

Inhalt

Vorwort	IX
1 Sicherheitsprobleme im Internet und deren Folgen	1
1.1 Sicherheitsprobleme auf kleinen Webseiten	1
1.2 Sicherheitsprobleme auf großen Plattformen	3
1.2.1 Mangelhafte Verschlüsselung und Authentifizierung im WhatsApp-Messenger	3
1.2.2 Die Facebook-Neujahrspanne 2012/2013	4
1.2.3 Der Hack des Facebook-Profiles von Mark Zuckerberg	4
1.3 Sicherheitsprobleme mit großen Folgen für die Nutzer	5
1.3.1 Angriff auf das Playstation Network	6
1.3.2 Datendiebstahl bei Vodafone	6
2 Grundlagen	7
2.1 Die Macht der Fantasie	7
2.1.1 Anwendungsbeispiel: Zugang zu einem Content-Management-System	7
2.1.2 Seiten- und Servicenamen erraten	10
2.2 Code-Injection	12
2.3 Physischer und virtueller Zugang	14
3 Passwörter knacken: eine Frage von Sekunden?	15
3.1 Brute Force – einfach, aber effektiv	15
3.1.1 Passwörter mit bekannter Länge	15
3.1.2 Passwörter mit unbekannter Länge	16
3.1.3 Das Problem des Flaschenhalses	18
3.1.4 Partitionierung des Alphabets	19
3.1.5 Informationen über ein Passwort	20
3.2 Die Arbeit mit Passwort-Listen	22
3.2.1 Credential Recycling	22
3.2.2 Reverse-Brute-Force-Angriffe	25

3.3	Verschlüsselte Passwörter knacken	25
3.3.1	Wie werden Passwörter gespeichert?	26
3.3.2	Brute-Force Attacke auf Hashwerte	27
3.3.3	Rainbow-Tables	28
3.4	Den Aufwand verteilen	29
3.4.1	Wann ist eine Aufteilung sinnvoll?	30
3.4.1.1	Verteilung auf mehrere Prozessoren	30
3.4.1.2	Verteilung zwischen physikalischen Computern	32
3.4.2	Organisation der beteiligten Rechner	34
3.4.2.1	Client-Server-Prinzip	34
3.4.2.2	Dezentrale Kommunikation	36
3.4.2.2.1	Vollständig vermaschtes Netz	36
3.4.2.2.2	Ringtopologie	37
3.4.3	Eine sinnvolle Aufteilung	38
3.5	Timeouts, Captchas und Co.	44
3.5.1	Die Sicherheitsfrage	45
3.5.2	Timeouts	46
3.5.3	Captchas	48
4	Der Entwurf sicherer Authentifikationssysteme	53
4.1	Die Benutzername-Passwort-Authentifizierung	53
4.1.1	Anforderungen an Passwörter	54
4.1.2	Speichern von Passwörtern	58
4.1.2.1	Hashing	59
4.1.2.2	Kryptografische Verfahren	61
4.1.3	Speicherung von Benutzerdaten	61
4.1.3.1	Benutzerdaten mit globalem Schlüssel speichern	63
4.1.3.2	Benutzerdaten mit benutzerspezifischem Schlüssel speichern	64
4.2	Weitere Authentifikationskonzepte	67
4.2.1	Passwortschutz einzelner Seiten	67
4.2.2	E-Mail-Versand benutzerdefinierter Links	68
4.2.3	Sicherheitsfragen	69
4.2.4	Authentifikation mit Systemeigenschaften als Passwort	69
4.3	Generelle Sicherheitshinweise	70
4.3.1	Brute-Force-Attacken verhindern	70
4.3.2	Wenn möglich, sichere Verbindungen nutzen	73
5	SQL-Injection: Zugriff auf die Datenbank	75
5.1	Was ist SQL?	75
5.1.1	Das relationale Datenbankkonzept	76
5.1.2	SQL-Befehlssyntax	77
5.1.2.1	Daten abfragen mittels SELECT	77

5.1.2.2	Bestehende Datensätze mittels UPDATE ändern	78
5.1.2.3	Neue Datensätze in eine Tabelle einfügen – INSERT	78
5.1.2.4	DELETE: Werte aus einer Tabelle löschen	78
5.1.2.5	Ganze Tabellen löschen – DROP	79
5.2	SQL-Code einschleusen	79
5.3	SQL-Injection erfolgreich verhindern	85
5.3.1	Rechte des Datenbankbenutzers	86
5.3.2	Prepared Statements	87
6	Cross-Site-Scripting (XSS)	89
6.1	Motive des Cross-Site-Scriptings	89
6.2	Varianten des Cross-Site-Scriptings	90
6.2.1	Reflektiertes Cross-Site-Scripting	90
6.2.2	Persistentes Cross-Site-Scripting	94
6.2.3	Clientseitiges Cross-Site-Scripting	95
6.2.4	Angriffe durch Suchmaschinen und andere Personen auslösen	96
6.3	Cross-Site-Tracing	98
6.4	Cross-Site-Scripting verhindern	100
7	Denial-of-Service-Attacken (DoS)	103
7.1	Maßnahmen gegen DoS-Attacken	104
7.1.1	DoS-Attacken erkennen	104
7.1.2	Die Performance von PHP-Programmen steigern	105
7.1.2.1	Sinnvolle Anordnung von Anweisungen	106
7.1.2.2	Ergebnisse von Berechnungen wiederverwenden	106
7.1.2.3	Keine unnötigen Vergleiche oder unnötiges Kopieren von Variablen	109
7.1.2.4	Stringoperationen	110
7.1.2.5	Einsatz des ternären Operators	111
7.1.3	Kritische Aufrufe cachen	111
7.2	Fortgeschrittene DoS-Angriffe	113
7.2.1	Reflektierte DoS-Attacken	114
7.2.2	SYN-Flooding	114
8	Phishing	117
8.1	Phishing-Techniken	117
8.1.1	Phishing via E-Mail	118
8.1.2	Phishing in sozialen Netzwerken	119
8.1.3	Phishing durch Spam-Kommentare auf Webseiten	120
8.1.4	Phishing durch Cross-Site-Scripting	120
8.2	Phishing verhindern	121
8.2.1	Login über externe Webseiten verhindern	121
8.2.2	Phishing durch Spam-Kommentare verhindern	123

9	Social Engineering	125
9.1	Die Geschichte von Kevin Mitnick	125
9.2	Muster und Ziele des Social Engineerings	126
9.2.1	Social Engineering in sozialen Netzwerken und auf Online-Dating-Plattformen	127
9.2.2	Dumpster Diving	128
9.3	Abwehr von Social Engineering	129
9.3.1	Generelle Maßnahmen gegen Social Engineering	129
9.3.2	Technische Maßnahmen gegen Social Engineering	129
10	Kryptografie, Protokolle und fortgeschrittene Hacking-Technologien	133
10.1	Sessions	133
10.1.1	Die Funktionsweise von Sessions	133
10.1.2	Session Hijacking	136
10.1.2.1	TCP-Session Hijacking	136
10.1.2.2	Web-Session Hijacking	137
10.1.3	Session Fixation	137
10.2	Kryptografische Verfahren	139
10.2.1	Symmetrische Verschlüsselung	139
10.2.1.1	Substitutionschiffren	139
10.2.1.2	Permutationsverfahren	140
10.2.1.3	Moderne Blockverschlüsselungsverfahren – der AES	141
10.2.2	Asymmetrische Verschlüsselung	147
10.3	Das TLS/SSL-Protokoll	150
10.4	Geheimdienste und ihre Methoden und Möglichkeiten	151
10.4.1	DNS-Spoofing	151
10.4.1.1	Das Domain Name System	151
10.4.1.2	Angriffsmöglichkeiten auf die Namensauflösung	152
10.4.1.2.1	Änderung der hosts-Datei	152
10.4.1.3	DNS-Spoofing durch einen Provider (DNS-Injection)	153
10.4.1.3.1	Temporäres DNS-Spoofing	153
10.4.2	Abhören von Kommunikation im Internet	154
10.5	Grundlegende Low-Level-Hacking-Techniken	156
10.5.1	Simple Programmierfehler: Off-by-One-Fehler	156
10.5.2	Buffer-Overflows	157
11	Exkurs A: Alphabet zum Knacken eines Passwortes	161
12	Exkurs B: Bäume, Listen und Graphen	163
12.1	Verkettete Listen	163
12.2	Binärbäume	165
12.3	Graphen	169

13	Exkurs C: Netzwerkprogrammierung – Grundlagen mit C/C++ ..	173
14	Exkurs D: Rasteralgorithmus (Brute-Force-Attacke)	179
14.1	Ein festes Raster	179
14.2	Statistische Partitionierung des Lösungsraums	180
15	Exkurs E: Die grundlegende Funktionsweise eines Prozessors ..	193
15.1	Aufbau eines Prozessors	193
15.2	Der Befehlssatz eines Prozessors	196
Index	197