

"A great addition to an arsenal to find, exploit, and overcome Web security issues."—Heather Adkins, *Google Security*

Foreword by
Jeremiah Grossman,
Co-Founder of the
Web Application
Security Consortium
(WASC)

SECOND EDITION

HACKING Web Applications EXPOSED

Web Application Security Secrets and Solutions

Joel Scambray, Mike Shema, and Caleb Sima

CONTENTS

Foreword	xvii
Acknowledgments	xxi
Introduction	xxiii
▼ 1 Hacking Web Apps 101	1
What Is Web Application Hacking?	2
GUI Web Hacking	2
URI Hacking	3
Methods, Headers, and Body	4
Resources	6
Authentication, Sessions, and Authorization	7
The Web Client and HTML	7
Other Protocols	8
Why Attack Web Applications?	9
Who, When, and Where?	10
Weak Spots	10
How Are Web Apps Attacked?	11
The Web Browser	12
Browser Extensions	13
HTTP Proxies	17
Command-line Tools	23
Older Tools	24

Hacking Exposed Web Applications

Summary	24
References and Further Reading	24
▼ 2 Profiling	27
Infrastructure Profiling	28
Footprinting and Scanning: Defining Scope	28
Basic Banner Grabbing	29
Advanced HTTP Fingerprinting	30
Infrastructure Intermediaries	32
Application Profiling	40
Manual Inspection	41
Using Search Tools for Profiling	60
Automated Web Crawling	65
Common Web Application Profiles	70
General Countermeasures	75
A Cautionary Note	75
Protecting Directories	75
Protecting include Files	76
Miscellaneous Tips	76
Summary	77
References and Further Reading	77
▼ 3 Hacking Web Platforms	79
Point-and-click Exploitation Using Metasploit	81
Manual Exploitation	84
Evading Detection	99
Web Platform Security Best Practices	102
Common Best Practices	102
IIS Hardening	104
Apache Hardening	110
PHP Best Practices	115
Summary	117
References and Further Reading	117
▼ 4 Attacking Web Authentication	121
Web Authentication Threats	122
Username/Password Threats	122
Strong(er) Web Authentication	139
Web Authentication Services	142
Bypassing Authentication	146
Token Replay	147
Identity Management	148
Client-side Piggybacking	152

Some Final Thoughts: Identity Theft	153
Summary	153
References and Further Reading	155
▼ 5 Attacking Web Authorization	159
Fingerprinting Authz	161
Crawling ACLs	161
Identifying Access/Session Tokens	162
Analyzing Session Tokens	165
Differential Analysis	166
Role Matrix	167
Attacking ACLs	168
Attacking Tokens	170
Manual Prediction	170
Automated Prediction	178
Capture/Replay	184
Session Fixation	184
Authorization Attack Case Studies	185
Horizontal Privilege Escalation	186
Vertical Privilege Escalation	191
Differential Analysis	194
Using Curl to Map Permissions	196
Authorization Best Practices	199
Web ACL Best Practices	200
Web Authorization/Session Token Security	202
Security Logs	205
Summary	206
References and Further Reading	206
▼ 6 Input Validation Attacks	209
Expect the Unexpected	210
Where to Find Attack Vectors	212
Bypass Client-side Validation Routines	213
Common Input Validation Attacks	213
Buffer Overflow	213
Canonicalization (dot-dot-slash)	215
HTML Injection	220
Boundary Checks	224
Manipulate Application Behavior	225
SQL Injection and Datastore Attacks	226
Command Execution	226
Encoding Abuse	228
PHP Global Variables	229

Hacking Exposed Web Applications

Common Side-effects	230
Summary	232
References and Further Reading	233
▼ 7 Attacking Web Datastores	235
SQL Primer	236
Syntax	237
SELECT, INSERT, and UPDATE	237
SQL Injection Discovery	238
Syntax and Errors	238
Semantics and Behavior	242
Alternate Character Encoding	246
Exploit SQL Injection Vulnerabilities	247
Alter a Process	247
Query Alternate Data	249
Platforms	256
Other Datastore Attacks	261
Input Validation	262
Decouple Query Logic from Query Data	262
Database Encryption	265
Database Configuration	265
Summary	266
▼ 8 Attacking XML Web Services	267
What Is a Web Service?	268
Transport: SOAP Over HTTP(S)	269
WSDL	271
Directory Services: UDDI and DISCO	275
Similarities to Web Application Security	279
Attacking Web Services	279
Web Service Security Basics	287
Web Services Security Measures	287
Summary	290
References and Further Reading	291
▼ 9 Attacking Web Application Management	293
Remote Server Management	294
Telnet	294
SSH	295
Proprietary Management Ports	295
Other Administration Services	295
Web Content Management	297
FTP	297
SSH/scp	297

FrontPage	298
WebDAV	301
Admin Misconfigurations	308
Unnecessary Web Server Extensions	308
Information Leakage	312
Developer-driven Mistakes	321
Summary	327
References and Further Reading	328
▼ 10 Hacking Web Clients	331
Exploits	332
Trickery	346
General Countermeasures	353
IE Security Zones	354
Firefox Secure Configuration	358
Low-privilege Browsing	359
Server-side Countermeasures	360
Summary	361
References and Further Reading	361
▼ 11 Denial-of-Service (DoS) Attacks	367
Common DoS Attack Techniques	368
Old School DoS: Vulnerabilities	369
Modern DoS: Capacity Depletion	370
Application-layer DoS	373
General DoS Countermeasures	383
Proactive DoS Mitigation	384
Detecting DoS	391
Responding to DoS	392
Summary	394
References and Further Reading	394
▼ 12 Full-Knowledge Analysis	397
Threat Modeling	398
Clarify Security Objectives	400
Identify Assets	400
Architecture Overview	400
Decompose the Application	401
Identify and Document Threats	404
Rank the Threats	405
Develop Threat Mitigation Strategies	406
Code Review	407
Manual Source Code Review	408

Hacking Exposed Web Applications

Automated Source Code Review	414
Binary Analysis	414
Security Testing of Web App Code	423
Fuzzing	424
Test Tools, Utilities, and Harnesses	426
Pen-testing	426
Security in the Web Development Process	427
People	427
Process	429
Technology	429
Summary	431
References and Further Reading	431
▼ 13 Web Application Security Scanners	435
Technology: Web App Security Scanners	436
The Testbed	437
The Tests	438
Reviews of Individual Scanners	443
Overall Test Results	455
Nontechnical Issues	459
Process	459
People	461
Summary	463
References and Further Reading	463
▼ A Web Application Security Checklist	465
▼ B Web Hacking Tools and Techniques Cribsheet	471
▼ C URLScan and ModSecurity	483
URLScan	484
Basic URLScan Deployment (IIS5.x and Earlier)	485
Advanced URLScan Configuration	492
Managing URLScan	497
ModSecurity	500
ModSecurity Installation	500
ModSecurity Configuration	501
Summary	505
References and Further Reading	505
▼ D About the Companion Web Site	507
▼ Index	509