THE ULTIMATE GUIDE OF API HACKING RESOURCES

By:Mahmoud ibrahim

follow me :

Linkedin :link: https://www.linkedin.com/in/mahmoud-ibrahim-9b5364244

github:https://github.com/Az0x7

API Hacking Tools

- 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!.
- ffuf - Fast web fuzzer written in Go
- fuzzapi - A tool used for REST API pentesting and uses API_Fuzzer gem.
- GraphQLmap - GraphQLmap is a scripting engine to interact with a graphql endpoint for pentesting purposes.
- graphql-playground - GraphQL IDE for better development workflows
- 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.

HTTP Fundamentals

- 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 Status Codes - A simplified and comprehensive table of HTTP status codes used in API calls, 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

API Protocols and Specifications

- 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.

API Hacking Videos and Podcasts

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

Floating Topic

API Fuzzing

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

BOOKS

- 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

if you need any book send me

online article

- https://pentestbook.six2dez.com/enumeration/webservices/apis
- https://github.com/cyprosecurity/API-SecurityEmpire
- https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/graphql
- https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/web-api-pentesting

Cheatsheets & Checklists

Cheatsheets

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

Checklists

- API Penetration Testing
- API Testing
- API Security Testing

Deliberately Vulnerable APIs

- 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.

API Hacking Articles

- 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 exploit GraphQL endpoint: introspection, query, mutations & tools
- Notes from Hacking APIs from Bug Bounty Bootcamp
- 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