Conclusion

I wrote this book to give ethical hackers the upper hand against cybercriminals, at least until the next technological advancement. We'll probably never see the end of this undertaking. The popularity of APIs will continue to grow, and they'll interact in new ways that expand the attack surface of every industry. The adversaries won't stop either. If you don't test an organization's APIs, a cybercriminal somewhere will do it instead. (The main difference is that they won't provide a report to improve anyone's API security.)

To help you become a master API hacker, I encourage you to sign up for bug bounty programs like BugCrowd, HackerOne, and Intigriti. Keep up with the latest API security news by following the OWASP API Security Project, APIsecurity.io, APIsec, PortSwigger Blog, Akamai, Salt Security Blog, Moss Adams Insights, and my own blog at *https://www.hackingapis.com*. Also, keep your skills sharp by participating in CTFs, the PortSwigger Web Security Academy, TryHackMe, HackTheBox, VulnHub, and similar cyber dojos.

Thank you for coming with me this far. May your API hacking experience be filled with prosperous bounties, CVEs, critical vulnerability findings, brilliant exploitation, and detailed reports.

hAPI Hacking!