INTRODUCTION

Today's researchers estimate that application programming interface (API) calls make up more than 80 percent of all web traffic. Yet despite their prevalence, web application hackers often fail to test them. And these vital business assets can be riddled with catastrophic weaknesses.

As you'll see in this book, APIs are an excellent attack vector. After all, they're designed to expose information to other applications. To compromise an organization's most sensitive data, you may not need to cleverly penetrate the perimeter of a network firewall, bypass an advanced antivirus, and release a zero day; instead, your task could be as simple as making an API request to the right endpoint.

The goal of this book is to introduce you to web APIs and show you how to test them for a myriad of weaknesses. We'll primarily focus on testing the security of REST APIs, the most common API format used in web applications, but will cover

attacking GraphQL APIs as well. You'll first learn tools and techniques for using APIs as intended. Next, you'll probe them for vulnerabilities and learn how to exploit those vulnerabilities. You can then report your findings and help prevent the next data breach.

The Allure of Hacking Web APIs

In 2017, *The Economist*, one of the leading sources of information for international business, ran the following headline: "The world's most valuable resource is no longer oil, but data." APIs are digital pipelines that allow a precious commodity to flow across the world in the blink of an eye.

Simply put, an API is a technology that enables communication between different applications. When, for example, a Python application needs to interact with the functionality of a Java app, things can get messy very quickly. By relying on APIs, developers can design modular applications that leverage the expertise of other applications. For example, they no longer need to create their own custom software to implement maps, payment processors, machine-learning algorithms, or authentication processes.

As a result, many modern web applications have been quick to adopt APIs. Yet new technologies often get quite a head start before cybersecurity has a chance to ask any questions, and APIs have hugely expanded these applications' attack surfaces. They've been so poorly defended that attackers can use them as a direct route to their data. In addition, many APIs lack the security controls that other at-

tack vectors have in place, making them the equivalent of the Death Star's thermal exhaust port: a path to doom and destruction for businesses.

Due to these reasons, Gartner predicted years ago that by 2022, APIs will be the leading attack vector. As hackers, we need to secure them by putting on our rollerblades, strapping the Acme rocket to our backs, and catching up to the speed of technological innovation. By attacking APIs, reporting our findings, and communicating risks to the business, we can do our part to thwart cybercrime.

This Book's Approach

Attacking APIs is not as challenging as you may think. Once you understand how they operate, hacking them is only a matter of issuing the right HTTP requests. That said, the tools and techniques typically leveraged to perform bug hunting and web application penetration testing do not translate well to APIs. You can't, for instance, throw a generic vulnerability scan at an API and expect useful results. I've often run these scans against vulnerable APIs only to receive false negatives. When APIs are not tested properly, organizations are given a false sense of security that leaves them with a risk of being compromised.

Each section of this book will build upon the previous one:

Part I: How Web API Security Works First, I will introduce you to the basic knowledge you need about web applications and the APIs that power them. You'll learn about REST APIs, the main topic of this book, as well as the increasingly popular GraphQL API format. I will also cover the most common API-related vulnerabilities you can expect to find.

Part II: Building an API Testing Lab In this section, you'll build your API hacking system and develop an understanding of the tools in play, including Burp Suite, Postman, and a variety of others. You'll also set up a lab of vulnerable targets you'll practice attacking throughout this book.

Part III: Attacking APIs In Part III, we'll turn to the API hacking methodology, and I'll walk you through performing common attacks against APIs. Here the fun begins: you'll discover APIs through the use of open-source intelligence techniques, analyze them to understand their attack surface, and finally dive into various attacks against them, such as injections. You'll learn how to reverse engineer an API, bypass its authentication, and fuzz it for a variety of security issues.

Part IV: Real-World API Hacking The final section of this book is dedicated to showing you how API weaknesses have been exploited in data breaches and bug bounties. You'll learn how hackers have employed the techniques covered throughout the book in real-world situations. You'll also walk through a sample attack against a GraphQL API, adapting many of the techniques introduced earlier in the book to the GraphQL format.

The Labs Each chapter in Parts II and III includes a hands-on lab that lets you practice the book's techniques on your own. Of course, you can use tools other than the ones presented here to complete the activities. I encourage you to use the labs as a stepping-stone to experiment with techniques I present and then try out your own attacks.

This book is for anyone looking to begin web application hacking, as well as penetration testers and bug bounty hunters looking to add another skill to their repertoire. I've designed the text so that even beginners can pick up the knowledge

they'll need about web applications in Part I, set up their hacking lab in Part II, and begin hacking in Part III.

Hacking the API Restaurant

Before we begin, let me leave you with a metaphor. Imagine that an application is a restaurant. Like an API's documentation, the menu describes what sort of things you can order. As an intermediary between the customer and the chef, the waiter is like the API itself; you can make requests to the waiter based on the menu, and the waiter will bring you what you ordered.

Crucially, an API user does not need to know how the chef prepares a dish or how the backend application operates. Instead, they should be able to follow a set of instructions to make a request and receive a corresponding response. Developers can then program their applications to fulfill the request however they'd like.

As an API hacker, you'll be probing every part of the metaphorical restaurant. You'll learn how the restaurant operates. You might attempt to bypass its "bouncer" or perhaps provide a stolen authentication token. Also, you'll analyze the menu for ways to trick the API into giving you the data you're not authorized to access, perhaps by tricking the waiter into handing you everything they have. You may even convince the API owner into giving you the keys to the whole restaurant.

This book takes a holistic approach toward hacking APIs by guiding you through the following topics:

- Understanding how web applications work and the anatomy of web APIs
- Mastering the top API vulnerabilities from a hacker's perspective
- Learning the most effective API hacking tools
- Performing passive and active API reconnaissance to discover the existence of APIs, find exposed secrets, and analyze API functionality
- Interacting with APIs and testing them with the power of fuzzing
- Performing a variety of attacks to exploit API vulnerabilities you discover

Throughout this book, you'll apply an adversarial mindset to take advantage of the functions and features of any API. The better we emulate adversaries, the better we will be at finding weaknesses we can report to the API provider. Together, I think we might even prevent the next big API data breaches.