# B

# ADDITIONAL RESOURCES

## Chapter 0: Preparing for Your Security Tests

Khawaja, Gus. *Kali Linux Penetration Testing Bible*. Indianapolis, IN: Wiley, 2021.

Li, Vickie. *Bug Bounty Bootcamp: The Guide to Finding and Reporting Web Vulnerabilities*. San Francisco: No Starch Press, 2021.

Weidman, Georgia. *Penetration Testing: A Hands-On Introduction to Hacking*. San Francisco: No Starch Press, 2014.

## Chapter 1: How Web Applications Work

Hoffman, Andrew. *Web Application Security: Exploitation and Countermeasures for Modern Web Applications*. Sebastopol, CA: O'Reilly, 2020.

"HTTP Response Status Codes." MDN Web Docs. *https://developer.mozilla.org/en-US/docs/Web/HTTP/Status*.

Stuttard, Dafydd, and Marcus Pinto. *Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*. Indianapolis, IN: Wiley, 2011.

## Chapter 2: The Anatomy of Web APIs

"API University: Best Practices, Tips & Tutorials for API Providers and Developers." ProgrammableWeb. *https://www.programmableweb.com/api-university*.

Barahona, Dan. "The Beginner's Guide to REST API: Everything You Need to Know." APIsec, June 22, 2020. *https://www.apisec.ai/blog/rest-api-and-its-significance-to-web-service-providers*.

Madden, Neil. *API Security in Action*. Shelter Island, NY: Manning, 2020.

Richardson, Leonard, and Mike Amundsen. *RESTful Web APIs*. Beijing: O'Reilly, 2013.

Siriwardena, Prabath. *Advanced API Security: Securing APIs with OAuth 2.0, OpenID Connect, JWS, and JWE*. Berkeley, CA: Apress, 2014.

## Chapter 3: Common API Vulnerabilities

Barahona, Dan. "Why APIs Are Your Biggest Security Risk." APIsec, August 3, 2021. *https://www.apisec.ai/blog/why-apis-are-your-biggest-security-risk*.

"OWASP API Security Project." OWASP. *https://owasp.org/www-project-api-security*.

"OWASP API Security Top 10." APIsecurity.io. *https://apisecurity.io/encyclopedia/content/owasp/owasp-api-security-top-10*.

Shkedy, Inon. "Introduction to the API Security Landscape." Traceable, April 14, 2021. *https://lp.traceable.ai/webinars.html?commid=477082*.

## Chapter 4: Your API Hacking System

"Introduction." Postman Learning Center. *https://learning.postman.com/docs/getting-started/introduction*.

O'Gorman, Jim, Mati Aharoni, and Raphael Hertzog. *Kali Linux Revealed: Mastering the Penetration Testing Distribution*. Cornelius, NC: Offsec Press, 2017.

"Web Security Academy." PortSwigger. *https://portswigger.net/web-security*.

## Chapter 5: Setting Up Vulnerable API Targets

Chandel, Raj. "Web Application Pentest Lab Setup on AWS." Hacking Articles, December 3, 2019. *https://www.hackingarticles.in/web-application-pentest-lab-setup-on-aws*.

KaalBhairav. "Tutorial: Setting Up a Virtual Pentesting Lab at Home." Cybrary, September 21, 2015. *https://www.cybrary.it/blog/0p3n/tutorial-for-setting-up-a-virtual-penetration-testing-lab-at-your-home*.

OccupyTheWeb. “How to Create a Virtual Hacking Lab.” Null Byte, November 2, 2016. *https://null-byte.wonderhowto.com/how-to/hack-like-pro-create-virtual-hacking-lab-0157333*.

Stearns, Bill, and John Strand. “Webcast: How to Build a Home Lab.” Black Hills Information Security, April 27, 2020. *https://www.blackhillsinfosec.com/webcast-how-to-build-a-home-lab*.

## Chapter 6: Discovery

“API Directory.” ProgrammableWeb. *https://www.programmableweb.com/apis/directory*.

Doerrfeld, Bill. “API Discovery: 15 Ways to Find APIs.” Nordic APIs, August 4, 2015. *https://nordicapis.com/api-discovery-15-ways-to-find-apis*.

Faircloth, Jeremy. *Penetration Tester’s Open Source Toolkit.* 4th ed. Amsterdam: Elsevier, 2017.

“Welcome to the RapidAPI Hub.” RapidAPI. *https://rapidapi.com/hub*.

## Chapter 7: Endpoint Analysis

Bush, Thomas. “5 Examples of Excellent API Documentation (and Why We Think So).” Nordic APIs, May 16, 2019. *https://nordicapis.com/5-examples-of-excellent-api-documentation*.

Isbitski, Michael. “AP13: 2019 Excessive Data Exposure.” Salt Security, February 9, 2021. *https://salt.security/blog/api3-2019-excessive-data-exposure*.

Scott, Tamara. “How to Use an API: Just the Basics.” Technology Advice, August 20, 2021. *https://technologyadvice.com/blog/information-technology/how-to-use-an-api*.

## Chapter 8: Attacking Authentication

Bathla, Shivam. “Hacking JWT Tokens: SQLi in JWT.” Pentester Academy, May 11, 2020. *https://blog.pentesteracademy.com/hacking-jwt-tokens-sqli-in-jwt-7fec22adbf7d*.

Lensmar, Ole. “API Security Testing: How to Hack an API and Get Away with It.” Smartbear, November 11, 2014. *https://smartbear.com/blog/api-security-testing-how-to-hack-an-api-part-1*.

## Chapter 9: Fuzzing

“Fuzzing.” OWASP. *https://owasp.org/www-community/Fuzzing*.

## Chapter 10: Exploiting Authorization

Shkedy, Inon. “A Deep Dive on the Most Critical API Vulnerability—BOLA (Broken Object Level Authorization).” *https://inonst.medium.com*.

## Chapter 11: Mass Assignment

"Mass Assignment Cheat Sheet." OWASP Cheat Sheet Series. *https://cheatsheetseries.owasp.org/cheatsheets/Mass_Assignment_Cheat_Sheet.html*.

## Chapter 12: Injection

Belmer, Charlie. "NoSQL Injection Cheatsheet." Null Sweep, June 7, 2021. *https://nullsweep.com/nosql-injection-cheatsheet*.

"SQL Injection." PortSwigger Web Security Academy. *https://portswigger.net/web-security/sql-injection*.

Zhang, YuQing, QiXu Liu, QiHan Luo, and XiaLi Wang. "XAS: Cross-API Scripting Attacks in Social Ecosystems." *Science China Information Sciences* 58 (2015): 1–14. *https://doi-org.ezproxy.sfpl.org/10.1007/s11432-014-5145-1*.

## Chapter 13: Applying Evasive Techniques and Rate Limit Testing

"How to Bypass WAF HackenProof Cheat Sheat." Hacken, December 2, 2020. *https://hacken.io/researches-and-investigations/how-to-bypass-waf-hackenproof-cheat-sheet*.

Simpson, J. "Everything You Need to Know About API Rate Limiting." Nordic APIs, April 18, 2019. *https://nordicapis.com/everything-you-need-to-know-about-api-rate-l*

*imiting*.

## Chapter 14: Attacking GraphQL

"How to Exploit GraphQL Endpoint: Introspection, Query, Mutations & Tools." YesWeRHackers, March 24, 2021. *https://blog.yeswehack.com/yeswerhackers/how-exploit-graphql-endpoint-bug-bounty*.

Shah, Shubham. "Exploiting GraphQL." Asset Note, August 29, 2021. *https://blog.assetnote.io/2021/08/29/exploiting-graphql*.

Swiadek, Tomasz, and Andrea Brancaleoni. "That Single GraphQL Issue That You Keep Missing." Doyensec, May 20, 2021. *https://blog.doyensec.com/2021/05/20/graphql-csrf.html*.

## Chapter 15: Data Breaches and Bug Bounties

"API Security Articles: The Latest API Security News, Vulnerabilities & Best Practices." APIsecurity.io. *https://apisecurity.io*.

"List of Bug Bounty Writeups." Pentester Land: Offensive InfoSec. *https://pentester.land/list-of-bug-bounty-writeups.html*.