

CONTENTS IN DETAIL

FOREWORD	xvii
-----------------	-------------

ACKNOWLEDGMENTS	xxi
------------------------	------------

INTRODUCTION	xxiii
---------------------	--------------

The Allure of Hacking Web APIs	xxiv
This Book's Approach	xxiv
Hacking the API Restaurant	xxv

PART I: HOW WEB API SECURITY WORKS 1

0 PREPARING FOR YOUR SECURITY TESTS 3

Receiving Authorization	4
Threat Modeling an API Test	4
Which API Features You Should Test	6
API Authenticated Testing	6
Web Application Firewalls	7
Mobile Application Testing	7
Auditing API Documentation	8
Rate Limit Testing	8
Restrictions and Exclusions	9
Security Testing Cloud APIs	10
DoS Testing	10
Reporting and Remediation Testing	11
A Note on Bug Bounty Scope	11
Summary	13

1 HOW WEB APPLICATIONS WORK 15

Web App Basics	15
The URL	16
HTTP Requests	17
HTTP Responses	18
HTTP Status Codes	19
HTTP Methods	20
Stateful and Stateless HTTP	22
Web Server Databases	23
SQL	23
NoSQL	24
How APIs Fit into the Picture	25
Summary	26

2 THE ANATOMY OF WEB APIS 27

How Web APIs Work	28
Standard Web API Types	30
RESTful APIs	30
GraphQL	34
REST API Specifications	38
API Data Interchange Formats	39
JSON	39
XML	41
YAML	42
API Authentication	42
Basic Authentication	43
API Keys	44
JSON Web Tokens	45
HMAC	46
OAuth 2.0	47
No Authentication	48
APIs in Action: Exploring Twitter’s API	48
Summary	51

3 COMMON API VULNERABILITIES 53

Information Disclosure	54
Broken Object Level Authorization	55
Broken User Authentication	56
Excessive Data Exposure	58
Lack of Resources and Rate Limiting	59
Broken Function Level Authorization	59
Mass Assignment	61
Security Misconfigurations	62
Injections	64
Improper Assets Management	65
Business Logic Vulnerabilities	66
Summary	67

PART II: BUILDING AN API TESTING LAB 69

4 YOUR API HACKING SYSTEM 71

Kali Linux	72
Analyzing Web Apps with DevTools	72
Capturing and Modifying Requests with Burp Suite	75
Setting Up FoxyProxy	76
Adding the Burp Suite Certificate	76
Navigating Burp Suite	77
Intercepting Traffic	79
Altering Requests with Intruder	81

Crafting API Requests in Postman, an API Browser	84
The Request Builder	86
Environments	89
Collections	90
The Collection Runner	93
Code Snippets	94
The Tests Panel	94
Configuring Postman to Work with Burp Suite	95
Supplemental Tools	96
Performing Reconnaissance with OWASP Amass	97
Discovering API Endpoints with Kiterunner	98
Scanning for Vulnerabilities with Nikto	99
Scanning for Vulnerabilities with OWASP ZAP	100
Fuzzing with Wfuzz	100
Discovering HTTP Parameters with Arjun	102
Summary	103
Lab #1: Enumerating the User Accounts in a REST API	103

5 SETTING UP VULNERABLE API TARGETS 109

Creating a Linux Host	110
Installing Docker and Docker Compose	110
Installing Vulnerable Applications	111
The completely ridiculous API (crAPI)	111
OWASP DevSlop’s Pixi	112
OWASP Juice Shop	112
Damn Vulnerable GraphQL Application	113
Adding Other Vulnerable Apps	114
Hacking APIs on TryHackMe and HackTheBox	115
Summary	116
Lab #2: Finding Your Vulnerable APIs	116

PART III: ATTACKING APIS 121

6 DISCOVERY 123

Passive Recon	124
The Passive Recon Process	124
Google Hacking	125
ProgrammableWeb’s API Search Directory	127
Shodan	129
OWASP Amass	131
Exposed Information on GitHub	133
Active Recon	136
The Active Recon Process	136
Baseline Scanning with Nmap	138
Finding Hidden Paths in Robots.txt	139
Finding Sensitive Information with Chrome DevTools	139
Validating APIs with Burp Suite	142

Crawling URIs with OWASP ZAP	143
Brute-Forcing URIs with Gobuster.	145
Discovering API Content with Kiterunner.	146
Summary	148

Lab #3: Performing Active Recon for a Black Box Test. 148

**7
ENDPOINT ANALYSIS 155**

Finding Request Information.	156
Finding Information in Documentation	156
Importing API Specifications	159
Reverse Engineering APIs	161
Adding API Authentication Requirements to Postman.	164
Analyzing Functionality.	166
Testing Intended Use	167
Performing Privileged Actions	168
Analyzing API Responses	169
Finding Information Disclosures	169
Finding Security Misconfigurations	170
Verbose Errors	170
Poor Transit Encryption	171
Problematic Configurations.	171
Finding Excessive Data Exposures	172
Finding Business Logic Flaws	173
Summary	174

Lab #4: Building a crAPI Collection and Discovering Excessive Data Exposure 174

**8
ATTACKING AUTHENTICATION 179**

Classic Authentication Attacks	180
Password Brute-Force Attacks	180
Password Reset and Multifactor Authentication Brute-Force Attacks	181
Password Spraying	183
Including Base64 Authentication in Brute-Force Attacks	185
Forging Tokens	187
Manual Load Analysis	187
Live Token Capture Analysis	189
Brute-Forcing Predictable Tokens	190
JSON Web Token Abuse.	192
Recognizing and Analyzing JWTs	193
The None Attack.	195
The Algorithm Switch Attack.	195
The JWT Crack Attack	197
Summary	197

Lab #5: Cracking a crAPI JWT Signature 197

9		
FUZZING		201
Effective Fuzzing		202
Choosing Fuzzing Payloads		203
Detecting Anomalies		204
Fuzzing Wide and Deep		207
Fuzzing Wide with Postman		207
Fuzzing Deep with Burp Suite		210
Fuzzing Deep with Wfuzz		212
Fuzzing Wide for Improper Assets Management		214
Testing Request Methods with Wfuzz		216
Fuzzing “Deeper” to Bypass Input Sanitization		217
Fuzzing for Directory Traversal		218
Summary		218
Lab #6: Fuzzing for Improper Assets Management Vulnerabilities		219

10		
EXPLOITING AUTHORIZATION		223
Finding BOLAs		223
Locating Resource IDs		224
A-B Testing for BOLA		225
Side-Channel BOLA		226
Finding BFLAs		227
A-B-A Testing for BFLA		227
Testing for BFLA in Postman		228
Authorization Hacking Tips		230
Postman’s Collection Variables		230
Burp Suite Match and Replace		231
Summary		231
Lab #7: Finding Another User’s Vehicle Location		232

11		
MASS ASSIGNMENT		237
Finding Mass Assignment Targets		238
Account Registration		238
Unauthorized Access to Organizations		238
Finding Mass Assignment Variables		239
Finding Variables in Documentation		239
Fuzzing Unknown Variables		240
Blind Mass Assignment Attacks		241
Automating Mass Assignment Attacks with Arjun and Burp Suite Intruder		241
Combining BFLA and Mass Assignment		242
Summary		243
Lab #8: Changing the Price of Items in an Online Store		243

12		
INJECTION		249
Discovering Injection Vulnerabilities		250
Cross-Site Scripting (XSS)		251
Cross-API Scripting (XAS)		252
SQL Injection		253
Manually Submitting Metacharacters		255
SQLmap		256
NoSQL Injection		257
Operating System Command Injection		259
Summary		261
Lab #9: Faking Coupons Using NoSQL Injection		261

PART IV: REAL-WORLD API HACKING **265**

13 **APPLYING EVASIVE TECHNIQUES AND RATE LIMIT TESTING** **267**

Evading API Security Controls		267
How Security Controls Work		268
API Security Control Detection		269
Using Burner Accounts		270
Evasive Techniques		270
Automating Evasion with Burp Suite		273
Automating Evasion with Wfuzz		274
Testing Rate Limits		276
A Note on Lax Rate Limits		276
Path Bypass		278
Origin Header Spoofing		279
Rotating IP Addresses in Burp Suite		280
Summary		284

14 **ATTACKING GRAPHQL** **285**

GraphQL Requests and IDEs		286
Active Reconnaissance		287
Scanning		287
Viewing DVGA in a Browser		288
Using DevTools		289
Reverse Engineering the GraphQL API		290
Directory Brute-Forcing for the GraphQL Endpoint		290
Cookie Tampering to Enable the GraphQL IDE		292
Reverse Engineering the GraphQL Requests		294
Reverse Engineering a GraphQL Collection Using Introspection		296
GraphQL API Analysis		297
Crafting Requests Using the GraphQL Documentation Explorer		297
Using the InQL Burp Extension		298
Fuzzing for Command Injection		301
Summary		305

15		
DATA BREACHES AND BUG BOUNTIES		307
The Breaches		308
Peloton		308
USPS Informed Visibility API		309
T-Mobile API Breach		311
The Bounties		312
The Price of Good API Keys		312
Private API Authorization Issues.		313
Starbucks: The Breach That Never Was		315
An Instagram GraphQL BOLA		317
Summary		318
CONCLUSION		319
A		
API HACKING CHECKLIST		321
B		
ADDITIONAL RESOURCES		323
INDEX		327