HACK HARD

THE ULTIMATE GUIDE OF API HACKING RESOURCES

BY DANA EPP

v220930

Over the years I have collected a lot of different resources that have helped me along my API hacking journey. I've combined all those resources into a single comprehensive guide of API hacking resources.

I hope you find it useful.

As you continue on your own journey to improve your API hacking tradecraft, feel free to check these resources out. Know any great resources not listed here? Drop me a line and let me know... I might include it in the next revision!

Hack hard!

- Dana Epp (aka SilverStr)

TABLE OF CONTENTS

HTTP Fundamentals

Before you can really hack on APIs, you need to know the fundamentals of how HTTP works. Here are some great resources to start with:

- **Basics of HTTP** - Mozilla's in-depth guide to everything about HTTP
- **HTTP Status Codes** - Mozilla's in-depth guide to HTTP response codes
- **Know your HTTP Well** - HTTP encodings, headers, media types, methods, relations, and status codes, all summarized and linked to their specification.
- **Know your HTTP Headers** - A simplified and comprehensive table of HTTP headers important for API security, stored in a single PDF.
- **Know your HTTP Methods** - A simplified and comprehensive table of HTTP methods used in API requests, stored in a single PDF.
- **Know your HTTP Status Codes** - A simplified and comprehensive table of HTTP status codes used in API calls, stored in a single PDF.

API Protocols and Specifications

With the fundamentals of how the web works under your belt, you're ready to understand the different API protocols and specifications that are out there.

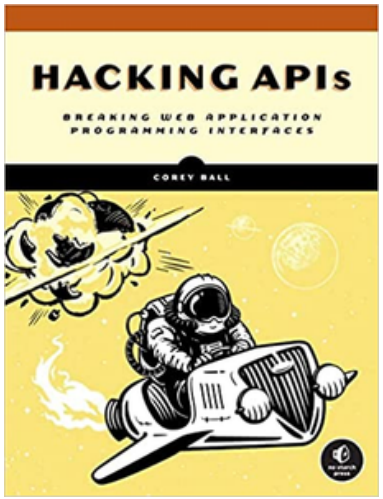
Here is a list of some of the more important ones you should really understand:

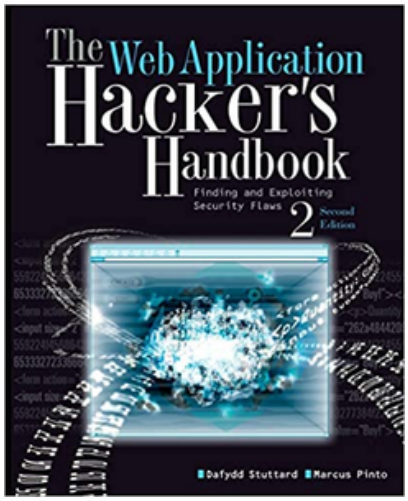
- **AsyncAPI** - The AsyncAPI Specification is a project used to describe and document message-driven APIs in a machine-readable format. It's protocol-agnostic, so you can use it for APIs that work over any protocol (e.g., AMQP, MQTT, WebSockets, Kafka, STOMP, HTTP, Mercure, etc).
- **GraphQL** - GraphQL is a query language designed to build client applications by providing an intuitive and flexible syntax and system for describing their data requirements and interactions.
- **JSON API** - JSON:API is a specification for how a client should request that resources be fetched or modified, and how a server should respond to those requests.
- **JSON-RPC** - JSON-RPC is a stateless, light-weight remote procedure call (RPC) protocol.
- **OpenAPI** - The OpenAPI Specification (OAS) defines a standard, language-agnostic interface to RESTful APIs which allows both humans and computers to discover and understand the capabilities of the service without access to source code, documentation, or through network traffic inspection.
- **RAML** - RAML is a language for the definition of HTTP-based APIs that embody most or all of the principles of Representational State Transfer (REST).
- **SOAP** - SOAP is a lightweight protocol intended for exchanging structured information in a decentralized, distributed environment. It uses XML to define an extensible messaging framework providing a message construct that can be exchanged over a variety of underlying protocols.
- **Standards.REST** - A collection of standards and specifications, that help make fantastic HTTP/REST APIs.
- **XML-RPC** - XML-RPC is a set of implementations that allow software running on disparate operating systems, running in different environments to make procedure calls over the Internet. It's remote procedure calling using HTTP as the transport and XML as the encoding.

BOOKS

Physical Books

If you're interested in learning how to hack web apps and APIs, then you need to check out these books. These are some of my favorite books on the subject, and they will teach you everything you need to know to improve.





- **Hacking APIs: Breaking Web Application Programming Interfaces**
- **The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws**
- **Web Application Security: Exploitation and Countermeasures for Modern Web Applications**

Online Books & Wikis

Many people before me have collected a bunch of API hacking information and shared it online. Here are some of the more useful ones I have come across:

- **API Pentest Book** - API penetration testing notes
- **API Security Empire** - Aims to present unique attack & defense methods in the API Security field
- **GraphQL Pentesting** - HackTrick's online book for hacking GraphQL
- **Web API Pentesting** - HackTrick's online book for hacking web APIs

Cheatsheets & Checklists

There are plenty of cheat sheets and checklists on the Internet that has been created to give a quick summary of high-value information on application and API security issues. The following are some of the most useful ones I've found that will assist you in your API hacking journey.

Cheatsheets

- API Security Top 10
- GraphQL
- Injection Prevention
- JSON Web Token (JWT) Security
- Microservices Security
- REST Assessment
- REST Security

Checklists

- API Penetration Testing
- API Testing
- API Security Testing

API Hacking Articles

OK. So we can all google to find articles and blog posts on hacking APIs. But with the tens of millions of results that come back, where do you begin? Here are some of the resources I've bookmarked over the years that are a great starting point:

- The Beginner's Guide to API Hacking
- API and microservice security
- Finding and Exploiting Unintended Functionality in Main Web App APIs
- How To Hack API In 60 Minutes With Open Source Tools
- How to Hack APIs in 2021
- How to Hack an API and Get Away with It
- How to Detect the Programming Language of an API
- How to exploit GraphQL endpoint: introspection, query, mutations & tools
- Notes from Hacking APIs from Bug Bounty Bootcamp
- How to craft rogue API docs for a target when they don't exist
- Sample API Penetration Testing Report
- Scanning APIs with Burp Scanner
- Simplifying API Pentesting With Swagger Files
- SOAP Security: Top Vulnerabilities and How to Prevent Them
- Using Burp to Enumerate a REST API
- Exploit APIs with cURL
- How to Make Money Hacking APIs
- When to give up on an API target

Deliberately Vulnerable APIs

Deliberately Vulnerable APIs (DVAs) are a type of API that is purposely created to be vulnerable to attack. While this may sound counterintuitive, DVAs can actually be a valuable tool for practicing API hacking.

Below are a bunch of different targets you can hack on.

- **APISandbox** - Pre-Built Vulnerable Multiple API Scenarios Environments Based on Docker-Compose
- **crAPI** - Completely ridiculous API (crAPI) will help you to understand the ten most critical API security risks.
- **Damn Vulnerable GraphQL App** - An intentionally vulnerable implementation of Facebook's GraphQL technology,
- **DVMS** - The Damn Vulnerable Microservice is written in many languages to demonstrate OWASP API Top Security Risks
- **DVWS-Node** - Damn Vulnerable Web Services is a vulnerable application with a web service and an API that can be used to learn about web services/API-related vulnerabilities.
- **Generic University** - InsiderPhD's Laravel demo app that is purposely vulnerable to a number of vulnerabilities on the OWASP API Top 10.
- **VAmPI** - VAmPI is a vulnerable API made with Flask and it includes vulnerabilities from the OWASP top 10 vulnerabilities for APIs.
- **vAPI** - vAPI is a Vulnerable Adversely Programmed Interface which is Self-Hostable API that mimics OWASP API Top 10 scenarios through Exercises.
- **vulnerable-graphql-api** - A very vulnerable implementation of a GraphQL API.
- **WebSheep** - WebSheep is an app based on willingly vulnerable ReSTful APIs.

Want practice hacking APIs?

Use my private walkthrough room on TryHackMe to practice hacking against the **OWASP API Security TOP 10**.

https://tryhackme.com/jr/vulnapi

Don't have a TryHackMe account?
Sign up **FREE** here.

API Fuzzing

API fuzzing is a type of testing that is used to find vulnerabilities in application programming interfaces (APIs). It works by feeding the API random data (ie: wordlists) and then monitoring the API's response. If the API responds in an unexpected way, it may be due to a security flaw or could be exposing unknown or undocumented endpoints.

Having good wordlists, and knowing how to use them, can go a long way in your API hacking journey. Below is a list of some of the better resources for this.

Fuzzing

- **Fuzzing APIs** - Fuzzing APIs chapter from "The Fuzzing Book"
- **Fuzz Vectors** - OWASP's guidance on fuzzing in their Web Security Testing Guide (WSTG)
- **RESTler: Stateful REST API Fuzzing** - Microsoft's research on REST API fuzzing

Wordlists

- **API endpoints & objects** - 3203 common API endpoints and objects designed for fuzzing.
- **API HTTP Request Methods** - HTTP requests methods wordlist from SecLists
- **API Routes wordlist** - AssesNote's collection of API routes
- **api_wordlist** - SecList's collection of API names used for fuzzing web application APIs.
- **Common API endpoints** - SecList's collection of API endpoints
- **GraphQL wordlist** - SecList's collection of GraphQL endpoints
- **Hacking-API wordlists** - hAPI Hacker's collection of API paths and wordlists
- **Kiterunner wordlist** - AssestNote's collection of API wordlists for Kiterunner
- **Swagger / OpenAPI wordlist** - SecList's collection of wordlists for finding API docs
- **Bug Bounty Wordlists** - A collection of wordlist good for bug bounties

API Hacking Videos and Podcasts

Some people learn better when they can hear and/or see others demonstrate it for them. There are so many resources online for this these days that there is no way I could list them all.

However, here are some resources that I find really level sets anyone who is getting into API hacking. I hope you find them as helpful as I did.

Webinars

- **API Security Testing for Hackers** from BugCrowd's LevelUp
- **Bad API, hAPI Hackers!** from BugCrowd's LevelUp
- **Hidden in Plain Site: Disclosing Information via Your APIs** from BugCrowd's LevelUp
- **REST in Peace: Abusing GraphQL to Attack Underlying Infrastructure** from BugCrowd's LevelUp
- **A Hacker's View of APIs: Vulnerabilities, Exploits and Defense Options** from Ping Identity TV

YouTube Playlists

- **API Hacking** by Hack the Planet
- **API hacking with Postman** by The XSS rat
- **Everything API Hacking** by InsiderPhd

Podcasts

- **Erez Yalon -- The OWASP API Security Project**
- **The Hacker Mind Podcast: Hacking APIs**
- **Troy Hunt: Hack Your API-Security Testing**
- **We Hack Purple - API Security Best Practices**
- **When it comes to API security, expect the whole world to be testing your mettle, says Twitter CISO**

API Hacking Courses and Content

Some people like to invest time and money into their career with online courses, mailing lists and LinkedIn Groups.

Here are some resources that I find useful for anyone who is getting into API hacking. Please let me know if you have any vendor-neutral resources to add here!

Online Courses

- **API Security Certified Expert**
- **Hacking REST APIs - A beginner's guide**
- **API Security Testing Guide by The XSS Rat**
- **Rest API Testing (Automation) from Scratch-Rest Assured Java**

Mailing Lists and Groups

- **The API Security Newsletter** by APISecurity.io
- **The API Hacker's Inner Circle** by Dana Epp (hey, that's me :))
- **API security community** by Wallarm

Other

- **The Daily Swig - Latest API security news** by PortSwigger

API Hacking Tools

Last, but certainly not least is a list of tools that can help you in hacking APIs. I left it to the end of this resource guide as this is a VERY personal choice; each hacker will have their own quiver of tools that they prefer to use.

Find what works for you. While I'm a fan of *Burp* you might like *ZAP*. While I like *feroxbuster*, you might like *ffuf*. While *vi* is the only editor you need, you might feel *Word* is right for you. Use what works for YOU.

At the very least though, learn about other tools to see what works with your methodology. What is below are some of the more common tools used during API hacking.

- **APICheck** - The DevSecOps toolset for REST APIs.
- **APIClarity** - Reconstruct Open API Specifications from real-time workload traffic seamlessly.
- **APIFuzzer** - Fuzz test your application using your OpenAPI or Swagger API definition without coding
- **APIKit** - Discovery, Scan and Audit APIs Toolkit All In One.
- **Arjun** - HTTP parameter discovery suite.
- **Astra** - Automated Security Testing For REST API's
- **Automatic API Attack Tool** - Imperva's customizable API attack tool takes an API specification as an input, and generates and runs attacks that are based on it as an output.
- **BatchQL** - GraphQL security auditing script with a focus on performing batch GraphQL queries and mutations.
- **Burp Suite** - Robust app security testing tool capable of attacking APIs
- **CATS** - A REST API Fuzzer and negative testing tool for OpenAPI endpoints
- **Cherrybomb** - A CLI tool that helps you avoid undefined user behaviour by validating your API specifications.
- **clairvoyance** - Obtain GraphQL API schema despite disabled introspection!.

API Hacking Tools (continued)

- **ffuf** - Fast web fuzzer written in Go
- **fuzzapi** - A tool used for REST API pentesting and uses API_Fuzzer gem.
- **fuzz-lightyear** - A pytest-inspired, DAST framework, capable of identifying vulnerabilities in a distributed, micro-service ecosystem through chaos engineering testing and stateful, Swagger fuzzing.
- **GraphQLmap** - GraphQLmap is a scripting engine to interact with a graphql endpoint for pentesting purposes.
- **graphql-path-enum** - Tool that lists the different ways of reaching a given type in a GraphQL schema.
- **graphql-playground** - GraphQL IDE for better development workflows
- **graphql-threat-matrix** - GraphQL threat framework used by security professionals to research security gaps in GraphQL implementations.
- **graphw00f** - graphw00f is GraphQL Server Engine Fingerprinting utility for software security professionals looking to learn more about what technology is behind a given GraphQL endpoint.
- **gotestwaf** - An open-source project to test different web application firewalls (WAF) for detection logic and bypasses
- **InQL** - A Burp Extension for GraphQL Security Testing.
- **kiterunner** - Contextual Content Discovery Tool great for finding API endpoints
- **mitmproxy2swagger** - Automagically reverse-engineer REST APIs via capturing traffic
- **PostMan** - API platform for developers to design, build, test and iterate their APIs
- **RESTler** - RESTler is the first stateful REST API fuzzing tool for automatically testing cloud services through their REST APIs and finding security and reliability bugs in these services.
- **SoapUI** - SoapUI is a free and open-source cross-platform functional testing solution for APIs and web services
- **Swagger-EZ** - A tool geared towards pentesting APIs using OpenAPI definitions.

API Hacking Tools (continued)

- **TnT-Fuzzer** - OpenAPI 2.0 (Swagger) fuzzer.
- **wadl-dumper** - Dump all available paths and/or endpoints on WADL file.
- **Wsdler** - WSDL Parser extension for Burp.
- **wsdl-wizard** -WSDL Wizard is a Burp Suite plugin written in Python to detect current and discover new WSDL (Web Service Definition Language) files.
- **Zed Attack Proxy (ZAP)** - Web app scanner capable of attacking APIs

FIN