

CONTENTS

Foreword	xvii
Acknowledgements	xix
Preface	xxi

Part I

Reconnaissance

▼ 1 Introduction to Web Applications and Security	3
The Web Application Architecture	5
A Brief Word about HTML	6
Transport: HTTP	7
The Web Client	11
The Web Server	12
The Web Application	13
The Database	16
Complications and Intermediaries	16
The New Model: Web Services	18
Potential Weak Spots	19
The Methodology of Web Hacking	20
Profile the Infrastructure	20
Attack Web Servers	20
Survey the Application	20
Attack the Authentication Mechanism	21
Attack the Authorization Schemes	21
Perform a Functional Analysis	21

Exploit the Data Connectivity	21
Attack the Management Interfaces	22
Attack the Client	22
Launch a Denial-of-Service Attack	22
Summary	22
References and Further Reading	23
▼ 2 Profiling	25
Server Discovery	26
Intuition	26
Internet Footprinting	26
DNS Interrogation	31
Ping	32
Discovery Using Port Scanning	32
Dealing with Virtual Servers	34
Service Discovery	35
Server Identification	37
Dealing with SSL	38
Summary	39
References and Further Reading	40
▼ 3 Hacking Web Servers	41
Common Vulnerabilities by Platform	42
Apache	42
Microsoft Internet Information Server (IIS)	46
Attacks Against IIS Components	46
Attacks Against IIS	56
Escalating Privileges on IIS	63
Netscape Enterprise Server	72
Other Web Server Vulnerabilities	75
Miscellaneous Web Server Hacking Techniques	78
Automated Vulnerability Scanning Software	80
Whisker	80
Nikto	83
twwwscan/arirang	84
Stealth HTTP Scanner	85
Typhon	87
WebInspect	89
AppScan	90
FoundScan Web Module	91
Denial of Service Against Web Servers	92
Summary	95
References and Further Reading	95

▼ 4	Surveying the Application	99
	Documenting Application Structure	100
	Manually Inspecting the Application	102
	Statically and Dynamically Generated Pages	102
	Directory Structure	105
	Helper Files	108
	Java Classes and Applets	109
	HTML Comments and Content	110
	Forms	112
	Query Strings	114
	Back-End Connectivity	117
	Tools to Automate the Survey	117
	lynx	118
	Wget	119
	Teleport Pro	120
	Black Widow	121
	WebSleuth	122
	Common Countermeasures	125
	A Cautionary Note	125
	Protecting Directories	125
	Protecting Include Files	126
	Miscellaneous Tips	126
	Summary	127
	References and Further Reading	127

Part II

The Attack

▼ 5	Authentication	131
	Authentication Mechanisms	132
	HTTP Authentication: Basic and Digest	132
	Forms-Based Authentication	143
	Microsoft Passport	145
	Attacking Web Authentication	149
	Password Guessing	149
	Session ID Prediction and Brute Forcing	155
	Subverting Cookies	155
	Bypassing SQL-Backed Login Forms	157
	Bypassing Authentication	158
	Summary	159
	References and Further Reading	159

▼ 6	Authorization	161
	The Attacks	162
	Role Matrix	163
	The Methodology	164
	Query String	165
	POST Data	165
	Hidden Tags	166
	URI	166
	HTTP Headers	167
	Cookies	167
	Final Notes	168
	Case Study: Using Curl to Map Permissions	170
	Apache Authorization	173
	IIS Authorization	175
	Summary	176
	References and Further Reading	176
▼ 7	Attacking Session State Management	177
	Client-Side Techniques	179
	Hidden Fields	180
	The URL	182
	HTTP Headers and Cookies	182
	Server-Side Techniques	183
	Server-Generated Session IDs	184
	Session Database	184
	SessionID Analysis	185
	Content Analysis	185
	Time Windows	198
	Summary	200
	References and Further Reading	200
▼ 8	Input Validation Attacks	201
	Expecting the Unexpected	202
	Input Validation EndGame	203
	Where to Find Potential Targets	203
	Bypassing Client-Side Validation Routines	204
	Common Input Validation Attacks	205
	Buffer Overflow	205
	Canonicalization (dot-dot-slash)	207
	Script Attacks	212
	Boundary Checking	216
	Manipulating the Application	217
	SQL Injection and Datastore Attacks	218

Command Execution	218
Common Side Effects	220
Common Countermeasures	220
Summary	221
References and Further Reading	222
▼ 9 Attacking Web Datastores	225
A SQL Primer	226
SQL Injection	226
Common Countermeasures	240
Summary	241
References and Further Reading	241
▼ 10 Attacking Web Services	243
What Is a Web Service?	244
Transport: SOAP over HTTP(S)	245
WSDL	247
Directory Services: UDDI and DISCO	249
Sample Web Services Hacks	252
Basics of Web Service Security	253
Similarities to Web Application Security	254
Web Services Security Measures	254
Summary	258
References and Further Reading	258
▼ 11 Hacking Web Application Management	261
Web Server Administration	262
Telnet	262
SSH	263
Proprietary Management Ports	263
Other Administration Services	263
Web Content Management	264
FTP	265
SSH/scp	265
FrontPage	265
WebDAV	270
Web-Based Network and System Management	271
Other Web-Based Management Products	274
Summary	275
References and Further Reading	275

▼ 12	Web Client Hacking	277
	The Problem of Client-Side Security	278
	Attack Methodologies	279
	Active Content Attacks	279
	Java and JavaScript	280
	ActiveX	281
	Cross-Site Scripting	289
	Cookie Hijacking	292
	Summary	296
	References and Further Reading	297
▼ 13	Case Studies	299
	Case Study #1: From the URL to the Command Line and Back	300
	Case Study #2: XOR Does Not Equal Security	303
	Case Study #3: The Cross-Site Scripting Calendar	305
	Summary	307
	References and Further Reading	307

Part III

Appendixes

▼ A	Web Site Security Checklist	311
▼ B	Web Hacking Tools and Techniques Cribsheet	317
▼ C	Using Libwhisker	333
	Inside Libwhisker	334
	http_do_request Function	334
	crawl Function	337
	utils_randstr Function	340
	Building a Script with Libwhisker	340
	Sinjection.pl	341
▼ D	UrlScan Installation and Configuration	345
	Overview of UrlScan	346
	Obtaining UrlScan	347
	Updating UrlScan	347
	Updating Windows Family Products	348
	hfnetchk	348
	Third-Party Tools	349
	Basic UrlScan Deployment	351
	Rolling Back IISLockdown	356
	Unattended IISLockdown Installation	358

Advanced UrlScan Deployment	358
Extracting UrlScan.dll	359
Configuring UrlScan.ini	359
Installing the UrlScan ISAPI Filter in IIS	361
Removing UrlScan	364
UrlScan.ini Command Reference	365
Options Section	365
AllowVerbs Section	367
DenyVerbs Section	367
DenyHeaders Section	368
AllowExtensions Section	368
DenyExtensions Section	369
Summary	369
References and Further Reading	369
▼ E About the Companion Web Site	371
▼ Index	373