

Inhalt

Vorwort	xiii
Danksagung	xv
Einführung	xvii
Wer dieses Buch lesen sollte	xviii
Wie man dieses Buch liest	xix
Was Sie in diesem Buch finden	xix
Ein Disclaimer zum Hacking	xxi
1 Bug-Bounty-Grundlagen	1
1.1 Schwachstellen und Bug-Bounties	2
1.2 Client und Server	2
1.3 Was beim Besuch einer Website passiert	3
Schritt 1: Extrahieren des Domainnamens	3
Schritt 2: Auflösen der IP-Adresse	4
Schritt 3: Herstellen einer TCP-Verbindung	4
Schritt 4: Senden eines HTTP-Requests	5
Schritt 5: Die Response des Servers	6
Schritt 6: Rendering der Response	7
1.4 HTTP-Requests	8
1.4.1 Request-Methoden	9
1.4.2 HTTP ist zustandslos	10
1.5 Zusammenfassung	11
2 Offene Redirects	13
2.1 Wie offene Redirects funktionieren	14
2.2 Offener Redirect bei Shopify-Theme-Installation	16
2.3 Offener Redirect bei Shopify-Log-in	17
2.4 Interstitieller Redirect bei HackerOne	18
2.5 Zusammenfassung	20

3 HTTP Parameter Pollution	21
3.1 Serverseitiges HPP	22
3.2 Clientseitiges HPP	24
3.3 HackerOnes Social-Media-Buttons	26
3.4 Abmelden von Benachrichtigungen bei Twitter	27
3.5 Twitter Web Intents	28
3.6 Zusammenfassung	31
4 Cross Site Request Forgery	33
4.1 Authentifizierung	34
4.2 CSRF mit GET-Requests	36
4.3 CSRF mit POST-Requests	37
4.4 Schutz vor CSRF-Angriffen	39
4.5 Twitter-Abmeldung bei Shopify	41
4.6 Instacart-Zonen eines Nutzers ändern	42
4.7 Vollständige Übernahme eines Badoo-Accounts	44
4.8 Zusammenfassung	46
5 HTML Injection und Content Spoofing	47
5.1 Coinbase: Kommentare einfügen durch Zeichencodierung	48
5.2 Ungewolltes Einbinden von HTML bei HackerOne	50
5.3 Den Fix zu obigem Bug bei HackerOne umgehen	53
5.4 Content Spoofing bei Within Security	54
5.5 Zusammenfassung	56
6 Carriage Return/Line Feed Injection	57
6.1 HTTP Request Smuggling	58
6.2 Response-Splitting bei v.shopify.com	59
6.3 HTTP Response Splitting bei Twitter	60
6.4 Zusammenfassung	63
7 Cross-Site Scripting (XSS)	65
7.1 Arten von XSS	69
7.2 Shopify-Großhandel	72
7.3 Shopifys Währungsformatierung	74
7.4 Gespeichertes XSS bei Yahoo! Mail	75

7.5	Google-Bildersuche	77
7.6	Google Tag Manager: Gespeichertes XSS	79
7.7	XSS bei United Airlines	80
7.8	Zusammenfassung	84
8	Template Injection	85
8.1	Serverseitige Template Injections	86
8.2	Clientseitige Template Injections	86
8.3	Angular Template Injection bei Uber	87
8.4	Flask Jinja2 Template Injection bei Uber	88
8.5	Dynamisches Rendering bei Rails	91
8.6	Smarty Template Injection bei Unikrn	93
8.7	Zusammenfassung	96
9	SQL Injection	97
9.1	SQL-Datenbanken	97
9.2	SQLi-Gegenmaßnahmen	100
9.3	Blinde SQLi bei Yahoo! Sports	100
9.4	Blinde SQLi bei Uber	104
9.5	Drupal-SQLi	107
9.6	Zusammenfassung	111
10	Server-Side Request Forgery	113
10.1	Die Auswirkungen eines SSRF-Angriffs demonstrieren	113
10.2	GET- oder POST-Requests	115
10.3	Blinde SSRFs durchführen	115
10.4	Nutzer mit SSRF-Responses angreifen	116
10.5	ESEA-SSRF und Abfrage von AWS-Metadaten	117
10.6	Internes DNS-SSRF bei Google	119
10.7	Internes Port-Scanning mit Webhooks	124
10.8	Zusammenfassung	125
11	Externe Entitäten bei XML	127
11.1	eXtensible Markup Language	127
11.1.1	Document Type Definition	128
11.1.2	XML-Entitäten	130

11.2	Wie XXE-Angriffe funktionieren	131
11.3	Lese-Zugriff auf Google	133
11.4	Facebook-XXE mit Microsoft Word	134
11.5	Wikiloc XXE	136
11.6	Zusammenfassung	139
12	Remote Code Execution	141
12.1	Shell-Befehle ausführen	141
12.2	Funktionen ausführen	143
12.3	Strategien zur Ausweitung der Remote Code Execution	144
12.4	ImageMagick-RCE bei Polyvore	146
12.5	Algolia-RCE auf facebooksearch.algolia.com	149
12.6	RCE durch SSH	151
12.7	Zusammenfassung	153
13	Speicher-Schwachstellen	155
13.1	Pufferüberlauf	156
13.2	Out-of-Bounds	160
13.3	Integer-Überlauf bei PHP-ftp_genlist()	160
13.4	Pythons hotshot-Modul	161
13.5	Libcurl-Out-of-Bounds	162
13.6	Zusammenfassung	164
14	Übernahme von Subdomains	165
14.1	Domainnamen verstehen	165
14.2	Wie Subdomain-Übernahmen funktionieren	166
14.3	Subdomain-Übernahme bei Ubiquiti	168
14.4	Scan.me verweist auf Zendesk	169
14.5	Windsor-Subdomain-Übernahme bei Shopify	169
14.6	Fastly-Übernahme bei Snapchat	170
14.7	Legal Robot-Übernahme	172
14.8	SendGrid-Mail-Übernahme bei Uber	173
14.9	Zusammenfassung	174

15 Race Conditions	177
15.1 HackerOne-Einladungen mehrfach akzeptieren	178
15.2 Überschreiten des Keybase-Einladungs-Limits	180
15.3 Race Condition bei HackerOne-Zahlungen	181
15.4 Race Condition bei Shopify-Partnern	183
15.5 Zusammenfassung	185
16 Insecure Direct Object References	187
16.1 Einfache IDORs aufspüren	187
16.2 Komplexere IDORs aufspüren	188
16.3 Rechte-Ausweitung (Privilege Escalation) bei Binary.com	189
16.4 App-Erzeugung bei Moneybird	190
16.5 API-Token-Diebstahl bei Twitter Mopub	192
16.6 Preisgabe von Kundeninformationen bei ACME	194
16.7 Zusammenfassung	196
17 OAuth-Schwachstellen	197
17.1 Der OAuth-Workflow	198
17.2 Slack-OAuth-Token stehlen	201
17.3 Umgehen der Authentifizierung mit Standard-Passwörtern	202
17.4 Microsoft-Log-in-Token stehlen	204
17.5 Offizielle Facebook-Access-Token stehlen	206
17.6 Zusammenfassung	207
18 Schwachstellen in Anwendungslogik und -konfiguration	209
18.1 Shopify-Administrator-Rechte umgehen	211
18.2 Account-Schutz bei Twitter umgehen	212
18.3 Signal-Manipulation bei HackerOne	213
18.4 Fehlerhafte S3-Bucket-Rechte bei HackerOne	214
18.5 GitLabs Zwei-Faktor-Authentifizierung umgehen	216
18.6 Preisgabe der PHP-Info bei Yahoo!	218
18.7 HackerOne-Hackativity-Wahl	220
18.8 Zugriff auf PornHubs Memcache-Installation	222
18.9 Zusammenfassung	224

19 Eigene Bug-Bounties	225
19.1 Erkundung	226
19.1.1 Subdomain-Auflistung	227
19.1.2 Port-Scanning	227
19.1.3 Screenshots	228
19.1.4 Content Discovery – Inhalte entdecken	229
19.1.5 Frühere Bugs	231
19.2 Die Anwendung testen	231
19.2.1 Der Technologie-Stack	232
19.2.2 Abbildung der Funktionalitäten	233
19.2.3 Schwachstellen aufspüren	234
19.3 Nächste Schritte	236
19.3.1 Ihre Arbeit automatisieren	236
19.3.2 Mobile Apps untersuchen	237
19.3.3 Neue Funktionalitäten identifizieren	237
19.3.4 JavaScript-Dateien finden	237
19.3.5 Den Zugriff auf neue Funktionalitäten bezahlen	238
19.3.6 Die Technologie lernen	238
19.4 Zusammenfassung	239
20 Bug-Reports	241
20.1 Lesen Sie die Regeln	241
20.2 Zuerst die Details und dann mehr	242
20.3 Überprüfen Sie die Schwachstelle noch einmal	243
20.4 Ihre Reputation	244
20.5 Zeigen Sie dem Unternehmen gegenüber Respekt	244
20.6 Die Höhe von Bounties ansprechen	246
20.7 Zusammenfassung	247
Anhang A Tools	249
A.1 Web-Proxies	249
A.2 Subdomain-Auflistung	251
A.3 Entdeckung (Discovery)	252
A.4 Screenshots	252
A.5 Port-Scanning	253
A.6 Erkundung (Reconnaissance)	254

A.7	Hacking-Tools	255
A.8	Mobile Apps	256
A.9	Browser-Plug-ins	257
Anhang B Ressourcen		259
B.1	Onlinetraining	259
B.2	Bug-Bounty-Plattformen	261
B.3	Empfohlene Literatur	262
B.4	Videos	264
B.5	Empfohlene Blogs	265
Stichwortverzeichnis		269