# 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

一、系统说明	3
1.1 系统架构	4
1.2 主要功能结构	4
1.2.1 用户登录	4
1.2.2 首页	5
1.2.3 项目管理	6
1.2.4 检测规则管理	6
1.2.5 知识库	7
1.2.6 集成管理	7
1.2.7 用户权限管理	7
1.2.8 配置管理	8
1.2.9 日志管理	8
1.3 代码检测流程	8
二、 首页	9
2.1 设置	9
2.2 快速检测	11
2.3 系统使用情况	12
2.4 发现的缺陷	15
2.5 发现缺陷的等级	25
2.6 缺陷密度(按部门)	25
2.7 缺陷密度(按项目组)	26
2.8 缺陷密度(按项目)	26
三、项目管理	28
3.1 新建及管理项目组	28
3.2 创建	
3.2.1 创建工程(上传)	
3.2.2 创建工程(版本控制工具)	
3.2.3 创建周期工程	37
3.3 查看	
3.3.1 查看工程	
3.3.2 上程检测结果	
3.3.3 缺陷明细	
3.3.4 导出报告	
3.3.4 删除	
3.4 修改/删除	
四、检测规则官埋	
4.1	
五、 知识库 ₩1K1	
六、 集成管理	
6.1 maven 管埋	59

目 录

七、	用户权限管理	60
	7.1 部门管理	60
	7.2 用户管理	61
	7.3 角色管理	63
八、	配置管理	64
, .	8.1 通用设置	64
	8.1.1 历史数据	64
	8.1.2 服务器监控	64
九、	日志管理	66
/	9.1 系统日志	66
	9.2 后台日志	67

# 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:

- 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。
- 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。
- 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。



登录			
yorsal			
suhv	×	SUHV 换—张	
<b>4</b> 提交登录			

### 1.2.2 首页

	<	您参与了 2个项目组 »				€ 快速检测	□ 新建项目组 # 查看更多
welcome, 张三		☞ 系统使用情况		? 发现的缺陷		创 发现缺陷的等级	
		ŧβſ ]	3	总数	214	严重	67
<b>希</b> 首页		用户数量	1	需要审计	214	高风险	33
■ 项目管理		项目组	2	需要复审	0	中等风险	25
检测规则管理	<	已检测项目	1	需要修复	0	低风险	79
☎ 知识库WIKI	<	代码总行数	13975	缺陷类型总数	13	警告和信息	10
₩ 集成管理	<	2 1 1 10 4 min and 1 ( 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		The first set of the later of t	(0)		
🚰 用户权限管理	<	● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●		₩182度(按坝日	1日)	₩ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
🔅 配置管理	<	默认部门	39.7	TestGroup	39.7	c1	39.7
■ 日志管理	<	开发1部	0.0	默认	0.0		
		测试1部	0.0				
						尚	衍舌 Windows 到"设置"以激活 Windows。

#### 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。

	<	♀您在这里:项目管理	> 项目管理				或如此一页
welcome, 张三		项目组名称: 请输入项	日组名称 项目名称	: 请输入项目名利	项目创建人: 请辩	Q 查询	<b>住新建築目</b> 組
<b>谷</b> 首页		项目组名称	所属部门	工程总数	周期工程总数	创建时间◆	操作
■ 项目管理		默认	默认部门	0	0	2019-04-10 18:17:19	<b>查看→</b> 创建→ <b>》</b> 修改
🧧 检测规则管理	<	TestGroup	默认部门	1	0	2019-04-04 14:35:54	意看 - 创建 - <b>●修改</b> × 删除
╞ 知识库WIKI	<	★ 您总共参与了	2个项目组;完成检测	1个, 检测异常0个	、 检测中0个。		
■ 集成管理	<						1/1 1
嶜 用户权限管理	<						
• 配置管理	<						
🧾 日志管理	<						

# 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。

	<	♀ 您在这里: :	检测规则管理 > 缺陷规则集					《返回上一页	
	1	缺购规则集	沃加东种哈抑则体						
weicome, <u>sp</u>		缺陷规则集名利	() () () () () () () () () () () () () (	程语言 全部		V Q 查询			
<b>希</b> 首页			缺陷规则集名称		编程语言	创建人	创建时间	操作	
■ 项目管理			default(默认,系统固定规则)		JAVA/JSP	yorsal	2016-07-05 16:13:17	●查若	
🧧 检测规则管理	~		high(严重及高风险,系统固定规则	D	JAVA/JSP	yorsal	2016-07-05 16:13:17	●查君	
缺陷规则集			default(默认,系统固定规则)		C/C++	yorsal	2016-07-05 16:13:41	●查若	
➢ 知识库WIKI	<		high(严重及高风险,系统固定规则	D	C/C++	yorsal	2018-11-24 18:15:11	●直君	
■ 集成管理	<								
🚰 用户权限管理	<							1/1	
✿ 配置管理	<								
🧧 日志管理	¢								

# 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。

	<	♀ 您在这里:集成管理 → maven管理				《返周上一页
Y						
welcome, 张三		maven信息列表 添加maven信息				
		金库名称: Q 查询				
<b>合</b> 首页		仓库名称	仓库地址	创建时间	修改时间	操作
■ 项目管理		s	http://192.168.1.20:8081/nexus/content/groups/public	2019-08-20 12:00:20		✔ 修改 × 删除
🧧 检测规则管理	<	显示第 1 到第 1 佘记录,总共 1 佘记录				
☎ 知识库WIKI	<					
■ 集成管理	~					
maven管理						
警 用户权限管理	<					
☆ 配置管理	<					
🧧 日志管理	<					

# 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:

项目组一>新建检测项目一>设置一>检测分析一>问题追踪审计一>结果导出 一>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。

8

# 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。

0
2 个人信息
 € 修改密码
() 退出登录

(1) 个人信息

完善个人信息	修改密码	
	登录名/账号	login2
	手机	13577778888
	*邮箱	(Commentation of the second
	姓名	管理员login2
	性别	女 *
	学历	请选择  ▼
	出生年月	2000-11-23
	QQ	
	用户唯一授权码	5ad30db3c814436f97bd453200d0fefb
		☞ 提交修改

(2) 修改密码

完善个人信息	修改密码		
	*旧密码		
	*新密码	******	
	*再次输入新密码	••••••	]
		<b>记</b> 提交修改	

# (3) 退出登录,点击退出登录直接退出

参与了7个项目组》				◆ 快速检测 [] 穿	· 除水 和 加 和 和 和 和 和 和 和 和 和 和 和 和 和 和 和 和 和
? 发现的缺陷		创 发现缺陷的等级		✓ 发现缺陷的工程	£ 修改密码
总数	582	严重	331	上传-C-5.28 (v1.0)	
需要审计	582	高风险	33	sql-5.28-1 (v1.0)	O IEdizak

# 2.2 快速检测

1. 快速检测: 创建工程(上传),属于默认部门;

	📀 快速检测	已新建项目组	# 查看更多
--	--------	--------	--------

#### 项目组名称为:默认,所属部门:默认部门,不可删除。

login2						
	项目组名称	所属部门	工程总数	周期工程总数	创建时间⇔	操作
<b>谷</b> 首页	默认	默认部门	0	0	2019-05-23 09:26:28	查看 + 创建 + ■对比分析 <b>/</b> 修改
■ 项目管理	坚实的客户的会计师	555555555555555555555555555555555555555	0	0	2019-05-14 17:50:54	查看→ 创建→ ②对比分析 <b>/</b> 祭改 × 翻除
山 统计分析	JAVA	41	1	0	2019-05-10 15:32:26	· 查看 • 创建 • 目对比分析 / / 修改 × 删除

2. 新建项目组:开始"新建项目组";

		٠
◆ 快速检测	①新建项目组	# 查看更多

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。

	<	♀您在这里:项目管理 > 新建项目组			
welcome, 张三		*项目组名称			
_		*所属部门	默认部门	Ŧ	
☆ 首页		*项目组成员			*
■ 项目管理			▼yorsal		
🧧 检测规则管理	<		…王测试1部		
➢ 知识库WIKI	<				
■■ 集成管理	<		4		Þ
🚰 用户权限管理	٢	项目目标基线	请选择	Ŧ	
• 配置管理	<		6 提父		
🧧 日志管理	<				

3. 查看更多: 快速查看更多与当前用户相关的工程;

							٠	
				速检测	日新	建项目组	查看更多	
进入	项目	管理页面						
Ş	`	♥您在这里:项目管理 项目组名称: 请输入项	2 > 项目管理 目组名称 项目名	<b>称:</b> 请输入项目名称	项目创建人: 清输	入项目创建人 (账号、姓名 Q 查询		《返回上一页
welcome, 张三							-	计新建项目组
<b>谷</b> 首页		项目组名称	所属部门	工程总数	周期工程总数	创建时间 \$	操作	E
■ 项目管理		默认	默认部门	0	0	2019-04-10 18:17:19	查看 - 创建 - 《修改	
🧧 检測规則管理	<	TestGroup	默认部门	2	0	2019-04-04 14:35:54	查看▼ 创建▼ 2修改	★ 删除
➢ 知识库WIKI	¢	★ 您总共参与]	72个项目组;完成检测	则2个, 检测异常0个	, 检测中0个。			
Ⅲ 集成管理	<							1/1 1
🚰 用户权限管理	¢							
✿ 配置管理	¢							
🧧 日志管理	<							

# 2.3 系统使用情况

1. 点击部门后的数字

部门	4
用户数量	18
项目组	134
已检测项目	1083
代码总行数	40909374

#### 页面跳转到部门管理,显示部门详情

♀您在这里:用户权限管理	> 部门管理		《返回上一页
部门列表添加部门			
部门名称	用户数量	创建时间	操作
测试1部	0	2018-10-14 14:57:36	▲ 編輯 × 删除
默认部门	1	2016-01-11 10:57:25	
开发1部	0	2015-12-16 15:43:12	▲ 編載 × 删除
			1/1 1

## 2. 点击用户数量右侧的数字

部门	3
用户数量	1
项目组	2
已检测项目	2
代码总行数	47908

## 页面跳转到用户管理页面

户列	「表1」 添加	用户	批量导入用户	1						
名:	根据姓名查询		登录账号: 根据	登录账号查询	基础角色:	全部	▼ 部门: 全部	▼ Q 查询		
姓名	角色	部门名称	登录账 号	注册时问	上次登录时间	用户有效期至	用户授权码		操作	
ŧΞ	超级管理员	默认部门	yorsal	2014-12-28 18:58:06	2019-08-26 15:55:12	无	4c979443a1d4ff56205487945dbb812a			
张三	超级管理员	默认部门	yorsal	2014-12-28 18:58:06	2019-08-26 15:55:12	无	4c979443a1d4ff56205487945dbb812a			

3. 点击项目组右侧数字

3
1
2
2
47908

# 页面跳转到项目管理页

Ki入部门 0 0 2019-04-10 18:17:19 査音・ 修建・ // 形成 TestGroup 新入部门 2 0 2019-04-04 14:35:54 査音・ 修建・ // 形成 X 1996	项目组名称 所属部门 工程总数 周期工程总数 创建时问 \$	操作
TestGroup 数认問门 2 0 2019-04-04 14:35:54 含石 - 68法 / 26夜 × 開始	就人 新入部门 0 0 2019-04-10 18:17:19 査石 V (統建 V )	æ
	TestGroup 款认部门 2 0 2019-04-04 14:35:54 音音 编建 /	改 × 删除

4. 可查看已检测项目总数, 一致

⑦ 系统使用情况	
部门	3
用户数量	1
项目组	2
已检测项目	2
代码总行数	47908

# 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

	《 您参与了 28个项目组 》			
welcome vorsal	? 发现的缺陷		(1) 发现缺陷的等级	
welcome, yorsu	总数	285802	严重	30582
👫 首页	需要审计	283165	高风险	25513
■ 项目管理	需要复审	0	中等风险	79298
山統计分析	需要修复	2637	低风险	100956
2 检测规则管理	<		警告和信息	53851
☞ 知识库WIKI	<			

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

	<	♥ 您在这里:项目管理:	缺陷列表							
		缺陷列表 283165								
welcome, yorsu		所属项目组 全部	ß	w.	所属工程	全部	*	缺陷类型	全部	w.
👫 首页		文件名			方法名			□ 与基約	成对比的违禁缺陷	搜索
项目管理		所属工程	缺陷状态 🗸	缺陷	缺陷分类 🗸	缺陷类型	风险等级 🖌	未审计 🗸	审计时间	操作
<u>山</u> 统计分析		上傳+findbugs	未分配	com.ibm.wsdl.Constants:	质量缺陷	MS: Field should be	高风险	未新计	无	■ 查看详情
检測规则管理	<	上传+findbugs	未分配	com.ibm.wsdl.Constants:	质量缺陷	MS: Field should be	黨风险	未审计	无	■ 查看洋街
■ 知识库WIKI	<	上傳+findbugs	未分配	com.ibm.wsdl.Constants:	质量缺陷	MS: Field should be	高风险	未新计	无	■ 查看详情
	<	上传+findbugs	未分配	com.ibm.wsdl.Constants: 377	质量缺陷	MS: Field should be	海风险	未审计	无	<b>≡</b> 查看洋情
7 用户仪账管理	< ,	上传+findbugs	未分配	com.ibm.wsdl.Constants: 215	质量缺陷	MS: Field should be package protected	黨风险	未审计	无	■ 查看洋情
文档中心	`	上传+findbugs	未分配	com.ibm.wsdl.Constants: 406	质量缺陷	MS: Field should be package protected	黨风险	未前计	无	■ 查看洋情
7 日志管理	¢	上传+findbugs	未分配	com.ibm.wsdl.Constants: 232	质量缺陷	MS: Field should be package protected	黨风险	未审计	无	■ 査石洋格 2805手 Mind on Min
		上传+findbugs	未分配	com.ibm.wsdl.Constants:	质量缺陷	MS: Field should be	高风险	未审计	无	一成1日 WHIGOWS 转 <mark>通查召详情</mark> 数括 Windows。

3) 点击缺陷右侧的【查看详情】,可查看缺陷明细

列表 (1958)								
所属项目组	默认	Ŧ	所属工程	全部	•	缺陷类型	全部	Ŧ
文件名			方法名			与基线	对比的违禁缺陷	搜索
所属工程	缺陷状态	✔ 缺陷	缺陷分类 🗸	缺陷类型	风险等级 🖌	未审计 💙	审计时间	操作
java	未分配	JavaScriptValidation.jav a:156	安全缺陷	反射型跨站脚本	严重	未审计	无	■ 查看详情
java	未分配	redirect.jsp:12	安全缺陷	URL重定向	严重	未审计	无	■ 查看详情
java	未分配	main.jsp:163	安全缺陷	反射型跨站脚本	严重	未审计	无	■ 查看详情
java	未分配	UpdateProfile.java:340	安全缺陷	SQL注入	严重	未审计	无	≡ 查看详情
java	未分配	ReflectedXSS.java:165	安全缺陷	反射型跨站脚本	严重	未审计	无	■ 查看详情
java	未分配	ECSFactory.java:292	安全缺陷	存储型跨站脚本	严重	未审计	无	■ 查看详情

4) 进入到缺陷详情页,查看缺陷,可对缺陷进行缺陷审计

	<	♥您在这里:项目管理 > 项目组成认] > 项目[java] >	缺陷列救	> 缺陷详情		
4		缺略审计视图		WebGoat5.	0/JavaSource/org/owasp/webgoat/lessons/JavaScriptValidation.java	
welcome, yorsal		- House - Const		130	<pre>+ "if (!regex5.test(document.form.field5.value)) {err+=1; msg+='\\n bad field5';}" </pre>	,
				131	<pre>+ linesep + "if (!regex6.test(document.form.field6.value)) {err+=1; msg+='\\n bad field6';}"</pre>	
		★ JavaScriptValidation.java:156 ()反射型跨站脚本	^	133	+ lineSep + "if (!regex7.test(document.form.field7.value)) {err+=1; msg+="\\n bad field7';}"	
😭 首页				135	+ lineSep + "if ( err > 0 ) alert(msg);" + lineSep	
				137	+ "" + lineSep;	
10日管理				138 ti	ry	
				140	<pre>String param1 = s.getParser().getRawParameter("field1", "abc");</pre>	
山山統计分析				141 142	<pre>String param2 = s.getParser().getRawParameter("field2", "123"); String param3 = s.getParser().getRawParameter("field3",</pre>	
				143	"abc 123 ABC"); String paramé = s getParser() getRauParameter("field4", "seven");	
				145	<pre>String param5 = s.getParser().getRawParameter("field5", "90210");</pre>	
				146 147	String paramb = s.getParser().getRawParameter("fieldb", "90210-1111");	
	,			148	<pre>String param7 = s.getParser().getRawParameter("field7", "201 s04 deep".</pre>	
- /40041110				150	ec.addElement(new StringElement(script));	
	,			151	TextArea input1 = new TextArea("field1", 1, 25).addElement(param1); TextArea input2 = new TextArea("field2", 1, 25).addElement(param2);	
*** MURELY				153	TextArea input3 - new TextArea("field3", 1, 25).addElement(param3);	
201 田白切加会加				154	TextArea inputs = new TextArea("field5", 1, 25).addElement(params);	
TU/ DAREAL				A156 157	TextArea input6 - new TextArea("field6", 1, 25).addElement(param6); TextArea input7 = new TextArea("field7", 1, 25).addElement(param7);	
ALL DELANS TH				158	Territ In Territ ()	
₩ 配直當理	5			160	b.setType(Input.BUTTON);	
A sherblinets de				161 162	<pre>b.setValue("Submit"); b.addAttribute("onclick", "validate():");</pre>	~
			~	<	an add@lamant/ann. Nl./// add@lamant/ann. finian@lamant/	>
		the state of state and state				
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	\$	10代的100分分析		SERVICE IN	加口心 缺陷原理评述 夢考信息 缺陷的原因	
		No. 2 No. 5 Science Science		当前缺陷	反射型跨站脚本	
		ParameterParser.java:627 [来源]	^	缺窮注情	向一个 Web 浏览器发送未经验证的数据会导致该浏览器执行恶意代码。	
		ParameterParser.java:627 [跟踪]		sector by		
		ParameterParser.java:638 [跟踪]		风险级别	严重	~
		ParameterParser.java:608 [跟踪]				
		ParameterParser.Java:608 [親餘]		审计状态	未审计	~
		JavaScriptValidation.java:146 [現瞭]				
		JavaScriptValidation.java:146 【銀踪】		注题	最多允许200个字符	
		JavaScriptValidation.java:156 [爆发点]		111++		
				10.00		
				操作	2000 ·	

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"

康 🚺								
所属项目组	默认	<b>T</b>	所属工程	全部	Ŧ	缺陷类型	全部	Ŧ
(件名	I		方法名			日本	或对比的违禁缺陷	搜索
所属工程	已分配未修复 🗸	缺陷	缺陷分类 🗸	缺陷类型	风脸等级 💙	存在缺陷 🖌	审计时间	操作
java	已分配,未修复	JavaScriptValidation.jav a:156	安全缺陷	反射型跨站脚本	严重	存在缺陷	2019-08-13 12:59:30	■ 查看详情

6) 缺陷进入到分配人首页中"需要修复"中

welcome, vorsal	? 发现的缺陷		山 发现缺陷的等级		代码评分(按项目)     (     按项目)	
	总数	285802	严重	30582	SVN-立检-更新建工程-非增量(07-10.12:	479.4
🚔 首页	需要审计	283164	高风险	25513	50) SVN-立检-更新建工程-非增量(07-10.15;	479.33
■ 项目管理	需要复审	0	中等风险	79298	00)	
山餘十分析	需要修复	2638	低风险	100956	默认+fortify	351.9
			警告和信息	53851	svn-全引擎-非增量	340.13
🧧 检测规则管理 🛛 <					SVN-立检-更新建工程-非增量	313.35
₱ 知识库WIKI <						

	<	♥ 您在这里:项目	1管理 > 缺陷列表									
welcome vorsal		缺陷列表 🜖										
		所属项目组	<b>第</b> 6人	Ŧ	所属工程	全部	×					
<b>希</b> 首页		所属工程	已分配未修复 🗸	缺陷	缺陷分类 🗸	缺陷类型	风险等级 🖌	优先级 🗸	审计人	审计时间	操作	
■ 项目管理		java	待修复	JavaScriptValidation.j	安全缺陷	反射型跨站脚本	严重	商	wjj	2019-08-13 12:59:30	■ 查看详情	已修复
<u>业</u> 统计分析												
🧧 检测规则管理 🛛 🗸												

2. 需要修复:

1) 点击需要修复右侧的数字

发现的缺陷	
总数	285802
需要审计	283164
需要复审	0
需要修复	2638

2) 进入到缺陷列表,显示出所有该用户待修复的缺陷

	<	♀您在这里:项目	管理 缺陷列表								
		缺陷列表 2638									
welcome, yorst		所属项目组	全部		所属工程	全部	×				
🕈 首页		所属工程	已分配未修复、	✔ 缺陷	缺陷分类 🗸	缺陷类型	风险等级 🗸	优先级 🗸	审计人	审计时间	操作
■ 项目管理 ▲ 统计分析		携带审计信息 - java-7.2	目 待修复	com.ibm.wsdl.Definiti onImpl:88	质量缺陷	ES: Comparison of String parameter using == or !=	低风险	商	wjj	2019-07-04 17:59:27	III 查看详格 已錄复
2 检测规则管理	¢	<del>携带审计信息</del> -java-7.2	1. 待修复	com.ibm.wsdl.Definiti onImpl:124	质量缺陷	ES: Comparison of String parameter using == or !=	(ERU))	商	wjj	2019-07-04 17:59:27	這 查看洋街 已修复
☞ 知识库WIKI	<	携带审计信息 -java-7.2	. 待修复	com.ibm.wsdl.Definiti onImpl:70	质量缺陷	ES: Comparison of String parameter	(ERI))	高	wjj	2019-07-04 17:59:27	III 查看详情 已修复
重成管理	<	携带审计信息	1 待修复	com.ibm.wsdl.extensi	质量缺陷	using == or != Nm: Confusing	GNIN	商	wiji	2019-07-04 17:59:27	這 查對详持 已然复
66 田白灯和参加	,	-java-7.2		ons.schema.SchemaR		method names	007072		- M		Constant and

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"

♀您在这里:项目管理 > 缺陷列表

所属项目组	默认	*	所属工程	全部	Ŧ				
所属工程	已分配未修复 🗸	缺陷	缺陷分类 🗸	缺陷类型	风险等级 🖌	优先级 🗸	审计人	审计时间	操作
java	待修复	JavaScriptValidation.j ava:156	安全缺陷	反射型跨站脚本	严重	in	wjj	2019-08-13 12:59:30	■ 查看详情
java	待修复	Exec.java:103	安全缺陷	命令注入	严重	首	wjj	2019-08-13 13:22:21	■ 查看详情 已修复
java	待修复	Exec.iava:292	安全缺陷	命令注入	严重	商	wjj	2019-08-13 13:22:21	書 查若详信

## 4) 或者点击缺陷右侧的【查看详情】, 可查看缺陷的详细信息

」表 2638										
项目组	全部		×	所属工程	全部	v				
所属工程		已分配未修复 🗸	缺陷	缺陷分类 ✔	缺陷类型	风险等级 🗸	优先级 🗸	审计人	审计时间	操作
携带审计信 -java-7.2	息	待修复	com.ibm.wsdl.Definiti onImpl:88	质量缺陷	ES: Comparison of String parameter using == or !=	(ERIS)	商	wjj	2019-07-04 17:59:27	■ <u>●</u> 番详情 已修复
携带审计信 -java-7.2	息	待修复	com.ibm.wsdl.Definiti onImpl:124	质量缺陷	ES: Comparison of String parameter using == or !=	(674)	副	wjj	2019-07-04 17:59:27	■ 查若详情 已修复
携带审计信 -java-7.2	息	待修复	com.ibm.wsdl.Definiti onImpl:70	质量缺陷	ES: Comparison of String parameter	低风险	讀	wjj	2019-07-04 17:59:27	圖 查看详情 <b>已修复</b>

#### 进入缺陷详情

缺陷亩计视图		WebGo	at5.0/JavaSource/org/owasp/webgoat/lessons/HttpOnly.java
and the Link Particular	_	221 222	TR tr = null; Form f = null;
→ HttpOnly.java:212 () HTTP头文件操纵	~	223 224	<pre>ec.addElement(new StringElement(getJavaScript()));</pre>
		225 226 227	<pre>f = new Form();</pre>
		228	t - new Table();
		230	L.Setwidth(Sou);
		231 232	<pre>tr = new TR();</pre>
		233 234	<pre>tr.addElement(new TD(new StringElement("Your browser appears to be: " + getBrowserType(s)))); t.addElement(tr);</pre>
		235	<pre>tr = new TR();</pre>
		237 238	<pre>t.addElement(tr);</pre>
		239 240	<pre>tr = new TR();</pre>
		241	<pre>tr.addElement( new TD(new StringElement ("Do you wish to turn HTTPOnly on?")));</pre>
		243	<pre>tr.addElement( new TD(new StringElement ("Yes")));</pre>
		244	if(httpOnly true) {
		246 247	<pre>r = new Input(Input.RADIO, HITPONLY, "True" ).addAttribute("Checked", "true"); } else {</pre>
		248 249	<pre>r = new Input(Input.RADIO, HTTPONLY, "True" ).addAttribute("onClick", "document.form.submit()"); }</pre>
		250	tr.addElement(new TD(r)):
		252	tr.addElement( new ID(new StringElement ("No")));
	~	< PEA	>
缺陷细节分析		缺陷审计	缺陷原理详述
	_	当前封	NB HTTP头文件操纵
WebSession.java:621 【来源】	^	*187**	HTTP 响应头文件中包含未验证的数据会引发 cache-poisoning、cross-site scripting、cross-user defacement、page hijacking、
WebSession.java:621 【親線】		acean	cookie manipulation 或 open redirect。
WebSession.java:627 [跟踪]		风险绩	別严重
WebSession.java:627 [誤踪] Http://pivi.eva:206 [原踪]		审计划	态 存在缺陷
HttpOnly.java:206 [限除]		审讨	大 wij
HttpOnlv.java:212 [爆发点]			
		优先	<b>援</b> 高
		ä	77在加約11
	~	扬	windows ※注 Windows

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";

<	>
缺陷审计 部	陷原理详述
当前缺陷	反射型跨站脚本
缺陷详情	向一个 Web 浏览器发送未经验证的数据会导致该浏览器执行恶意代码。
风险级别	严重
审计状态	存在缺陷
审计人	wjj
优先级	育同
注释	存在缺陷
操作	✓E編決 ×未編決 激活 Windows

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

参与了 28个项目组 »			
? 发现的缺陷		(1) 发现缺陷的等级	
总数	285802	严重	30582
需要审计	283157	高风险	25513
需要复审	6	中等风险	79298
需要修复	2639	低风险	100956
		警告和信息	53851

#### 3. 需要复审:

1) 点击"需要复审"右侧的数字

? 发现的缺陷		山 发现缺陷的等级	
数	285799	严重	30582
要审计	283157	高风险	25513
要复审	3	中等风险	79298
要修复	2639	低风险	100956
		警告和信息	53851

# 2) 进入到缺陷列表中,显示出该用户所有需要复审的缺陷

una U								
循项目组	全部	×	所属工程	全部	×	缺陷类型	全部	¥
文件名			方法名			与基	绿对比的违禁缺陷	Bittle
所属工程	已修复待关闭 🗸	ak/Ki	缺陷分类 🗸	缺陷类型	风险等级 🖌	审计状态 🖌	审计时间	操作
java	已錄編, 待关闭	JavaScriptValidation.jav a:156	安全缺陷	反射型的法脚本	严重	存在制用	2019-08-13 12:59:30	■ 查看详情 图关闭缺陷
						( 1.1. POPP)		

3)可直接点击缺陷右侧的【关闭缺陷】按钮,关闭缺陷

缺陷列表 3								
所属项目	组全部	Y	所属工程	全部	Ψ.	缺陷类型	全部	¥
文件名			方法名			□ 与基	线对比的违禁缺陷	搜索
所属工程	星 已修复待关 <b>时</b>	↓ ◇ 缺陷	缺陷分类 🗸	缺陷类型	风险等级 💙	审计状态 🗸	审计时间	操作
java	已修复、待关诉	JavaScriptValidation.jav a:156	安全缺陷	反射型跨站脚本	严重	存在缺陷	2019-08-13 12:59:30	III 查看详情 图关闭缺陷
java	已修复,待关闭	Exec.java:103	安全缺陷	命令注入	严重	存在缺陷	2019-08-13 13:22:21	■ 查看详情 四关闭缺陷
java	已修复,待关闭	Exec.java:292	安全缺陷	命令注入	严重	存在缺陷	2019-08-13 13:22:21	■ 查看详有 图关闭缺陷

## 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

缺陷列表 2								
所属项目组	全部	Ŧ	所属工程	全部	•	缺陷类型	全部	7
文件名			方法名			5基约	或对比的违禁缺陷	搜索
所属工程	已修复待关闭 🗸	缺陷	缺陷分类 🗸	缺陷类型	风险等级 🗸	审计状态 💙	审计时间	操作
java	已修复,待关闭	Exec.java:103	安全缺陷	命令注入	严重	存在缺陷	2019-08-13 13:22:21	□ ● 美術製作
java	已修复,待关闭	Exec.java:292	安全缺陷	命令注入	严重	存在缺陷	2019-08-13 13:22:21	· 章 雪洋情 图关闭缺陷

5) 点击进入详情页

♀您在这里:项目管理 > 项目组[默认] > 项目[java] > 缺陷列表 > 缺陷详情

■ 地名英格兰子克拉斯	→         →	<pre>ViaVaSourCeOrg/OWaSpweegoaluluk-xecjava timeout); Sich introjott = mew Sitset(1); sedwatcher watcher; // start the command // start the command inputStream processin = child.getErputStream(); inputStream processin = child.getErputStream(); // get the streams in and out of the command inputStream processin = child.getErputStream(); // start the clock running if (timeout &gt; 0) if (timeout &gt; 0) // write to the child process' input stream if ((input != null) &amp;&amp; linput.getBytes()); processOut.flumb(); processOut.flumb(); processOut.close(); } atchef = new Thread(watcher); } // Write to the child process' input stream if ((input != null) &amp;&amp; linput.getBytes()); processOut.flumb(); processOut.close(); } atchef (IOException e1) { // results.setThrowable(e1); } </pre>	
缺陷细节分析	缺陷审计审	计日志 缺陷原理详述 参考信息 缺陷相似图	
ParameterParter java 627 [本海]	当前缺陷	命令注入	
ParameterParser.java:627 [跟踪]	缺陷详情	执行包含无效用户输入的命令,会导致应用程序以攻击者的名义执行恶意命令。	
ParameterParser.java:638 [跟踪]	风险级别		
ParameterParser.java:608 [跟踪]			
ParameterParser.java:608 [跟踪]	审计状态	存在缺陷	
Challenge2Screen.java:642 [跟踪]			
Challenge2Screen.java:642 [跟踪]	分配	wjj	
Challenge2Screen.java:653 [跟踪]	停生期	9F	
Challenge2Screen.java:654 [跟踪]	11.7638		2
Exectioner/155 [ gg the 1		存在缺陷	
ryeriananan Felalul			
Exec.java:103 [爆发点] ~	注释		

6) 点击【关闭缺陷】, 弹出提示: "操作成功", 缺陷状态改为: "已关 闭"

列表 👩								
所属项目组	全部	(w)	所属工程	全部	•	缺陷类型	全部	×
文件名			方法名			与基线	对比的违禁缺陷	搜索
所属工程	已关闭	▼ 缺陷	缺陷分类 🗸	缺陷类型	风险等级 🖌	审计状态 💙	审计时间	操作
fortify+findb	ougs 已关闭	HttpOnly.java:212	安全缺陷	HTTP头文件操纵	严重	存在缺陷	2019-06-24 17:52:07	■ 查看详情
fortify+findb	ougs 已关闭	JavaScriptValidation.jav a:156	安全缺陷	反射型跨站脚本	严重	存在缺陷	2019-06-27 13:49:57	■ 查看详情
fortify+findb	ougs 已关闭	WeakAuthenticationCoo kie.java:377	安全缺陷	反射型跨站脚本	严重	存在缺陷	2019-06-27 13:50:42	■ 查看详情
java	已关闭	JavaScriptValidation.jav a:156	安全缺陷	反射型跨站脚本	严重	存在缺陷	2019-08-13 12:59:30	■ 查看详情
java	已关闭	Exec.java:103	安全缺陷	命令注入	严重	存在缺陷	2019-08-13 13:22:21	■ 查看详情

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

漏项目组 全	部	*	所属工程	全部	Ŧ	缺陷类型	全部	*
(件名			方法名			与基	线对比的违禁缺陷	搜索
所属工程	已关闭 🗸	缺陷	缺陷分类 🗸	缺陷类型	风险等级 🗸	审计状态 💙	审计时间	操作
fortify+findbugs	已关闭	HttpOnly.java:212	安全缺陷	HTTP头文件操纵	严重	存在缺陷	2019-06-24 17:52:07	■ 查看详情
ortify+findbugs	已关闭	JavaScriptValidation.jav a:156	安全缺陷	反射型跨站脚本	严重	存在缺陷	2019-06-27 13:49:57	圖 查看详情
fortify+findbugs	已关闭	WeakAuthenticationCoo kie.java:377	安全缺陷	反射型跨站脚本	严重	存在缺陷	2019-06-27 13:50:42	■ 查看详情
ava	已关闭	JavaScriptValidation.jav	安全缺陷	反射型跨站脚本	严重	存在缺陷	2019-08-13 12:59:30	■ 查看详情

# 2) 在缺陷审计中,点击【重新打开缺陷】按钮

131		
缺陷审计审	计日志 缺陷原理详述 参考信息 缺陷相似图	
当前缺陷	命令注入	
缺陷详情	执行包含无效用户输入的命令,会导致应用程序以攻击者的名义执行恶意命令。	
风险级别	严重	```
审计状态	存在缺陷	`
分配	wjj	
优先级	高	Ś
注释	存在缺陷	
操作	<b>B里新打开缺陷</b> 激活 Windows	

# 弹出提示:"操作成功"

$\bigcirc$	
U	
操作成	叻
	操作成

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"

所属项目组	默认		所属工程	全部	٣				
所属工程	已分配未修复 🗸	缺陷	缺陷分类 🗸	缺陷类型	风险等级 🖌	优先级 🗸	审计人	审计时间	操作
java	待修复	Exec.java:103	安全缺陷	命令注入	严重	窗	wjj	2019-08-13 13:22:21	■ 查 若洋情 已修复
java	待修复	WSDLScanning.java:1 43	安全缺陷	命令注入	严重	通	wjj	2019-08-13 13:22:21	■ 查看详情 已修复
java	待修复	Challenge2Screen.jav a:649	安全缺陷	命令注入	严重	高	wjj	2019-08-13 13:22:21	■ 查看洋情 已修复
java	待修复	Challenge2Screen.jav a:654	安全缺陷	命令注入	严重	商	wjj	2019-08-13 13:22:21	■ 查看洋情 <b>已修复</b>
java	待修复	CommandInjection.ja va:171	安全缺陷	命令注入	严重	通信	wjj	2019-08-13 13:22:21	書 查看洋情   已修复
java	待修复	CommandInjection.ja va:185	安全缺陷	命令注入	严重	高	wjj	2019-08-13 13:22:21	■ 查 <b></b> 酒洋情 已修复

# 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。

山 发现缺陷的等级	
严重	971
高风险	169
中等风险	1007
低风险	634
警告和信息	160

# 2.6 缺陷密度(按部门)

可查看各个部门中的缺陷密度

育务部	112.91
	52.00
切务部	52.22
默认部门	34.98
<b>韦场</b> 部	0.0

# 2.7 缺陷密度(按项目组)

可查看按项目组区分的缺陷密度

₩₩1112(按坝日组)	
webgoat5.0	2568.75
白名单	697. <mark>1</mark> 2
ceshi 111	331.8
7.9	212.42
7.10	201.61

# 2.8 缺陷密度(按项目)

可查看不同项目之间的缺陷密度

金路密度(按项目)	
则试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。

♀您在这里:项目管理	里 > 项目组列表					
Q 请输入项目组	名称,支持模糊查询					<b>己 新建项目组</b>
项目组名称	所屬部门	工程总数	周期工程总数	创建时间◆	操作	

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。

*所属部门	请选择 🔻	
*项目组成员	<u>+</u> 1	
	+41	
	+ 123	-
	+ 312	
	王王默认部门	
	王二素求测试部	
	王	
	4	•
话日日与甘华	法 從 ▼	
坝日日怀是线	阴应注 ,	

#### 3. 创建成功的项目组

请输入项目组织	名称,支持模糊查询				Œ
项目组名称	所属部门	工程总数	周期工程总数	创建时问◆	操作
C/C++	222222222222222222222222222222222222222	2	3	2019-04-28 13:24:10	查看 • 创建 • 目对比分析 /修改
JAVASCRIPT	222222222222222222222222222222222222222	14	1	2019-04-25 10:34:54	查看 → 创建 → 目対比分析 /修改
PHP	默认部门	6	0	2019-04-25 10:34:33	查看 → 创建 → 国对比分析 /修改
PYTHON	需求测试部	5	0	2019-04-25 10:34:01	查看 🔹 创建 🔹 国对比分析 🥒修改 🔰
SQL	需求测试部	6	î.	2019-04-25 10:33:35	香看 ▼ 创建 ▼ 目対比分析 2修改 5

#### ★ 您总共参与了4个项目组;完成检测31个,检测异常2个,检测中0个。

#### 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。

项目组名称	所属部门	工程总数	周期工程总数	创建时间 ≑	操作	
C/C++	222222222222222222222222222222222222222	2	3	2019-04-28 13:24:10	查看→ 创建→ 自对比分析 / 修改 × 删除	
JAVASCRIPT	222222222222222222222222222222222222222	14	1	2019-04-25 10:34:54	查看→创建→目対比分析 /修改 ×删除	
PHP	默认部门	6	0	2019-04-25 10:34:33	查看→创建→ 副刘比分析 /修改 ×删除	
PYTHON	需求测试部	5	0	2019-04-25 10:34:01	查看→ 创建→ 国际比分析 /修改 × 删除	
SQL	需求测试部	6	1	2019-04-25 10:33:35	查看→创建→自对比分析 /修改 ×删除	

★您总共参与了4个项目组;完成检测31个,检测异常2个,检测中0个。

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。

多改项目组信息	
*项目组名称	PYTHON
*所属部门	▼ 箱武顺朱壽
*创建时间	2019-04-25 10:34:01
*项目组成员	- 王 1 ▲1 - 王 123 - 王 312 - 王 默认部门 - 王 测试1 ▼
项目目标基线	请选择 ▼
	2 确定修改

# 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)

				CALLED A LAN DA CALL	<u></u> 新建项
项目组名称	所属部门	工程总数	周期工程总数	创建时间 \$	操作
默认	默认部门	0	0	2019-04-10 18:17:19	查看 → 创建 → /修改
TestGroup	默认部门	1	0	2019-04-04 14:35:54	

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。

♀您在这里:项目管理 > 项目组[TestGroup] >	新建工程
	《查查 <u>工</u> 屋列类
*工程名称	test
*版本或说明	v1.0
*编程语言类型	JAVA/JSP v
*引擎选择	
*检测安全级别	
*是否Maven工程	是 v
私服倚像url	test-maven X
	1-45594PED-violFEREIntellise-Assertio
	● 检测前,请把与检测无关的文件(svn,git,exe,word等)都删除以负影响检测效率
	● 王编包清使用zip格式
	Sub-Set X and Set

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

			izat lesicase	
的▼ 新建文件夹				= 🔹 🛄
SWPS网盘 ▲ 名称	<u>^</u>	修改日期	类型	大小
c_test_case	e.zip	2017/5/11 10:57	WinRAR ZIP 压缩	164 KB
cs_test_cas	se.zip	2016/10/20 13:57	WinRAR ZIP 压缩	933 KB
J 3D 刘蒙 ios_test.zip	þ	2017/12/7 15:21	WinRAR ZIP 压缩	8,901 KB
📲 视频 🔤 java_test1.	zip	2017/10/13 16:01	WinRAR ZIP 压缩	5,444 KB
No. 10 International Internat	nt.zip	2017/11/9 9:54	WinRAR ZIP 压缩	4 KB
🔮 文档 🛛 🚺 maven_jav	a_test.zip	2018/3/29 10:44	WinRAR ZIP 压缩	470 KB
↓ 下载 php_test.z	ip	2017/6/26 9:32	WinRAR ZIP 压缩	1,333 KB
♪ 音乐 Withon_tes	st.zip	2015/9/6 14:08	WinRAR ZIP 压缩	43 KB
三 桌面 🔛 sql_test.zip	þ	2019/4/15 14:50	WinRAR ZIP 压缩	18,868 KB
🏪 本地磁盘 (C:)				
本地磁盘 (D:)				
- *				
文件名(N):			✓ 所有文件 (*.*)	~

4. 创建完成后,点击"查看我的检测工程"

♥ 總在这里:项目管理 > 项目组[TestGroup] >	新建工程	
		*****
* T 把 冬 指	java-test	《宣君上祖列录
TITION		
*版本或说明	v1.0	
*6		
完成检测	1, 查看我的检测工程	x
*#4		
*是否Maven工程	Ϋ́Ε Υ	
	上传源代码zip压缩包或jar/war包	
	● 检测前,请把与检测无关的文件(.svn,.git,exe,word等)都删除,以免影响	》前检测效率
	❶ 压缩包请使用zip格式	

## 5. 进入该工程的检测详情页

缺陷审计视图	风险级别(默认) ~	检测结果摘要缺陷分布图列	&TOP10 批量审	计(按缺陷类型)	批星审计(导入) 项目检测信息	
共667个缺陷, 0个未显示(忽略、误響	,当前显示667个, 曾报、未判定问题智不处理)	安全缺陷/质量缺陷	TRA		审计情况	
▶ 严重(201)		总数	183	484	已审计/未审计	0 / 667
▶ 高风险(15)		严重	105	96	未判定问题,暂不处理	0
■ 中等风险(300) ■ (F区)除(87)		高风险	11	4	忽略	0
<ul> <li>管告和信息(64)</li> </ul>		中等风险	60	240	误报警	0
		低风险	6	81	存在缺陷	0
		警告和信息	1	63	存在缺陷,在下个版本处理	0
					存在缺陷,以后再考虑处理	0
	v	SIZE 21124 (可执行代码行数)/3	3933 (代码总行数)		检测文件	
		21124(回341)(1913)(373) 【代码评分 <b>1</b>	282 (2019) (1 (1 CCCC)		+LXIA27	
		系统默认代码评分规则	度)		★	
		与目标基线对比分析				
		目标基线:			法禁約階数 報 「あ」「日本	/indows

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)

目组名称: 请输入项	词目组名称 项目名称	: 请输入项目名	称 项目创建人: 诗输入	项目创建人(账号、姓名 Q 宣询	日新建项
项目组名称	所属部门	工程总数	周期工程总数	创建时问 \$	操作
默认	默认部门	0	0	2019-04-10 18:17:19	查若 - 创建 - 》修改
TestGroup	默认部门	2	0	2019-04-04 14:35:54	<b>査査 → 创建 → 2修夜 × 勝徐</b> 工程(上传)
★ 您总共参与	了2个项目组;完成检测	2个, 检测异常 <mark>0</mark>	个, 检测中 <mark>0</mark> 个。		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。

*T#246	tect-2
二任日初	
*版本或说明	v2.0
*编程语言类型	PYTHON *
*引擎选择	☑默认
*检测安全级别	回 默认 严重及高风险 自定义
*检测时间	立即检测
*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 v
	<ul> <li>✔ 创建检测工程</li> <li>● SVN URL示例: https://192.168.1.20:8443/svn/test/</li> <li>● Git URL示例: http://192.168.1.20:28686/projects/test.git</li> </ul>

#### 3) 创建完成后,点击"查看我的检测工程"

THON 获认 E看我的检测工	<b>、</b>						ж
铁认 查 <mark>看我的检测</mark> 工	定程						ж
電着我的检测工	程						×
國我的检测工	程						
:p://192.168.0	0.233/liuq	ingjun/di	ispatcher	-test.git			
qingjun							
	٣						
	p://192.168. qingjun •••••	:p://192.168.0.233/liuq qingjun  • 的剧社会知工程	ip://192.168.0.233/liuqingjun/di qingjun ••••• •	p://192.168.0.233/liuqingjun/dispatcher qingjun ••••• • 的副社会测工程	p://192.168.0.233/liuqingjun/dispatcher-test.git qingjun ••••• • 的副社会和工程	p://192.168.0.233/liuqingjun/dispatcher-test.git qingjun •••••	p://192.168.0.233/liuqingjun/dispatcher-test.git qingjun •••••• ▼

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。

缺陷审计视图	风险级别(野认) >	检测结果摘要缺陷分布图入	及TOP10 批量审	前十(按缺陷类型)	批量审计(导入) 项目检测信息	
共325个缺陷。 0个未显示(忽略、误警	当前显示325个, 雅、未判定问题暂不处理)	🕜 安全缺陷/质量缺陷	â		审计情况	
▶ 严重(32)		总数	20	305	已审计/未审计	0/325
■ 高风险(3)		严重	9	23	未判定问题,暂不处理	0
		高风险	0	3	忽略	0
▶ 警告和信息(72)		中等风险	9	116	误报警	0
		低风险	1	92	存在缺陷	0
		警告和信息	1	71	存在缺陷,在下个版本处理	0
					存在缺陷,以后再考虑处理	0
	×	SIZE			+0.30++-/#	
		(4932)(7)(1000)(3)	1131 (1055-1380)		1220,2,1+	
		系统默认代码评分规则		「副保存」		
		15.31 ‰ (千行代码缺陷密	度)			
		┃ 与目标基线对比分析				
		目标基线:			违禁缺陷数量; 历以白 转到"设置	0 indows "以激话 Windows

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] > 新發	a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 <b>v</b>
*是否Maven工程	否 v
	<ul> <li>② 创建检测工程</li> <li>③ SVN URL示例: https://192.168.1.20:8443/svn/test/</li> <li>④ Git URL示例: http://192.168.1.20:28686/projects/test.git</li> <li>④ 墙量检测释义: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</li> </ul>
2)检测完成后弹出提示	
MavenT程 否 V	
E	36
<ul> <li>●里程碑创建成功, 检测将于</li> </ul>	- 2019-08-27 10:00:00 进行
CLEMGAGX97 TRAVEL	

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。

您在这里:项目管理 > 项目	8[8.23] > 按指定时间检测工程列表			
λ į				
显示状态	按指定时间检测工程名 称	检测时间	创建时间	操作
☞正常	[JAVA] test-2	2019-08-27 11:00:00	2019-08-27 10:09:31	●修改 ★删除

# 3.2.3 创建周期工程

1. 选择"周期工程"

<b>夏目组名称:</b> 清输入J	页目组名称 项目名称	: 请输入项目名称	项目创建人: 请输	入项目创建人(账号、姓全 Q 查询	计翻译
项目组名称	所属部门	工程总数	周期工程总数	创建时间 \$	操作
默认	默认部门	0	0	2019-04-10 18:17:19	查看 → 创建 → 《修改
TestGroup	默认部门	5	0	2019-04-04 14:35:54	查看→ 创建→ /修改 × 制除 工程(上传)
★ 您总共参与	了2个项目组; 完成检测	5个, 检测异常 <mark>0</mark> 个	,检测中0个。		工程(版本控制工具) 工程(周期检测)
					1/1

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。

♀ 您在这里:项目管理 > 项目组[TestGroup] >	新建周期工程
*工程名称	test
*编程语言类型	JAVA/JSP •
*引擎选择	▼默认
*检测安全级别	111 默认 严重及高风险 自定义
*周期类型	按天 ▼
*检测计划	每 1 天扫描一次
*检测时间	11 点整
*版本工具	git v
*Git URL	http://192.168.0.233/liuqingjun/dispatcher-test.git
*用户名	liuqingjun
*密码	******
*是否Maven工程	否 <b>v</b>
*是否进行增量检测	否 <b>v</b>
	G 创建周期自动检测工程
	<ul> <li>SVN URL示例: https://192.168.1.20:8443/svn/test/ svn://192.168.1.20:8443/svn/test/</li> <li>Git URL示例: http://192.168.1.20:28686/projects/test.git</li> </ul>

3. 填写必填项后,点击【创建周期自动检测工程】按钮

	*项目路径	git	*		
	*Git URL	https://githu	b.com/scribejava,	/scribejava	
	*用户名	yorsal			
					×
文件路			D 创建周期自z	动检测工程	
		C 创建周期自 Offortify引擎中	动检测工程		

4. 创建完成,查看工程

	*项目路径	git •			
	*Git URL	https://github.com/scribe	java/scribejava		
	*用户名	yorsal			
	文件證	创建成功,首次检测将 2 做题周期自动检测工程 Ofortify引擎中文路径可能导致 0 SVN URL示例: https://192.1 0 Git URL示例: http://192.1	F 2019-05-14 07:00:00 进行 减码 2.168.1.20:8443/syn/test/ syn://192.16 68.1.20:28686/projects/test.git	<b>38</b> 58.1.20:8443/svn/test/	
<	♀ 您在这里:项目管理 > 项目组[JAVA] >	周期工程列表			
welcome SHE	Q 请输入周期工程名称,支持模糊:				<u></u> 白 创建周期工程
Welcome, Eleg	显示状态	检测工程名称	下次检测时间	创建时间	操作
<b>希</b> 首页	≌ II\$	[JAVA] 周期工程	2019-05-14 07:00:00	2019-05-13 09:33:10	✔修改 ■停止 ×删除
■ 项目管理					
山 统计分析					

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

<b>组名称:</b> 清输入项	词目组名称 项目名称	请输入项目名称	项目创建人: 请输〉	Q. 查询	日新建项目
项目组名称	所属部门	工程总数	周期工程总数	创建时间 \$	操作
默认	默认部门	0	0	2019-04-10 18:17:19	查看 → 创建 → ●修政
TestGroup	默认部门	5	0	2019-04-04 14:35:54	<ul> <li>查看 → 的建 → //修改 × 酬除</li> <li>工程</li> </ul>
★ 您总共参与"	72个项目组;完成检测9	个, 检测异常 <mark>0</mark> 个	,检测中0个。		按照指定时间检测工程 周期检测工程 1/1 1

进入工程列表页面,查看该项目组下的所有工程

的项目	民的缺陷						
请输入工程	名称,支持模糊查询						土 创建新检测
显示状态 🗸	检测工程名称	版本	代码行数 ≑	安全缺陷/质量缺陷	已修复/审计/总数	创建时间 \$	操作
◎ 检测完成	[JAVA] TEST	v1.0	15105	7 / 746	0 / 0 / 753	2019-08-27 09:55:23	
● 检测完成	[JAVA] test-2	v1.0	31191	20 / 305	0 / 0 / 325	2019-08-27 09:38:33	≝ - ≤ - 💼
● 检测完成	[PYTHON] test-2	v2.0	1662	0/0	0/0/0	2019-08-27 09:35:01	<b>≧</b> - <b>≤</b> - <b>≡</b>
-		v1.0	22022	102 / 404	0/0/667	2010-08-26 17:52:15	

#### 2. 按照指定时间检测工程的查看

组名称: 请输入项	目组名称 项目名称	请输入项目名称	项目创建人: 请输入	项目创建人(账号、姓名 Q 查询	[] 新建项
项目组名称	所属部门	工程总数	周期工程总数	创建时间 \$	操作
默认	默认部门	0	0	2019-04-10 18:17:19	查看→创建→ /修改
TestGroup	默认部门	5	0	2019-04-04 14:35:54	<u> 査</u> 査 - 创建 -
★ 您总共参与了	72个项目组;完成检测	个, 检测异常 <mark>0</mark> 个,	检测中0个。		按照指定时间检测工程

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。

示状态	按指定时间检测工程名 称	检测时间	创建时间	操作
正常	[JAVA] test-2	2019-08-27 11:00:00	2019-08-27 10:09:31	修改 X删除

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

目组名称: 请输入工	页目组名称 项目名称:	请输入项目名称	项目创建人: 请输入	项目创建人(账号、姓名 Q 查询	[] 新建项
项目组名称	所属部门	工程总数	周期工程总数	创建时问 \$	操作
默认	默认部门	0	0	2019-04-10 18:17:19	查若 → 创建 → 』 多数
TestGroup	默认部门	5	0	2019-04-04 14:35:54	<u> 金石</u> ◆ 创建 → <b>●</b> 修改 × 删除 工程
★ 您总共参与	了2个项目组;完成检测5-	个, 检测异常0个,	检测中0个。		按照指定时间检测工程

#### 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。

:	♀您在这里:项目管理 > 项目	目组[JAVA] > 周期工程列表			
	Q 请输入周期工程名称,	支持機關			<b>注 创建周期工程</b>
	显示状态	检测工程名称	下次检测时间	创建时间	操作
	☞ 正常	[JAVA] 周期工程	2019-05-14 07:00:00	2019-05-13 09:33:10	✔修改 日停止 苯删除

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

的项目	我的缺陷						
请输入工程	名称,支持模糊查询						[] 创建新检测]
显示状态 🗸	检测工程名称	版本	代码行数◆	安全缺陷/质量缺陷	已修复/审计/总数	创建时间♀	操作
● 检测完成	[JAVA] TEST	v1.0	15105	7 / 746	0/0/753	2019-08-27 09:55:23	<b>■ - ▲ - </b>
9 检测完成	[JAVA] test-2	v1.0	31191	20 / 305	0 / 0 / 325	2019-08-27 09:38:33	检测结果
●检测完成	[PYTHON] test-2	v2.0	1662	0/0	0/0/0	2019-08-27 09:35:01	
9 检测完成	[JAVA] java-test	v1.0	33933	183 / 484	0/0/667	2019-08-26 17:52:15	🖹 - 🔺 📋
● 检测完成	[C] <b>c1</b>	v1.0	13975	65 / 149	0/0/214	2019-08-21 11:22:28	

2. 进入检测详情页

陷审计视图	风险级别(默认) ~	位则结果搁置 或相力 印图	QTOPTO 加里F	単い(1958(PEI963E) 1	心里申口(守八) 现日应改造息	
共753个缺陷,当前显 0个未显示(忽略) 译警报 未	示753个, 判定问题暂不处理)	② 安全缺陷/质量缺	掐		☞ 审计情况	
『重(12)	P 2 Marth - Shake HH - 1 Print Pake	总数	7	746	已审计/未审计	0 / 753
风险(5)		严重	1	11	未判定问题,暂不处理	0
利以验(1) 11命(654)		商风险	2	3	忽略	0
和信息(81)		中等风险	0	1	误报警	0
		低风险	0	654	存在缺陷	0
		警告和信息	4	77	存在缺陷,在下个版本处理	0
					存在缺陷,以后再考虑处理	0
	. <del></del>	SIZE 9131 (可执行代码行数)/15	检测文件	检测文件		
		【 代码评分 8				
		系统默认代码评分规则		* 🖹 (###	*	<u> 술</u>
		26.59 ‰ (千行代码缺陷密	度)			
		┃ 与目标基线对比分析				

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

43

♀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	webGoatb.u/JavaSource/org/owasp/webgoat/lessons/HttpDnly.java
▶ 严重(371)	113 if(httpOnly) {
▶ HTTP响应分割(4)	<pre>114 // System.but.printin( httponiy: setting httponiy for cookie ); 115 setHttponly(s);</pre>
HttpOnly.java:198(setHttpOnly)	<pre>116 } else { 117 // System.out.println("HttpOnly: Removing HttpOnly for cookie");</pre>
HttpOnly.java:212(removeHttpOnly)	<pre>118 removeHttpOnly(s); 119 }</pre>
config.isp:10( ispService)	120 121 if(action != null) {
A redirect isn:10( isnService)	122 if(action.equals(READ)) {
■ HTTP头文件揭U(2)	125   and reveauce con(s); 124 } else if(action.equals(WRITE)) {
	125 handleWriteAction(s); 126 } else {
	<pre>127 //s.setMessage("Invalid Request. Please try again."); 128 }</pre>
	129 }
	131 try
	<pre>132 133 ec.addElement(makeContent(s));</pre>
XPath)±A(1)	134 } 135 catch (Exception e)
	136 { 137 s.setMessage( "Error generating " + this.getClass().getName() );
→ XMIL97日20年1年(1) ■ XMIL97日2日日1日(1)	138 e.printStackTrace(); 139 }
- APath)土人(1)	142 }
■ 反射型跨站脚本(135)	143 144
■ 命令注入(7)	145 /** 146 * DOCUMENT ME!
■ 存储型跨站脚本(54)	147 * 149 * Anaturn DOCIMENT MEL
密钥安全(硬编码加密密钥)(3)	149 */
<ul> <li>UNL単足凹(J)</li> <li>VMLは認定(注)(4)</li> </ul>	150 protected Category getDefaultCategory() 151 {
■ XIVIL/Y部头体注入(1)	152 return AbstractLesson.A4; 153 }
■ XML牌衍蒲注入(1)	154
XPath)土入(1)	156 /** 157 * Gate the bints attribute of the Emplicement phiert
■ 反射型跨站脚本(135)	157 dets the mints attribute of the emailstreen object
■ 命令注入(7)	159 ° greturn The hints value 160 */
■ 存储型跨站脚本(54)	161 protected List getHints() 162 {
■ 密钥安全(硬编码加密密钥)(3)	163 List <string> hints = new ArrayList<string>(); 164 hints add( "Read the directions and try out the huttons." );</string></string>
■ 文件名泄露(4)	165 return hints;
<del>决</del> 陷细节分析	(
HttpOphyiaya102【本項】 (唐讷近回 aptCophia()) *	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
THOOLETERING THE RECOOKIE ()	172 BASE64Encoder encoder = new BASE64Encoder();
XML外部实体注入(1)	173 174 try {
■ XML解析器注入(1)	<pre>175 md = MessageDigest.getInstance("SHA"); 176 buffer = new Date() toString() getBytes();</pre>
■ XPath注入(1)	177 178 md undate/buffan):
■ 反射型跨站脚本(135)	<pre>179 value = encode.encode(md.digest());</pre>
■ 命令注入(7)	100 original = value; 181
■ 存储型跨站脚本(54)	<pre>182 } catch (Exception e) { 183 e.printStackTrace();</pre>
■ 密钥安全(硬编码加密密钥)(3)	184 }
文件名泄露(4)	186 return value;
购细节分析	
	▲
HttpOnly.java:192【来源】 值被返回 getCookie ()	
tpOnly.java:198【跟踪】 字符串连接	
pOnly.java:198 【跟踪】 字符串连接	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
pOnly.java:198【爆发点】 参数 UNIQUE2U + "=" + coc	风险级别 严重
	dial dial dial dial dial dial dial dial
	#K14AAG
	<b>审计信息</b> 最多200个字符
*	
	2801 Cr DAD
	Statistical according to the second sec

# (1) 缺陷详情

轴购审计加图		检测结果摘要 缺陷分布圈及TOP10 批量审计(按缺陷类型) 批量审计(导入) 项目检测信息
	风险级别(默认) ~	WebGoat5.0/JavaSource/org/owasp/webgoat/lessons/HttpOnly.java
共发现1958个问题。	当前1958个问题可见	1 package org.owasp.webgoat.lessons:
严重(371)		z import java util Accavlist:
HTTP响应分割(4)		4 import java.util.Date;
HttpOnly.java:1	98(setHttpOnly)	6 import java.security.MessageDigest;
·····☆ HttpOnly.java:2	12(removeHttpOnly)	<pre>7 8 import javax.servlet.http.HttpServletResponse;</pre>
	pService)	9 import organache ers Element:
redirect.jsp:10(	jspService)	<pre>import org.apache.ecs.ElementContainer;</pre>
▶ HTTP头文件操纵(2)		13 import org.apache.ecs.html.A;
		<pre>14 import org.apache.ecs.html.Form; 15 import org.apache.ecs.html.IMG;</pre>
■ URI 亜完向(5)		<pre>16 import org.apache.ecs.html.Input; 17 import org.apache.ecs.html.ID;</pre>
► YMI 小部立(計注 ) (1)		18 import org.apache.ecs.html.TR;
XAN AT A 74 C 582 + ) (4)		<pre>import org.apacne.ecs.ntmlad.e; 20 import org.apacne.ecs.ntm.lad.e;</pre>
		<pre>21 22 import sun.misc.BASE64Encoder;</pre>
		23 /************************************

(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

缺陷审计 审计	十日志 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 () \'. 不可信 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	存在缺陷
分配	login2
优先级	高
审计信息	存在缺陷
操作	常保存

## 被指派人首页:需要修复信息

<	您参与了 6个项目组 »	
welcome, 管理员	? 发现的缺陷	
	总数	9161
脅 首页	需要审计	9120
■ 项目管理	需要复审	1
山 统计分析	需要修复	40
🧧 检测规则管理 💦 <		

(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。

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			
审计人 login2(管理员)	审计时间 (2019-05-	-15 13:14:37)	风险级别严重	审计状态 存在缺陷	分配 login2	优先级 <mark>高</mark>	审计信息存在缺陷	
(4) S Cookieges Co	缺陷原理 ( 全保使用HTPS发送cocc SessionD Java209 AuthenticationCockie, avar209 [電影点]	里/修复建 kkie/(4) ] java:146		H出缺陷的 tring password = null tring password = null username = s.getPi actch (PerameterNotFor ); ry H日志 缺陷原理/修 全(未使用HTT 器波持命介 cookle 的 se	り原理及修 arser()-getStringParamet andException pnfe) 実建议 参考信息 相称 TPS发送cookid urre 続記、如果定要了法統統	<ul> <li>复的建</li> <li>(USERNAHE);</li> <li>(AMABINE</li> <li>(AMABINE</li> <li>(AMABINE</li> </ul>	议 HTTPS 物族 cookie。 德过未加密的新	→ 画描学注 cookle 将行

创建了 cookie, 但未将 secure 标记设置为 true.

示例 1: 在下面的示例中, 在未设置 secure 标记的情况下将 cookie 添加到响应中。

示例

4

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。

Cookie cookie = new Cookie("emailCookie", email); response.addCookie(cookie); 如果应用现程用调性用 HTTS A HTTP。但没有设置 secure 标记,那么在 HTTPS 请求过程中发送的 cookie 也会在随后的 HTTP 请求过程中被发送。通过未知密的无线这接截取网络信息流对攻击省而E

检测结果摘要	缺陷分布图及TOP10	批量审	审计(按缺陷类型)	批量审计(导入)	项目检测信息 缺陷详	情
🕜 安全部	决陷/质量缺陷			() 审	计情况	
总数		7	746	已审计,	/未审计	0 / 753
严重		1	11	未判定	问题,暂不处理	0
高风险		2	3	忽略		0
中等风险		0	1	误报警		0
低风险		0	654	存在缺	陷	0
警告和信息	3	4	77	存在缺	陷,在下个版本处理	0
				存在缺	陷,以后再考虑处理	0
2019-08-2 SIZE 9131 (可执	7 09:55:23—2019-08-27 行代码行数)/15105 (代码#	09:55:58 急行数)	3		总用时: 35秒 检测离(先)、	Vindows
【代码评分 系统默认(	1		▼ 圖 强待			
26.59 ‰ (	千行代码缺陷密度)					
与目标基	线对比分析					
目标基线:					违禁缺陷数量	: 0

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。

检测结果摘要	缺陷分布图及TOP10 批	建审计(按缺陷类型)	批量审计(导入)	项目检测信息	缺陷详情
筛选条件					
风险级别	严重				v.
缺陷类型	全部				¥
审计状态	未审计				v
操作	計查询				
批量审计					
审计状态	未审计				*
审计信息	最多允许200个字符				1
操作	開保存				

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。

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	
筛选条件						
风险级别	严重					Ŧ
缺陷类型	变量空指针引用(5)					v
审计状态	未审计					Ŧ
操作	<b>計查询</b> 符合条件相	的总共有5条缺陷				

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。

批量审计		
审计状态	存在缺陷	
分配	yorsal	
优先级	南	
审计信息	存在缺陷	
操作	<b>周保存</b>	

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)

				15日46月11年日 445年3年4年	
缺陷审计视图 风险级别(默认) ~	位则结果捕装	现的力和图及10P10 批里車	北度報告经生) 批里审计(导人)		
	原审计信息	5.13.3(v1.0)			
共发现1958个问题,当前1958个问题可见	124-	(First)			
- 一里(3/1) ■ 高回除(131)	J#TF	<b>M M</b>			
■ 中等风除(837)					
▶ 低风险(509)					
警告和信息(110)					

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。

检测	则结果摘要	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
	项目名称		TEST			
	检测时间		2019-0	8-27 09:55:23		
	编程语言类	美型	JAVA			
	检测安全级	2月1	默认			
	创建人		yorsal			
	maven工利	里	不是ma	ven项目		
	白名单规则	川集	无			
	文件路径过	İ 滤规则集	无			
	携带审计信	息	原审计工	页目		
	引擎名称					
	检测项目类	美型	源代码机	金测		
	是否是增量	と 检測	岙			
	项目路径		https://	github.com/shao1	1988007/javatest	3
	检测状态		检测完成	戉		NALMET A 4 P 1

# 3.3.3 缺陷明细

#### 1. 选择工程,点击右侧的【缺陷明细】按钮

♀您在这里:项目管理 > 项目组[TestGroup] > 工程列表

我的项目	我的缺陷						
Q 请输入工程	名称,支持模糊查询						□ 创建新检测工程 -
显示状态 •	检测工程名称	版本	代码行数 🕏	安全缺陷/质量缺陷	已修复/审计/总数	创建时间 \$	操作
◎检测完成	[JAVA] TEST	v1.0	15105	7 / 746	0/5/753	2019-08-27 09:55:23	
◎ 检测完成	[JAVA] test-2	v1.0	31191	20 / 305	0/0/325	2019-08-27 09:38:33	检测结果 ++Pagelfm
◎ 检测完成	[PYTHON] test-2	v2.0	1662	0/0	0/0/0	2019-08-27 09:35:01	
◎ 检测完成	[JAVA] java-test	v1.0	33933	183 / 484	0 / 0 / 667	2019-08-26 17:52:15	<b>₽</b> - <b>2</b> - <b>8</b>
●检测完成	[C] <b>c1</b>	v1.0	13975	65 / 149	0/0/214	2019-08-21 11:22:28	<b>≧</b> - <b>≜</b> - <u>8</u>

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

循项 目组	TestGroup	w	所属工程	TEST (v1.0)		缺陷类型	全部	×
(件名			方法名			与基	线对比的违禁缺陷	搜索
所属工程	缺陷状态 •	缺陷	缺陷分类 ▼	缺陷类型	风险等级 *	审计状态 🔻	审计时间	操作
TEST	未分配	compressclient.java:4	质量缺陷	未捕获异常	低风险	未审计	无	<b>三</b> 查若详情
TEST	未分配	compressclient.java:4	质量缺陷	未捕获异常	低风险	未审计	无	■ 查看详情
TEST	未分配	compressclient.java:4	质量缺陷	未捕获异常	低风险	未审计	无	■ 查若详情
TEST	未分配	compressclient.java:4	质量缺陷	未捕获异常	低风险	未审计	无	<b>冒 查</b> 君详情

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。

所属工程	已分配未修复 *	缺陷	缺陷分类 ▼	缺陷类型	风险等级 🔻	审计状态 🔻	审计时间	操作
5.13.3	已分配,未修复	redirect.jsp:12	安全缺陷	URL重定向	严重	存在缺陷	2019-05-15 15:05:49	■ 查看详情
5.13.3	已分配,未修复	JavaScriptValidation.jav a:156	安全缺陷	反射型跨站脚本	严重	存在缺陷	2019-05-15 15:05:49	■ 查看详情
5.13.3	已分配,未修复	EditProfile.jsp:10	安全缺陷	跨站请求伪造	严重	存在缺陷	2019-05-15 15:05:49	■ 查看详情
♀您在这里:项 缺陷审计视迟 ★ redirect.jsp:	目管理 > 项目组[JAVA] 图 12 () URL里定向	> 项目(5.13.3) > 缺陷列		/ebContent/lessons/C language="java" cont ccding="150-8859-1 html PuBLIC "-//H3C 9-equiv="Content-Typ P Splitting :s.sendRedIrect("/We "Screens" + re "Skreens" + re "Skreens" + re	Seneral/redirect.jsp entType="text/html; c % //DTD HTML 4.01 Trans e" content="text/html b0ost/atteck?" + equest.getParameter(" t=yzeSlanguage=" + re	<pre>harset=ISO-8859-1 itional//EN" "http ;; charset=ISO-885; Sereen") + emu") + emu") +</pre>	://www.w3.org/TR/html4/ -1"> ("language"));	/loose.dtd">
缺陷审计	审计日志 缺	陷原理详述 参	16 考信息 缺	各相似图				
当前缺	略 未捕获异常							
缺陷详	情 方法 \'main	n\'未捕获异常\'java	a.awt.Headles	sException\'.				
风险级	別严重							
审计状	态存在缺陷	1						8
分	vorsal							
优先	级高							
注	存在缺陷							
操	作日保存					21 11	數活 Windov	VS

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

	14201710/22/2	1K+	10175-96		口收生产生产数	Alizantia 🔺	19.16
显示状念 ▼	恆湖土性白帅	版本	TUE91J£X ₹	安主畎阳/ 顶重畎阳	已陰夏/审计/忌奴	的狂剧的	BRTF
检测完成	[JAVA] java-test	v1.0	33933	183 / 484	0 / 0 / 667	2019-08-26 17:52:15	
检测完成	[C] <b>c1</b>	v1.0	13975	65 / 149	0/0/214	2019-08-21 11:22:28	PDF
							EVCEL
							HÆXIKHƏH

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;

		~
的合	自定义导出报告(多选)	
	PDF	
家,	◎ WORD	
	导出摘要✓	
检		1
[J)	☑ 信息详情 ☑ 开源组件CVE漏洞检测	
[]/	L	
[11	- 导出缺陷 ✓	
[]/		1
g	□ 按风险类型	
E.	按書任人	
	────────────────────────────────────	
	按安全缺陷/质量缺陷	
	L	4
ePe		
	[] 导出报告	
2		

# 3.3.4 删除

# 该删除是将上传的工程删除

的项目	我的缺陷						
请输入工程	名称,支持模糊查询						① 创建新检测
显示状态 🗸	检测工程名称	版本	代码行数 🗢	安全缺陷/质量缺陷	已修复/审计/总数	创建时问 \$	操作
❷ 检测完成	[JAVA] <b>java-test</b>	v1.0	33933	183 / 484	0 / 0 / 667	2019-08-26 17:52:15	
	(C) c1	v1.0	13975	65 / 149	0/0/214	2019-08-21 11:22:28	

# 3.4 修改/删除

#### 1. 修改项目组

1组名称: 请输入项	近日组名称 <b>项目名称</b>	请输入项目名称	项目创建人: 请输入	项目创建人(账号、姓名) Q,查询	<u></u> 1 新建项
项目组名称	所属部门	工程总数	周期工程总数	创建时间 \$	操作
默认	默认部门	0	0	2019-04-10 18:17:19	査石 → 创建 → ●修改
TestGroup	默认部门	2	0	2019-04-04 14:35:54	查看 - 创建 - <b>创建</b> - 翻除
★ 您总共参与	了2个项目组;完成检测2	2个, 检测异常 <mark>0</mark> 个,	检测中0个。		

2. 可修改项目组名称、所属部门、项目组成员、项目目标基线

修改项目组信息	
*15日422	TestGroup
坝口坦口尔	
*所属部门	默认部门 ▼
*创建时间	2019-04-04 14:35:54
*项目组成员	vorsal
	*
	<
项目目标基线	请选择 ▼

3. 删除

# 删除项目组,及可将项目组中的所有工程也删除

组名称: 清输入项	5日组名称 <b>项目名</b>	称: 请输入项目名积	你 <b>项目创建人:</b> 请输入	项目创建人(账号、姓谷 Q 查询	<b>造 新建</b> 項
项目组名称	所属部门	工程总数	周期工程总数	创建时间 \$	操作
默认	默认部门	0	0	2019-04-10 18:17:19	查君 → 创建 → 》修改
TestGroup	默认部门	2	0	2019-04-04 14:35:54	查看→ 创建→ 2修改 × 影除

# 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

	<	♀您在这里:	配置管理 > 執路规则集				
welcome, 管理员		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	*	Q 查询		
<b>谷</b> 首页			缺陷规则集名称	编程语言	创建人	创建时间	操作
□ 项目管理			default(默认系统固定规则)	JAVA/JSP	yorsal	2016-07-05 16:13:17	●查若
山山 统计分析			high(严重及高风险,系统固定规则)	JAVA/JSP	yorsal	2016-07-05 16:13:17	@ 查石
🧧 检测规则管理	~		default(默认,系统固定规则)	C/C++	yorsal	2016-07-05 16:13:41	●查查
缺陷规则管理	<		high(严重及高风险,系统固定规则)	C/C++	yorsal	2018-11-24 18:15:11	●查吞
缺陷规则集			default(默认,系统固定规则)	PHP	yorsal	2018-11-24 18:15:33	●古斎
自定义规则	<			0110	002020	2040 44 24 40 46 40	
自定义白名单	<		high(严重)及同风险,系统固定规则)	PHP	yorsal	2018-11-24 18:16:49	●查者

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

缺陷规则集	添加新缺陷规则集
	"缺陷规则集名称
	*编程语言 JAVA/JSP v
	金莲
	- Tornsteina and
	- + 「其他问题
	□ API巡用(不安全的API)
	- 1 (信息泄露
	- 2 环境问题
	- 2
	- 1 1 输入验证
	- 1 IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
	_ ★findbugs
	✓ ¥8/01

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。

陷规则集	添加新缺陷规则集					
<b>各规则集</b> 名称	2	编程语言	全部	V Q 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	✔ 編輯 × 删除
	cs-all		C#	yorsal	2019-01-24 17:22:59	▲ 新橋 × 翻絵
	java-test		JAVA/JSP	yorsal	2019-02-25 09:54:42	✔ 編編 × 删除
	java规则集		JAVA/JSP	login2	2019-04-26 10:40:55	✔ 編編 × 翻除
	test1		C#	login2	2019-04-26 13:27:52	✓ 編編 × 翻絵
	Ü		C#	login2	2019-05-13 13:56:36	▲ 編輯

# 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。

- 成幼祖:	-	<	♀您在这里:知识库WIKI > JAVA漂代	网缺陷			
welcome, 张三         一吸納船:         ····································							
welcome, 张三							
<ul> <li>Weikolne, Sk</li> <li>● 読む車中回窓(NSS)</li> <li>● 致源注入印度</li> <li>● 致源注入印度</li> <li>● 致源注入印度</li> <li>● 按照印刷印度</li> <li>● 计算机中国</li> <li>● 可能的目前</li> <li>● 可能的目前目前</li> <li>● 可能的目前</li> <li>● 可能</li> <li>● 可能</li> <li>● 可能</li> <li>● 可能</li> <li>● 目前</li> <li>● 目前&lt;</li></ul>	welcome 2K-		一级缺陷:请选择	▼ 二级缺陷	:请选择	▼ Q 香油	
	welcome, sk_					and the second s	
			+ 跨於樹本问题(XSS)				
	首页		王 数据注入问题				
通言管理         •         进程和描述之人问题           论 地界风的管理         ·			王 未验证用户输入问题				
·	项目管理		王 进程和路径注入问题				
			→ : : : : : : : : : : : : : : : : : : :				
blctarWIKI      cline     clin	检测规则管理	<	王 克隆问题				
JAVAI#CH3bH3     - 日 钱制回题       JAVAI#CH3bH3     - 日 转线回题       C/C+#ErCH3bH3     - 日 转线回题       - 日 转线回题     - 日 时线时回题       - 日 打线时题     - 日 比线和局部代词问题       - 日 打线和局部代词问题     - 日 北和局部代词问题       - 日 大和代码     - 日 北和局部代词问题	☎ 知识库WIKI	~	-王 拒绝服务问题				
JAVA29CV28494     - 5 時時時間       C/C++100C08498     - 6 時時時間       - 1 時時以間間     - 1 時時以間間       - 1 時時以間回聴     - 1 時時以間回聴       - 1 時時以間回聴     - 1 時時以間回聴       - 1 時時以間回聴     - 1 時時以間回聴       - 1 時時以間     - 1 時時以間回聴       - 1 時時以間     - 1 時時以間       - 1 日本以前時代時间回聴     - 1 日本以前時代時间       - 1 日本以前時代時间     - 1 日本(1)			-王 性能问题				
C/C++/銀代初時期         -10 期時回週           # 成成管理         -10 期時回週           # 成成管理         -10 期時回週           -10 期時回週         -10 期時回週           # 周中仅限管理         -10 期時回週           -10 期時回週         -10 期時回週           -10 期時回週         -10 期時回週           -10 期時回週         -10 明時回週           -10 期時回週         -10 明時回週           -10 開始中台的问题         -10 可能的牛街同週           -10 可能的牛街回週         -10 可能的牛街時回週           -10 可能的牛街時間         -10 10 10 10 10 10 10 10 10 10 10 10 10 1	JAVA源代码缺陷	1	1. 明封装问题				
	C/C++源代码缺	貊	11 朔加密问题				
集成管理         ・コロ14PDCEPU40G           第 月户収録管理         ・ロロ14PDCEPU40G           第 月户収録管理         ・ロロ14PDCEPU40G           第 配置管理         ・ロロ14PDCEPU40G           • 配置管理         ・ロロ14PDCEPU40G           • 配置管理         ・ロロ14PDCEPU40G           • 可加4PDCEPU40G         ・ロロ14PDCEPU40G           • 可加4PDCEPU40G         ・ロロ14PDCEPU40G           • 和田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田			二土 信息液漏问题				
日中収録審査     ・     <	集成管理	<	- 王 始時近年回越 王 忽略近回信问题				
HUT DURg 書理     C							
<ul> <li>         ・ 配置管理         く         ・         ・         ・</li></ul>	10/11×102官理		1 可维护性的问题				
-田 冗余代码	記置管理	<	王 比较和哈希代码问题				
			王 冗余代码				
副 日志管理 < □● 资源泄漏问题	● 日志管理	<	★ 資源泄漏问题				

#### 输入查询条件查看具体缺陷详情。

□ 跨站脚本问题(XSS)	_ 跨站脚本
月站脚本           存储型跨站脚本           反射型跨站脚本           数据注入问题           + 未验证用户输入问题           + 未验证用户输入问题           + 过程和路径注入问题	* 跨站脚本 (cross-site scripting, XSS) ,跨站脚本攻击,是一种安全攻击,其中,攻击者在看上去来源可靠的能操中恶意被入译码。当有人点击能接,最入程码 作为每户网络要求的一部分搜发并且会在用中电脑上执行,一股来说会被双击者监狱信息。* 动动包要包括用中输入酸塑成内的抽染得意这种网络形式使得双击者 能改变影响场响以成页面的行为,取者者用多体方式进行球击,加速型石论运信意或这级副伴信息链接中嵌入密码,攻击者的用电助诈骗舰使现击者 它网络攻击一样,如SQL injection,很多对预给脚本 (cross-site scripting, XSS) 的距离都隔的过程时能的不安全应用,动态产生页面的网络服务器应用知规求 能输从用+输入并相慢产生的页面都已确确容了。他的合品受势能越非农旺、能适应做资料和存的电视指是是影响率承测。* 为了不受受助缺端和 (cross-site scripting, XSS) 的波击,有家建议,网络应用边球包括适当的安全机制,且服务器应该理所当然地响证输入。* 利用好XSS完全可以做一些意想不到的事情,而 XSS又是普遍存在的,就算是一些大的网站也不能笨免。 原理,风险又预防
<ul> <li>         ・</li></ul>	器站脚车都按为CSS (Cross Site Scripting), 因为思想知己一个会词"层藏性武变" (Cascarding Syle Sheets, CSS) 混淆, 为了区别, 网络安全人士为烦税 简称为XSS攻击, 器站脚车是近年来最为流行的网络攻击方式之一, 占到了网络攻击相当大的比例,由于在各种网络攻击中占有重要的地位,已经同SQL注入一起 为最正要的网络攻击形式,众多网站,如著名的Tacebook等都通通过此类攻击,国内知名的新股做得最近重遇的地位,已经同SQL注入一起 脚本起的的论言主要是监察用户的Cookie信意。Cookie信息中包含了別挖者和网络迷惑器之间的资料用艺术。包括登载记录,浏览记录等,如果攻击者得到了用户 Cookie信息。可以提供用户和网站社行交互,得到空场考虑的影响,双击者在实际这上发布一个URL能够。用户户点比较短点,用户的说道器称总体 Cookie信息。可以提供用户和网站比较近,是一次要求到Cookie信息可以比划闭者身份边间网站, 进入邮件,建筑管理和它们说道教。在中的过度器总体 Cookie信息可以说到你看自你的风险,攻击者收集到Cookie信息包括可以比划闭者身份边间网站,进入都停着,建築资料和优化信息,器站都可以包含任意的端本文件, 所以可以做的事情还不止追取Cookie信息这么滥单,希白游站脚本由于将脚本上为了网站后台数据序中,建筑资料和优于通过人争。而是构成重要开始的波道。此本者还会对发布的思思URL进行瞬间,用比说透到波给和文单,是我自要因在于网站对于用户地交的数据过途不严信,导致问题产生,从双击方式上来看,器站脚本主要分为两大美,一类是反射型的游战脚本,一美 存储起的路站脚本。
<ul> <li>②時返回値回题</li> <li>● 可能的运行时指误问题</li> <li>● 可能的住台问题</li> <li>● 比較和総希代码问题</li> <li>● 比較和総希代码问题</li> <li>● 冗余代码</li> <li>● 資源泄漏问题</li> <li>● 資源池漏问题</li> <li>● 序列化API问题</li> </ul>	15 protected void printComment(Connection conn, ServletOutputStream out, String user) throws SQLException, IOException { 16 PreparedStatement pr = conn.prepareStatement("SELECT * FROM comms WHERE user = ?"); 17 pr.setString(9, user); 18 String comment = pr.executeQuery().getString("comment"); 19 out.println("Comments: * + comment); 20 } *comment"中包含了来自數据库的數据(第 18 行)。在第 19 行,它被用于渲染 Web 页面。这意味著之前存掉在數据库中的信息未经验证使用于渲染 Web 页

# 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

	<	♀ 您在这里: 集成管理	> maven管理		《返回上一页
welcome, 张三		maven信息列表	添加maven信息		
			*仓库名称	test-maven	
斧 首页			*A+1041	http://102.159.1.20:9091/pours/content/orgung	
■ 项目管理			四神地	http://152.106.1.20.0001/16AuS/content/groups	
🧧 检测规则管理	ĸ			✓ Kin	
▶ 知识库WIKI	<			▲ 今回時時小小三時i、beta//1021/2012/09/09//annue/constant/annue/cubile	
11 集成管理	Ŷ			Compage and as a most race on the contract of the mast contract of the m	
maven管理					
🚰 用户权限管理	<				

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);

	<	♀您在这里:集成管理 >	maven管理				《返回上一页
welcome, 张三		maven信息列表 ;	添加maven信息				
		合库名称:	Q, 查询				
<b>谷</b> 首页			A#90	Adultid	Al/20142	Mahat/2	18.0-
□ 项目管理			因神句柳	七件地址	的建筑加中	1512(19)	1#TF
		1	est-maven	http://192.168.1.20:8081/nexus/content/groups/public	2019-08-27 10:46:42		✓ 修改 ¥ 删除
🧧 检测规则管理	<		S	http://192.168.1.20:8081/nexus/content/groups/public	2019-08-20 12:00:20		✔ 修改 × 删除
➢ 知识库WIKI	<	显示第 1 到第 2 条记录,总	共 2 条记录				
11 集成管理	~						
maven管理							
警 用户权限管理	<						

3. 可对添加的 maven 信息进行查询、修改和删除操作。

naven信息列表	添加maven信息				
》库名称:	Q查询				
	仓库名称	仓库地址	创建时间	修改时间	操作
	test-maven	http://192.168.1.20:8081/nexus/content/groups/public	2019-08-27 10:46:42		✔ 修改 🗙 翻
			2010 08 20 12:00:20		A 15217

# 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。

♀ 您在这里:	用户权限 >	部门管理	1				
部门列表	添加部	כז	*部门名称	市场部	]		
				✔ 添加			

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。

♀您在这里:用户权限 > 部门管理			
部门列表 添加部门			
部门名称	用户数量	创建时间	操作
1	0	2019-05-09 14:13:45	✔ 编辑 ★ 删除
1	0	2019-05-09 14:13:42	▲ 編載
测试2部门	3	2019-05-07 18:57:42	✔ 編織 🗙 删除
测试1部门	3	2019-05-07 18:57:38	✔ 編磁 × 删除
人事部	1	2019-05-07 17:52:22	✔ 編輯 × 删除
行政部	1	2019-05-07 17:52:06	✔ 編載

# 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。

田户列表60	添加用户	批量导入用户	角色分配		 	 	
		390aaa 53 7 (7 13)					
		*登录账号	yorsal				
		*邮箱	1348248665@qq.com				
		*密码	•••••				
		*重复输入密码					
		*姓名	默认				
		*性别	男	٣			
		出生日期	请选择日期				
		手机号	请输入手机号				
		QQ	请输入QQ				
		*基础角色	管理员	Ŧ			
		*部门	默认部门	¥			
		用户有效期至	请选择日期,默认永久有效				1461-1- 1 A P
			✔ 添加				) 就古 Wind 转到"设置"以

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。

用户列表。61	添加	用户 批量导	入用户 角色	百分配				
性名: 根据数	性名查询	登录账号:	根据登录账号查询	ป	Q查询			
姓名	角色	部门名称	登录账号	注册时问	上次登录时间	用户有效期至	用户授权码	操作
测试三号	管理员	默认部门	测试三号	2019-05-10 17:21:54	2019-05-10 17:22:11	无	b2416b7df5c8413589935b003ecce78c	☑ 权限 ✔ 编辑 ★ 删除
测试二号	管理员	默认部门	测试二号	2019-05-10 16:30:18	2019-05-10 16:46:47	无	ba4c518520794dcd8a2010c69564de4d	☞ 权限 🥒 編組 🗙 删除
测试一号	管理员	默认部门	测试一号	2019-05-10 16:29:45	2019-05-10 16:46:14	无	d626ca88fae14263ac512724377af5ce	C3 权限 🖌 編輯 🗙 删除
管理员6	管理员	默认部门	管理员6	2019-05-10 10:46:29	2019-05-10 13:36:12	无	d694eab589f0457389ecd6d8e75a9ec5	☑ 权限 ✔ 编辑 ★ 删除
输错密码自 动锁定	普通用户	默认部门	输错密码自 动锁定	2019-05-09 14:49:00	2019-05-10 10:36:48	无	002569df522949e9a24f3ce6a30ff5d4	☞ 权限 ● 編編 × 删除
手动锁定用 户	管理员	默认部门	手动锁定用 户	2019-05-09 14:48:03	2019-05-10 09:59:56	无	c8a0cfd7623e4796a0b6dd96cefcd2ed	☑ 权限 ✔ 编辑 🗙 删除

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。

<	♀您在这里:用户权限 > 用户管理			
	用户列表100 添加用户 批畫	晶目 計算 計算 計算 計算 一 第 色 分配 一 一 一 一 一 一 一 第 色 分配 一 一 一 一 一 一 一 一 一 一 一 一 一		
	*基础角色: ◎ 超级管理员 ●管理员 ●普道 附加角色:	题用户		
	+ 0 测试管理员			
	+ 🖸 1321			
<	+ □ 超级管理员1			
<				
~		LE 保存		

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。

♀您在这里:用户权限 > 月	用户管理			
用户列表 61 添加用	户 批量导入用户	角色分配		
		<b>选择文件</b> 未选择任何文件	Q 导入 团下载模板	

# 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。

角色列表 添加	加角色	修改角色	
		*角色名称	管理员助理
		*角色编码	000007
+ 🕑 项目管理			
➡ O APP项目管理			
+ 🕑 统计分析			
▲ ○ 检测规则管理			
+ □ 知识库WIKI			
▶ 🕑 用户权限管理			
+ 0 配置管理			
◆ ○ 文档中心			
◆ 0 日志管理			
			<b>四</b> 保存

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。

色列表 添加角色 修改角色		
色名称: 角色鄉	码: Q 查询	
角色名称	角色编码	操作
超级管理员	admin[系统自带角色,不可操作]	Q详情
管理员	leader[系统自带角色,不可操作]	Q详情
普通用户	developer[系统自带角色,不可操作]	Q详情
测试管理员	0001	(27 修改) 自删除
1321	313	G7修改 · 商服除
超级管理员1	admin1	GF 修改 商服除
超级管理员权限	12138	☑ 修改 高器除
管理员助理	000007	@修改 會删除

# 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。

♀您在这里:配置管理 > 通用设置 > 历史数据	管理	
*检测历史数据清理方式	数据产生N天后清理	Y.
数据产生N天后清理	3年	*
	☑ 提交修改	

# 8.1.2 服务器监控

可通过查询条件选择监控

	理 > 服务器监控
监测服务器选择	请选择 * * * 查询
	请选择 192.168.0.43(Fortify引擎、)
CFU使用率0	192.168.0.45(平台、数据库、默认引擎Findbugs引擎)

♀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 100% 5000N 80% 4000N 3000M 60% 40% 2000M 20% 1000M 0% 60s 55s 50s 45s 40s 35s 30s 25s 20s 15s 10s 5s OM 60s 55s 50s 45s 40s 35s 30s 25s 20s 15s 10s 5s 磁盘读写速率:0KB/秒 💼 当前可用 🛑 已使用 500 1000GE 800GE 400 300 600GE





🧐 code	peck	er					
	<	♀您在这里:系统日志 > 系统日志查问					
	4	操作信息 操作用	户名称	日志开始时间	日志截止时间		
weicome, yors	ai	操作信息	操作结果	操作用户	用户IP地址	操作时间	操作
☆ 首页		项目管理-查询js2工程检测详情	成功	张三(yorsal)	0:0:0:0:0:0:0:1	2019-01-14 16:29:02	★ 删除
📃 项目管理		项目管理-提交检测工程js2	成功	张三(yorsal)	0:0:0:0:0:0:0:1	2019-01-14 16:17:49	★ 删除
业 統计分析		项目管理-查询项目组默认检测工程	成功	张三(yorsal)	0:0:0:0:0:0:0:1	2019-01-14 16:17:24	× 删除
每 缺路规则管理	<	项目管理-查询项目组默认检测工程	成功	张三(yorsal)	0:0:0:0:0:0:0:1	2019-01-14 15:56:49	× 删除
		项目管理-查询项目组test项目组检测工程	成功	张三(yorsal)	0:0:0:0:0:0:0:1	2019-01-14 15:56:46	★ 删除
P 知识年WIKI	<	系统登录	成功	张三(yorsal)	0:0:0:0:0:0:0:1	2019-01-14 15:56:42	★ 删除
👕 用户权限	<	项目管理-查词sss工程检测详情	成功	张三(yorsal)	0:0:0:0:0:0:0:1	2019-01-14 15:47:12	★ 删除
	<	项目管理-查询项目组engine检测工程	成功	张三(yorsal)	0:0:0:0:0:0:0:1	2019-01-14 15:47:11	× 删除
▋ 系统日志		系统登录	成功	张三(yorsal)	0:0:0:0:0:0:0:1	2019-01-14 15:47:05	× 删除
		项目管理-查询wwwwwwwwwwwwuu工程检测详情	成功	张三(yorsal)	0:0:0:0:0:0:0:1	2019-01-14 15:30:36	× 删除
			29/28	3 首页 上一页 25	26 27 28	29 30 31 32 33	34 下一页 末页

# 九、日志管理

产品	软硬件要求					
源代码缺陷	企业级服务器1台(实体机或虚拟化服务器均可):					
分析系统	PU: 主频 2GHz, 四核八线程及以上;					
V4.0	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。

操作信息 摄	作用户名称	日志开始时间	日志截止时间	宣询 [ 导出日志	
操作信息	操作结果	操作用户	用户IP地址	操作时间	操作
项目管理-查询项目组123检测工程	成功	张三(yorsal)	192.168.0.143	2019-05-14 16:10:30	★ 删除
项目管理-删除周期工程GO周期工程	成功	张三(yorsal)	192.168.0.143	2019-05-14 16:10:03	★ 副除
项目管理-查询项目组123检测工程	成功	张三(yorsal)	192.168.0.143	2019-05-14 16:09:40	* 翻除
项目管理-查询Cfortify-2019-05-14工程检测详	青成功	张三(yorsal)	192.168.0.143	2019-05-14 16:09:33	* 2018
项目管理-查询项目组123检测工程	成功	张 <u></u> (yorsal)	192.168.0.143	2019-05-14 16:09:21	× 副称
项目管理-查询项目组JAVA检测工程	成功	张三(yorsal)	192.168.0.143	2019-05-14 16:09:14	* 删除
项目管理-删除检测工程周期工程-2019-05-14	成功	张三(yorsal)	192.168.0.143	2019-05-14 16:09:12	× 劉除
系统登录	成功	刘庆军(liuqj)	192.168.0.2	2019-05-14 16:08:14	* 删除
项目管理-查询项目组JAVA检测工程	成功	张 <u></u> (yorsal)	192.168.0.143	2019-05-14 16:07:37	X 删除
项目管理-查询项目组测试计划末班截图项目检测	工程 成功	张三(yorsal)	192.168.0.143	2019-05-14 16:07:23	× 副除

# 9.2 后台日志

# 通过时间段导出日志

<	♀您在这里:日志管理 > 后台日志管理						
		日志开始时间	日志截止时间	日田市			