

# SZCZEGÓŁOWY SPIS TREŚCI

<b>PRZEDMOWA</b> .....	xvii
------------------------	------

<b>PODZIĘKOWANIA</b> .....	xix
----------------------------	-----

<b>WSTĘP</b> .....	xxi
--------------------	-----

Dla kogo jest ta książka? .....	xxii
---------------------------------	------

Jak czytać tę książkę? .....	xxiii
------------------------------	-------

Co znajdziesz w tej książce? .....	xxiii
------------------------------------	-------

Zastrzeżenie dotyczące hakowania .....	xxv
--	-----

## 1

<b>PODSTAWY BUG BOUNTY</b> .....	1
----------------------------------	---

Podatności i Bug Bounty .....	2
-------------------------------	---

Klient i serwer .....	3
-----------------------	---

Co się dzieje, kiedy odwiedzasz stronę .....	3
--	---

Krok 1: Identyfikacja domeny internetowej .....	3
---	---

Krok 2: Ustalanie adresu IP .....	4
-----------------------------------	---

Krok 3: Nawiązanie połączenia TCP .....	4
---	---

Krok 4: Wysyłanie zapytania HTTP .....	5
--	---

Krok 5: Odpowiedź serwera .....	6
---------------------------------	---

Krok 6: Renderowanie odpowiedzi .....	7
---------------------------------------	---

Żądania HTTP .....	8
--------------------	---

Metody żądań .....	8
--------------------	---

Protokół HTTP jest bezstanowy .....	9
-------------------------------------	---

Podsumowanie .....	10
--------------------	----

## 2

<b>OTWARTE PRZEKIEROWANIE</b> .....	11
-------------------------------------	----

Jak działają otwarte przekierowania? .....	12
--	----

Otwarte przekierowanie przy instalacji motywu Shopify .....	14
---	----

Wnioski .....	14
---------------	----

Otwarte przekierowanie przy logowaniu do Shopify .....	15
--	----

Wnioski .....	15
---------------	----

Przekierowanie pośrednie na HackerOne .....	16
---	----

Wnioski .....	17
---------------	----

Podsumowanie .....	17
--------------------	----

<b>3</b>	
<b>HTTP PARAMETER POLLUTION</b>	19
HPP po stronie serwera	20
HPP po stronie klienta	22
Przyciski do udostępniania na HackerOne	23
Wnioski	24
Anulowanie subskrypcji powiadomień na Twitterze	24
Wnioski	25
Web Intents Twittera	26
Wnioski	28
Podsumowanie	28

<b>4</b>	
<b>CROSS-SITE REQUEST FORGERY</b>	29
Uwierzytelnianie	30
CSRF przez żądanie GET	32
CSRF przez żądanie POST	33
Ochrona przed atakami CSRF	35
Odtęczenie Twittera z Shopify	36
Wnioski	37
Zmiana stref użytkowników Instacart	38
Wnioski	39
Przejęcie konta Badoo	39
Wnioski	41
Podsumowanie	41

<b>5</b>	
<b>HTML INJECTION I FAŁSZOWANIE TREŚCI</b>	43
Wstrzyknięcie formularza na stronie Coinbase	44
Wnioski	46
Dodanie kodu HTML w serwisie HackerOne	46
Wnioski	48
Dodanie kodu HTML w serwisie HackerOne – część 2	49
Wnioski	50
Content spoofing w Within Security	50
Wnioski	51
Podsumowanie	52

<b>6</b>	
<b>CARRIAGE RETURN LINE FEED INJECTION</b>	53
HTTP request smuggling	54
HTTP response splitting v.shopify.com	55
Wnioski	56
HTTP response splitting Twittera	56
Wnioski	58
Podsumowanie	58

## 7

<b>CROSS-SITE SCRIPTING</b> .....	59
Rodzaje podatności XSS .....	63
Hurtownia Shopify .....	66
Wnioski .....	67
Formatowanie walut w Shopify .....	67
Wnioski .....	69
Stored XSS w mailu .....	69
Wnioski .....	70
Wyszukiwarka zdjęć Google .....	71
Wnioski .....	72
Stored XSS w menedżerze tagów Google .....	72
Wnioski .....	73
United Airlines XSS .....	73
Wnioski .....	76
Podsumowanie .....	76

## 8

<b>TEMPLATE INJECTION</b> .....	79
Template injection po stronie serwera .....	80
Template injection po stronie klienta .....	80
Template injection w Uberze przez AngularJS .....	81
Wnioski .....	82
Template Injection w Uberze przez Flask i Jinja2 .....	82
Wnioski .....	85
Dynamiczne renderowanie w Rails .....	85
Wnioski .....	86
Template injection w Smarty .....	86
Wnioski .....	89
Podsumowanie .....	89

## 9

<b>SQL INJECTION</b> .....	91
Bazy danych .....	91
Przeciwdziałanie SQLi .....	93
Blind SQLi w Yahoo! Sports .....	94
Wnioski .....	97
Uber Blind SQLi .....	98
Wnioski .....	100
SQLi w Drupal .....	101
Wnioski .....	104
Podsumowanie .....	104

## 10

<b>SERVER-SIDE REQUEST FORGERY</b> .....	105
Demonstracja zagrożeń podatności SSRF .....	106
Wywoływanie żądań GET vs. POST .....	107

Wykonywanie "ślepych" SSRF-ów . . . . .	107
Atakowanie użytkowników przy użyciu odpowiedzi SSRF . . . . .	108
SSRF w ESEA oraz wysyłanie zapytań o metadane AWS . . . . .	109
Wnioski . . . . .	111
SSRF wewnętrznego DNS Google . . . . .	111
Wnioski . . . . .	115
Wewnętrzne skanowanie portów przy użyciu webhooków . . . . .	115
Wnioski . . . . .	117
Podsumowanie . . . . .	117

## 11

<b>XML EXTERNAL ENTITY</b> . . . . .	119
eXtensible Markup Language . . . . .	119
Document Type Definition . . . . .	120
Zewnętrzny DTD . . . . .	121
Wewnętrzny DTD . . . . .	121
Encje XML . . . . .	122
Jak działają ataki XXE . . . . .	123
Dostęp do odczytu w Google . . . . .	125
Wnioski . . . . .	125
XXE w Facebooku . . . . .	125
Wnioski . . . . .	127
XXE w Wikiloc . . . . .	128
Wnioski . . . . .	130
Podsumowanie . . . . .	130

## 12

<b>ZDALNE WYKONANIE KODU</b> . . . . .	131
Wykonywanie poleceń shell . . . . .	131
Wykonywanie funkcji . . . . .	133
Strategie na eskalację zdalnego wykonania kodu . . . . .	134
RCE w bibliotece ImageMagick . . . . .	136
Wnioski . . . . .	138
Algolia RCE na facebooksearch.algolia.com . . . . .	138
Wnioski . . . . .	140
RCE przez SSH . . . . .	140
Wnioski . . . . .	142
Podsumowanie . . . . .	142

## 13

<b>PODATNOŚCI W MANUALNEJ OBSŁUDZE PAMIĘCI</b> . . . . .	143
Przepiętnienie bufora . . . . .	144
Odczyt poza granicami bufora . . . . .	147
Przepiętnienie typu całkowitego w PHP ftp_genlist() . . . . .	148
Wnioski . . . . .	149
Moduł hotshot w Pythonie . . . . .	149
Wnioski . . . . .	150

Odczyt poza granicami bufora w Libcurl . . . . .	150
Wnioski . . . . .	151
Podsumowanie . . . . .	151

## 14

<b>PRZEJĘCIE SUBDOMENY</b> . . . . .	153
Jak działają nazwy domen? . . . . .	153
Jak działa przejęcie subdomeny? . . . . .	154
Przejęcie subdomeny Ubiquiti . . . . .	155
Wnioski . . . . .	156
Przypisanie Scan.me do Zendesk . . . . .	156
Wnioski . . . . .	157
Przejęcie subdomeny Shopify Windsor . . . . .	157
Wnioski . . . . .	158
Przejęcie Snapchata przez Fastly . . . . .	158
Wnioski . . . . .	159
Przejęcie Legal Robot . . . . .	159
Wnioski . . . . .	160
Przejęcie Uber SendGrid . . . . .	160
Wnioski . . . . .	161
Podsumowanie . . . . .	162

## 15

<b>RACE CONDITION</b> . . . . .	163
Kilkukrotne zaakceptowanie zaproszenia do HackerOne . . . . .	164
Wnioski . . . . .	166
Przekroczenie limitu zaproszeń do Keybase . . . . .	166
Wnioski . . . . .	167
Race condition w płatnościach HackerOne . . . . .	167
Wnioski . . . . .	168
Race condition w Shopify Partners . . . . .	168
Wnioski . . . . .	170
Podsumowanie . . . . .	170

## 16

<b>INSECURE DIRECT OBJECT REFERENCE</b> . . . . .	171
Szukanie prostych IDOR-ów . . . . .	172
Szukanie bardziej złożonych IDOR-ów . . . . .	172
Eskalacja uprawnień w Binary.com . . . . .	173
Wnioski . . . . .	174
Tworzenie aplikacji w Moneybird . . . . .	174
Wnioski . . . . .	176
Kradzież tokena API w Twitter Mopub . . . . .	176
Wnioski . . . . .	178
Ujawnianie informacji o klientach ACME . . . . .	178
Wnioski . . . . .	180
Podsumowanie . . . . .	180

## 17

<b>PODATNOŚCI OAUTH</b> .....	181
Przepływ pracy OAuth .....	182
Kradzież tokenów OAuth w Slack .....	185
Wnioski .....	186
Logowanie z domyślnym hasłem .....	186
Wnioski .....	187
Kradzież tokenów logowania Microsoft .....	187
Wnioski .....	189
Przechwytywanie tokenów dostępu Facebooka .....	189
Wnioski .....	190
Podsumowanie .....	190

## 18

<b>PODATNOŚCI W LOGICE I KONFIGURACJI APLIKACJI</b> .....	193
Omijanie uprawnień administratora w Shopify .....	195
Wnioski .....	196
Omijanie zabezpieczeń konta na Twitterze .....	196
Wnioski .....	197
Manipulacja wartościami Signal w HackerOne .....	197
Wnioski .....	197
Niepoprawne uprawnienia bucket-u S3 w HackerOne .....	198
Wnioski .....	199
Omijanie dwuetapowej weryfikacji GitLab .....	200
Wnioski .....	201
Ujawnienie informacji o kodzie PHP Yahoo! .....	201
Wnioski .....	203
Głosowanie w Hacktivity .....	203
Wnioski .....	205
Dostęp do instalacji pamięci podręcznej PornHub .....	205
Wnioski .....	207
Podsumowanie .....	207

## 19

<b>POSZUKIWANIE PODATNOŚCI NA WŁASNĄ RĘKĘ</b> .....	209
Rekonesans .....	210
Enumeracja subdomen .....	211
Skanowanie portów .....	211
Wykonywanie zrzutów ekranu .....	212
Odkrywanie zawartości .....	213
Historia błędów .....	214
Testowanie aplikacji .....	215
Zbiór technologii .....	215
Mapowanie funkcjonalności .....	216
Znajdowanie podatności .....	217
Idąc dalej .....	219
Automatyzacja swojej pracy .....	219
Sprawdzanie aplikacji mobilnych .....	220

Identyfikacja nowej funkcjonalności . . . . .	220
Śledzenie plików JavaScript . . . . .	220
Poznawanie technologii . . . . .	221
Podsumowanie . . . . .	221

## **20**

<b>ZGŁASZANIE PODATNOŚCI</b> . . . . .	223
Sprawdź zasady programu bug bounty . . . . .	224
Dodaj szczegóły; następnie dodaj ich więcej . . . . .	224
Sprawdź podatność dwa razy . . . . .	225
Twoja reputacja . . . . .	226
Szacunek do drugiej strony . . . . .	226
Atrakcyjne nagrody . . . . .	228
Podsumowanie . . . . .	229

## **A**

<b>NARZĘDZIA</b> . . . . .	231
Serwery proxy . . . . .	232
Enumeracja subdomen . . . . .	233
Rekonesans . . . . .	234
Zrzuty ekranu . . . . .	234
Skanowanie portów . . . . .	235
Rozpoznanie aplikacji . . . . .	236
Narzędzia do hakowania . . . . .	237
Analiza aplikacji mobilnych . . . . .	238
Wtyczki do przeglądarki . . . . .	238

## **B**

<b>ŹRÓDŁA</b> . . . . .	241
Kursy online . . . . .	241
Platformy Bug Bounty . . . . .	243
Rekomendowane zasoby . . . . .	244
Filmy . . . . .	246
Rekomendowane blogi . . . . .	247

<b>SKOROWIDZ</b> . . . . .	251
----------------------------	-----