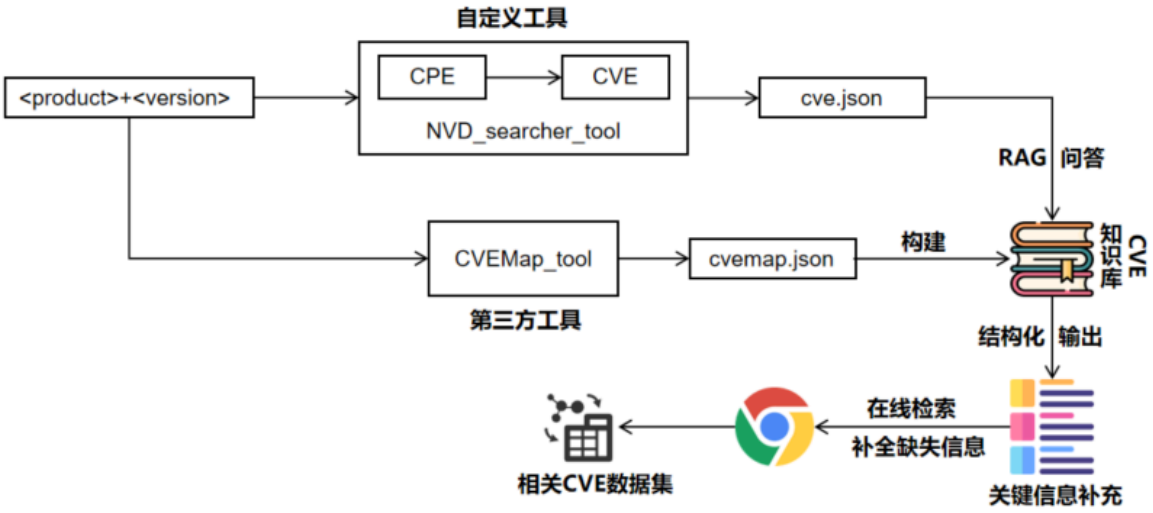
7.17汇报

CVE数据获取流程



cve.json如下图


```
{
  "metadata": {
    "vendor": "grafana",
    "product": "grafana",
    "version": "8.2.6",
    "cpe": "cpe:2.3:a:grafana:grafana:8.2.6:*:*:*:*:*:*:*",
    "cve_count": 23
  },
  "cve_ids": [
    "CVE-2021-43798",
    "CVE-2021-43813",
    "CVE-2021-43815",
    "CVE-2022-21673",
    "CVE-2022-21702",
    "CVE-2022-21703",
    "CVE-2022-21713",
    "CVE-2022-31097",
    "CVE-2022-31107",
    "CVE-2022-35957",
    "CVE-2022-36062",
    "CVE-2022-31123",
    "CVE-2022-31130",
    "CVE-2022-39201",
    "CVE-2022-39229",
    "CVE-2022-39306",
    "CVE-2022-39307",
    "CVE-2022-23552",
    "CVE-2022-39324",
    "CVE-2023-0507",
    "CVE-2023-0594",
    "CVE-2023-1410",
    "CVE-2023-2183"
  ]
}
```


cvemap.json数据样例如下图

```
{
  "cve_id": "CVE-2024-9264",
  "cve_description": "The SQL Expressions experimental feature of Grafana allows for the evaluation of `d
  "severity": "critical",
  "cvss_score": 9.9,
  "cvss_metrics": {
    "cvss31": {
      "score": 9.9,
      "vector": "CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H",
      "severity": "critical"
    }
  },
  "weaknesses": [
    {
      "cwe_id": "CWE-94",
      "cwe_name": "Improper Control of Generation of Code ('Code Injection')"
    },
    {
      "cwe_id": "CWE-77",
      "cwe_name": "Improper Neutralization of Special Elements used in a Command ('Command Injection')"
    }
  ],
  "epss": {
    "epss_score": 0.92337,
    "epss_percentile": 0.99709
  },
  "cpe": {
    "cpe": "cpe:2.3:a:grafana:grafana:11.0.0:*:*:*:*:*:*:*",
    "vendor": "grafana",
    "product": "grafana"
  },
  "reference": [
    "https://security.netapp.com/advisory/ntap-20250314-0007/",
    "https://github.com/Linxloop/fork_POC",
    "https://github.com/hsvhora/research_blogs",
    "https://github.com/nomi-sec/PoC-in-GitHub",
    "https://github.com/eeeeeeeeee-code/POC",
    "https://github.com/z3k0sec/File-Read-CVE-2024-9264",
    "https://github.com/PuddinCat/GithubRepoSpider",
```


通过RAG问答之后补充的结构化数据


```
{
  "cve_id": "CVE-2021-43798",
  "cve_description": "Grafana is an open-source platform for monitoring and observability. Grafana
  "cvss_score": 7.5,
  "epss_score": 0.94334,
  "cvss_vector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N",
  "cwe_id": "CWE-22",
  "cwe_name": "Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')",
  "is_poc": true,
  "is_exploited": false,
  "is_patch": true,
  "cpe": "cpe:2.3:a:grafana:grafana:*:*:*:*:*:*:*:*",
  "age_in_days": 1293,
  "env_match_score": ""
},
{
  "cve_id": "CVE-2017-12794",
  "error": "CVE ID not found in document metadata",
  "raw": ""
},
```


`cvss_score`：CVSS基础分数，直接反映漏洞严重性

`epss_score`：外部漏洞利用概率预测

`cvss_vector`：AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

`cwe_ids/cwe_name`:漏洞类型分类

`is_poc`：是否存在概念验证（PoC），提高可利用性

`is_exploited`：是否有已知漏洞利用（比PoC更严重）

`is_patch`：补丁可用性（逆向因子：无补丁优先）

`age_in_days`：漏洞自发布至今的时间

`env_match_score`：靶机环境适配分数

计算最终威胁分=（其他影响因素）×CVSS基础分^（1+验证系数×漏洞存在概率）

Score=环境适配×σ（α×CVSS+β×（A×B）+γ×e^(-λ·age))

σ（x）=1/（1+e^-x）

其中A×B为可利用性，A通过`is_poc`、`is_exploited`与`epss_score`得到，B通过解析`cvss_vector`中的`AC`与`PR`求得