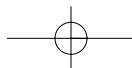


Contents

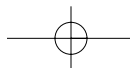
Chapter 1 Cross-site Scripting Fundamentals	1
Introduction	2
Web Application Security	4
XML and AJAX Introduction	6
Summary	11
Solutions Fast Track	11
Frequently Asked Questions	12
Chapter 2 The XSS Discovery Toolkit	15
Introduction	16
Burp	16
Debugging DHTML With Firefox Extensions	21
DOM Inspector	21
Web Developer Firefox Extension	26
Insert Edit HTML Picture	27
XSS Example in Web Developer Web Site	28
FireBug	29
Analyzing HTTP Traffic with Firefox Extensions	35
LiveHTTPHeaders	35
ModifyHeaders	39
TamperData	42
GreaseMonkey	46
GreaseMonkey Internals	47
Creating and Installing User Scripts	50
PostInterpreter	52
XSS Assistant	54
Active Exploitation with GreaseMonkey	55
Hacking with Bookmarklets	57
Using Technika	60
Summary	63
Solutions Fast Track	64
Frequently Asked Questions	65



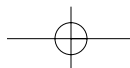
Chapter 3 XSS Theory	67
Introduction	68
Getting XSS'ed	68
Non-persistent	69
DOM-based	73
Persistent	75
DOM-based XSS In Detail	75
Identifying DOM-based XSS Vulnerabilities	76
Exploiting Non-persistent DOM-based XSS Vulnerabilities	80
Exploiting Persistent DOM-based XSS Vulnerabilities ..	82
Preventing DOM-based XSS Vulnerabilities	84
Redirection	86
Redirection Services	90
Referring URLs	91
CSRF	93
Flash, QuickTime, PDF, Oh My	97
Playing with Flash Fire	98
Hidden PDF Features	105
QuickTime Hacks for Fun and Profit	116
Backdooring Image Files	121
HTTP Response Injection	123
Source vs. DHTML Reality	125
Bypassing XSS Length Limitations	131
XSS Filter Evasion	133
When Script Gets Blocked	139
Browser Peculiarities	150
CSS Filter Evasion	152
XML Vectors	154
Attacking Obscure Filters	155
Encoding Issues	156
Summary	159
Solutions Fast Track	159
Frequently Asked Questions	162
Chapter 4 XSS Attack Methods	163
Introduction	164
History Stealing	164



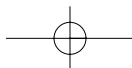
JavaScript/CSS API “getComputedStyle”	164
Code for Firefox/Mozilla. May	
Work In Other Browsers	164
Stealing Search Engine Queries	167
JavaScript Console Error Login Checker	167
Intranet Hacking	173
Exploit Procedures	174
Persistent Control	174
Obtaining NAT’ed IP Addresses	176
Port Scanning	177
Blind Web Server Fingerprinting	180
Attacking the Intranet	181
XSS Defacements	184
Summary	188
Solutions Fast Track	188
Frequently Asked Questions	189
References	190
Chapter 5 Advanced XSS Attack Vectors	191
Introduction	192
DNS Pinning	192
Anti-DNS Pinning	194
Anti-Anti-DNS Pinning	196
Anti-anti-anti-DNS Pinning	
AKA Circumventing Anti-anti-DNS Pinning	196
Additional Applications of Anti-DNS Pinning	197
IMAP3	199
MHTML	204
Expect Vulnerability	207
Hacking JSON	209
Summary	216
Frequently Asked Questions	217
Chapter 6 XSS Exploited	219
Introduction	220
XSS vs. Firefox Password Manager	220
SeXXS Offenders	223
Equifraked	228
Finding the Bug	229

**xii Contents**

Building the Exploit Code	230
Owning the Cingular Xpress Mail User	232
The Xpress Mail Personal Edition Solution	232
Seven.com	234
The Ackid (AKA Custom Session ID)	234
The Inbox	235
The Document Folder	236
E-mail Cross-linkage	237
CSFR Proof of Concepts	238
Cookie Grab	238
Xpressmail Snarfer	241
Owning the Documents	248
Alternate XSS: Outside the BoXXS	248
Owning the Owner	249
The SILICA and CANVAS	249
Building the Scripted Share	250
Owning the Owner	251
Lessons Learned and Free Advertising	252
Airpwned with XSS	252
XSS Injection: XSSing Protected Systems	256
The Decompiled Flash Method	256
Application Memory Massaging –	
XSS via an Executable	261
XSS Old School - Windows Mobile PIE 4.2	262
Cross-frame Scripting Illustrated	263
XSSing Firefox Extensions	267
GreaseMonkey Backdoors	267
GreaseMonkey Bugs	270
XSS the Backend: Snoopwned	275
XSS Anonymous Script Storage - TinyURL 0day	277
XSS Exploitation: Point-Click-Own with EZPhotoSales	285
Summary	288
Solutions Fast Track	288
Frequently Asked Questions	291
Chapter 7 Exploit Frameworks	293
Introduction	294
AttackAPI	294



Enumerating the Client	298
Attacking Networks	307
Hijacking the Browser	315
Controlling Zombies	319
BeEF	322
Installing and Configuring BeEF	323
Controlling Zombies	323
BeEF Modules	325
Standard Browser Exploits	327
Port Scanning with BeEF	327
Inter-protocol Exploitation and Communication with BeEF	328
CAL9000	330
XSS Attacks, Cheat Sheets, and Checklists	331
Encoder, Decoders, and Miscellaneous Tools	334
HTTP Requests/Responses and Automatic Testing	335
Overview of XSS-Proxy	338
XSS-Proxy Hijacking Explained	341
Browser Hijacking Details	343
Attacker Control Interface	346
Using XSS-Proxy: Examples	347
Setting Up XSS-Proxy	347
Injection and Initialization Vectors For XSS-Proxy	350
Handoff and CSRF With Hijacks	352
Sage and File:// Hijack With Malicious RSS Feed	354
Summary	371
Solutions Fast Track	371
Frequently Asked Questions	372
Chapter 8 XSS Worms	375
Introduction	376
Exponential XSS	376
XSS Warhol Worm	379
Linear XSS Worm	380
Samy Is My Hero	386
Summary	391
Solutions Fast Track	391
Frequently Asked Questions	393



Chapter 9 Preventing XSS Attacks	395
Introduction	396
Filtering	396
Input Encoding	400
Output Encoding	402
Web Browser's Security	402
Browser Selection	403
Add More Security To Your Web Browser	403
Disabling Features	404
Use a Virtual Machine	404
Don't Click On Links in E-mail, Almost Ever	404
Defend your Web Mail	404
Beware of Overly Long URL's	404
URL Shorteners	405
Secrets Questions and Lost Answers	405
Summary	406
Solutions Fast Track	406
Frequently Asked Questions	407
Appendix A The Owned List	409
Index	439

