APIcalypse Now

Hunting APIs to Profit 💰

Nithin Ravi

#opentowork

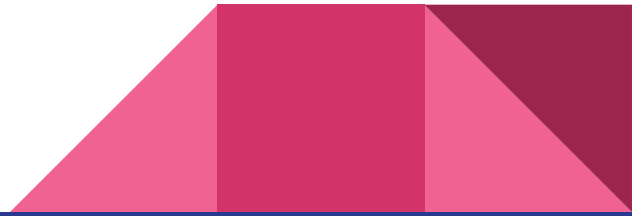
$whoami || @thebinarybot

- Masters in ISM at University of Galway 🎓
- Ex-Security Solutions Engineer ⚒️
- Security Nerd / Developer 🦹
- Holds eJPT, CRTP 🥳
- Content Creator ⭐

- More about me at https://thebotsite.com

Agenda

- What is an API?
  - Classifications, Types and Nuances
  - Why hack them?
- API Reconnaissance
  - Passive Recon
  - Active Recon
- Authorization Vulnerabilities
  - BOLA
  - BFLA
- Miscellaneous
  - Other Classes
  - Generic Tips



What is an API?

API and Classifications

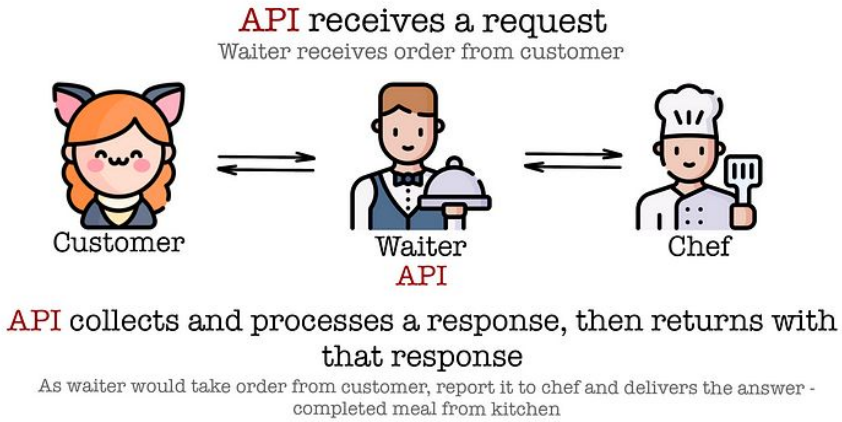
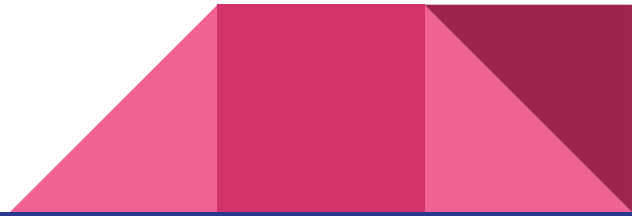


Image Source:
https://medium.com/@data.science.enthusiast
https://decentro.tech

Types of API

- Rest APIs
  - “RESTful APIs”
  - Return data in either JSON or plain text format
  - Have a defined structure or pattern

- GraphQL
  - REST returns fixed data structures, while GraphQL is organized by schema and type system.
  - GraphQL can fetch all data in a single request, while REST often requires multiple requests.



Why Hack APIs?

APIs Drive the Majority of Internet Traffic and Cybercriminals are Taking Advantage

Mar 19, 2024 · The Hacker News · API Security / Vulnerability

Application programming interfaces (APIs) are the connective tissue behind digital modernization, helping applications and databases exchange data more effectively. The State of API Security in 2024 Report from Imperva, a Thales company, found that the majority of internet traffic (71%) in 2023 was API calls. What's more, a typical enterprise site saw an average of 1.5 billion API calls in 2023.

The expansive volume of internet traffic that passes through APIs should be concerning for every security professional. Despite best efforts to adopt shift-left frameworks and SDLC processes, APIs are often still pushed into production before they're cataloged, authenticated, or audited. On average, organizations have 613 API endpoints in production, but that number is rapidly expanding as pressure grows to deliver digital services to customers more quickly and efficiently. Over time, these APIs can become risky, vulnerable endpoints.

— Trending News


THN Weekly Recap: Top Cybersecurity Threats, Tools and Tips


Top 10 Cybersecurity Trends to Expect in 2025

THN Weekly Recap: Top Cybersecurity Threats, Tools and Tips [6 Jan]


LDAPNightmare PoC Exploit Crashes LSASS and Reboots Windows Domain Controllers


New "DoubleClickjacking" Exploit Bypasses Clickjacking Protections on Major Websites

Show More

— Popular Resources

Issue 17: 83 percent of web traffic is API, and why query parameters are bad for secrets

February 7, 2019

Share this article:

This week we are mostly discussing best practices and tools, such as:

- The best methods to pass API keys and other sensitive data
- Tools that attackers use to discover APIs
- Why API security is never set-&-forget

Risks

Never put API keys or other sensitive information in **URLs or query parameters**. These are visible to browser extensions, server logs, browser history, shared links, and as the referrer address. Always use headers or `POST` method instead. See this article by Paris Mitton for details.

Landscape of API Traffic

2022-01-26


Daniele Molteni

10 min read

In recent years we have witnessed an explosion of Internet-connected applications. Whether it is a new mobile app to find your soulmate, the latest wearable to monitor your vitals, or an industrial solution to detect corrosion, our life is becoming packed with connected systems.

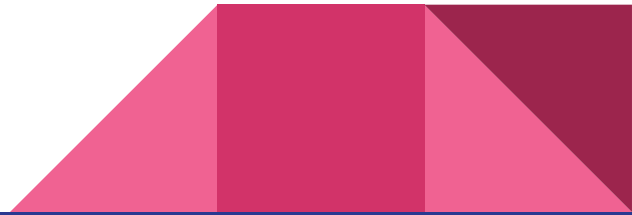
API Reconnaissance

Reconnaissance

- Search for API documentation
- Lookout for: api, swagger, openapi
  - Build your own documentation
- Monitor URLs while general browsing
- Interesting Subdomains:
  - api
  - uat
  - dev
  - test

Passive Reconnaissance

- Google Dorking:
  - target api
  - inurl:/wp-json/wp/v2/users
  - inurl:"/api/v1" intext:"index of /"
- Github Dorking:
  - target extension:.json
  - target filename:swagger.json
- Shodan Dorking:
  - content-type: application/json.
  - wp-json



Active Reconnaissance

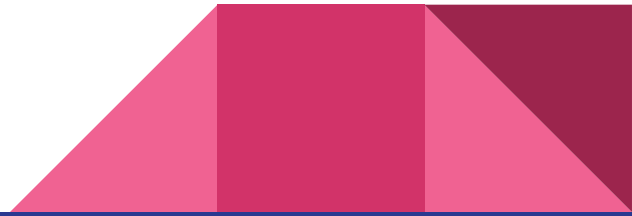
- Amass:
  - `amass enum -active -brute -w API_Wordlist -d [target domain] -dir [output directory name]`
- Gobuster:
  - `gobuster dir -u https://targetaddress/ -w your_api_wordlist -x 200,202,301 -b 302`
- Kiterunner:
  - Brute Force: `cat hosts | kr brute - -w wordlist.txt -e aspx,asmx,ashx,asp --dirsearch-compat`
  - Quick Scan: `kr scan targetIP -w ~/api/wordlists/data/kiterunner/routes-large.kite`

If you see the server responding uniquely to requests to certain /api/ paths, then it's a nice indication to show that the API exists.

Authorization Vulnerabilities

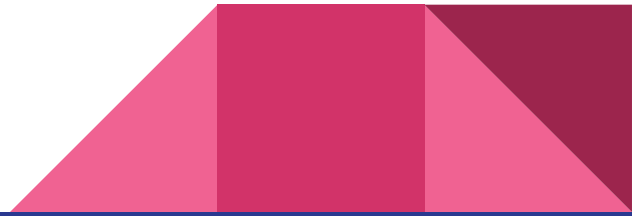
BOLA

- BOLA stands for Broken Object Level Authorization.
- Misconfigured authorization controls will let UserA access resources of UserB (and more).
- APIs use values, such as names or numbers, to identify various objects.



Find Resource IDs and Requests

- GET /api/resource/**1**
- GET /user/account/find?**user_id=15**
- POST /company/account/**Apple**/balance
- POST /admin/pwreset/account/**90**



Testing Strategy

- Create a UserA account.
- Use the API and discover requests that involve resource IDs as UserA.
- Document requests that include resource IDs and should require authorization.
- Create a UserB account.
- Obtaining a valid UserB token and attempt to access UserA's resources.

Testing Mechanisms

Type	Request	Request Tampered
Predictable ID	GET /api/v1/user/222	GET /api/v1/user/333
Integer as ID	POST /api/v1/user {“Account”:2222}	POST /api/v1/user {“Account”:[3333]}
Nested Object	POST /api/v1/user {“Account”:2222}	POST /api/v1/user {“Account”:{“Account”: 3333}}
Multiple Objects	POST /api/v1/user {“Account”:2222}	POST /api/v1/user {“Account”:2222, “Account”:3333, “Account”:4444}

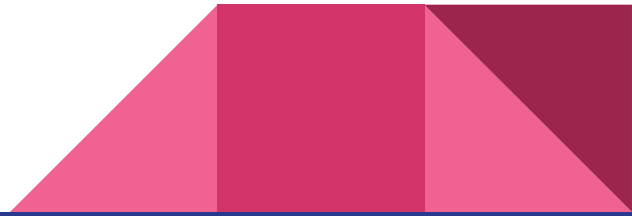
and so on...

BFLA

- BFLA stands for Broken Function Level Authorization.

  While BOLA is all about accessing resources that do not belong to you, BFLA is all about performing unauthorized actions.

- Think of requests where CRUD operations can be performed
- Do A-B-A testing



Miscellaneous

Other Vulnerabilities

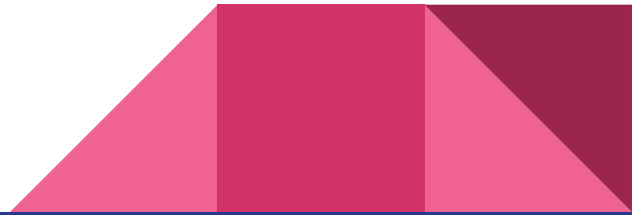
- Injection Attacks:
  - What happens when you enter negative number, 0, unicode character?
- Mass Assignment Attacks
  - Send unexpected parameters in request body
  - isAdmin:true
- Server Side Parameter Pollution
  - Inject Parameters
  - Truncate information using syntax characters
  - `GET /users/search?name=peter&publicProfile=true -> GET /userSearch?name=peter%23foo&back=/home`

And more…

Tips

- Version Checks
  - /api/v2/register exists? Check /api/v1/register
- Got SSRF?
  - Perform internal port scanning
  - Leverage cloud services
- Multiple ways to authentication API?
  - /api/v3
  - /api/mobile
  - /api/link

Get creative 🤘



Connect With Me - @thebinarybot