

Inhaltsverzeichnis

	Danksagungen	11
	Über den Autor	15
I	Einfache Suche mit Google	19
1.1	Einführung.....	19
1.2	Einführung in die Web-Schnittstelle von Google.....	20
1.2.1	Die Google-Suchseite im Web.....	20
1.2.2	Google-Web-Ergebnisseite.....	21
1.2.3	Google Groups.....	23
1.2.4	Google-Bildersuche.....	24
1.2.5	Google-Einstellungen.....	25
1.2.6	Sprachtools.....	28
1.3	Google-Suchen formulieren.....	30
1.3.1	Die Goldenen Regeln der Google-Suche.....	31
1.3.2	Grundlegende Suche.....	33
1.3.3	Nutzen von Booleschen Operatoren und Sonderzeichen....	34
1.3.4	Eingrenzen der Suche.....	36
1.4	Wie man mit Google-URLs arbeitet.....	40
1.4.1	URL-Syntax.....	41
1.4.2	Sonderzeichen.....	41
1.4.3	Kombinieren.....	42
1.5	Zusammenfassung.....	60
1.6	Lösungen im Schnellüberblick.....	61
1.7	Links für Sites.....	62
1.8	FAQ.....	62
2	Erweiterte Operatoren	65
2.1	Einführung.....	65
2.2	Syntax der Operatoren.....	66
2.2.1	Syntax-Troubleshooting.....	67
2.3	Einführung in die erweiterten Operatoren von Google.....	69
2.3.1	intitle und allintitle: Suchen innerhalb des Seitentitels....	69
2.3.2	allintext: Findet einen String im Seitentext.....	72
2.3.3	inurl und allinurl: Finden Text in einer URL.....	72
2.3.4	site: Eingrenzung der Suche auf bestimmte Sites.....	74

2.3.5	filetype: Suche nach Dateien eines bestimmten Dateityps . . .	76
2.3.6	link: Suche nach Links zu einer Seite	81
2.3.7	inanchor: Text innerhalb des Linktextes finden	84
2.3.8	cache: Zeigt die gecachte Version einer Seite	84
2.3.9	numrange: Die Suche nach einer Zahl	85
2.3.10	daterange: Suche nach Seiten, die innerhalb eines bestimmten Zeitraums veröffentlicht wurden	85
2.3.11	info: Google-Zusammenfassung anzeigen lassen	86
2.3.12	related: Verwandte Sites zeigen	87
2.3.13	author: Durchsucht Groups nach dem Autor einer Newsgroup-Veröffentlichung	88
2.3.14	group: Suche in Gruppentiteln	90
2.3.15	insubject: Suche nach Begriffen in den Betreffzeilen der Groups	91
2.3.16	msgid: Findet eine Groups-Veröffentlichung anhand der Nachrichten-ID	91
2.3.17	stocks: Findet Informationen zu Aktienkursen	93
2.3.18	define: Zeigt die Definition eines Begriffs	94
2.3.19	phonebook: Suche in Telefonbucheinträgen	94
2.4	Kollidierende Operatoren und schlechtes Such-Fu	97
2.5	Zusammenfassung	101
2.6	Lösungen im Schnellüberblick	102
2.7	Links für Sites	104
2.8	FAQ	105
3	Grundtechniken des Google-Hackings	107
3.1	Einführung	107
3.2	Anonymität mit dem Cache	108
3.3	Verzeichnislisten	114
3.3.1	Verzeichnislisten aufspüren	115
3.3.2	Bestimmte Verzeichnisse finden	116
3.3.3	Bestimmte Dateien finden	117
3.3.4	Serverversion ermitteln	118
3.4	Hangeln Sie sich von Ast zu Ast: Traversal-Techniken	125
3.4.1	Verzeichnis-Traversal	125
3.4.2	Inkrementale Substitution	127
3.4.3	Spaß mit Erweiterungen	128
3.5	Zusammenfassung	131
3.6	Lösungen im Schnellüberblick	131
3.7	Site Links	133
3.8	FAQ	134

4	Dokumente analysieren und Datenbanken erforschen	135
4.1	Einführung.	135
4.2	Konfigurationsdateien.	136
4.3	Logfiles	143
	4.3.1 Office-Dokumente	146
4.4	Datenbanken erforschen.	148
	4.4.1 Login-Portale.	148
	4.4.2 Support-Dateien	151
	4.4.3 Fehlermeldungen.	153
	4.4.4 Datenbank-Auszüge.	160
	4.4.5 Tatsächliche Datenbankdateien	161
4.5	Automatische Analyse.	163
4.6	Die Suche mit Google Desktop	167
4.7	Zusammenfassung	168
4.8	Lösungen im Schnellüberblick.	169
4.9	Links für Sites	170
4.10	FAQ	170
5	Google als Framework zur Informationssammlung	173
5.1	Einführung.	173
5.2	Grundlegendes zur Automatisierung von Suchen	174
	5.2.1 Der ursprüngliche Suchbegriff	177
	5.2.2 Suchbegriffe erweitern.	177
	5.2.3 Scraping – Die Daten von der Quelle abholen.	185
	5.2.4 Daten untersuchen.	200
	5.2.5 Nachbearbeitung	208
5.3	Data-Mining-Anwendungen.	212
	5.3.1 Amüsant	212
	5.3.2 Höchst interessant	215
5.4	Suchbegriffe sammeln	229
	5.4.1 Im Web	229
	5.4.2 Spionieren.	231
	5.4.3 Honig	237
	5.4.4 Referrals	238
5.5	Zusammenfassung	239
6	Angriffe und Ziele finden.	241
6.1	Einführung.	241
6.2	Angriffscode aufspüren	241
	6.2.1 Sites mit öffentlichem Angriffscode aufspüren.	242

6.3	Angriffe über gängige Code-Strings aufspüren.	243
6.4	Code mithilfe der Google-Codesuche aufspüren	245
6.5	Malware und ausführbare Dateien finden.	248
6.6	Angreifbare Ziele finden.	253
6.6.1	Ziele anhand von Demonstrationsseiten aufspüren	253
6.6.2	Ziele über den Quellcode aufspüren.	256
6.6.3	Ziele mithilfe von CGI-Scans entdecken	275
6.7	Zusammenfassung	277
6.8	Lösungen im Schnellüberblick.	278
6.9	Links für Sites	279
6.10	FAQ.	279
7	10 einfache Sicherheitsabfragen, die funktionieren	281
7.1	Einführung.	281
7.2	site	282
7.3	intitle:index.of	283
7.4	error warning	283
7.5	login logon	285
7.6	username userid employee.ID "your username is"	286
7.7	password passcode "your password is"	287
7.8	admin administrator	288
7.9	-ext:html -ext:htm -ext:shtml -ext:asp -ext:php	290
7.10	inurl:temp inurl:tmp inurl:backup inurl:bak.	293
7.11	intranet help.desk	294
7.12	Zusammenfassung	295
7.13	Lösungen im Schnellüberblick.	295
7.14	FAQ.	297
8	Webserver, Login-Portale und Netzwerkhardware aufspüren	299
8.1	Einführung.	299
8.2	Webserver aufspüren und analysieren.	300
8.2.1	Verzeichnislisten	301
8.2.2	Fehlermeldungen der Webserver-Software	302
8.2.3	Fehlermeldungen der Anwendungssoftware.	315
8.2.4	Standardseiten	318
8.2.5	Standarddokumentation	323
8.2.6	Beispielprogramme	325
8.3	Login-Portale aufspüren	327
8.3.1	Verschiedene Web-Utilities aufspüren und nutzen.	339

8.4	Web-aktivierte Netzwerk-Devices als Ziel	344
8.5	Netzwerkberichte aufspüren	345
8.6	Netzwerkhardware aufspüren	348
8.7	Zusammenfassung	357
8.8	Lösungen im Schnellüberblick.	358
8.9	FAQ	359
9	Benutzername, Passwörter und allerlei Geheimnisse – Spannend! . .	363
9.1	Einführung.	363
9.2	Die Suche nach Benutzernamen	364
9.3	Die Suche nach Passwörtern	369
9.4	Die Suche nach Kreditkartennummern, Sozialversicherungsnummern und mehr	378
	9.4.1 Sozialversicherungsnummern	381
	9.4.2 Persönliche Finanzdaten	381
9.5	Die Suche nach allerlei sonstigen Leckerbissen	382
9.6	Zusammenfassung	386
9.7	Lösungen im Schnellüberblick.	387
9.8	FAQ	388
10	Der Angriff auf Google-Services.	389
10.1	AJAX Search-API.	389
	10.1.1 Integrieren der Google AJAX-Search-API	391
	10.1.2 Weiter mit AJAX-Search	395
	10.1.3 Der große AJAX-Suchmaschinen-Hack	400
10.2	Kalender	405
10.3	Blogger und Googles Blog-Suche.	408
	10.3.1 Google-Splogger	410
10.4	Alerts signalisieren	419
10.5	Google Co-op	421
	10.5.1 Integration der Google AJAX-Search-API	426
10.6	Google Code.	427
	10.6.1 Eine kurze Einführung in SVN	428
	10.6.2 Online mit den Dateien	430
	10.6.3 Den Code durchsuchen	432
11	Die Google-Hacking-Show	437
11.1	Einführung.	437
11.2	Für die Freaks	438
	11.2.1 Utilities	438

II.2.2	Offene Netzwerk-Devices	442
II.2.3	Offene Anwendungen	450
II.3	Kameras	455
II.4	Telekommunikationsanlagen	463
II.5	Strom	469
II.6	Sensible Daten	473
II.6.I	Polizeiberichte	479
II.7	Sozialversicherungsnummern	481
II.7.I	Kreditkartendaten	486
II.8	Jenseits von Google	489
II.9	Zusammenfassung	494
12	Wie man sich vor Google-Hackern schützt	495
12.1	Einführung	495
12.2	Eine gute, robuste, Sicherheitsrichtlinie	496
12.3	Webserver-Schutzmechanismen	496
12.3.1	Verzeichnislisten und fehlende Indexdateien	497
12.3.2	Robots.txt: Wie man das Caching vermeidet	498
12.3.3	NOARCHIVE: Der Cache-»Killer«	501
12.3.4	NOSNIPPET: Wie man Snippets loswird	501
12.3.5	Passwortschutzmechanismen	502
12.3.6	Standardeinstellungen bei Software und Programmen	503
12.4	Wie Sie Ihre eigene Site hacken	505
12.4.1	Suchen Sie die eigene Site	505
12.4.2	Gooscan	506
12.4.3	Windows Tools und das .NET-Framework	516
12.4.4	Athena	517
12.4.5	Wikto	523
12.4.6	Google Rower	526
12.4.7	Google Site Indexer	528
12.4.8	Advanced Dork	530
12.5	Wie Sie Hilfe von Google bekommen	533
12.6	Zusammenfassung	534
12.7	Lösungen im Schnellüberblick	535
12.8	Links für Sites	536
12.9	FAQ	537
	Stichwortverzeichnis	539