

Inhalt

Cracking eCommerce.....	1
for fun and profit.....	1
Vorwort.....	10
Buchübersicht.....	14
Wer sollte dieses Buch lesen?.....	15
Warum jetzt?.....	15
Mein Schreibstil.....	16
Es gibt keinen Königsweg.....	17
Rechtliches.....	18
Besonderer Dank.....	19
Kapitel 1: DNS und TCP - Grundlagen der Anwendungssicherheit.....	20
Am Anfang war DNS.....	21
Same Origin Policy und DNS Rebinding.....	23
DNS-Pinning Angriffe verhindern.....	29
DNS-Pinning mit DNS Rebinding umgehen.....	32
DNS-Zonenübertragungen und -updates.....	34
DNS-Enumeration.....	38
TCP / IP.....	39
Spoofing und der Drei-Wege-Handshake.....	42
Netzwerk-DoS und DDoS-Attacken.....	43
Angriffe gegen DNS.....	44
TCP-DoS.....	45
DoS mit niedriger Bandbreite.....	46
DoS als Selbstverteidigung.....	47
Motive für DoS-Angriffe.....	48
DoS-Verschwörungstheorie.....	49
Port Scanning.....	50
Fazit.....	53

Kapitel 2: IP-Adress-Forensik.....	54
IP.....	56
WHOIS.....	57
IP-Vergabe.....	58
Ortsgebundenheit.....	59
IPv4 und IPv6.....	61
Was kann Dir die IP-Adresse verraten?.....	62
Reverse-DNS-Auflösung.....	63
WHOIS-Datenbank.....	65
Geolokalisierung.....	65
Echtzeit-Sperrlisten und IP-Adress-Reputation.....	70
Verwandte IP-Adressen.....	71
IP-Adresse ist ein Server.....	74
Web-Server als Clients.....	74
Virtuelle Hosts.....	76
Proxies und Auswirkungen auf IP-Adress-Forensik.....	79
Netzwerk-Level-Proxies.....	79
HTTP-Proxies.....	81
Anonymisierungsdienste.....	82
Tor Onion Routing.....	83
Obskure Möglichkeiten die IP-Adresse zu verbergen.....	87
Fazit IP-Adress-Forensik.....	89
Blockieren oder nicht?.....	91
Kapitel 3: Anfragemethoden und HTTP-Protokolle.....	97
Anfragemethoden.....	98
GET.....	98
POST.....	100
PUT und DELETE.....	104
OPTIONS.....	106
CONNECT.....	107
HEAD.....	109

TRACE.....	111
Ungültige Anfragemethoden.....	111
Random Binary Anfragemethoden.....	111
Lowercase Methodennamen.....	112
Irrelevante Leerzeichen.....	112
HTTP-Protokolle.....	115
Fehlende Protokollinformationen.....	115
HTTP 1.0 vs HTTP 1.1 vs HTTP/2.....	116
Ungültige Protokolle und Versionsnummern.....	117
Zeilenumbrüche und Wagenrücklauf.....	118
Zusammenfassung.....	118
Kapitel 4: Referrer URL.....	119
Referrer-Header.....	121
Information Leakage durch Referer.....	122
Zu Freizügig.....	123
Gefälschte Referrer-URL.....	124
Inhalte Dritter und der Referrer.....	125
Was lauert in Deinen Logs.....	127
Referrer und Suchmaschinen.....	129
Google Dorks.....	129
Natürliche Suchbegriffe.....	133
Vanity Search.....	134
Black Hat SEO.....	135
Outsourcing.....	140
Verfügbarkeit der Referrer-URL.....	145
Direkter Seitenzugriff.....	145
Weiterleitungen.....	145
Links von https-Seiten.....	147
Links lokaler Dateien.....	147
Kein Referrer? Warum?.....	149
Referrer Zuverlässigkeit.....	150

Weiterleitung.....	150
Auswirkungen von Cross-Site-Request-Forgery.....	151
Ist die Referrer URL eine Fälschung?.....	154
Referrer-Spam.....	156
Fazit.....	157
Kapitel 5: Request-URL.....	158
Wie sieht ein typischer HTTP-Request aus?.....	159
Abweichungen vom Standard.....	161
Domainnamen im Anforderungsfeld.....	161
Zugriffsversuche per Proxy.....	162
Anker-Tags.....	163
Phishing über Unicode.....	164
Typische URL-Request-Angriffe.....	165
Remote File Inclusion.....	165
SQL Injection.....	167
HTTP-Response-Splitting.....	173
NUL Byte Injection.....	176
Pipes und Systembefehle.....	177
Cross-Site-Scripting (XSS).....	179
Webserver Fingerprinting.....	180
Ungültige URL-Codierung.....	180
Bekannte Server-Dateien.....	181
Admin-Verzeichnisse.....	182
Automatische Application Discovery.....	184
Bekannte Dateien.....	185
crossdomain.xml.....	185
robots.txt.....	188
Google Sitemaps.....	189
Fazit.....	190
Kapitel 6: User-Agent Identifikation.....	191
Wie sieht ein User-Agent-Header aus?.....	193

Malware und Plugins.....	193
Software-Versionen und Patch-Level.....	195
User-Agent-Spoofing.....	196
User-Agent mit anderen Headern prüfen.....	197
User-Agent Spam.....	199
Indirekte Zugriffsdienste.....	200
Google Translate.....	201
Web-Application Security Scanner.....	202
User-Agent-Angriffe.....	203
Suchmaschinen Identitätsübernahme.....	206
Fazit.....	210
Kapitel 7: Request-Header Anomalien.....	212
Hostname.....	213
Fehlende Host-Header.....	214
Schreibweisen des Host-Headers.....	215
Cookies.....	216
Missbrauch von Cookies.....	218
Cookie-Fingerprinting.....	218
HTTP-Cookies.....	219
Weitere Request-Header Anomalien.....	221
X-XSS-Protection.....	221
Content-Security-Policy.....	222
Strict-Transport-Security.....	224
Cache-Control-Header.....	225
Accept-Header gegen CSRF.....	227
Sprache und Zeichensatz.....	230
- - -.....	232
Content-Type Fehler.....	234
Prefetching, Preloading und Prerendering.....	235
Fazit.....	237
Kapitel 8: Eingebettete Inhalte.....	239

Stylesheets.....	240
Bots erkennen.....	241
CSRF-Angriffe erkennen.....	245
JavaScript.....	246
Object.....	249
Request Reihenfolge.....	251
Cookie Stuffing.....	253
Content Delivery Networks vs Sicherheit.....	258
APIs.....	260
Fazit.....	261
Kapitel 9: Angriffe gegen Site-Funktionalität.....	262
Angriffe gegen Deinen Login.....	263
Brute Force.....	264
Phishing.....	267
Anmeldung.....	268
Benutzernamen.....	269
Brute Force.....	270
Spaß mit Passwörtern.....	273
Passwort vergessen.....	274
DoS per Kennwort.....	275
Kommunikation mit Benutzern.....	277
Fazit.....	278
Kapitel 10: Browser-Verlauf.....	279
Die Geschichte wiederholt sich.....	280
Cookies.....	281
JavaScript-Datenbank.....	283
Web Storage.....	284
Refresh.....	285
Gleiche Seite, gleiche IP aber verschiedene Header.....	286
Einzigartigkeit.....	287
DNS-Pinning Teil 2.....	290

Beispiel: Umfrage-Optimierung.....	291
Fazit.....	295
Kapitel 11: Denial of Service.....	297
Was ist Denial of Service?.....	299
Distributed DoS-Angriffe.....	300
Request Flooding.....	302
Wie reagieren?.....	304
Datenbank DoS.....	305
DoS per Websuche.....	306
Ungewöhnliche DoS-Vektoren.....	308
DoS per Bannerwerbung.....	309
DoS per Zahlungsrückgabe.....	310
E-Mail-Blacklist.....	311
Der Umgang mit Denial of Service-Attacken.....	314
Entdeckung.....	314
Vereitelung.....	316
Fazit.....	318
Kapitel 12: Bots.....	319
Content Webscraping.....	320
Formular-/Kommentar Spam.....	321
Preis-Scraping.....	322
Klickbetrug.....	323
Daten-Aggregation.....	323
Diebstahl persönlicher Informationen.....	324
Verlangsamung der Seitenladezeit.....	325
Erkennung von Bots.....	325
Zeitunterschiede.....	326
CAPTCHAs.....	327
Klickbetrug.....	333
Wiederholung.....	340
Fazit.....	341

Kapitel 13: Hochgeladener Inhalt.....	343
Content.....	344
Bilder.....	345
Hashing.....	346
Wasserzeichen.....	348
EXIF-Daten in Bildern.....	350
Bilder mit fragwürdigem Inhalt.....	354
Crash.....	356
Text.....	356
Blog- und Kommentar-Spam.....	357
Case Study: OnSite Spam.....	359
Spam-Erkennung crowdsourcen.....	360
Lokalisierung und Internationalisierung.....	361
HTML.....	362
Fazit.....	363
Kapitel 14: Loss Prevention.....	364
Unterbewusste Wahrnehmung.....	365
Sicherheitsabzeichen.....	367
Honeytokens.....	369
Fazit.....	371
Kapitel 15: Zusammenfassung.....	372
Deine Anwendung „verminen“.....	376
Risikobewertung.....	377
Schlussfolgerung.....	378
Kapitel 16: Tools / Werkzeuge.....	380
Über Peter Wilfahrt.....	383
Abbildungsverzeichnis.....	385
Tabellenverzeichnis.....	386
- Ende -.....	387