

Contents

Chapter 1 Google Searching Basics	1
Introduction	2
Exploring Google’s Web-based Interface	2
Google’s Web Search Page	2
Google Web Results Page	4
Google Groups	6
Google Image Search	7
Google Preferences	8
Language Tools	11
Building Google Queries	13
The Golden Rules of Google Searching	13
Basic Searching	15
Using Boolean Operators and Special Characters	16
Search Reduction	18
Working With Google URLs	22
URL Syntax	23
Special Characters	23
Putting the Pieces Together	24
Summary	44
Solutions Fast Track	44
Links to Sites	45
Frequently Asked Questions	46
Chapter 2 Advanced Operators	49
Introduction	50
Operator Syntax	51
Troubleshooting Your Syntax	52
Introducing Google’s Advanced Operators	53
Intitle and Allintitle: Search Within the Title of a Page	54
Allintext: Locate a String Within the Text of a Page	57
Inurl and Allinurl: Finding Text in a URL	57
Site: Narrow Search to Specific Sites	59
Filetype: Search for Files of a Specific Type	61
Link: Search for Links to a Page	65

Inanchor: Locate Text Within Link Text 68

Cache: Show the Cached Version of a Page 69

Numrange: Search for a Number 69

Daterange: Search for Pages
 Published Within a Certain Date Range 70

Info: Show Google’s Summary Information 71

Related: Show Related Sites 72

Author: Search Groups
 for an Author of a Newsgroup Post 72

Group: Search Group Titles 75

Insubject: Search Google Groups Subject Lines 75

Msgid: Locate a Group Post by Message ID 76

Stocks: Search for Stock Information 77

Define: Show the Definition of a Term 78

Phonebook: Search Phone Listings 79

Colliding Operators and Bad Search-Fu 81

Summary 86

Solutions Fast Track 86

Links to Sites 90

Frequently Asked Questions 91

Chapter 3 Google Hacking Basics 93

Introduction 94

Anonymity with Caches 94

Directory Listings 100

 Locating Directory Listings 101

 Finding Specific Directories 102

 Finding Specific Files 103

 Server Versioning 103

Going Out on a Limb: Traversal Techniques 110

 Directory Traversal 110

 Incremental Substitution 112

 Extension Walking 112

Summary 116

Solutions Fast Track 116

Links to Sites 118

Frequently Asked Questions 118

Chapter 4 Document Grinding and Database Digging . 121

Introduction	122
Configuration Files	123
Log Files	130
Office Documents	133
Database Digging	134
Login Portals	135
Support Files	137
Error Messages	139
Database Dumps	147
Actual Database Files	149
Automated Grinding	150
Google Desktop Search	153
Summary	156
Solutions Fast Track	156
Links to Sites	157
Frequently Asked Questions	158

Chapter 5 Google’s Part in an Information Collection Framework 161

Introduction	162
The Principles of Automating Searches	162
The Original Search Term	165
Expanding Search Terms	166
E-mail Addresses	166
Telephone Numbers	168
People	169
Getting Lots of Results	170
More Combinations	171
Using “Special” Operators	172
Getting the Data From the Source	173
Scraping it Yourself—Requesting and Receiving Responses	173
Scraping it Yourself – The Butcher Shop	179
Dapper	184
Aura/EvilAPI	184
Using Other Search Engines	185
Parsing the Data	186

Parsing E-mail Addresses	186
Domains and Sub-domains	190
Telephone Numbers	191
Post Processing	193
Sorting Results by Relevance	193
Beyond Snippets	195
Presenting Results	196
Applications of Data Mining	196
Mildly Amusing	196
Most Interesting	199
Taking It One Step Further	209
Collecting Search Terms	212
On the Web	212
Spying on Your Own	214
Search Terms	214
Gmail	217
Honey Words	219
Referrals	221
Summary	222
Chapter 6 Locating Exploits and Finding Targets	223
Introduction	224
Locating Exploit Code	224
Locating Public Exploit Sites	224
Locating Exploits Via Common Code Strings	226
Locating Code with Google Code Search	227
Locating Malware and Executables	230
Locating Vulnerable Targets	234
Locating Targets Via Demonstration Pages	235
Locating Targets Via Source Code	238
Locating Targets Via CGI Scanning	257
Summary	260
Solutions Fast Track	260
Links to Sites	261
Frequently Asked Questions	262
Chapter 7 Ten Simple Security Searches That Work . . .	263
Introduction	264

site	.264
intitle:index.of	.265
error warning	.265
login logon	.267
username userid employee.ID “your username is”	.268
password passcode “your password is”	.268
admin administrator	.269
–ext:html –ext:htm –ext:shtml –ext:asp –ext:php	.271
inurl:temp inurl:tmp inurl:backup inurl:bak	.275
intranet help.desk	.275
Summary	.277
Solutions Fast Track	.277
Frequently Asked Questions	.279

Chapter 8 Tracking Down Web Servers, Login Portals, and Network Hardware 281

Introduction	.282
Locating and Profiling Web Servers	.282
Directory Listings	.283
Web Server Software Error Messages	.284
Microsoft IIS	.284
Apache Web Server	.288
Application Software Error Messages	.296
Default Pages	.299
Default Documentation	.304
Sample Programs	.307
Locating Login Portals	.309
Using and Locating Various Web Utilities	.321
Targeting Web-Enabled Network Devices	.326
Locating Various Network Reports	.327
Locating Network Hardware	.330
Summary	.340
Solutions Fast Track	.340
Frequently Asked Questions	.342

Chapter 9 Usernames, Passwords, and Secret Stuff, Oh My!	345
Introduction	346
Searching for Usernames	346
Searching for Passwords	352
Searching for Credit Card Numbers, Social Security Numbers, and More	361
Social Security Numbers	363
Personal Financial Data	363
Searching for Other Juicy Info	365
Summary	369
Solutions Fast Track	369
Frequently Asked Questions	370
Chapter 10 Hacking Google Services	373
AJAX Search API	374
Embedding Google AJAX Search API	375
Deeper into the AJAX Search	379
Hacking into the AJAX Search Engine	384
Calendar	389
Blogger and Google's Blog Search	392
Google Splogger	393
Signaling Alerts	402
Google Co-op	404
Google AJAX Search API Integration	409
Google Code	410
Brief Introduction to SVN	411
Getting the files online	412
Searching the Code	414
Chapter 11 Google Hacking Showcase	419
Introduction	420
Geek Stuff	421
Utilities	421
Open Network Devices	424
Open Applications	432
Cameras	438
Telco Gear	446
Power	451

Sensitive Info	455
Police Reports	461
Social Security Numbers	464
Credit Card Information	469
Beyond Google	472
Summary	477
Chapter 12 Protecting Yourself from Google Hackers. .	479
Introduction	480
A Good, Solid Security Policy	480
Web Server Safeguards	481
Directory Listings and Missing Index Files	481
Robots.txt: Preventing Caching	482
NOARCHIVE: The Cache “Killer”	485
NOSNIPPET: Getting Rid of Snippets	485
Password-Protection Mechanisms	485
Software Default Settings and Programs	487
Hacking Your Own Site	488
Site Yourself	489
Gooscan	489
Installing Gooscan	490
Gooscan’s Options	490
Gooscan’s Data Files	492
Using Gooscan	494
Windows Tools and the .NET Framework	499
Athena	500
Using Athena’s Config Files	502
Constructing Athena Config Files	503
Wikto	505
Google Rower	508
Google Site Indexer	510
Advanced Dork	512
Getting Help from Google	515
Summary	517
Solutions Fast Track	517
Links to Sites	518
Frequently Asked Questions	519
Index	521

