

Inhaltsverzeichnis

I	Einleitung.....	15
1.1	Der Ansatz.....	16
1.2	Das Ziel.....	16
1.3	Der Aufbau.....	16
1.4	Die Grenzen.....	19
1.5	Das (Kern-)Problem.....	20
2	Evolution des Webs.....	23
2.1	Die Anfänge des Webs.....	23
2.2	Die Boomphase des Webs.....	25
2.3	Webapplikationen heute.....	26
2.4	Webapplikationen in der Zukunft.....	28
2.5	Entwicklung der Websicherheit.....	28
3	Basiswissen.....	33
3.1	HTTP.....	33
3.1.1	HTTP-Anfrage.....	35
3.1.2	HTTP-Antwort.....	36
3.1.3	HTTP-Headerfelder.....	37
3.1.4	HTTP-Methoden.....	39
3.1.5	Statuscode und Reason Phrase.....	40
3.1.6	Cookies.....	41
3.2	Sprachen des Webs.....	44
3.2.1	Clientseitige Sprachen.....	44
3.2.2	Serverseitige Sprachen.....	58
3.3	URL.....	74
3.4	Webbrowser.....	77
3.4.1	Document Object Model (DOM).....	80
3.4.2	Browsersicherheit.....	80
3.4.3	Same-Origin-Policy (SOP).....	81
3.5	Codierung.....	82
3.5.1	HTML-Codierung.....	83
3.5.2	URL-Codierung.....	84
3.5.3	Unicode-Codierung.....	85
3.5.4	UTF-8.....	86
3.5.5	base64-Codierung.....	87
3.5.6	Hexadezimale Codierung.....	88
3.5.7	Zusammenfassung.....	88

4	Session-Angriffe	89
4.1	Man-in-the-Middle-Angriff	91
4.2	Cookie-Replay-Angriff	92
4.3	Session-Hijacking	93
4.4	Session-Fixation	97
4.5	Session-Riding bzw. CSRF (Cross Site Request Forgery)	98
4.6	Zusammenfassung: Abhilfe aus Entwicklersicht	101
4.6.1	Verschlüsselung	101
4.6.2	Sichere Generierung von Session-IDs	102
4.6.3	Sonstige Maßnahmen	103
4.6.4	Hinweise zu Session-Riding bzw. CSRF	106
5	Cross-Site-Scripting (XSS)	109
5.1	Reflexives XSS	110
5.2	Persistentes XSS	118
5.3	DOM-based XSS	121
5.4	self-XSS	123
5.5	Social-engineered XSS	123
5.6	uXSS	125
5.7	Flash-based XSS	126
5.8	Abhilfe aus Entwicklersicht	127
5.8.1	Sonstige Hinweise/Umgehen von Filtern	128
5.8.2	Schutz vor reflexivem und persistentem XSS	131
5.8.3	Schutz vor DOM-XSS	143
5.8.4	Schutz vor self-XSS	144
5.8.5	Hinweise zu Social-engineered XSS	144
5.8.6	Hinweise zu uXSS	145
5.8.7	Schutz vor Flash-based XSS	146
5.9	Sonstige Maßnahmen gegen XSS	149
5.9.1	CSP (Content-Security-Policy)	149
5.9.2	XSS-Filter im Browser	153
5.9.3	http-only-Flags	154
5.10	Zusammenfassung der Maßnahmen	154
5.11	Wissenswertes über XSS	155
5.12	Scriptless Attacks	157
6	Angriffe auf nachgelagerte Datenbanksysteme	159
6.1	SQL-Injections	160
6.1.1	Login Bypass mit SQL-Injection	161
6.1.2	Basisangriffe durch SQL-Injection	163
6.1.3	Blind-SQL-Injection	181
6.1.4	Wesentliche Erkenntnisse: Angreifersicht	188
6.1.5	Sicherung von SQL-Datenbanken	188

6.1.6	Wesentliche Erkenntnisse: Entwicklersicht	195
6.1.7	Wissenswertes über SQL-Injections.....	195
6.2	Grundlagen von LDAP.....	197
6.2.1	Operatoren innerhalb von LDAP	200
6.2.2	Verknüpfung von Operatoren	201
6.2.3	LDAP-Injection	202
6.2.4	Blind-LDAP-Injection	203
6.2.5	Sicherung von LDAP-Systemen.....	204
6.3	XPath.....	205
6.3.1	XPath-Injection.....	206
6.3.2	Blind-XPath-Injection.....	208
6.3.3	Sicherung von XPath.....	208
6.3.4	Zusammenfassung: Sicherung nachgelagerter Dateisysteme	208
7	Sicherheit von Authentifizierungsmechanismen	211
7.1	Verschiedene Angriffsvektoren.....	211
7.1.1	Simple Angriffe gegen Authentifizierungsmechanismen.....	212
7.1.2	Wörterbuchangriff.....	212
7.1.3	Brute-Force-Methode.....	212
7.2	Grundlagen zum Passworthashing.....	213
7.3	Kryptografische Hashfunktionen	216
7.4	Passwortcracking.....	217
7.4.1	Lookup-Tabellen mittels Brute-Force-Methode oder Wörterbuchangriff.....	218
7.4.2	Rainbow Tables	218
7.4.3	Google-Suche.....	219
7.4.4	Tools	219
7.5	Typenunsicherer Vergleich.....	219
7.6	Abhilfe aus Entwicklersicht.....	223
7.6.1	Salt hinzufügen	223
7.6.2	Sicheres Passworthashing.....	225
7.6.3	Passwort-Policy.....	226
7.6.4	Passwortvalidierung.....	226
7.6.5	Sicherer Vergleich.....	228
7.6.6	Weitere Authentifizierungsarten	228
7.6.7	Hinweise zur Log-in-Änderung.....	230
7.6.8	Hinweise zur »Passwort vergessen?«-Funktion	230
7.6.9	Protokollierung (Logging).....	231
7.6.10	Zusammenfassung.....	232

8	File Inclusion	235
8.1	Path Traversal	235
8.1.1	Abhilfe aus Entwicklersicht	237
8.2	Local File Inclusion (LFI)	239
8.2.1	Abhilfe aus Entwicklersicht	241
8.3	Nullbyte-Injection	241
8.3.1	Abhilfe zur Nullbyte-Injection	242
8.4	Uneingeschränkte Dateiuploads	243
8.4.1	Hinweis zum Upload von Dateien	246
8.5	Remote File Inclusion (RFI)	247
8.5.1	Abhilfe aus Entwicklersicht	248
8.6	XML-External-Entities-Injection (XXE)	248
8.6.1	Abhilfe aus Entwicklersicht	251
8.7	Code-Injection	252
8.7.1	Abhilfe aus Entwicklersicht	253
8.8	HTTP-Header-Injection	254
8.8.1	Cookie-Injection	254
8.8.2	SMTP-Header-Injection	255
8.8.3	Abhilfe aus Entwicklersicht	260
8.9	Zusammenfassung	261
9	Logische Fehler	263
9.1	Zugriffsrechte	263
9.1.1	Rechteausweitungen	264
9.1.2	Ungeschützte Funktionen	267
9.1.3	Kontextabhängige Zugriffe	268
9.1.4	Parametrisierte Zugriffskontrollen	269
9.1.5	Referrer-basierte Zugriffskontrolle	270
9.1.6	Schrittweise Zugriffskontrolle	270
9.2	Ungeprüfte Um- und Weiterleitungen	270
9.2.1	Abhilfe aus Entwicklersicht	271
9.3	Namenskonflikte	272
9.3.1	Namenskonflikte in URLs	272
9.3.2	Namenskonflikte in Nutzernamen	273
9.3.3	Namenskonflikte bei Uploads	274
9.4	Cookie-Manipulation	275
9.4.1	Abhilfe aus Entwicklersicht	275
9.5	Zusammenfassung	275
10	Informationspreisgabe	277
10.1	Fehlermeldungen	277
10.2	Directory Listing	280
10.3	Öffentlich zugängliche Informationen	281

10.3.1	Versteckte Subdomains	281
10.3.2	»Versteckte« Pfade/Standardpfade.....	282
10.3.3	Informationen aus dem Quelltext	283
10.3.4	Öffentliche Dateien	284
10.3.5	Öffentliche Logdateien	285
10.3.6	Sonstige Konfigurationsdateien.....	286
10.3.7	Sonstige Informationen.....	291
10.3.8	Unsichere direkte Objektreferenzen.....	291
10.3.9	Standardwerte	291
10.3.10	Suchmaschinen	292
10.3.11	Soziale Manipulation (Social Engineering).....	303
10.4	Abhilfe: Informationspreisgabe	312
10.4.1	Abhilfe: Fehlermeldungen	313
10.4.2	Abhilfe: Directory Listing.....	313
10.4.3	Abhilfe: öffentlich zugängliche Informationen	314
10.4.4	Abhilfe: Standardwerte	316
10.4.5	Abhilfe: Suchmaschinen	316
10.4.6	Abhilfe: Phishing-Angriffe.....	319
10.4.7	Abhilfe: Social Hacking.....	320
10.4.8	Abhilfe: Social Hacking gegen Plattformbetreiber	320
10.4.9	Abhilfe: Social Hacking innerhalb von Plattformen.....	321
11	UI-Redressing	323
11.1	Die Methoden der Angreifer	323
11.1.1	Clickjacking.....	324
11.1.2	Cursorjacking.....	327
11.1.3	Fortgeschrittene UI-Redressing-Angriffe.....	330
11.2	Abhilfe aus Entwicklersicht.....	332
11.2.1	CSP (Content-Security-Policy)	332
11.2.2	X-Frame-Options (XFO)	333
11.2.3	Frame-Busting mittels JavaScript.....	334
11.2.4	Zusammenfassung.....	335
12	Weitere Angriffsarten	337
12.1	SQL-Injections zu XSS.....	337
12.2	XSS zu SQL-Injection.....	338
12.3	Domain- bzw. Typosquatting	339
12.4	Google-Bombing.....	343
12.5	Exploits	345
12.6	Rent a Hacker/Untergrundforen.....	347
13	Die 10 wichtigsten Regeln für Entwickler und Sicherheitsverantwortliche	349

A	Tools	353
A.1	Toolübersicht.....	354
A.2	Mozilla Firefox-Erweiterungen.....	356
A.2.1	Tamper Data.....	357
A.2.2	Hackbar.....	358
A.2.3	Live HTTP headers.....	360
A.2.4	User Agent Switcher.....	362
A.2.5	Wappalyser.....	364
A.2.6	XSS ME.....	366
A.2.7	SQL Inject ME.....	368
A.3	HTTP-Proxy-Tools.....	369
A.3.1	Burp Suite.....	369
A.3.2	OWASP Zed Attack Proxy (ZAP).....	383
A.4	Tools zu Session-Angriffen.....	391
A.4.1	Wireshark.....	392
A.4.2	CSRFGenerator.....	395
A.5	Angriffstools zu XSS.....	395
A.5.1	XSSer.....	396
A.5.2	Xenotix XSS Exploit Framework.....	398
A.5.3	Adobe SWF Investigator.....	402
A.6	Tools zu nachgelagerten Datenbanksystemen.....	404
A.6.1	SQL-Ninja.....	404
A.6.2	sqlmap.....	407
A.6.3	Havij.....	409
A.6.4	LDAP Blind Explorer.....	413
A.6.5	XPath Blind Explorer.....	414
A.7	Angriffe gegen Authentifizierungsmechanismen.....	415
A.7.1	Brutus.....	416
A.7.2	Cintruder.....	419
A.8	Passwortcracking.....	419
A.8.1	Hash Identifier.....	419
A.8.2	findmyhash.....	421
A.8.3	John the Ripper.....	423
A.9	Tools zur Informationspreisgabe.....	424
A.9.1	Subbrute.....	424
A.9.2	Knock Subdomain Scan.....	426
A.9.3	Wfuzz.....	427
A.9.4	DirBuster.....	430
A.9.5	WPScan.....	431
A.9.6	joomscan.....	433
A.9.7	GitTools (Finder, Dumper, Extractor).....	435
A.9.8	theHarvester.....	438
A.9.9	Social Engineering Toolkit (SET).....	439

A.10	Tools zu UI-Redressing	444
A.10.1	Clickjacking Tester	444
A.10.2	Clickjacking Tool	445
A.11	Kommentar zu automatischen Schwachstellenscannern	446
B	Bug-Bounty-Programme	447
C	Legal Webhacking durchführen	451
C.1.1	HackITs	451
C.1.2	Capture the Flag	453
C.1.3	Responsible-Disclosure-Programme/Bug-Bounty- Programme	453
C.1.4	Zusammenfassung	454
D	SCADA-Hacking	457
D.1.1	Ich sehe was, was du nicht siehst, und das bist ... DU — öffentlich zugängliche Kameras	458
D.1.2	Zugriff auf elektronische Geräte	462
D.1.3	Öffentlich zugängliche Human Machine Interfaces (HMI)	466
D.1.4	Öffentlich zugängliche PLCs (Programmable Logic Controller)	476
D.1.5	Shodan — das dunkle Google	477
D.1.6	Fazit	479
	Epilog	481
	Abkürzungsverzeichnis	483
	Literaturempfehlungen	487
	Quellenverzeichnis	491
	Stichwortverzeichnis	499