

SourceCheck

用户操作手册

公司概况

公司简介

开源网安成立于 2013 年 5 月，是国内软件安全行业创领者和领先的软件安全开发生命周期（SSDLC）解决方案提供商，专注于软件安全领域技术研究。开源网安团队由来自思科、微软、惠普、Google、华为等行业顶级的安全专家组成，团队成员从业经验均为 10 年以上。开源网安总部在深圳，同时在北京、上海、武汉、成都、合肥设有分支机构。

开源网安始终以自主创新为发展源动力，以 S-SDLC 解决方案为核心，以 S-SDLC 平台为载体，向不同行业的客户提供覆盖软件开发全生命周期的软件安全开发咨询和落地服务，包括但不限于安全开发培训、安全需求识别、安全架构设计、安全代码实现、安全确认、安全审核及安全运营的完整业务生态，同时提供配套的工具链支持。帮助客户提升软件安全开发能力，构建安全可靠的软件产品。

未来，开源网安将持续聚焦软件安全领域，努力成为全球软件安全领域极具竞争力的领导品牌。

公司愿景 - 捍卫中国软件安全

核心价值 - 专业开源、信赖

联系方式 - 电话：4000-983-183

网址：www.seczone.cn

邮箱：service@seczone.cn

微信公众号



版权声明

本文所有内容文字、图片、方法、过程等内容，除另有特别注明，版权均属[深圳开源互联网安全技术有限公司](#)所有，受到有关产权和版权法保护。任何个人、机构未经[深圳开源互联网安全技术有限公司](#)的书面授权许可，不得以任何方式复制或引用本文的任何片段。违者将依法追究责任。

1. 快速开始

1.1 术语解释

SCA Software Composition Analysis

2019 年，Gartner 定义：软件成分分析产品对应用程序进行分析，以检测开源软件组件是否带有已知的安全漏洞或功能漏洞，及需要恰当授权许可的商业软件或第三方产品。它有助于确保企业软件供应链仅包含安全的组件，从而支持安全的应用程序开发和组装。

应用软件

用户可以使用的各种程序设计语言，以及用各种程序设计语言编制的应用程序的集合，分为源码包、应用软件包等，既包含开源软件，也包含非开源软件。

开源软件

允许用户直接访问源代码，通过开源许可证将其复制、修改、再发布的权利向公众开放的计算机软件。

开源许可证

开源软件的版权拥有人可通过开源许可证，授权用户免费使用、修改、共享版权软件，规范受著作权保护的软件的使用或者分发行为。

包管理器

又叫软件包管理系统，指不同编程语言的专用的包管理和构建系统。

1.2 登录平台

使用平台之前需要先登录平台，登录平台的步骤如下所示。

- 1) 打开浏览器，在地址栏输入 SourceCheck 平台的 ip 地址或者域名
- 2) 输入账号、密码和验证码，点击登陆

2. 常用功能

2.1 开始检测

SourceCheck 平台可以进行以下几种检测：

- [单应用检测](#)
- [批量仓库检测](#)

2.1.1 创建项目

场景与功能简介

创建项目功能是为了方便企业对单应用和批量仓库应用的管理而设置的功能。在进行单应用或批量仓库应用检测之前，需要先创建项目，之后在项目中添加应用。用户可以将多个应用添加到一个项目中进行管理。点击顶部导航栏的“项目”。

2.1.2 单应用检测

场景与功能简介

单应用检测有三种情况。第一种是在普通项目下添加本地上传的单应用，指的是通过本地上传或者特征文件上传的方式在项目中添加应用，再进行检测。第二种是在普通项目下添加在线代码仓库的单应用。第三种是在仓库项目下添加在线代码仓库的单应用。下面是以在普通项目下添加本地上传单应用为例进行说明。选择本地上传的单应用检测时应提前准备好 3G 以内的检测包，检测包的格式支持 zip, rar, tar, 7z, tar.gz, war, jar 等。单应用检测涉及到的场景有两种，一种是在已有项目中添加本地应用，此场景一般适用于在已经创建好的项目中添加相关检测包进行检测；另一种是在已有应用中再次上传本地应用，这种场景下，原有应用会被最新上传的应用覆盖。

2.2 检测结果查看

2.2.1 项目详情

场景与页面简介

项目详情是对每个项目检测结果的详情汇总。通过浏览项目详情，既可以宏观了解项目的风险等级，漏洞分布等重要信息，也可以了解该项目下所属的应用，组件，漏洞等详情。项目详情中主要有8个部分的内容，分别为项目基本信息，概览信息，应用信息，组件信息，漏洞信息，许可信息，风险说明，项目成员。

2.2.2 应用详情

场景与页面简介

应用详情是对每个应用检测结果的详情汇总。通过浏览应用详情，既可以宏观了解应用的风险等级，漏洞分布等重要信息，也可以了解该应用下的组件，许可，漏洞等详情。应用详情中主要有9个部分的内容，分别为应用基本信息，概览信息，组件信息，漏洞信息，许可信息，告警信息，风险说明，检测历史，架构信息。

2.3 报告管理

2.3.1 报告生成与导出

场景与功能简介

使用报告的生成与导出功能可以将平台的检测数据导出成本地文件，当需要将检测数据进行团队共享或者对重点对象数据进行存档时，可以使用此功能。

2.4 预警中心

场景与功能介绍

预警中心提供了新漏洞预警和违反策略告警两个板块的内容。新漏洞预警指的是当知识库中出现了新的漏洞，新漏洞的信息也会在第一时间推送到 SourceCheck 平台。违反策略告警指的是当被引入到平台的组件，许可或漏洞违反了已经在平台设置好的策略或规则时，平台会提出告警。预警中心的设置是为了实时为用户检测危险因素，当出现任何危险信息时，都会第一时间推送至平台，尽可能做到风险最小化。您可以通过点击个人中心-预警中心，进入到相关告警页面。

2.5 版本信息查看

场景与功能介绍

版本信息查看中提供了平台版本号信息，数据版本号信息以及引擎版本号信息。可以通过点击“版本更新记录”查看历史版本信息。需要查看版本信息可通过点击个人中心-版本信息进行查看。

2.6 许可信息查看

场景与功能介绍

许可信息中展示了机器信息 ID，序列号，适配应用，开始时间和到期时间等信息。需要查看许可信息可通过点击个人中心-许可信息进行查看。