CONTENTS IN DETAIL

FOREWORD by Michiel Prins and Jobert Abma **xvii**

ACKNOWLEDGMENTS **xix**

INTRODUCTION **xxi**

Who Should Read This Book xxii
How to Read This Book xxii
What's in This Book xxiii
A Disclaimer About Hacking xxv

1
BUG BOUNTY BASICS **1**

Vulnerabilities and Bug Bounties 2
Client and Server 2
What Happens When You Visit a Website 3
Step 1: Extracting the Domain Name 3
Step 2: Resolving an IP Address 3
Step 3: Establishing a TCP Connection 4
Step 4: Sending an HTTP Request 4
Step 5: Server Response 5
Step 6: Rendering the Response 6
HTTP Requests 7
Request Methods 7
HTTP Is Stateless 8
Summary 9

2
OPEN REDIRECT **11**

How Open Redirects Work 12
Shopify Theme Install Open Redirect 13
Takeaways 14
Shopify Login Open Redirect 14
Takeaways 15
HackerOne Interstitial Redirect 15
Takeaways 16
Summary 17

3
HTTP PARAMETER POLLUTION **19**

Server-Side HPP 20
Client-Side HPP 22
HackerOne Social Sharing Buttons 23
Takeaways 24

Twitter Unsubscribe Notifications 24
Takeaways 25
Twitter Web Intents 25
Takeaways 27
Summary 27

4
CROSS-SITE REQUEST FORGERY 29

Authentication 30
CSRF with GET Requests 31
CSRF with POST Requests 32
Defenses Against CSRF Attacks 34
Shopify Twitter Disconnect 36
Takeaways 37
Change Users Instacart Zones 37
Takeaways 38
Badoo Full Account Takeover 38
Takeaways 40
Summary 40

5
HTML INJECTION AND CONTENT SPOOFING 41

Coinbase Comment Injection Through Character Encoding 42
Takeaways 44
HackerOne Unintended HTML Inclusion 44
Takeaways 46
HackerOne Unintended HTML Include Fix Bypass 46
Takeaways 47
Within Security Content Spoofing 47
Takeaways 47
Summary 48

6
CARRIAGE RETURN LINE FEED INJECTION 49

HTTP Request Smuggling 50
v.shopify.com Response Splitting 51
Takeaways 52
Twitter HTTP Response Splitting 52
Takeaways 54
Summary 54

7
CROSS-SITE SCRIPTING 55

Types of XSS 58
Shopify Wholesale 61
Takeaways 62
Shopify Currency Formatting 62
Takeaways 63

Yahoo! Mail Stored XSS 63
Takeaways 65
Google Image Search 65
Takeaways 66
Google Tag Manager Stored XSS 66
Takeaways 67
United Airlines XSS 67
Takeaways 70
Summary 70

8
TEMPLATE INJECTION **71**

Server-Side Template Injections 72
Client-Side Template Injections 72
Uber AngularJS Template Injection 73
Takeaways 74
Uber Flask Jinja2 Template Injection 74
Takeaways 76
Rails Dynamic Render 76
Takeaways 77
Unikrn Smarty Template Injection 78
Takeaways 80
Summary 80

9
SQL INJECTION **81**

SQL Databases 82
Countermeasures Against SQLi 83
Yahoo! Sports Blind SQLi 84
Takeaways 87
Uber Blind SQLi 87
Takeaways 90
Drupal SQLi 90
Takeaways 93
Summary 93

10
SERVER-SIDE REQUEST FORGERY **95**

Demonstrating the Impact of Server-Side Request Forgery 96
Invoking GET vs. POST Requests 97
Performing Blind SSRFs 97
Attacking Users with SSRF Responses 98
ESEA SSRF and Querying AWS Metadata 98
Takeaways 100
Google Internal DNS SSRF 100
Takeaways 104
Internal Port Scanning Using Webhooks 104
Takeaways 105
Summary 105

11
XML EXTERNAL ENTITY **107**

eXtensible Markup Language 107
Document Type Definitions 108
XML Entities 110
How XXE Attacks Work 111
Read Access to Google 112
Takeaways 112
Facebook XXE with Microsoft Word 112
Takeaways 114
Wikiloc XXE 115
Takeaways 117
Summary 117

12
REMOTE CODE EXECUTION **119**

Executing Shell Commands 119
Executing Functions 121
Strategies for Escalating Remote Code Execution 122
Polyvore ImageMagick 123
Takeaways 125
Algolia RCE on facebooksearch.algolia.com 125
Takeaways 127
RCE Through SSH 127
Takeaways 128
Summary 128

13
MEMORY VULNERABILITIES **129**

Buffer Overflows 130
Read Out of Bounds 133
PHP ftp_genlist() Integer Overflow 134
Takeaways 134
Python Hotshot Module 135
Takeaways 135
Libcurl Read Out of Bounds 136
Takeaways 136
Summary 136

14
SUBDOMAIN TAKEOVER **139**

Understanding Domain Names 139
How Subdomain Takeovers Work 140
Ubiquiti Subdomain Takeover 141
Takeaways 142
Scan.me Pointing to Zendesk 142
Takeaways 142

Shopify Windsor Subdomain Takeover 142
Takeaways 143
Snapchat Fastly Takeover 143
Takeaways 144
Legal Robot Takeover 144
Takeaways 145
Uber SendGrid Mail Takeover 145
Takeaways 146
Summary 147

15
RACE CONDITIONS **149**

Accepting a HackerOne Invite Multiple Times 150
Takeaways 151
Exceeding Keybase Invitation Limits 152
Takeaways 152
HackerOne Payments Race Condition 153
Takeaways 154
Shopify Partners Race Condition 154
Takeaways 155
Summary 156

16
INSECURE DIRECT OBJECT REFERENCES **157**

Finding Simple IDORs 158
Finding More Complex IDORs 158
Binary.com Privilege Escalation 159
Takeaways 160
Moneybird App Creation 160
Takeaways 161
Twitter Mopub API Token Theft 161
Takeaways 163
ACME Customer Information Disclosure 163
Takeaways 164
Summary 165

17
OAUTH VULNERABILITIES **167**

The OAuth Workflow 168
Stealing Slack OAuth Tokens 171
Takeaways 171
Passing Authentication with Default Passwords 171
Takeaways 172
Stealing Microsoft Login Tokens 173
Takeaways 174
Swiping Facebook Official Access Tokens 174
Takeaways 175
Summary 176

18
APPLICATION LOGIC AND CONFIGURATION VULNERABILITIES 177

Bypassing Shopify Administrator Privileges 179
Takeaways 179
Bypassing Twitter Account Protections 180
Takeaways 180
HackerOne Signal Manipulation 180
Takeaways 181
HackerOne Incorrect S3 Bucket Permissions 181
Takeaways 183
Bypassing GitLab Two-Factor Authentication 183
Takeaways 184
Yahoo! PHP Info Disclosure 184
Takeaways 186
HackerOne Hacktivity Voting 186
Takeaways 187
Accessing PornHub's Memcache Installation 188
Takeaways 189
Summary 189

19
FINDING YOUR OWN BUG BOUNTIES 191

Reconnaissance 192
Subdomain Enumeration 192
Port Scanning 193
Screenshotting 194
Content Discovery 195
Previous Bugs 196
Testing the Application 196
The Technology Stack 196
Functionality Mapping 197
Finding Vulnerabilities 198
Going Further 200
Automating Your Work 200
Looking at Mobile Apps 200
Identifying New Fuctionality 201
Tracking JavaScript Files 201
Paying for Access to New Functionality 201
Learning the Technology 201
Summary 202

20
VULNERABILITY REPORTS 203

Read the Policy 204
Include Details; Then Include More 204
Reconfirm the Vulnerability 205
Your Reputation 205
Show Respect for the Company 206
Appealing Bounty Rewards 207
Summary 208

A
TOOLS **209**
Web Proxies 210
Subdomain Enumeration 211
Discovery 212
Screenshotting 212
Port Scanning 213
Reconnaissance 213
Hacking Tools 214
Mobile 215
Browser Plug-Ins 216

B
RESOURCES **217**
Online Training 217
Bug Bounty Platforms 219
Recommended Reading 220
Video Resources 222
Recommended Blogs 222

INDEX **225**