



CodeSec 用户手册\_V3.2

文档编号：V3.2 发布日期 2023-12-30

开源网安（珠海）技术有限公司

目录

[变更日志 1](#bookmark1)

[第一章：CODESEC 概述 2](#bookmark2)

[1.1 文档目的 2](#bookmark3)

[1.2 平台介绍 2](#bookmark4)

[1.3 角色介绍 4](#bookmark5)

[第二章：CODESEC 快速入门指南 5](#bookmark6)

[2.1 准备工作 5](#bookmark7)

[2.2 创建团队和成员 6](#bookmark8)

[2.3 配置规则和报告模板 7](#bookmark9)

[2.4 检查一个项目 7](#bookmark10)

[2.4.1 创建项目 7](#bookmark11)

[2.4.2 项目检查和分析 9](#bookmark12)

[2.4.3 生成和导出报告 15](#bookmark13)

[第三章：平台安装说明 16](#bookmark14)

[第四章：功能介绍和操作说明 17](#bookmark15)

[4.1 用户功能介绍 17](#bookmark16)

[4.2 企业管理员操作手册 18](#bookmark17)

[4.2.1 系统登录 18](#bookmark18)

[4.2.2 用户信息管理 19](#bookmark19)

[4.2.3 首页 20](#bookmark20)

[4.2.4 项目管理 21](#bookmark21)

[4.2.5 团队管理 35](#bookmark22)

[4.2.6 用户管理 38](#bookmark23)

[4.2.7 报告管理 42](#bookmark24)

[4.2.8 规则管理 47](#bookmark25)

[4.2.9 引擎管理 52](#bookmark26)

[4.2.10 日志管理 54](#bookmark27)

[4.2.11 系统管理 58](#bookmark28)

[4.3 审计员操作手册 62](#bookmark29)

[4.3.1 系统登录 62](#bookmark30)

[4.3.2 首页 62](#bookmark31)

[4.3.2 项目管理 64](#bookmark32)

[4.3.3 数据中心 79](#bookmark33)

[4.4 团队管理员操作手册 80](#bookmark34)

[4.4.1 系统登录 80](#bookmark35)

[4.4.2 用户列表 81](#bookmark36)

[4.4.3 团队管理 85](#bookmark37)

[4.4.4 项目管理 87](#bookmark38)

[4.4.5 数据中心 104](#bookmark39)

[4.5 普通用户操作手册 105](#bookmark40)

[4.5.1 系统登录 105](#bookmark41)

[4.5.2 项目管理 105](#bookmark42)

变更日志

|  |  |
| --- | --- |
| 平台版本/  手册版本 | 变更 |
| V3.2.8 | 新增  · 新增 CodeSec概述，请参见*[第一章：CodeSec概述](#bookmark43)*[，](#bookmark43)对文档 编写的目的、平台简介和用户角色进行介绍和说明；  · 新增 CodeSec 快速入门指南， 请参见*[第二章节：CodeSec快](#bookmark44)* *[速入门指南](#bookmark45)*[，](#bookmark45)帮助用户快速了解和使用 CodeSec 平台；  · 新增平台安装步骤， 请参见*[第三章节：平台部署安装](#bookmark46)*[，](#bookmark46)用 户可快速准确完成平台的部署和安装；  · 按照用户角色对功能和平台操作的介绍进行修改，请参见 *[第四章：功能介绍和操作说明](#bookmark47)*[，](#bookmark47)对不同用户角色的平台功能介 绍和平台操作介绍 |

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

· 平台安装说明

· 功能介绍和操作说明

第一章： **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。

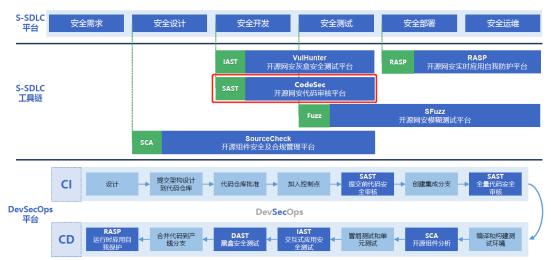
1.2 平台介绍

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。

第二章： **CodeSec** 快速入门指南

下面几个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：

CodeSec 部署安装

CodeSec 必须提前部署安装，以便为用户快速通过电脑浏览器访问平台和查看分析和

汇总的数据。CodeSec 支持本地部署和云端部署， 建议采用本地部署的方式。

请参见*[第三章：平台部署安装](#bookmark48)*[，](#bookmark48)详细介绍了本地部署安装的有关要求和配置信息。

访问 CodeSec 需要准备以下信息

· 主机名

· 端口号和类型

· 用户名（邮箱）

· 密码

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。

请参见*[第四章：用户功能介绍和平台操作](#bookmark49)*[，](#bookmark49)详细介绍创建项目时获取代码的方法。

也可以通过 IDE 插件（IDEA/Eclipse/Visual Studio/VS Code/Android Studio 等）、 Jenkins 插件、 API 接口、命令行等多种方式发起扫描。*可详见《IDE 插件安装手册》、《Jenkins 插*

*件安装手册》和《API 接口文档》。*

支持的编程语言

CodeSec 支持主流的 C 、C++ 、Java 、JavaScript 、Python 、PHP ，和常用 C# 、Go、

Perl 、Ruby 、Swift 等编程语言。

浏览器要求

为了更好的体验和显示 CodeSec 平台的各个功能，建议用户在以下版本的浏览器上进

行浏览：

· Chrome 63 以上

· 火狐 69 以上

· EdgeV79 以上

· OperaV50 以上

CodeSec 安装程序和许可文件

CodeSec 安装程序和 License 可以从开源网安的技术支持人员获得。

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，搭建软件

安全体系的组织架构。

关于项目团队的创建

请参见*[4.2.4 团队管理](#bookmark50)*[，](#bookmark50)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；

关于审计员的创建

请参见*[4.2.6 用户管理](#bookmark51)*[，](#bookmark51)系统管理员可创建审计员的用户信息，用于对各个团队的项 目进行审计和代码漏洞的管理；

关于团队管理员的创建

请参见*[4.2.6 用户管理](#bookmark52)*[，](#bookmark52)系统管理员可创建团队管理员的用户信息，团队管理员负责 团队项目的创建、项目管理和漏洞管理， 以及团队成员的创建于管理。

2.3 配置规则和报告模板

企业管理员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 目前支持对各类编程语言不同级别漏洞的配置操作， 请参见 *[4.2.8](#bookmark53) [规则管理](#bookmark54)*[。](#bookmark54)

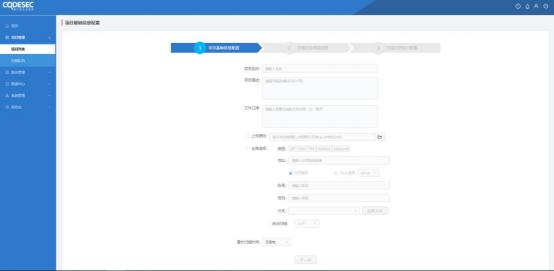
企业管理员可以配置项目扫描结果的报告格式的配置，包括封面的配置、

导出内容、导出格式等的设置，请参见*[4.2.7 报告管理](#bookmark55)*[。](#bookmark55)

2.4 检查一个项目

**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：



1、配置项目基础信息，依次填写以下信息：

· 【项目名称】用户手工输入项目名称，必填项

· 【项目描述】用户手工输入项目描述

· 【文件过滤】用户手工输入需要过滤的源码文件名称，以“, ”隔开

· 【上传源码】支持选择上传的源码（支持 zip,rar 格式文件）

· 【仓库选择】支持选择仓库地址，仓库类型支持 GIT、SVN、TFS、Perforce、

Mercurial；

· 【最长扫描时长】支持设置最长扫描时长。

以上信息填写完成后，点击【下一步】完成项目基础信息配置，进入扫描任务类型选

择页面。

注：如果未上传源码或者填写仓库地址信息， 下一步则不能创建静态代码进行扫描。

2、选择扫描任务类型， 选择以下任务类型：



静态代码任务

注：默认为静态代码任务，下一版本将支持选择编码规范和动态代码任务。

3、配置扫描任务执行，依次填写以下信息：



· 【项目任务类型】默认为“静态代码任务”， 不可修改

· 【自动识别语言】支持选择是否支持自动语言识别功能

· 【代码语言】支持多类型代码语言的选择，包括 Java/JSP、C#/ASP.NET、PHP、

C/C++、Python、JavaScript、Object-C、swift、go

· 【扫描二进制】支持选择是否扫描二进制

· 【JDK 版本选择】选择 JDK 版本，包括 JDK1.5、1.6、1.7、1.8、1.9、11

· 【文件过滤】支持选择扫描过滤的文件， 包括 javascript、css、png 等格式的文件

· 【扫描规则】支持选择后台预定义扫描的规则

· 【安全函数】自定义过滤安全函数名，例如： main,test,print

· 【快速扫描】支持选择是否进行快速扫描功能

以上信息配置完成，点击【创建】项目创建成功，系统自动按照设置的时 间执行代码扫描任务；点击【创建并执行】，项目创建成功并执行项目代码扫

描任务。

**2.4.2** 项目检查和分析

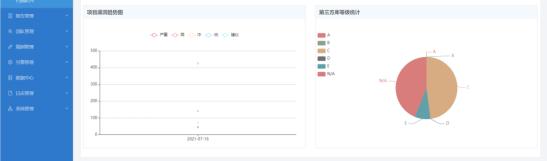
平台可根据设置的时间循环扫描，也支持手动执行扫描任务。扫描结果可 通过查看【项目列表】 ->【查看项目详情】 ->【静态代码扫描结果】查看。项 目详情页包含四个部分内容： 漏洞概述、漏洞详情、修复建议和第三方组件。

漏洞详情

对项目扫描的结果进行汇总统计分析，包括： ①安全弱点、严重弱点和误报数进行统 计； ②第三方库、CVE、CNNVD 漏洞库中对用的漏洞数的统计； ③最近一次扫描新发现的漏

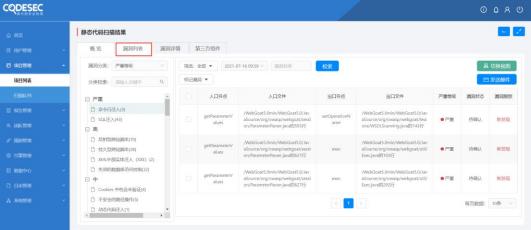
洞数统计， 复发的漏洞书统计， 已修复的漏洞数统计； ④代码总行数的统计。





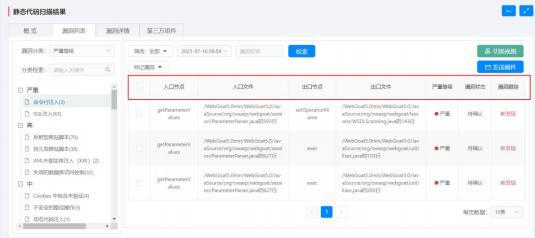
漏洞列表

对系统检测出的漏洞进行汇总， 如下图：

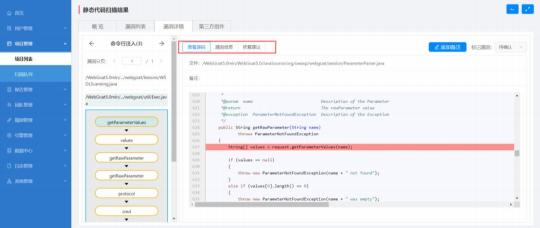


1）查看漏洞： 通过【漏洞列表】查看漏洞信息，包括漏洞的入口节点、入口文件、出

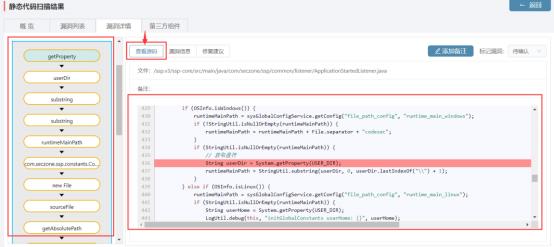
口节点和出口文件、对应的严重等级、漏洞状态和漏洞跟踪。如下图：



点击列表中对应的漏洞【入口文件】，即可查询漏洞信息。如下图：



通过【漏洞详情】， 可分别查看漏洞入、出口节点，以及对应的源码， 如下图：



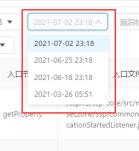
通过【漏洞信息】， 可查看对应的漏洞的概述，包括漏洞的概念及示例代码，如下

图：



通过【修复建议】可查看对该漏洞的修复建议，如下图：





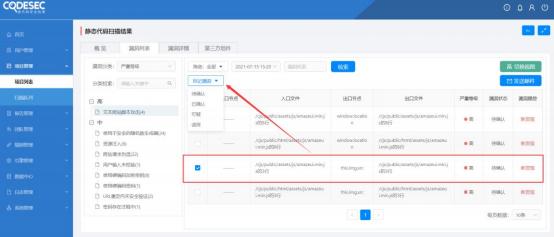
2）漏洞筛选： 通过【漏洞列表】也可通过多个维度对漏洞进行查询，包括按照漏洞分

类、漏洞状态和时间维度对漏洞进行查询，如下图：



3）漏洞标记：在【漏洞列表】页勾选漏洞进行标记，标记的状态分为： 待确认（漏洞

默认状态） 、已确认、可疑和误报四种。如下图：



4）切换视图： 用户可在【漏洞列表】页勾漏洞执行切换视图的操作，可在列表和结构

图之间进行切换，如下图所示：



5）发送邮件： 在【漏洞列表】页勾选漏洞，可将漏洞通过邮件的方式发送给项目团队

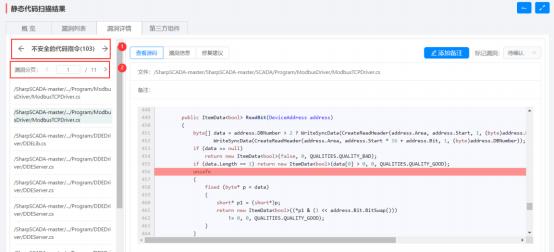
管理员或项目成员等，如下图：



漏洞详情

用户可通过【漏洞列表】点击漏洞对应的文件，直接跳转到漏洞详情页，也可以通过

点击【漏洞详情】查看漏洞详细信息。



可通过左上角标识为①、②的区域切换不同等级的漏洞和漏洞间的切换。

关于【查看源码】、【漏洞信息】和【修复建议】详细介绍见上文。

第三方组件

通常情况下，第三方组件都是开源的。由于第三方组件不是由本项目开发者编写的组件 或者应用。第三方组件的作者遵循行业内的一些协议， 允许其他软件开发者自由使用这些组

件。但这些组件安全性未知，通过平台代码扫描服务，可以检测到潜在的威胁。如下图：



点击列表中的【查看】按钮，可查看第三方组件的扫描详情， 如下图：



全屏显示

支持全屏显示功能。



**2.4.3** 生成和导出报告

生成报告

点击【生成报告】按钮， 可生成静态代码扫描报告，生成报告的格式为系统默认格

式，审计员在使用该功能时，可根据需求选择和定义，如下图：

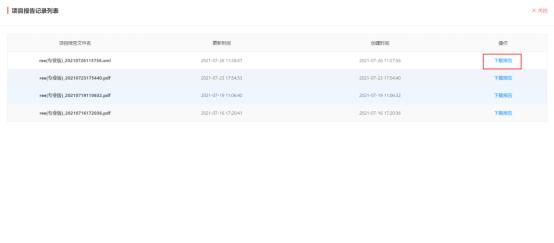


生成报告时用户可已选择导出报告的格式（支持 Word、PDF 和 XML）、可选择报告的

模板、漏洞分类（可按照严重等级、 OWASP Top10 2017 等格式导出）等。

导出报告

点击【下载报告】， 页面跳转到生成报告列表页， 如下图：



用户可根据需要选择相应的报告，点击【下载报告】，可将报告下载到本地，报告示

例如下图：





注：仅截取报告的部分内容。

第三章： 平台安装说明

CodeSec 主要有两种部署方式： 1)软件 + 硬件（企业本地机房部署） ;

2)纯软件（公网 SaaS 部署 / 企业虚拟机部署）



B/S 软件系统架构 CodeSec-HD 系列服务器

CodeSec 产品一般采用硬件交付，我公司会预先配置好授权码， 开箱即用。 用户只需准备服务器机架位置、电源和内部网络安装系统时需要提供固定 IP、 网关、子网掩码等网络参数。若采购多个扫描引擎， 则每个引擎都需要预留机架 位置、电源和内部网络。用户无需安装客户端，通过浏览器即可访。CodeSec 用 户端操作系统不限。 为了保证源代码安全， CodeSec 服务器一般不连接互联网，

CodeSec 系统升级及漏洞库升级采用离线方式线下进行。

第四章： 功能介绍和操作说明

本章节按照不同的用户角色对用户功能的介绍，重点介绍各个角色对平台操作。

4.1 用户功能介绍

CodeSec 平台各个角色的功能清单如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 用户角色 | 功能模块 | 功能点 | 备注 |
| 企业  管理员 | 系统登录 | 系统登录 | 通过 CodeSec 支持人员分配的用户名和密码登录 |
| 账号信息 | 查询个人账户信息 | 包括账户基本信息和密码设置功能 |
| 首页 | 项目安全信息展示 | 项目信息统计、安全弱点信息统计、弱点检出量 排行（Top5）等 |
| 项目管理 | 项目列表 | 查看所有项目中检测到的安全弱点信息， 查看漏 洞，管理项目、查看项目报告等 |
| 扫描队列 | 查看正在扫描中的项目 |
| 团队管理 | 团队列表 | 包括新建、查询、编辑、删除等操作 |
| 用户管理 | 用户列表 | 包括新建、编辑、删除等操作 |
| 审核列表 | 对用户账号进行审核，包括通过和拒绝 |
| 报告管理 | 模板配置 | 新建报告模板、编辑、删除和批量删除模板的操 作 |
| 导出配置 | 新建、查看、编辑、删除和批量删除导出设置模 板 |
| 规则管理 | 漏洞规则配置 | 实现对多种开发语言实现漏洞规则的配置 |
| 静态代码规则集配 置 | 配置多种静态代码扫描规则 |
| 引擎管理 | 新建引擎 | 新建和配置引擎信息 |
| 引擎列表 | 管理引擎 |
| 日志管理 | 用户日志 | 管理用户操作日志信息 |
| 引擎日志 | 管理系统引擎日志信息 |
| 服务日志 | 管理系统服务日志信息 |
| 系统管理 | JIRA 配置 | 配置 JIRA 地址和账号密码和 JIRA 状态 |
| 许可信息 | 展示机器码、授权截止日期等信息 |
| 邮件管理 | 配置发送邮件的邮箱 |
| 系统监控 | 对系统内存占用率、 CPU 使用率、磁盘存储实时 监控 |
| 回收站 | 回收站 | 支持对删除文件搜索、恢复、删除、清空 |
| 审计员 | 系统登录 | 系统登录 | 通过企业管理员分配的用户名和密码登录 |
| 首页 | 项目安全信息展示 | 项目信息统计、安全弱点信息统计、弱点检出量 排行（Top5）等 |
| 项目管理 | 项目列表 | 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 |
| 扫描队列 | 查看正在扫描中的项目 |
| 数据中心 | 项目数据汇总 | 各个项目所对应的团队、用户和各类型漏洞统计 |
| 漏洞数据汇总 | 支持按照漏洞级别、开发语言维度查询各类漏洞 的数量统计 |
| 团队管理 员 | 系统登录 | 系统登录 | 通过用户名和密码登录 |
| 用户管理 | 用户列表 | 新建、编辑、重置密码、删除用户等操作 |

|  |  |  |  |
| --- | --- | --- | --- |
|  | 团队管理 | 团队列表 | 编辑团队、管理团队成员 |
| 项目管理 | 项目列表 | 管理项目、跟踪漏洞导出报告等 |
| 数据中心 | 项目数据汇总 | 团队项目的各类漏洞的数据汇总统计 |
| 漏洞数据汇总 | 支持按照漏洞级别、开发语言维度查询各类漏洞 的数量统计 |
| 普通用户 | 系统登录 | 系统登录 | 通过团队管理员分配的用户名和密码登录 |
| 项目管理 | 项目列表 | 新建项目、跟踪漏洞、漏洞标记等 |

4.2 企业管理员操作手册

4.2.1 系统登录

业务场景：用户登录系统

操作路径：【输入 URL】->【输入用户名/密码】

操作说明：

1、在浏览器中输入 URL：http://ip:port 即可打开开源网安 CodeSec 平台登录界 面， 其中 IP 是指扫描工具的服务器 IP 地址， PORT 是指端口(端口默认是 28081)。使用 开源网安代码审核平台服务商提供的企业管理员的用户名及密码，即可登录，如下图：



2、企业管理员完成登陆后，进入到系统界面，如下图：





注：企业管理员具有开源网安代码审核平台的最高权限。

**4.2.2** 用户信息管理

业务场景：用户查看个人账号信息，重置密码

操作路径：【系统页面】->【右上角信息设置图标】

操作说明：通过【账号信息】查看用户的个人账号信息，如下图：



字段说明：

1.个人信息

【企业集团】由超级管理员分配企业账户时设置，当前账户不可修改

【登录账号】由管理员分配账户时设置，当前账户不可修改

【用户姓名】由管理员分配账户时填写，当前用户可修改，点击更新按钮可更新用户 姓名信息

【手机账号】由管理员分配账户时填写，当前用户可修改，点击更新按钮可更新手机 账号信息

【有效日期】由管理员分配账户时设置，当前账户不可修改

【团队】由管理员分配账户时设置，当前账户不可修改

【角色】由管理员分配账户时设置，当前账户不可修改

2.密码设置

【当前密码】如若重置密码，需输入当前账户的登录密码

【新密码】输入新密码

【重复密码】重复输入新密码予以确认

**4.2.3** 首页

业务场景：查看系统仪表盘

操作路径：【登录系统】->【系统首页】

操作说明：通过【首页】查看系统仪表盘，如下图：



字段说明：

【团队数量】统计企业集团内项目团队的数量

【项目数量】统计企业集团内的项目数量

【安全弱点】统计企业集团内所有项目的安全弱点数量

【严重弱点】统计企业集团内所有项目中严重弱点的数量

【第三方库】统计企业集团内项目第三方库的数量

【CNNVD】统计项目中漏洞与 CNNVD 库中匹配的漏洞数量

【CVE】统计项目中漏洞与 CVE 库中匹配的漏洞数量

【安全弱点信息统计】按照严重性/OWASP TOP 10 对项目安全弱点进行统计的饼状图 【弱点项目检出量排行 Top5】对各个项目中弱点总数排名前 5 的统计

【项目风险值图】对项目风险等级进行评估的走势图（项目安全风险值= （严重漏洞书 \*严重漏洞权重+高危漏洞数\*高危漏洞权重+中危漏洞数\*中危漏权重+低危漏洞数\*低危 漏洞数） /行数系数

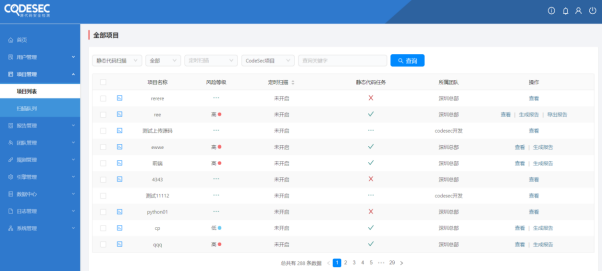
**4.2.4** 项目管理

<4.2.4.1> 项目列表

业务场景：查看所有项目中检测到的安全弱点信息， 查看漏洞，管理项目、查看项目 报告等。

操作路径：【项目管理】->【项目列表】

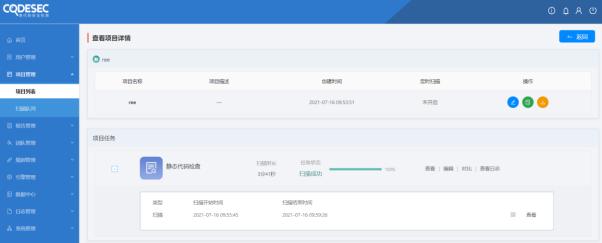
操作说明：通过以上操作路径进入到项目列表界面，企业管理员通过项目列表管理项 目、生成报告、导出报告，快速查询项目等，如下图：



项目管理

项目基本信息

点击项目列表中的【查看】按钮，可查看项目详情，包括项目基本信息，项目扫 描任务信息。如下图：



通过项目详情页对项目的信息进行【编辑】、【生成报告】、【导出报告】的操 作。

1、编辑项目

（1）基础信息修改



字段说明：

【项目名称】支持修改项目名称

【项目描述】支持修改项目描述

【文件过滤】支持修改需要过滤的源码文件名称，以“, ”隔开

【上传源码】支持修改上传的源码（支持 zip,rar 格式文件）

【仓库选择】支持修改仓库，仓库类型支持 GIT、SVN、TFS、Perforce、Mercurial； 手动输入仓库地址链接，可选择账号登录或 Token 登录；支持选择是否自动扫描，自 动扫描支持每天、每周、每月

【最长扫描时长】支持修改最长扫描时长

（2）静态代码修改



字段说明：

【项目任务类型】默认为“静态代码任务”，不可修改

【自动识别语言】可选择是否支持自动语言识别功能

【代码语言】可修改代码语言，包括 Java/JSP、C#/ASP.NET、PHP、C/C++、Python、 JavaScript、Object-C、swift、go

【渲染 DOM 数】支持选择是否渲染 DOM 树

【文件过滤】支持修改扫描过滤的文件，包括 javascript、css、png 等格式的文件 【扫描规则】支持修改后台预定义扫描的规则

【安全函数】支持修改过滤安全函数名，例如： main,test,print

【快速扫描】支持修改是否进行快速扫描功能

注：修改完成后系统将按照新的配置规则对静态代码执行扫描

2、生成报告

点击【生成报告】按钮，可生成静态代码扫描报告，生成报告的格式为系统默认 格式， 用户在使用该功能时，可根据需求选择和定义，如下图：



3、下载报告

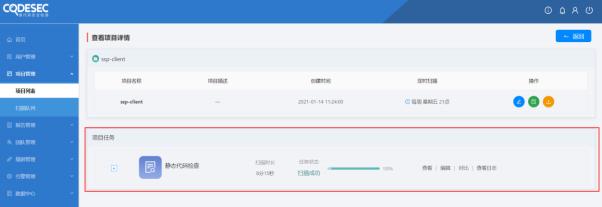
点击【下载报告】，页面跳转到生成报告列表页，列表页展示生成的历史报告， 如下图：



企业管理员可根据需要选择相应的报告，点击【下载报告】，可将报告下载到本 地。

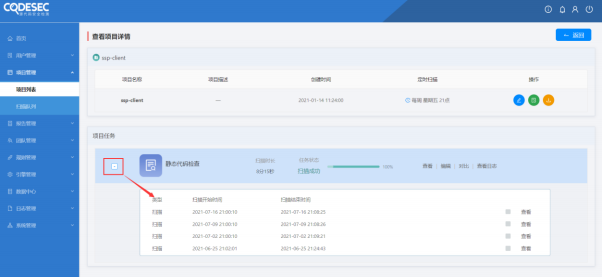
项目任务详情

项目任务显示静态代码检查情况，默认显示最近一次静态代码的检查情况，包括 最近一次代码检查的扫描时长，任务状态。通过项目任务栏可展开历史检查记录、查 看静态代码的检查结果、支持对检查任务的编辑、支持对扫描结果的对比和日志查看 等功能。



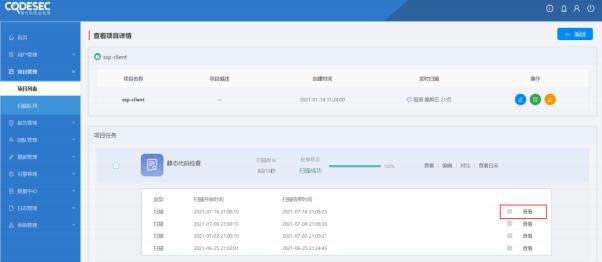
1、展开历史检查记录

点击【+】展开按钮可查看历史检查记录，如下图：



2、查看静态代码的检查结果

点击【查看】按钮可查看项目静态代码检查结果，如下图：



通过静态代码扫描结果页，可以查看项目扫描结果的【概览】、【漏洞列表】、

【漏洞详情】和【第三方组件】。





（1）【概览】：主要是对项目静态代码检查的统计。

项目概览统计： ①安全弱点、严重弱点和误报数进行统计； ②第三方库、 CVE、 CNNVD 漏洞库中对用的漏洞数的统计； ③最近一次扫描新发现的漏洞数统计，复发的 漏洞书统计，已修复的漏洞数统计； ④代码总行数的统计。如下图：



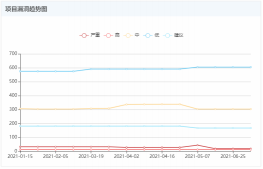
安全弱点信息统计图：按照严重性/OWASP TOP 10 对项目安全弱点进行统计，如 下图：



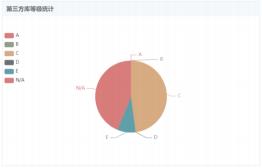
项目风险等级图：对项目风险等级进行评估（项目安全风险值= （严重漏洞书\*严 重漏洞权重+高危漏洞数\*高危漏洞权重+中危漏洞数\*中危漏权重+低危漏洞数\*低危漏 洞数） /行数系数，如下图所示：



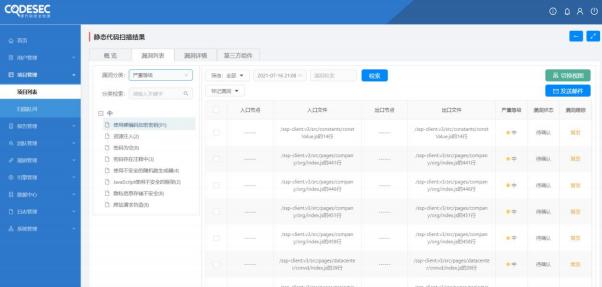
项目漏洞趋势图：按照时间维度，对每次代码项目各个等级漏洞检查的漏洞趋势 图，如下图：



第三方库等级统计：



（2） 【漏洞列表】是对系统检测出的漏洞进行汇总，如下图：



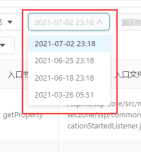
1）漏洞筛选：通过【漏洞列表】也可通过多个维度对漏洞进行查询，包括按照漏 洞分类、漏洞状态和时间维度对漏洞进行查询，如下图：



*漏洞分类*

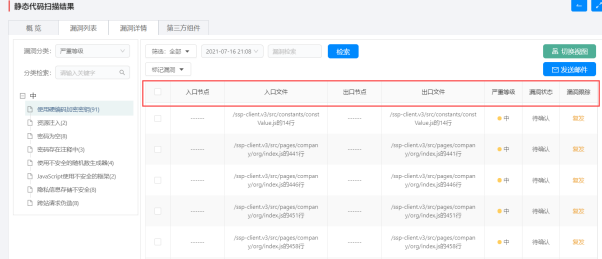


*漏洞状态*

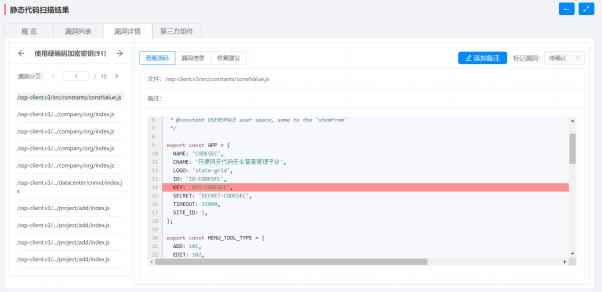


*时间维度*

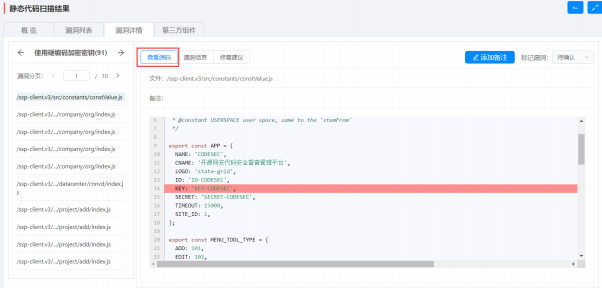
2）查看漏洞：通过【漏洞列表】查看漏洞信息，包括漏洞的入口节点、入口文 件、出口节点和出口文件、对应的严重等级、漏洞状态和漏洞跟踪。如下图：



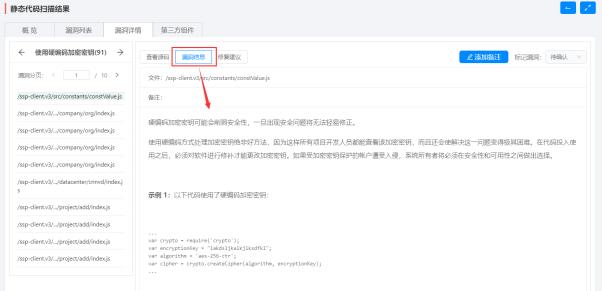
点击列表中对应的漏洞“入口文件”，即可查询漏洞信息。如下图：



通过【漏洞详情】，可分别查看漏洞入、出口节点，以及对应的源码，如下图：



通过【漏洞信息】，可查看对应的漏洞的概述，包括漏洞的概念及示例代码，如 下图：

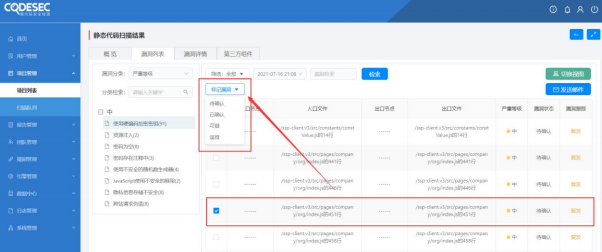


通过【修复建议】可查看对该漏洞的修复建议，如下图：



3）漏洞标记

企业管理员可在【漏洞列表】页勾选漏洞进行标记，标记的状态分为：待确认 （漏洞默认状态）、已确认、可疑和误报四种。如下图：



4）切换视图

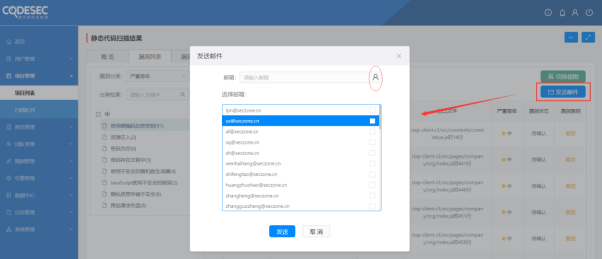


用户可在【漏洞列表】页勾选相应的漏洞执行切换视图的操作，可在列表和结构 图之间进行切换，如下图所示：



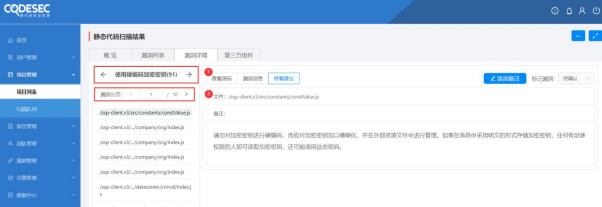
5）发送邮件

用户可在【漏洞列表】页勾选漏洞，可将漏洞通过邮件的方式发送给项目团队管 理员或项目成员等，如下图：



（3）漏洞详情

用户可通过【漏洞列表】点击漏洞对应的文件，直接跳转到漏洞详情页，也可以 通过点击【漏洞详情】查看漏洞详细信息。



可通过左上角标识为①、②的区域切换不同等级的漏洞和同级漏洞间的切换。关 于【查看源码】、【漏洞信息】和【修复建议】详细介绍见上文。

（4）第三方组件

通常情况下， 第三方组件都是开源的。 由于第三方组件不是由本项目开发者编写的 组件或者应用。第三方组件的作者遵循行业内的一些协议， 允许其他软件开发者自由使 用这些组件。但这些组件安全性未知， 通过 CodeSec 源代码安全扫描平台源代码扫描服 务，可以检测到潜在的威胁。 如下图：

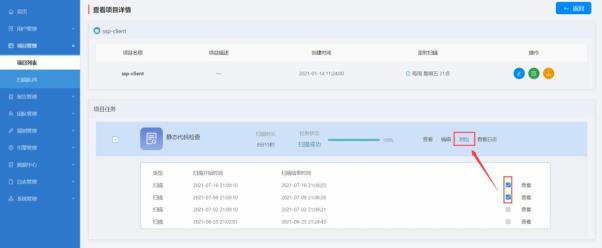


点击列表中的【查看】按钮，可查看第三方组件的扫描详情，如下图：



3、扫描结果对比

在项目详情页，勾选需要对比的扫描结果，如下图：

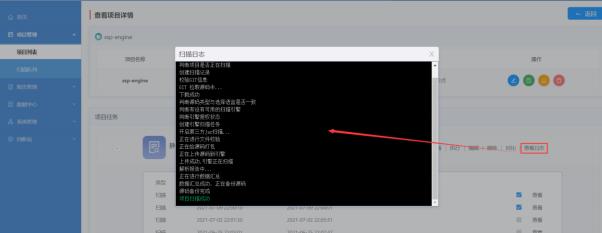


点击【对比】按钮， 系统将两次扫描的结果进行对比分析， 用户可以通过对比扫描 的结果对项目的安全性、项目团队绩效等多个维度进行分析。如下图：



4、查看日志：

通过项目详情页的【查看日志】按钮，可调出源代码扫描日志，如下图：



生成报告

点击【生成报告】按钮，可生成静态代码扫描报告，生成报告的格式为系统默认 格式， 用户在使用该功能时，可根据需求选择和定义，如下图：



导出报告

点击项目列表中【导出报告】按钮，页面跳转到生成报告列表，列表展示生成的 历史报告，如下图：



用户可根据需要下载不同时间、规则等生成的报告，点击【下载报告】，可将报 告下载到本地。

项目查询

在项目列表页面支持通过多维度对项目进行查询，包括：项目扫描状态、定时扫 描、同时也支持关键字查询，如下图：



<4.2.4.2> 扫描队列

业务场景：查看当前正在扫扫描的队列

操作路径：【项目管理】 ->【扫描队列】

操作说明： 用户通过以上操作路径可以查看正在等待扫描的队列。 当服务器并发量达 到上限时，静态代码扫描任务将在扫描队列呈现，在此页面显示正在等待扫描的队

列，如下图：



**4.2.5** 团队管理

<4.2.5.1> 团队列表

业务场景：管理团队及团队成员信息

操作路径：【团队管理】->【团队列表】

操作说明：通过以上操作路径可查看团队列表，在【团队列表】可执行的操作包括： 新建团队、查询、编辑、成员管理、删除、批量删除。

新建团队

在项目团队页面，点击【新建团队】， 完善以下项目团队信息，即可完成团队的 创建。 如下如：



字段说明：

【父级团队】默认为项目创建时公司的名称，必选项

【团队名称】由企业管理员手动输入，必填项

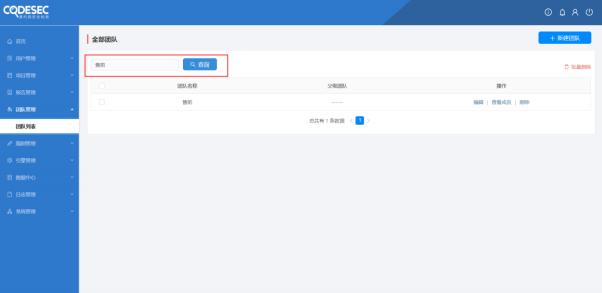
以上信息填写完成后，点击【新建】完成项目团队的创建，点击【取消】当前对 话窗口关闭。

列表概述

通过团队列表可查看所有团队信息和团队相对应的父级团队，可对各个团队进行 查询、查看成员和删除的操作。

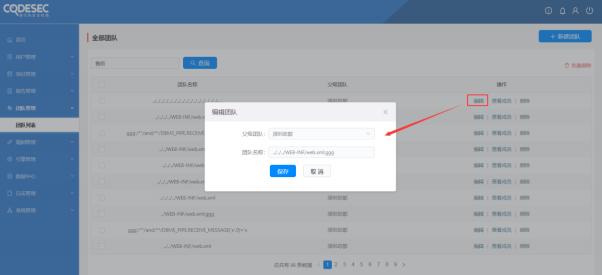
查询团队

在搜索输入框输出团队名称可快速查询到相应的团队，如下图：



编辑团队

点击【编辑】按钮，可执行对团队信息的编辑，如下图：



查看成员

点击【查看成员】按钮，可查看团队成员信息；也可执行【添加成员】的操作对 团队成员信息进行维护，如下图：



字段说明：

【选择成员】企业管理员选择成员，选择成员的选择框模糊搜索功能

【选择角色】支持选择普通用户或团队管理员

完成以上操作，完成项目团队成员的分配，包括普通用户和团队管理员。

删除团队

点击团队列表【删除】按钮，可执行对项目团队删除的操作，如下图：



批量删除

勾选需要批量删除的团队，点击【批量删除】，可执行对项目团队批量删除的操 作，如下图：



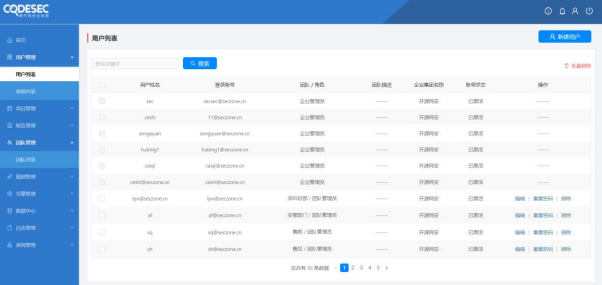
**4.2.6** 用户管理

<4.2.6.1> 用户列表

业务场景：管理用户信息

操作路径：【用户管理】->【用户列表】

操作说明：通过以上操作路径进入到用户列表界面，企业管理员可通过【用户列表】 执行的操作包括：新建用户、查询、编辑、重置密码、删除和批量删除操作，如下 图：



新建用户

1、在用户列表页面，点击【新建团队】，如下如：



字段说明

【选择企业集团】默认为企业集团名称，不可修改

【选择团队】企业管理员可从创建的团队列表中为用户选择团队

【用户姓名】企业管理员手动输入用户真实姓名，可重名

【登录账号】使用邮箱账号登录平台，企业管理员手动输入

【登录密码】手动输入登录密码，密码必须由 8-20 位字母数字特殊字符组成 【确认密码】登录密码和确认密码需保持一致

【手机账号】系统支持手机号登录，手动输入

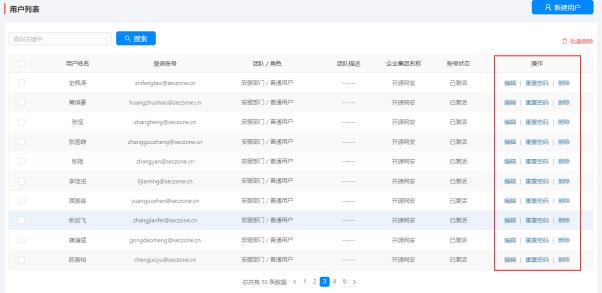
【角色分配】手动选择用户角色，包含团队管理员、普通用户和审计员，必填项 【有效期】需设置账户的有效期，手动选择

【账号状态】创建账号时可选择账号激活或禁用状态，被禁用的账号没有系统登录权 限

以上信息填写完成后，点击【新建】完成用户的创建，点击【取消】当前对话窗 口关闭。

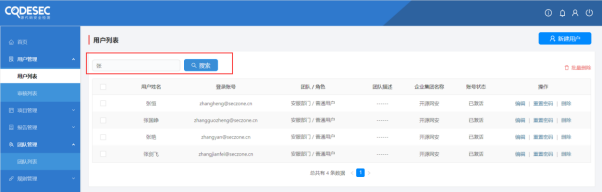
列表概述

通过用户列表可查看所有用户信息，可对各个用户进行编辑、重置密码和删除的 操作。



查询用户

在查询输入框输入要查询的用户信息，支持用户姓名、登录账号的模糊查询，可 快速查询到对应的用户。



编辑用户

点击【编辑】按钮，可执行对用户信息的编辑，如下图：



字段说明：

【选择企业集团】默认为企业集团名称，不可编辑

【用户姓名】支持手动修改

【登录账号】默认为初始登录账号，不可修改

【手机账号】支持修改手机账号

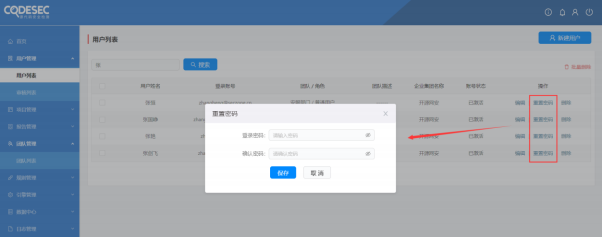
【有效期】支持手动修改账号有效期

【账号状态】支持修改账号启用/禁用状态

完成修改对应的字段，点击【保存】，用户信息修改成功。

重置密码

在用户列表界面点击【重置密码】可对用户密码进行重置，如下图：



注：密码必须由 8-20 位字母数字特殊字符组成

删除用户

点击团队列表【删除】按钮，可执行对用户删除的操作，如下图：



批量删除

勾选需要批量删除的用户，点击【批量删除】，可执行对用户批量删除的操作， 如下图：



<4.2.5.2> 审核列表

业务场景：审核用户权限

操作路径：【用户管理】->【审核列表】

操作说明：通过以上操作路径进入到审核列表界面，企业管理员可通过【审核列表】 执行的操作包括： 通过、批量通过、拒绝和批量拒绝，如下图：



**4.2.7** 报告管理

<4.2.7.1> 模板配置

业务场景：配置报告模板

操作路径：【报告管理】->【模板配置】

操作说明：通过以上操作路径进入到用模板配置界面，企业管理员可通过【模板配 置】页面实现新建报告模板、编辑、删除和批量删除模板的操作，如下图：



新建配置

在用户列表页面，点击【新建配置】， 进行模板的配置， 如下图：



字段说明：

【模板名称】企业管理员可自定义模板名称

【报告标题】企业管理员手动输入报告标题

【版本类型后缀】开启版本类型后缀后下载报告名称将会附带版本类型后缀 【左页眉】定义报告的左页眉

【右页眉】定义报告的右页眉

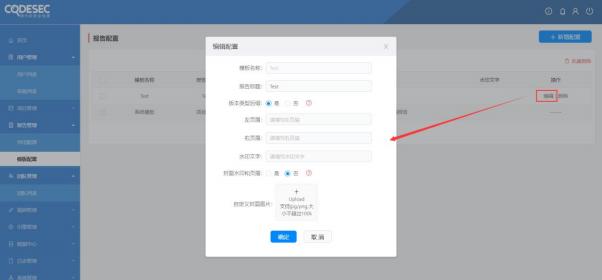
【水印文字】支持手动输入水印文字

【封面水印】支持是否显示封面水印，开启后 PDF 类型将会生成封面水印 【自定义封面图片】支持上传 jpg/png 格式的文件，大小不超过 100k

以上信息填写完成后，点击【创建】生成模板配置的创建，点击【取消】当前对 话窗口关闭。

编辑配置

点击【编辑】按钮，可执行对模板配置进行编辑，如下图：



删除配置

点击模板列表【删除】按钮，可执行对模板删除的操作，如下图：



批量删除

勾选需要批量删除的模板，点击【批量删除】，可执行对模板批量删除的操作， 如下图：



<4.2.6.2> 导出配置

业务场景：导出报告配置

操作路径：【报告管理】->【导出配置】

操作说明：通过以上操作路径进入到用模板配置界面，企业管理员可通过【导出配

置】页面实现生成/导出报告的格式。支持新建、查看、编辑、删除和批量删除导出设 置模板的操作，如下图：



新建配置

在用户列表页面，点击【新建配置】， 进行报告导出模板的配置， 如下图：



字段说明：

【配置名称】支持企业管理员手动输入

【选择报告类型】支持报告导出格式的选择，可选择 PDF、Word 和 XML 格式的报告 【选择报告模块】支持选择 <3.1.6.1> 配置的报告模板

【选择漏洞分类】支持选择漏洞分类，可选择 OWASP2017、PCI3.2.1、 SANSTop252011、CodeSec2020、GB/T39412

【选择内容模块】 默认可选择为静态任务漏洞

【选择漏洞级别】支持筛选漏洞级别，包括：严重、高、中、低、建议

【选择漏洞状态】支持筛选漏洞状态，包括待确定、已确定、可疑和误报 【代码片段】可选择是否导出漏洞代码的片段

【对比结果】可选择是否与最近一次扫描结果进行对比

【版本类型】系统提供专业版和精简版报告格式的选择

以上信息填写完成后，点击【确定】生成导出报告模板配置的创建，点击【取 消】当前对话窗口关闭。

查看配置

点击【查看】按钮，可查询报告配置详情，如下图：



编辑配置

点击【编辑】按钮，可执行对模板配置进行编辑，如下图：



注：弹窗内的所有字段对应的内容均可修改， 一旦修改，导出的报告将按照修改 后的配置生成报告。

删除配置

点击模板列表【删除】按钮，可执行对导出配置删除的操作，如下图：



批量删除

勾选需要批量删除的导出配置，点击【批量删除】，可执行对导出配置批量删除 的操作，如下图：



**4.2.8** 规则管理

<4.2.8.1> 漏洞规则配置

业务场景：针对不同语言漏洞规则的配置

操作路径：【规则管理】->【漏洞规则配置】

操作说明：通过以上操作路径进入到用漏洞规则配置界面， 用户可通过【漏洞规则配 置】页面实现对多种开发语言实现漏洞规则的配置，支持对各类语言不同级别漏洞的 配置操作，支持通过漏洞名称快速查询，如下图：



支持多种语言不同等级的漏洞的配置， 支持的语言包括： Java/Jsp、C#/ASP.NET、 PHP、C/C++、Python、Javascript、Objective-C、html、swift、go。漏洞等级分为严 重、高、中、低和建议五种。

注：企业管理员没有新增或删除漏洞类型的权限，只能对漏洞类型进行编辑。

漏洞规则编辑

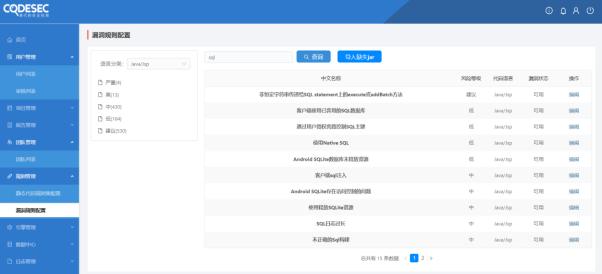
系统支持漏洞规则的编辑操作，编辑页面支持通过中英文对漏洞的定义和概念的 描述，和中英文的修复建议。如下图：





漏洞名称查询

在查询输入框输入要查询的漏洞类型名称，可快速查询到对应的漏洞类型。



<4.2.8.2> 静态代码规则集配置

业务场景：配置静态代码扫描规则集

操作路径：【规则管理】->【静态代码规则集配置】

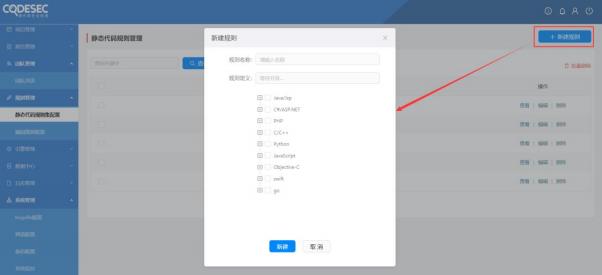
操作说明：通过以上操作路径进入到静态代码规则集配置界面，用户可通过【静态代 码规则集配置】页面配置多种静态代码扫描规则，系统支持静态代码扫描规则的新

建、查看、编辑、删除和批量删除的操作。如下图：



新建规则

在静态代码规则管理列表页面， 点击【新建规则】，进行静态代码扫描规则的配置， 如下图：



静态代码规则的定义，可以根据项目的不同需求，不同性质，使用的语言和关注 点对规则进行定义选择，系统定义了多种语言对应不同等级的漏洞类型供企业管理员

选择配置。

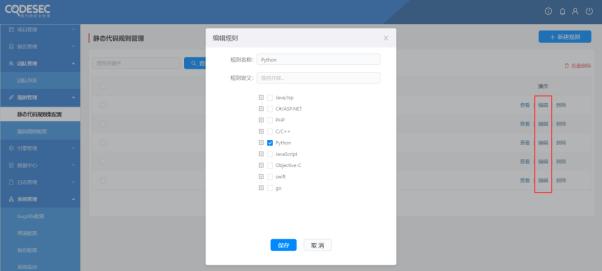
查看规则

点击【查看】按钮，可查看静态代码规则配置详情，如下图：



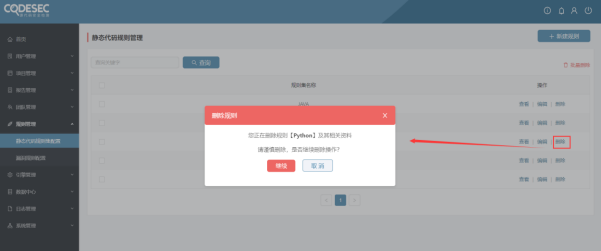
编辑规则

点击【编辑】按钮，可执行对模板配置进行编辑，如下图：



删除规则

点击模板列表【删除】按钮，可执行对静态代码规则删除的操作，如下图：



批量删除

勾选需要批量删除的静态代码规则集，点击【批量删除】，可执行对静态代码规 则删除的操作，如下图：



**4.2.9** 引擎管理

<4.2.9.1> 新增引擎

业务场景：添加企业内其他服务器部署的引擎

操作路径：【引擎管理】->【引擎列表】 ->【新增引擎】

操作说明：通过以上操作路径，输入服务器 IP 和端口选择引擎的状态以及可以使用引 擎类型，完成企业内部服务器部署引擎的添加。如下图：



<4.2.9.2> 引擎列表

业务场景：查看、管理企业内部其他服务器引擎部署

操作路径：【引擎管理】->【引擎列表】

操作说明：通过以上操作路径，进入到引擎列表界面，通过引擎列表可对引擎进行认 证、编辑、删除和批量删除以及新增（详见 <3.1.9.1>）的操作。如下图：



引擎认证

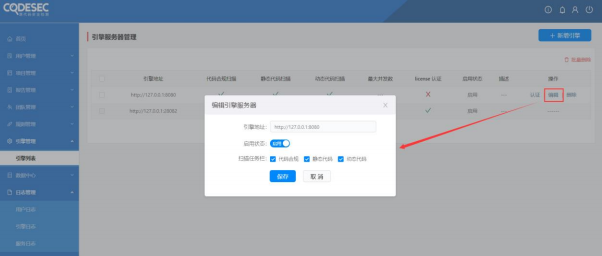
需要对服务器引擎进行认证，将机器码发送给 CodeSec 工作人员生成许可，进行 认证。





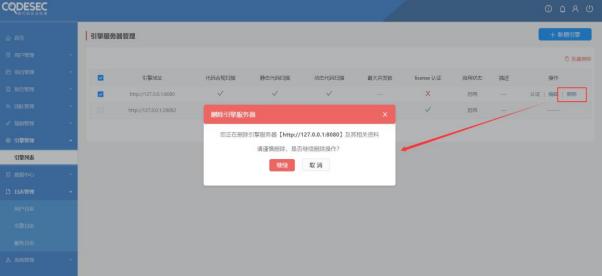
编辑引擎

点击【编辑】按钮可对引擎服务器进行编辑，如下图：



引擎删除

点击列表【删除】按钮，可执行对引擎服务器删除的操作，如下图：



批量删除

勾选需要批量删除的引擎服务器，点击【批量删除】，可执行对引擎服务器删除 的操作，如下图：



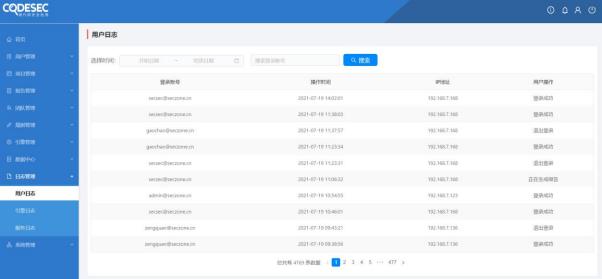
**4.2.10** 日志管理

<4.2.10.1> 用户日志

业务场景： 查看用户操作日志

操作路径：【日志管理】->【用户日志】

操作说明： 通过以上操作路径可以查看系统登录账号、操作时间、 IP 地址以及对应 的用户操作，便于对系统操作溯源，如下图 ;



<4.2.10.2> 引擎日志

业务场景： 查看引擎运行日志

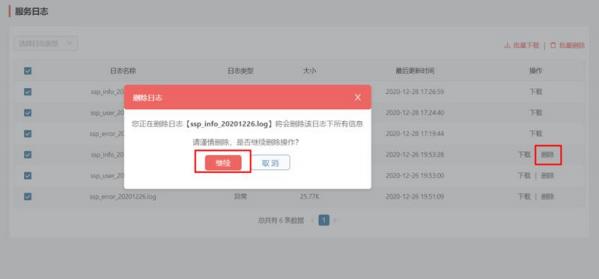
操作路径：【日志管理】->【引擎日志】

操作说明： 通过以上操作路径可以查看引擎日志，包括日志名称、地址、日志类型、 文件大小、最后更新时间，可对引擎日志执行下载、批量下载、删除和批量删除的操 作，如下图：

引擎日志下载：



引擎日志删除：



批量删除



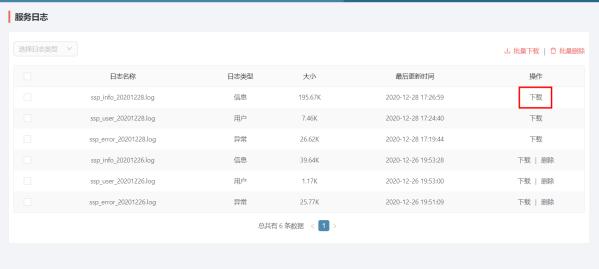
<4.2.10.3> 服务日志

业务场景： 查看服务日志

操作路径：【日志管理】->【服务日志】

操作说明： 通过以上操作路径可以查看服务日志，包括日志名称、日志类型、文件大 小、最后更新时间，可对服务日志执行下载、批量下载、删除和批量删除的操作，如 下图;

日志下载



批量下载



删除日志



批量删除



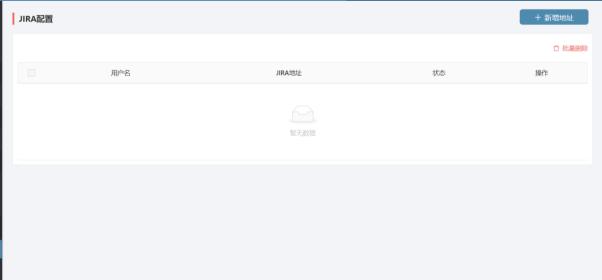
**4.2.11** 系统管理

<4.2.11.1> JIRA 配置

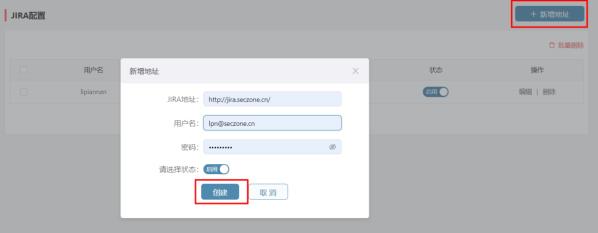
业务场景：管理 Bug 管理器

操作路径：【系统配置】->【JIRA 配置】

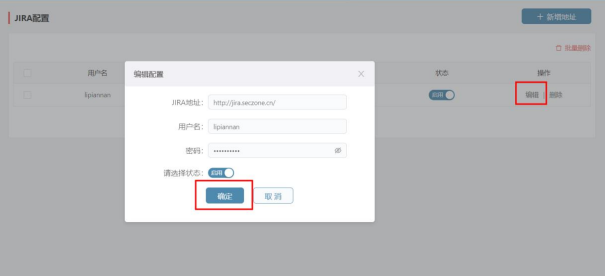
操作说明：通过系统配置支持添加 Bug 管理器（JIRA），系统支持编辑、删除和批量 删除，如下所述：



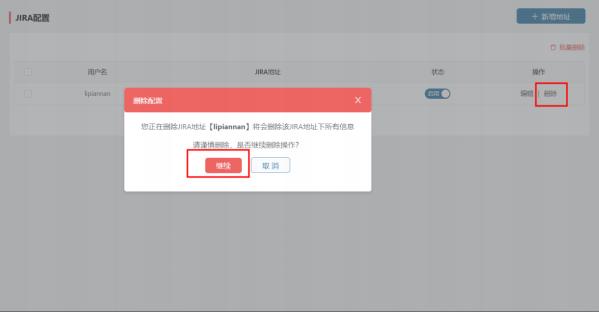
点击【新增地址】按钮，输入 JIRA 地址和账号密码并开启 JIRA 状态，点击创建；



点击【编辑】按钮，可以修改 JIRA 的地址和账号密码及状态；



点击【删除】按钮，删除 JIRA 的配置



勾选需要删除 JIRA 配置，点击【批量删除】按钮，删除对应 JIRA 的配置

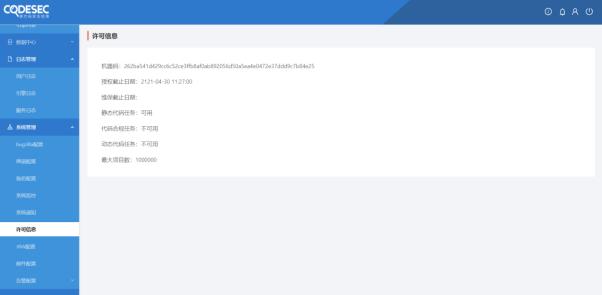


<3.1.11.2> 许可信息

业务场景：查看许可信息

操作路径：【系统配置】->【许可信息】

操作说明：通过以上操作路径可查看项目的许可信息，如下图：

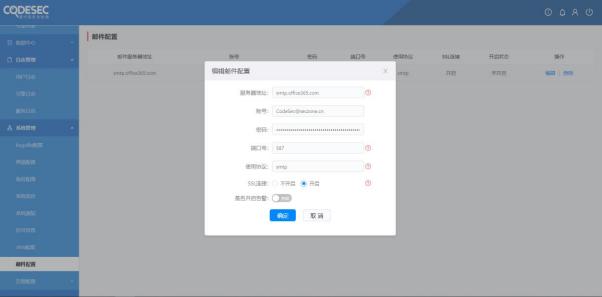


<3.1.11.3> 邮件管理

业务场景：查看许可信息

操作路径：【系统配置】->【许可信息】

操作说明：通过以上操作路径可增加邮件配置功能， 配置的邮箱默认为系统发送邮件 的默认邮箱。

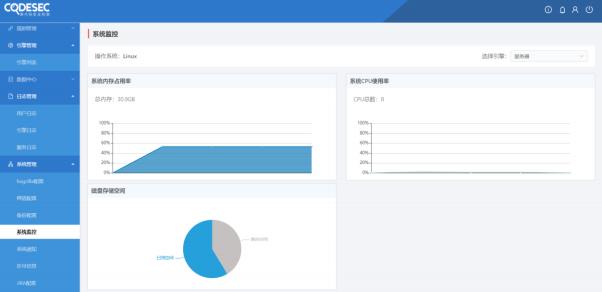


<3.1.11.4> 系统监控

业务场景：查看硬件系统运行情况

操作路径：【系统配置】->【系统监控】

操作说明：通过以上操作路径可查看服务器内存使用率、 CPU 使用率及磁盘使用情 况，如下图：



4.3 审计员操作手册

**4.3.1** 系统登录

业务场景：用户登录系统

操作路径：【输入 URL】->【输入用户名/密码】

操作说明：

1、在浏览器中输入 URL：http://ip:port 即可打开开源网安 CodeSec 平台 登录界面，其中 IP 是指扫描工具的服务器 IP 地址， PORT 是指端口(端口默认

是 28081)。使用分配的用户名及密码，即可登录。 如下图：



注意：建议使用推荐的浏览器；

**4.3.2** 首页

业务场景：查看系统仪表盘

操作路径：【登录系统】->【系统首页】

操作说明：通过【首页】查看系统仪表盘，如下图：





字段说明：

【团队数量】统计企业集团内项目团队的数量

【项目数量】统计企业集团内的项目数量

【安全弱点】统计企业集团内所有项目的安全弱点数量

【严重弱点】统计企业集团内所有项目中严重弱点的数量

【第三方库】统计企业集团内项目第三方库的数量

【CNNVD】统计项目中漏洞与 CNNVD 库中匹配的漏洞数量

【CVE】统计项目中漏洞与 CVE 库中匹配的漏洞数量

【安全弱点信息统计】按照严重性/OWASP TOP 10 对项目安全弱点进行统计的

饼状图

【弱点项目检出量排行 Top5】对各个项目中弱点总数排名前 5 的统计

【项目风险值图】对项目风险等级进行评估的走势图（项目安全风险值= （严重 漏洞书\*严重漏洞权重+高危漏洞数\*高危漏洞权重+中危漏洞数\*中危漏权重+低

危漏洞数\*低危漏洞数） /行数系数

**4.3.2** 项目管理

<4.3.2.1> 项目列表

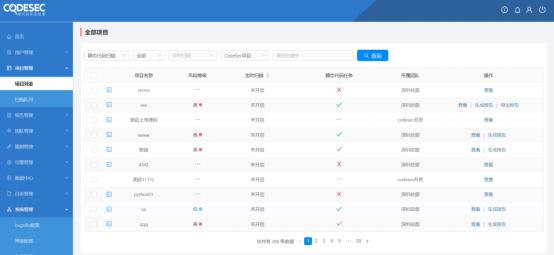
业务场景：查看所有项目中检测到的安全弱点信息， 查看漏洞，管理项目、查

看项目报告等。

操作路径：【项目管理】->【项目列表】

操作说明：通过以上操作路径进入到项目列表界面， 用户通过项目列表管理项

目、生成报告、导出报告，快速查询项目等，如下图：



字段说明：

【项目名称】由项目团队创建项目时自定义

【风险等级】分为高、中、低等

【定时扫描】分为自动扫描和手动扫描，状态对应开启/未开启

【静态代码】静态代码任务分为“× ”和“ √ ”,分别对应扫描失败/成功

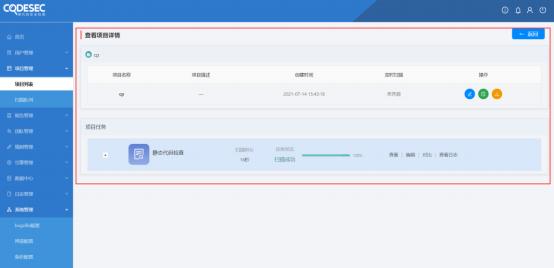
【所属团队】项目对应的所属团队

项目管理

项目基本信息

点击项目列表中的【查看】按钮，可查看项目详情，包括项目基本信息，

项目扫描信息。



通过项目详情页可对项目的信息进行【编辑】、【生成报告】、【导出报

告】的操作。

1、编辑项目

（1）基础信息修改



字段说明：

【项目名称】支持修改项目名称

【项目描述】支持修改项目描述

【文件过滤】支持修改需要过滤的源码文件名称，以“, ”隔开

【上传源码】支持修改上传的源码（支持 zip,rar 格式文件）

【仓库选择】支持修改仓库，仓库类型支持 GIT、SVN、TFS、Perforce、

Mercurial；手动输入仓库地址链接，可选择账号登录或 Token 登录；支持选择

是否自动扫描，自动扫描支持每天、每周、每月

【最长扫描时长】选择扫描对象为仓库时，支持修改最长扫描时长

（2）静态代码修改



字段说明：

【项目任务类型】默认为“静态代码任务”，不可修改

【自动识别语言】可选择是否支持自动语言识别功能

【代码语言】可修改代码语言，包括 Java/JSP、C#/ASP.NET、PHP、C/C++、

Python、JavaScript、Object-C、swift、go

【渲染 DOM 数】支持选择是否渲染 DOM 树

【文件过滤】支持修改扫描过滤的文件，包括 javascript、css、png 等格式的

文件

【扫描规则】支持修改后台预定义扫描的规则，规则管理详见 3.1.7

【安全函数】支持修改过滤安全函数名，例如： main,test,print

【快速扫描】支持修改是否进行快速扫描功能

注：修改完成后系统将按照新的配置规则对静态代码执行扫描

4、生成报告

点击【生成报告】按钮，可生成静态代码扫描报告，生成报告的格式为系

统默认格式，审计员在使用该功能时，可根据需求选择和定义，如下图：





5、下载报告

点击【下载报告】，页面跳转到生成报告列表页，列表页展示生成的历史

报告，如下图：



审计人员可根据需要选择相应的报告，点击【下载报告】，可将报告下载

到本地，报告示例如下图：



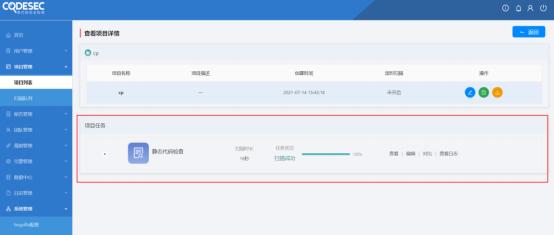
注：仅截取报告的部分内容。

项目任务详情

项目任务显示静态代码检查情况，默认显示最近一次静态代码的检查情

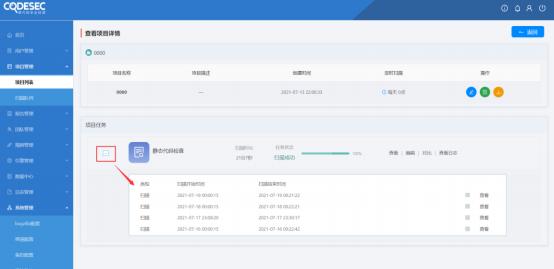
况，包括最近一次代码检查的扫描时长，任务状态。通过项目任务栏可展开历 史检查记录、查看静态代码的检查结果、支持对检查任务的编辑、支持对多次

扫描结果的对比和查看日志等功能。



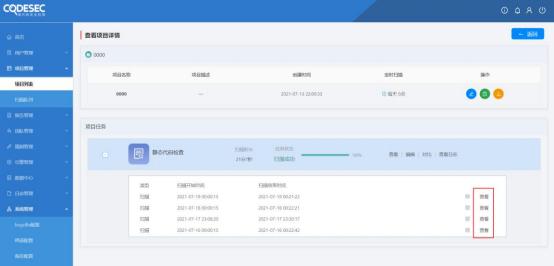
1、展开历史检查记录

点击【+】展开按钮可查看历史检查记录，如下图：



2、查看静态代码的检查结果

点击【查看】按钮可查看项目静态代码检查结果，如下图：



通过静态代码扫描结果页，可以查看项目扫描结果的【概览】、【漏洞列

表】、【漏洞详情】和【第三方组件】。



（1）【概览】：主要是对项目静态代码检查的统计。

项目概览统计： ①安全弱点、严重弱点和误报数进行统计； ②第三方库、 CVE、CNNVD 漏洞库中对用的漏洞数的统计； ③最近一次扫描新发现的漏洞数统

计，复发的漏洞书统计，已修复的漏洞数统计； ④代码总行数的统计。如下

图：





安全弱点信息统计图：按照严重性/OWASP TOP 10 对项目安全弱点进行统

计，如下图：



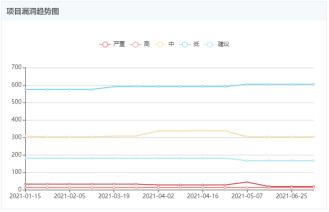
项目风险等级图：对项目风险等级进行评估（项目安全风险值= （严重漏洞 书\*严重漏洞权重+高危漏洞数\*高危漏洞权重+中危漏洞数\*中危漏权重+低危漏

洞数\*低危漏洞数） /行数系数，如下图所示：

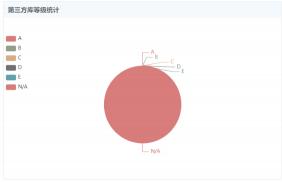


项目漏洞趋势图：按照时间维度，对每次代码项目各个等级漏洞检查的漏

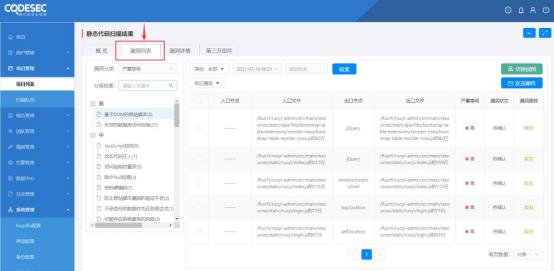
洞趋势图，如下图：



第三方库等级统计：



（2） 【漏洞列表】是对系统检测出的漏洞进行汇总，如下图：



1）漏洞筛选：通过【漏洞列表】也可通过多个维度对漏洞进行查询，包括

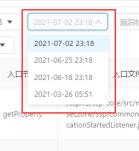
按照漏洞分类、漏洞状态和时间维度对漏洞进行查询，如下图：



*漏洞分类*



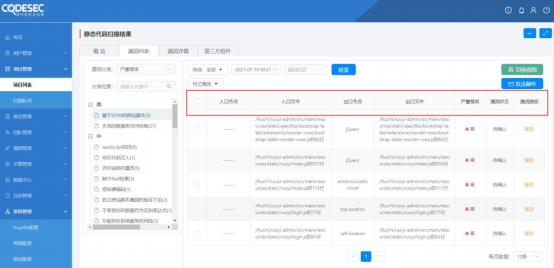
*漏洞状态*



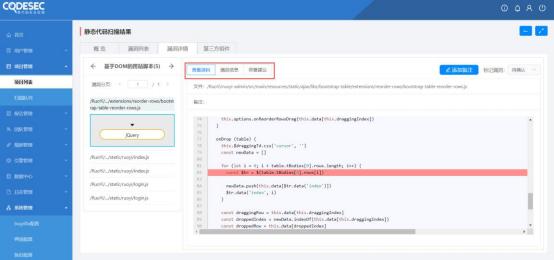
*时间维度*

2）查看漏洞：通过【漏洞列表】查看漏洞信息，包括漏洞的入口节点、入 口文件、出口节点和出口文件、对应的严重等级、漏洞状态和漏洞跟踪。如下

图：



点击列表中对应的漏洞【入口文件】，即可查询漏洞信息。如下图：



通过【漏洞详情】，可分别查看漏洞入、出口节点，以及对应的源码，如

下图：



通过【漏洞信息】，可查看对应的漏洞的概述，包括漏洞的概念及示例代

码，如下图：



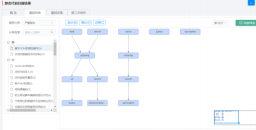
通过【修复建议】可查看对该漏洞的修复建议，如下图：

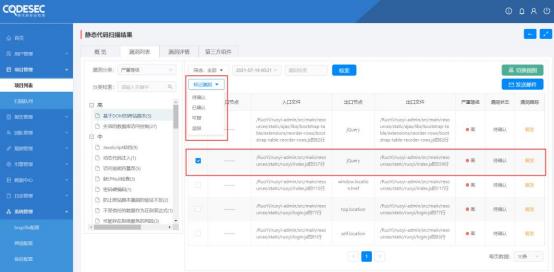


3）漏洞标记

审计员可在【漏洞列表】页勾选相应的漏洞进行标记，标记的状态分为：

待确认（漏洞默认状态）、已确认、可疑和误报四种。如下图：

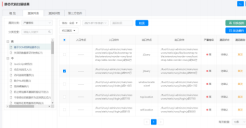




4）切换视图

审计员可在【漏洞列表】页勾选相应的漏洞执行切换视图的操作，可在列

表和结构图之间进行切换，如下图所示：



5）发送邮件

审计员可在【漏洞列表】页勾选相应的漏洞，可将漏洞通过邮件的方式发

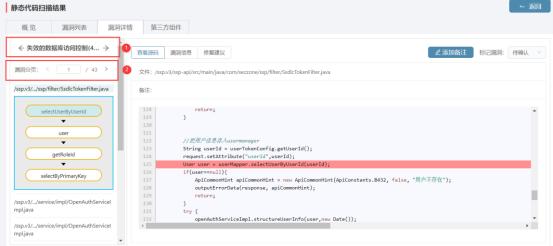
送给项目团队管理员或项目成员等，如下图：



（3）漏洞详情

审计员可通过【漏洞列表】点击漏洞对应的文件，直接跳转到漏洞详情

页，也可以通过点击【漏洞详情】查看漏洞详细信息。



可通过左上角标识为①、②的区域切换不同等级的漏洞和漏洞间的切换。

关于【查看源码】、【漏洞信息】和【修复建议】详细介绍见上文。

（4）第三方组件

通常情况下， 第三方组件都是开源的。 由于第三方组件不是由本项目开发者 编写的组件或者应用。第三方组件的作者遵循行业内的一些协议， 允许其他软件 开发者自由使用这些组件。但这些组件安全性未知， 通过 CodeSec 源代码安全扫

描平台源代码扫描服务，可以检测到潜在的威胁。 如下图：

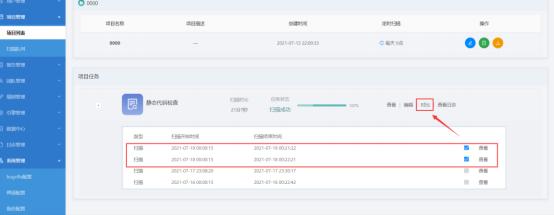


点击列表中的【查看】按钮，可查看第三方组件的扫描详情，如下图：



3、扫描结果对比

在项目详情页，勾选需要对比的扫描结果，如下图：



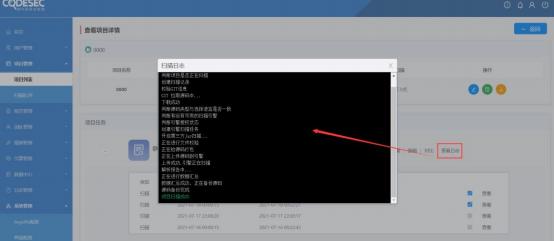
点击【对比】按钮， 系统将两次扫描的结果进行对比分析， 用户可以通过对

比扫描的结果对项目的安全性、项目团队绩效等多个维度进行审计分析。如下图：



4、查看日志：

通过项目详情页的【查看日志】按钮，可调出源代码扫描日志，如下图：



生成报告

点击【生成报告】按钮，可生成静态代码扫描报告，生成报告的格式为系

统默认格式，审计员在使用该功能时，可根据需求选择和定义，如下图：



导出报告

点击项目列表中【导出报告】按钮，页面跳转到生成报告列表页，列表页

展示生成的历史报告，如下图：





审计人员可根据需要下载不同时间、规则等生成的报告，点击【下载报

告】，可将报告下载到本地，报告示例如下图：





注：仅截取报告的部分内容。

项目查询

在项目列表页面支持通过多维度对项目进行查询，包括：项目扫描状态、

定时扫描、同时也支持关键字查询，如下图：



<4.3.2.2> 扫描队列

业务场景：查看当前正在扫扫描的队列

操作路径：【项目管理】 ->【扫描队列】

操作说明： 当服务器并发量达到上限时，静态代码扫描任务将在扫描队列呈

现，在此页面显示排队状态，如下图：



**4.3.3** 数据中心

<3.3.3.1> 项目数据汇总

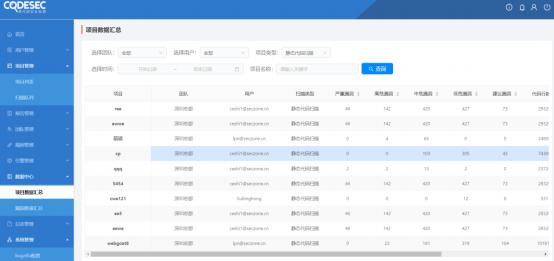
业务场景：查看项目数据汇总，查看各个项目的所属团队、创建人员，以及各

个项目漏洞情况。对各个项目和团队以及代码的安全性进行统计分析。

操作路径：【数据中心】 ->【项目数据汇总】

操作说明： 通过以上操作路径进入到【项目数据汇总】页面，可查看各个项目

所对应的团队、用户和各类型漏洞统计，支持多维度数据查询，如下图：



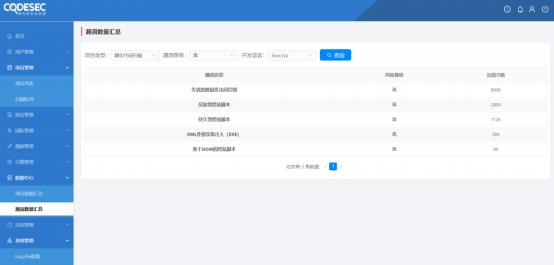
<3.3.3.2> 漏洞数量汇总

业务场景：基于企业维度查询各个漏洞级别和相应开发语言下各类漏洞的数量

统计

操作路径：【数据中心】 ->【漏洞数量汇总】

操作说明： 通过以上操作路径进入到【漏洞汇总】页面，如下图：



支持按照漏洞级别、开发语言维度查询各类漏洞的数量统计。

4.4 团队管理员操作手册

**4.4.1** 系统登录

业务场景：用户登录系统

操作路径：【输入 URL】->【输入用户名/密码】

操作说明：

1、在浏览器中输入 URL：http://ip:port 即可打开开源网安 CodeSec 平台 登录界面，其中 IP 是指扫描工具的服务器 IP 地址， PORT 是指端口(端口默认 是 28081)。使用开源网安代码审核平台服务商提供的团队管理员的用户名及密

码登录。 如下图：



注意：建议使用推荐的浏览器；

**4.4.2** 用户列表

业务场景：管理团队用户信息

操作路径：【用户管理】->【用户列表】

操作说明：通过以上操作路径进入到用户列表界面，团队管理员可通过【用户 列表】执行的操作包括：新建用户、查询、编辑、重置密码、删除和批量删除

操作，如下图：



新建用户

1、在用户列表页面，点击【新建团队】，如下如：



字段说明

【选择企业集团】默认为企业集团名称，不可修改

【选择团队】可从创建的团队列表中为用户选择团队

【用户姓名】手动输入用户真实姓名，可重名

【登录账号】使用邮箱账号登录平台，手动输入

【登录密码】手动输入登录密码，密码必须由 8-20 位字母数字特殊字符组成

【确认密码】登录密码和确认密码需保持一致

【手机账号】系统支持手机号登录，手动输入

【角色分配】手动选择用户角色，包含团队管理员或者普通用户，必填项

【有效期】需设置账户的有效期，手动选择

【账号状态】创建账号时可选择账号激活或禁用状态，被禁用的账号没有系统

登录权限

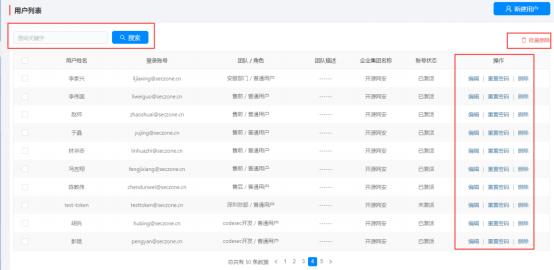
以上信息填写完成后，点击【新建】完成用户的创建，点击【取消】当前

对话窗口关闭。

列表概述

通过用户列表可查看所有用户信息，可对各个用户进行编辑、重置密码和

删除的操作。



查询用户

在查询输入框输入要查询的用户信息，支持用户姓名、登录账号的模糊查

询，可快速查询到对应的用户。



编辑用户

点击【编辑】按钮，可执行对用户信息的编辑，如下图：



字段说明：

【选择企业集团】默认为企业集团名称，不可编辑

【用户姓名】支持手动修改

【登录账号】默认为初始登录账号，不可修改

【手机账号】支持修改手机账号

【有效期】支持手动修改账号有效期

【账号状态】支持修改账号启用/禁用状态

完成修改对应的字段，点击【保存】，用户信息修改成功。

重置密码

在用户列表界面点击【重置密码】可对用户密码进行重置，如下图：



注：密码必须由 8-20 位字母数字特殊字符组成

删除用户

点击团队列表【删除】按钮，可执行对用户删除的操作，如下图：



批量删除

勾选需要批量删除的用户，点击【批量删除】，可执行对用户批量删除的

操作，如下图：



**4.4.3** 团队管理

业务场景：维护团队基础信息及团队成员信息

操作路径：【团队管理】->【团队列表】

操作说明：通过以上操作路径可查看团队列表，在【团队列表】可执行的操作

包括：编辑团队信息、管理团队成员,如下图：



编辑团队

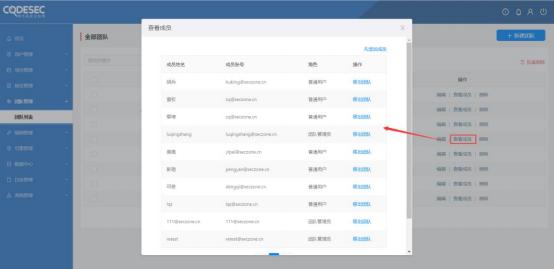
点击【编辑】按钮，可执行对团队名称进行编辑，如下图：

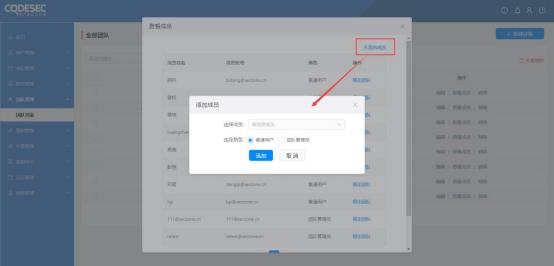


查看成员

点击【查看成员】按钮，可查看团队成员信息；也可执行【添加成员】的

操作对团队成员进行维护，如下图：





字段说明：

【选择成员】用户可选择团队成员，选择成员时支持模糊搜索功能

【选择角色】支持选择普通用户或团队管理员。

完成以上操作，完成项目团队成员的分配，包括普通用户和团队管理员。

**4.4.4** 项目管理

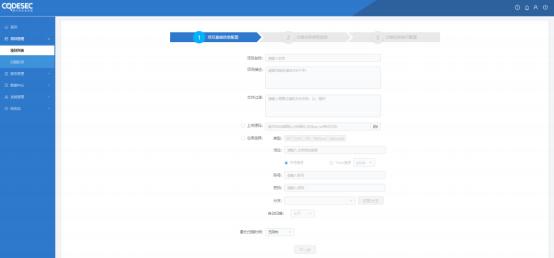
<4.4.4.1> 新建项目

业务场景：团队管理员新建静态代码检测项目

操作路径：【项目管理】->【项目列表】 ->【新建项目】

操作说明：

1、配置项目基础信息，如下图：



字段说明：

【项目名称】用户手工输入项目名称，必填项

【项目描述】用户手工输入项目描述

【文件过滤】用户手工输入需要过滤的源码文件名称，以“ , ”隔开

【上传源码】支持选择上传的源码（支持 zip,rar 格式文件）

【仓库选择】支持选择仓库，仓库类型支持 GIT、SVN、TFS、Perforce、

Mercurial；手动输入仓库地址链接，可选择账号登录或 Token 登录；支持选择

是否自动扫描，自动扫描支持每天、每周、每月

【最长扫描时长】支持设置项目最长扫描时长

以上信息填写完成后，点击【下一步】完成项目基础信息配置，进入扫描

任务类型选择页面。

注：如果未上传源码或者填写 Git/Svn 信息，下一步则不能创建静态代码

进行扫描。

2、选择扫描任务类型，如下图：



点击【下一步】，进入到扫描任务执行配置页面，也可点击【上一步】编

辑项目基础信息配置。

注：默认为静态代码任务

3、配置扫描任务执行，如下图：



字段说明：

【项目任务类型】默认为“静态代码任务”，不可修改

【自动识别语言】支持选择是否支持自动语言识别功能

【代码语言】支持多类型代码语言的选择，包括 Java/JSP、C#/ASP.NET、

PHP、C/C++、Python、JavaScript、Object-C、swift、go

【扫描二进制】支持选择是否扫描二进制

【JDK 版本选择】选择 JDK 版本，包括 JDK1.5、1.6、1.7、1.8、1.9、11

【文件过滤】支持选择扫描过滤的文件，包括 javascript、css、png 等格式的

文件

【扫描规则】支持选择后台预定义扫描的规则

【安全函数】自定义过滤安全函数名，例如： main,test,print

【快速扫描】支持选择是否进行快速扫描功能

以上信息配置完成，点击【创建】，项目创建成功；点击【创建并执行】， 项目创建成功并执行项目源码扫描； 点击【上一步】， 跳转到扫描任务类型选择

页面。

<4.4.4.2> 项目管理

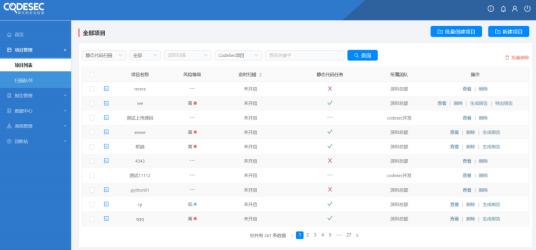
业务场景：查看所有项目中检测到的安全弱点信息，跟踪漏洞，管理项目、查

看项目报告等。

操作路径：【项目管理】->【项目列表】

操作说明：通过以上操作路径进入到项目列表界面， 团队管理员通过项目列表

管理项目、生成报告、导出报告，快速查询项目等，如下图：



字段说明：

【项目名称】由项目团队创建项目时自定义

【风险等级】分为高、中、低等

【定时扫描】分为自动扫描和手动扫描，状态对应开启/未开启

【静态代码】静态代码任务分为“× ”和“ √ ”,分别对应扫描失败/成功

【所属团队】项目对应的所属团队

项目管理

项目基本信息

点击项目列表中的【查看】按钮，可查看项目详情，包括项目基本信息，

项目扫描信息。



通过项目详情页可对项目的信息进行【编辑】、【生成报告】、【导出报

告】的操作。

1、编辑项目

（1）基础信息修改



字段说明：

【项目名称】支持修改项目名称

【项目描述】支持修改项目描述

【文件过滤】支持修改需要过滤的源码文件名称，以“, ”隔开

【上传源码】支持修改上传的源码（支持 zip,rar 格式文件）

【仓库选择】支持修改仓库，仓库类型支持 GIT、SVN、TFS、Perforce、

Mercurial；手动输入仓库地址链接，可选择账号登录或 Token 登录；支持选择

是否自动扫描，自动扫描支持每天、每周、每月定时扫描

【最长扫描时长】支持修改最长扫描时长

（2）静态代码修改



字段说明：

【项目任务类型】默认为“静态代码任务”，不可修改

【自动识别语言】可选择是否支持自动语言识别功能

【代码语言】可修改代码语言，包括 Java/JSP、C#/ASP.NET、PHP、C/C++、

Python、JavaScript、Object-C、swift、go

【渲染 DOM 数】支持选择是否渲染 DOM 树

【文件过滤】支持修改扫描过滤的文件，包括 javascript、css、png 等格式的

文件

【扫描规则】支持修改后台预定义扫描的规则

【安全函数】支持修改过滤安全函数名，例如： main,test,print

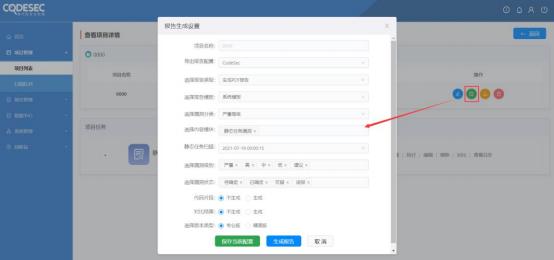
【快速扫描】支持修改是否进行快速扫描功能

注：修改完成后系统将按照新的配置规则对静态代码执行扫描

2、生成报告

点击【生成报告】按钮，可生成静态代码扫描报告，生成报告的格式为系

统默认格式， 用户在使用该功能时，可根据需求选择和定义，如下图：



3、下载报告

点击【下载报告】，页面跳转到生成报告列表页，列表页展示生成的历史

报告，如下图：



团队管理员可根据需要选择相应的报告，点击【下载报告】，可将报告下

载到本地。

项目任务详情

项目任务显示静态代码检查情况，默认显示最近一次静态代码的检查情

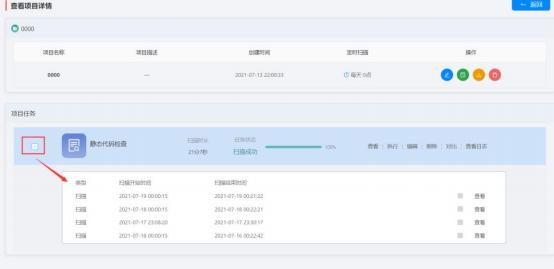
况，包括最近一次代码检查的扫描时长，任务状态。通过项目任务栏可展开历 史检查记录、查看静态代码的检查结果、支持对检查任务的编辑、支持对多次

扫描结果的对比和查看日志等功能。



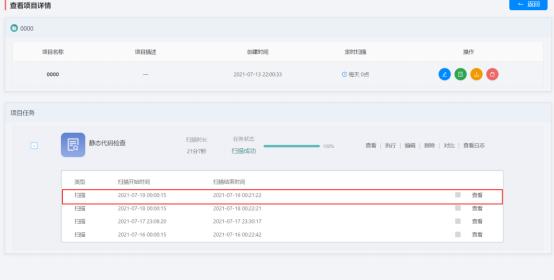
1、展开历史检查记录

点击【+】展开按钮可查看历史检查记录，如下图：



2、查看静态代码的检查结果

点击【查看】按钮可查看项目静态代码检查结果，如下图：



通过静态代码扫描结果页，可以查看项目扫描结果的概览、漏洞列表、漏

洞详情和第三方组件



（1）【概览】：主要是对项目静态代码检查的统计。

项目概览统计： ①安全弱点、严重弱点和误报数进行统计； ②第三方库、 CVE、CNNVD 漏洞库中对用的漏洞数的统计； ③最近一次扫描新发现的漏洞数统

计，复发的漏洞书统计，已修复的漏洞数统计； ④代码总行数的统计。如下

图：





安全弱点信息统计图：按照严重性/OWASP TOP 10 对项目安全弱点进行

统计，如下图：



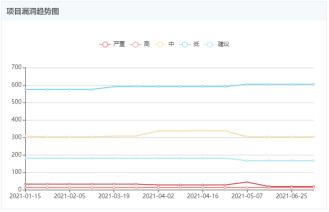
项目风险等级图：对项目风险等级进行评估（项目安全风险值= （严重漏洞 书\*严重漏洞权重+高危漏洞数\*高危漏洞权重+中危漏洞数\*中危漏权重+低危漏

洞数\*低危漏洞数） /行数系数，如下图所示：

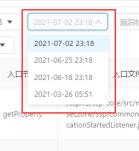


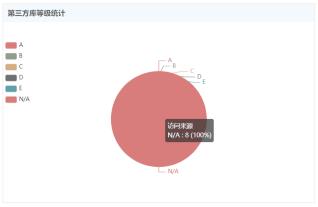
项目漏洞趋势图：按照时间维度，对每次代码项目各个等级漏洞检查的漏

洞趋势图，如下图：

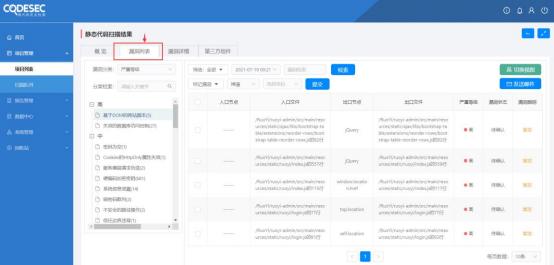


第三方库等级统计：





（2） 【漏洞列表】是对系统检测出的漏洞进行汇总，如下图：



1）漏洞筛选：通过【漏洞列表】也可通过多个维度对漏洞进行查询，包括

按照漏洞分类、漏洞状态和时间维度对漏洞进行查询，如下图：



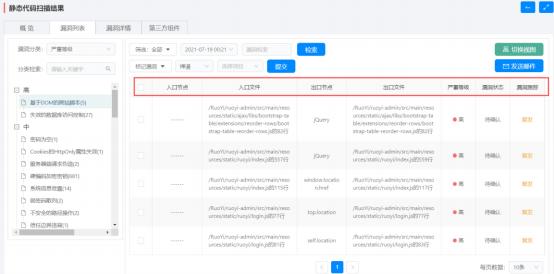
*漏洞分类*

*漏洞状态*

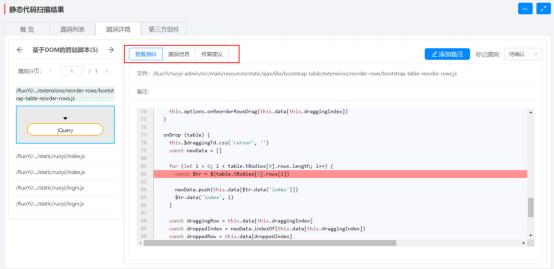
*时间维度*

2）查看漏洞：通过【漏洞列表】查看漏洞信息，包括漏洞的入口节点、入 口文件、出口节点和出口文件、对应的严重等级、漏洞状态和漏洞跟踪。如下

图：

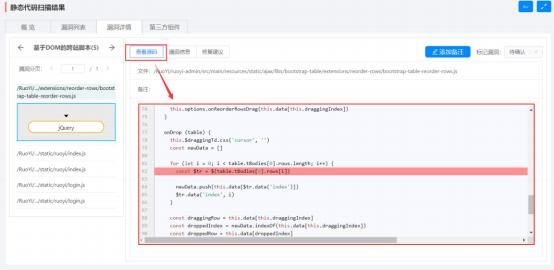


点击列表中对应的漏洞【入口文件】，即可查询漏洞信息。如下图：



通过【漏洞详情】，可分别查看漏洞入、出口节点，以及对应的源码，如

下图：



通过【漏洞信息】，可查看对应的漏洞的概述，包括漏洞的概念及示例代

码，如下图：



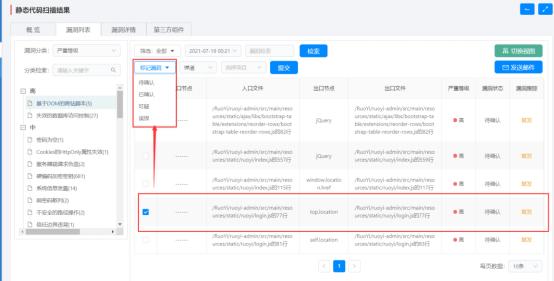
通过【修复建议】可查看对该漏洞的修复建议，如下图：



3）漏洞标记

审计员可在【漏洞列表】页勾选漏洞进行标记，标记的状态分为：待确认

（漏洞默认状态）、已确认、可疑和误报四种。如下图：



4）切换视图

审计员可在【漏洞列表】页勾漏洞执行切换视图的操作，可在列表和结构

图之间进行切换，如下图所示：

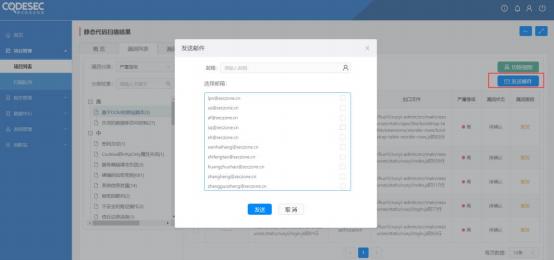




5）发送邮件

审计员可在【漏洞列表】页勾选漏洞，可将漏洞通过邮件的方式发送给项

目团队管理员或项目成员等，如下图：



（3）漏洞详情

审计员可通过【漏洞列表】点击漏洞对应的文件，直接跳转到漏洞详情

页，也可以通过点击【漏洞详情】查看漏洞详细信息。



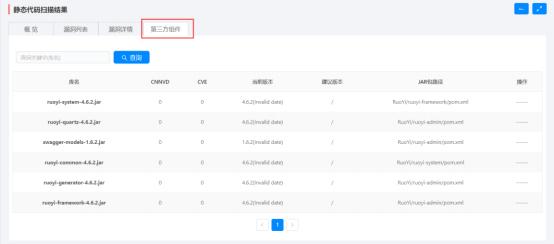
可通过左上角标识为①、②的区域切换不同等级的漏洞和漏洞间的切换。

关于【查看源码】、【漏洞信息】和【修复建议】详细介绍见上文。

（4）第三方组件

通常情况下， 第三方组件都是开源的。 由于第三方组件不是由本项目开发者 编写的组件或者应用。第三方组件的作者遵循行业内的一些协议， 允许其他软件 开发者自由使用这些组件。但这些组件安全性未知， 通过 CodeSec 源代码安全扫

描平台源代码扫描服务，可以检测到潜在的威胁。 如下图：



点击列表中的【查看】按钮，可查看第三方组件的扫描详情，如下图：



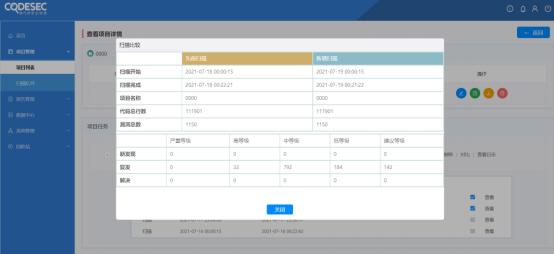
3、扫描结果对比

在项目详情页，勾选需要对比的扫描结果，如下图：



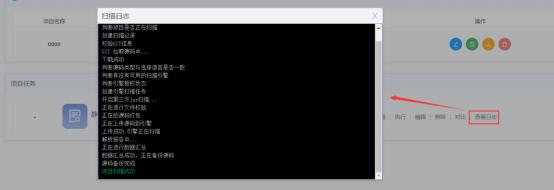
点击【对比】按钮， 系统将两次扫描的结果进行对比分析， 审计人员可以通 过对比扫描的结果对项目的安全性、项目团队绩效等多个维度进行审计分析。如

下图：



4、查看日志：

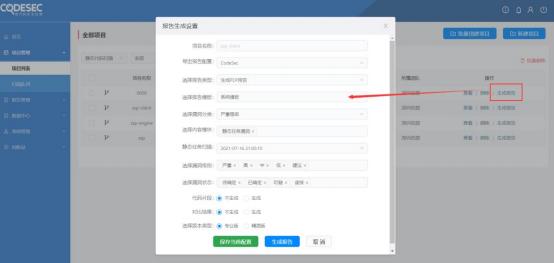
通过项目详情页的【查看日志】按钮，可调出源代码扫描日志，如下图：



生成报告

点击【生成报告】按钮，可生成静态代码扫描报告，生成报告的格式为系

统默认格式，团队管理员在使用该功能时，可根据需求选择和定义，如下图：



导出报告

点击项目列表中【导出报告】按钮，页面跳转到报告记录列表，列表展示

生成的历史报告，如下图：



团队管理员可根据需要下载不同时间、规则等生成的报告，点击【下载报

告】，可将报告下载到本地。

项目查询

在项目列表页面支持通过多维度对项目进行查询，包括：项目扫描状态、

定时扫描、同时也支持关键字查询，如下图：



**4.4.5** 数据中心

<4.4.5.1> 项目数据汇总

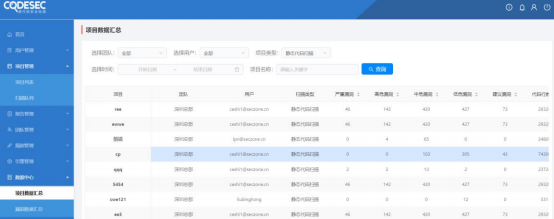
业务场景：查看项目数据汇总，查看团队的各个项目、创建人员，以及各个项

目漏洞情况。对所在团队项目代码的安全性进行统计分析。

操作路径：【数据中心】 ->【项目数据汇总】

操作说明： 通过以上操作路径进入到【项目数据汇总】页面，可查看各个项目

各类型漏洞统计，支持多维度数据查询，如下图：

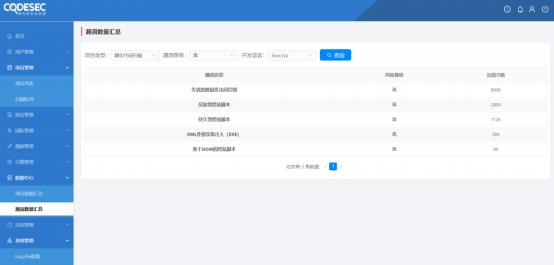


<4.4.5.2> 漏洞数量汇总

业务场景：查询团队项目各个漏洞级别和相应开发语言下各类漏洞的数据统计

操作路径：【数据中心】 ->【漏洞数量汇总】

操作说明： 通过以上操作路径进入到【漏洞汇总】页面，如下图：



4.5 普通用户操作手册

**4.5.1** 系统登录

业务场景：用户登录系统

操作路径：【输入 URL】->【输入用户名/密码】

操作说明：

1、在浏览器中输入 URL：http://ip:port 即可打开开源网安 CodeSec 平台 登录界面，其中 IP 是指扫描工具的服务器 IP 地址， PORT 是指端口(端口默认 是 28081)。使用开源网安代码审核平台服务商提供的普通用户名及密码，即可

登录。 如下图：



注意：建议使用推荐的浏览器；

**4.5.2** 项目管理

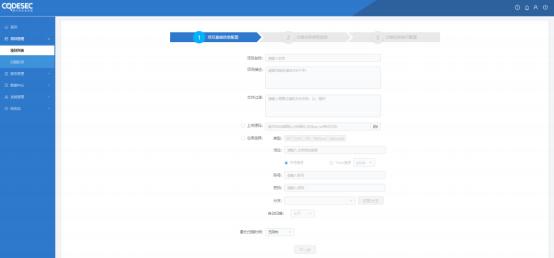
<4.5.2.1> 新建项目

业务场景：新建 CodeSec 源码检测项目

操作路径：【项目管理】->【项目列表】 ->【新建项目】

操作说明：支持普通用户（项目团队成员）新建项目，如下所述：

1、配置项目基础信息，如下图：



字段说明：

【项目名称】用户手工输入项目名称，必填项

【项目描述】用户手工输入项目描述

【文件过滤】用户手工输入需要过滤的源码文件名称，以“ , ”隔开

【上传源码】支持选择上传的源码（支持 zip,rar 格式文件）

【仓库选择】支持选择仓库，仓库类型支持 GIT、SVN、TFS、Perforce、

Mercurial；手动输入仓库地址链接，可选择账号登录或 Token 登录；支持选择

是否自动扫描，自动扫描支持每天、每周、每月定时扫描

【最长扫描时长】支持设置最长扫描时长

以上信息填写完成后，点击【下一步】完成项目基础信息配置，进入扫描

任务类型选择页面。

注：如果未上传源码或者填写 Git/Svn 信息，下一步则不能创建静态代码

进行扫描。

2、选择扫描任务类型，如下图：



点击【下一步】，进入到扫描任务执行配置页面，也可点击【上一步】编

辑项目基础信息配置。

注：默认为静态代码任务

3、配置扫描任务执行，如下图：



字段说明：

【项目任务类型】默认为“静态代码任务”，不可修改

【自动识别语言】支持选择是否支持自动语言识别功能

【代码语言】支持多类型代码语言的选择，包括 Java/JSP、C#/ASP.NET、

PHP、C/C++、Python、JavaScript、Object-C、swift、go

【扫描二进制】支持选择是否扫描二进制

【JDK 版本选择】选择 JDK 版本，包括 JDK1.5~1.9

【文件过滤】支持选择扫描过滤的文件，包括 javascript、css、png 等格式的

文件

【扫描规则】支持选择后台预定义扫描的规则

【安全函数】自定义过滤安全函数名，例如： main,test,print

【快速扫描】支持选择是否进行快速扫描功能

以上信息配置完成，点击【创建】，项目创建成功；点击【创建并执

行】，项目创建成功并执行项目源码扫描；点击【上一步】，跳转到扫描任务

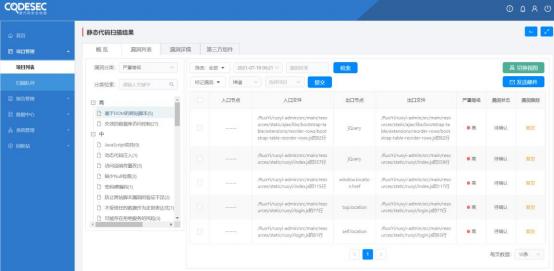
类型选择页面。

<4.5.2.2> 项目列表

业务场景： 查看项目中检测到的安全弱点信息，跟踪漏洞。

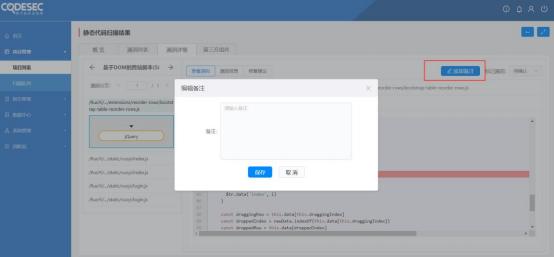
操作路径：【项目管理】 ->【项目列表】 ->【查看】操作说明：通过以上操作

路径进入到项目详情页，查看项目安全弱点信息、跟踪及处理漏洞。



1、漏洞查看：点击漏洞对应的入口文件，可查看漏洞的详细信息，针对漏

洞可添加备注，如下图：



2、漏洞标记：当前页支持对漏洞进行标记，标记类型包括：待确认、已确

认、可疑、误报。

