

A person wearing a dark hoodie is seen from behind, sitting at a desk. In front of them are several computer monitors. The monitors display various types of data: some show lines of code in a dark-themed editor, others show tables of data with columns and rows, and one shows a world map. Overlaid on the entire image is large, bold text. The text 'STEP-BY-STEP' is in white, 'GUIDE TO' is in yellow, 'PERFORM' is in yellow, 'PASSIVE' is in orange, and 'API RECON' is in white. The background is a dark, slightly blurred image of the person and their workspace.

When we are gathering information about an **API** we use two different methods :

Passive Recon and **Active** Recon.

Passive Reconnaissance: in which we don't interact directly with the API or the provider of the API, However we use the **Open Source Intelligence (OSINT)** to get as much information as possible.

What we are looking after when we recon an API is :

- **Public information** about the API
- **Documentations** about an API
- Exposed **Credentials or Tokens**
- **Version** information
- API business purpose to **get better understanding** about the expected functionality

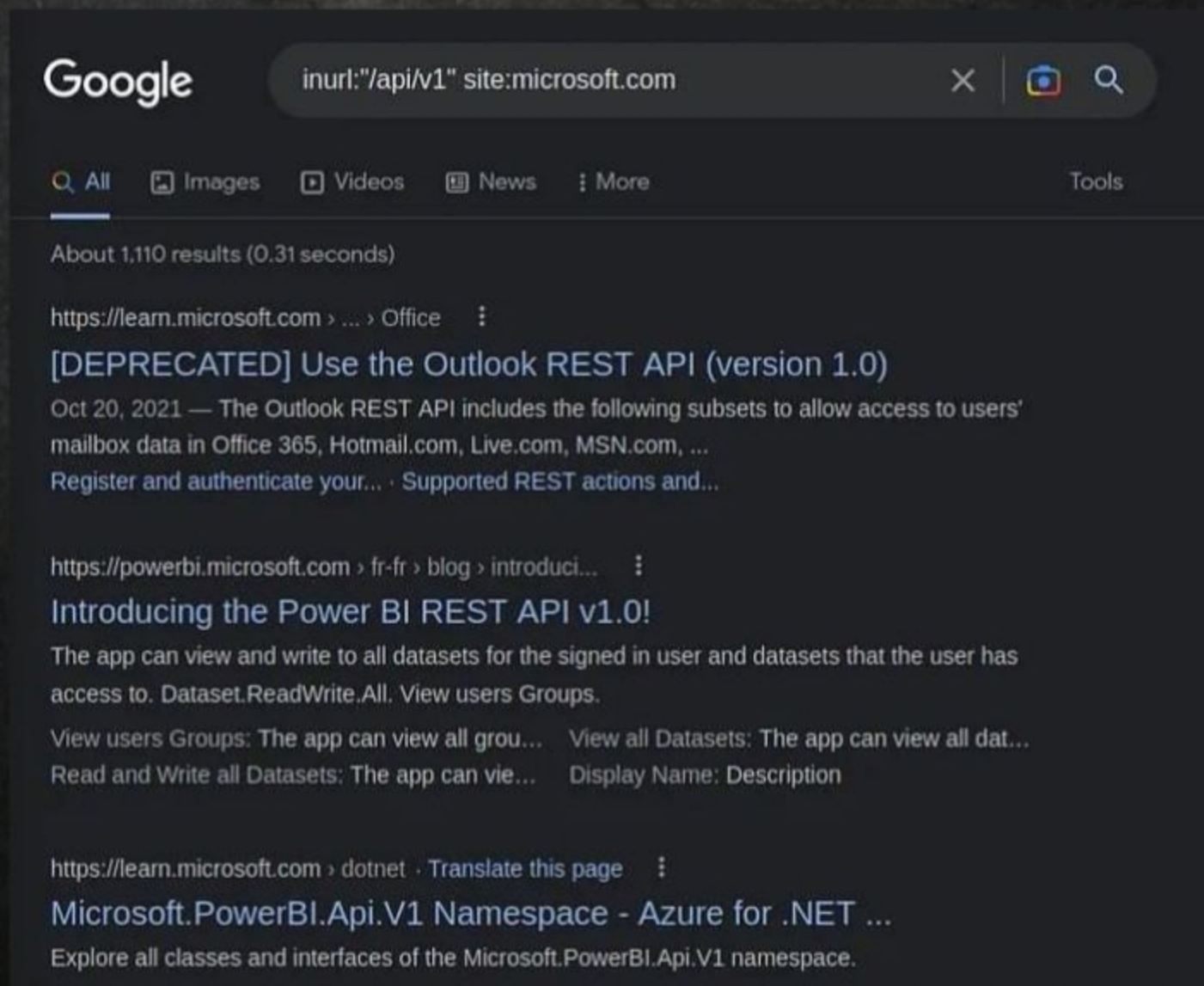
We will use the following tools/sites to perform our Passive Recon :

- Google/Search Engines
- Github/ Git dorking
- Shodan
- The Wayback Machine

Google/Search Engines

Here we can use the google filtering **techniques** (**Google Dork**) to get more results like :

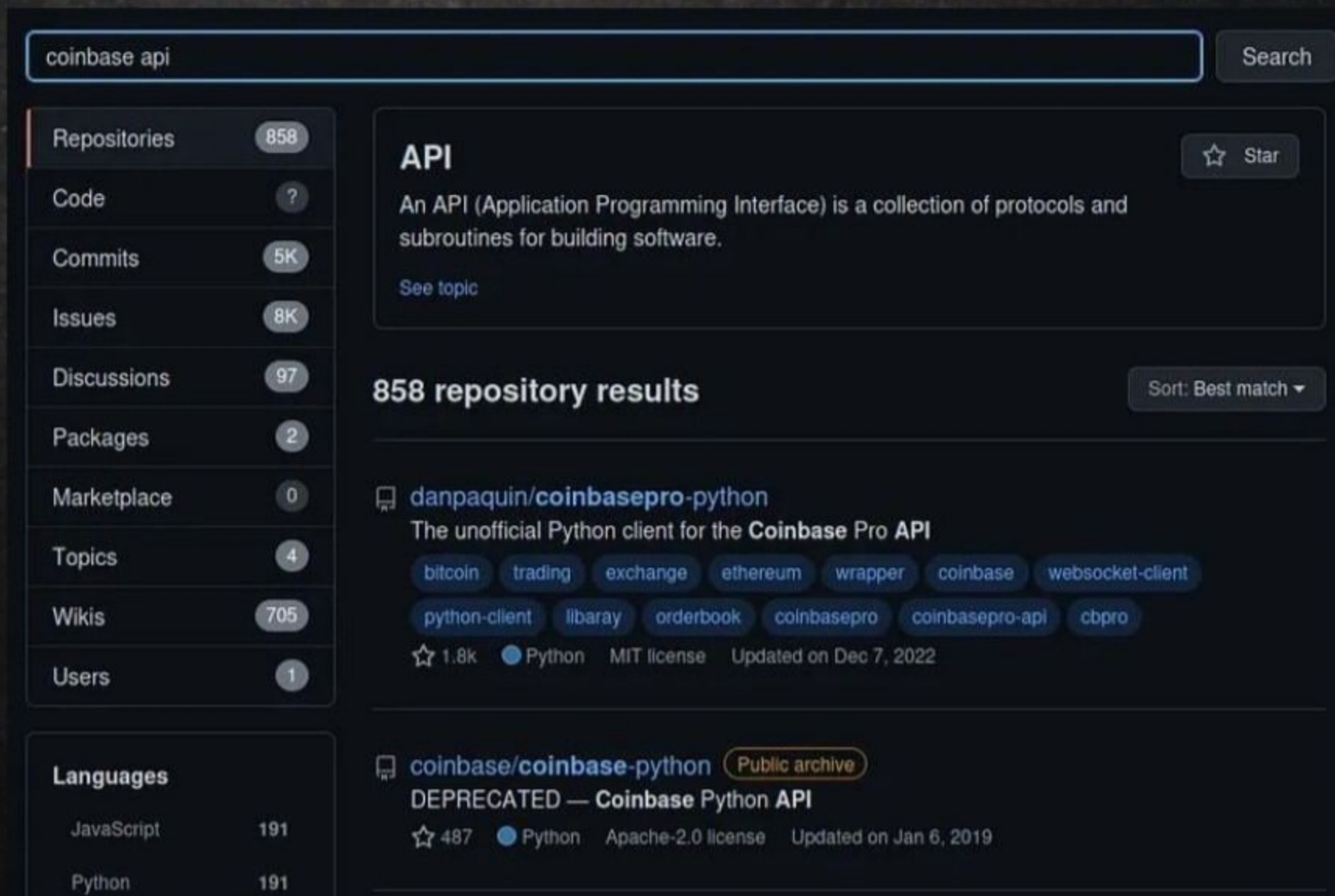
```
inurl:"/api/v1" site:microsoft.com
```



Github Dorking

our next is we can search using Github and try to get juicy information by using **Github Dorking**. in the Github search bar we can search for the site that we are looking:

for example (coinbase api)



The screenshot shows a GitHub search interface with the query 'coinbase api' entered in the search bar. The left sidebar displays filters for Repositories (858), Code (?), Commits (5K), Issues (8K), Discussions (97), Packages (2), Marketplace (0), Topics (4), Wikis (705), and Users (1). Below these are language filters for JavaScript (191) and Python (191). The main content area shows the 'API' topic description and a list of 858 repository results. The top result is 'danpaquin/coinbasepro-python', described as 'The unofficial Python client for the Coinbase Pro API', with tags like 'bitcoin', 'trading', 'exchange', 'ethereum', 'wrapper', 'coinbase', 'websocket-client', 'python-client', 'library', 'orderbook', 'coinbasepro', 'coinbasepro-api', and 'cbpro'. It has 1.8k stars, is Python-based, uses the MIT license, and was updated on Dec 7, 2022. The second result is 'coinbase/coinbase-python', marked as a 'Public archive' and 'DEPRECATED — Coinbase Python API', with 487 stars, Python-based, Apache-2.0 license, and updated on Jan 6, 2019.

coinbase api Search

Repositories 858

Code ?

Commits 5K

Issues 8K

Discussions 97

Packages 2

Marketplace 0

Topics 4

Wikis 705

Users 1

Languages

JavaScript 191

Python 191

API ☆ Star

An API (Application Programming Interface) is a collection of protocols and subroutines for building software.

[See topic](#)

858 repository results Sort: Best match ▾

📦 [danpaquin/coinbasepro-python](#)

The unofficial Python client for the **Coinbase Pro API**

bitcoin trading exchange ethereum wrapper coinbase websocket-client

python-client library orderbook coinbasepro coinbasepro-api cbpro

☆ 1.8k ● Python MIT license Updated on Dec 7, 2022

📦 [coinbase/coinbase-python](#) **Public archive**

DEPRECATED — Coinbase Python API

☆ 487 ● Python Apache-2.0 license Updated on Jan 6, 2019

Few more github dorks :

`(api key exposed)`

`extensions:json`


`("Authorization: Bearer")`

`(filename:swagger.json)`


Shodan

We can also use Shodan to gain information about **particular API** and we can get **information** by using the following search :

“content-type: application/json”

 SHODAN


content-type: application/json



TOTAL RESULTS


4,606,350


TOP COUNTRIES



United States	1,791,004
Korea, Republic of	688,681
China	346,158
Germany	255,321
Ireland	218,550

[More...](#)

 View Report


 View on Map

Partner Spotlight: Looking for a place to store all the Shodan data? Check out [Grawwell](#)

13.55.182.49

api.prod.sprigg
y.com.au
api.prod.next-a
pp.com.au
ec2-13-55-182-
49.ap-southeas
t-2.compute.a
mazonaws.co
m
Amazon
Corporate
Services Pty
Ltd
Australia, Sydney

cloud

 SSL Certificate

Issued By:
|- Common
Name:
Amazon
|-
Organization:
Amazon

Issued To:
|- Common
Name:
api.prod.sprigg
y.com.au

Supported SSL
Versions:
TLSv1.2

HTTP/1.1 404 Not Found

Date: Tue, 31 Jan 2023 22:21:34 GMT

Content-Type: application/json; charset=utf-8

Content-Length: 48

Connection: keep-alive

X-Kong-Response-Latency: 0

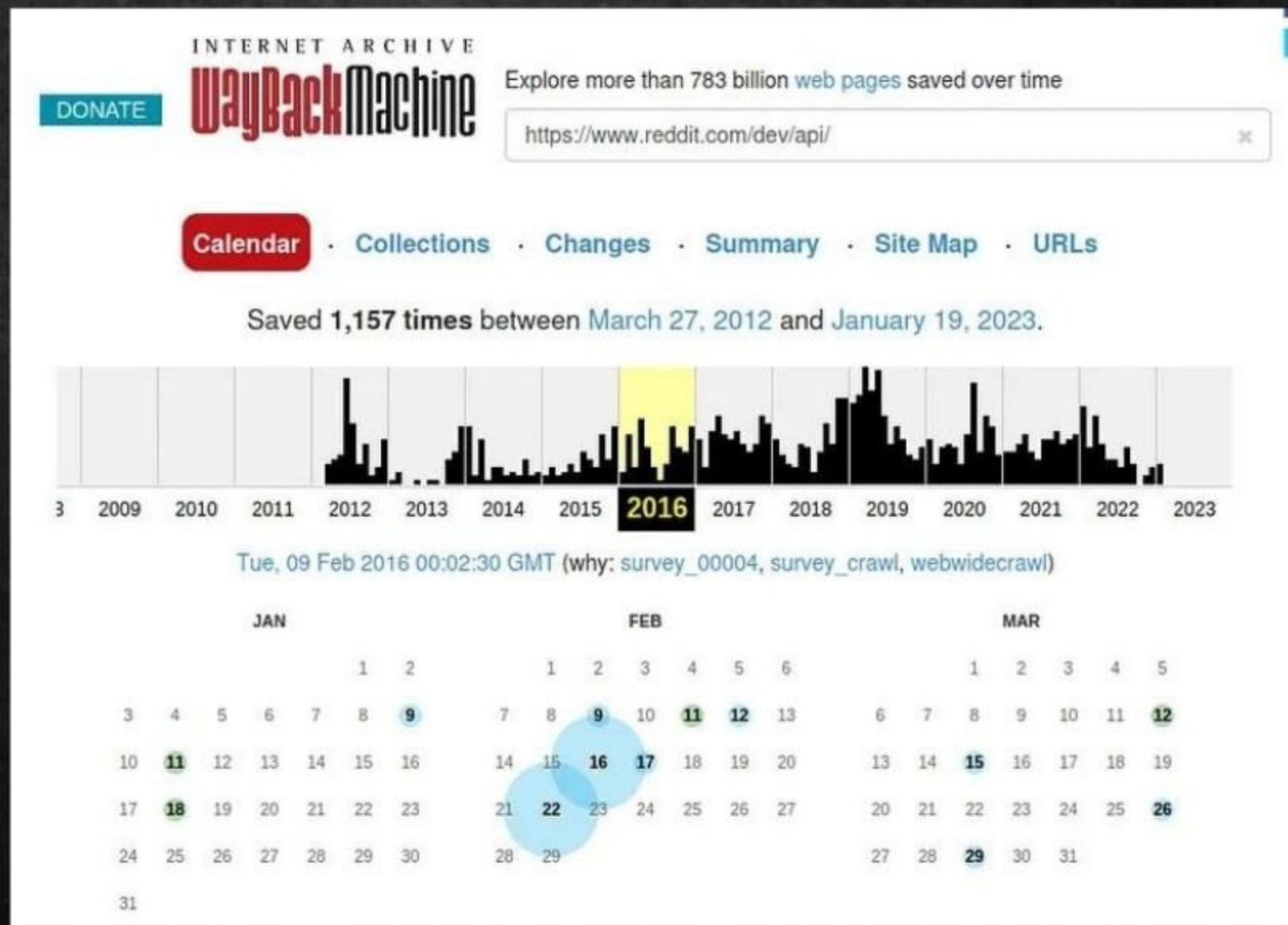
Server: kong/2.8.1

2023-01-31T22:26:38.398457

Wayback Machine

Finally we can gather information about **old versions of an API** from the Wayback machine by **writing** in the search bar the following :

`https://example.com/dev/api/`



SHARE AND AWARE

