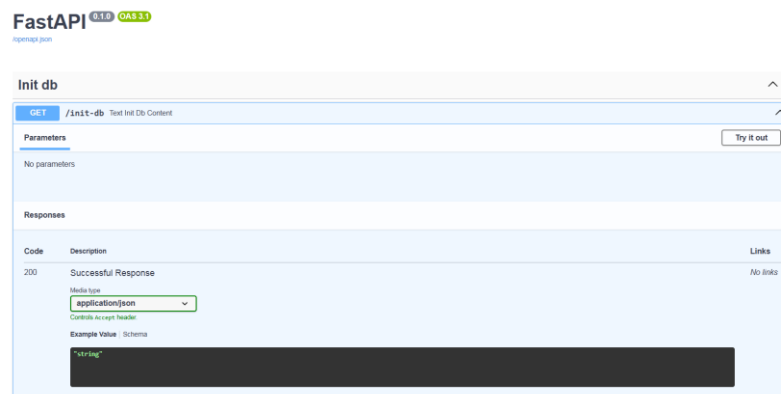


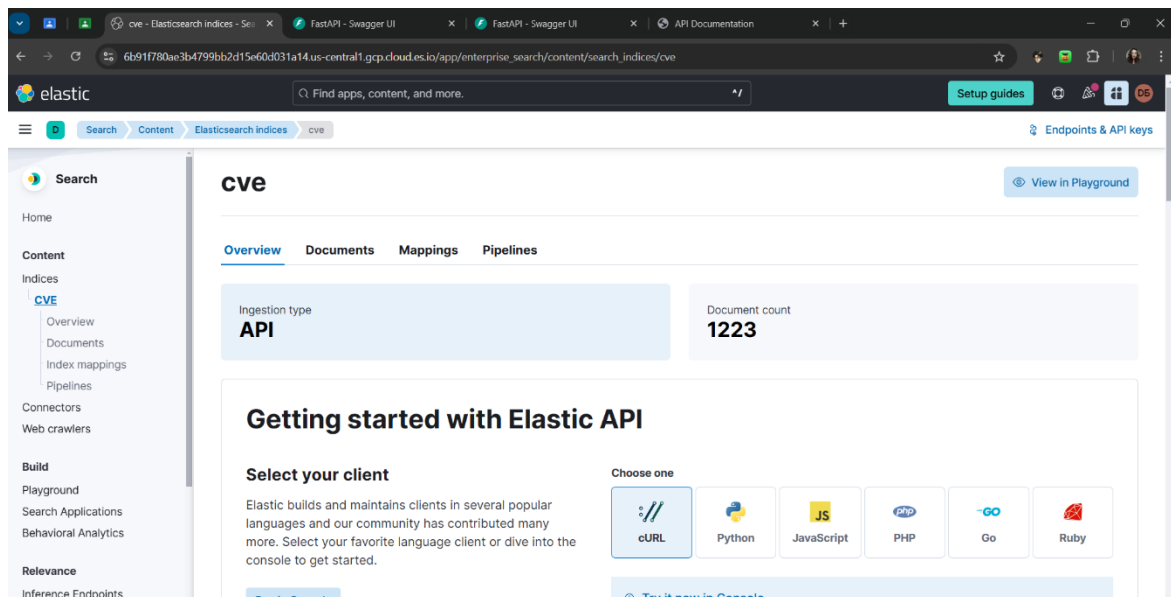
РЕЗУЛЬТАТ

Створюю index= "cve", отримую повідомлення Success!

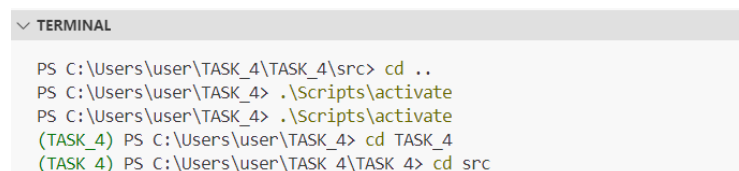


1 раз за допомогою /init-db ініціалізую базу даних даними з файлу json

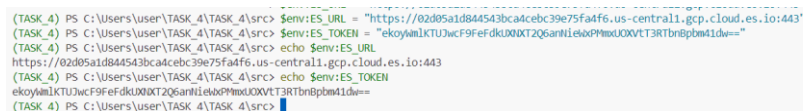
Отримую Success!!! Таким чином, маю 1223 документів



активація venv

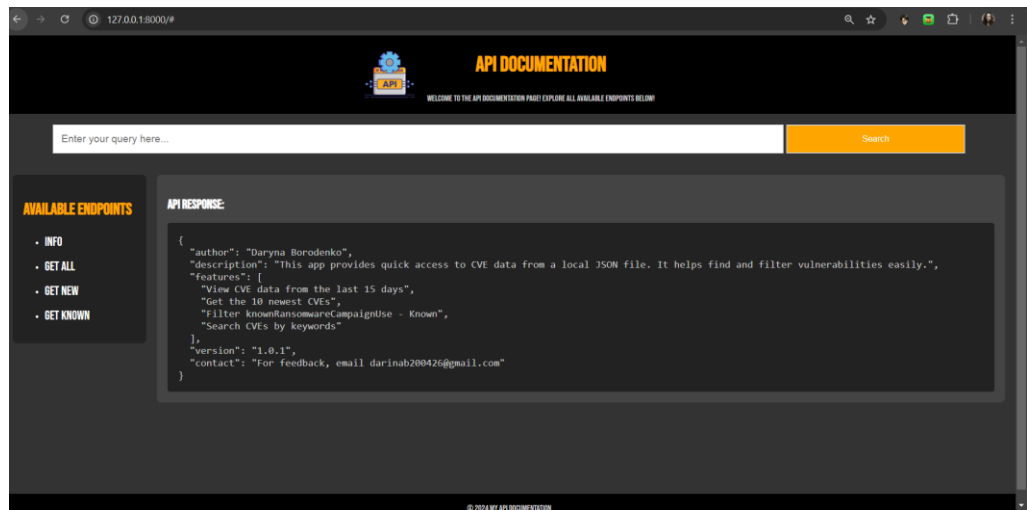


змінні середовища

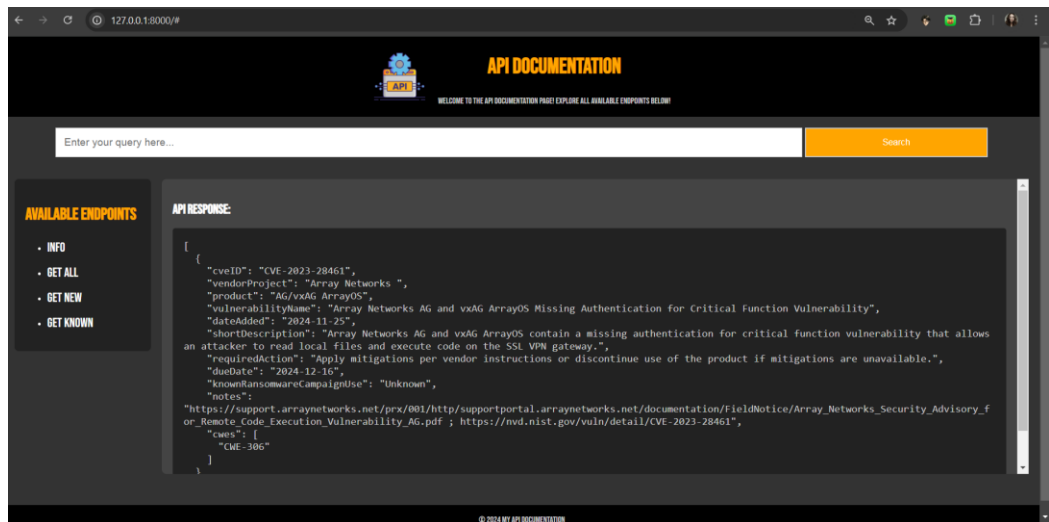


uvicorn main:app --reload

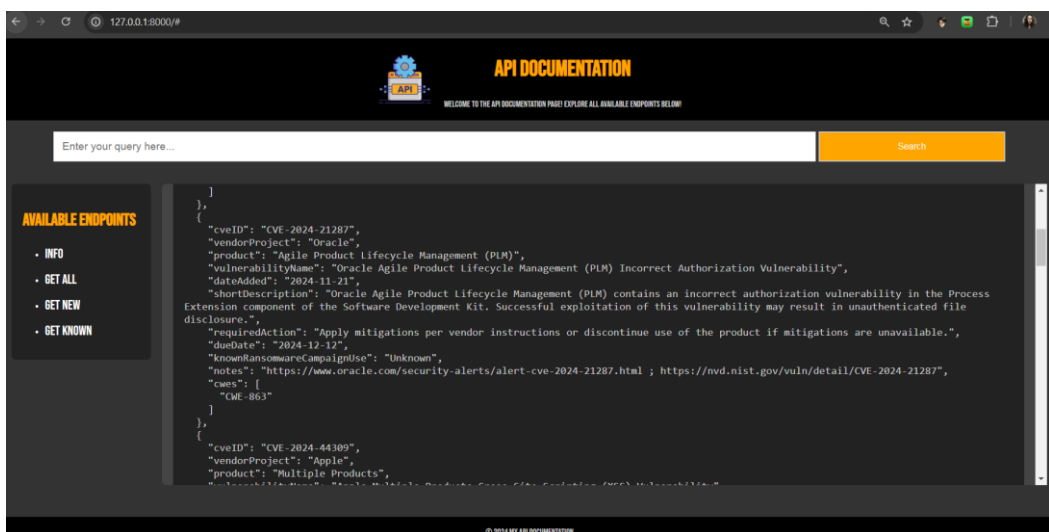
INFO



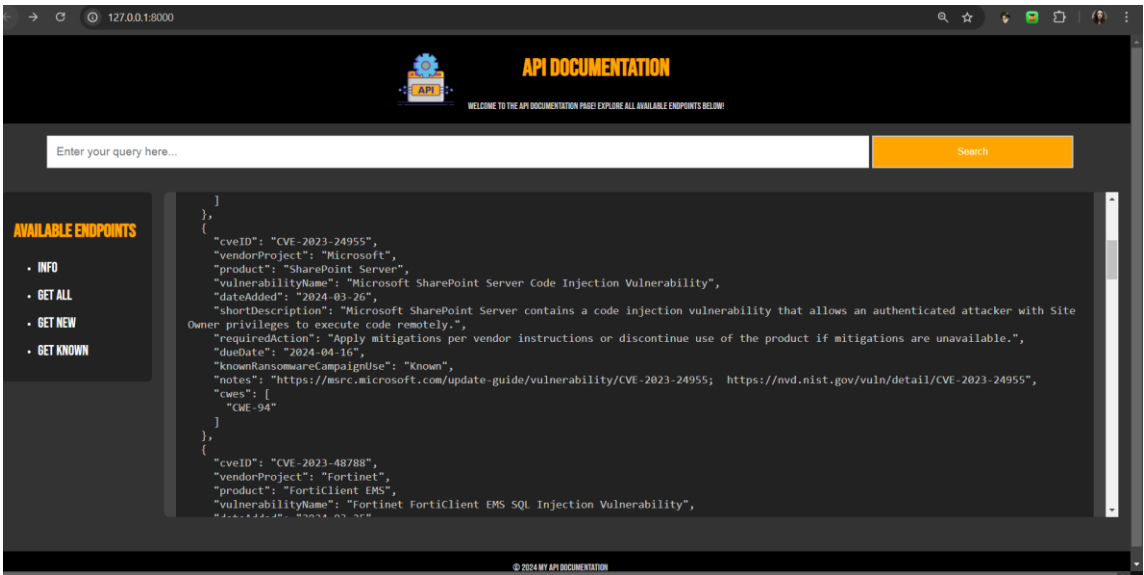
GET ALL (10 дефолтно)



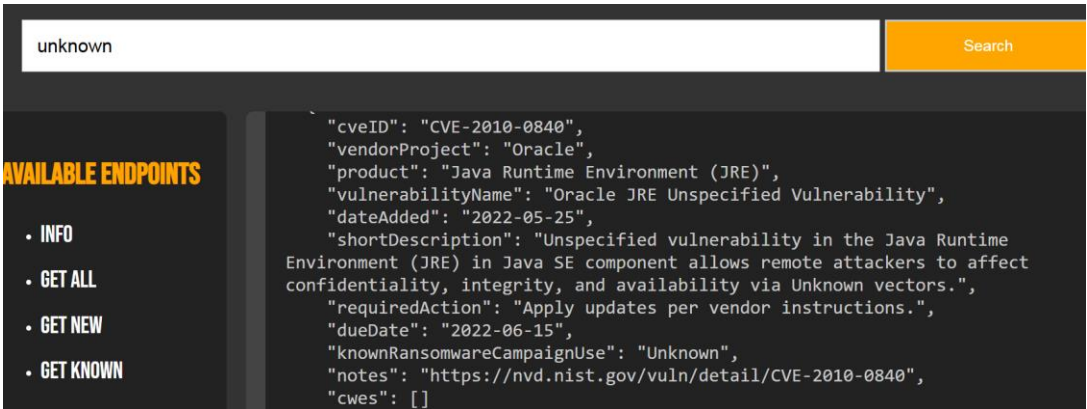
GET NEW



GET KNOWN

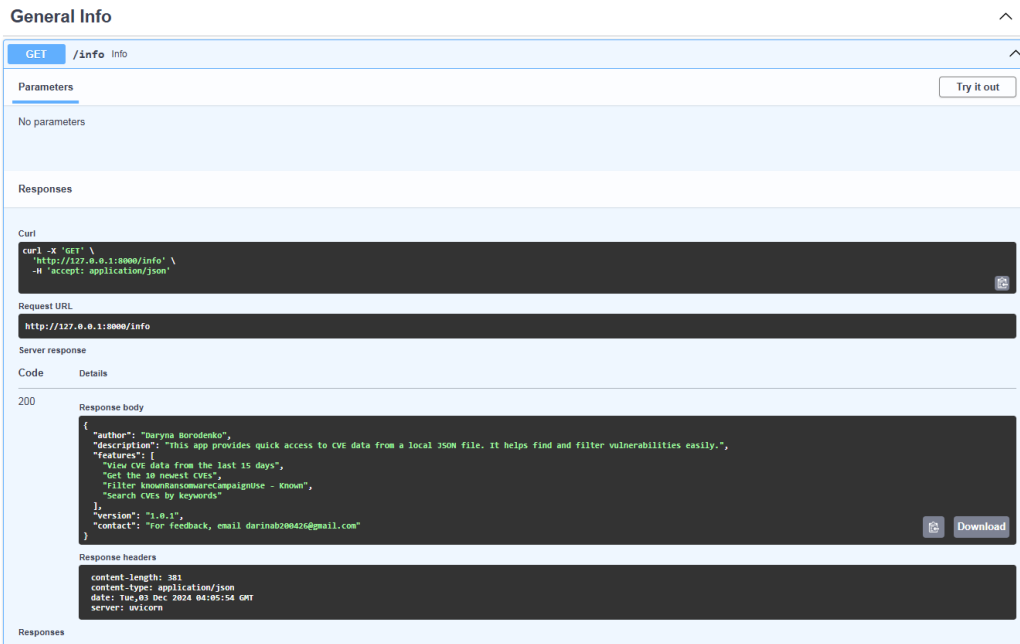


SEARCH



fastapi dev main.py

Загальна інф



Дефолтно 10, можна змінити. Так само ліміт записів

Last N Days CVEs

GET /get/all Get Vulnerabilities From Last Month

Parameters

Cancel

Name	Description
limit integer (query)	<input type="text" value="40"/>
days integer (query)	<input type="text" value="10"/>

Execute

Clear

Responses

Known до 10

Known Ransomware CVEs

GET /get/known Get Known

Parameters

Try it out

No parameters

Responses

Curl

```
curl -X 'GET' \
  'http://127.0.0.1:8000/get/known' \
  -H 'accept: application/json'
```

Request URL

```
http://127.0.0.1:8000/get/known
```

Server response

Code

Details

200

Response body

```
{
  "cveID": "CVE-2024-40711",
  "vendorProject": "Veeam",
  "product": "Backup & Replication",
  "vulnerabilityName": "Veeam Backup and Replication Deserialization Vulnerability",
  "dateAdded": "2024-10-17",
  "shortDescription": "Veeam Backup and Replication contains a deserialization vulnerability allowing an unauthenticated user to perform remote code execution.",
  "requiredAction": "Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.",
  "dateRet": "2024-10-09",
  "knownRansomwareCampaignUse": "Known",
  "notes": "https://www.veeam.com/xb4649 ; https://nvd.nist.gov/vuln/detail/CVE-2024-40711",
  "cwe": [
    "CWE-502"
  ]
},
{
  "cveID": "CVE-2024-6670",
  "vendorProject": "Progress",
  "product": "Whatsip Gold",
  "vulnerabilityName": "Progress Whatsip Gold SQL Injection Vulnerability",
  "dateAdded": "2024-09-16",
  "shortDescription": "Progress Whatsip Gold contains a SQL injection vulnerability that allows an unauthenticated attacker to retrieve the user's encrypted password if the application is configured with only a single user.",
  "requiredAction": "Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.",
  "dateRet": "2024-10-09",
  "knownRansomwareCampaignUse": "Known",
}
```

Download

Пошук по слову

GET

/search Search Vulnerabilities

Parameters

Cancel

Name	Description
query * required	Search keyword for CVE entries
string	
(query)	Unknown

ExecuteClear

Responses

Curl

curl -X 'GET' \n'http://127.0.0.1:8080/search?query=Unknown' \n-H 'accept: application/json'

Request URL

http://127.0.0.1:8080/search?query=Unknown

Server response

Code	Details
200	<div><div>Response body</div><div><pre>{ "cveID": "CVE-2015-4903", "vendorProject": "Oracle", "product": "Java SE", "vulnerabilityName": "Oracle Java SE Integrity Check Vulnerability", "dateAdded": "2021-03-03", "shortDescription": "Unspecified vulnerability in Oracle Java SE allows remote attackers to affect integrity via Unknown vectors related to deployment.", "requiredAction": "Apply updates per vendor instructions.", "dueDate": "2022-03-24", "knownRansomwareCampaigns": "Unknown", "notes": "https://nvd.nist.gov/vuln/detail/CVE-2015-4903", "cwe": [] }, { "cveID": "CVE-2019-0840", "vendorProject": "Oracle", "product": "Java Runtime Environment (JRE)", "vulnerabilityName": "Oracle JRE Unspecified Vulnerability", "dateAdded": "2022-05-25", "shortDescription": "Unspecified vulnerability in the Java Runtime Environment (JRE) in Java SE component allows remote attackers to affect confidentiality, integrity, and availability via Unknown vectors.", "requiredAction": "Apply updates per vendor instructions.", "dueDate": "2022-06-15", "knownRansomwareCampaigns": "Unknown", "notes": "https://nvd.nist.gov/vuln/detail/CVE-2019-0840", }</pre></div><div>Download</div></div>