

Contents

Acknowledgments	xi
Introduction	xix
Chapter 1: Penetration Testing Web Applications	1
Security Industry Weaknesses	1
Application Development Considerations	2
Limitations of Edge Security Models	2
The Case for Pen Testing	3
Industry Preparedness	3
The Bottom Line	5
The Mindset	6
Creativity	6
Digging Deep	7
The Goal	8
Methodology	8
Rolling Documentation	9
This Book	9
The Business	10
Requirements	11
Rules of Engagement	11
Self Protection	12
Summary	13
Chapter 2: Web Applications: Some Basics	15
Architectural Aspects	15
What Is a Web Application?	16
The Tiers	19
The HTTP Protocol	21
HTTP Proxy	25
SSL/TLS	28
Application Aspects	35
State	35
Dynamic Technologies	37
Web-Based Authentication	41

Contents

Data Aspects	42
Encryption vs. Encoding	42
XML	51
Emerging Web Application Models	56
Integration	56
Frameworks	67
Wireless	68
Summary	70
Chapter 3: Discovery	71
Logistics	72
WHOIS	72
DNS	75
ARIN	76
SamSpade	77
Filter Detection	80
OS Fingerprinting	85
Netcraft	85
pOf	86
Web Server Fingerprinting	89
HTTP Headers	89
httprint	92
Application Fingerprinting	93
Port Mapping	94
Service Identification	97
Database Identification	103
Analyze Error Pages	104
File Type Probes	106
Resource Enumeration	107
HTML Source Sifting	116
Information Harvesting	118
Web Services	124
UDDI and DISCO	125
WSIL	127
J2EE	128
Summary	131
Chapter 4: Vulnerability Analysis	133
OWASP and the Top Ten Threats	134
WASC	134

A1 – Unvalidated Input	136
Validation	136
Manipulation	136
A2 – Broken Access Control	141
A3 – Broken Authentication and Session Management	142
Authentication	142
Session	146
A4 – Cross-Site Scripting (XSS) Flaws	154
Cross-Site Tracing (XST)	157
A5 – Buffer Overflows	158
A6 – Injection Flaws	163
LDAP Injection	163
OS Commanding	165
SQL Injection	166
SSI Injection	173
XPath Injection	173
XXE	174
A7 – Improper Error Handling	175
A8 – Insecure Storage	176
Live Data	177
Archived Data	177
A9 – Denial of Service (DoS)	178
Target: Web Server	179
Target: User	180
Target: DB	180
A10 – Insecure Configuration Management	181
Other Areas	183
Insufficient Authentication	183
Weak Password Recovery Validation	183
Content Spoofing	183
Information Leakage	184
Abuse of Functionality	184
Insufficient Anti-Automation	185
Insufficient Process Validation	185
Reverse Engineering	185
Threat Modeling	186
1. Decompose and Understand the Application	187
2. Analysis of Threats	188
3. Categorization and Ranking of Threats	189
4. Identification of Mitigation Strategies	190
5. Pen Test	193
Methodologies and Tools	193
Summary	194

Contents

Chapter 5: Attack Simulation Techniques and Tools: Web Server **195**

Identifying Threats	196
Default Content and Settings	196
Attacks on the System	197
Configuration	201
Product-Specific Issues	204
Tools	214
Nessus	214
Commercial Tools	215
Summary	217

Chapter 6: Attack Simulation Techniques and Tools: Web Application **219**

The App Checklist	220
Manual Testing	222
The Proxy	222
Custom Scripts	234
Frameworks	244
SQL Injection	246
Authentication	248
Buffer Overflow	266
Client-Side Attacks	268
XSS	268
Active Content	270
Cookies	271
Client-Side Example	272
Automated Testing	273
The Proxy	274
Scanners	285
Multi-Purpose Scanners	294
Commercial Tools	306
Web Application Related	306
DB Related	313
Summary	313

Chapter 7: Attack Simulation Techniques and Tools: Known Exploits **315**

Manual Examples	317
Example 1 — Domino WebMail	317
Example 2 — IIS	326
Using MetaSploit	338

Moving Forward . . .	347
SecurityFocus	347
HSC	349
CERT	351
Secunia	351
eEye	351
OSVDB	351
CVE	352
Warning	352
Commercial Products	355
Immunity CANVAS	355
Core Impact	356
Summary	356
<u>Chapter 8: Attack Simulation Techniques and Tools: Web Services</u>	<u>357</u>
The Reality	358
Identifying Threats	359
XML Content Attacks	359
Web Service Attacks	362
Infrastructure Attacks	362
Simulating the Attack	364
Footprinting	364
Enumeration	368
Analysis	371
Testing/Attacking	373
Documentation	392
Commercial Tools	394
WebInspect	395
Moving Forward . . .	396
WSID4ID	396
AJAX	397
Summary	399
<u>Chapter 9: Documentation and Presentation</u>	<u>401</u>
Results Verification	402
False Positives	402
Document Structure	406
Executive Summary	406
Risk Matrix	408
Best Practices	413

Contents

Final Summary	416
Results Document Security	416
Compliance Factors	417
Presentation Techniques	423
Summary	423
<hr/> Chapter 10: Remediation	<hr/> 425
Edge-Level Protection	426
Web Application Firewalls	426
Web Services	430
Some Best Practices	432
Input Validation	432
Session Management	442
Code Audit	445
Summary	446
<hr/> Chapter 11: Your Lab	<hr/> 449
Hardware	450
Servers	450
Network	450
Storage	450
Software	451
Client Tools	451
Server OS Installations	452
Web Applications	457
webAppHoneyPot	468
Summary	469
<hr/> Appendix A: Basic SQL	<hr/> 471
<hr/> Appendix B: Basic LDAP	<hr/> 477
<hr/> Appendix C: XPath and XQuery	<hr/> 483
<hr/> Appendix D: Injection Attack Dictionaries	<hr/> 495
 Index	 505