官方数据集 CWE to CVE

1. C/Cpp

应用	待检测的CVE	该CVE所属的CWE
curl-curl-7_30_0	CVE-2000-0973	CWE-119 => CWE-126
openssl-1.0.1f	CVE-2014-0160	CWE-125 Out-of-bounds Read
libexif-libexif-0_6_21	CVE-2020-0093	CWE-125 Out-of-bounds Read

第三列说明，json文件有CWE信息就直接用；如果没有，则考虑：CWE也有包含关系，如果辨认例如`CWE-119 => CWE-126`，可以归为更细粒度的`CWE-126`

2. Java

应用	待检测的CVE	该CVE所属的CWE
vropsplugin-service	CVE-2021-21972	CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
h5-vsan-service	CVE-2021-21985	CWE-918 Server-Side Request Forgery (SSRF)
apache/logging-log4j2	CVE-2021-44228	CWE-502 Deserialization of Untrusted Data CWE-400 Uncontrolled Resource Consumption CWE-20 Improper Input Validation
commons-text-commons-text-1.7	CVE-2022-42889	CWE-94: Improper Control of Generation of Code

3. Python

应用	待检测的CVE	该CVE所属的CWE
Pillow-8.4.0	CVE-2022-22817	CWE-190: Integer Overflow or Wraparound(CWE-682/131/20)
QAnything-1.4.1	CVE-2024-7099	CWE-89 Improper Neutralization of Special Elements used in an SQL Command
Shakal-NG-1.3.2	CVE-2024-8412	CWE-601 Open Redirect
langchain-langchain-openai-0.1.17	CVE-2024-10940	CWE-497 Exposure of Sensitive System Information to an Unauthorized Control Sphere
langroid-0.53.14	CVE-2025-46725	CWE-94: Improper Control of Generation of Code ('Code Injection')
horilla-1.3	CVE-2025-47789	CWE-601: URL Redirection to Untrusted Site ('Open Redirect
BentoML-1.4.10	CVE-2025-54381	CWE-918: Server-Side Request Forgery (SSRF)
pyload-develop	CVE-2025-54802	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

4. 判定依据

- 对应文件夹里面的json文件是否有关CWE的描述
- 官网链接：https://www.cve.org/CVERecord?id=CVE-2025-46725，修改CVE-2025-46725对应的CVE编号，查询是否有CWE的描述
- 官网链接：https://www.cvedetails.com/cve/CVE-2022-42889/，修改CVE-2022-42889对应的CVE编号，查询是否有CWE的描述

5. 补充资料

- 各类CWE具体信息：https://www.cvedetails.com/cwe-definitions/1/cwelist.html