



Contents

Introduction	xv
Chapter 1 Web Browser Security	1
A Principal Principle	2
Exploring the Browser	3
Symbiosis with the Web Application	4
Same Origin Policy	4
HTTP Headers	5
Markup Languages	5
Cascading Style Sheets	6
Scripting	6
Document Object Model	7
Rendering Engines	7
Geolocation	9
Web Storage	9
Cross-origin Resource Sharing	9
HTML5	10
Vulnerabilities	11
Evolutionary Pressures	12
HTTP Headers	13
Reflected XSS Filtering	15
Sandboxing	15
Anti-phishing and Anti-malware	16
Mixed Content	17
Core Security Problems	17
Attack Surface	17
Surrendering Control	20
TCP Protocol Control	20

	Encrypted Communication	20
	Same Origin Policy	21
	Fallacies	21
	Browser Hacking Methodology	22
	Summary	28
	Questions	28
	Notes	29
Chapter 2	Initiating Control	31
	Understanding Control Initiation	32
	Control Initiation Techniques	32
	Using Cross-site Scripting Attacks	32
	Using Compromised Web Applications	46
	Using Advertising Networks	46
	Using Social Engineering Attacks	47
	Using Man-in-the-Middle Attacks	59
	Summary	72
	Questions	73
	Notes	73
Chapter 3	Retaining Control	77
	Understanding Control Retention	78
	Exploring Communication Techniques	79
	Using XMLHttpRequest Polling	80
	Using Cross-origin Resource Sharing	83
	Using WebSocket Communication	84
	Using Messaging Communication	86
	Using DNS Tunnel Communication	89
	Exploring Persistence Techniques	96
	Using IFrames	96
	Using Browser Events	98
	Using Pop-Under Windows	101
	Using Man-in-the-Browser Attacks	104
	Evading Detection	110
	Evasion using Encoding	111
	Evasion using Obfuscation	116
	Summary	125
	Questions	126
	Notes	127
Chapter 4	Bypassing the Same Origin Policy	129
	Understanding the Same Origin Policy	130
	Understanding the SOP with the DOM	130
	Understanding the SOP with CORS	131
	Understanding the SOP with Plugins	132
	Understanding the SOP with UI Redressing	133
	Understanding the SOP with Browser History	133

Exploring SOP Bypasses	134
Bypassing SOP in Java	134
Bypassing SOP in Adobe Reader	140
Bypassing SOP in Adobe Flash	141
Bypassing SOP in Silverlight	142
Bypassing SOP in Internet Explorer	142
Bypassing SOP in Safari	143
Bypassing SOP in Firefox	144
Bypassing SOP in Opera	145
Bypassing SOP in Cloud Storage	149
Bypassing SOP in CORS	150
Exploiting SOP Bypasses	151
Proxying Requests	151
Exploiting UI Redressing Attacks	153
Exploiting Browser History	170
Summary	178
Questions	179
Notes	179
Chapter 5	
Attacking Users	183
Defacing Content	183
Capturing User Input	187
Using Focus Events	188
Using Keyboard Events	190
Using Mouse and Pointer Events	192
Using Form Events	195
Using IFrame Key Logging	196
Social Engineering	197
Using TabNabbing	198
Using the Fullscreen	199
Abusing UI Expectations	204
Using Signed Java Applets	223
Privacy Attacks	228
Non-cookie Session Tracking	230
Bypassing Anonymization	231
Attacking Password Managers	234
Controlling the Webcam and Microphone	236
Summary	242
Questions	243
Notes	243
Chapter 6	
Attacking Browsers	247
Fingerprinting Browsers	248
Fingerprinting using HTTP Headers	249
Fingerprinting using DOM Properties	253
Fingerprinting using Software Bugs	258
Fingerprinting using Quirks	259

Bypassing Cookie Protections	260
Understanding the Structure	261
Understanding Attributes	263
Bypassing Path Attribute Restrictions	265
Overflowing the Cookie Jar	268
Using Cookies for Tracking	270
Sidejacking Attacks	271
Bypassing HTTPS	272
Downgrading HTTPS to HTTP	272
Attacking Certificates	276
Attacking the SSL/TLS Layer	277
Abusing Schemes	278
Abusing iOS	279
Abusing the Samsung Galaxy	281
Attacking JavaScript	283
Attacking Encryption in JavaScript	283
JavaScript and Heap Exploitation	286
Getting Shells using Metasploit	293
Getting Started with Metasploit	294
Choosing the Exploit	295
Executing a Single Exploit	296
Using Browser Autopwn	300
Using BeEF with Metasploit	302
Summary	305
Questions	305
Notes	306
Chapter 7 Attacking Extensions	311
Understanding Extension Anatomy	312
How Extensions Differ from Plugins	312
How Extensions Differ from Add-ons	313
Exploring Privileges	313
Understanding Firefox Extensions	314
Understanding Chrome Extensions	321
Discussing Internet Explorer Extensions	330
Fingerprinting Extensions	331
Fingerprinting using HTTP Headers	331
Fingerprinting using the DOM	332
Fingerprinting using the Manifest	335
Attacking Extensions	336
Impersonating Extensions	336
Cross-context Scripting	339
Achieving OS Command Execution	355
Achieving OS Command Injection	359
Summary	364
Questions	365
Notes	365

Chapter 8	Attacking Plugins	371
	Understanding Plugin Anatomy	372
	How Plugins Differ from Extensions	372
	How Plugins Differ from Standard Programs	374
	Calling Plugins	374
	How Plugins are Blocked	376
	Fingerprinting Plugins	377
	Detecting Plugins	377
	Automatic Plugin Detection	379
	Detecting Plugins in BeEF	380
	Attacking Plugins	382
	Bypassing Click to Play	382
	Attacking Java	388
	Attacking Flash	400
	Attacking ActiveX Controls	403
	Attacking PDF Readers	408
	Attacking Media Plugins	410
	Summary	415
	Questions	416
	Notes	416
Chapter 9	Attacking Web Applications	421
	Sending Cross-origin Requests	422
	Enumerating Cross-origin Quirks	422
	Preflight Requests	425
	Implications	425
	Cross-origin Web Application Detection	426
	Discovering Intranet Device IP Addresses	426
	Enumerating Internal Domain Names	427
	Cross-origin Web Application Fingerprinting	429
	Requesting Known Resources	430
	Cross-origin Authentication Detection	436
	Exploiting Cross-site Request Forgery	440
	Understanding Cross-site Request Forgery	440
	Attacking Password Reset with XSRF	443
	Using CSRF Tokens for Protection	444
	Cross-origin Resource Detection	445
	Cross-origin Web Application Vulnerability Detection	450
	SQL Injection Vulnerabilities	450
	Detecting Cross-site Scripting Vulnerabilities	465
	Proxying through the Browser	469
	Browsing through a Browser	472
	Burp through a Browser	477
	Sqlmap through a Browser	480
	Browser through Flash	482
	Launching Denial-of-Service Attacks	487
	Web Application Pinch Points	487
	DDoS Using Multiple Hooked Browsers	489

Launching Web Application Exploits	493
Cross-origin DNS Hijack	493
Cross-origin JBoss JMX Remote Command Execution	495
Cross-origin GlassFish Remote Command Execution	497
Cross-origin m0n0wall Remote Command Execution	501
Cross-origin Embedded Device Command Execution	502
Summary	508
Questions	508
Notes	509
Chapter 10 Attacking Networks	513
Identifying Targets	514
Identifying the Hooked Browser's Internal IP	514
Identifying the Hooked Browser's Subnet	520
Ping Sweeping	523
Ping Sweeping using XMLHttpRequest	523
Ping Sweeping using Java	528
Port Scanning	531
Bypassing Port Banning	532
Port Scanning using the IMG Tag	537
Distributed Port Scanning	539
Fingerprinting Non-HTTP Services	542
Attacking Non-HTTP Services	545
NAT Pinning	545
Achieving Inter-protocol Communication	549
Achieving Inter-protocol Exploitation	564
Getting Shells using BeEF Bind	579
The BeEF Bind Shellcode	579
Using BeEF Bind in your Exploits	585
Using BeEF Bind as a Web Shell	596
Summary	599
Questions	600
Notes	601
Chapter 11 Epilogue: Final Thoughts	605
Index	609