OpenSCA: Manage Open Source Risks by an Open Source Solution

Qiuyue QI
Open Source Community Operation
Xmirror Security

CONTENTS

01 Our Motivation

02 OpenSCA

03 Our community & cases

04 Build together

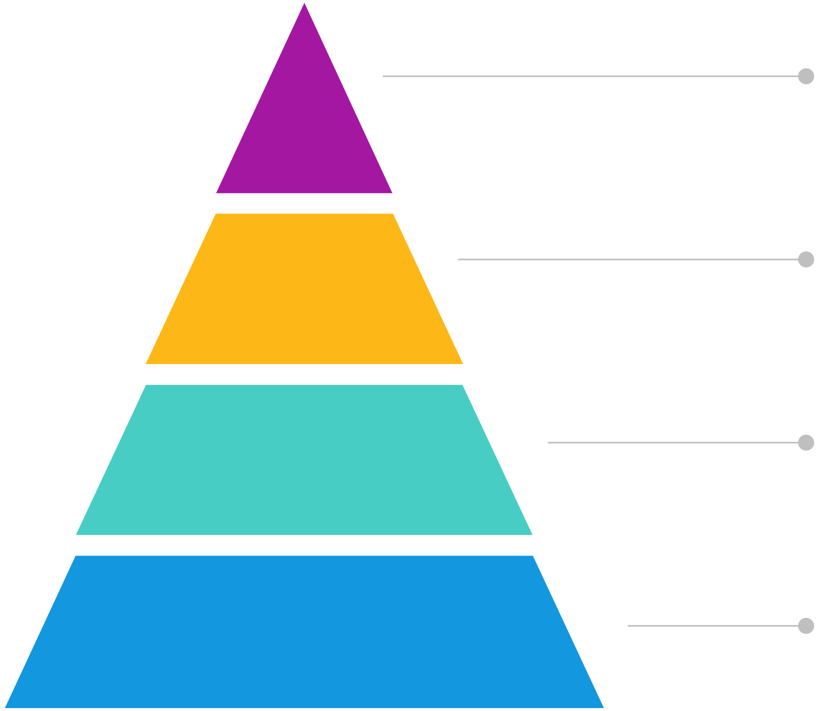
Part

01

Motivation

The purpose and potential of an Open Source solution

The Purpose of Using SCA (Software Composition Analysis)



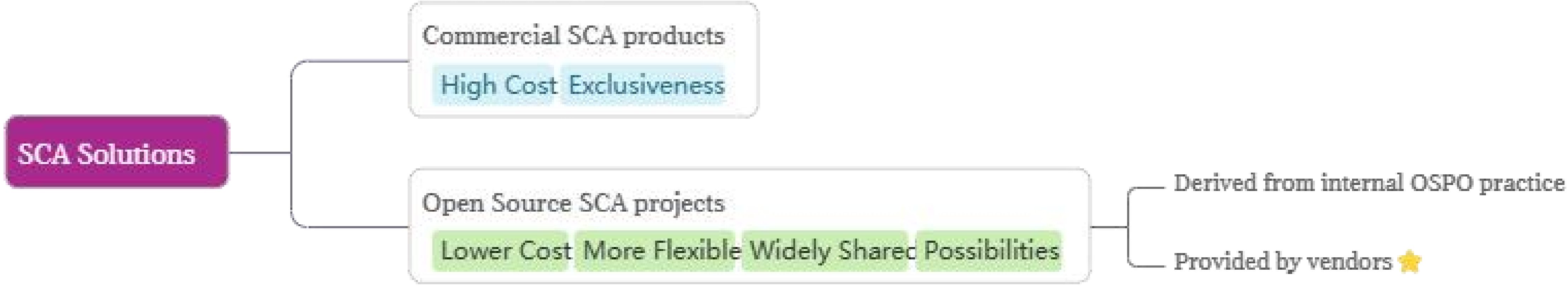
Manage the Security of the Whole Software Supply Chain

Respond ASAP when New Open Source Vulnerabilities Break out

Manage and Mitigate Known Risks According to the List

Get the list of Open Source Components and Vulnerabilities Introduced

Solutions



SCA Solutions

Commercial SCA products

High Cost Exclusiveness

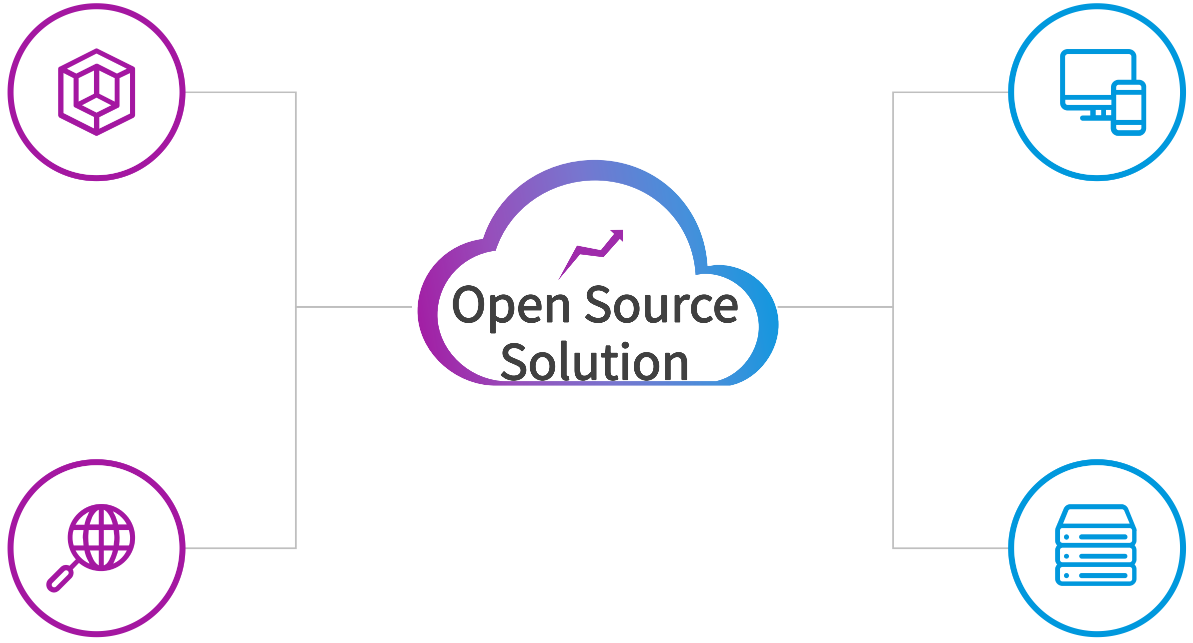
Open Source SCA projects

Lower Cost More Flexible Widely Sharec Possibilities

Derived from internal OSPO practice

Provided by vendors ⭐

Advantages of the Open Source Solution



Open Source Solution

Lower Cost

Visible & transparent source code

More Flexible

Access to redevelopment in terms of diverse scenarios

Widely Shared

Open & available for each part of the chain to use freely

More Possibilities

Not limited in vendors’ perspective

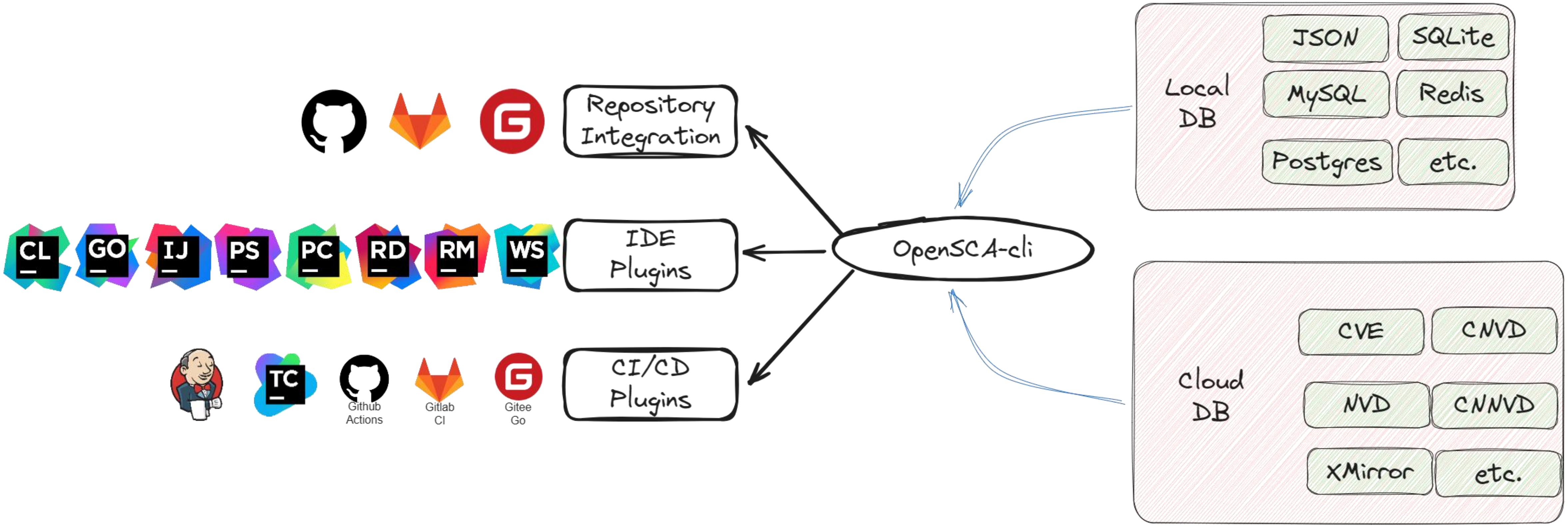
Part

02

OpenSCA

What is it? How can it help?

About us



Repository Integration

IDE Plugins

CI/CD Plugins

OpenSCA-cli

Local DB

JSON

SQLite

MySQL

Redis

Postgres

etc.

Cloud DB

CVE

CNVD

NVD

CNNVD

XMirror

etc.

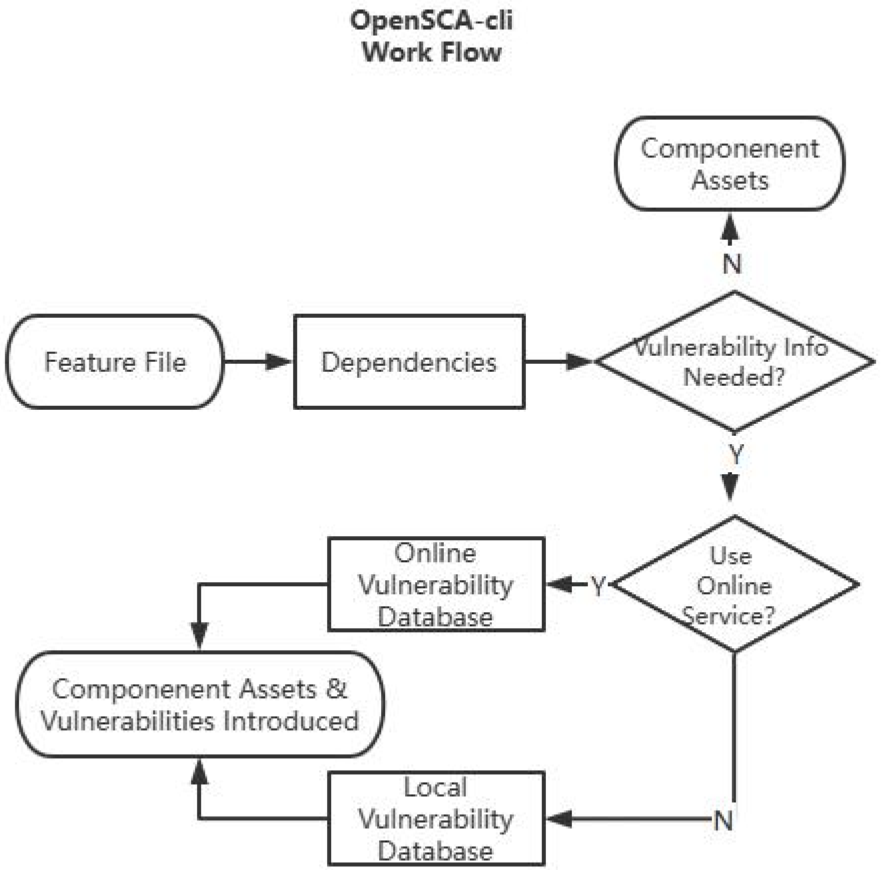
Open Source

Unlimited access

User-friendly

Multiple capabilities

Open Engine


OpenSCA-cli
Work Flow
Componenent Assets
N
Feature File
Dependencies
Vulnerability Info Needed?
Y
Use Online Service?
Y
Online Vulnerability Database
Componenent Assets & Vulnerabilities Introduced
Local Vulnerability Database
N

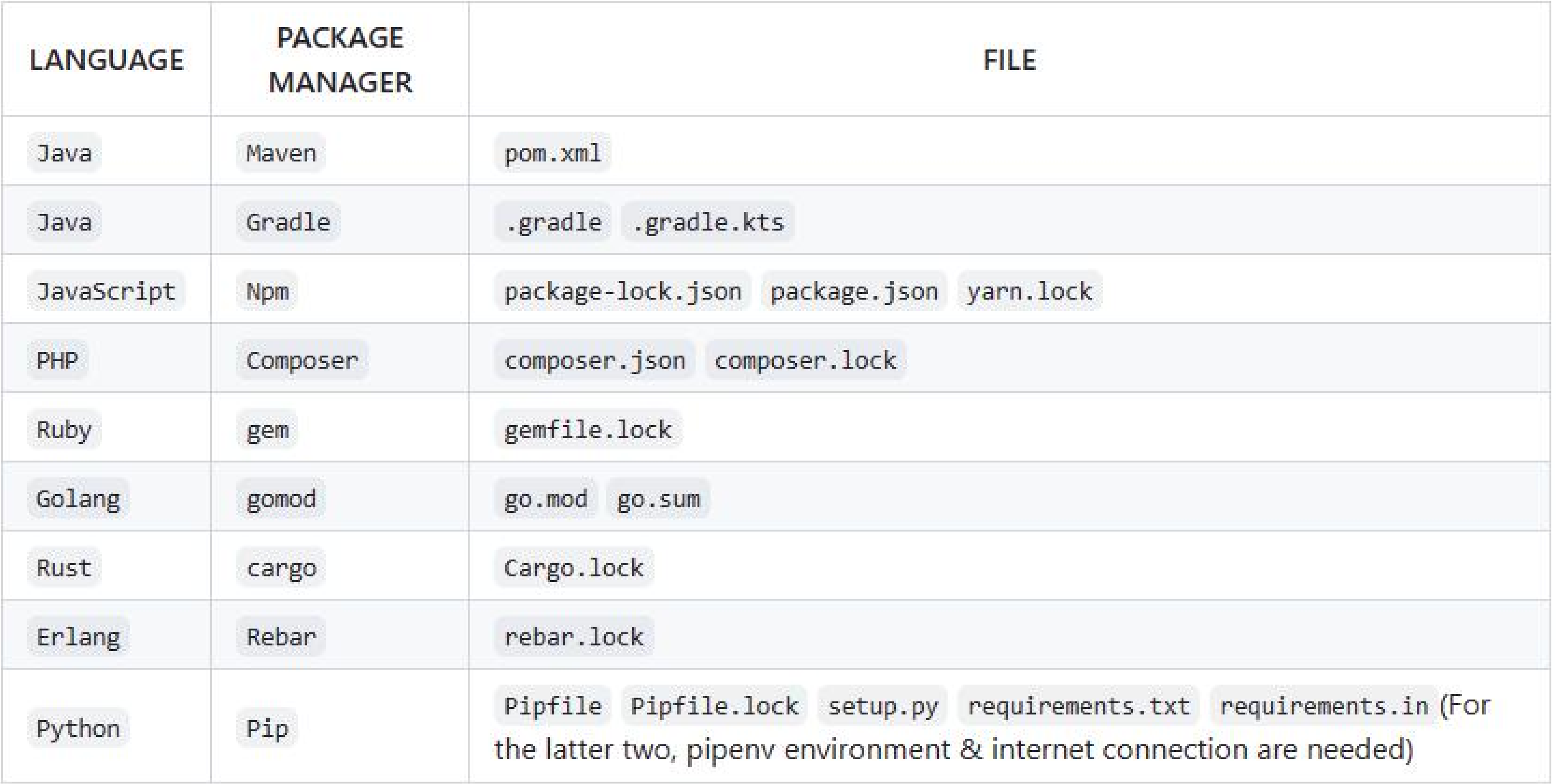
Localhost: open source engine

- Analyze dependencies
- Get info from online or local knowledge base
- Generate reports

Online knowledge base

- Return vulnerability & license info to the engine

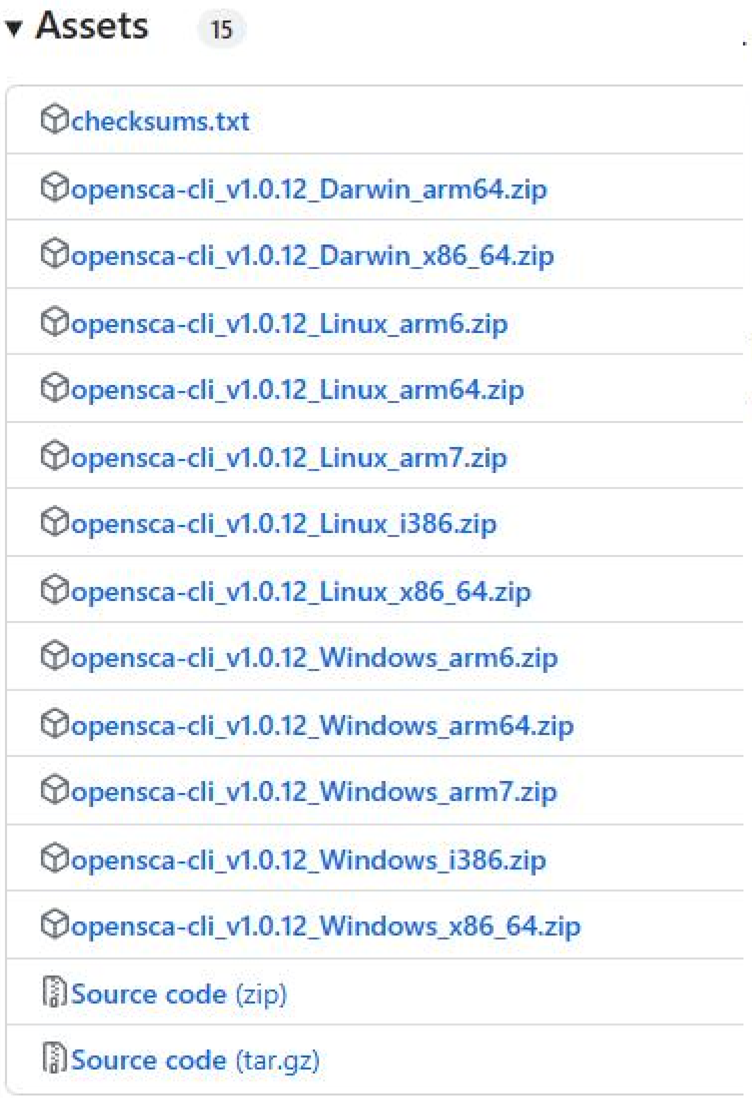
Applicability



LANGUAGE	PACKAGE MANAGER	FILE
Java	Maven	pom.xml
Java	Gradle	.gradle .gradle.kts
JavaScript	Npm	package-lock.json package.json yarn.lock
PHP	Composer	composer.json composer.lock
Ruby	gem	gemfile.lock
Golang	gomod	go.mod go.sum
Rust	cargo	Cargo.lock
Erlang	Rebar	rebar.lock
Python	Pip	Pipfile Pipfile.lock setup.py requirements.txt requirements.in (For the latter two, pipenv environment & internet connection are needed)

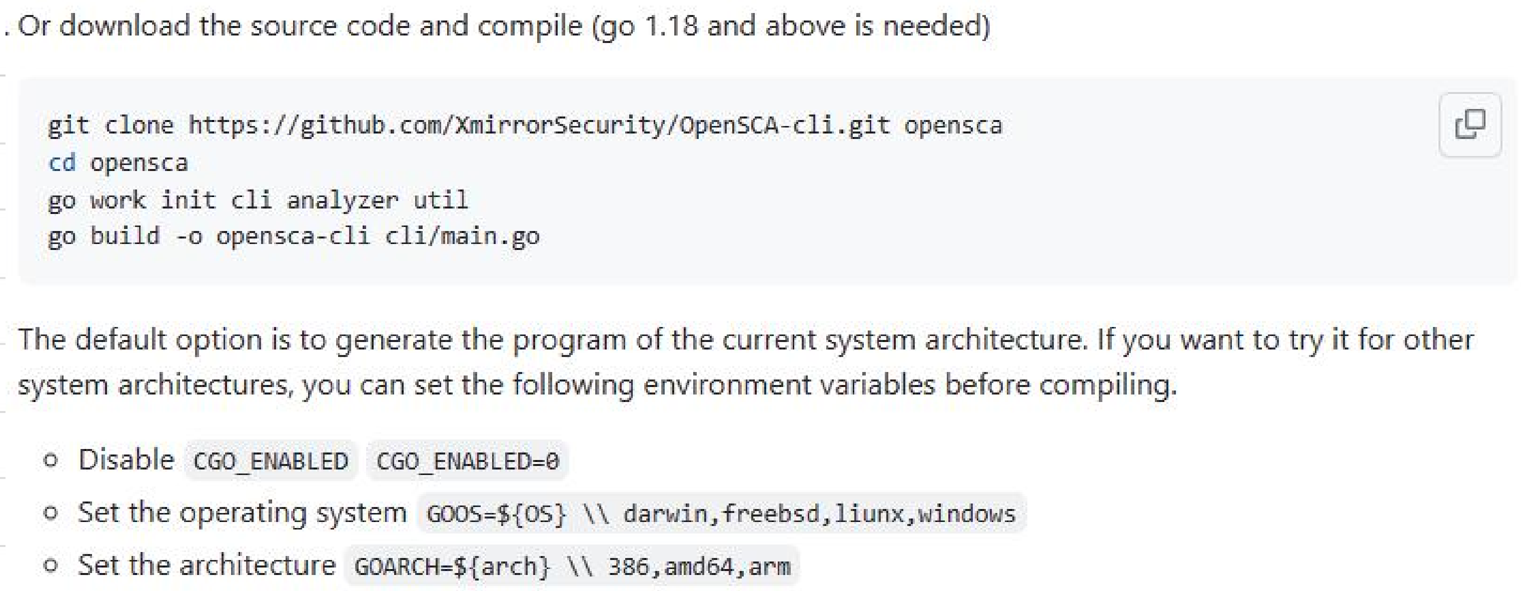
No environment is needed (except the analysis of 2 Python feature files)

Applicability



▾ Assets 15

- checksums.txt
- opensca-cli_v1.0.12_Darwin_arm64.zip
- opensca-cli_v1.0.12_Darwin_x86_64.zip
- opensca-cli_v1.0.12_Linux_arm6.zip
- opensca-cli_v1.0.12_Linux_arm64.zip
- opensca-cli_v1.0.12_Linux_arm7.zip
- opensca-cli_v1.0.12_Linux_i386.zip
- opensca-cli_v1.0.12_Linux_x86_64.zip
- opensca-cli_v1.0.12_Windows_arm6.zip
- opensca-cli_v1.0.12_Windows_arm64.zip
- opensca-cli_v1.0.12_Windows_arm7.zip
- opensca-cli_v1.0.12_Windows_i386.zip
- opensca-cli_v1.0.12_Windows_x86_64.zip
- Source code (zip)
- Source code (tar.gz)



. Or download the source code and compile (go 1.18 and above is needed)

```
git clone https://github.com/XmirrorSecurity/OpenSCA-cli.git opensca
cd opensca
go work init cli analyzer util
go build -o opensca-cli cli/main.go
```

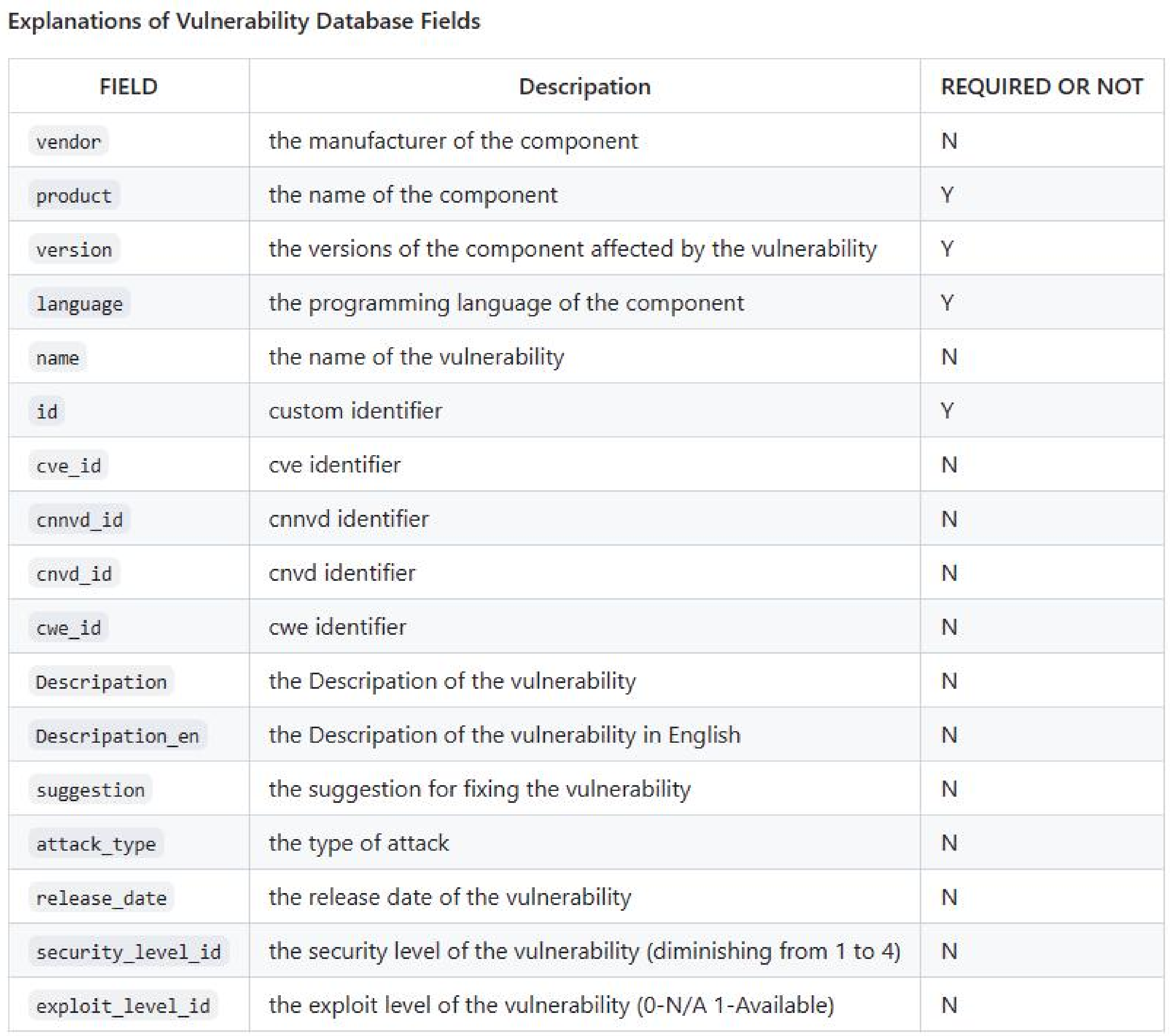
The default option is to generate the program of the current system architecture. If you want to try it for other system architectures, you can set the following environment variables before compiling.

- Disable `CGO_ENABLED` `CGO_ENABLED=0`
- Set the operating system `GOOS=${OS} \\ darwin,freebsd,liunx,windows`
- Set the architecture `GOARCH=${arch} \\ 386,amd64,arm`

- Windows
- Linux
- Freebsd
- MacOS

Compatibility

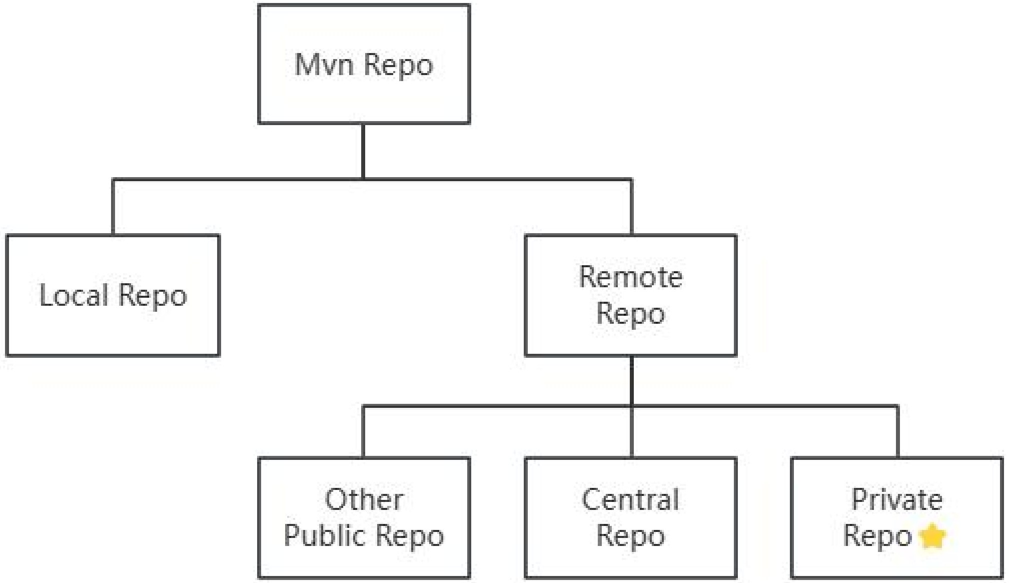
- Support both online and local knowledge bases
- Allow diverse formats of local knowledge base, including JSON, SQLite, MySQL, Redis and Postgres

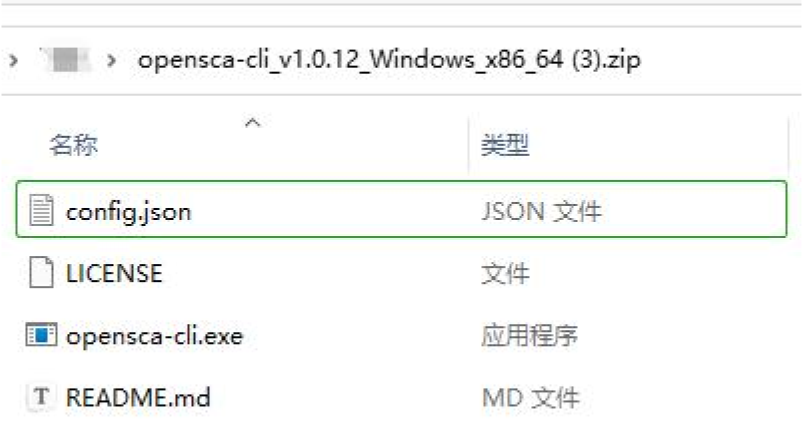


Explanations of Vulnerability Database Fields

FIELD	Description	REQUIRED OR NOT
`vendor`	the manufacturer of the component	N
`product`	the name of the component	Y
`version`	the versions of the component affected by the vulnerability	Y
`language`	the programming language of the component	Y
`name`	the name of the vulnerability	N
`id`	custom identifier	Y
`cve_id`	cve identifier	N
`cnnvd_id`	cnnvd identifier	N
`cnvd_id`	cnvd identifier	N
`cwe_id`	cwe identifier	N
`Descripation`	the Descripation of the vulnerability	N
`Descripation_en`	the Descripation of the vulnerability in English	N
`suggestion`	the suggestion for fixing the vulnerability	N
`attack_type`	the type of attack	N
`release_date`	the release date of the vulnerability	N
`security_level_id`	the security level of the vulnerability (diminishing from 1 to 4)	N
`exploit_level_id`	the exploit level of the vulnerability (0-N/A 1-Available)	N

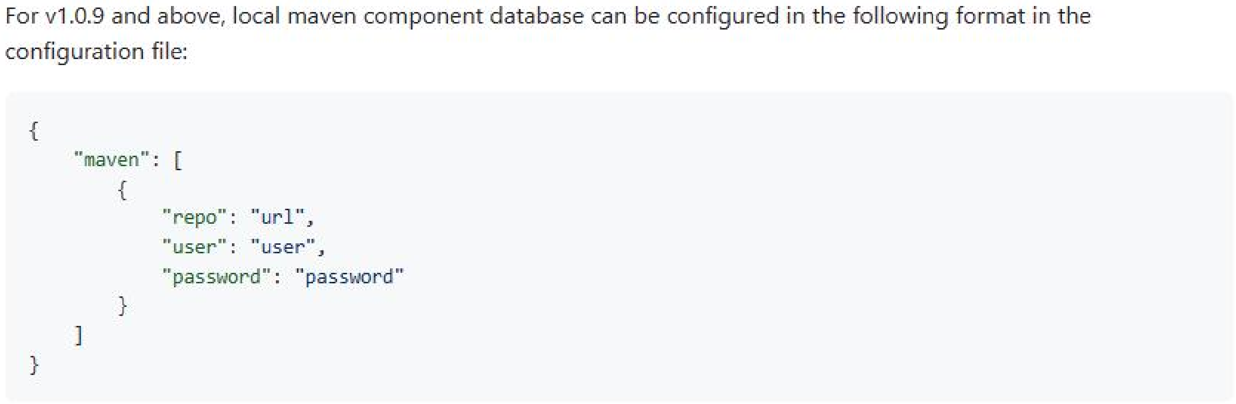
Compatibility





opensca-cli_v1.0.12_Windows_x86_64 (3).zip

名称	类型
config.json	JSON 文件
LICENSE	文件
opensca-cli.exe	应用程序
README.md	MD 文件



For v1.0.9 and above, local maven component database can be configured in the following format in the configuration file:

```
{
    "maven": [
        {
            "repo": "url",
            "user": "user",
            "password": "password"
        }
    ]
}
```

- Allow using private Maven Repo through configuration

Features

Easy to start

One command in CMD/CRT to scan and get the result

Complete ability

Independent logic executed in localhost

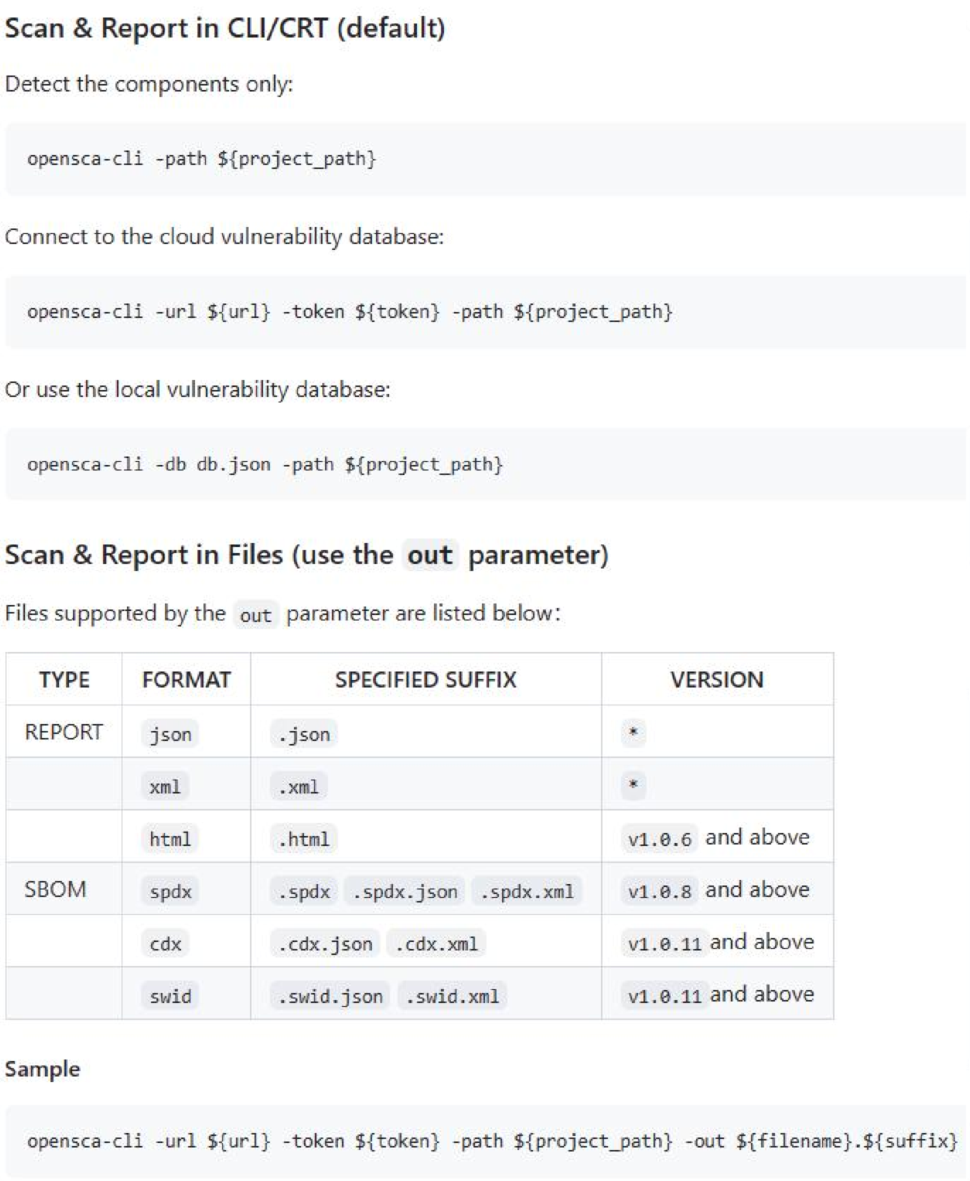
Online/offline applicable

Choose freely according to the specific scenario

Flexible

Freely integrated into the process of R&D

How to Use



Scan & Report in CLI/CRT (default)

Detect the components only:

```
opensca-cli -path ${project_path}
```

Connect to the cloud vulnerability database:

```
opensca-cli -url ${url} -token ${token} -path ${project_path}
```

Or use the local vulnerability database:

```
opensca-cli -db db.json -path ${project_path}
```

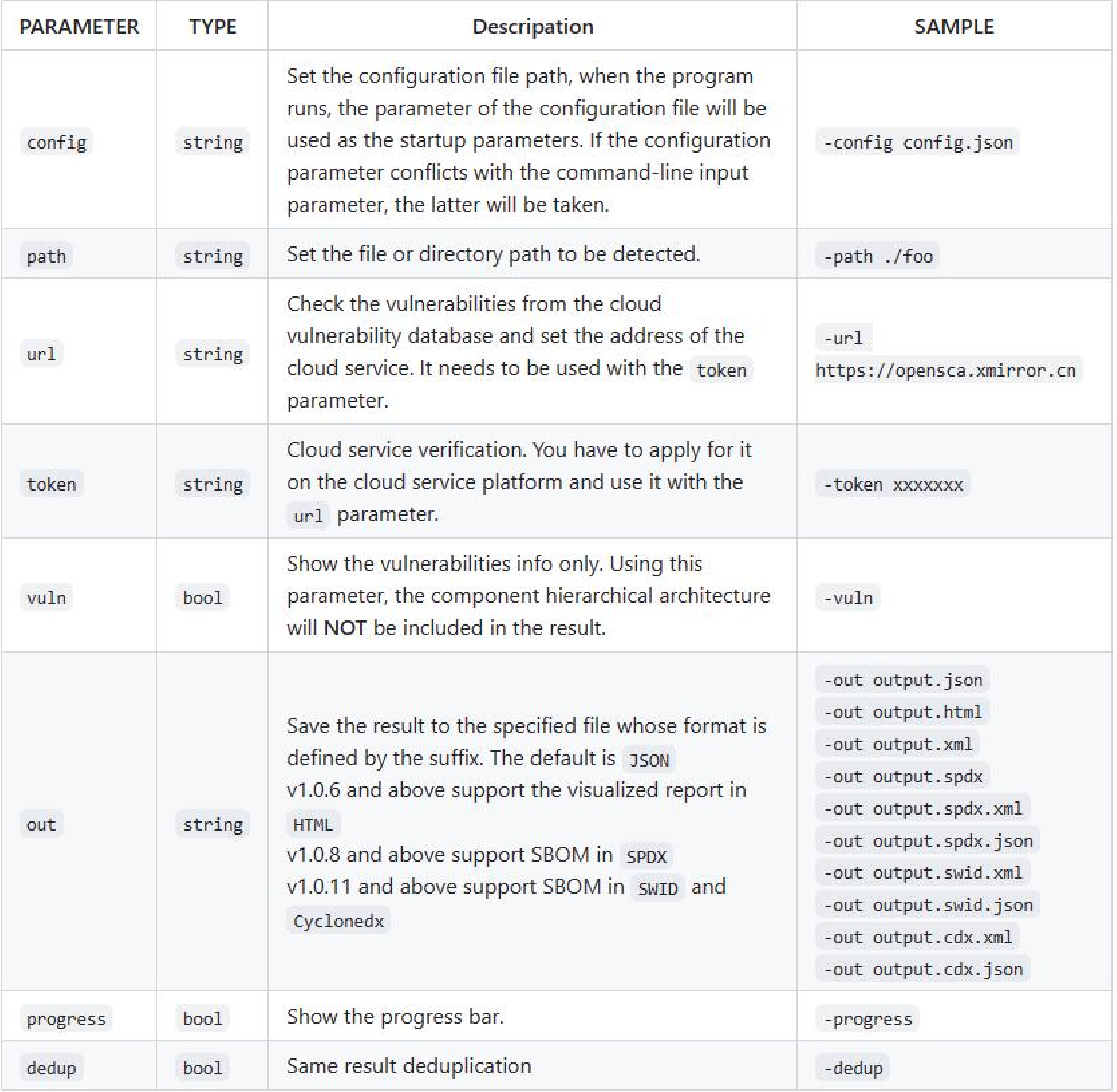
Scan & Report in Files (use the `out` parameter)

Files supported by the `out` parameter are listed below:

TYPE	FORMAT	SPECIFIED SUFFIX	VERSION
REPORT	`json`	`.json`	`*`
	`xml`	`.xml`	`*`
	`html`	`.html`	`v1.0.6` and above
SBOM	`spdx`	`.spdx` `.spdx.json` `.spdx.xml`	`v1.0.8` and above
	`cdx`	`.cdx.json` `.cdx.xml`	`v1.0.11` and above
	`swid`	`.swid.json` `.swid.xml`	`v1.0.11` and above

Sample

```
opensca-cli -url ${url} -token ${token} -path ${project_path} -out ${filename}.${suffix}
```

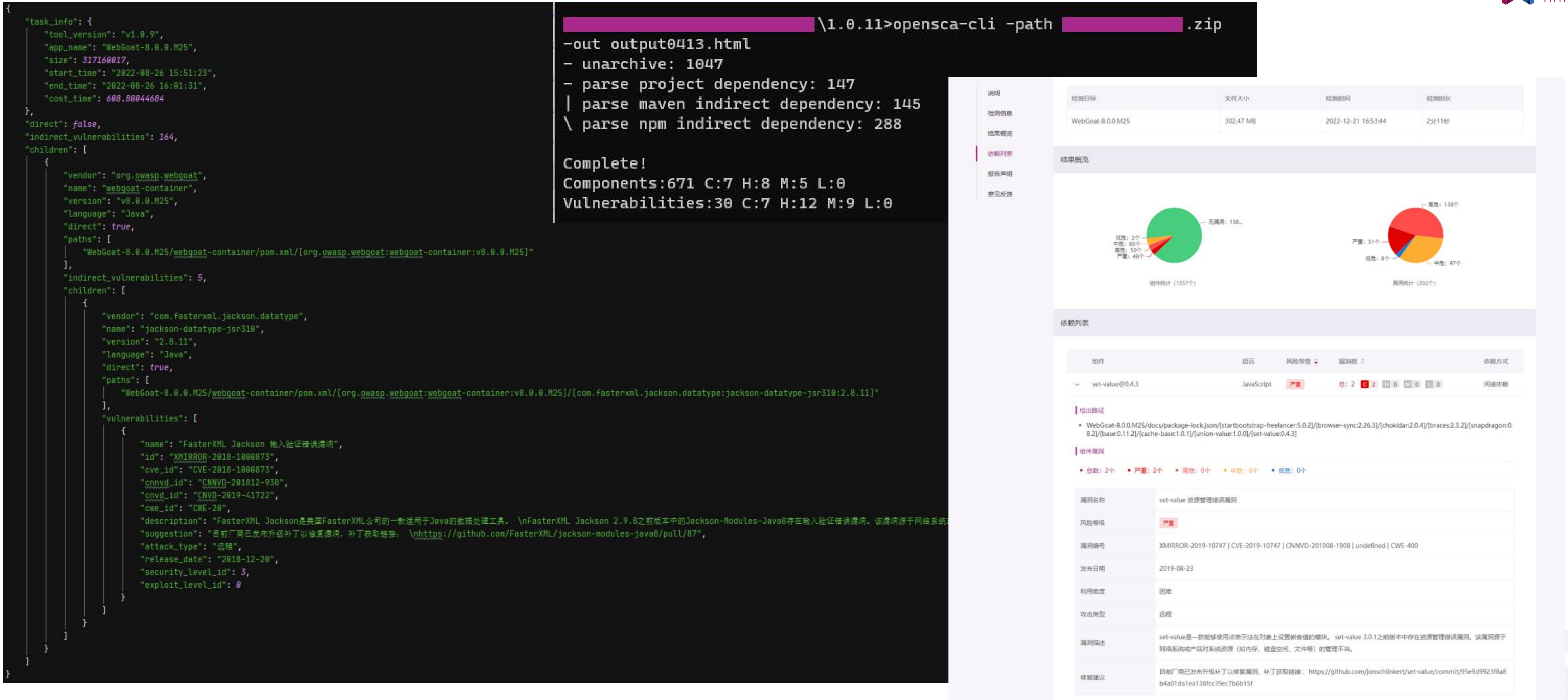


PARAMETER	TYPE	Description	SAMPLE
`config`	`string`	Set the configuration file path, when the program runs, the parameter of the configuration file will be used as the startup parameters. If the configuration parameter conflicts with the command-line input parameter, the latter will be taken.	`-config config.json`
`path`	`string`	Set the file or directory path to be detected.	`-path ./foo`
`url`	`string`	Check the vulnerabilities from the cloud vulnerability database and set the address of the cloud service. It needs to be used with the `token` parameter.	`-url https://opensca.xmirror.cn`
`token`	`string`	Cloud service verification. You have to apply for it on the cloud service platform and use it with the `url` parameter.	`-token xxxxxxx`
`vuln`	`bool`	Show the vulnerabilities info only. Using this parameter, the component hierarchical architecture will **NOT** be included in the result.	`-vuln`

`out`	`string`	Save the result to the specified file whose format is defined by the suffix. The default is `JSON`
		v1.0.6 and above support the visualized report in `HTML`
		v1.0.8 and above support SBOM in `SPDX`
		v1.0.11 and above support SBOM in `SWID` and `Cyclonedx`
			`-out output.json`
			`-out output.html`
			`-out output.xml`
			`-out output.spdx`
			`-out output.spdx.xml`
			`-out output.spdx.json`
			`-out output.swid.xml`
			`-out output.swid.json`
			`-out output.cdx.xml`
			`-out output.cdx.json`

`progress`	`bool`	Show the progress bar.	`-progress`
`dedup`	`bool`	Same result deduplication	`-dedup`

Results



```
{
    "task_info": {
        "tool_version": "v1.0.9",
        "app_name": "WebGoat-8.0.0.M25",
        "size": 317160017,
        "start_time": "2022-08-26 15:51:23",
        "end_time": "2022-08-26 16:01:31",
        "cost_time": 608.80044684
    },
    "direct": false,
    "indirect_vulnerabilities": 164,
    "children": [
        {
            "vendor": "org.owasp.webgoat",
            "name": "webgoat-container",
            "version": "v8.0.0.M25",
            "language": "Java",
            "direct": true,
            "paths": [
                "WebGoat-8.0.0.M25/webgoat-container/pom.xml/[org.owasp.webgoat:webgoat-container:v8.0.0.M25]"
            ],
            "indirect_vulnerabilities": 5,
            "children": [
                {
                    "vendor": "com.fasterxml.jackson.datatype",
                    "name": "jackson-datatype-jsr310",
                    "version": "2.8.11",
                    "language": "Java",
                    "direct": true,
                    "paths": [
                        "WebGoat-8.0.0.M25/webgoat-container/pom.xml/[org.owasp.webgoat:webgoat-container:v8.0.0.M25]/[com.fasterxml.jackson.datatype:jackson-datatype-jsr310:2.8.11]"
                    ],
                    "vulnerabilities": [
                        {
                            "name": "FasterXML Jackson 输入验证错误漏洞",
                            "id": "XMIRROR-2018-1000873",
                            "cve_id": "CVE-2018-1000873",
                            "cnnvd_id": "CNNVD-201812-938",
                            "cnvd_id": "CNVD-2019-41722",
                            "cwe_id": "CWE-20",
                            "description": "FasterXML Jackson是美国FasterXML公司的一款适用于Java的数据处理工具. \nFasterXML Jackson 2.9.8之前版本中的Jackson-Modules-Java8存在输入验证错误漏洞. 该漏洞源于网络系统
                            "suggestion": "目前厂商已发布升级补丁以修复漏洞, 补丁获取链接: \nhttps://github.com/FasterXML/jackson-modules-java8/pull/87",
                            "attack_type": "远程",
                            "release_date": "2018-12-20",
                            "security_level_id": 3,
                            "exploit_level_id": 0
                        }
                    ]
                }
            ]
        }
    ]
}
```

```
[redacted]\1.0.11>opensca-cli -path [redacted].zip
-out output0413.html
- unarchive: 1047
- parse project dependency: 147
| parse maven indirect dependency: 145
\ parse npm indirect dependency: 288

Complete!
Components:671 C:7 H:8 M:5 L:0
Vulnerabilities:30 C:7 H:12 M:9 L:0
```

检测目标	文件大小	检测时间	检测时长
WebGoat-8.0.0.M25	302.47 MB	2022-12-21 16:53:44	2分11秒

结果概览

依赖列表

组件	语言	风险等级	漏洞数	依赖方式
set-value@0.4.3	JavaScript	严重	总：2 C 2 H 0 M 0 L 0	间接依赖

检出路径

- WebGoat-8.0.0.M25/docs/package-lock.json/[startbootstrap-freelancer:5.0.2]/[browser-sync:2.26.3]/[chokidar:2.0.4]/[braces:2.3.2]/[snapdragon:0.8.2]/[base:0.11.2]/[cache-base:1.0.1]/[union-value:1.0.0]/[set-value:0.4.3]

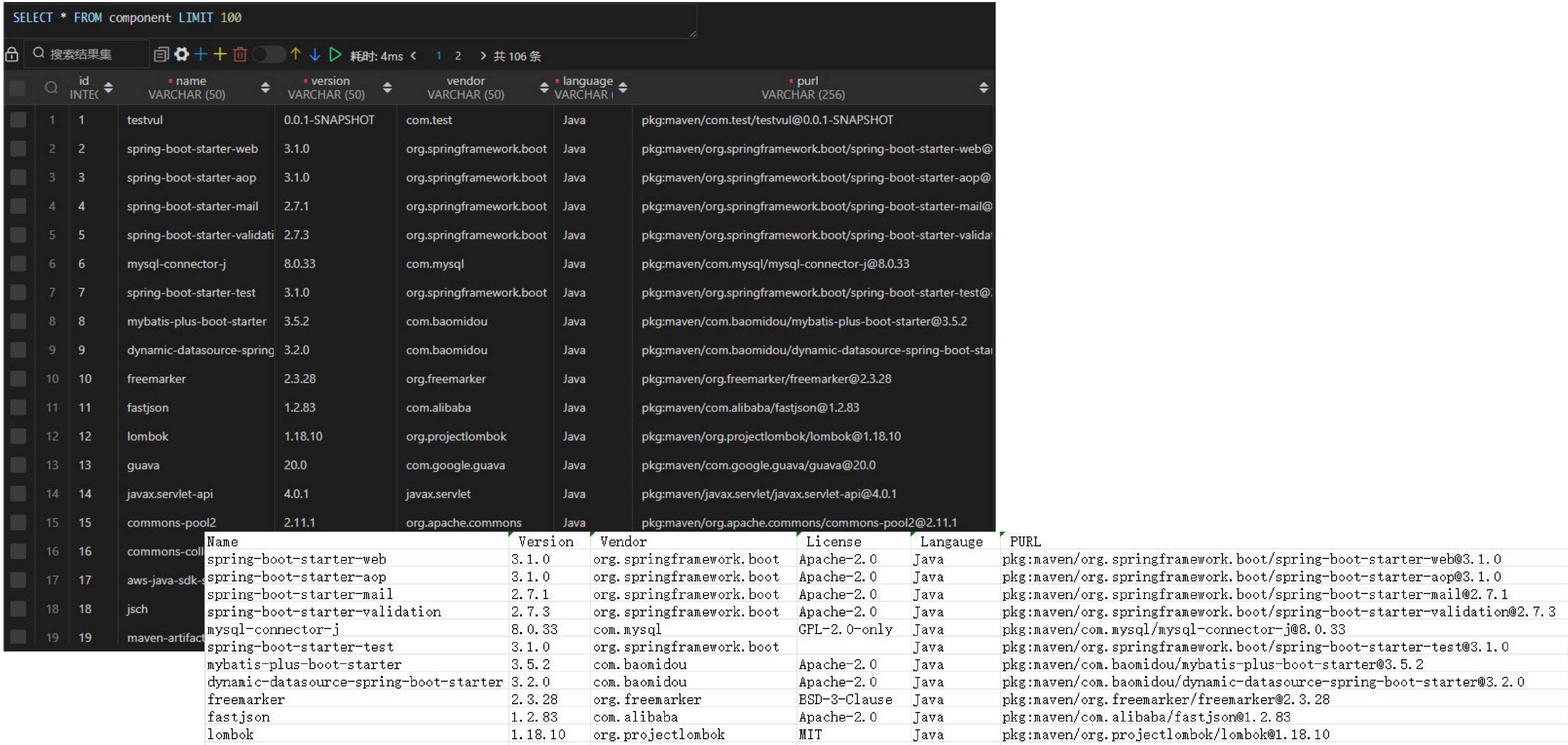
组件漏洞

• 总数：2个 • 严重：2个 • 高危：0个 • 中危：0个 • 低危：0个

漏洞名称	set-value 资源管理错误漏洞
风险等级	严重
漏洞编号	XMIRROR-2019-10747 | CVE-2019-10747 | CNNVD-201908-1908 | undefined | CWE-400
发布日期	2019-08-23
利用难度	困难
攻击类型	远程
漏洞描述	set-value是一款能够使用点表示法在对象上设置嵌套值的模块。 set-value 3.0.1之前版本中存在资源管理错误漏洞。该漏洞源于网络系统或产品对系统资源（如内存、磁盘空间、文件等）的管理不当。
修复建议	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://github.com/jonschlinkert/set-value/commit/95e9d9923f8a8b4a01da1ea138fcc39ec7b6b15f

- Overview of the result is printed in CMD
- Results in detail including dependency structure and vulnerability introduced can be shown in JSON/HTML/csv/SQLite

Results

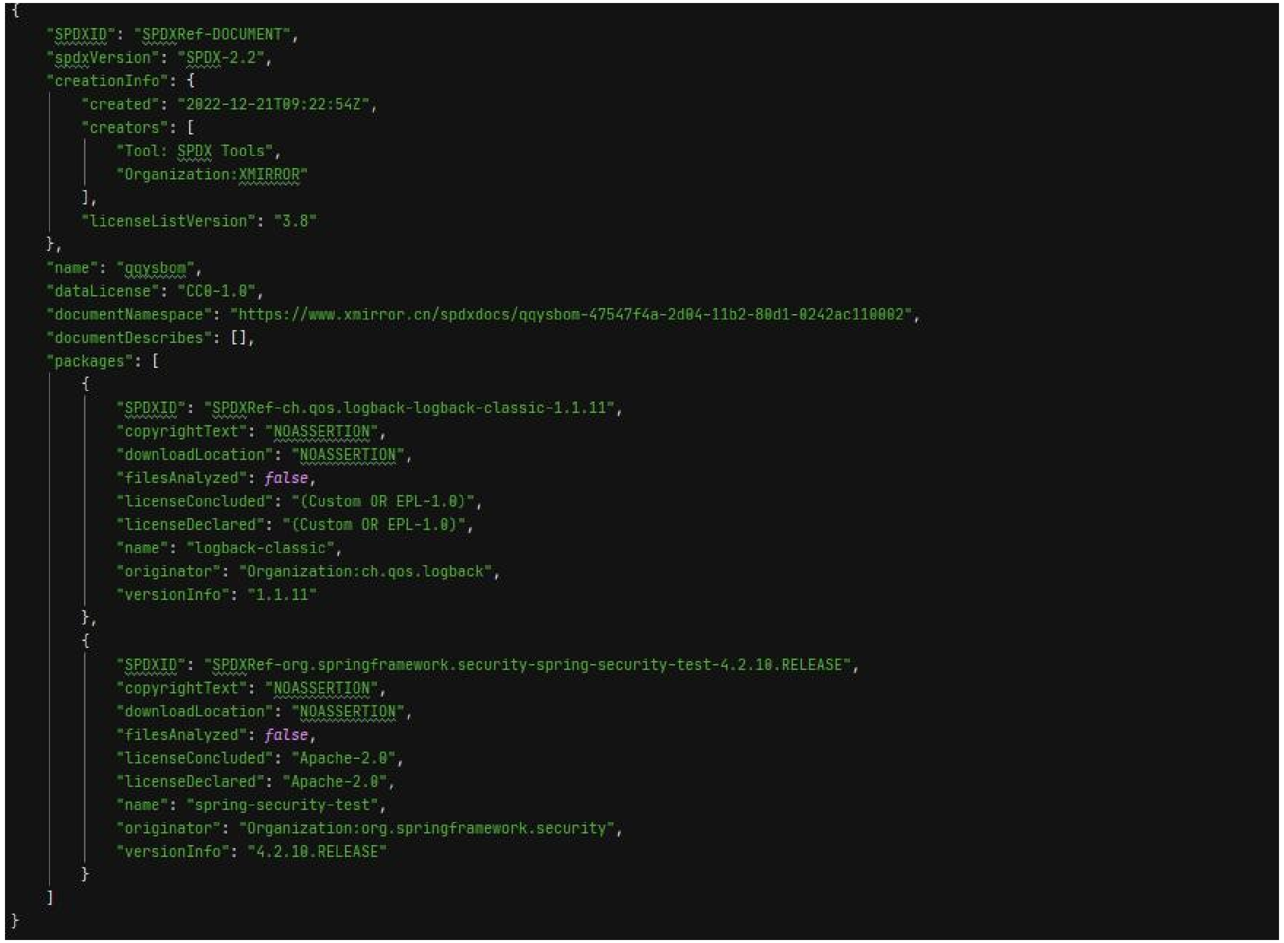


```
SELECT * FROM component LIMIT 100
```

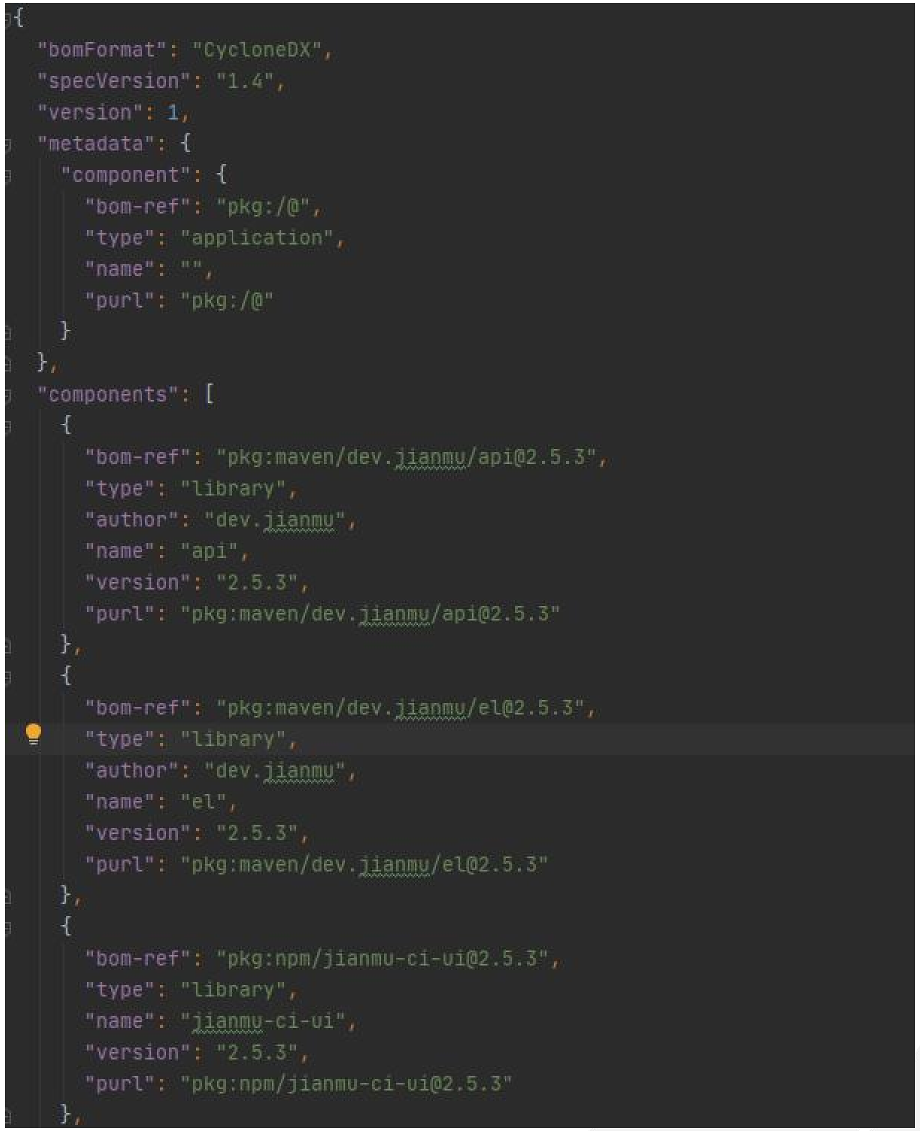
	id INTE	name VARCHAR (50)	version VARCHAR (50)	vendor VARCHAR (50)	language VARCHAR	purl VARCHAR (256)
1	1	testvul	0.0.1-SNAPSHOT	com.test	Java	pkg:maven/com.test/testvul@0.0.1-SNAPSHOT
2	2	spring-boot-starter-web	3.1.0	org.springframework.boot	Java	pkg:maven/org.springframework.boot/spring-boot-starter-web@
3	3	spring-boot-starter-aop	3.1.0	org.springframework.boot	Java	pkg:maven/org.springframework.boot/spring-boot-starter-aop@
4	4	spring-boot-starter-mail	2.7.1	org.springframework.boot	Java	pkg:maven/org.springframework.boot/spring-boot-starter-mail@
5	5	spring-boot-starter-validati	2.7.3	org.springframework.boot	Java	pkg:maven/org.springframework.boot/spring-boot-starter-valida
6	6	mysql-connector-j	8.0.33	com.mysql	Java	pkg:maven/com.mysql/mysql-connector-j@8.0.33
7	7	spring-boot-starter-test	3.1.0	org.springframework.boot	Java	pkg:maven/org.springframework.boot/spring-boot-starter-test@
8	8	mybatis-plus-boot-starter	3.5.2	com.baomidou	Java	pkg:maven/com.baomidou/mybatis-plus-boot-starter@3.5.2
9	9	dynamic-datasource-spring	3.2.0	com.baomidou	Java	pkg:maven/com.baomidou/dynamic-datasource-spring-boot-sta
10	10	freemarker	2.3.28	org.freemarker	Java	pkg:maven/org.freemarker/freemarker@2.3.28
11	11	fastjson	1.2.83	com.alibaba	Java	pkg:maven/com.alibaba/fastjson@1.2.83
12	12	lombok	1.18.10	org.projectlombok	Java	pkg:maven/org.projectlombok/lombok@1.18.10
13	13	guava	20.0	com.google.guava	Java	pkg:maven/com.google.guava/guava@20.0
14	14	javax.servlet-api	4.0.1	javax.servlet	Java	pkg:maven/javax.servlet/javax.servlet-api@4.0.1
15	15	commons-pool2	2.11.1	org.apache.commons	Java	pkg:maven/org.apache.commons/commons-pool2@2.11.1
16	16	commons-coll				
17	17	aws-java-sdk-s				
18	18	jsch				
19	19	maven-artifact				

Name	Version	Vendor	License	Langauge	PURL
spring-boot-starter-web	3.1.0	org.springframework.boot	Apache-2.0	Java	pkg:maven/org.springframework.boot/spring-boot-starter-web@3.1.0
spring-boot-starter-aop	3.1.0	org.springframework.boot	Apache-2.0	Java	pkg:maven/org.springframework.boot/spring-boot-starter-aop@3.1.0
spring-boot-starter-mail	2.7.1	org.springframework.boot	Apache-2.0	Java	pkg:maven/org.springframework.boot/spring-boot-starter-mail@2.7.1
spring-boot-starter-validation	2.7.3	org.springframework.boot	Apache-2.0	Java	pkg:maven/org.springframework.boot/spring-boot-starter-validation@2.7.3
mysql-connector-j	8.0.33	com.mysql	GPL-2.0-only	Java	pkg:maven/com.mysql/mysql-connector-j@8.0.33
spring-boot-starter-test	3.1.0	org.springframework.boot		Java	pkg:maven/org.springframework.boot/spring-boot-starter-test@3.1.0
mybatis-plus-boot-starter	3.5.2	com.baomidou	Apache-2.0	Java	pkg:maven/com.baomidou/mybatis-plus-boot-starter@3.5.2
dynamic-datasource-spring-boot-starter	3.2.0	com.baomidou	Apache-2.0	Java	pkg:maven/com.baomidou/dynamic-datasource-spring-boot-starter@3.2.0
freemarker	2.3.28	org.freemarker	BSD-3-Clause	Java	pkg:maven/org.freemarker/freemarker@2.3.28
fastjson	1.2.83	com.alibaba	Apache-2.0	Java	pkg:maven/com.alibaba/fastjson@1.2.83
lombok	1.18.10	org.projectlombok	MIT	Java	pkg:maven/org.projectlombok/lombok@1.18.10

Standard SBOM(Software Bill of Materials) Supported



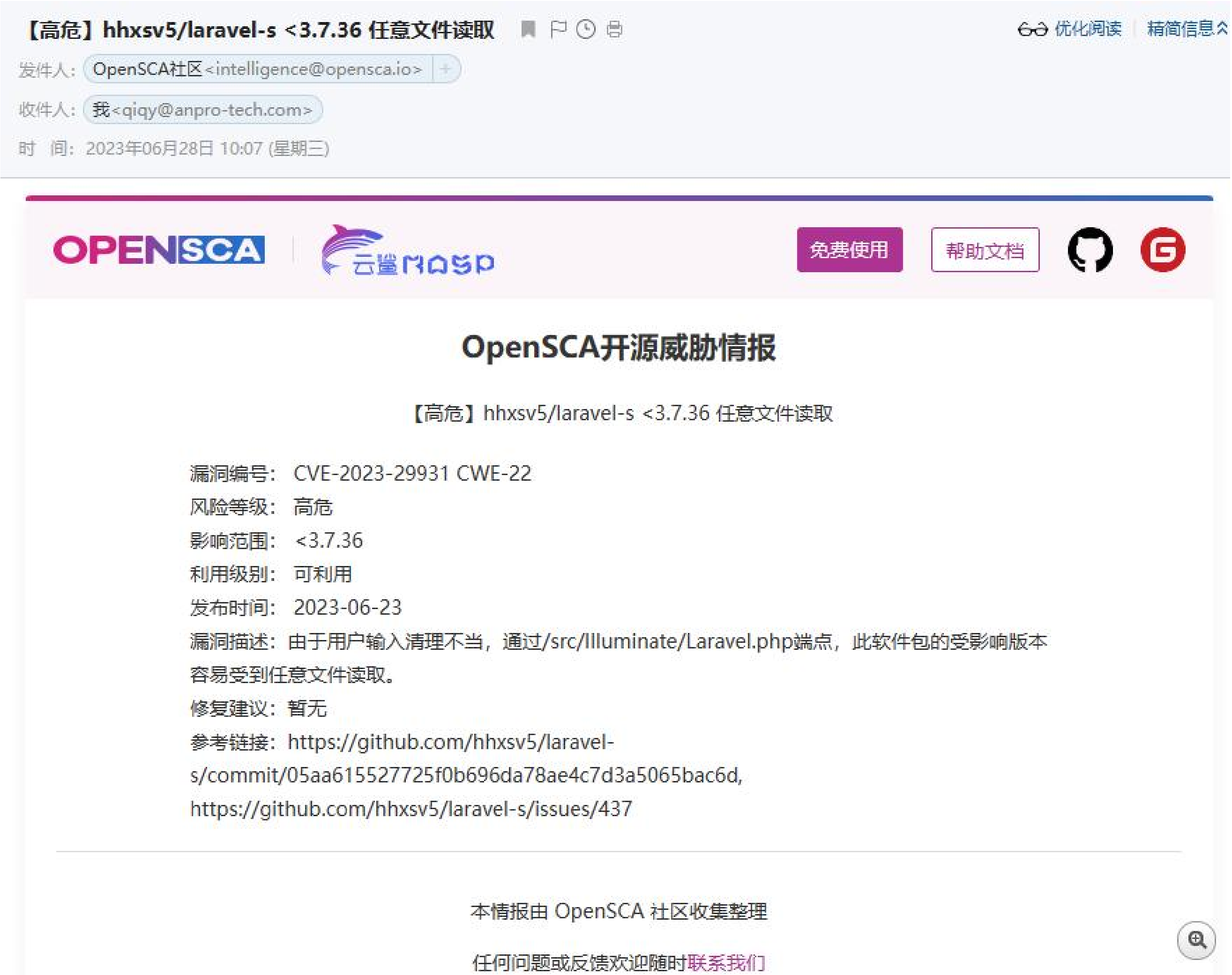
```
{
    "SPDXID": "SPDXRef-DOCUMENT",
    "spdxVersion": "SPDX-2.2",
    "creationInfo": {
        "created": "2022-12-21T09:22:54Z",
        "creators": [
            "Tool: SPDX Tools",
            "Organization:XMIRROR"
        ],
        "licenseListVersion": "3.8"
    },
    "name": "qqysbom",
    "dataLicense": "CC0-1.0",
    "documentNamespace": "https://www.xmirror.cn/spdxdocs/qqysbom-47547f4a-2d04-11b2-80d1-0242ac110002",
    "documentDescribes": [],
    "packages": [
        {
            "SPDXID": "SPDXRef-ch.qos.logback-logback-classic-1.1.11",
            "copyrightText": "NOASSERTION",
            "downloadLocation": "NOASSERTION",
            "filesAnalyzed": false,
            "licenseConcluded": "(Custom OR EPL-1.0)",
            "licenseDeclared": "(Custom OR EPL-1.0)",
            "name": "logback-classic",
            "originator": "Organization:ch.qos.logback",
            "versionInfo": "1.1.11"
        },
        {
            "SPDXID": "SPDXRef-org.springframework.security-spring-security-test-4.2.10.RELEASE",
            "copyrightText": "NOASSERTION",
            "downloadLocation": "NOASSERTION",
            "filesAnalyzed": false,
            "licenseConcluded": "Apache-2.0",
            "licenseDeclared": "Apache-2.0",
            "name": "spring-security-test",
            "originator": "Organization:org.springframework.security",
            "versionInfo": "4.2.10.RELEASE"
        }
    ]
}
```



```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.4",
  "version": 1,
  "metadata": {
    "component": {
      "bom-ref": "pkg:/@",
      "type": "application",
      "name": "",
      "purl": "pkg:/@"
    }
  },
  "components": [
    {
      "bom-ref": "pkg:maven/dev.jianmu/api@2.5.3",
      "type": "library",
      "author": "dev.jianmu",
      "name": "api",
      "version": "2.5.3",
      "purl": "pkg:maven/dev.jianmu/api@2.5.3"
    },
    {
      "bom-ref": "pkg:maven/dev.jianmu/el@2.5.3",
      "type": "library",
      "author": "dev.jianmu",
      "name": "el",
      "version": "2.5.3",
      "purl": "pkg:maven/dev.jianmu/el@2.5.3"
    },
    {
      "bom-ref": "pkg:npm/jianmu-ci-ui@2.5.3",
      "type": "library",
      "name": "jianmu-ci-ui",
      "version": "2.5.3",
      "purl": "pkg:npm/jianmu-ci-ui@2.5.3"
    },
```

Example of SBOM in SPDX & CycloneDX

Open Source Vulnerability Intelligence



【高危】hhxsv5/laravel-s <3.7.36 任意文件读取

发件人：OpenSCA社区<intelligence@opensca.io>

收件人：我<qiqy@anpro-tech.com>

时　间：2023年06月28日 10:07 (星期三)

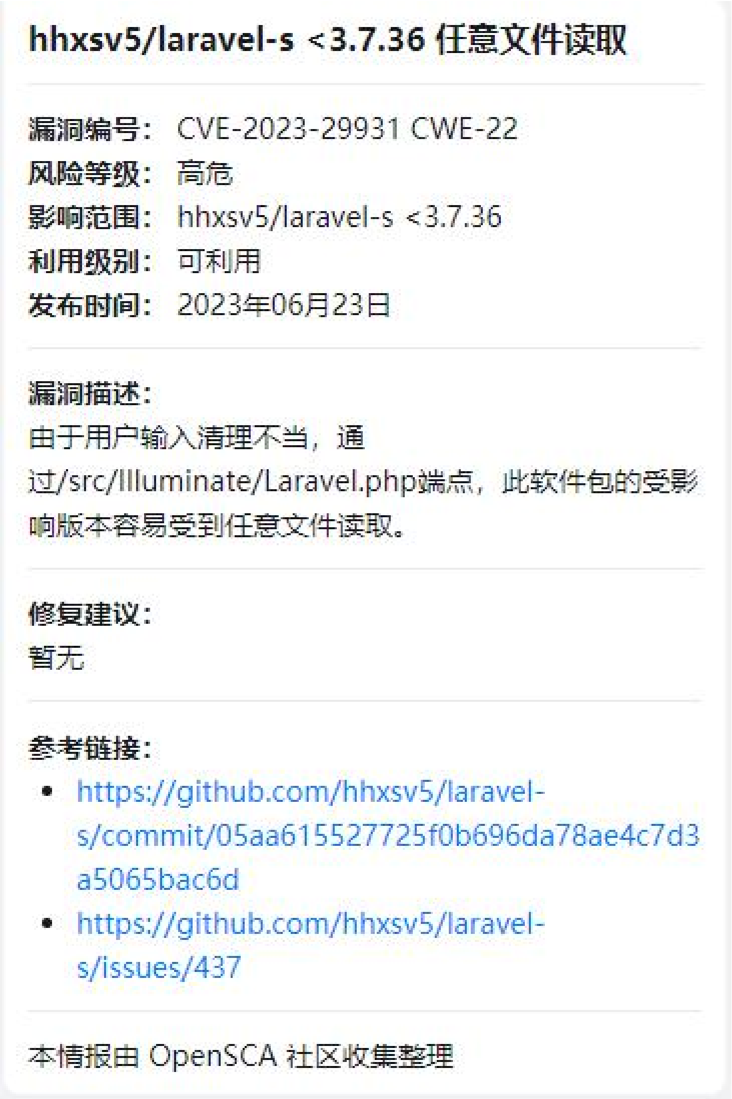
OpenSCA开源威胁情报

【高危】hhxsv5/laravel-s <3.7.36 任意文件读取

漏洞编号： CVE-2023-29931 CWE-22
风险等级： 高危
影响范围： <3.7.36
利用级别： 可利用
发布时间： 2023-06-23
漏洞描述：由于用户输入清理不当，通过/src/Illuminate/Laravel.php端点，此软件包的受影响版本容易受到任意文件读取。
修复建议：暂无
参考链接：https://github.com/hhxsv5/laravel-s/commit/05aa615527725f0b696da78ae4c7d3a5065bac6d, https://github.com/hhxsv5/laravel-s/issues/437

本情报由 OpenSCA 社区收集整理

任何问题或反馈欢迎随时联系我们



hhxsv5/laravel-s <3.7.36 任意文件读取

漏洞编号： CVE-2023-29931 CWE-22
风险等级： 高危
影响范围： hhxsv5/laravel-s <3.7.36
利用级别： 可利用
发布时间： 2023年06月23日

漏洞描述：
由于用户输入清理不当，通过/src/Illuminate/Laravel.php端点，此软件包的受影响版本容易受到任意文件读取。

修复建议：
暂无

参考链接：
- https://github.com/hhxsv5/laravel-s/commit/05aa615527725f0b696da78ae4c7d3a5065bac6d
- https://github.com/hhxsv5/laravel-s/issues/437

本情报由 OpenSCA 社区收集整理

Intelligence provided for community subscribers through email & IM

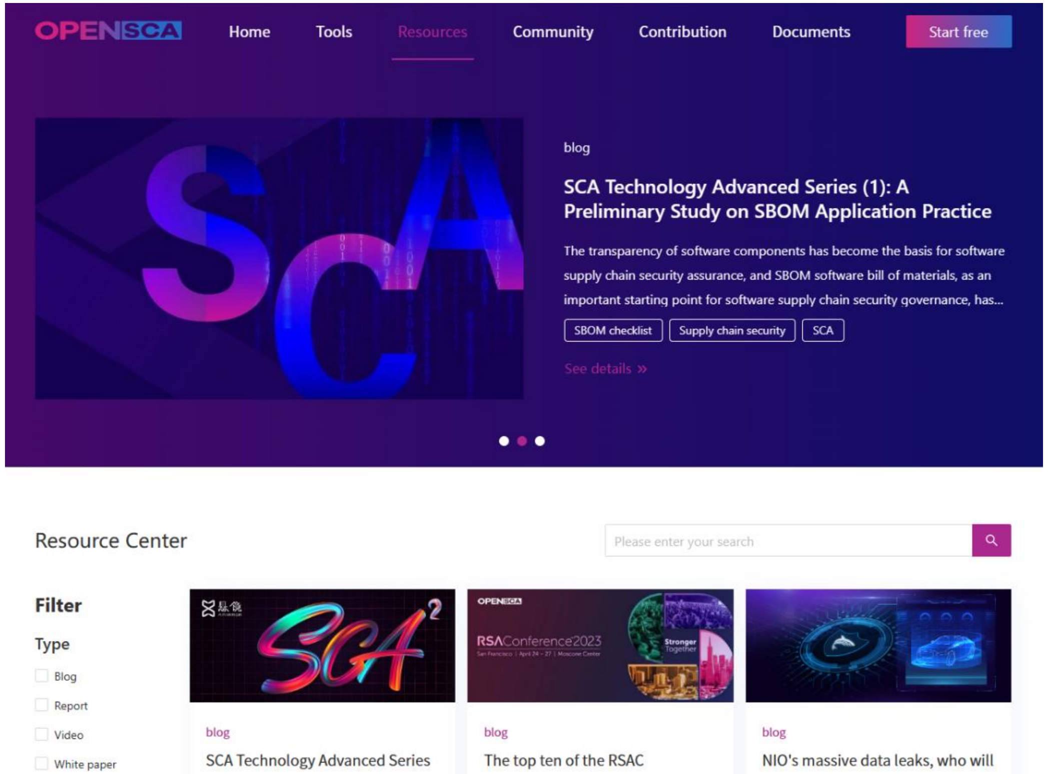
Part

03

Our community & cases

What have we done?

Our Community



blog

SCA Technology Advanced Series (1): A Preliminary Study on SBOM Application Practice

The transparency of software components has become the basis for software supply chain security assurance, and SBOM software bill of materials, as an important starting point for software supply chain security governance, has...

SBOM checklist | Supply chain security | SCA

See details »

Resource Center

Please enter your search

Filter

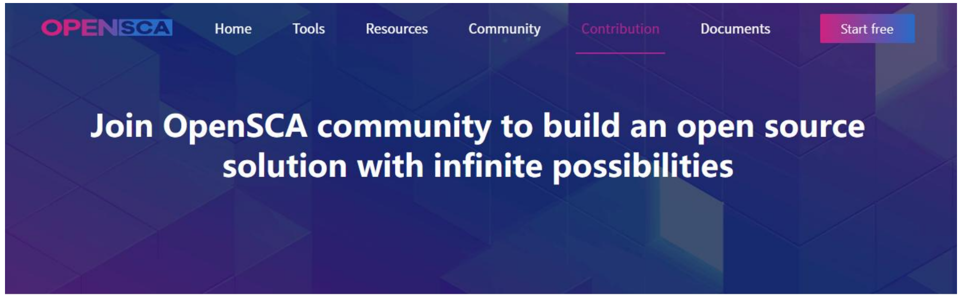
Type

□ Blog
□ Report
□ Video
□ White paper

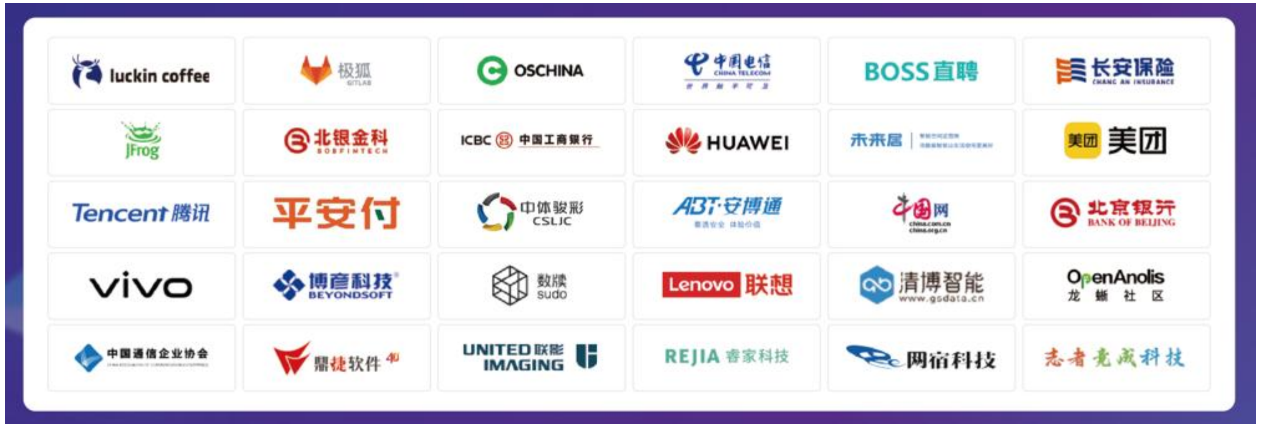
blog
SCA Technology Advanced Series

blog
The top ten of the RSAC

blog
NIO's massive data leaks, who will



Join OpenSCA community to build an open source solution with infinite possibilities



Contributors

itxiaohu001 China · Changsha	0Jvang China · Chengdu	luotianqi777 China · Hengshui	zidianzhimeng China · Changsha	donghuarui China · Chengdu
Wslzz China · Changsha	java-shixiaotao China · Chengdu	zc373721880 China · Changsha	zrxJuly China · Chengdu	TI4NLI4NG China · Chengdu
xxcka China · Changsha	lst201448 China · Beijing	404NOTFounDYC China · Changsha	npc7 China · NA	zhangdapeng520 China · Chengdu
Jack Wu China · Beijing	Fnzer0 China · Chengdu	magicyou China · Beijing	Liu Wanli China · Changsha	wenheshan China · Changsha
wtx0 China · Chengdu	huyongfeng China · Changsha	lzw_and_zs China · Chengdu	xssle ON	Yuan Shengjun China · Changsha
Teng Jiulin China · Chengdu				
lzx China · Beijing				

优秀开源项目
OpenSCA
中国开源云联盟
自主研发
创新成果
信息通信软件供应链安全社区
GVP-Gitee最有价值开源项目
OpenSCA-cli
OSCHINA
gitee
全球十大
开源产品
软博会
GLOBAL INFOSEC AWARDS
WINNER
CYBER DEFENSE MAGAZINE
2022
CYBER SECURITY
EXCELLENCE
AWARDS
WINNER
2022

Use Case: the SRC Department of an Internet Company

Security Team

Problem

DevOps flow’s requirement for effectiveness demands a flexible and reliable Open Source security management tool.

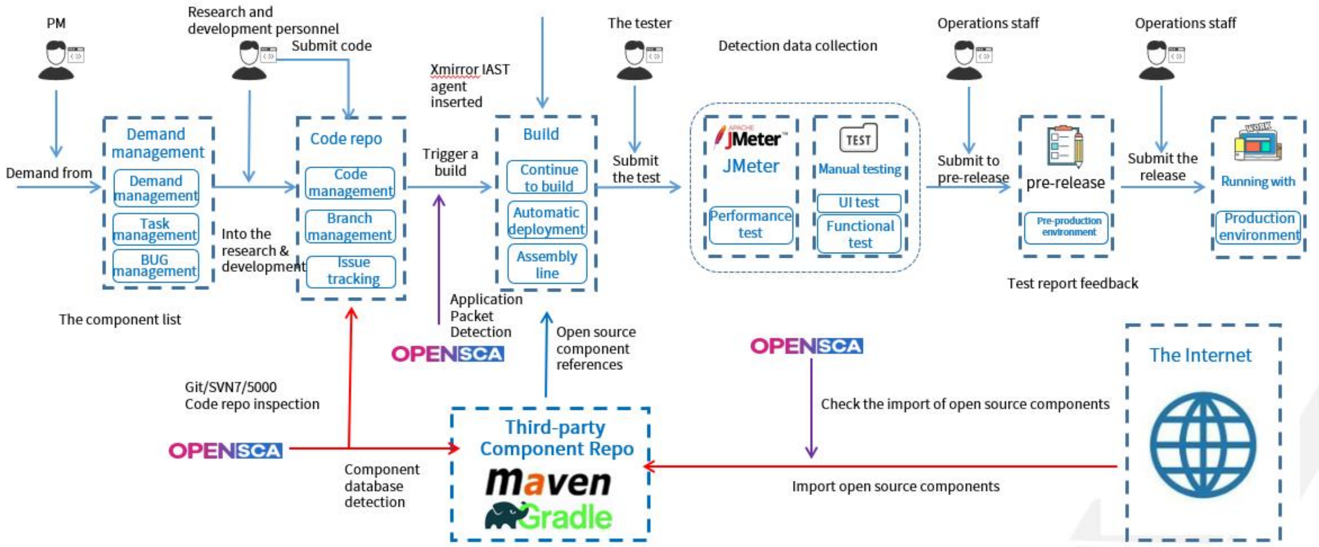
OpenSCA Solution

Redeveloped on the basis of OpenSCA, integrating it into different phases in DevOps and setting up a security management process using its result as a checking point.

Result

- ✓ Security integrated into DevOps flow
- ✓ Reveal OS risks introduced in code constantly
- ✓ Clarify relevant OS components & vulnerabilities

Scenario



The risk of vulnerabilities introduced by third-party OS components has been greatly reduced, achieving the inventory of internal component assets and vulnerability risks

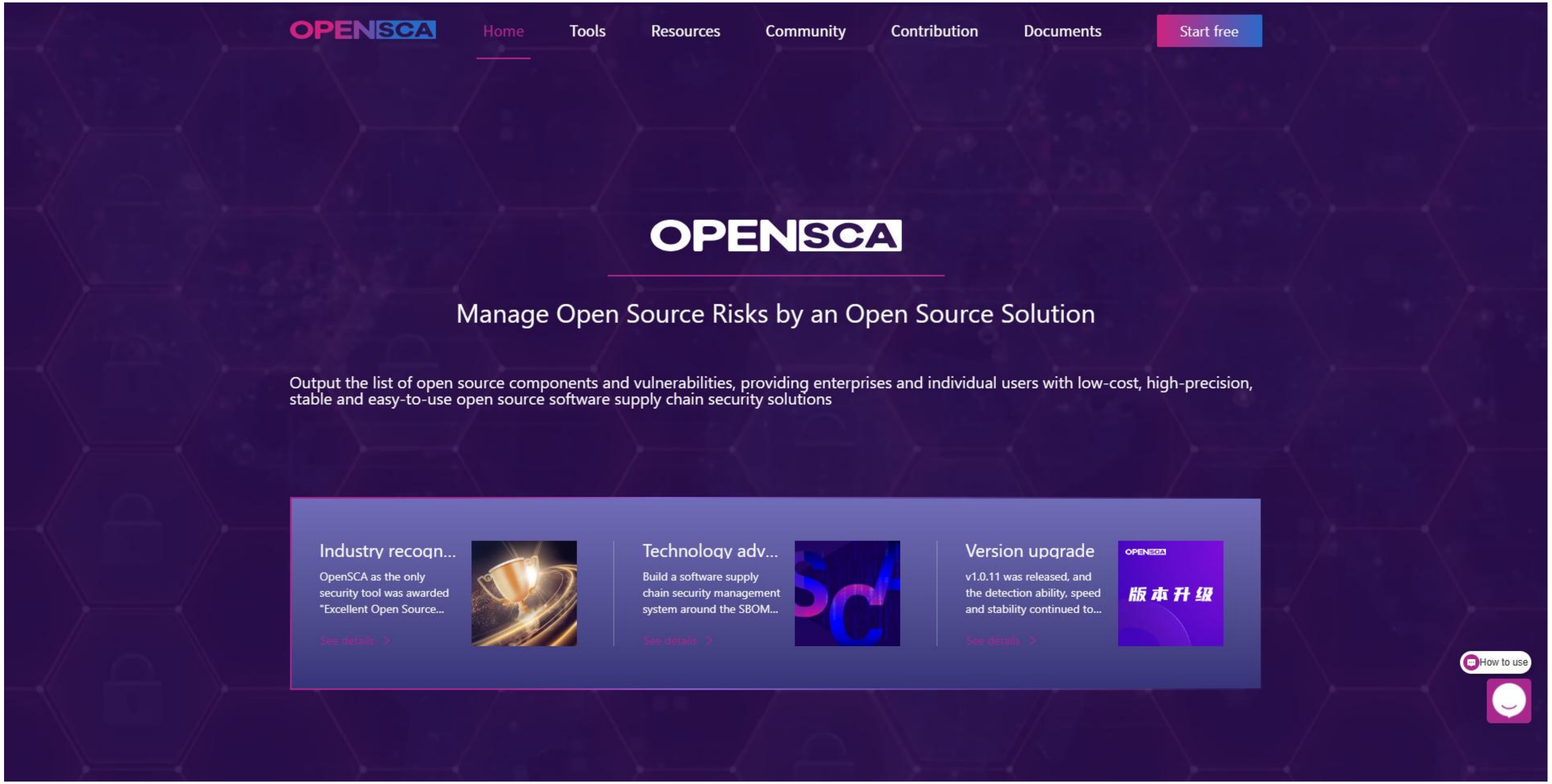
Part

04

Build together

Join us for the shared future

To the Open Source Future



Manage Open Source Risks by an Open Source Solution

Output the list of open source components and vulnerabilities, providing enterprises and individual users with low-cost, high-precision, stable and easy-to-use open source software supply chain security solutions

Industry recogn...
OpenSCA as the only security tool was awarded "Excellent Open Source...

See details >

Technology adv...
Build a software supply chain security management system around the SBOM...

See details >

Version upgrade
v1.0.11 was released, and the detection ability, speed and stability continued to...

See details >

- Provide solutions to international users
- Explorations to more applicable scenarios
- Work together for enhancing the security of the open source world

THANKS

Watch us