

Inhalt

Einleitung	1
Die Leser	2
Die Regeln	3
Die Beispiele	4
Die Kapitel	5
Was ist nicht in diesem Buch?	6
Anmerkung des Autors	7
Leserkommentare	7
1 Die Grundlagen	9
1.1 HTTP	9
1.1.1 Anfragen und Antworten	10
1.1.2 Der Referer-Header	14
1.1.3 Caching	15
1.1.4 Cookies	17
1.2 Sessions	18
1.2.1 Session-Hijacking	20
1.3 HTTPS	24
1.4 Zusammenfassung	28
1.5 Lesenswerte Literatur	28
2 Übermittlung von Daten an Subsysteme	29
2.1 SQL-Injection	30
2.1.1 Beispiele, Beispiele und nochmals Beispiele	30
2.1.2 Informationen aus Fehlermeldungen	39
2.1.3 SQL-Injection vermeiden	41
2.2 Shell-Command-Injection	48
2.2.1 Beispiele	48
2.2.2 Shell-Command-Injection vermeiden	51
2.3 Kommunikation mit C/C++-Programmen	57
2.3.1 Beispiel	58
2.4 Das schlimme Eval	59
2.5 Lösung von Metazeichenproblemen	60
2.5.1 Mehrschichtige Interpretation	62
2.5.2 Architektur	62
2.5.3 Gestaffelte Abwehr	63
2.6 Zusammenfassung	65

3	Benutzereingaben	67
3.1	Was sind eigentlich Eingaben?	67
3.1.1	Die unsichtbare Sicherheitsbarriere	72
3.1.2	Spracheigenarten: Völlig unerwartete Eingaben	75
3.2	Eingaben validieren	77
3.2.1	Whitelisting oder Blacklisting	82
3.3	Ungültige Eingaben behandeln	85
3.3.1	Protokollierung	87
3.4	Die Gefahren clientseitiger Validierung	90
3.5	Autorisierungsprobleme	94
3.5.1	Indirekter Zugriff auf Daten	96
3.5.2	Übermittlung zu vieler Daten an den Client	98
3.5.3	Fehlende Autorisierungstests	103
3.5.4	Autorisierung durch Verschleierung (»Authorization by Obscurity«)	104
3.6	Servererzeugte Eingaben schützen	105
3.7	Zusammenfassung	109
4	Ausgabebehandlung: Das Cross-Site-Scripting-Problem	111
4.1	Beispiele	111
4.1.1	Session-Hijacking	113
4.1.2	Textmodifizierung	117
4.1.3	Cross-Site-Scripting kombiniert mit Social-Engineering	118
4.1.4	Diebstahl von Passwörtern	122
4.1.5	Zu kurz für Skripte?	124
4.2	Das Problem	126
4.3	Die Lösung	127
4.3.1	HTML-Kodierung	129
4.3.2	Selektive Tag-Filterung	130
4.3.3	Programmdesign	135
4.4	Browser-Zeichensätze	136
4.5	Zusammenfassung	138
4.6	Lesenswerte Literatur	138
5	Web-Trojaner	139
5.1	Beispiele	139
5.2	Das Problem	144
5.3	Eine Lösung	145
5.4	Zusammenfassung	147
6	Passwörter und andere Geheimnisse	149
6.1	Kryptozeug	149
6.1.1	Symmetrische Verschlüsselung	151
6.1.2	Asymmetrische Verschlüsselung	152
6.1.3	Message Digests	153

6.1.4	Digitale Signaturen	154
6.1.5	Public-Key-Zertifikate	155
6.2	Passwortbasierte Authentifizierung	157
6.2.1	Klartextpasswörter	157
6.2.2	Verlorene Passwörter	160
6.2.3	Gehashte Passwörter knacken	161
6.2.4	Automatische Anmeldung	166
6.3	Geheime Kennungen	167
6.4	Durchsickern von Geheimnissen	170
6.4.1	Durchlässigkeit durch GET-Anfragen	171
6.4.2	Fehlende Verschlüsselung	173
6.5	Verfügbarkeit serverseitiger Codes	174
6.5.1	Unsichere Dateinamen	174
6.5.2	Systemsoftware-Bugs	176
6.6	Zusammenfassung	177
6.7	Lesenswerte Literatur	178
7	Feinde des sicheren Codes	181
7.1	Ignoranz	181
7.2	Unordnung	183
7.3	Deadlines	190
7.4	Vertriebsleute	192
7.5	Schlussbemerkungen	193
7.6	Lesenswerte Literatur	194
8	Die Regeln für sichere Programmierung im Überblick	195
A	Bugs im Webserver	203
B	Paket-Sniffing	209
B.1	Lerne TCP/IP in fünf Minuten	209
B.2	Pakete ausschnüffeln	211
B.3	Man-in-the-Middle-Attacken	212
B.4	MITM mit HTTPS	213
B.5	Zusammenfassung	214
B.6	Lesenswerte Literatur	215
C	HTML-formatierte E-Mails mit gefälschter Absenderadresse senden	217
D	Weitere Informationen	219
D.1	Mailinglisten	219
D.2	OWASP	221
	Abkürzungsverzeichnis	223
	Literaturverzeichnis	225
	Index	233