CodePecker®
安 全 解 决 方 案

- 源代码缺陷分析

CodePecker 源代码缺陷分析系统 V4.0

白皮书

北京酷德啄木鸟信息技术有限公司

目录

1. 产品概述

CodePecker 源代码缺陷分析系统 V4.0 是北京酷德啄木鸟信息技术有限公司采用业界领先的源代码静态分析技术开发的一款针对源代码缺陷进行静态分析检测的产品，是国内第一款成熟的源代码缺陷分析产品。CodePecker 由酷德啄木鸟公司自主研发，具有完全自主知识产权。它在对目标软件代码进行语法、语义分析的技术上，辅以数据流分析、控制流分析和特有的缺陷分析算法等高级静态分析手段，能够高效的检测出软件源代码中的可能导致严重缺陷漏洞和系统运行异常的安全问题和程序缺陷，并准确定位告警，从而有效的帮助开发人员消除代码中的缺陷、减少不必要的软件补丁升级，为软件的信息安全保驾护航。

CodePecker 是北京酷德啄木鸟信息技术有限公司的核心品牌，北京酷德啄木鸟信息技术有限公司是一家专注于软件源代码信息安全业务的高新技术企业。公司成立于 2013 年，由多位信息安全领域资深专家发起成立，为政府、金融、电信、能源、互联网等各行业用户提供源代码缺陷审计产品及服务，帮助客户保障源代码安全。

2. 主要功能

CodePecker 提供企业级的软件安全开发生命周期管理，包括：检测项目管理、源代码缺陷分析、自动化检测、全流程缺陷管理、源代码安全评级、缺陷查询定位、缺陷审计、代码缺陷统计分析、检测规则配置管理、检测报告、函数白名单、检测目标基线设置、Bug 管理系统集成、代码库集成、缺陷知识库等多项强大的功能。CodePecker 使得软件源代码缺陷分析和审计工作实现了系统化管理，使得开发人员、测审计人员和管理人员在一个平台上都能够简单地、高效地完成代码审计工作，帮助客户形成一套完整的源代码质量管理流程和体系，提高整体编码质量和水平，为客户的信息安全助力护航。

2.1. 架构图

2.2.检测能力

CodePecker 基于市场领先的缺陷检测引擎和规则库，支持对 Java/JSP、C、C++、C#、PHP、Python、Objective-C、HTML5、JavaScript、SQL 等主流编程语言开发的软件源代码安全缺陷的检测。

支持对源代码安全缺陷和质量缺陷的检测。检测结果涵盖代码注入、跨站脚本、缓冲区溢出、配置错误、API 误用、拒绝服务、未验证的用户输入、弱加密问题、信息泄露、危险函数等类型，共 1000 多个缺陷类型。

检测缺陷可按照 CWE、OWASP Top 10、CVE、WASC、NIST、PCI 等国际组织或行业安全标准进行分类、分级。

支持分析百万行级别的源代码，检测速度不低于 1 万行/分钟（CPU 2.0 GHz 以上，内存 32GB 以上）。

CodePecker 在对目标软件代码进行语法、语义分析的技术上，辅以数据流分析、控制流分析、配置分析等特有的缺陷分析算法等高级静态分析手段，CodePecker 软件对同样的目标系统进行检测时，能提供过程内（Intra-procedure）、过程间（Inter-procedure）等各种层次的分析，能够高效的检测出软件源代码中的可能导致严重缺陷漏洞和系统运行异常的安全问题和程序缺陷。和国内外同类产品相比，具有能力强、速度快，低误报、低漏报的特点。

2.3.检测项目管理

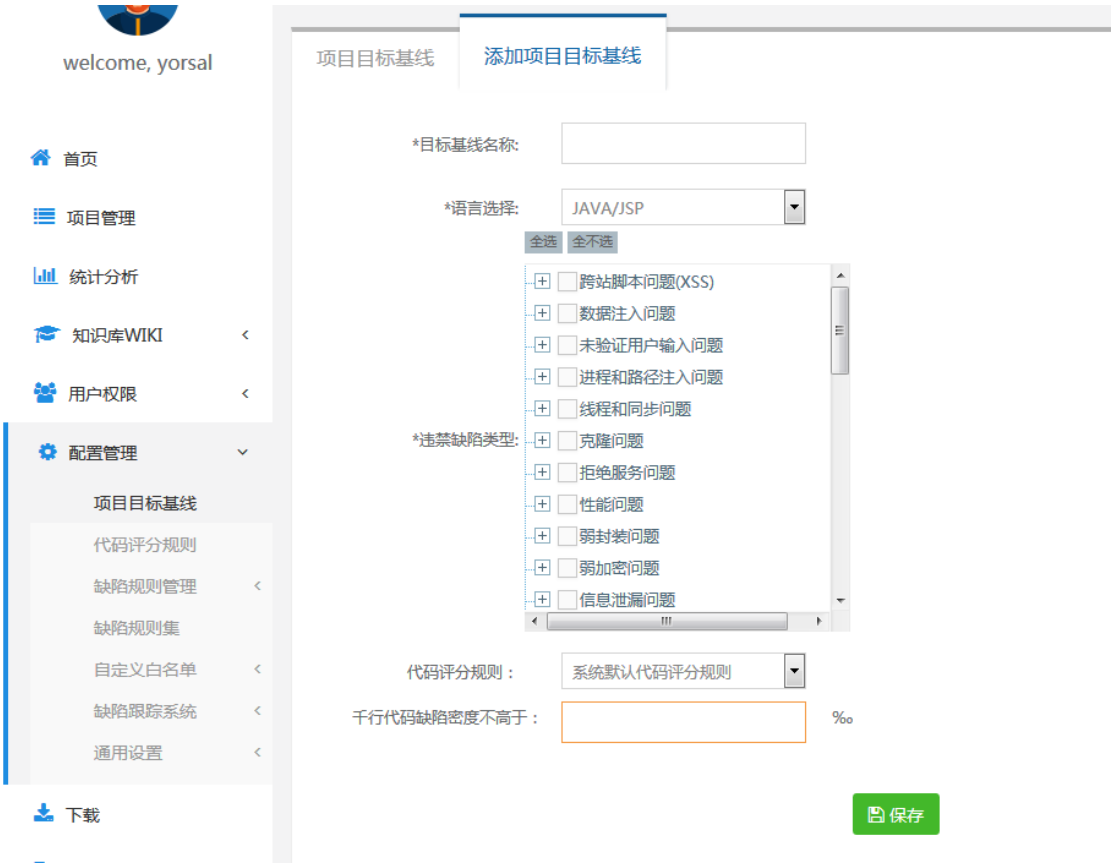
支持用户管理和权限管理。以项目组形式进行代码审计项目管理，支持对多部门、多项目组的团队级代码审计管理功能。

支持缺陷从发现到分配到解决的全生命周期管理。

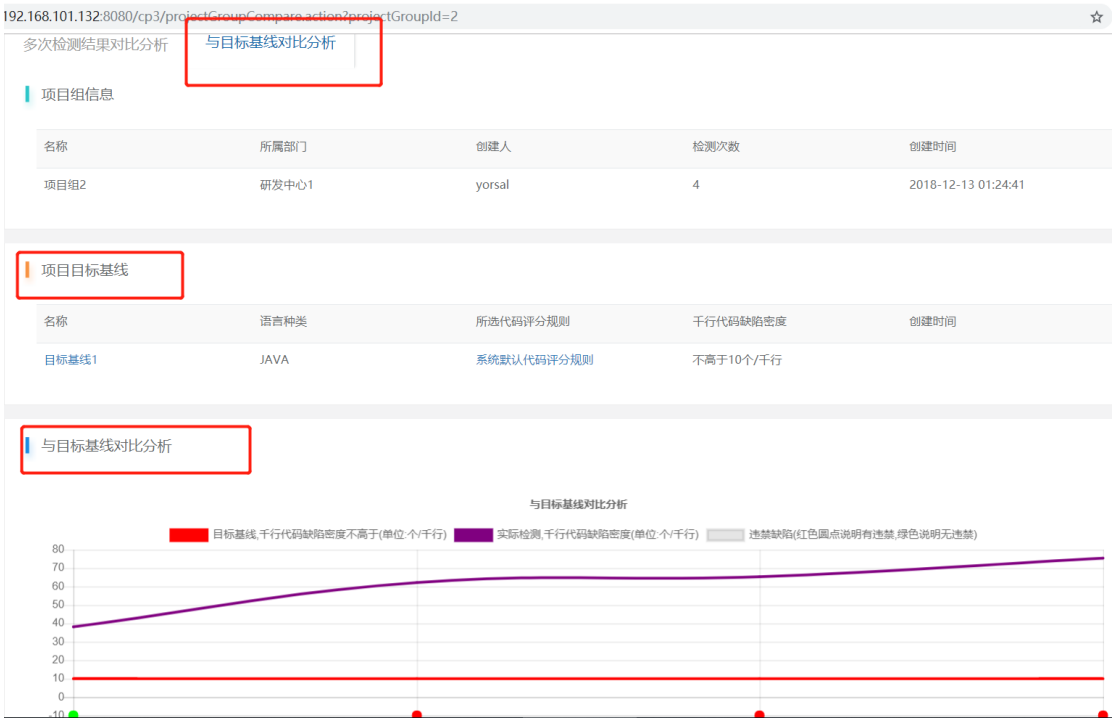
用户可通过上传代码压缩包进行检测。支持对 SVN/GIT/TFS 等版本管理系统的集成，可直接从代码库获取代码实时或者周期性的自动化检测。

检测进度可实时查看跟踪。

根据项目的历次检测结果，提供对比分析及安全趋势分析。结合已设置的项目目标基线，提供检测结果与目标基线的对比分析。



wb3.0	v3.0	977	2019-01-19 18:53:18
wb2.0	v2.0	1903	2019-01-17 01:22:58
wb1.1	v1.1	1901	2019-01-16 23:57:52
wb1.0	v1.0	1901	2019-01-08 18:09:49



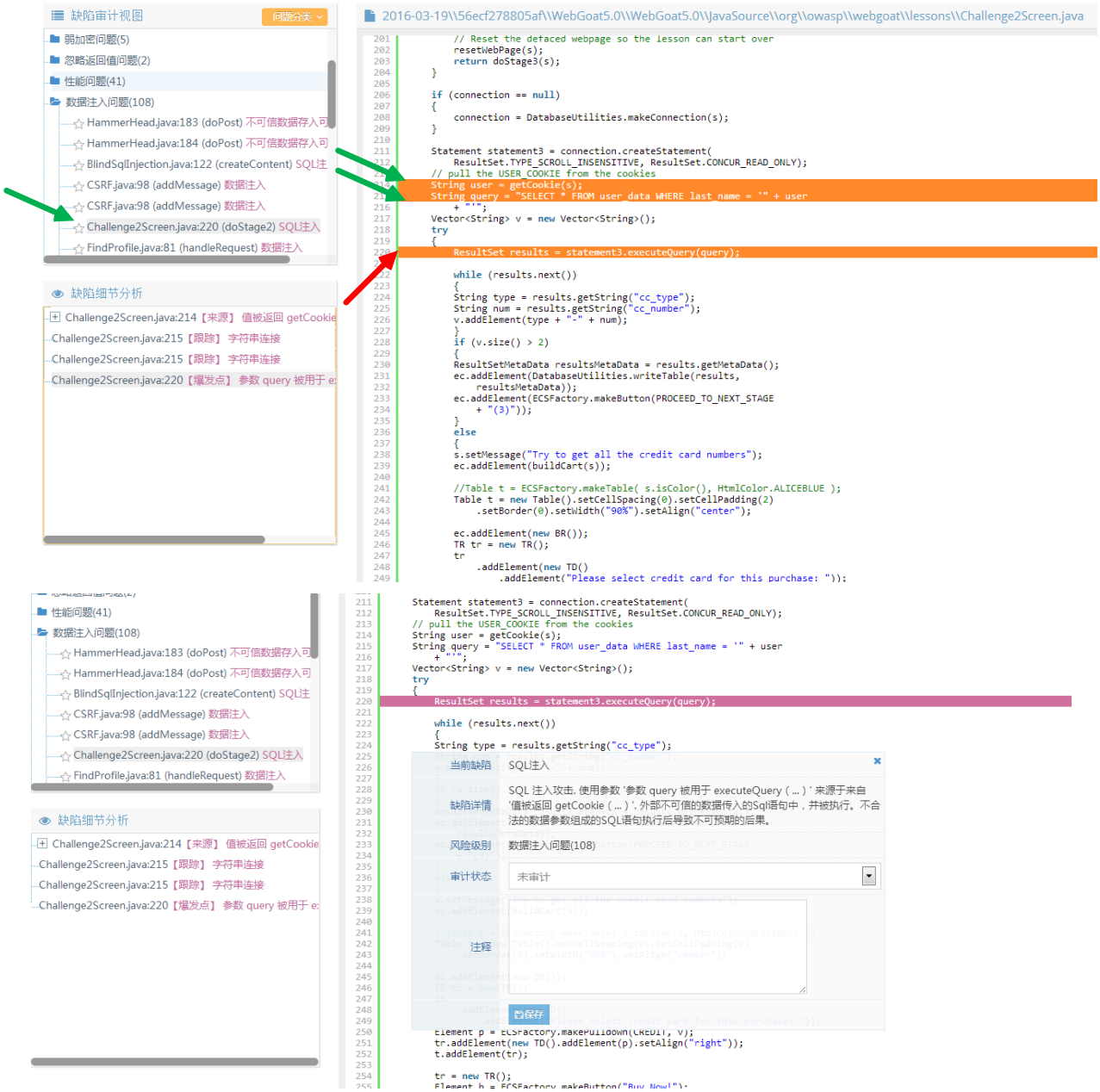
2.4. 图形化展示和缺陷定位追踪

系统使用 WEB 浏览器访问，图形化操作，界面友好，操作简单，不需要复杂的检测流程。检测完成后，可根据检测结果生成可视化缺陷展示图，从多个维度展示缺陷分布。

检测结果简单明了，并有详细的缺陷分析，同时提供了缺陷分析的追踪定位，用户只需要简单的鼠标操作，就能够对缺陷追踪定位。

针对检测结果给出缺陷细节分析、修复建议及详细的知识库参考，为开发人员修复缺陷提供建议和帮助。

系统支持对缺陷分析结果以及分析人员进行审计的结果做持久化保存，方便后续对缺陷的维护管理。

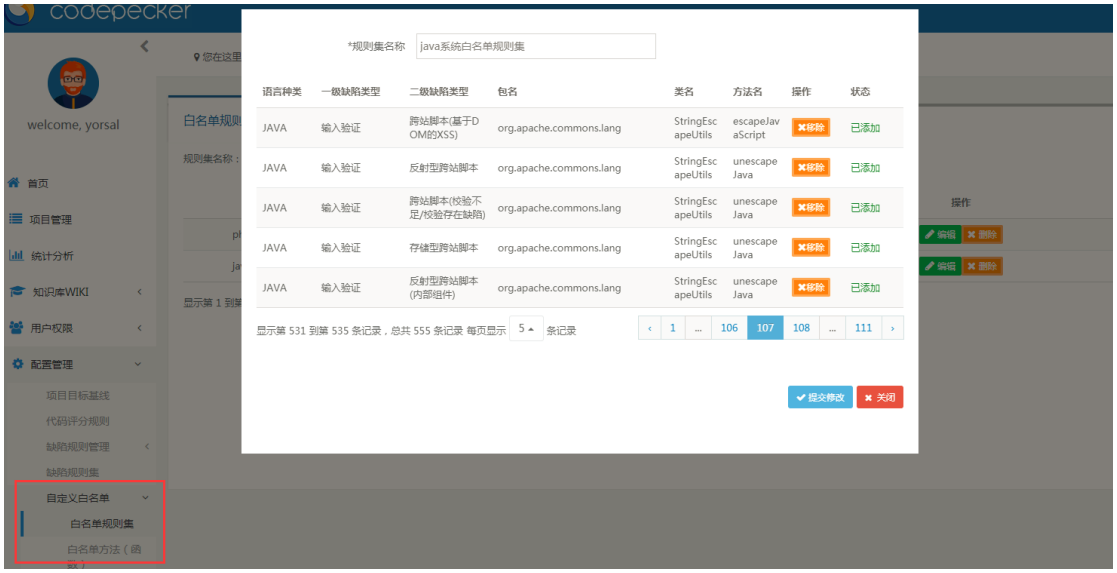


2.5. 缺陷类型规则定制

针对上千种缺陷检测类型，产品提供了可选择缺陷检测规则配置操作（高级检测），如在大型应用系统中，存在各种级别的多种缺陷类型，检测结果可能偏多，会干扰错误排查，影响审计效率，用户可只针对高危或者某几类缺陷做有针对性的深度检测，只关注特定的缺陷类型。同时 CodePecker 也提供了多种默认缺陷检测类型（普通检测），涵盖了常见的缺陷种类。

2.6. 函数白名单

支持用户自定义函数白名单功能，检测引擎可自动识别白名单函数进行过滤净化，减少误报。



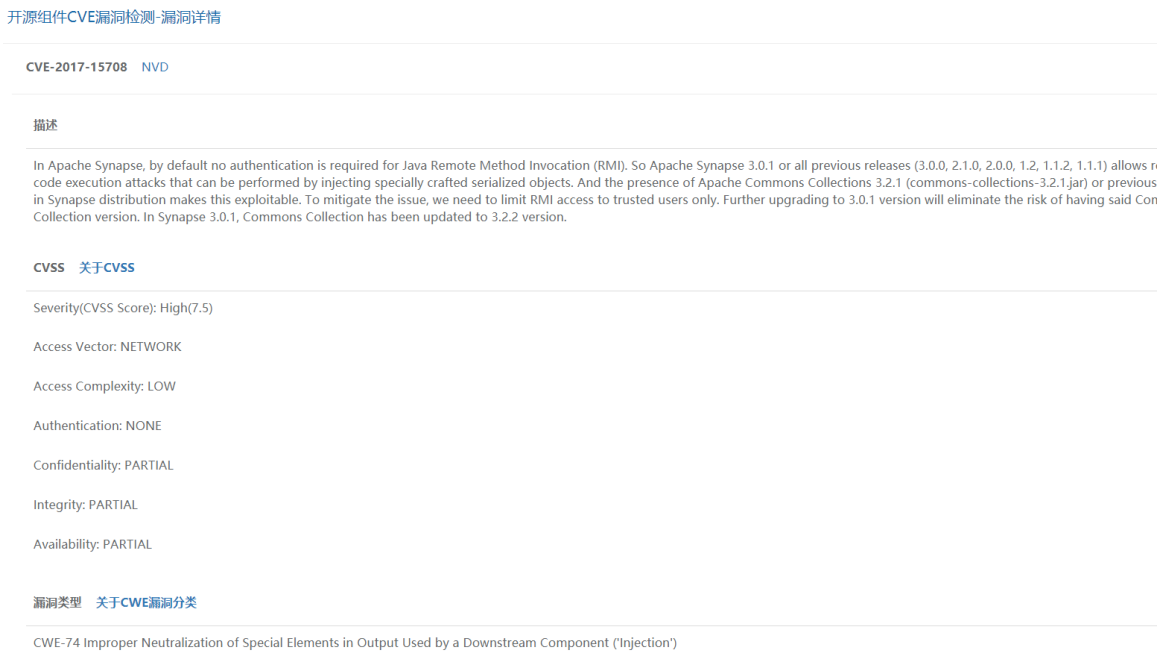
2.7. 开源组件检测

本产品可对软件项目中使用的开源组件进行安全检测，找出存在 CVE 漏洞的开源组件，并给出准确的漏洞详情及修复建议。

JAR文件检测

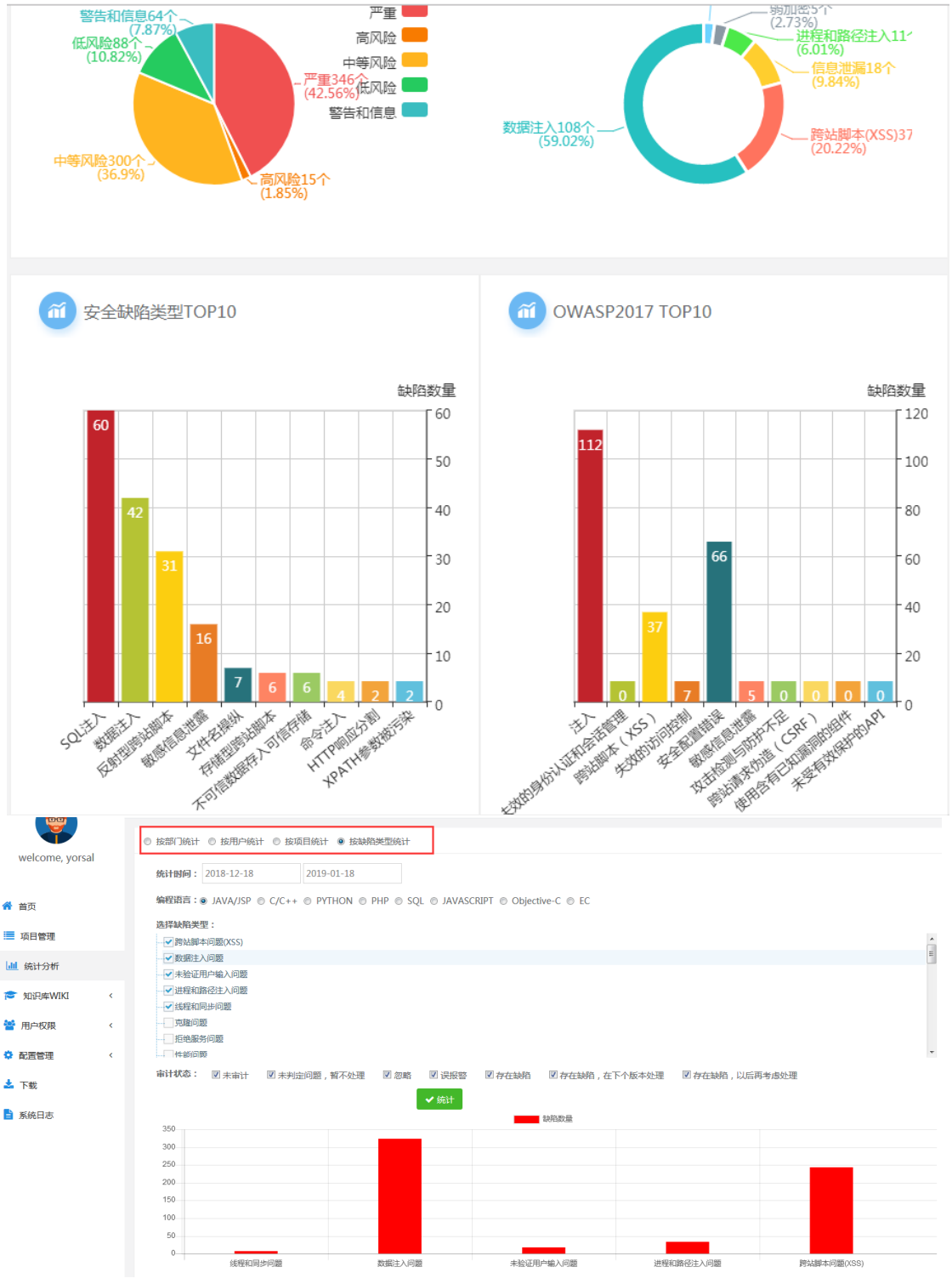
JAR检测引擎版本：V1.4.3　生成报告时间：2018-05-13 19:02:00　JAR文件数量：15　检测出CVE漏洞：12

CVE	CWE	危害等级(CVSS)	JAR文件
CVE-2017-15708	CWE-74 Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	High(7.5)	commons-collections-3.1.jar
CVE-2016-1182	CWE-20 Improper Input Validation	Medium(6.4)	struts.jar
CVE-2016-1181	未知	Medium(6.8)	struts.jar
CVE-2015-6420	CWE-502 Deserialization of Untrusted Data	High(7.5)	commons-collections-3.1.jar
CVE-2015-0899	CWE-20 Improper Input Validation	Medium(5.0)	struts.jar
CVE-2014-3596	未知	Medium(5.8)	axis.jar
CVE-2014-0114	CWE-20 Improper Input Validation	High(7.5)	struts.jar
CVE-2012-5784	CWE-20 Improper Input Validation	Medium(5.8)	axis.jar
CVE-2008-2025	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Medium(4.3)	struts.jar
CVE-2006-1548	未知	Medium(4.3)	struts.jar
CVE-2006-1547	未知	High(7.8)	struts.jar



2.8. 统计分析

本系统的设计目标在于在用户系统上线之前尽最大可能的发现源代码中的安全隐患和代码质量问题，从多个视角深刻反映系统源代码的整体安全状况，对高危安全缺陷的分布、代码质量问题分布、缺陷的危害、缺陷信息细化等多视角信息进行了细粒度的统计分析，并通过柱状图、饼图等形式，直观、清晰的从总体上反映了代码缺陷分布情况，提供定位追踪代码中的问题，挖掘出系统中潜在的安全隐患，避免由于代码缺陷导致系统上线运行之后出现信息安全问题。

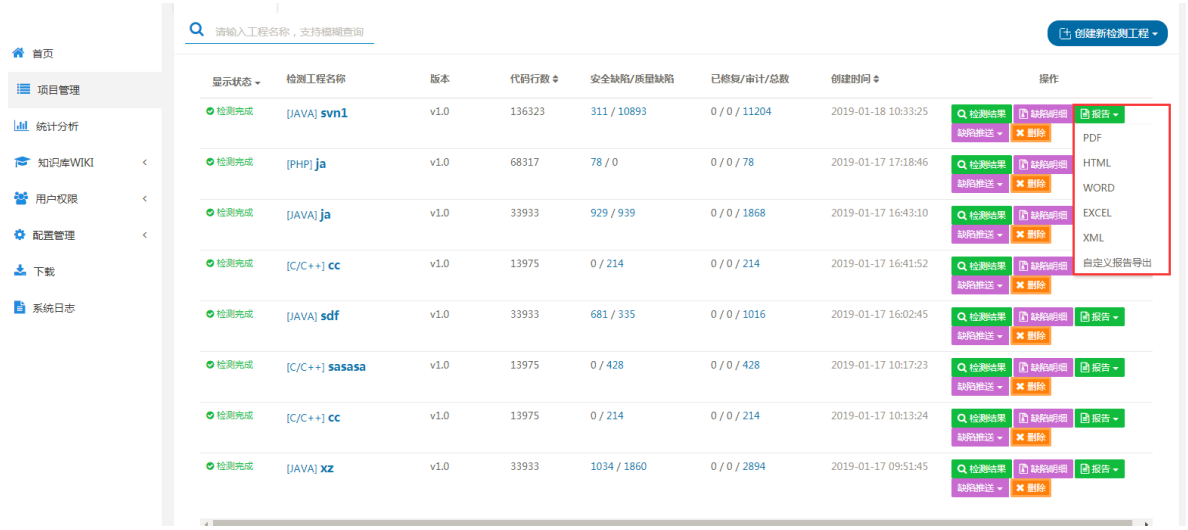


2.9. 检测报告

用户可根据需要，通过多个维度查看检测统计分析及检测报告，检测报告功能丰富，详实

全面，包括项目的基本信息、统计信息及缺陷详情。检测报告支持 PDF、WORD、EXCEL 等格式。

支持自定义报告内容，用户可根据项目、缺陷类型、严重等级、审计状态等导出报告。



2.10. 缺陷知识库

团队成员有着多年的源码安全检测经验，依靠专业的安全团队的研究，CodePecker 缺陷知识库功能丰富，知识库包含所有缺陷类型，每个缺陷都有详尽的描述和修补建议，同时积极与国际化接轨，大多缺陷类型都可以映射到 CWE、OWASP、PCI 等权威国际安全组织公布的缺陷分类中。缺陷知识库可作为审计人员和开发人员的重要学习参考，提高代码的安全开发水平。

2.11. 与外部系统的集成整合

支持与版本控制系统（如 SVN、Git 、TFS 等）的集成，实现从代码库获取代码实时或者周期性自动化检测功能。

支持与 Bug 管理系统（Bugzilla、JIRA 等）的集成，把检测结果自动导入到 Bug 管理系统。

提供了代码检测 API，可通过 API 进行代码检测及获取检测结果。

提供了与邮件系统的集成，可把检测结果以邮件形式发送。

可根据用户特殊需求进行定制化开发，满足用户对代码审计系统与其它系统的集成整合。

3. 自主知识产权及销售许可证

CodePecker 是国内第一款成熟的源代码缺陷分析产品。由北京酷德啄木鸟信息技术有限公司自主研发，具有完全自主知识产权。具有公安部《计算机信息系统安全专用产品销售许可证》。

4. 产品形态及参数

产品形态	详细
CodePecker Web 版（含硬件）	■ 标准硬件服务器（2U 机架式服务器，CPU E5-2620*2，内存 128G，存储 4TB） ■ CodePecker Web 版 ■ 支持 JAVA 等语言的检测（语言种类可灵活定制） ■ 操作系统支持 Windows 64 位/CentOS 7 64 位/ RedHat 7 64 位 ■ 适合项目数量较多的用户

	■ 支持缺陷流程管理 ■ 支持 5 个并发检测（并发数可根据硬件配置进行扩展） ■ 同时在线用户数及注册用户数无限制 ■ 无检测次数限制 ■ 永久 License
CodePecker Web 版（纯软件）	■ CodePecker Web 版 ■ 支持 JAVA 等语言的检测（语言种类可灵活定制） ■ 操作系统支持 Windows 64 位/CentOS 7 64 位/ RedHat 7 64 位 ■ 硬件需求：CPU 2.0 GHz 以上，内存 32G 以上 ■ 适合项目数量较多的用户 ■ 支持缺陷流程管理 ■ 支持 5 个并发检测（并发数可根据硬件配置进行扩展） ■ 同时在线用户数及注册用户数无限制 ■ 无检测次数限制 ■ 永久 License
CodePecker 单机版	■ 缺陷分析软件安装包 ■ 支持 JAVA 等语言的检测（语言种类可灵活定制） ■ 支持 Windows 64 位操作系统 ■ 至少需 16G 内存 ■ 适合项目数量较少的用户 ■ 免安装，简单易用 ■ 单用户使用，不支持并发检测 ■ 无检测次数限制 ■ 永久 License