CodePecker 源代码缺陷分析系统 V4.0
用户手册

北京酷德啄木鸟信息技术有限公司

目 录

一、系统说明

1.CodePecker 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码缺陷分析产品。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漏洞、减少不必要的软件补丁升级，为软件的信息安全保驾护航。

2.与同类产品相比，CodePecker 产品具有很多突出的特征：

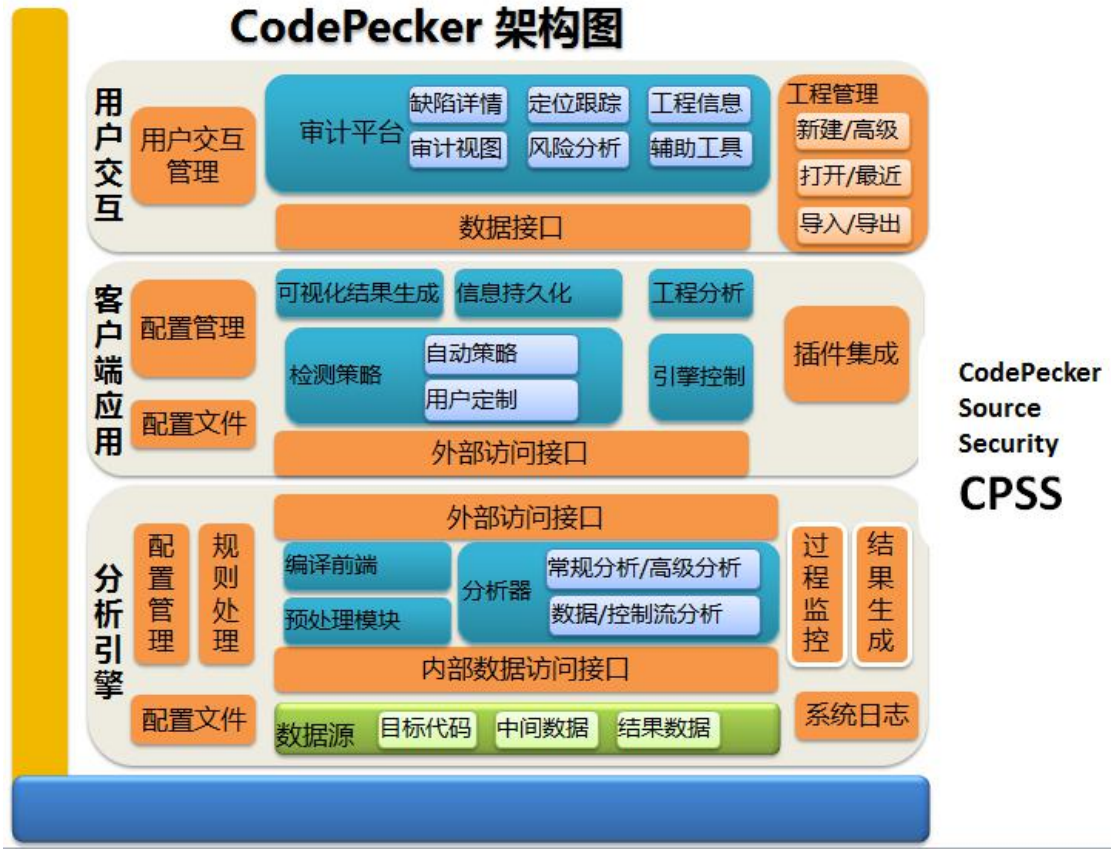
1) CodePecker 支持的语言种类多，能够分析 Java、Jsp、C/C++、Php、Python 等常用编程语言编写的代码，其中，在 CodePecker 最具代表性的 Java/Jsp 语言分析方面，能够对几百种缺陷类型进行代码安全和质量检测，并且可以检测 Java 源代码编译后的字节码文件，还可以直接检测第三方 Jar 包。
2) 能够全面的发现软件代码中的缺陷，这其中包括软件安全漏洞，也包括软件代码质量问题，还能够发现编程中违反编程规则的情况。
3) 提供友好的图形分析界面，简化了缺陷分析操作和流程。
4) 支持分析百万行级别的源代码。
5) 快速的分析检测缺陷，检测结果的低误报率、低漏报率。
6) 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。
7) 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。
8) 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。
9) 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。

10) 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。

11) 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。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。

1.1 系统架构



1.2 主要功能结构

1.2.1 用户登录

通过 Chrome 浏览器访问系统地址 http://ip:8080/cp3,进入系统登录页面。其中“ip”指的是系统所部署服务器的 ip 地址。完整的系统访问地址如“http://192.168.0.23:8080/cp3”。点击登录按钮，输入用户名、密码、验证码后登录系统。系统首次安装后已有默认超级管理员账号/密码(yorsal/222222)，用户登录后可修改密码，可新建其他用户。

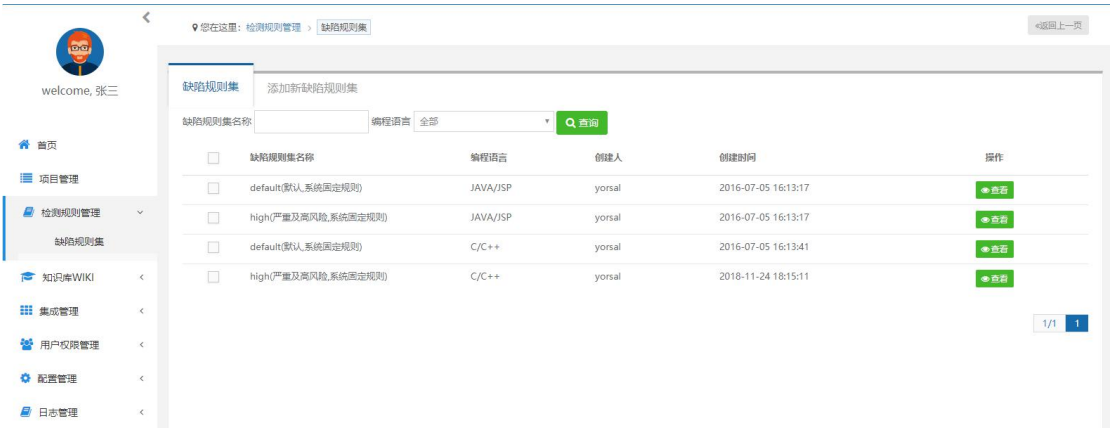
1.2.2 首页

1.2.3 项目管理

用户可在此模块管理项目组、管理检测项目、发起项目代码检测、查看检测结果、查看和下载检测报告、审计缺陷等。

1.2.4 检测规则管理

可以查看系统中的缺陷规则，也可以新添加缺陷规则。

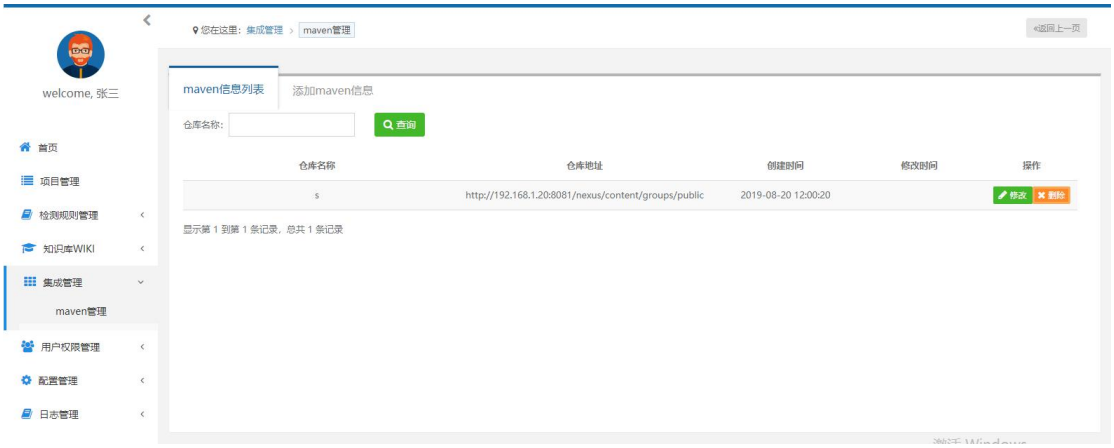


1.2.5 知识库

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。

1.2.6 集成管理

Maven 的添加、修改、删除、查询功能。



1.2.7 用户权限管理

提供部门管理、用户管理、菜单管理、角色管理功能。

1. 部门管理：添加实际用户所属的部门；

2.用户管理：单个或批量增加新的用户，且不同的用户，因为所属角色不同，权限也不同，通过划分权限来限定用户的操作行为；

3.角色管理：根据需求，增加新的角色，满足限定用户行为需求。

1.2.8 配置管理

包括通用设置中历史数据、服务器监控功能。

1.2.9 日志管理

提供了系统重要操作日志的查询、导出、删除等功能。

1.3 代码检测流程

检测流程如下：

项目组—>新建检测项目—>设置—>检测分析—>问题追踪审计—>结果导出—>记录查看。

用户新建项目组，在项目组下提交检测工程进行检测，用户可以在该工程目录下导入 ZIP 包进行检测，也可以通过 SVN 或 Git 地址指定项目进行检测，可实时进行检测，也可以在固定时间进行周期性的检测。

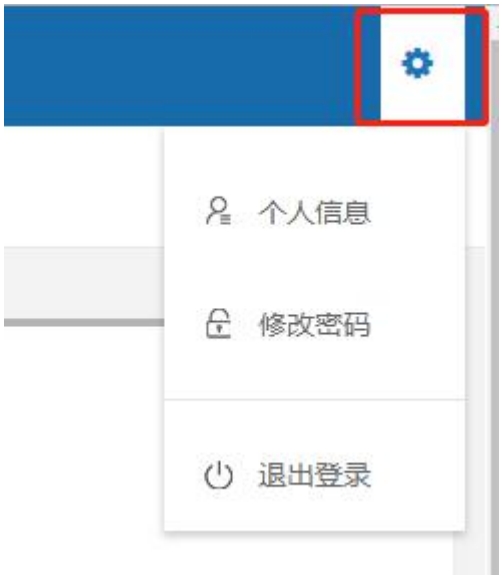
在检测工程之前，需要指定检测缺陷类型，用户可以用默认的设置，也可以自己选择检测缺陷类型，设置完成后，就可以对工程进行检测了。检测完毕后，将会在输出区输出检测结果。可以依据输出结果来进行缺陷的追踪及审计确认，检测结果能够自动定位到相应的代码行。可以将检测结果以 PDF、WORD 等格式文件导出。用户也可以查看某个项目的检测历史记录信息。

二、首页

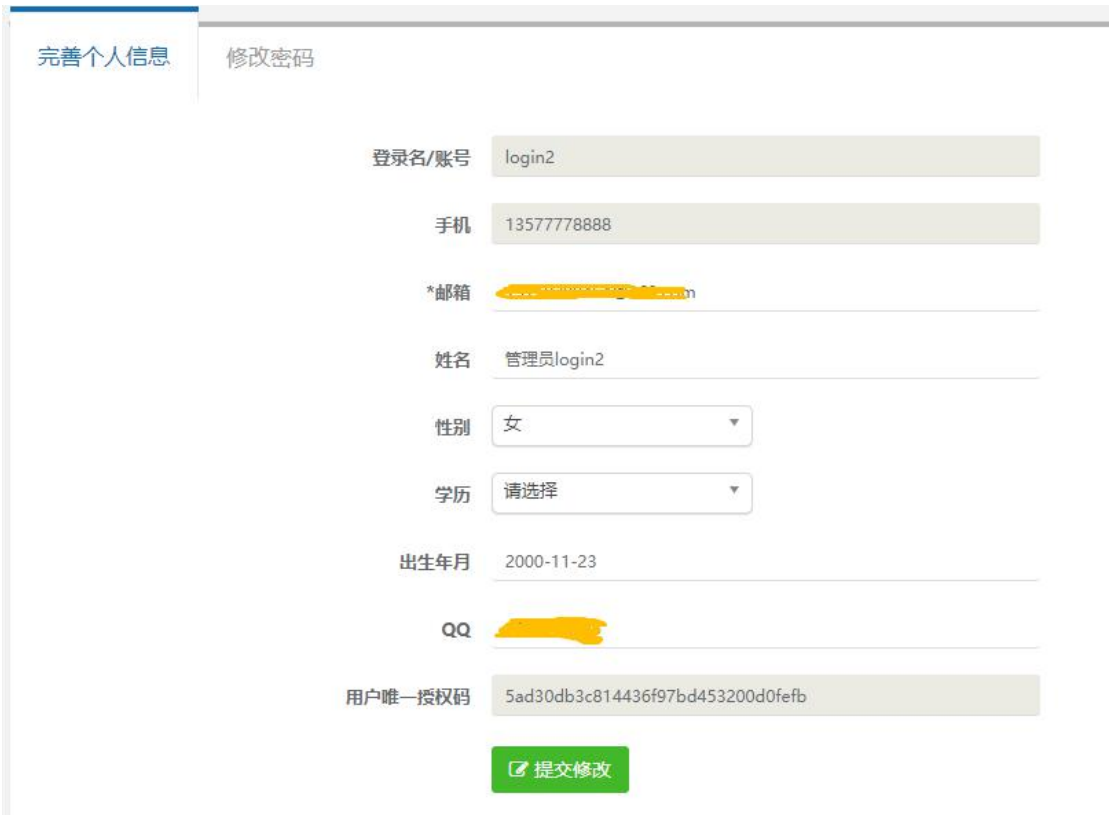
2.1 设置

1. 设置：

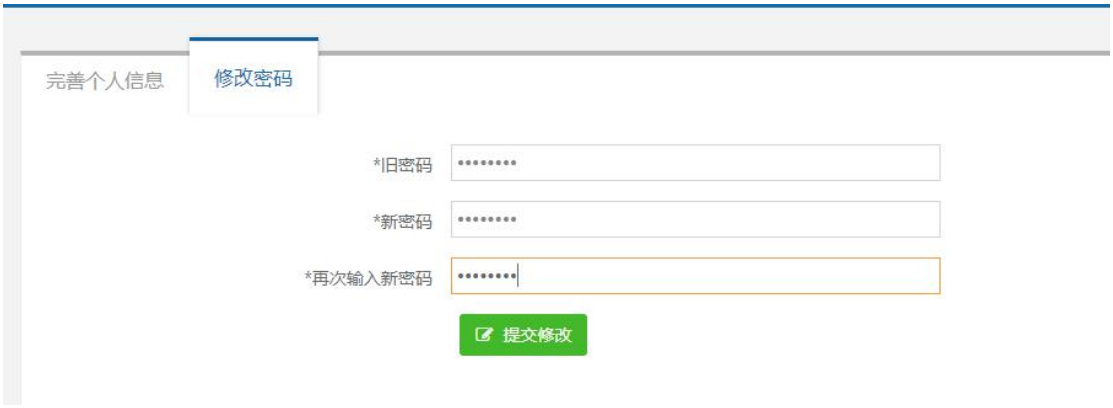
登录成功后，进入首页的右上角有个设置按钮，点击按钮展开下拉框：个人信息、修改密码、退出登录。



（1）个人信息



（2）修改密码



（3）退出登录，点击退出登录直接退出

2.2 快速检测

1. 快速检测：创建工程（上传），属于默认部门；

项目组名称为：默认，所属部门：默认部门，不可删除。

2. 新建项目组：开始“新建项目组”；

页面跳转到“新建项目组”页，可选择所属部门、项目组成员、项目目标基线。

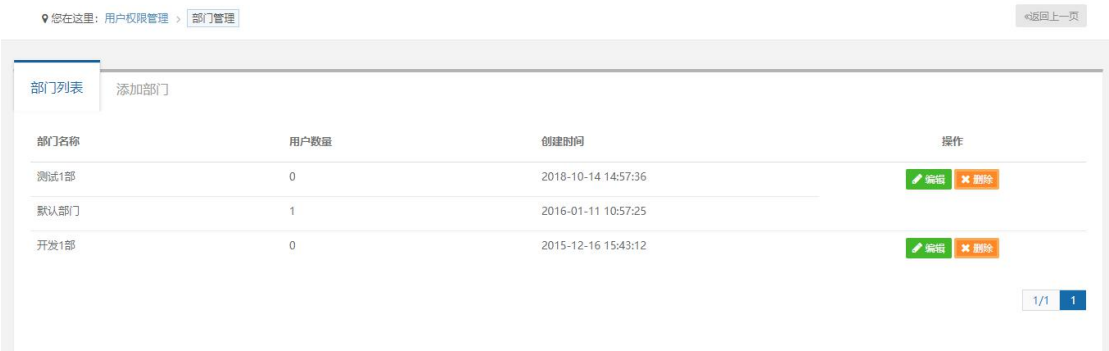
3. 查看更多：快速查看更多与当前用户相关的工程；

进入项目管理页面

2.3 系统使用情况

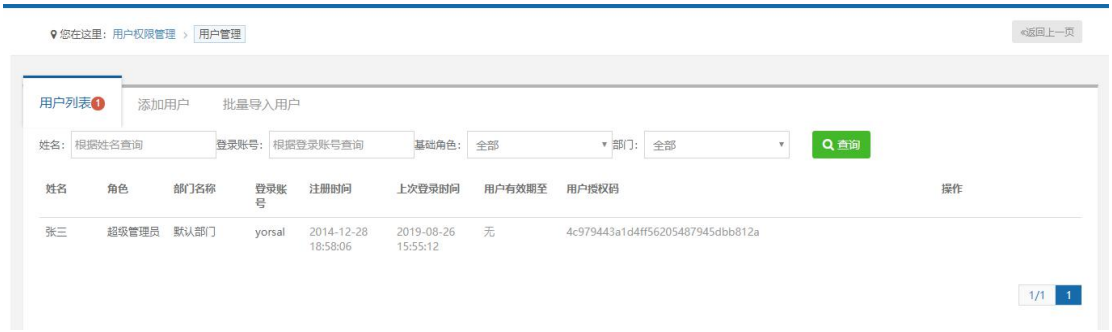
1. 点击部门后的数字

页面跳转到部门管理，显示部门详情



2. 点击用户数量右侧的数字

页面跳转到用户管理页面



3. 点击项目组右侧数字

页面跳转到项目管理页

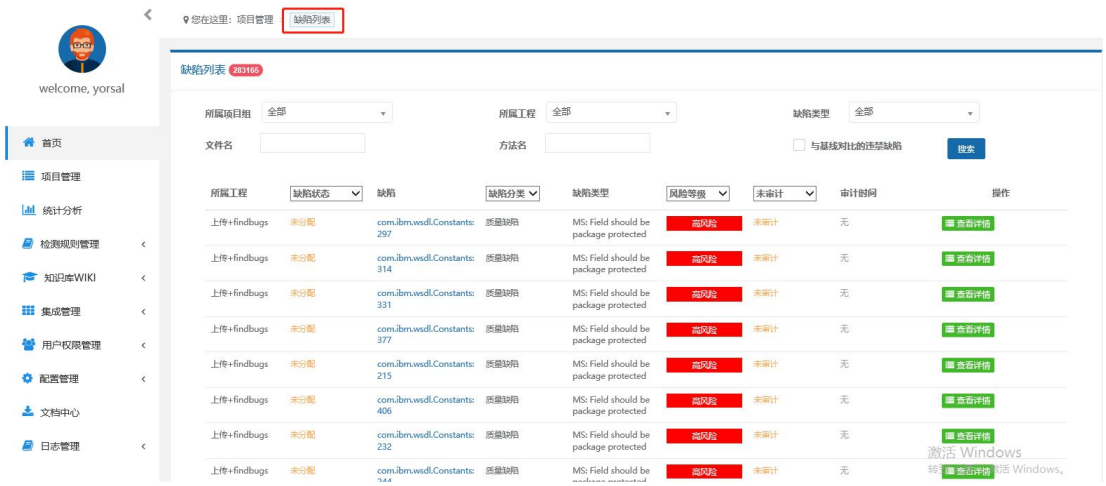
4. 可查看已检测项目总数，一致

2.4 发现的缺陷

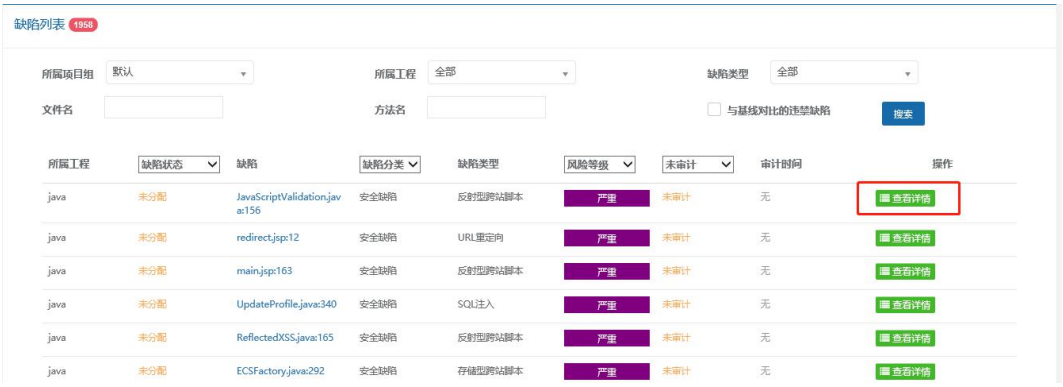
1. 需要审计：

1）点击首页“需要审计”右侧的数字

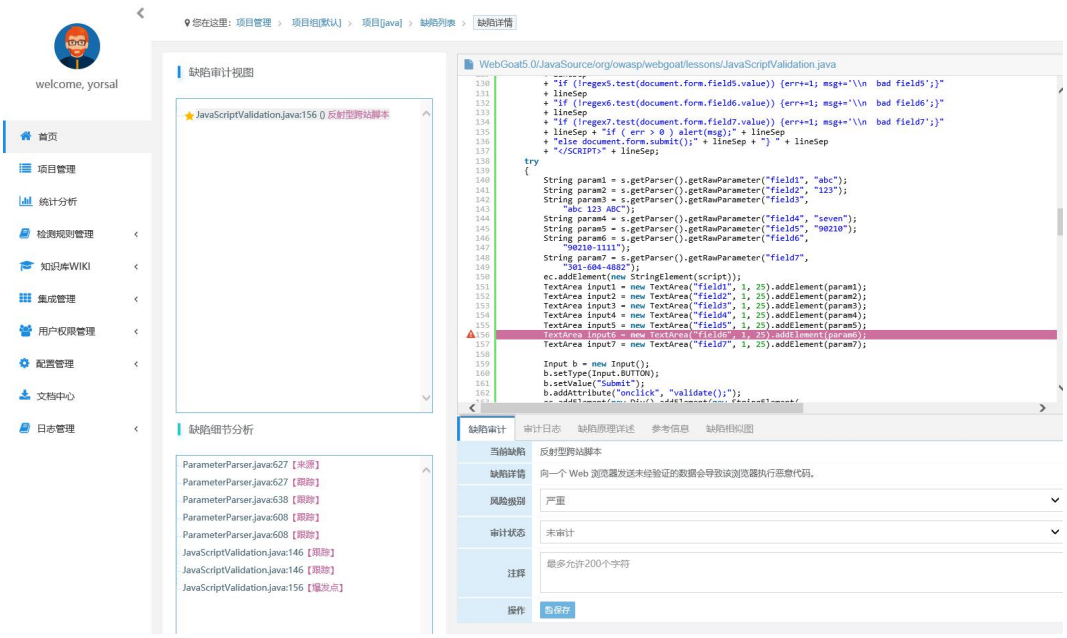
2）页面跳转缺陷列表页，显示出该用户下所有工程的未审计的缺陷，可通过查询条件（所属项目组、所属工程、缺陷类型、文件名、方法名），查询出相对应的缺陷，进入页面默认是显示全部



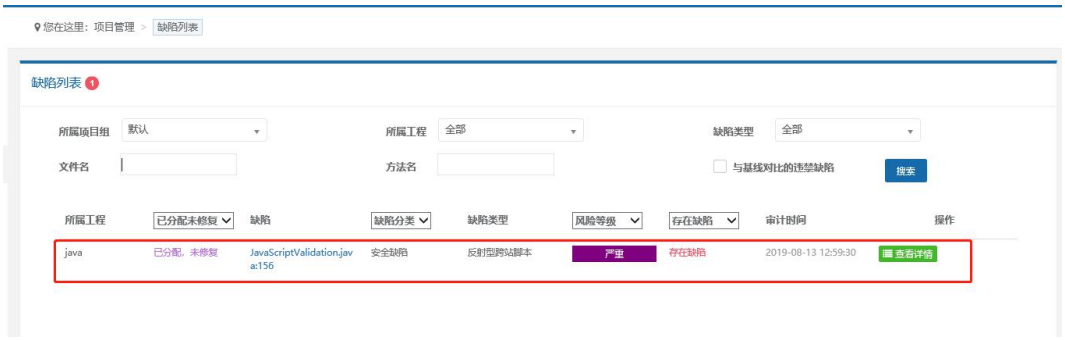
3）点击缺陷右侧的【查看详情】，可查看缺陷明细



4）进入到缺陷详情页，查看缺陷，可对缺陷进行缺陷审计



5）选择缺陷的风险级别、审计状态、分配人、优先级，点击【保存】按钮，弹出提示：保存成功，缺陷状态由“未分配”变成“已分配未修复”

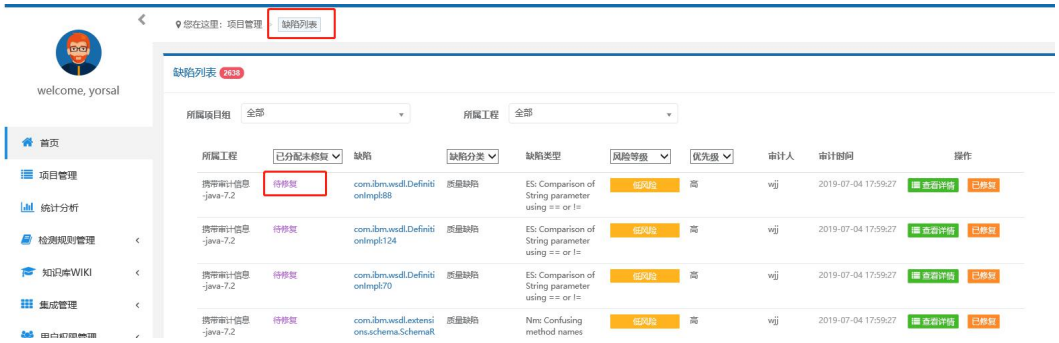


6）缺陷进入到分配人首页中“需要修复”中

2. 需要修复：

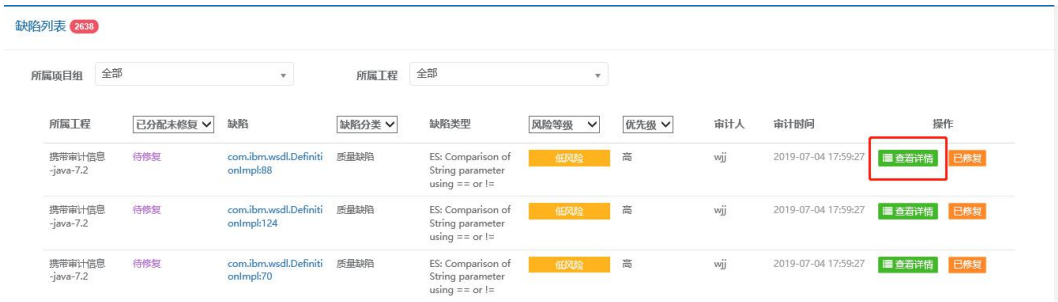
1）点击需要修复右侧的数字

2）进入到缺陷列表，显示出所有该用户待修复的缺陷

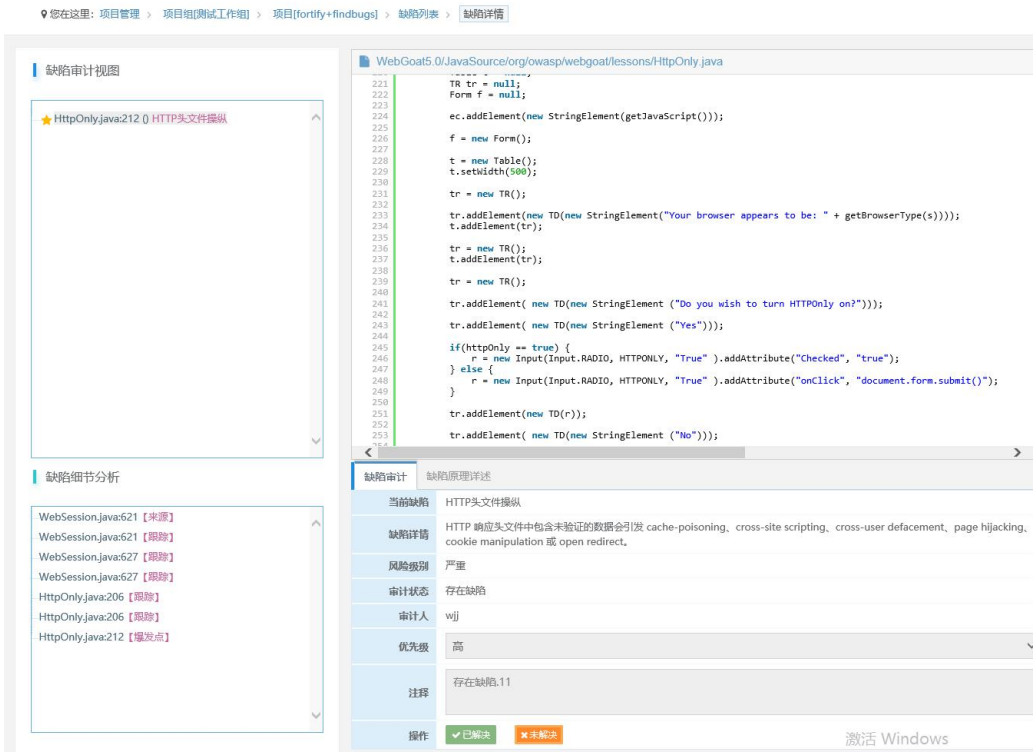


3）可直接点击【已修复】按钮，进行缺陷审计，进入提交缺陷人的“需要复审”中，状态为“已修复”

4）或者点击缺陷右侧的【查看详情】，可查看缺陷的详细信息



进入缺陷详情



5）进入到“缺陷详情”页，可对缺陷进行审计为“已解决”或“未解决”；

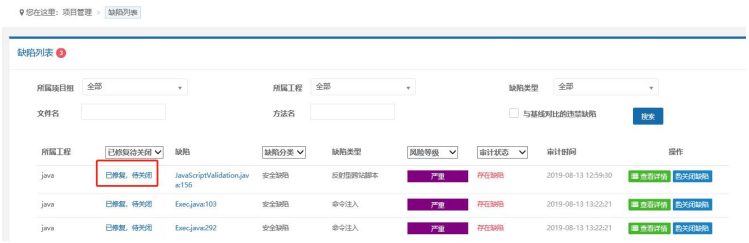
6）点击【已解决】或【未解决】，弹出提示：“更新成功”；点击【已解决】后缺陷状态变为“已修复，待关闭”，进入到提交缺陷人首页中的“需要复审”中；点击【未解决】缺陷状态不变

7）点击【已解决】后，进入需要复审中

3. 需要复审：

1）点击“需要复审”右侧的数字

2）进入到缺陷列表中，显示出该用户所有需要复审的缺陷

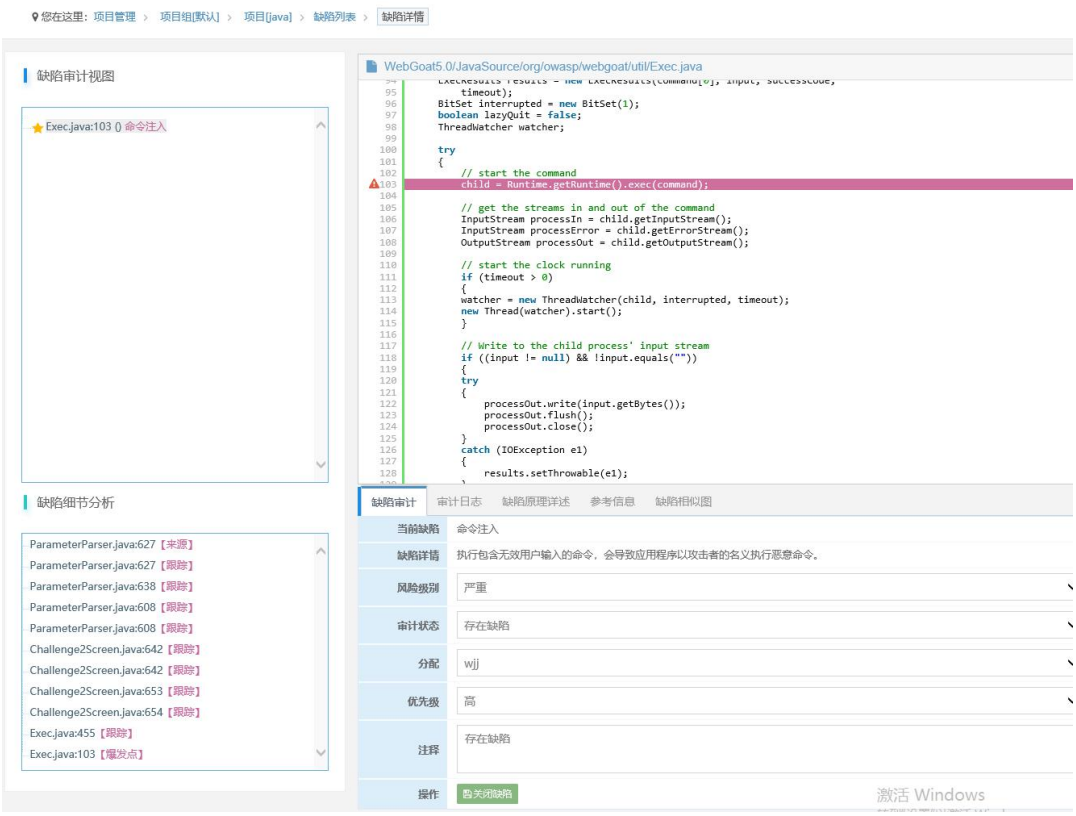


3）可直接点击缺陷右侧的【关闭缺陷】按钮，关闭缺陷

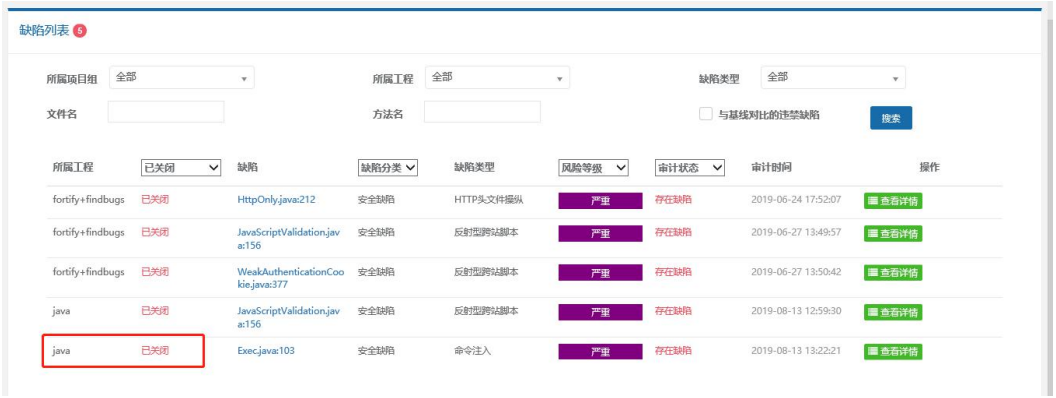
点击关闭缺陷，缺陷状态：已关闭

4）或点击【查看详情】，查看缺陷详情，可点击【关闭缺陷】按钮，关闭缺陷

5）点击进入详情页

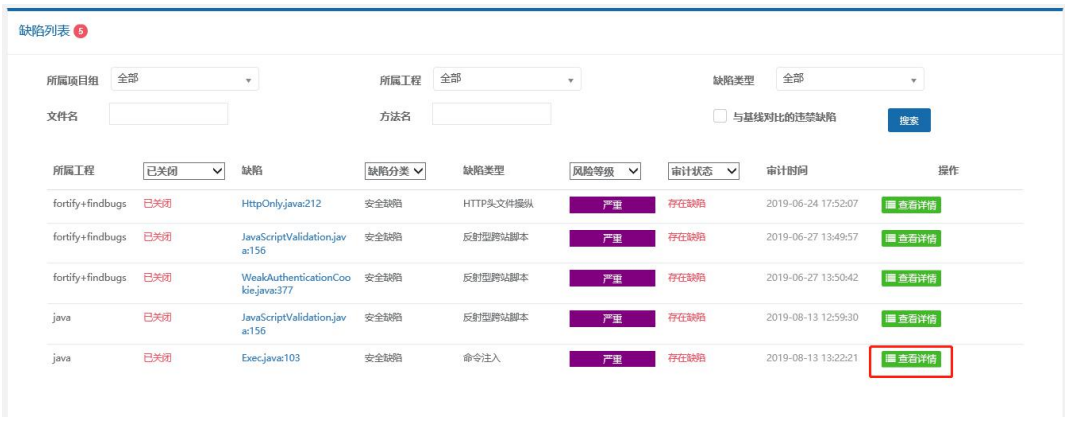


6）点击【关闭缺陷】，弹出提示：“操作成功”，缺陷状态改为：“已关闭”



4. 重新打开缺陷：

1）选择状态为“已关闭”的缺陷，点击【查看详情】，进入到缺陷详情页



2）在缺陷审计中，点击【重新打开缺陷】按钮

弹出提示：“操作成功”

3）缺陷进入到原来分配人首页中的“需要修复”中，缺陷状态由“已关闭”变为“待修复”

2.5 发现缺陷的等级

问题等级：与当前相关的缺陷严重程度的级别划分，其中严重级别最高，时效性最紧急，警告信息级别最低，可根据需求适当修复。

2.6 缺陷密度（按部门）

可查看各个部门中的缺陷密度

2.7 缺陷密度（按项目组）

可查看按项目组区分的缺陷密度

2.8 缺陷密度（按项目）

可查看不同项目之间的缺陷密度

缺陷密度(按项目)

测试3 JAVA 默认和 fortify	4284.76
testt	697.12
白名单	697.12
SVN-立检-更新建工程-非增量 (07-10.12：00)	479.4
SVN-立检-更新建工程-非增量 (07-10.15：00)	479.33

三、项目管理

3.1 新建及管理项目组

1.新建项目组：点击【新建项目组】按钮

规则：

1）项目组名称不能超过 20 个字符；

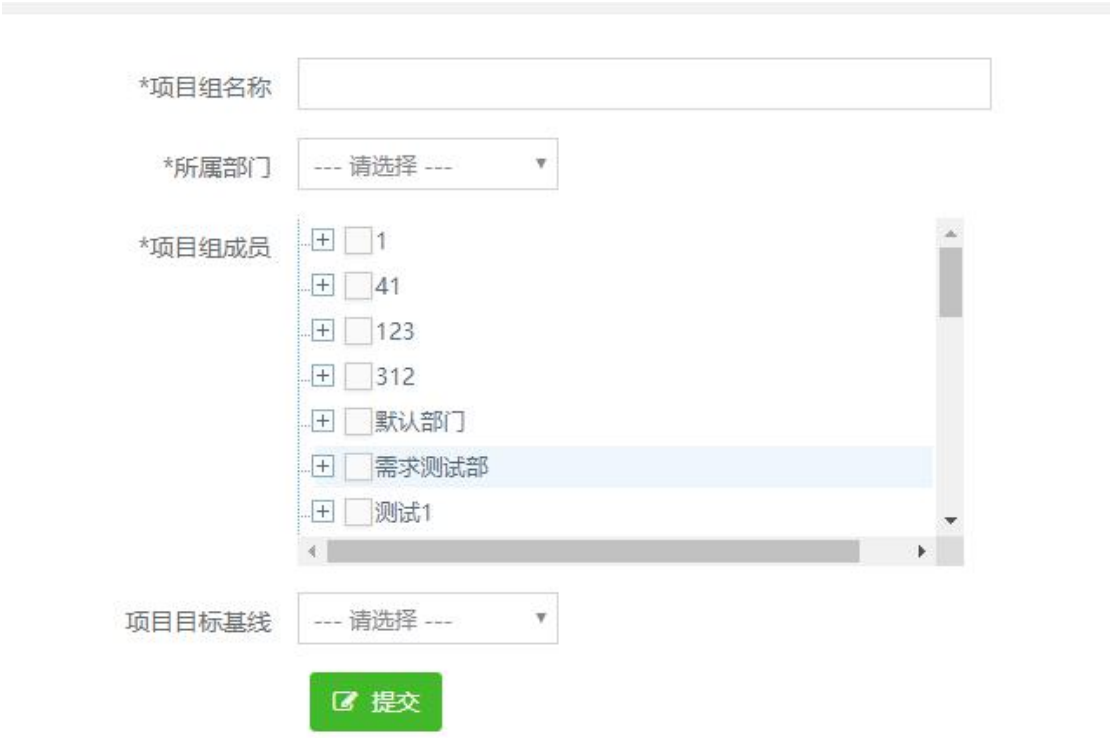
2）带*号的文本框为必填/选项，不能为空。

2.弹出新建项目组文本框，填写相关信息点击【提交】按钮，项目组新建成功

规则：

1）所属部门相当于牵头项目部门；

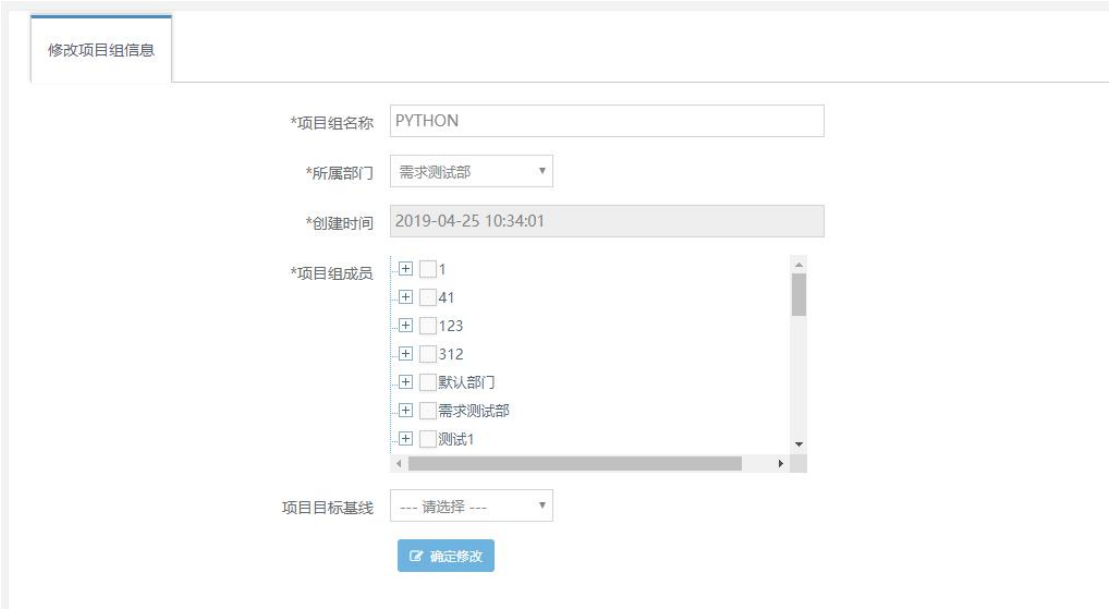
2）项目组成员：勾选了的部门成员才可看到相关项目组及工程，admin 都可看到。



3. 创建成功的项目组

4. 删除项目组，会把该项目组下的项目历次检测记录都删除。

5. 修改项目组，可以修改项目组的名称、所属部门、项目组所属成员、项目的目标基线。



3.2 创建

3.2.1 创建工程（上传）

1. 点击【创建】下拉框，选择工程（上传）

2. 弹出创建工程的文本框，必填项都输入，点击【上传源代码 zip 压缩包或 jar/war 包】按钮；

规则：

1） 工程名称：名称不能超过 50 个字符；

2） 版本或说明：自定义版本，不填默认 V1.0；

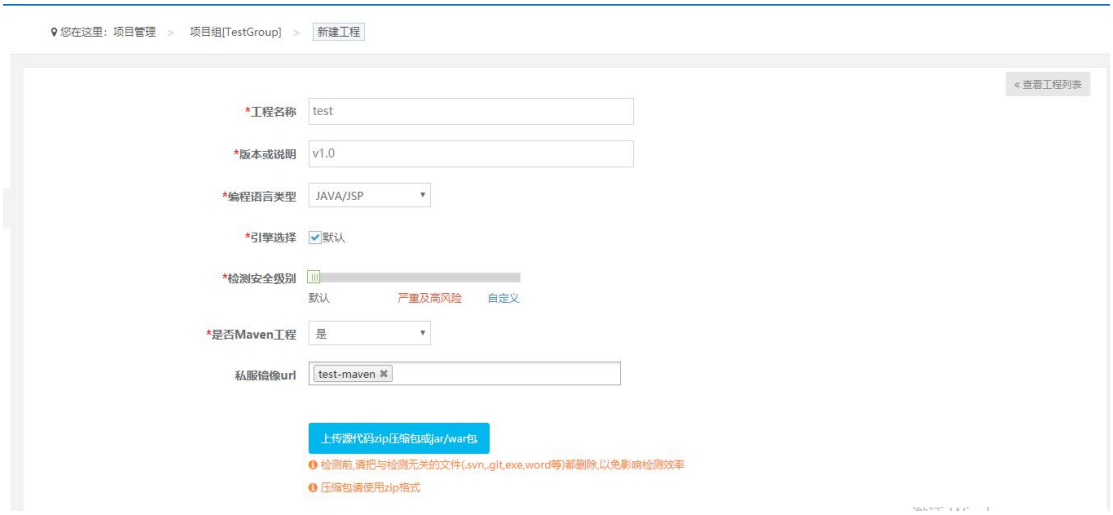
3） 引擎：默认

4） 语言：JAVA、C/C++、PYTHON、PHP、JAVASCRIPT；

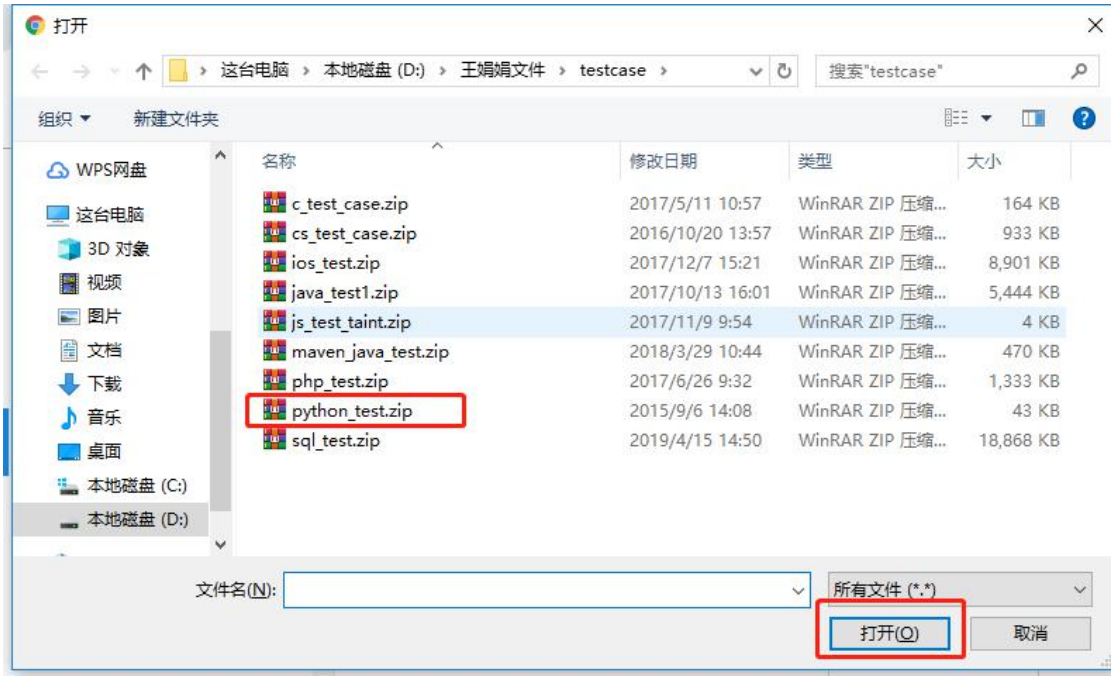
5） 检测安全级别：默认（系统默认）、严重及高风险（检测严重及高风险

的缺陷）、自定义（自己定义规则）；

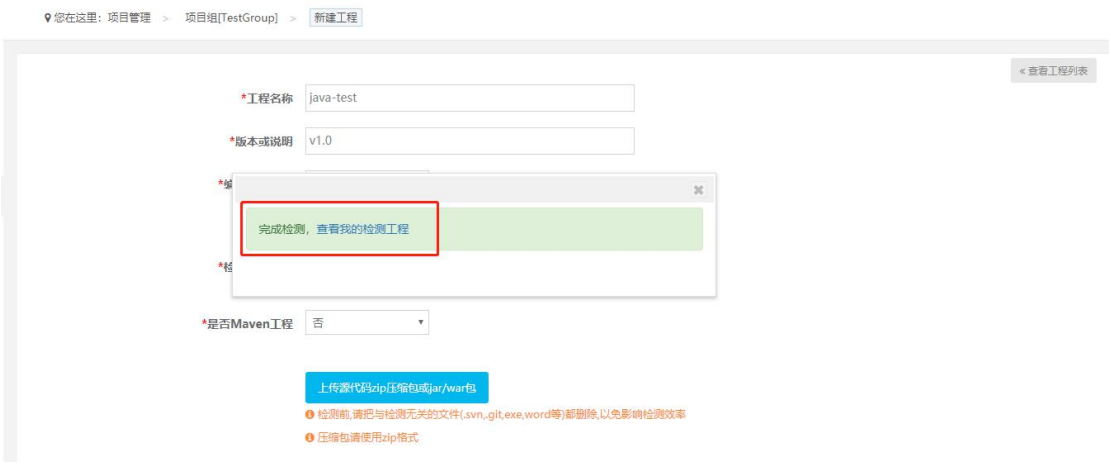
6） 是否 Maven 工程：默认“否”，选“是”时关联 maven 管理中创建的 maven 信息。



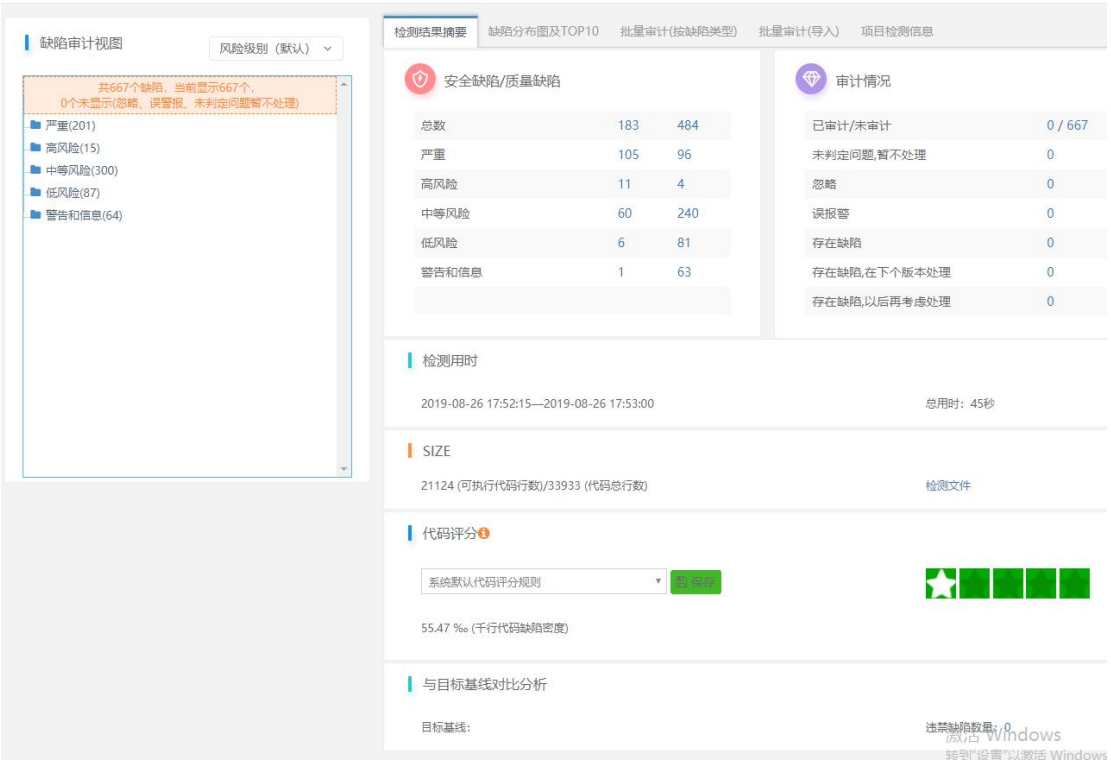
3. 弹出可选文本框，选择相对应的压缩包点击打开，进入上传



4. 创建完成后，点击“查看我的检测工程”



5. 进入该工程的检测详情页



备注：根据检测工程的大小、语言类型及硬件环境配置，检测时间会有不同。

3.2.2 创建工程（版本控制工具）

1. 创建工程：点击【创建】下拉框，选择工程（版本控制工具）

1）2.弹出创建工程的文本框，必填项都输入，点击【创建检测工程】按钮；

2）规则：

3）工程名称：不能超过 50 个字符；

4）版本或说明：自定义版本，不填默认为 v1.0；

5）编程语言：JAVA、C/C++、PYTHON、PHP、JAVASCRIPT；

6）引擎：默认；

7）安全级别：默认、严重及高风险、自定义；

8）检测时间：立即检测、自定时间检测；

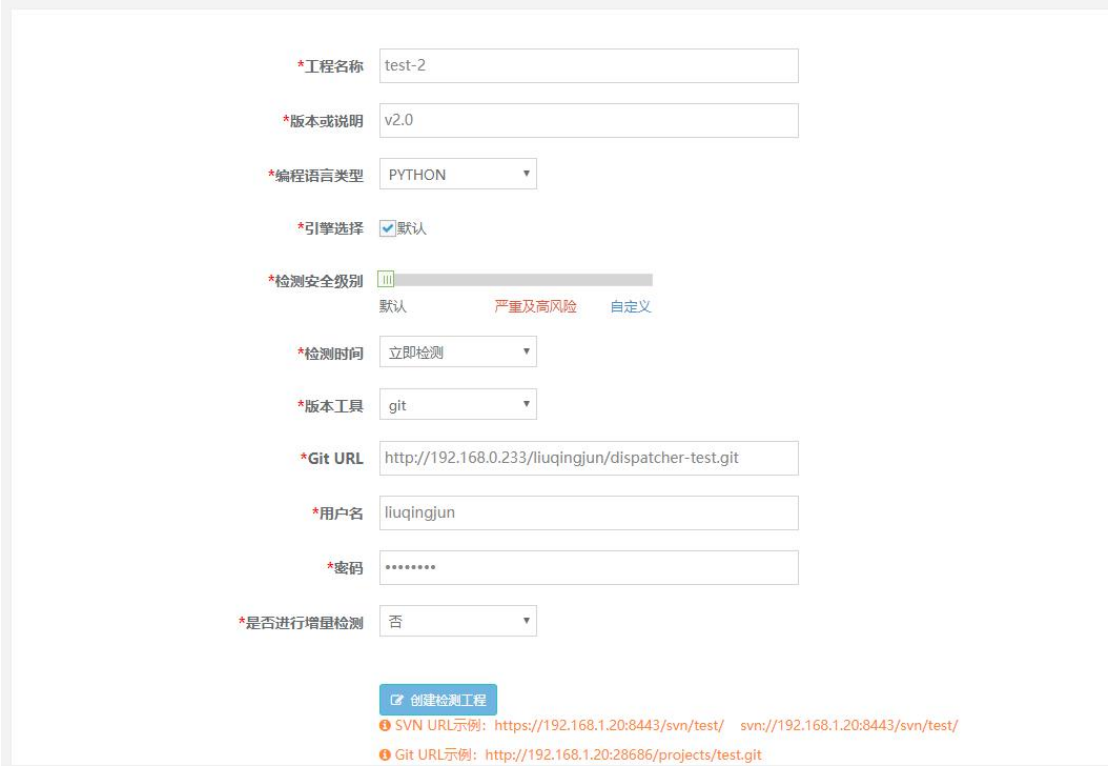
9）版本工具：可选择 Git 或 SVN；

8）Git URL：指定准确的项目路径；

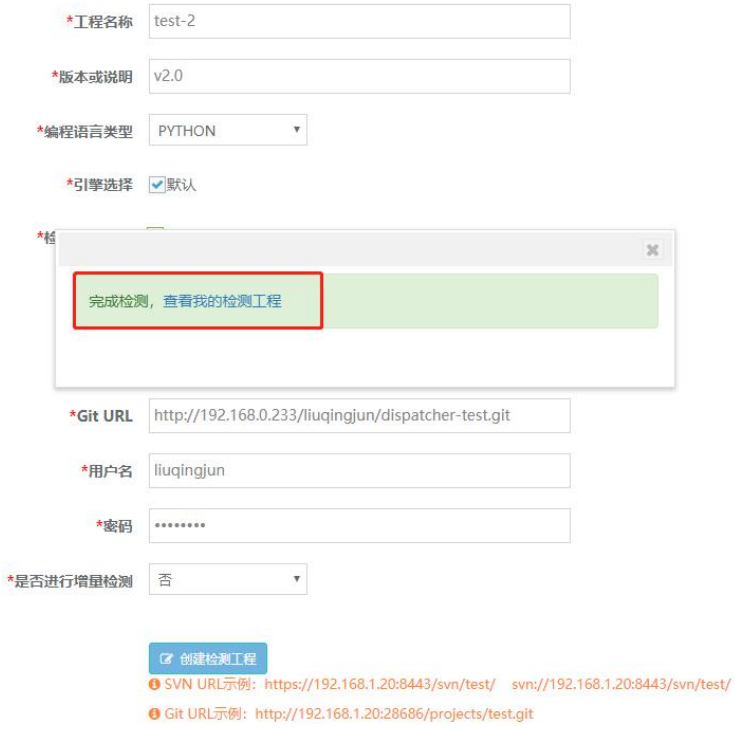
9）用户名：项目 Git 或 SVN 的用户名；

10）密码：项目 Git 或 SVN 的密码；

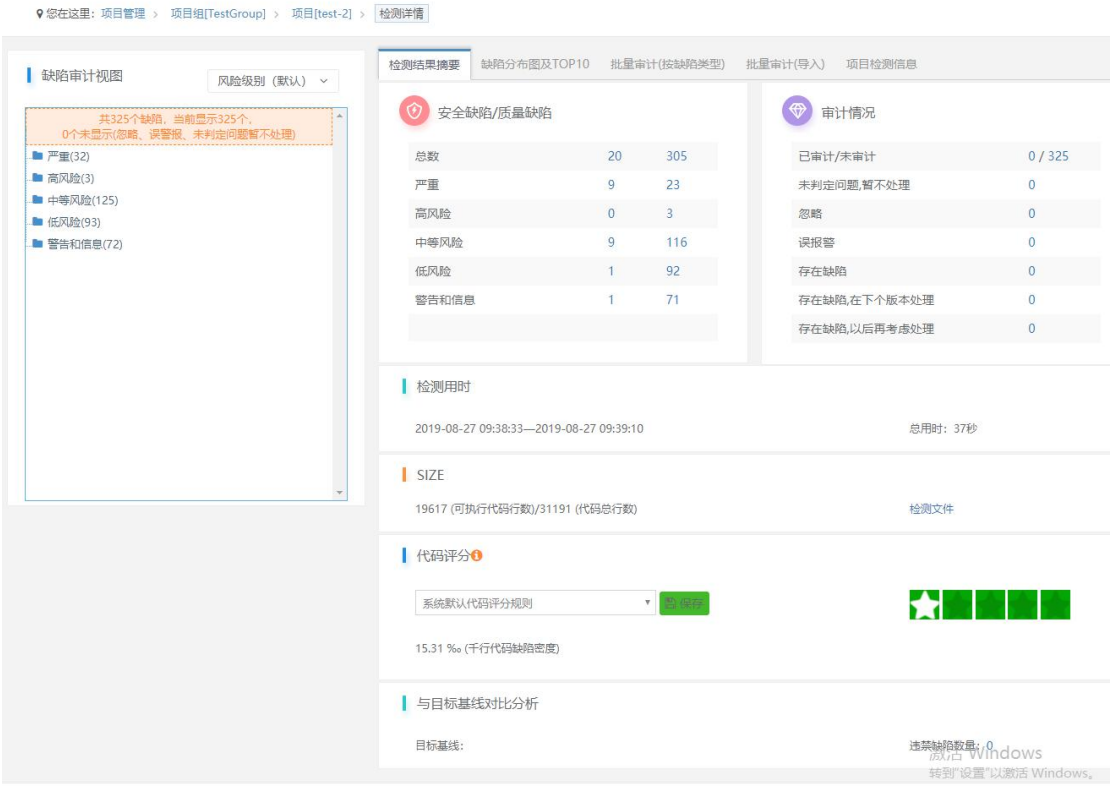
11）是否进行增量检测：选择“否”检测时检测全部，选择“是”检测时只检测新增部分。



3）创建完成后，点击“查看我的检测工程”



4）进入到该工程的检测详情页，可查看工程的检测结果摘要、缺陷分布图及 TOP10、批量审计（按缺陷类型）、批量审计（导入）、项目检测信息等。



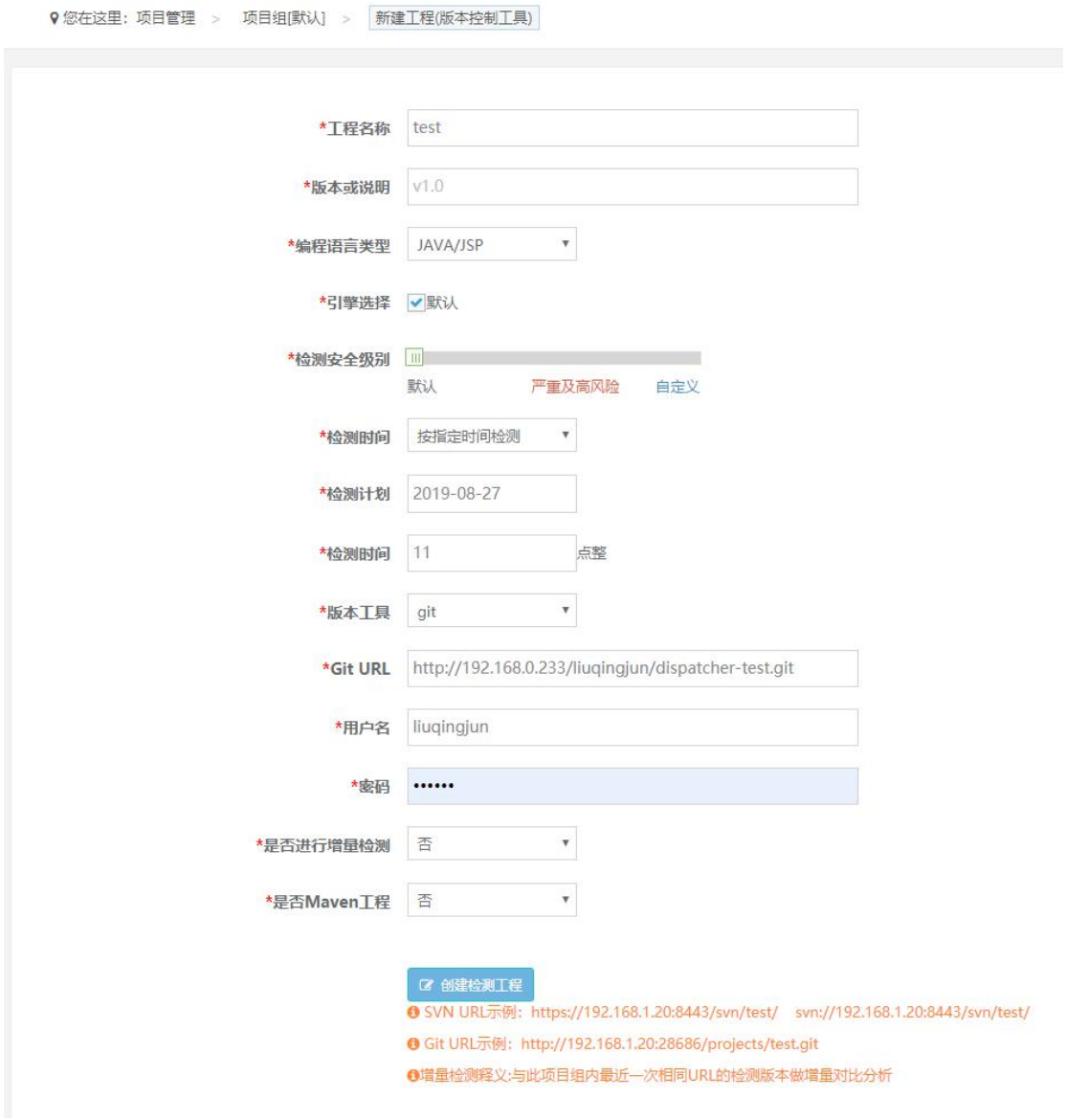
2. 创建“指定时间检测”工程

1）进入创建工程（版本控制）页面，输入必填项，点击【创建检测工程】按钮；

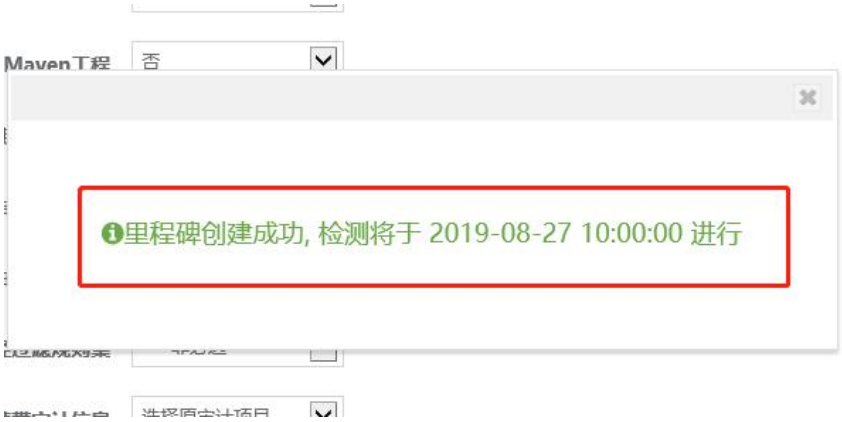
规则：

检测时间：按指定时间检测；

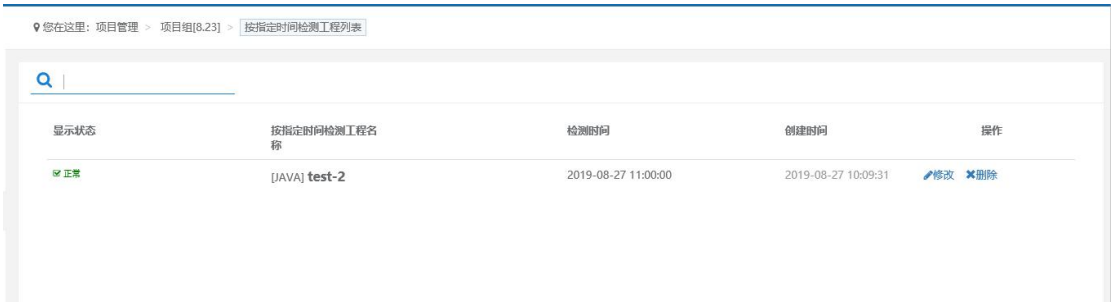
检测计划：时间大于等于当前日期；


您在这里：项目管理 > 项目组[默认] > 新建工程(版本控制工具)
*工程名称
test
*版本或说明
v1.0
*编程语言类型
JAVA/JSP
*引擎选择
默认
*检测安全级别
默认
严重及高风险
自定义
*检测时间
按指定时间检测
*检测计划
2019-08-27
*检测时间
11
点整
*版本工具
git
*Git URL
http://192.168.0.233/liuqingjun/dispatcher-test.git
*用户名
liuqingjun
*密码
*是否进行增量检测
否
*是否Maven工程
否
创建检测工程
SVN URL示例：https://192.168.1.20:8443/svn/test/ svn://192.168.1.20:8443/svn/test/
Git URL示例：http://192.168.1.20:28686/projects/test.git
增量检测释义:与此项目组内最近一次相同URL的检测版本做增量对比分析

2）检测完成后弹出提示

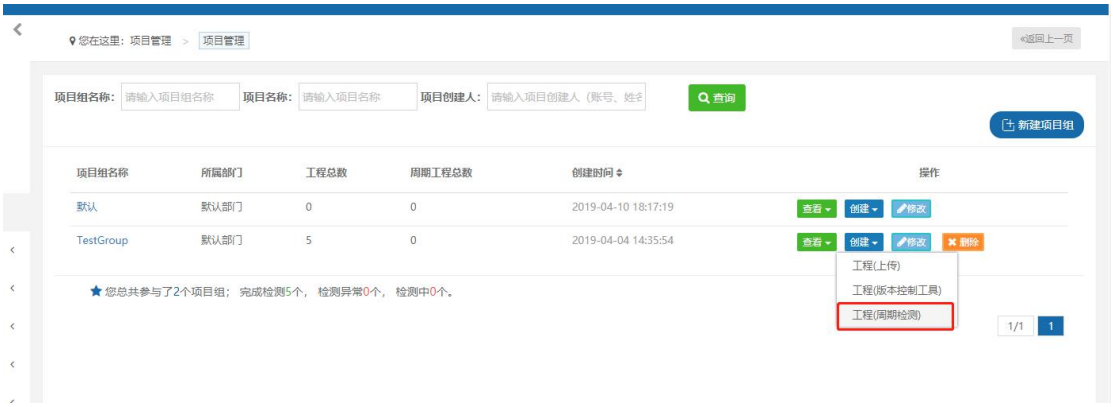

Maven工程
否
里程碑创建成功, 检测将于 2019-08-27 10:00:00 进行

3）创建完成后，进入到【查看】-【按指定时间检测工程】中，待到检测时间开始检测，检测完成后工程进入到了【工程列表】中。



3.2.3 创建周期工程

1. 选择“周期工程”

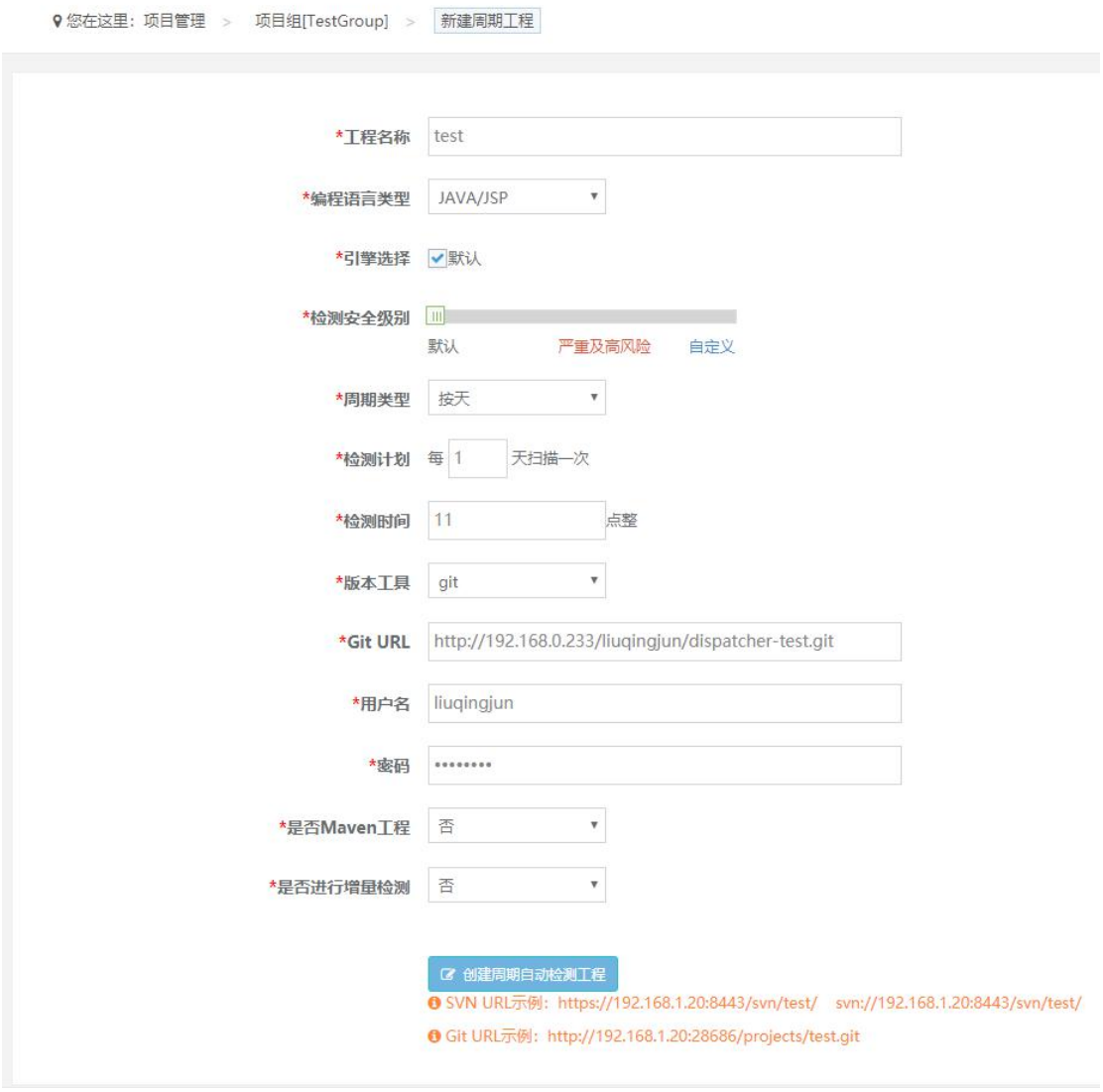


2. 页面进入到填写周期工程页面

规则：

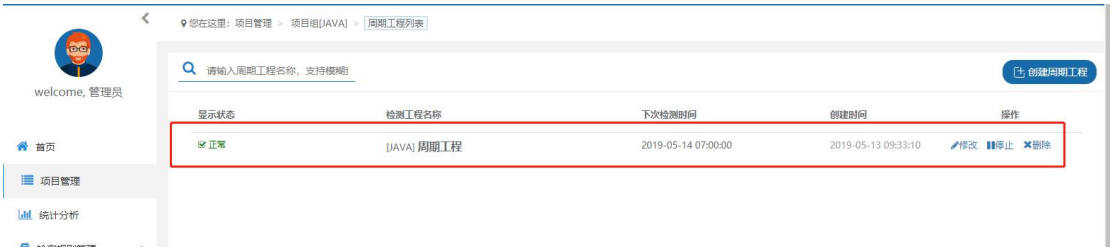
1）周期类型：按天（每隔几天扫描）、按周（每周周几扫描）、按月（每月哪几天扫描）；

2）扫描时间：0-23 整点。



3. 填写必填项后，点击【创建周期自动检测工程】按钮

4. 创建完成，查看工程

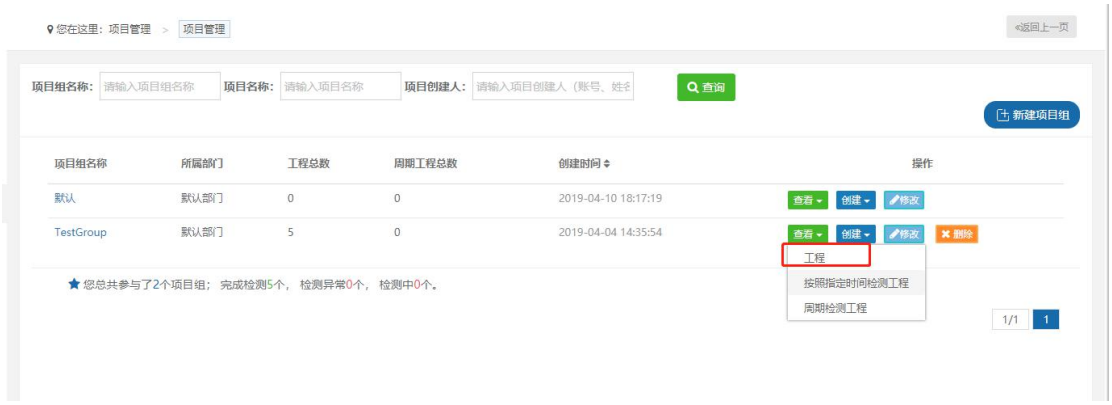


备注：创建成功后，可对该工程进行修改、停止、删除操作

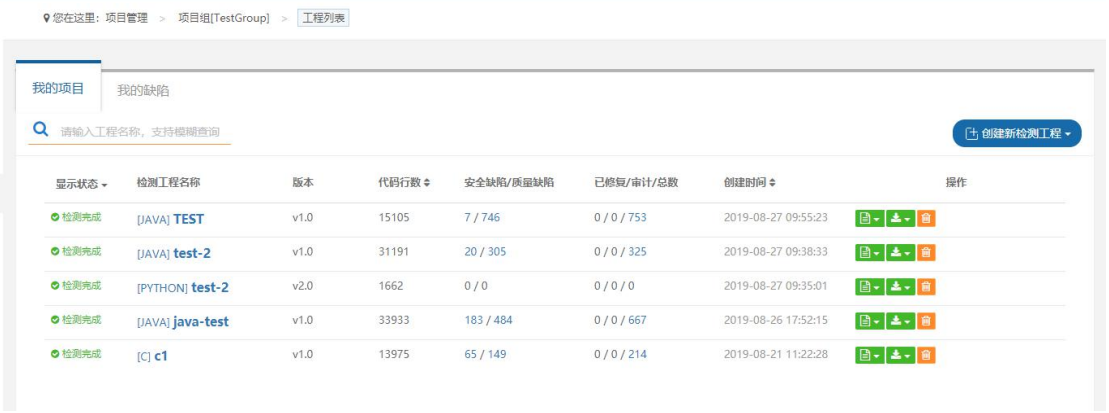
3.3 查看

3.3.1 查看工程

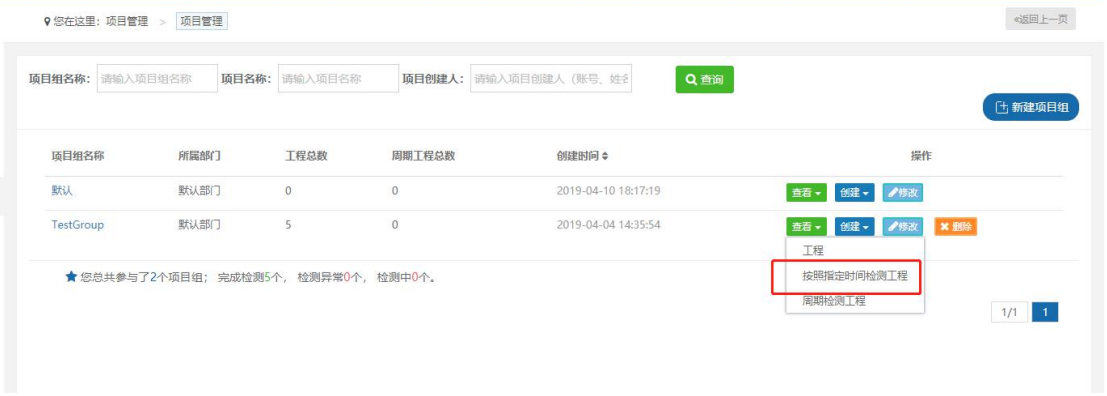
1. 工程的查看，点击【查看】-【工程】，或者点击项目组名称



进入工程列表页面，查看该项目组下的所有工程

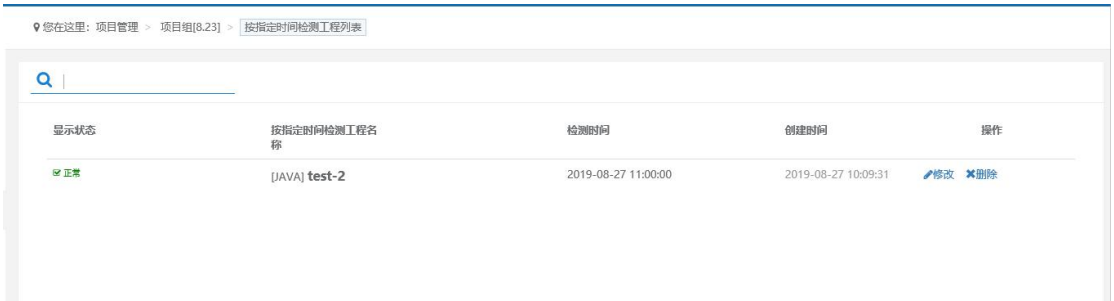


2. 按照指定时间检测工程的查看



进入到“指定时间检测工程列表”页，可对工程进行修改和删除。

备注：周期指定时间检测工程按照周期检测完成后，相当于一个工程进入到工程中，我的项目中工程数量会增加，在周期工程中的数量将减少。



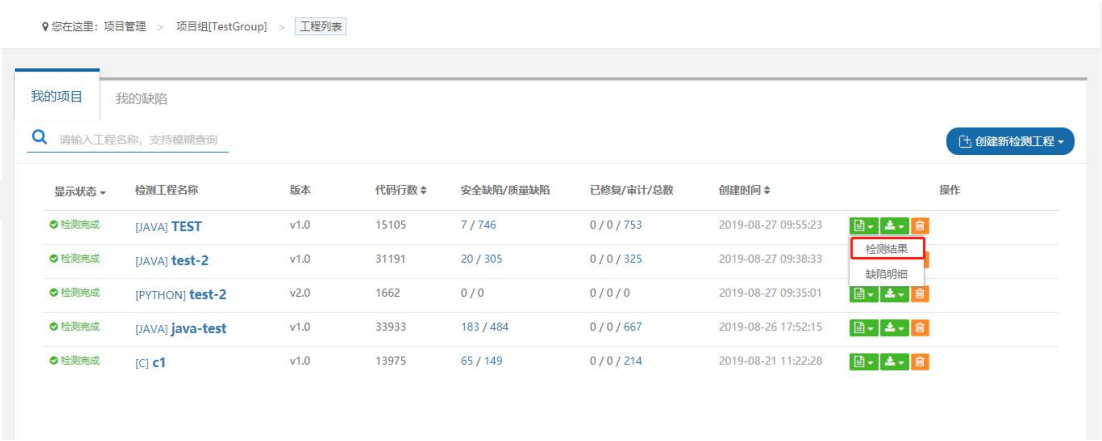
3. 周期工程的查看，点击【查看】-【周期检测工程】，可查看该项目组中的所有周期工程

进入到周期工程列表页，可对周期工程进行修改和删除的操作。

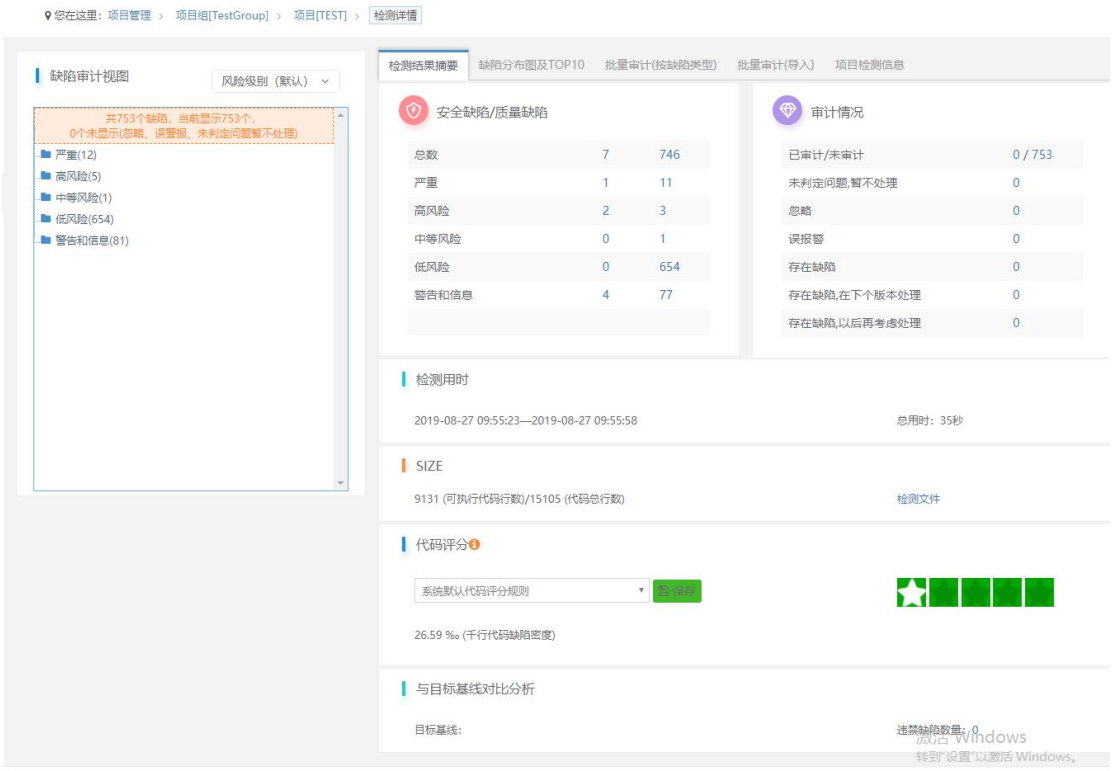
备注：周期工程按照周期检测完成后，相当于一个工程进入到工程中，我的项目中工程数量会增加，在周期工程中的数量将减少。

3.3.2 工程检测结果

1. 选择工程点击右侧【检测结果】按钮

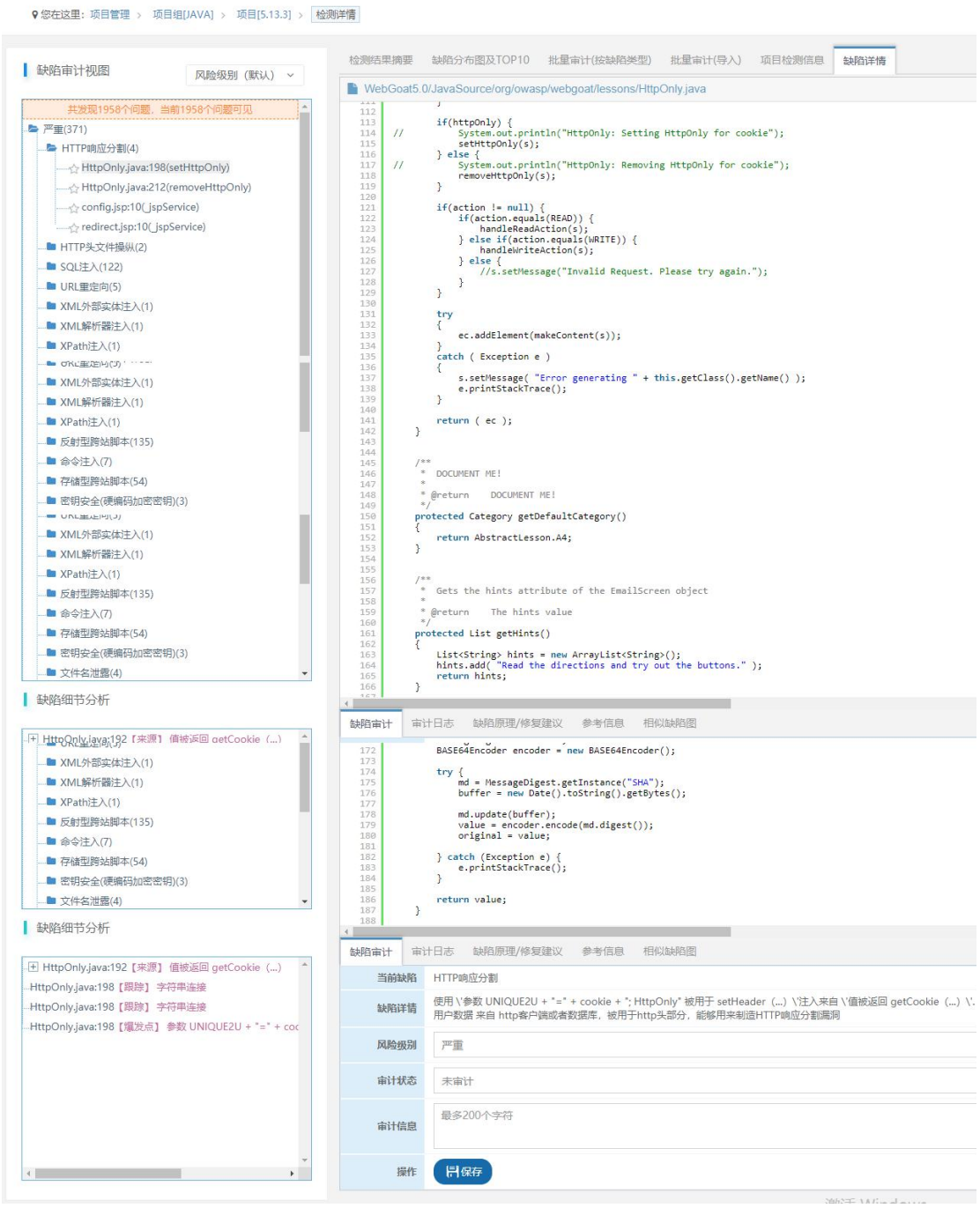


2. 进入检测详情页

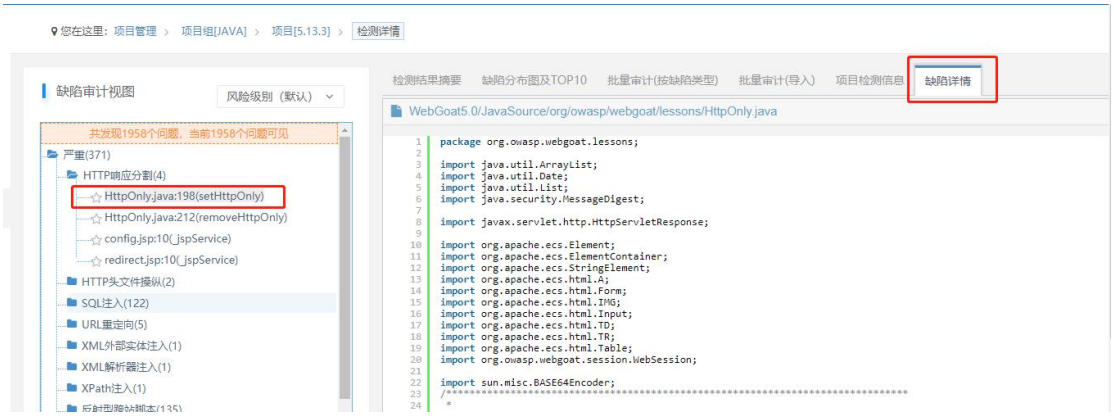


3. 可以通过不同选择查看缺陷，默认是风险级别，还有缺陷类型（一级）、缺陷类型（二级）、审计状态、修复状态、安全/质量等查看

4. 点击一条缺陷，可以查看其详情，也可在下方将该缺陷指派给相关人员解决


您在这里：项目管理 > 项目组[JAVA] > 项目[5.13.3] > 检测详情
缺陷审计视图
风险级别（默认）
共发现1958个问题，当前1958个问题可见
严重(371)
HTTP响应分割(4)
HttpOnly.java:198(setHttpOnly)
HttpOnly.java:212(removeHttpOnly)
config.jsp:10(_jspService)
redirect.jsp:10(_jspService)
HTTP头文件操纵(2)
SQL注入(122)
URL重定向(5)
XML外部实体注入(1)
XML解析器注入(1)
XPath注入(1)
反射型跨站脚本(135)
命令注入(7)
存储型跨站脚本(54)
密钥安全(硬编码加密密钥)(3)
文件名泄露(4)
缺陷细节分析
HttpOnly.java:192【来源】值被返回 getCookie（...）
HttpOnly.java:198【跟踪】字符串连接
HttpOnly.java:198【跟踪】字符串连接
HttpOnly.java:198【爆发点】参数 UNIQUE2U + "=" + coc
检测结果摘要
缺陷分布图及TOP10
批量审计(按缺陷类型)
批量审计(导入)
项目检测信息
缺陷详情
WebGoat5.0/JavaSource/org/owasp/webgoat/lessons/HttpOnly.java
缺陷审计
审计日志
缺陷原理/修复建议
参考信息
相似缺陷图
当前缺陷
HTTP响应分割
缺陷详情
使用 \"参数 UNIQUE2U + "=" + cookie + "; HttpOnly" 被用于 setHeader（...）\"注入来自 \"值被返回 getCookie（...）\"。用户数据 来自 http客户端或者数据库，被用于http头部分，能够用来制造HTTP响应分割漏洞
风险级别
严重
审计状态
未审计
审计信息
最多200个字符
操作
保存

（1）缺陷详情

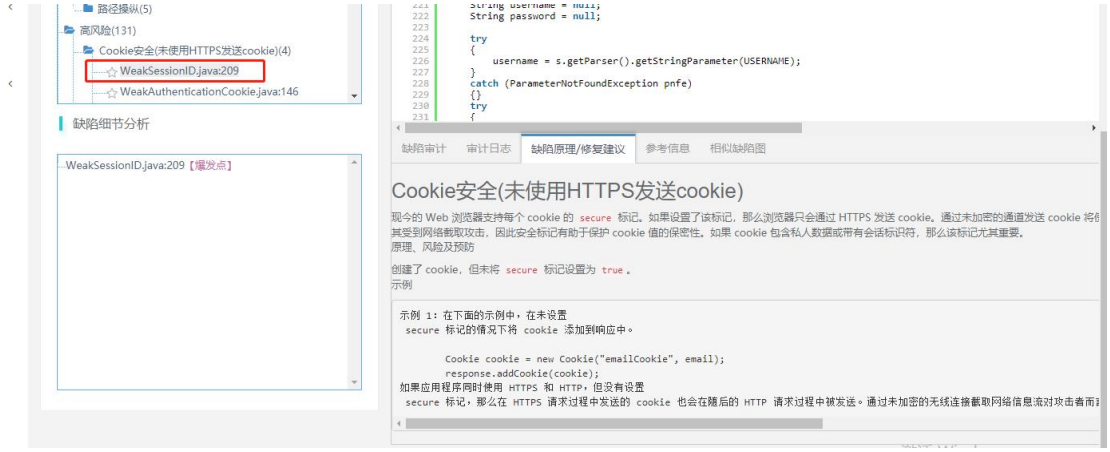


（2）缺陷审计：可以指派缺陷给相关解决人员，点击【保存】提交成功，在被指派人首页的“发现的缺陷”处可以查看到

被指派人首页：需要修复信息

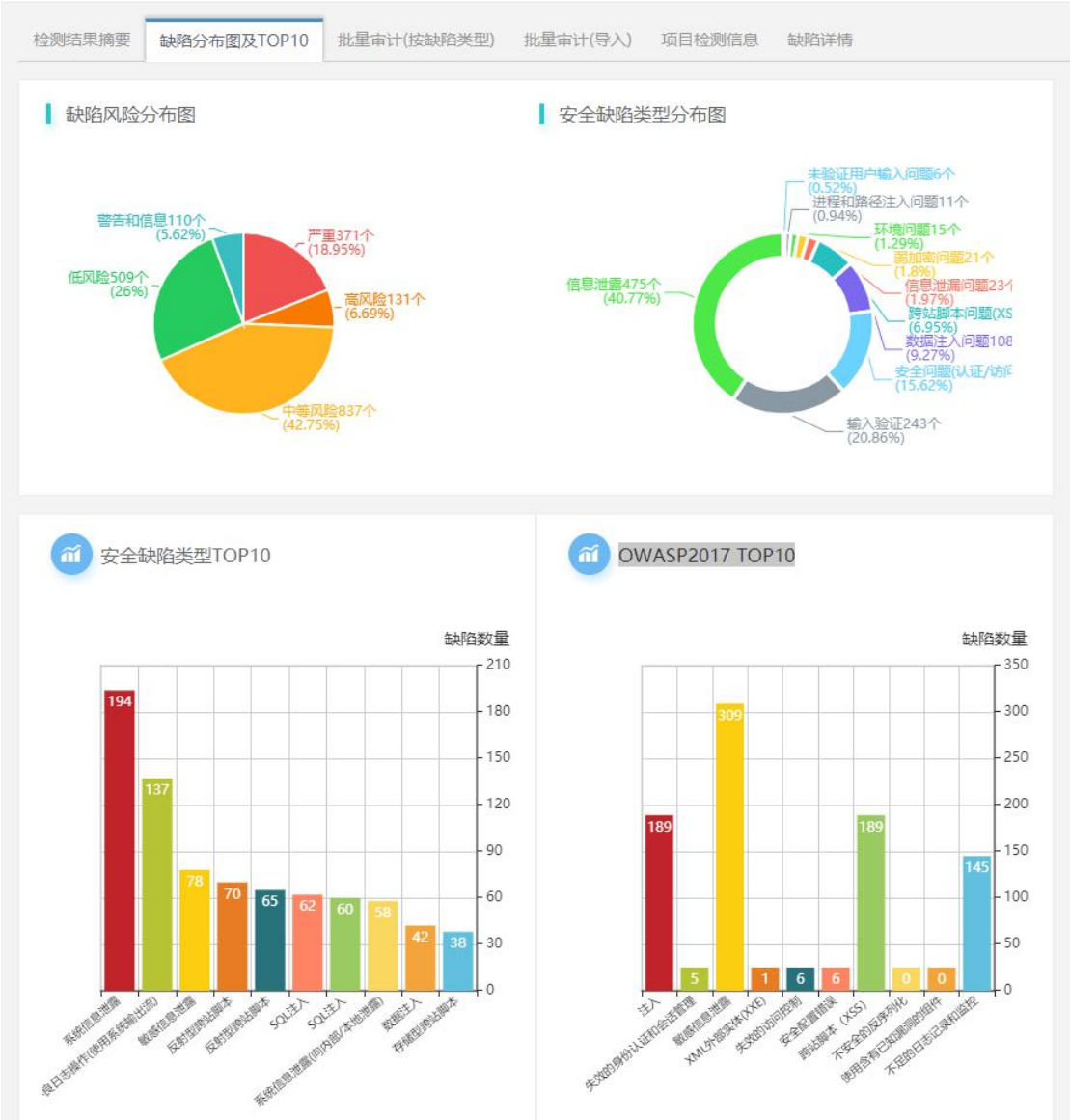
（3）审计日志：查看该条缺陷的审计人、审计时间、风险级别、审计状态、分配人、优先级等信息。

（4）缺陷原理/修复建议：给出缺陷的原理及修复的建议



5. 检测结果摘要：展示出安全缺陷/质量缺陷、缺陷的审计情况、检测用时、SIZE、代码评分等。

6.缺陷分布图 TOP10：缺陷风险分布图、安全缺陷类型分布图、安全缺陷类型 TOP10、OWASP2017 TOP10



7. 批量审计（按缺陷类型）：可以批量的指派缺陷。

1）筛选条件：

风险级别：严重、高风险、中等风险、低风险、警告和信息；

缺陷类型：工程中按风险级别划分的缺陷类型；

审计状态：未审计（默认）、未判定问题暂不处理、忽略、误报警、存在缺陷、存在缺陷，在下个版本处理、存在缺陷，以后再考虑处理；

操作：点击【查询】按钮可查询出条件缺陷。

2）批量审计：

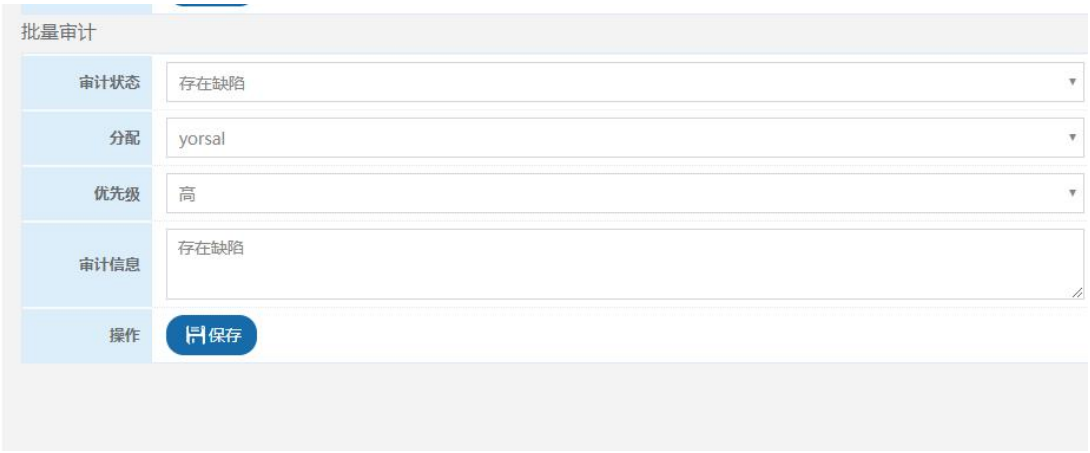
审计状态：未审计（默认）、未判定问题暂不处理、忽略、误报警、存在缺陷、存在缺陷，在下个版本处理、存在缺陷，以后再考虑处理；

分配：项目组成员；

优先级：高、中、低；

审计信息：可自定义；

操作：点击【保存】按钮，审计成功。



备注：

审计状态为：未判定问题暂不处理、忽略、误报警这三种提交的缺陷，在“缺陷审计视图”中提交后该缺陷不可见。

审计状态为：存在缺陷、存在缺陷，在下个版本处理、存在缺陷，以后再考虑处理，这三种提交后，在“缺陷审计视图”中提交后该缺陷不可见。

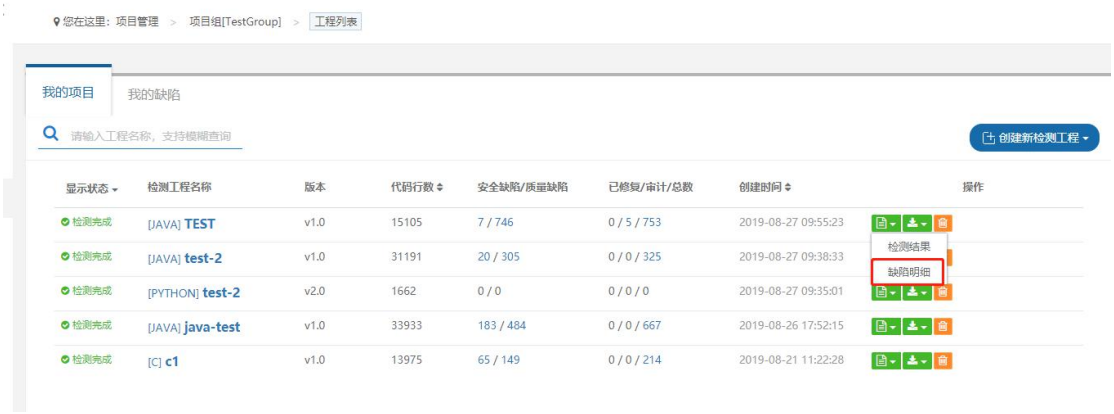
8. 批量审计（导入）

9. 项目检测信息

记录项目导入时的关键信息：项目名称、上传文件名称、检测时间、编程语言类型、检测安全级别、创建人等。

3.3.3 缺陷明细

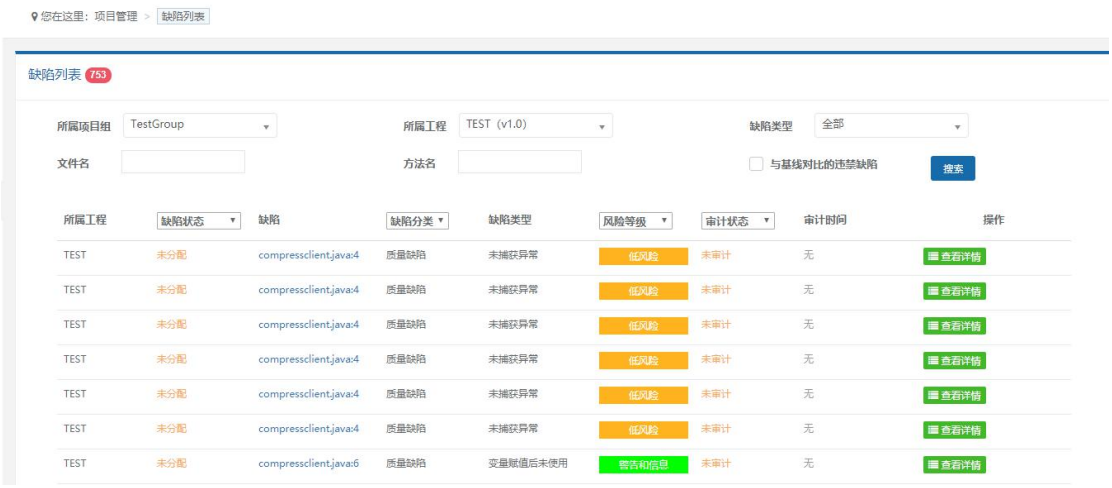
1. 选择工程，点击右侧的【缺陷明细】按钮



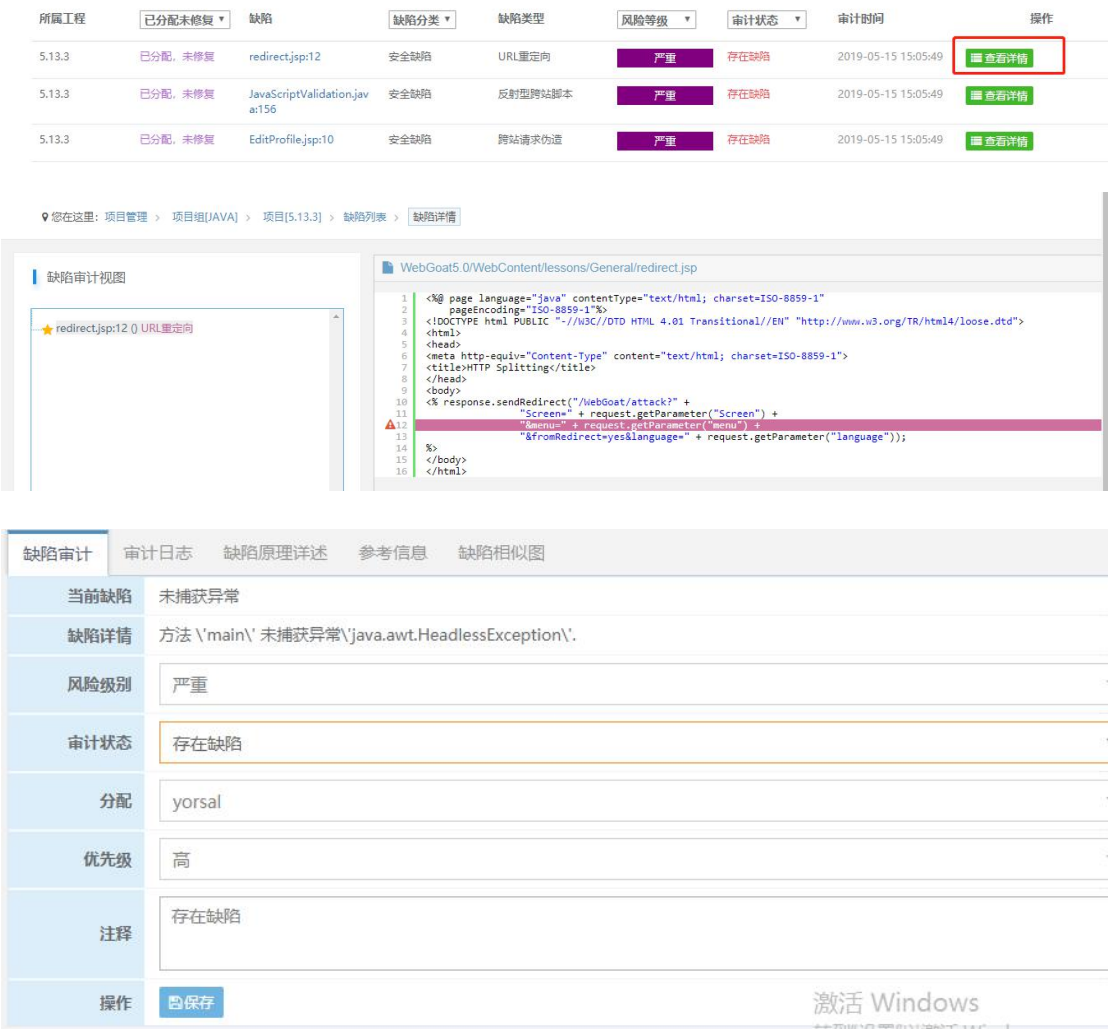
2. 进入缺陷列表

可通过所属项目组、所属工程、缺陷类型、文件名、方法名来查询

也可通过缺陷状态、缺陷分类、风险等级、审计状态来筛选缺陷



点击【查看详情】按钮，可以查看缺陷的详细信息，也可对缺陷进行指派，指派的缺陷进入到指派人的【首页】-【发现的缺陷】-【需要修复】中。



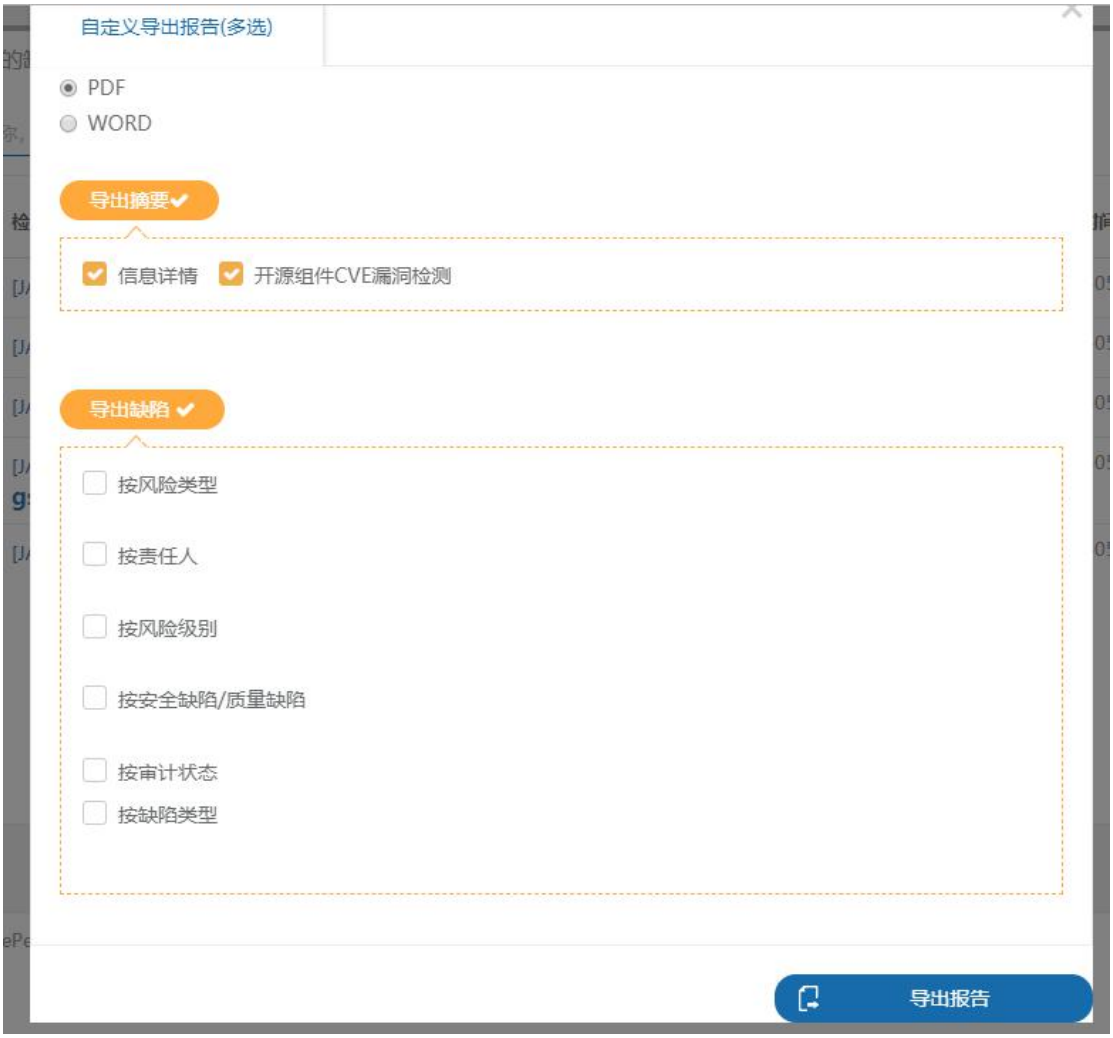
3.3.4 导出报告

1. 导出报告的格式：PDF、Word、Excel、自定义导出报告

2. 自定义导出报告：

可选两个格式 PDF 和 Word；

可勾选导出摘要和导出缺陷，导出摘要和导出缺陷不能都不勾选；



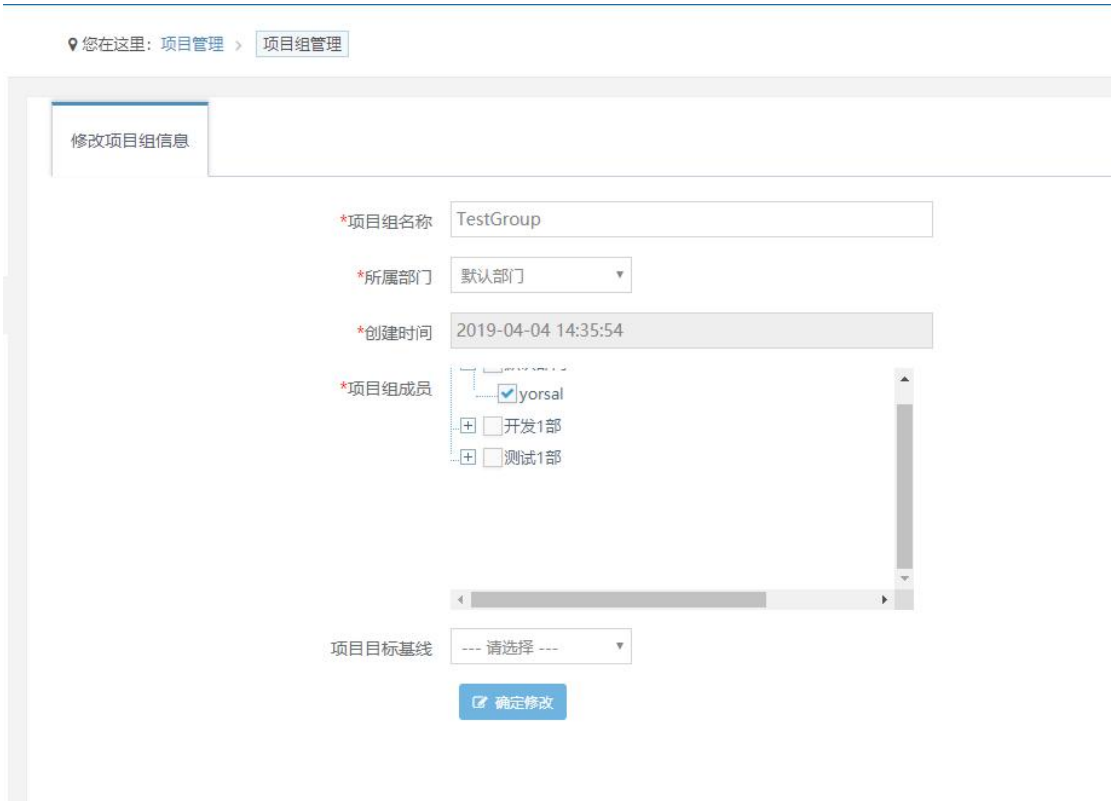
3.3.4 删除

该删除是将上传的工程删除

3.4 修改/删除

1. 修改项目组

2. 可修改项目组名称、所属部门、项目组成员、项目目标基线



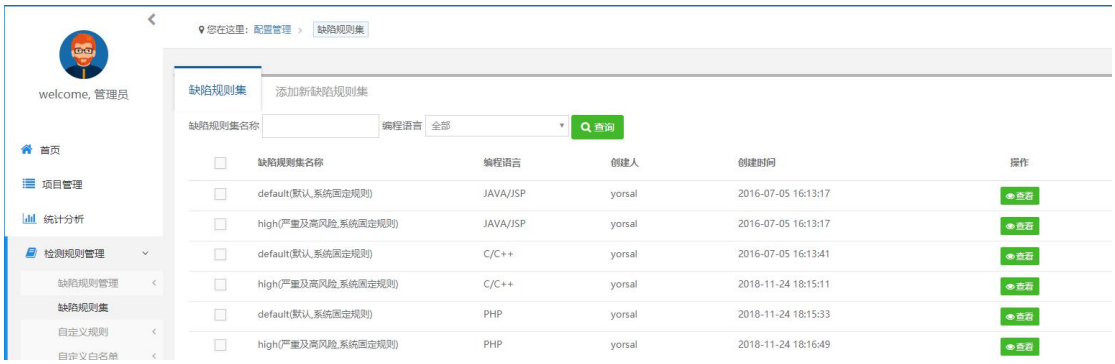
3. 删除

删除项目组，及可将项目组中的所有工程也删除

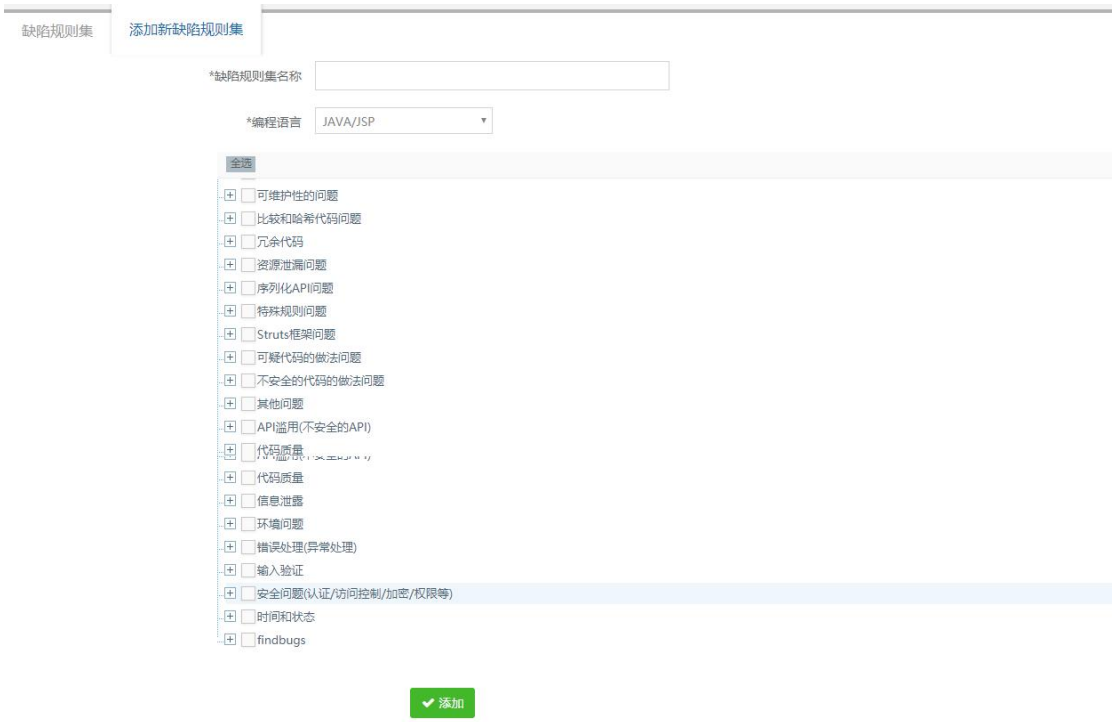
四、检测规则管理

4.1 缺陷规则集

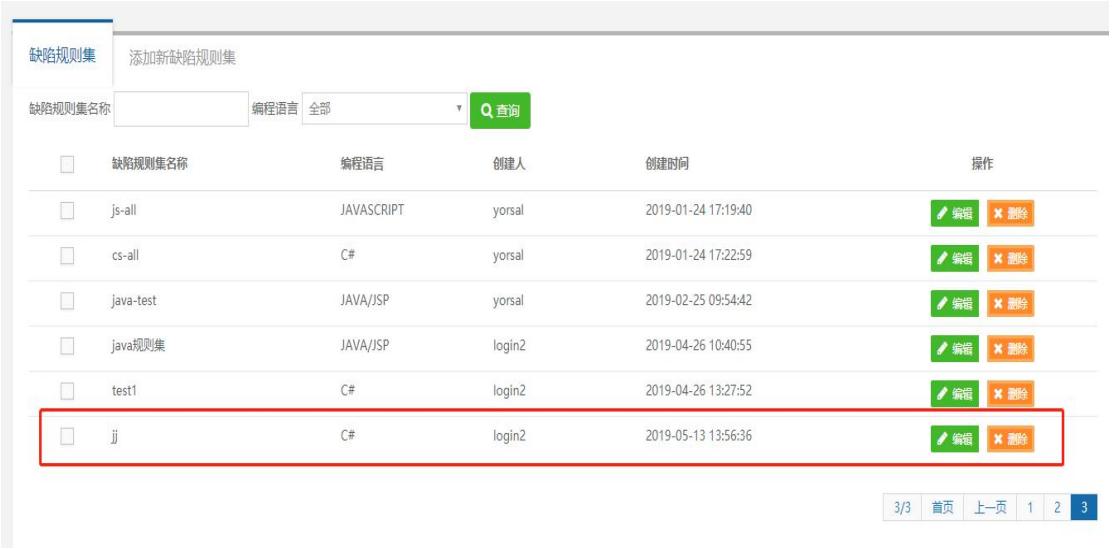
1. 系统自带的规则集，只可查看，不可修改和删除



2. 添加新的规则集，输入缺陷规则集名称，勾选其规则，点击【保存】按钮



3. 新添加的规则集在最末页，可对新添加的规则集进行修改和删除的操作。


缺陷规则集
添加新缺陷规则集
缺陷规则集名称
编程语言
全部
查询
缺陷规则集名称
编程语言
创建人
创建时间
操作
js-all
JAVASCRIPT
yorsal
2019-01-24 17:19:40
cs-all
C#
yorsal
2019-01-24 17:22:59
java-test
JAVA/JSP
yorsal
2019-02-25 09:54:42
java规则集
JAVA/JSP
login2
2019-04-26 10:40:55
test1
C#
login2
2019-04-26 13:27:52
jj
C#
login2
2019-05-13 13:56:36
编辑
删除
3/3
首页
上一页
1
2
3

五、知识库 WIKI

功能介绍：关于各种语言的缺陷明细，可通过查询条件一级缺陷、二级缺陷查询缺陷明细。

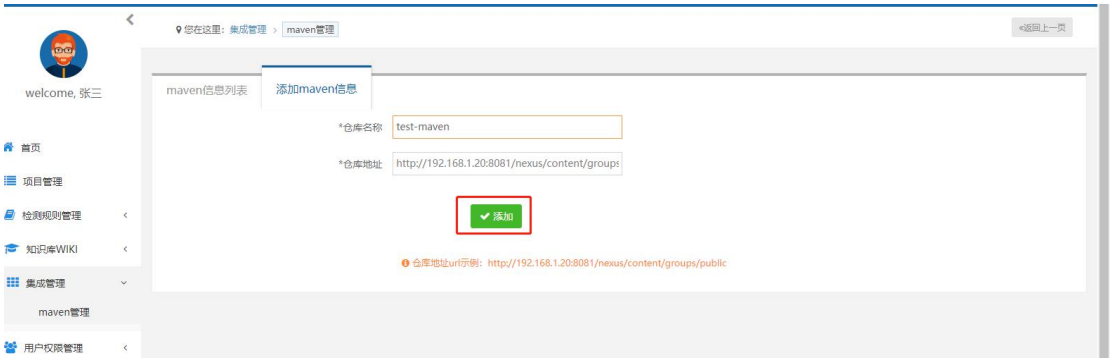
输入查询条件查看具体缺陷详情。

六、集成管理

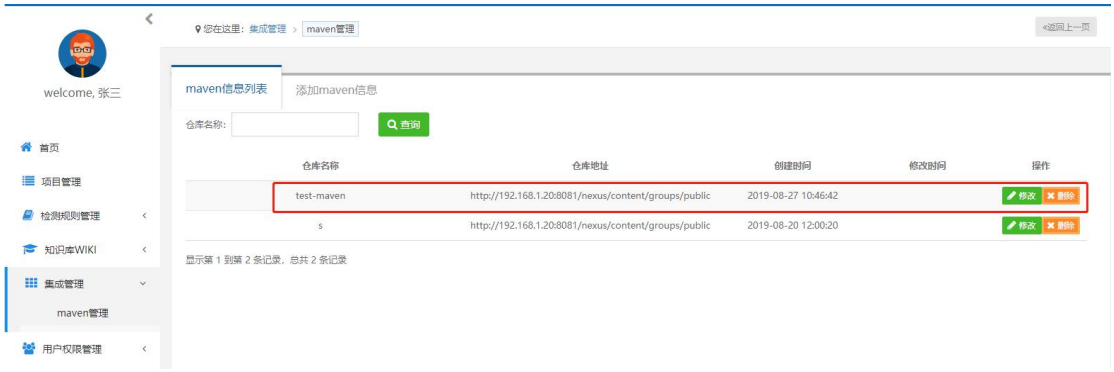
6.1 maven 管理

1. 添加 maven 信息

输入正确的仓库名称、仓库地址，点击【添加】按钮



2. 添加成功，进入到 maven 信息列表中（添加成功后即关联到项目管理创建工程时 maven 工程选择“是”时，可关联选择添加的 maven 信息）；



3. 可对添加的 maven 信息进行查询、修改和删除操作。

七、用户权限管理

本模块提供了部门管理、用户管理、权限管理功能。

系统用户分三类：超级管理员，管理员及普通用户。系统提供默认的权限设置，超级管理员可进行权限的细化分配。

以超级管理员身份登录系统后，超级管理员具有所有权限，可以进行用户创建和用户授权的操作，可创建管理员和普通用户。管理员可以创建项目组和检测工程，可以审计分配缺陷，对已解决的缺陷进行复审，关闭或重新打开缺陷。普通用户主要指开发人员，普通用户登录后可查看分配给自己的缺陷，解决缺陷。

在用户列表页面，可修改和删除用户。点击“添加用户”菜单，可录入用户信息，可新增用户。

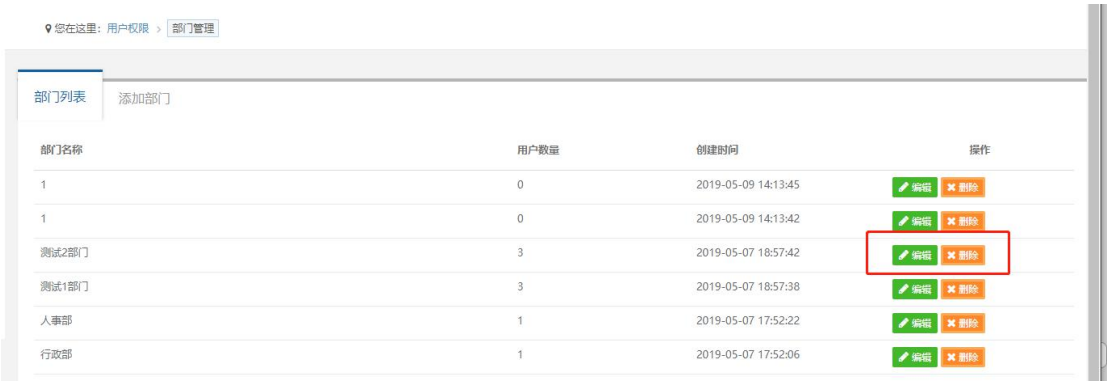
超级管理员可进行权限管理，包括新增、修改和删除角色，可对角色进行细化授权。一般的，使用系统默认的角色设置即可。

7.1 部门管理

1. 部门的添加：输入部门名称，点击【添加】按钮

规则：部门名称长度不超过 20 个字符。

2. 添加成功后，在“部门列表”中实时生成，可对部门进行修改和删除的操作。



7.2 用户管理

1. 单个用户的添加：输入必填项，点击【添加】

备注：输入正确的邮箱，建好工程后可通过邮箱进行缺陷推送

规则：登录账号长度不超过 20 个字符

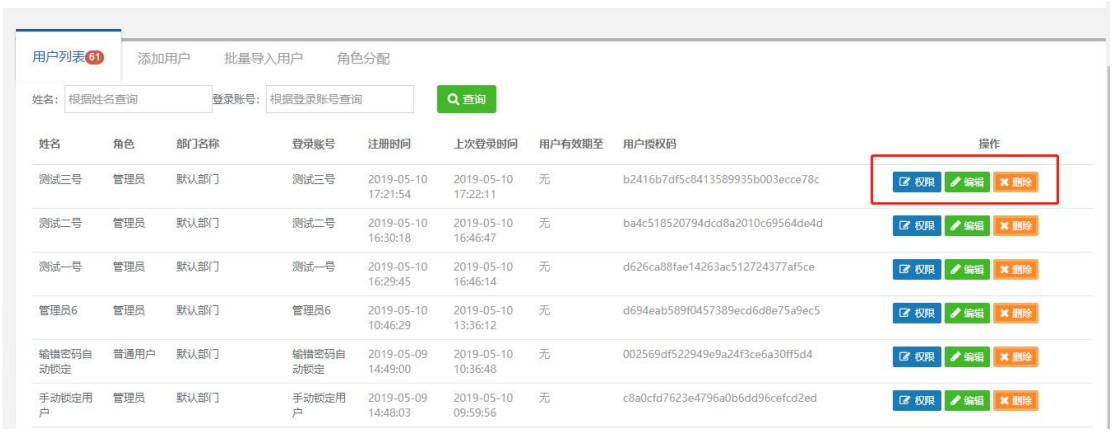
邮箱填写正确格式的邮箱；

密码：必须是 6-20 位字符，必须为包含数字、字母的字符串组合，不包含空格(不符合则默认为‘cp123456’)。

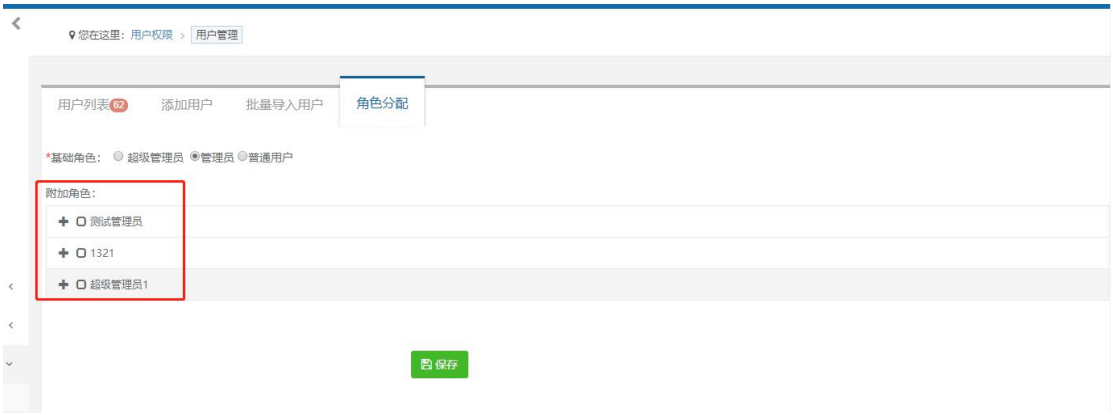
姓名：不超过 20 个字符；

基础角色默认为管理员，部门默认为默认部门，带*号的文本框为必填项。

2. 在用户列表中实时生成，可对该用户的操作是配置权限、编辑、删除。若用户为超级管理员，不能对超级管理员进行权限、编辑、删除的操作。



点击【权限】，进入到角色分配页面，可以修改基础角色，也可勾选附加角色。



3. 批量导入用户：先下载模板，正确填写模板后点击【选择文件】，选中自己填写好的 Excel 模板后，点击【导入】按钮；

导入成功后，在用户列表中显示导入成功的用户。

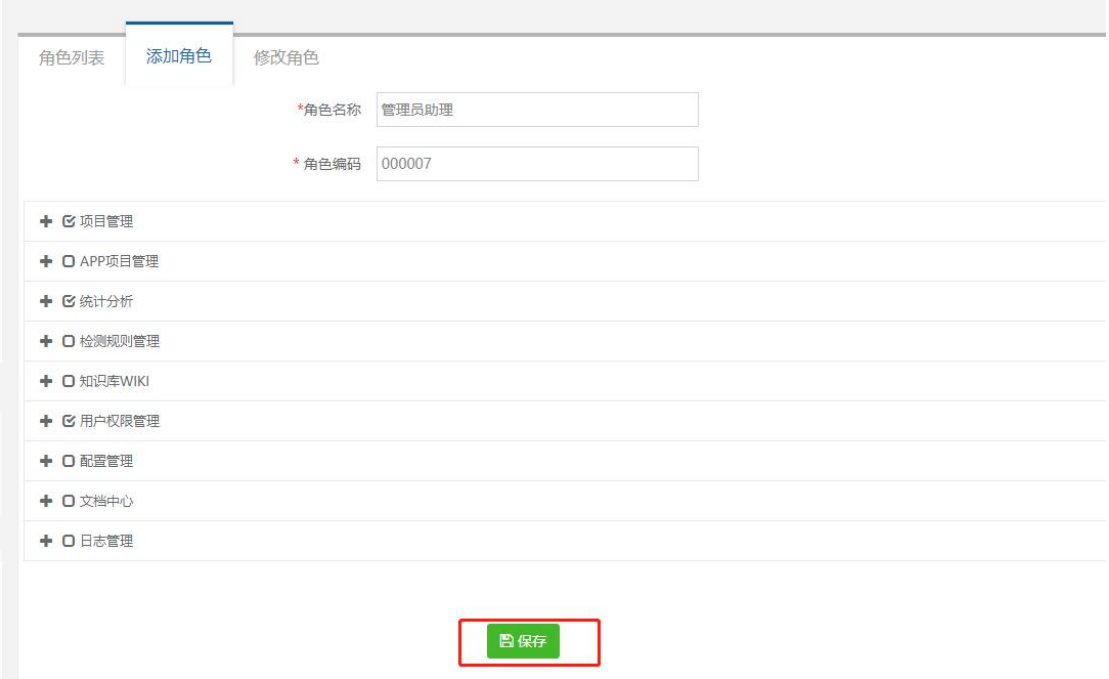
7.3 角色管理

1. 添加角色：输入角色名称、角色编码（不可重复）、勾选角色权限，点击【保存】按钮；

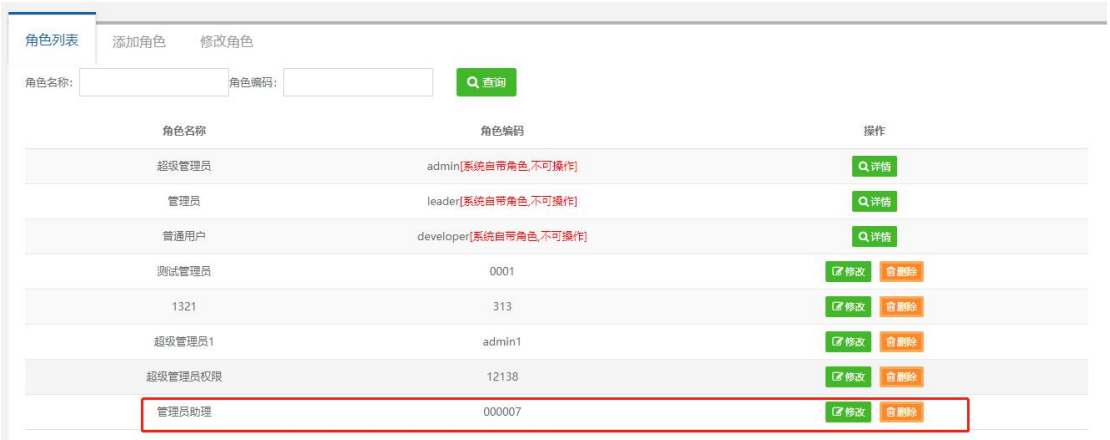
规则：角色名称长度不超过 30 个字符，且名称不能重复；

角色编码长度不超过 30 个字符，且角色编码不能重复；

带*号的为必填项，不能为空。



2. 角色生成在角色列表中，可执行的操作：查询、修改、删除。系统默认有三个角色只可查看不可修改和删除。



八、配置管理

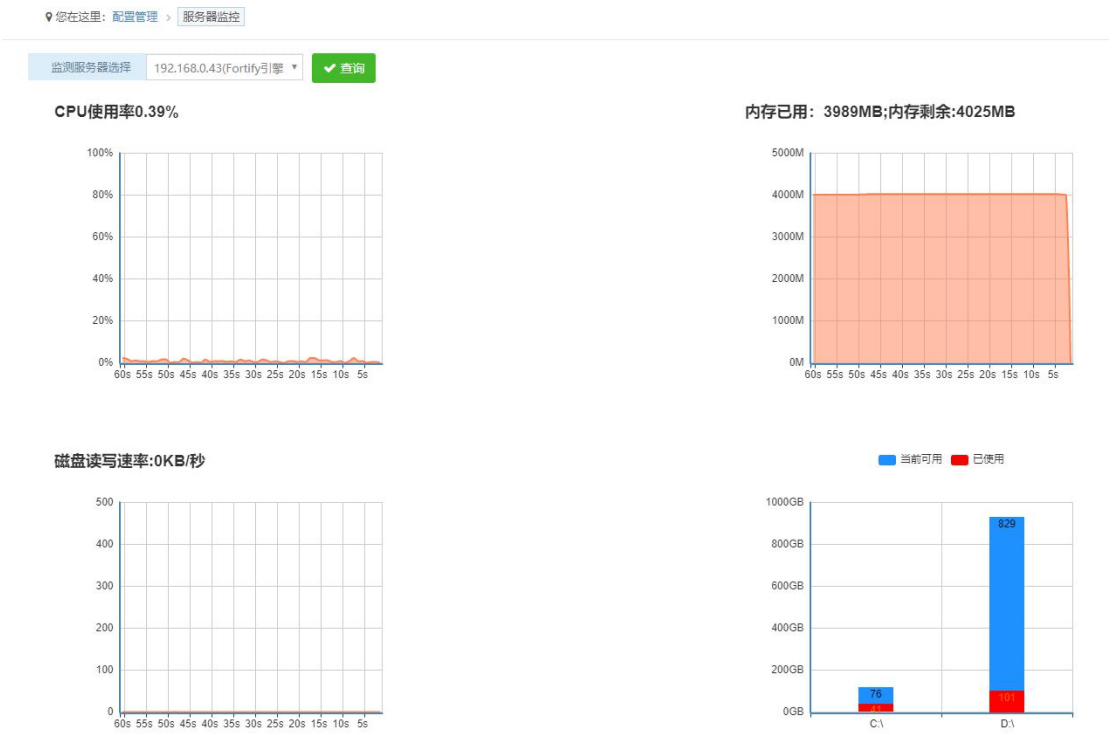
8.1 通用设置

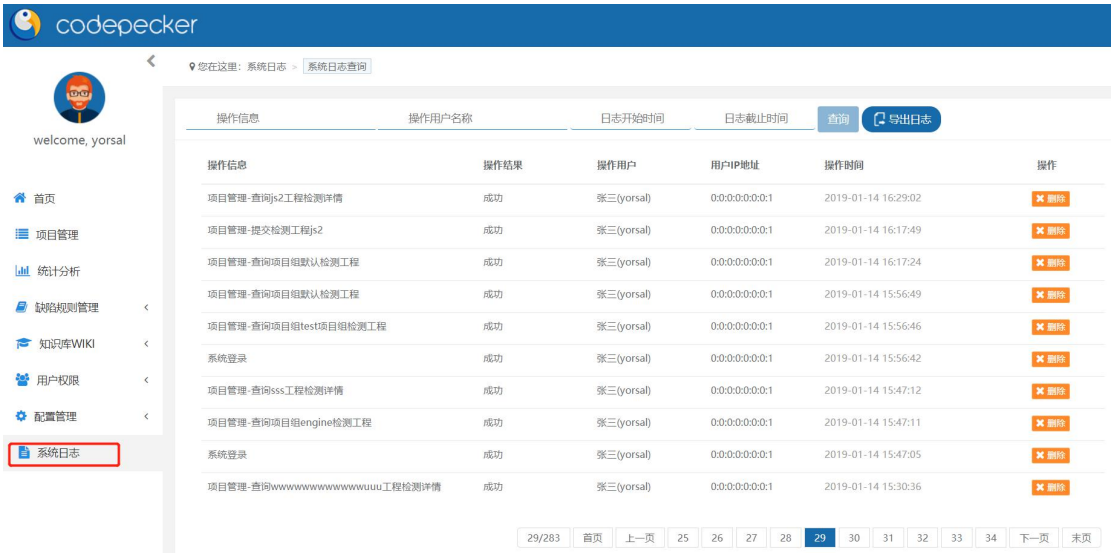
8.1.1 历史数据

系统提供了历史数据管理功能，历史数据处理方式包括：永久保留、定期清理和立即清理，用户可根据业务需要进行设置。

8.1.2 服务器监控

可通过查询条件选择监控


您在这里：配置管理 > 服务器监控
监测服务器选择
192.168.0.43(Fortify引擎
查询
CPU使用率0.39%
内存已用：3989MB;内存剩余:4025MB
磁盘读写速率:0KB/秒
当前可用
已使用
C:\
D:\

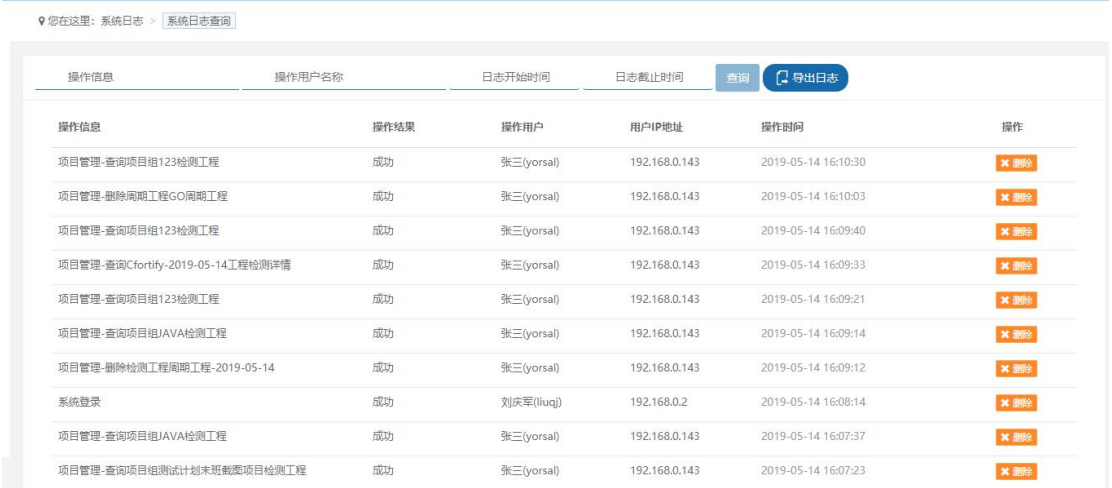

codepecker
welcome, yorsal
您在这里：系统日志 > 系统日志查询
操作信息
操作用户名称
日志开始时间
日志截止时间
查询
导出日志
首页
项目管理
统计分析
缺陷规则管理
知识库WIKI
用户权限
配置管理
系统日志

九、日志管理

产品	软硬件要求
源代码缺陷分析系统 V4.0	企业级服务器 1 台（实体机或虚拟化服务器均可）： CPU：主频 2GHz，四核八线程及以上； 内存：64G 及以上； 硬盘：不低于 1TB 剩余空间（依据检测项目的数量可扩展）； 操作系统 1 套： Windows Server 系列 64 位或 CentOS7.4 64 位 （厂商可提供 CentOS）；
	用户端： 浏览器：Chrome（或者支持 HTML5 的浏览器） 分辨率：1600X900 以上 内存：4GB 或以上 网络：用户端与服务器网络可达

9.1 系统日志

此模块提供了系统重要操作日志的查询、导出、删除等功能。



9.2 后台日志

通过时间段导出日志