

CONTENTS

Foreword	xv
Acknowledgments	xvii
Introduction	xix

Part I Attacking Web 2.0

▼ 1	Common Injection Attacks	3
	How Injection Attacks Work	4
	SQL Injection	4
	Choosing Appropriate SQL Injection Code	7
	XPath Injection	8
	Command Injection	10
	Directory Traversal Attacks	11
	XXE (XML eXternal Entity) Attacks	13
	LDAP Injection	15
	Buffer Overflows	16
	Testing for Injection Exposures	18
	Automated Testing with iSEC's SecurityQA Toolbar	18
	Summary	20
▼ 2	Cross-Site Scripting	21
	Web Browser Security Models	22
	Same Origin/Domain Policy	22
	Cookie Security Model	26
	Problems with Setting and Parsing Cookies	27
	Using JavaScript to Reduce the Cookie Security Model to the Same Origin Policy	28
	Flash Security Model	30
	Reflecting Policy Files	31
	Three Steps to XSS	32

Step 1: HTML Injection	32
Classic Reflected and Stored HTML Injection	33
Finding Stored and Reflected HTML Injections	37
Reflected HTML Injection in Redirectors	41
HTML Injection in Mobile Applications	41
HTML Injection in AJAX Responses and Error Messages	41
HTML Injection Using UTF-7 Encodings	42
HTML Injection Using MIME Type Mismatch	42
Using Flash for HTML Injection	43
Step 2: Doing Something Evil	44
Stealing Cookies	44
Phishing Attacks	45
Acting as the Victim	45
XSS Worms	46
Step 3: Luring the Victim	47
Obscuring HTML Injection Links	47
Motivating User to Click HTML Injections	49
Testing for Cross-Site Scripting	50
Automated Testing with iSEC's SecurityQA Toolbar	50
Summary	52
References and Further Reading	53
Case Study: Background	55
Finding Script Injection in MySpace	55
Writing the Attack Code	56
Important Code Snippets in SAMY	56
Samy's Supporting Variables and Functions	61
The Original SAMY Worm	66

Part II Next Generation Web Application Attacks

▼ 3 Cross-Domain Attacks	71
Weaving a Tangled Web: The Need for Cross-Domain Actions	72
Uses for Cross-Domain Interaction	72
So What's the Problem?	74
Cross-Domain Image Tags	74
Cross-Domain Attacks for Fun and Profit	77
Cross-Domain POSTs	80
CSRF in a Web 2.0 World: JavaScript Hijacking	83
Summary	86
▼ 4 Malicious JavaScript and AJAX	87
Malicious JavaScript	88
XSS Proxy	89
BeEF Proxy	91

Visited URL Enumeration	95
JavaScript Port Scanner	96
Bypass Input Filters	99
Malicious AJAX	103
XMLHttpRequest	103
Automated AJAX Testing	106
SAMY Worm	107
Yammer Virus	110
Summary	111
▼ 5 .Net Security	113
General Framework Attacks	115
Reversing the .Net Framework	115
XML Attacks	116
Forcing the Application Server to Become Unavailable when Parsing XML	117
Manipulating Application Behavior Through XPath Injection	119
XPath Injection in .Net	119
SQL Injection	120
SQL Injection by Directly Including User Data when Building an SqlCommand	121
Cross-Site Scripting and ASP.Net	123
Input Validation	123
Bypassing Validation by Directly Targeting Server Event Handlers	123
Default Page Validation	124
Disabling ASP.Net's Default Page Validation	124
Output Encoding	125
XSS and Web Form Controls	126
Causing XSS by Targeting ASP.Net Web Form Control Properties	126
More on Cross-Site Scripting	127
Viewstate	128
Viewstate Implementation	128
Gaining Access to Sensitive Data by Decoding Viewstate	129
Using Error Pages to View System Information	131
Attacking Web Services	132
Discovering Web Service Information by Viewing the WSDL File	132
Summary	134
Case Study: Cross-Domain Attacks	135
Cross-Domain Stock-Pumping	135
Security Boundaries	138

Part III **AJAX**

▼ 6	AJAX Types, Discovery, and Parameter Manipulation	145
	Types of AJAX	146
	Client-Server Proxy	146
	Client-Side Rendering	147
	AJAX on the Wire	147
	Downstream Traffic	148
	Upstream Traffic	150
	AJAX Toolkit Wrap-Up	152
	Framework Method Discovery	153
	Microsoft ASP.NET AJAX (Microsoft Atlas)	153
	Google Web Toolkit	154
	Direct Web Remoting	154
	XAJAX	154
	SAJAX	155
	Framework Identification/Method Discovery Example	156
	Framework Wrap-Up	158
	Parameter Manipulation	159
	Hidden Field Manipulation	159
	URL Manipulation	160
	Header Manipulation	160
	Example	160
	Manipulation Wrap-Up	163
	Unintended Exposure	164
	Exposure Wrap-Up	166
	Cookies	166
	The Ugly	166
	The Bad	166
	Example	168
	Cookie Flags	173
	Example	174
	Cookie Wrap-Up	176
	Summary	176
▼ 7	AJAX Framework Exposures	177
	Direct Web Remoting	178
	Installation Procedures	179
	Unintended Method Exposure	179
	Debug Mode	180
	Google Web Toolkit	181
	Installation Procedures	181
	Unintended Method Exposure	182

XAJAX	183
Installation Procedures	183
Unintended Method Exposure	184
SAJAX	185
Installation Procedures	185
Common Exposures	185
Unintended Method Exposure	186
Dojo Toolkit	186
Serialization Security	187
jQuery	187
Serialization Security	187
Summary	188
Case Study: Web 2.0 Migration Exposures	189
Web 2.0 Migration Process	189
Common Exposures	191
Internal Methods	191
Debug Functionality	191
Hidden URLs	192
Full Functionality	192

Part IV Thick Clients

▼ 8 ActiveX Security	197
Overview of ActiveX	199
ActiveX Flaws and Countermeasures	201
Allowing ActiveX Controls to be Invoked by Anyone	202
Not Signing ActiveX Controls	203
Marking ActiveX Controls Safe for Scripting (SFS)	205
Marking ActiveX Controls Safe for Initialization (SFI)	205
Performing Dangerous Actions via ActiveX Controls	207
Buffer Overflows in ActiveX Objects	208
Allowing SFS/SFI Subversion	208
ActiveX Attacks	209
Axenum and Axfuzz	214
AxMan	217
Protecting Against Unsafe ActiveX Objects with IE	219
Summary	222
▼ 9 Attacking Flash Applications	223
A Brief Look at the Flash Security Model	224
Security Policy Reflection Attacks	225
Security Policy Stored Attacks	226

Flash Hacking Tools	227
XSS and XSF via Flash Applications	229
XSS Based on getURL()	230
XSS via clickTAG	231
XSS via HTML TextField.htmlText and TextArea.htmlText ...	232
XSS via loadMovie() and Other URL Loading Functions	233
XSF via loadMovie and Other SWF, Image, and Sound Loading Functions	234
Leveraging URL Redirectors for XSF Attacks	235
XSS in Automatically Generated and Controller SWFs	236
Intranet Attacks Based on Flash: DNS Rebinding	237
DNS in a Nutshell	238
Back to DNS Rebinding	238
Summary	242
Case Study: Internet Explorer 7 Security Changes	243
ActiveX Opt-In	243
SSL Protections	244
URL Parsing	244
Cross-Domain Protection	245
Phishing Filter	245
Protected Mode	246
▼ Index	247