

# Inhaltsverzeichnis

	<b>Einleitung</b> . . . . .	11
<b>1</b>	<b>Sicherheit im Kontext von PHP und Webanwendungen</b> . . . . .	17
1.1	Historie: PHP . . . . .	17
1.2	PHP heute . . . . .	19
1.3	PHP und Apache . . . . .	20
1.4	PHP als eigenständige Anwendung . . . . .	21
1.5	PHP mit alternativen Webservern . . . . .	22
1.6	Sicherheitskonzepte für Webanwendungen . . . . .	22
<b>2</b>	<b>Fehlerquellen, die jeder PHP-Entwickler kennen sollte</b> . . . . .	29
2.1	Variablenverfügbarkeit . . . . .	29
2.2	Superglobale Arrays . . . . .	35
2.3	Zugriff auf Uploads . . . . .	37
2.4	Verzeichnisindizierung und Suchmaschinen . . . . .	38
2.5	Index- und Default-Dateien . . . . .	40
<b>3</b>	<b>PHP und Dateien: Die häufigsten Fehler</b> . . . . .	43
3.1	Temporäre Dateien . . . . .	43
3.1.1	Backup-Dateien, Versionsverwaltung und Zugriffsschutz . . . . .	44
3.2	Sessions: Permissive Konfiguration oder »Alles ist erlaubt« . . . . .	52
3.2.1	Session-IDs nur durch Server vergeben . . . . .	54
3.2.2	Regenerierung der Session-ID bei sensitiven Aktionen . . . . .	55
3.2.3	Absicherung durch TAN . . . . .	56
3.3	Globaler Dateisystemzugriff . . . . .	57
3.4	Auslieferung von Dateien . . . . .	65
3.5	Include-Dateien . . . . .	67
3.5.1	Ungeparste Dateiendung . . . . .	67
3.5.2	Dateien in öffentlich zugänglichem Verzeichnis . . . . .	71
3.5.3	Externe Dateien und include . . . . .	76

<b>4</b>	<b>Sensitive Daten richtig behandeln</b>	<b>83</b>
4.1	Grundsatzprobleme	83
4.1.1	Falsche Request-Methode	83
4.1.2	Fehlerhafte Verarbeitung	86
4.1.3	Fehlerhafte SQL-Verwertung	90
4.1.4	Zwischenspeicherung von Sessions und Cookies	91
4.1.5	Cross Site Scripting	92
4.2	Lösungsansätze	97
4.2.1	Hash-Austausch via AJAX	98
4.2.2	Vermeidung von unsicheren Passwörtern	108
4.2.3	Vergessene Passwörter	116
4.2.4	Nur notwendige Daten übermitteln	123
4.2.5	Datenprüfung	125
<b>5</b>	<b>Sessions</b>	<b>135</b>
5.1	Flexibilität	135
5.2	Strikte Erzeugung	141
5.3	Gültigkeit	151
5.4	Session-Umgebung sichern	154
5.4.1	Clientüberprüfung	154
5.4.2	Ausschließlich Cookies verwenden	157
5.4.3	Session-ID aus dem Referrer entfernen	158
5.4.4	Zugriff auf Session-Dateien	159
5.4.5	TAN-System	160
5.5	Speicherung	165
5.5.1	files	165
5.5.2	mm	167
5.5.3	user	168
5.6	Sessions und Frames	181
<b>6</b>	<b>Upload und Download</b>	<b>183</b>
6.1	Upload und PHP	183
6.1.1	Uploads beschränken	185
6.2	Uploads prüfen	199
6.2.1	Prüfen von Bilddateien	199
6.2.2	Dateityp feststellen	203
6.2.3	Dateiarchive	204
6.3	Download und PHP	205
6.3.1	Throttling	205
6.3.2	Referenzierung	210

<b>7</b>	<b>Dateisystemzugriffe</b> .....	217
7.1	Wie greift PHP auf Dateien zu? .....	217
7.1.1	Verschlüsselung .....	218
7.1.2	Verschleierung .....	220
7.1.3	Skripte schützen .....	222
7.2	Angriff auf dateibasierte Webanwendungen .....	224
7.2.1	Vollständiges Auslesen .....	225
7.2.2	Direkte Ausgabe .....	228
7.2.3	Zeilen/-blockweises Auslesen .....	229
7.2.4	Vollständiges Speichern .....	229
7.2.5	Blockweises Speichern .....	230
7.3	Pfade und ihre Tücken .....	230
7.4	Dateiangaben als Parameter .....	237
7.4.1	include, include_once, require und require_once .....	237
7.4.2	Datendateien auslesen .....	241
7.4.3	Dateisystemoperationen .....	242
7.4.4	Prozesse ausführen .....	244
7.4.5	dl: Module nachladen .....	247
7.5	Thread- und Binär-Sicherheit .....	248
<b>8</b>	<b>SSL</b> .....	251
8.1	Allgemeine Hinweise .....	252
8.2	OpenSSL-Installation .....	253
8.2.1	Installation unter Linux und Unix (Sourcen) .....	253
8.2.2	Installation unter Linux (Paket) .....	254
8.2.3	Installation unter Windows .....	254
8.2.4	Konfiguration .....	254
8.3	Erzeugung eines Zertifikats .....	255
8.4	Ein eigenes Zertifikat .....	257
8.4.1	Erzeugung einer CA .....	258
8.4.2	Das eigene Zertifikat erstellen .....	259
8.5	Zertifikat in den Webserver integrieren .....	261
8.5.1	Apache-Webserver .....	261
8.5.2	Roxen Webserver .....	262
8.5.3	Microsoft Internet Information Server (IIS) .....	262
8.6	SSL zur Authentifizierung nutzen .....	266
8.6.1	Apache-Webserver .....	267
8.6.2	Roxen Webserver .....	272

8.6.3	Microsoft Internet Information Server (IIS) . . . . .	272
8.6.4	Import der Zertifikate mit dem Mozilla Firefox . . . . .	273
8.6.5	Import der Zertifikate mit dem Internet Explorer . . . . .	274
8.7	SSL-Funktionen in PHP . . . . .	274
8.7.1	OpenSSL für PHP aktivieren . . . . .	275
8.7.2	Zertifikatzugriff unter dem Apache-Webserver. . . . .	276
8.7.3	Zertifikatzugriff unter dem Microsoft Internet Information Server (IIS) . . . . .	277
<b>9</b>	<b>Konfiguration: PHP</b> . . . . .	<b>279</b>
9.1	php.ini. . . . .	279
9.2	Safe Mode. . . . .	280
9.3	Basisverzeichnis mit open_basedir . . . . .	283
9.4	Speicherlimits . . . . .	285
9.5	Ausführungszeit . . . . .	291
9.6	Klassen und Funktionen deaktivieren . . . . .	292
9.7	dl: Nachladen von Erweiterungen . . . . .	293
9.8	allow_url_fopen und allow_url_includeURLs. . . . .	294
9.9	Variablenverfügbarkeit . . . . .	295
9.10	Uploads. . . . .	299
9.11	Sessions . . . . .	301
9.12	Fehlerausgabe und -verfolgung . . . . .	310
9.13	PHP verbergen. . . . .	312
<b>10</b>	<b>PHP ohne Webserver</b> . . . . .	<b>313</b>
10.1	Buffer Overflows und andere Tücken . . . . .	313
10.1.1	Variablengültigkeit. . . . .	313
10.1.2	Buffer und Stack Overflows . . . . .	315
10.1.3	Nullbytes. . . . .	318
10.2	Einschränkungen der Kommandozeile . . . . .	318
10.2.1	Keine Zeitbeschränkung . . . . .	319
10.2.2	Arbeitsverzeichnis . . . . .	321
10.2.3	Argumentübergabe . . . . .	322
10.3	Netzwerkprogrammierung . . . . .	323
10.3.1	Authentifizierung . . . . .	323
10.3.2	Transaktionssicherung . . . . .	324
10.3.3	Eingelieferte Daten . . . . .	325

<b>II</b>	<b>Die Datenbank als Fehlerquelle</b> . . . . .	331
II.1	Unzureichende Berechtigungen . . . . .	331
II.1.1	MySQL . . . . .	331
II.1.2	PostgreSQL . . . . .	333
II.1.3	MS SQL Server 2000 und 2005. . . . .	337
II.2	Temporäre Dateien . . . . .	337
II.2.1	MySQL . . . . .	338
II.2.2	PostgreSQL . . . . .	339
II.2.3	MS SQL Server 2000 und 2005. . . . .	339
II.3	Unix-Sockets, Named Pipes und Shared Memory . . . . .	339
II.3.1	MySQL: Unix-Socket und Named Pipes . . . . .	340
II.3.2	PostgreSQL: Unix-Socket und Loopback . . . . .	342
II.3.3	MS SQL 2000: Shared Memory. . . . .	343
II.3.4	MS SQL 2005: Shared Memory . . . . .	345
II.4	SSL-Verbindungen . . . . .	346
II.4.1	MySQL . . . . .	347
II.4.2	PostgreSQL . . . . .	350
II.4.3	MS SQL Server 2000 und 2005. . . . .	350
<b>12</b>	<b>Die SQL-Injection</b> . . . . .	351
12.1	Kommentare . . . . .	353
12.2	Ergänzung . . . . .	355
12.3	Zusätzliche SQL-Anweisungen . . . . .	364
12.4	Falsche Daten. . . . .	366
12.5	Abhilfe gegen SQL-Injections. . . . .	367
<b>13</b>	<b>JavaScript: Der Client als Fehlerquelle</b> . . . . .	371
13.1	Fremde Aufrufe. . . . .	371
13.2	Fehlerhafte Parameterverwertung . . . . .	377
13.2.1	Datentypprüfung . . . . .	378
13.2.2	Größenprüfung . . . . .	382
13.2.3	Logikprüfung . . . . .	385
13.3	Was nicht in JavaScript-Code gehört . . . . .	395
13.4	Formularvervollständigung und Co. . . . .	398
<b>14</b>	<b>Konfiguration: Webserver</b> . . . . .	401
14.1	PHP-Konfiguration durch Apache. . . . .	401
14.2	Einsicht von Konfigurationsdateien. . . . .	402
14.3	CGI oder integriertes Modul . . . . .	404

14.4	suExec .....	406
14.5	chroot mit mod_chroot .....	410
14.6	URL-Sicherung mit mod_rewrite .....	415
14.7	Benutzerverfolgung mit mod_log_forensic .....	417
<b>15</b>	<b>Entwicklungs-Guidelines .....</b>	<b>419</b>
15.1	Variablen .....	419
15.1.1	Existenzprüfung .....	419
15.1.2	Typ- und Wertprüfung .....	419
15.1.3	Typumwandlung (Casting) .....	422
15.1.4	Übergabeparameter .....	423
15.2	Sessions .....	428
15.3	Klassen und Funktionen .....	428
15.3.1	Objektorientierte Programmierung .....	429
15.3.2	Funktionen .....	435
15.4	Dateizugriff .....	438
15.4.1	Lesen von Dateien .....	438
15.4.2	Schreiben von Dateien .....	442
15.4.3	Dateisuche .....	444
15.5	Ausgabe .....	445
15.5.1	echo() und printf() .....	445
15.5.2	Übertragung .....	446
15.5.3	HTTP-Header .....	447
15.6	Aufruf externer Programme .....	448
	<b>Stichwortverzeichnis .....</b>	<b>453</b>