

Contents

Chapter 1 Hacking Methodology	1
Introduction	2
Understanding the Terms	3
A Brief History of Hacking	3
Phone System Hacking	4
Computer Hacking	5
What Motivates a Hacker?	7
Ethical Hacking versus Malicious Hacking	8
Working with Security Professionals	9
Associated Risks with Hiring a Security Professional	9
Understanding Current Attack Types	10
DoS/DDoS	10
Virus Hacking	12
End-User Virus Protection	14
Worms	16
Rogue Applets	18
Stealing	18
Credit Card Theft	19
Theft of Identity	21
Information Piracy	22
Recognizing Web Application Security Threats	23
Hidden Manipulation	23
Parameter Tampering	24
Cross-Site Scripting	24
Buffer Overflow	24
Cookie Poisoning	25
Preventing Break-Ins by Thinking like a Hacker	25
Summary	28
Solutions Fast Track	28
Frequently Asked Questions	32
Chapter 2 How to Avoid Becoming a Code Grinder	35
Introduction	36
What Is a Code Grinder?	37

Following the Rules	39
Thinking Creatively when Coding	41
Use All Available Resources at Your Disposal	43
Allowing for Thought	44
Modular Programming Done Correctly	44
Security from the Perspective of a Code Grinder	46
Coding in a Vacuum	48
Building Functional and Secure Web Applications	49
But My Code Is Functional!	54
There Is More to an Application than Functionality	55
You Can Make the Difference!	56
Let's Make It Secure and Functional	58
Summary	62
Solutions Fast Track	63
Frequently Asked Questions	64

Chapter 3 Understanding the Risk Associated with Mobile Code 67

Introduction	68
Recognizing the Impact of Mobile Code Attacks	69
Browser Attacks	69
Mail Client Attacks	69
Malicious Scripts or Macros	72
Identifying Common Forms of Mobile Code	72
Macro Languages: Visual Basic for Applications (VBA)	73
Security Problems with VBA	74
The Melissa Virus	79
Protecting against VBA Viruses	80
JavaScript	83
JavaScript Security Overview	84
Security Problems	84
Exploiting Plug-In Commands	86
Web-Based E-Mail Attacks	87
Social Engineering	87
Lowering JavaScript Security Risks	88
VBScript	88
VBScript Security Overview	89

VBScript Security Problems	89
VBScript Security Precautions	90
Java Applets	91
Granting Additional Access to Applets	92
Security Problems with Java	92
Background Threads	92
Contacting the Host Server	93
Java Security Precautions	93
ActiveX Controls	94
ActiveX Security Overview	94
Security Problems with ActiveX	95
Preinstalled ActiveX Controls	96
Buffer Overrun Error	97
Intentionally Malicious ActiveX	98
Unsafe for Scripting	98
ActiveX Security Precautions	98
Disabling an ActiveX Control	98
E-Mail Attachments and Downloaded Executables	99
Back Orifice 2000 Trojan	99
Protecting Your System from Mobile Code Attacks	103
Security Applications	103
ActiveX Manager	103
Back Orifice Detectors	104
Firewall Software	108
Web-Based Tools	108
Online Scanners	108
Client Security Updates	109
Summary	110
Solutions Fast Track	110
Frequently Asked Questions	112
Chapter 4 Vulnerable CGI Scripts	113
Introduction	114
What Is a CGI Script, and What Does It Do?	114
Typical Uses of CGI Scripts	116
When Should You Use CGI?	121
CGI Script Hosting Issues	122

Break-Ins Resulting from Weak CGI Scripts	123
How to Write “Tighter” CGI Scripts	124
Searchable Index Commands	128
CGI Wrappers	128
Nikto	129
Acquiring and Using Nikto	131
Nikto Commands	133
Web Hack Control Center	137
SQL Injection	138
Languages for Writing CGI Scripts	140
UNIX Shell	141
Perl	141
C/C++	142
Visual Basic	142
Advantages of Using CGI Scripts	143
Rules for Writing Secure CGI Scripts	143
Storing CGI Scripts	147
Summary	149
Solutions Fast Track	149
Frequently Asked Questions	152
Chapter 5 Hacking Techniques and Tools	155
Introduction	156
A Hacker’s Goals	157
Minimize the Warning Signs	158
Maximize the Access	160
Damage, Damage, Damage	163
Turning the Tables	165
The Five Phases of Hacking	166
Creating an Attack Map	166
Building an Execution Plan	170
Establishing a Point of Entry	171
Continued and Further Access	172
The Attack	174
Defacing Web Sites	176
Social Engineering	178
Sensitive Information	178
E-Mail or Messaging Services	179

Telephones and Documents	180
Credentials	182
The Intentional “Back Door” Attack	183
Hard-Coding a Back Door Password	184
Exploiting Inherent Weaknesses in Code or Programming Environments	186
The Tools of the Trade	187
Hex Editors	187
Debuggers	189
Disassemblers	189
PE Disassembler	190
DJ Java Decompiler	190
Hackman Disassembler	191
Summary	192
Solutions Fast Track	192
Frequently Asked Questions	196
Chapter 6 Code Auditing and Reverse Engineering . .	199
Introduction	200
How to Efficiently Trace through a Program	200
Auditing and Reviewing Selected Programming Languages	203
Java	203
Java Server Pages	204
Active Server Pages	204
Server Side Includes	204
Python	204
The Tool Command Language	205
Practical Extraction and Reporting Language	205
PHP: Hypertext Preprocessor	205
C/C++	205
ColdFusion	206
Looking for Vulnerabilities	206
Getting the Data from the User	207
Looking for Buffer Overflows	208
The str★ Family of Functions	209
The strn★ Family of Functions	209
The ★scanf Family of Functions	210
Other Functions Vulnerable to Buffer Overflows	210

Checking the Output Given to the User	211
Format String Vulnerabilities	211
Cross-Site Scripting	213
Information Disclosure	214
Checking for File System Access/Interaction	215
Checking External Program and Code Execution	218
Calling External Programs	218
Dynamic Code Execution	219
External Objects/Libraries	220
Checking Structured Query Language (SQL)/Database Queries	221
Checking Networking and Communication Streams	223
Pulling It All Together	224
Summary	225
Solutions Fast Track	225
Frequently Asked Questions	226
Chapter 7 Securing Your Java Code.	227
Introduction	228
Java Versions	228
Java Runtime Environment	229
Overview of the Java Security Architecture	232
The Java Security Model	233
The Sandbox	236
Security and Java Applets	238
How Java Handles Security	241
Class Loaders	242
The Applet Class Loader	243
Adding Security to a Custom Class Loader	243
Bytecode Verifier	246
Java Protected Domains	250
Java Security Manager	251
Policy Files	252
The SecurityManager Class	258
Potential Weaknesses in Java	259
DoS Attack/Degradation of Service Attacks	260
Third-Party Trojan Horse Attacks	262

Coding Functional but Secure Java Applets	263
Message Digests	264
Digital Signatures	268
Generating a Key Pair	270
Obtaining and Verifying a Signature	272
Authentication	274
X.509 Certificate Format	275
Obtaining Digital Certificates	276
Protecting Security with JAR Signing	280
Encryption	284
Sun Microsystems Recommendations for Java Security	287
Privileged Code Guidelines	288
Java Code Guidelines	288
C Code Guidelines	289
Summary	291
Solutions Fast Track	292
Frequently Asked Questions	293
Chapter 8 Securing XML	295
Introduction	296
Defining XML	296
Logical Structure	297
Elements	298
Attributes	299
Well-Formed Documents	300
Valid Document	300
XML and XSL/DTD Documents	301
XSL Use of Templates	302
XSL Use of Patterns	302
DTD	304
Schemas	306
Creating Web Applications Using XML	307
The Risks Associated with Using XML	311
Confidentiality Concerns	312
Securing XML	313
XML Encryption	313
XML Digital Signatures	318

Summary	321
Solutions Fast Track	321
Frequently Asked Questions	323
Chapter 9 Building Safe ActiveX Internet Controls . . .	325
Introduction	326
Dangers Associated with Using ActiveX	326
Avoiding Common ActiveX Vulnerabilities	329
Lessening the Impact of ActiveX Vulnerabilities	333
Protection at the Network Level	333
Protection at the Client Level	333
Methodology for Writing Safe ActiveX Controls	337
Object Safety Settings	337
Securing ActiveX Controls	338
Control Signing	339
Using Microsoft Authenticode	340
Control Marking	342
Using Safety Settings	342
Using IobjectSafety	343
Marking the Control in the Windows Registry	346
Summary	348
Solutions Fast Track	348
Frequently Asked Questions	351
Chapter 10 Securing ColdFusion	353
Introduction	354
How Does ColdFusion Work?	355
Using the Benefit of Rapid Development	356
Understanding ColdFusion Markup Language	358
Scalable Deployment	360
Preserving ColdFusion Security	360
Secure Development	365
CFINCLUDE	365
Relative Paths	366
Queries	369
Uploaded Files	373
Denial of Service	374
Turning Off Tags	375
Secure Deployment	375

ColdFusion Application Processing	.376
Checking for Existence of Data	.376
Checking Data Types	.378
Data Evaluation	.381
Risks Associated with Using ColdFusion	.382
Using Error Handling Programs	.384
Monitor.cfm Example	.386
Summary	.390
Solutions Fast Track	.390
Frequently Asked Questions	.392

Chapter 11 Developing Security-Enabled Applications 393

Introduction	.394
The Benefits of Using Security-Enabled Applications	.394
Types of Security Used in Applications	.395
Digital Signatures	.396
Pretty Good Privacy	.397
Outlook/Outlook Express	.400
Secure Multipurpose Internet Mail Extension	.401
Secure Sockets Layer	.401
Transport Layer Security	.403
Server Authentication	.404
Client Authentication	.405
Digital Certificates	.408
Reviewing the Basics of PKI	.410
Cookies	.412
Certificate Services	.415
Using PKI to Secure Web Applications	.416
Implementing PKI in Your Web Infrastructure	.417
Microsoft Certificate Services	.417
PKI for Apache Server	.421
Testing Your Security Implementation	.422
Summary	.425
Solutions Fast Track	.426
Frequently Asked Questions	.429

Chapter 12 Cradle to Grave:
Working with a Security Plan

431

Introduction

432

Examining Your Code

433

Code Reviews

434

Peer-to-Peer Code Reviews

435

Being Aware of Code Vulnerabilities

438

Testing, Testing, Testing

439

Using Common Sense when Coding

442

Planning

442

Coding Standards

443

Header Comments

443

Variable Declaration Comments

444

The Tools

444

Rule-Based Analyzers

444

Debugging and Error Handling

445

Version Control and Source Code Tracking

446

Visual SourceSafe

446

StarTeam

447

Creating a Security Plan

448

Security Planning at the Network Level

449

Security Planning at the Application Level

450

Security Planning at the Desktop Level

450

Web Application Security Process

451

Summary

453

Solutions Fast Track

454

Frequently Asked Questions

455

Index

457