

CONTENTS IN DETAIL

FOREWORD	xv
-----------------	-----------

ACKNOWLEDGMENTS	xix
------------------------	------------

INTRODUCTION	xxi
---------------------	------------

Who This Book Is For	xxii
The Book's Lab and Code Repository	xxii
What's in This Book	xxii

1	
A PRIMER ON GRAPHQL	1

The Basics	1
Origins	2
Use Cases	2
Specification	3
How Do Communications Work?	3
The Schema	4
Queries	6
The Query Parser and Resolver Functions	7
What Problems Does GraphQL Solve?	8
GraphQL APIs vs. REST APIs	9
The REST Example	10
The GraphQL Example	12
Other Differences	15
Your First Query	17
Summary	20

2	
SETTING UP A GRAPHQL SECURITY LAB	21

Taking Security Precautions	22
Installing Kali	23
Installing Web Clients	24
Querying from the Command Line with cURL	25
Querying from a GUI with Altair	25
Setting Up a Vulnerable GraphQL Server	28
Installing Docker	28
Deploying the Damn Vulnerable GraphQL Application	29
Testing DVGA	31
Installing GraphQL Hacking Tools	31
Burp Suite	32
Clairvoyance	33
InQL	34
Graphw00f	35
BatchQL	36

Nmap	37
Commix	37
graphql-path-enum	38
EyeWitness	39
GraphQL Cop	39
CrackQL	40
Summary	40

3 THE GRAPHQL ATTACK SURFACE 41

What Is an Attack Surface?	41
The Language	42
Queries, Mutations, and Subscriptions	43
Operation Names	46
Fields	47
Arguments	48
Aliases	50
Fragments	52
Variables	53
Directives	54
Data Types	56
Objects	57
Scalars	58
Enums	58
Unions	60
Interfaces	61
Inputs	62
Introspection	63
Validation and Execution	66
Common Weaknesses	67
Specification Rule and Implementation Weaknesses	67
Denial of Service	69
Information Disclosure	69
Authentication and Authorization Flaws	69
Injections	70
Summary	70

4 RECONNAISSANCE 71

Detecting GraphQL	72
Common Endpoints	73
Common Responses	74
Nmap Scans	76
The __typename Field	78
Graphw00f	80
Detecting GraphQL Explorer and GraphQL Playground	81
Scanning for Graphical Interfaces with EyeWitness	82
Attempting a Query Using Graphical Clients	84

Querying GraphQL by Using Introspection	87
Visualizing Introspection with GraphQL Voyager.	92
Generating Introspection Documentation with SpectaQL.	93
Exploring Disabled Introspection	93
Fingerprinting GraphQL	94
Detecting Servers with Graphw00f	97
Analyzing Results	98
Summary	99

5 DENIAL OF SERVICE 101

GraphQL DoS Vectors	102
Circular Queries	102
Circular Relationships in GraphQL Schemas.	103
How to Identify Circular Relationships	105
Circular Query Vulnerabilities.	109
Circular Introspection Vulnerabilities	110
Circular Fragment Vulnerabilities.	111
Field Duplication	113
Understanding How Field Duplication Works	113
Testing for Field Duplication Vulnerabilities	114
Alias Overloading	116
Abusing Aliases for Denial of Service	117
Chaining Aliases and Circular Queries	118
Directive Overloading.	119
Abusing Directives for Denial of Service.	119
Testing for Directive Overloading	120
Object Limit Overriding	121
Array-Based Query Batching	122
Understanding How Array-Based Query Batching Works	122
Testing for Array-Based Query Batching.	123
Chaining Circular Queries and Array-Based Query Batching	124
Detecting Query Batching by Using BatchQL	126
Performing a DoS Audit with GraphQL Cop	127
Denial-of-Service Defenses in GraphQL.	128
Query Cost Analysis	128
Query Depth Limits	131
Alias and Array-Based Batching Limits	132
Field Duplication Limits	132
Limits on the Number of Returned Records	133
Query Allow Lists	133
Automatic Persisted Queries	134
Timeouts.	135
Web Application Firewalls	136
Gateway Proxies.	136
Summary	137

6 INFORMATION DISCLOSURE 139

Identifying Information Disclosure Vectors in GraphQL	140
Automating Schema Extraction with InQL	140

Overcoming Disabled Introspection	142
Detecting Disabled Introspection	142
Exploiting Non-production Environments	142
Exploiting the __type Meta-field	143
Using Field Suggestions	145
Understanding the Edit-Distance Algorithm	146
Optimizing Field Suggestion Use	146
Considering Security Developments	148
Using Field Stuffing	149
Type Stuffing in the __type Meta-field	150
Automating Field Suggestion and Stuffing Using Clairvoyance	152
Abusing Error Messages	154
Exploring Excessive Error Messaging	156
Enabling Debugging	157
Inferring Information from Stack Traces	158
Leaking Data by Using GET-Based Queries	160
Summary	160

7

AUTHENTICATION AND AUTHORIZATION BYPASSES 163

The State of Authentication and Authorization in GraphQL	164
In-Band vs. Out-of-Band	164
Common Approaches	165
Authentication Testing	171
Detecting the Authentication Layer	172
Brute-Forcing Passwords by Using Query Batching	173
Brute-Forcing Passwords with CrackQL	176
Using Allow-Listed Operation Names	177
Forging and Leaking JWT Credentials	178
Authorization Testing	180
Detecting the Authorization Layer	181
Enumerating Paths with graphql-path-enum	182
Brute-Forcing Arguments and Fields with CrackQL	183
Summary	185

8

INJECTION 187

Injection Vulnerabilities in GraphQL	188
The Blast Radius of Malicious Input	188
The OWASP Top 10	189
The Injection Surface	190
Query Arguments	191
Field Arguments	193
Query Directive Arguments	193
Operation Names	194
Input Entry Points	195
SQL Injection	196
Understanding the Types of SQL Injection	196
Testing for SQLi	197
Testing DVGA for SQLi with Burp Suite	197
Automating SQL Injection	203

Operating System Command Injection	205
An Example	206
Manual Testing in DVGA	207
Automated Testing with Commix	208
Code Review of a Resolver Function	210
Cross-Site Scripting	211
Reflected XSS	211
Stored XSS	213
DOM-Based XSS	214
Testing for XSS in DVGA	214
Summary	219

9 REQUEST FORGERY AND HIJACKING 221

Cross-Site Request Forgery	222
Locating State-Changing Actions	223
Testing for POST-Based Vulnerabilities	225
Automatically Submitting a CSRF Form	227
Testing for GET-Based Vulnerabilities	228
Using HTML Injection	230
Automating Testing with BatchQL and GraphQL Cop	232
Preventing CSRF	232
Server-Side Request Forgery	234
Understanding the Types of SSRF	235
Searching for Vulnerable Operations, Fields, and Arguments	236
Testing for SSRF	236
Preventing SSRF	240
Cross-Site WebSocket Hijacking	240
Finding Subscription Operations	241
Hijacking a Subscription Query	241
Preventing CSWSH	244
Summary	245

10 DISCLOSED VULNERABILITIES AND EXPLOITS 247

Denial of Service	248
A Large Payload (HackerOne)	248
Regular Expressions (CS Money)	249
A Circular Introspection Query (GitLab)	251
Aliases for Field Duplication (Magento)	252
Array-Based Batching for Field Duplication (WPGraphQL)	253
Circular Fragments (Agoo)	255
Broken Authorization	256
Allowing Data Access to Deactivated Users (GitLab)	256
Allowing an Unprivileged Staff Member to Modify a Customer's Email (Shopify)	257
Disclosing the Number of Allowed Hackers Through a Team Object (HackerOne)	258
Reading Private Notes (GitLab)	259
Disclosing Payment Transaction Information (HackerOne)	260

Information Disclosure	261
Enumerating GraphQL Users (GitLab)	261
Accessing the Introspection Query via WebSocket (Nuri)	262
Injection	262
SQL Injection in a GET Query Parameter (HackerOne)	262
SQL Injection in an Object Argument (Apache SkyWalking)	264
Cross-Site Scripting (GraphQL Playground)	265
Cross-Site Request Forgery (GitLab)	267
Summary	268

A
GRAPHQL API TESTING CHECKLIST **269**

Reconnaissance	269
Denial of Service	270
Information Disclosure	270
Authentication and Authorization	270
Injection	271
Forging Requests	271
Hijacking Requests	271

B
GRAPHQL SECURITY RESOURCES **273**

Penetration Testing Tips and Tricks	273
Hands-on Hacking Labs	274
Security Videos	274

INDEX **275**