI) Injection Interactively 261
12.15 Attempting Server-Side Includes (SSI) Injection Systematically 262
12.16 Attempting LDAP Injection Interactively 264
12.17 Attempting Log Injection Interactively 266

Index. 269