CAICT 中国信通院

7月3日-4日-中国·北京

2019云计算开源产业大会

《开源代码合规性测试方法》

演讲人： 辛小秋

关于开源

- **开源不仅仅是开放源代码**
  - 开源是一种成功的创新模式，与闭源模式相互影响，形成“共生”。
  - 开源许可证是商业许可证的简化版，同样受著作权法或者知识产权法的保护。
- **开源许可证（授权协议）**
  - 保留原作者的署名权（与“CC”协议中的“BY”属性相似）。
  - 将自由获取、自由修改、自由再发布等权利授权给用户。
  - 分为开放型许可证和传染性许可证两类。
  - 不当使用会造成潜在风险。

Open Source Initiative

Guaranteeing the 'our' in source...

ABOUT LICENSES MEMBERSHIP COMMUNITY RESOURCES NEWS & EVENTS

Licenses by Name

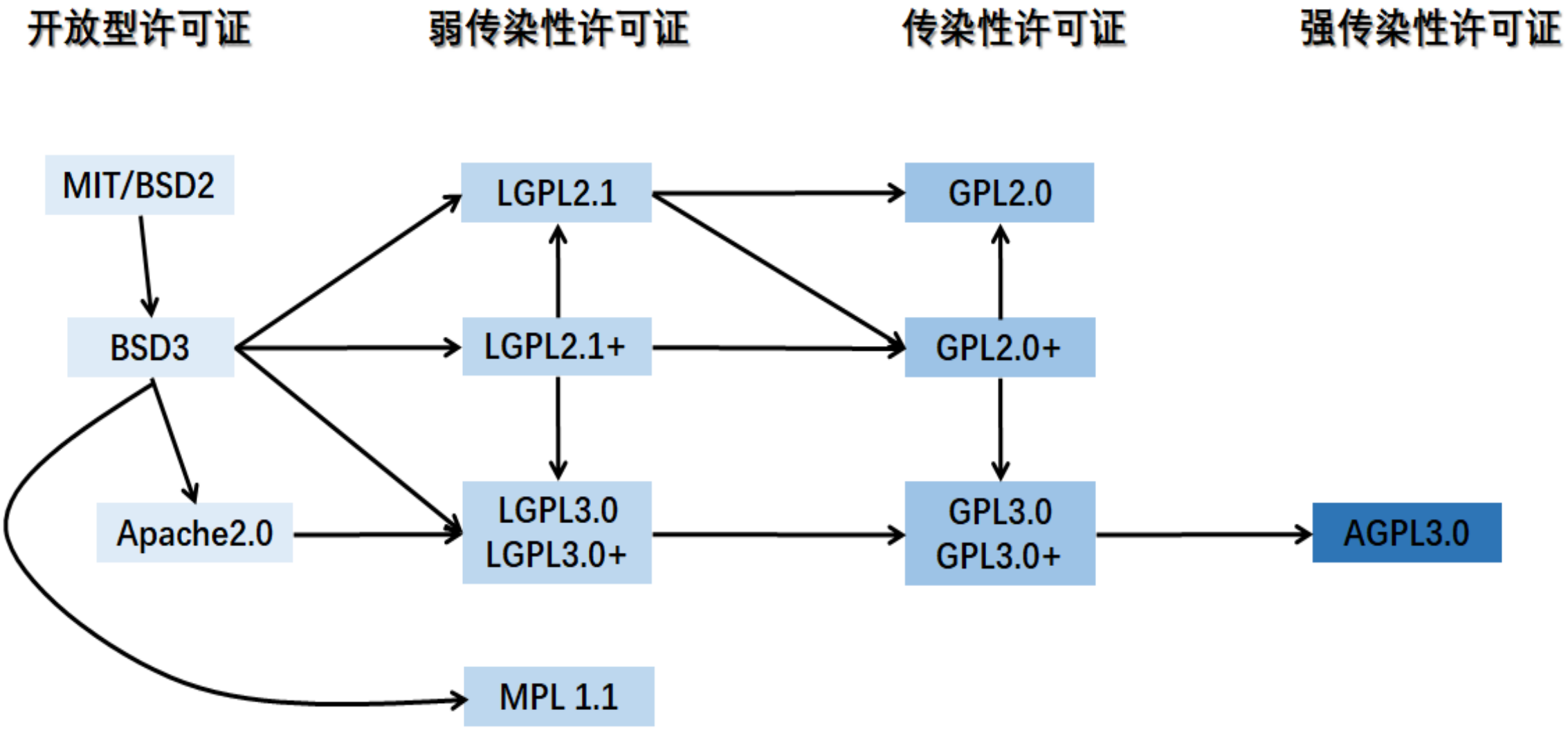
The following licenses have been approved by the OSI. The parenthesized expression following a license name is its SPDX short identifier (if one exists). This list does not include those OSI-approved licenses that have been voluntarily retired by their steward.

- 2-clause BSD License (BSD-2-Clause)
- 3-clause BSD License (BSD-3-Clause)
- Academic Free License 3.0 (AFL-3.0)
- Adaptive Public License (APL-1.0)
- Apache License 2.0 (Apache-2.0)
- Apple Public Source License (APSL-2.0)
- Artistic License 2.0 (Artistic-2.0)
- Attribution Assurance License (AAL)
- Boost Software License (BSL-1.0)

OSI：开源促进会，国际非盈利组织，经过OSI批准的开源许可证有82个。

open source initiative
Approved License

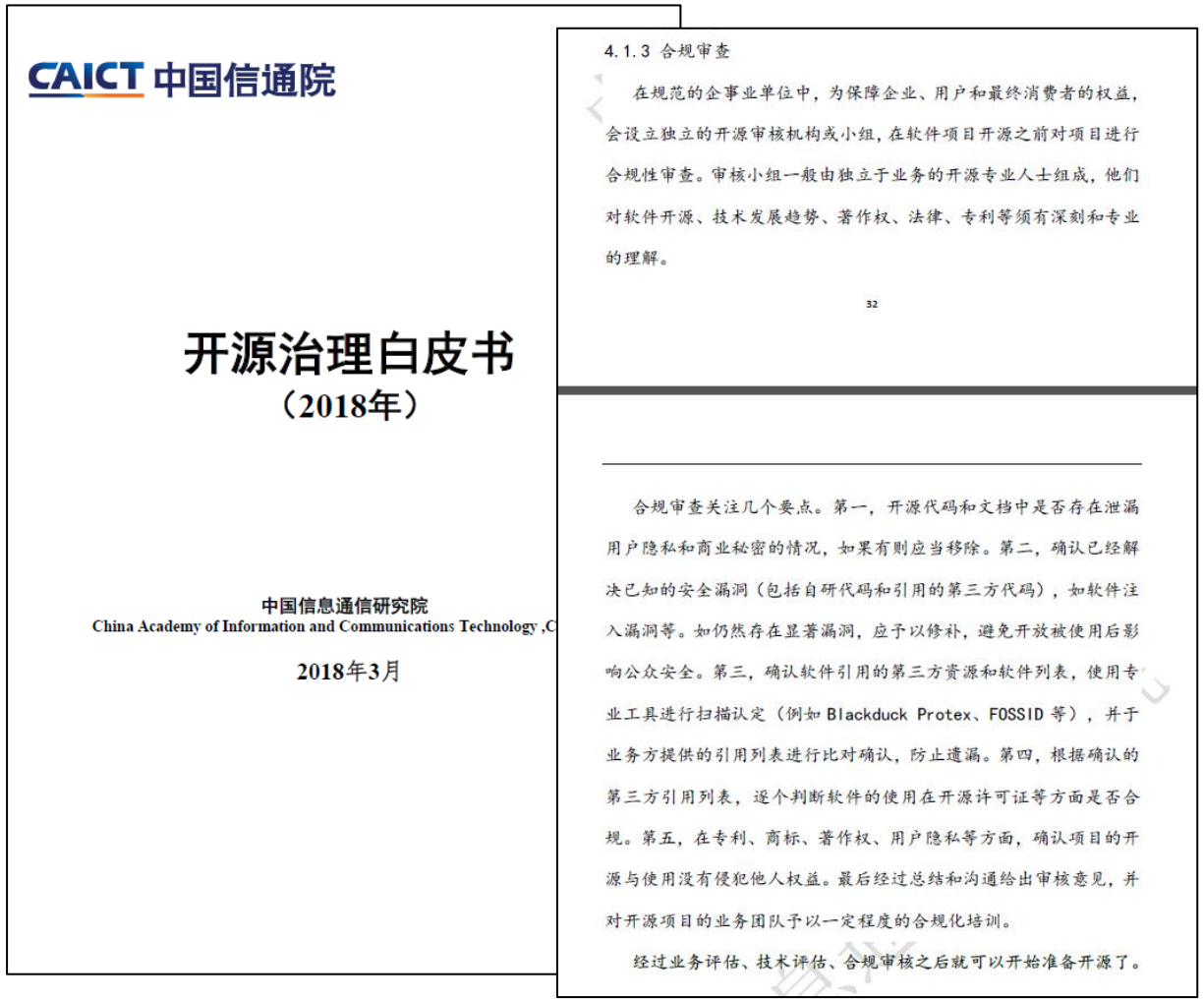
开源许可证的兼容性


开放型许可证
弱传染性许可证
传染性许可证
强传染性许可证
MIT/BSD2
BSD3
Apache2.0
LGPL2.1
LGPL2.1+
LGPL3.0
LGPL3.0+
MPL 1.1
GPL2.0
GPL2.0+
GPL3.0
GPL3.0+
AGPL3.0

开源带来的风险

- **合规性风险**
  - 开源许可证违规使用导致法律诉讼
    - 传染性风险、兼容性风险、其他违规风险
  - 风险：产品召回，自有代码被迫开源等
- **安全性风险**
  - 引入开源软件的同时，被动引入安全漏洞
  - 多数开源许可证没有承诺对安全性风险负责
  - 风险：安全漏洞爆发造成重大损失

开源监管力度在增强



CAICT 中国信通院

开源治理白皮书
（2018年）

中国信息通信研究院
China Academy of Information and Communications Technology ,C

2018年3月

4.1.3 合规审查

在规范的企事业单位中，为保障企业、用户和最终消费者的权益，会设立独立的开源审核机构或小组，在软件项目开源之前对项目进行合规性审查。审核小组一般由独立于业务的开源专业人士组成，他们对软件开源、技术发展趋势、著作权、法律、专利等须有深刻和专业的理解。

32

合规审查关注几个要点。第一，开源代码和文档中是否存在泄漏用户隐私和商业秘密的情况，如果有则应当移除。第二，确认已经解决已知的安全漏洞（包括自研代码和引用的第三方代码），如软件注入漏洞等。如仍然存在显著漏洞，应予以修补，避免开放被使用后影响公众安全。第三，确认软件引用的第三方资源和软件列表，使用专业工具进行扫描认定（例如 Blackduck Protex、FOSSID 等），并于业务方提供的引用列表进行比对确认，防止遗漏。第四，根据确认的第三方引用列表，逐个判断软件的使用在开源许可证等方面是否合规。第五，在专利、商标、著作权、用户隐私等方面，确认项目的开源与使用没有侵犯他人权益。最后经过总结和沟通给出审核意见，并对开源项目的业务团队予以一定程度的合规化培训。

经过业务评估、技术评估、合规审核之后就可以开始准备开源了。

2013 年国家信息安全专项 金融领域应用软件源代码安全检查产品测评方案

若TOE为单机程序，穿透性测试内容包括但不限于：信息泄露漏洞、用户口令安全性、用户权限安全性、数据存储安全性、资源泄漏等多类测试项，具体可根据实际产品的安全功能调整有关测试项。

4.4. 自主知识产权评估

4.4.1. 测评依据

通过将送检产品源代码同业界已有开源产品源代码进行对比分析，以及现场核查等多种手段，检测送检产品的自主知识产权情况。

4.4.4. 预期结果

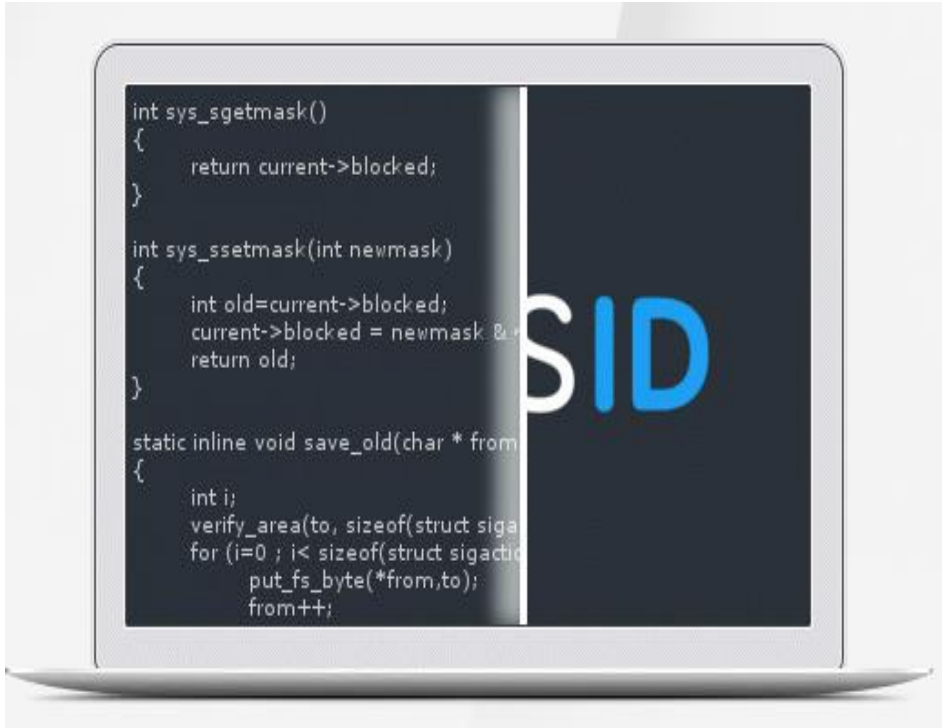
申报单位拥有送检产品的知识产权，且送检产品关键核心模块的源代码开源比例原则上不超过 30%，所使用的开源代码中不应包含 GPL（GNU 通用公共许可证）等强制要求开源的类型。（若测评机构经过测试发现产品由于其特殊

开源治理，工具先行

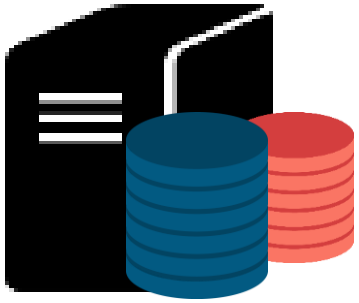
- **制度和流程**
  - “谁引入，谁负责”，开源代码登记制度等
- **人员和培训**
  - 开源治理委员会：工程师，法务，管理者
  - 定期进行政策、法律、技术培训
- **合适的工具（*发现问题是解决问题的前提*）**
  - 管理平台，开源代码扫描检测工具等
  - 及时发现存量和增量代码中使用开源软件的痕迹（包括许可证信息和安全漏洞信息）

开源代码扫描检测工具的应用场景

- **企业内部的代码检测需求**
  - 项目开源之前，查找自有代码中的开源风险；
  - 针对闭源商业代码，也需要规避合规性风险；
- **政府部门监管政策造成的开源治理需求**
  - 国家项目对自主知识产权的要求
  - 国家对某些重要领域的风险防控要求
- **国际合作中甲方提出的代码扫描需求**
  - 国内产品出口到欧美，甲方需要检测报告免责
- **企业兼并过程中的代码审计需求**
  - 邀请第三方进行审计，对收购标的进行软件资产评估



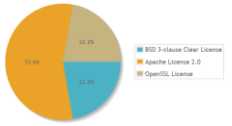
开源代码合规性测试原理



Scan Engine
& KB

开源组件清单
& License

安全漏洞列表



检测报告
&数据分析

用户代码

扫描 / 确认

结果输出

开源代码合规性测试举例（1）

FOSSID FOSS Audit Report test (20190528004)

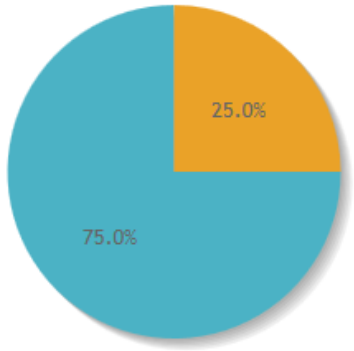
Summary | Components | Vulnerabilities | Identifications | Comments | Generated: 2019-05-28

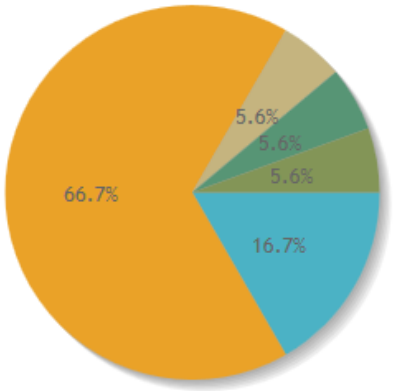
Summary

Audit

Created: 2019-05-28
Code: 20190528004
Name: test
Contact: victor victor (victor_demo@fs.com)

Description





Show 100 entries Search:

License	SPDX Identifier	Amount
GNU Affero General Public License v3.0	AGPL-3.0	12
GNU Lesser General Public License v2.1 or later	LGPL-2.1+	3
Apache License 2.0	Apache-2.0	1

FOSSID报告显示：用户代码中开源成分占比超过75%，其中有12个文件使用了AGPL3.0许可证。
如果用户代码用于提供互联网服务，使用AGPL3.0许可证，属于违规行为，存在被迫开源风险。

开源代码合规性测试举例（2）

FOSSID FOSS Audit Report

test (20190528004)

Summary | Components | Vulnerabilities | Identifications | Comments

Generated: 2019-05-28

Vulnerabilities

Copy | Excel | CSV

Search:

CPE	CVE	Severity	Attack Vector	Attack Complexity	Availability Impact
cpe:2.3:a:identityserver:identityserver3:2.5.0:*:*:*:*:*:*:*	CVE-2017-12677	MEDIUM (6.1)	NETWORK	LOW	NONE

IdentityServer3 authorize response页面跨站脚本漏洞

CNNVD编号：CNNVD-201708-360

CVE编号：CVE-2017-12677

发布时间：2017-08-10

更新时间：2017-08-10

漏洞来源：

危害等级：中危

漏洞类型：跨站脚本

威胁类型：远程

厂　商：identityserver

漏洞简介

IdentityServer3是一个基于.NET的对Web应用程序进行访问控制的插件。authorize response page是其中的一个授权响应页面。

IdentityServer3中的authorize response page的Angular表达式存在跨站脚本漏洞。远程攻击者可利用该漏洞获取有关IdentityServer授权响应的敏感信息。以下版本受到影响：IdentityServer3 2.4.x版本，2.5.x版本，2.6.1之前的2.6.x版本。

漏洞公告

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/IdentityServer/IdentityServer3/releases/tag/2.6.1

CVE-2017-12677 Detail

Current Description

IdentityServer3 2.4.x, 2.5.x, and 2.6.x before 2.6.1 has XSS in an Angular expression on the authorize response page, which might allow remote attackers to obtain sensitive information about the IdentityServer authorization response.

Source: MITRE

View Analysis Description

Impact

CVSS v3.0 Severity and Metrics:

Base Score: 6.1 MEDIUM

Vector: AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N (V3 legend)

Impact Score: 2.7

Exploitability Score: 2.8

Attack Vector (AV): Network

Attack Complexity (AC): Low

Privileges Required (PR): None

User Interaction (UI): Required

CVSS v2.0 Severity and Metrics:

Base Score: 4.3 MEDIUM

Vector: (AV:N/AC:M/Au:N/C:N/I:P/A:N) (V2 legend)

Impact Subscore: 2.9

Exploitability Subscore: 8.6

Access Vector (AV): Network

Access Complexity (AC): Medium

Authentication (AU): None

Confidentiality (C): None

None

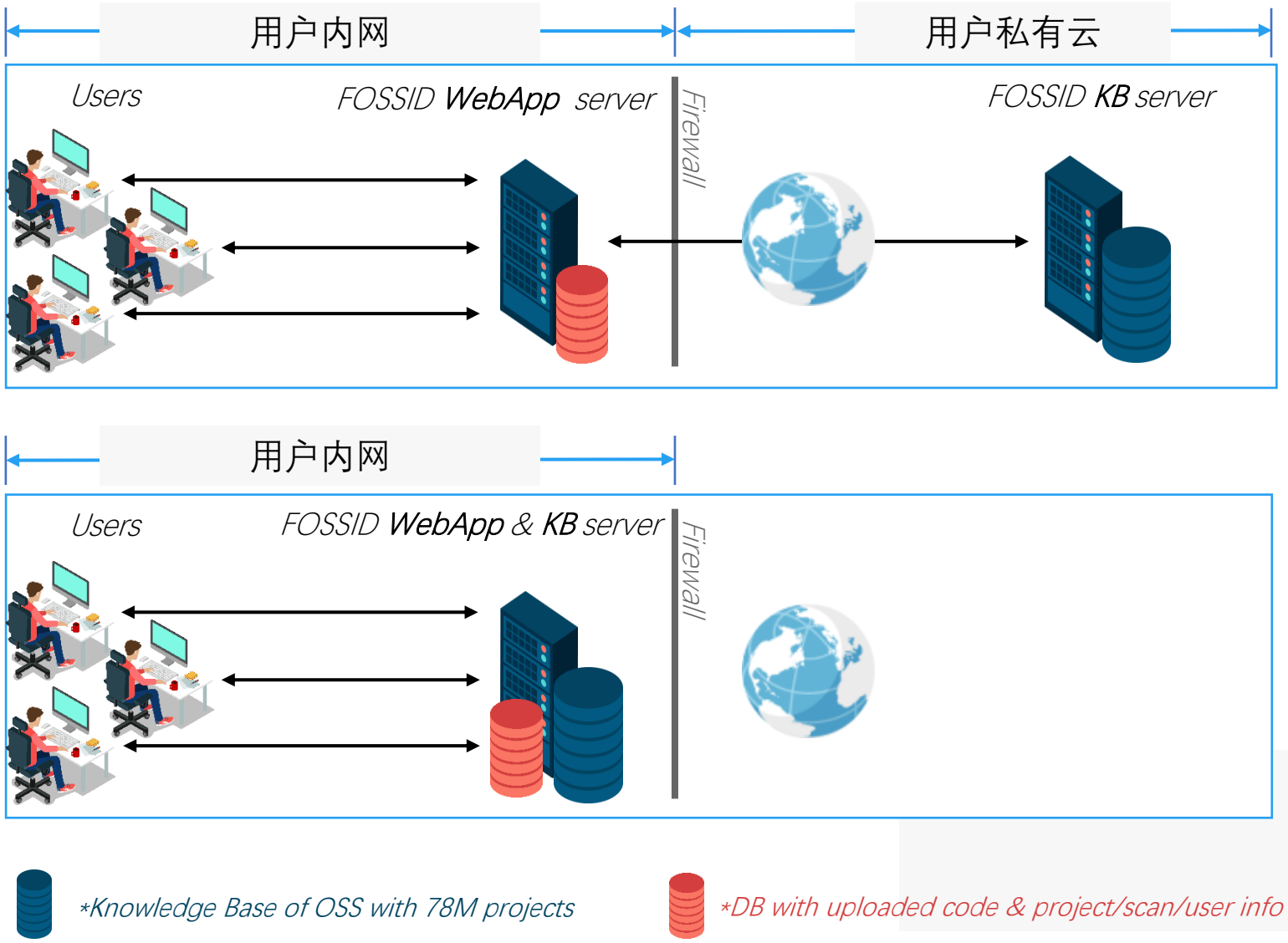
ntarily interact with attack mechanism

ized modification

FOSSID报告显示：用户代码中引用的开源组件存在安全漏洞，建议用户到NVD或者CNNVD网站中查询详细描述和补丁信息。

代码安全以及信息安全

- **完全离线**
  - 离线安装、离线注册
  - 离线扫描、离线报告
  - 离线升级、离线维护
- **盲审方式**
  - 工具与代码分离
  - 特殊场景下保证代码安全
- **安全前提**
  - 拒绝代码上传
  - 避免信息外泄



关注开源软件的扫描精度

- **整个组件**

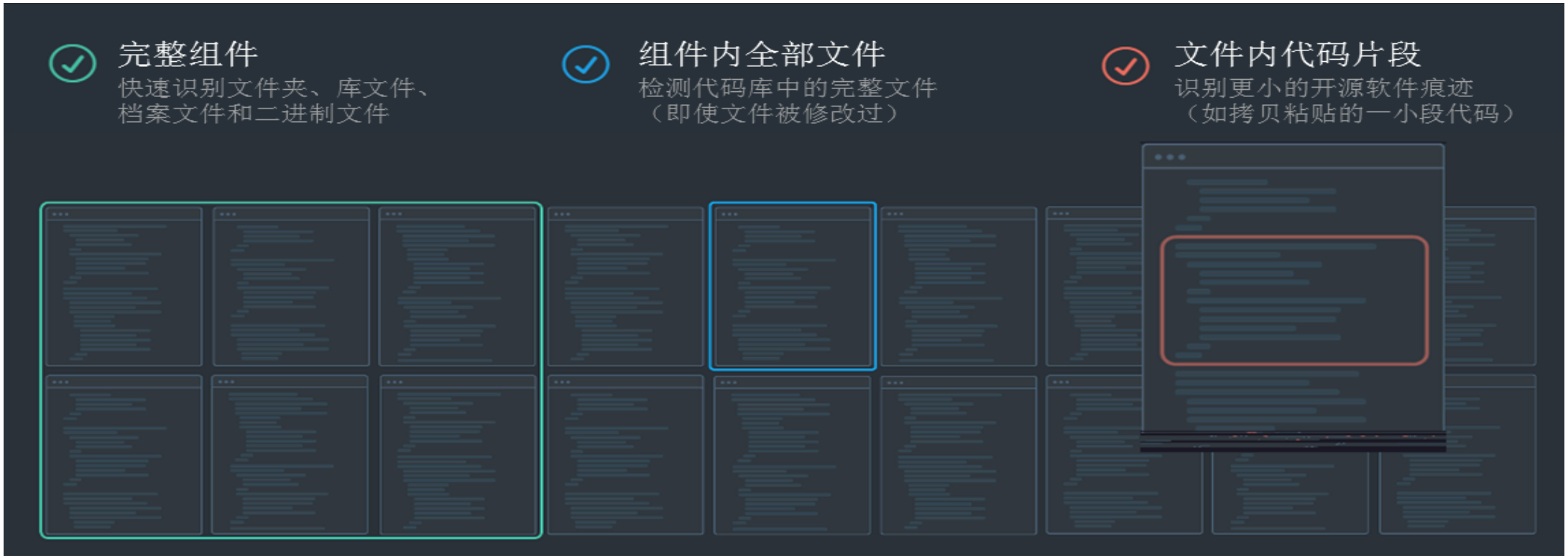
  快速识别文件夹、库、存档或者二进制文件。

- **完整文件**

  检查代码库中的完整文件，无论它们是否被修改过。

- **代码片段**

  识别更小的开源脚本，如复制粘贴的一小段代码。



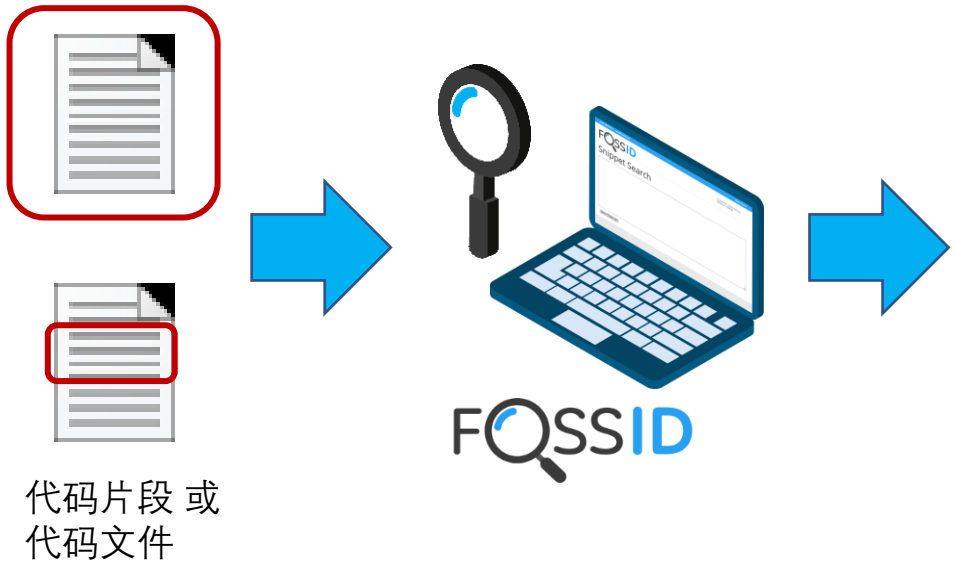
关注开源许可证嵌套风险

通过扫描此文件代码，工具将提供很多有价值的许可证信息。

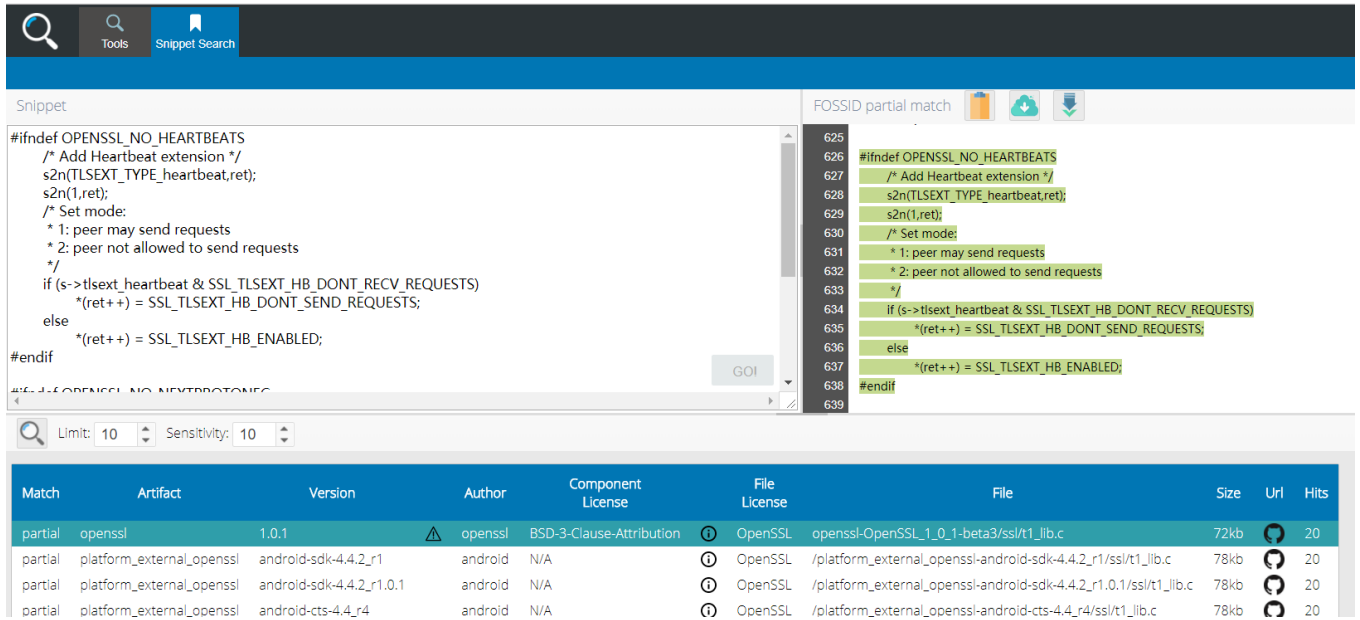
- **组件许可证**
  该组件的发布许可证
- **文件/代码片段许可证**
  如果该文件或者代码片段具有特定的许可证声明
- **底层许可证**
  该组件内部的不同的许可证

温馨提示：“通过许可证嵌套等方式规避风险”将导致更大风险。

开源代码检测前移可以降低风险



代码片段 或
代码文件



快速匹配结果

开源代码检测前移到研发部门，便于研发人员临时甄别一小段代码的风险，选择低风险代码，可以有效降低企业在开源治理过程中的纠错成本。

开源代码合规性风险的应对建议

- **合规性风险分类**
  - 传染性风险：由传染性许可证的违规使用造成的“被迫开源自有代码的风险”
  - 兼容性风险：由开源许可证的违规使用造成的许可证冲突
  - 其他违规风险：未遵守某些开源许可证的要求导致的风险
- **传染性风险应对**
  - 发现并确认传染性风险：不同应用场景的风险不同
  - “替代”优于“重写”：同一段代码可能被不同作者使用不同许可证开源多次
  - “逻辑模仿”优于“简单粗暴”：采用“A/B模式”进行逻辑模仿
- **合规性风险预防**
  - 将开源代码扫描检测与研发过程融合，可以有效降低合规性风险以及纠错成本

CAICT 中国信通院

7月3日-4日-中国·北京

2019云计算开源产业大会

THANKS