开源网安
SECZONE GROUP

CodeSec 用户手册

- 深圳开源互联网安全技术有限公司 -

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（S-SDLC）解决方案提供商，专注于软件安全领域的技术研究。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、合肥、成都设有分支机构。

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

开源网安代码审核平台（简称 CodeSec）是一种静态应用安全测试（SAST）解决方案，在产品全生命周期的安全开发和安全测试阶段为企业和开发者提供一种代码安全检测工具。

本操作手册提供了 CodeSec 平台的以下信息：

- CodeSec 概述
- CodeSec 快速入门指南
- 功能介绍和操作说明

1 CodeSec 概述

下面几节重点介绍本文档编写的目的、平台简介以及对平台使用角色的介绍和说明：

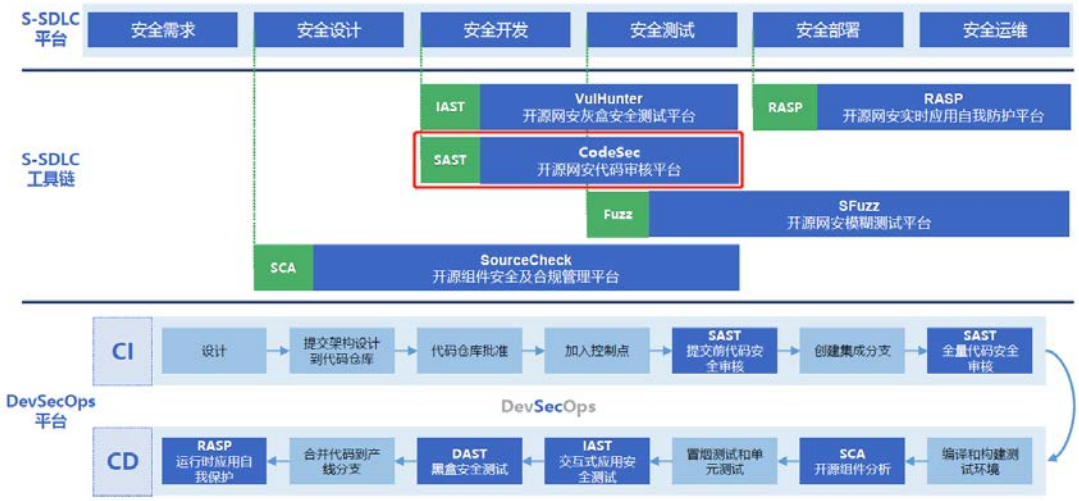
1.1 文档目的

为了帮助开源网安代码审核平台（以下简称 CodeSec）的用户更好地了解和使用该平台,提高用户与平台的亲和度。该手册简述了平台的系统架构图、功能清单、软件性能、产品的主要参数以及系统的操作指导，以及该软件使用过程中应注意的一些问题。

1.2 平台介绍

CodeSec 是全新一代静态应用安全测试（SAST）解决方案，主要用于软件源代码安全审核和质量分析，提供漏洞详情和代码级修复方案，帮助开发和安全团队在 S-SDLC 的早期发现并修复漏洞，提升软件代码安全质量。

CodeSec 全面覆盖各种编程语言，支持多达 2000+种安全漏洞和主流编码规范的检测；扫描结果精准呈现，界面简明易于操作；提供多种集成方式，更加适用于 DevOps 等场景。



CodeSec 具有较强的发现代码漏洞缺陷的能力。通过内置的五大引擎：数据流、语义、结构、控制流、配置流等对应用软件的源代码进行静态的分析，与软件 CodeSec 安全漏洞规则集进行匹配、查找，从而将源代码中存在的安全漏洞扫描出来，最终在 CodeSec 平台输出扫描的结果，并可以将扫描的结果生成报告，同时支持多种格式报告的导出功能。

CodeSec 产品架构

1.3 角色介绍

CodeSec 平台的用户主要包括：企业管理员、审计员、团队管理员和普通用户。CodeSec 的账号可分别由 CodeSec 支持人员添加（企业管理员），企业管理员添加（团队管理员、审计员或者普通用户）或者团队管理员添加（普通用户）。CodeSec 平台有一下四种用户角色：

- **企业管理员：**企业组用户，由 CodeSec 技术支持人员在系统中添加，拥有创建企业内团队审计员、管理员和普通用户，设置企业级规则以及配置企业内引擎列表权限。
- **审计员：**企业级用户，由企业管理员登陆后创建。权限包括：查看所有项目中检测到的安全弱点信息，跟踪漏洞，管理项目、查看项目报告等。
- **团队管理员：**团队级用户，由企业管理员登录后创建。团队管理员的权限包括：给本团队添加普用户，创建项目，扫描项目，查看项目中检测到的安全弱点信息，跟踪漏洞，查看数据中心的数据。
- **普通用户/团队成员：**团队的普通成员，由企业管理员或者团队管理员登录后添加。权限包括：查看项目中检测到的安全弱点信息，跟踪漏洞等。

2 快速入门指南

下面几个章节重点介绍项目配置和运行 CodeSec 的步骤。

2.1 准备工作

为了能够快速访问 CodeSec，确保以下内容：

代码获取方式

CodeSec 支持多种代码获取方式，包括：a)代码文件上传：直接从本地上传源代码；b)代码仓库获取：支持 GIT、SVN、TFS、Perforce、Mercurial。

支持的编程语言

CodeSec 支持 C、C++、Java、JavaScript、Python、PHP 、C#、Go、Swift 等主流编程语言。

2.2 创建团队和成员

企业管理员登录系统后可开始创建团队、审计员和团队管理员，搭建平台使用的组织架构。

关于项目团队的创建

系统管理员可根据企业的开发团队的规模进行创建并进行项目团队的管理；

关于用户的创建

通过企业管理员账号可创建审计人员、团队管理员等用户信息。

2.3 配置漏洞规则集和报告模板

企业管理员可以针对漏洞规则集和报告模板进行配置。

关于漏洞规则的配置

通过漏洞规则的配置，实现对多种开发语言实现漏洞规则进行管理。CodeSec 目前支持对各种编程语言不同级别漏洞的配置选择的操作。

关于报告模板配置

企业管理员可以配置项目扫描结果的报告格式的配置。包括封面的配置、导出内容、导出格式等的设置。

2.4 检测一个项目

2.4.1 创建项目

用户可通过项目管理-项目列表-新建项目来创建项目。

2.4.2 结果检查

创建成功的项目可以在项目列表中【漏洞详情】按钮查看项目扫描结果和对扫描结果进行审计等操作。

2.4.3 生成和下载报告

在项目列表页可对扫描成功的项目执行生成报告和下载报告的操作

3 产品功能说明

CodeSec 主要的核心功能模块主要包括扫描引擎、规则集管理、项目管理、审计管理、系统管理和用户管理模块。

图：功能架构图

扫描引擎

本模块是 CodeSec 的核心模块，系统引擎针对不同的语言使用其特定的语言解析器，基于抽象语法树构建统一数据模型，源码扫描器根据内置的规则，开始针对构建好的数据进行缺陷检测。可跨平台运行，解决编译模式下，编译器对运行环境的强依赖导致可移植性差的问题；减少漏报，检测时可以忽视源代码的完整性，也可提供较好的检测精确度，最大程度挖掘更多的漏洞。

规则集管理

支持按照不同语言和不同严重等级进行分类。可通过管理员对漏洞规则集进行维护，包括规则的新增、编辑和删除功能。支持 2000+种漏洞类型，包括不限于：SQL 注入、跨站脚本、路径遍历、缓冲区溢出、空指针解引用、变量未初始化使用、硬编码等常见漏洞。

项目管理模块

项目管理模块支持对项目的参数进行配置，包括设置扫描对象、配置扫描参数和设定扫描策略并控制扫描任务的执行和关闭。

审计管理模块

审计管理模块主要针对项目扫描结果产生的漏洞进行管理，由于静态应用安全检测技术原理的问题，扫描结果存在一定的误报，该模块支持对漏洞的标记功能，通过人工标记减少误报。

系统管理模块

实现了其他模块所需的底层功能，如可靠的时间戳、扫描引擎内存配置、项目最长扫描时间限制、生成报告大小限制、代码片段行数配置等。

用户管理模块

确定与系统交互的各类角色，并确保用户与正确的、包括其角色在内的安全属性相关联、用户管理模块也确保各个用户使用相应的安全功能前都已经被成功鉴别。