



# 商业银行DevSecOps探索与实践

张达 · 2023年5月27日



# 目录

## CONTENTS

1. 数字化转型时代面临的安全风险
2. DevSecOps介绍
3. 浅谈DevSecOps在中小银行落地方式
4. 云原生时代安全思考





# 1.数字化转型时代面临的安全风险



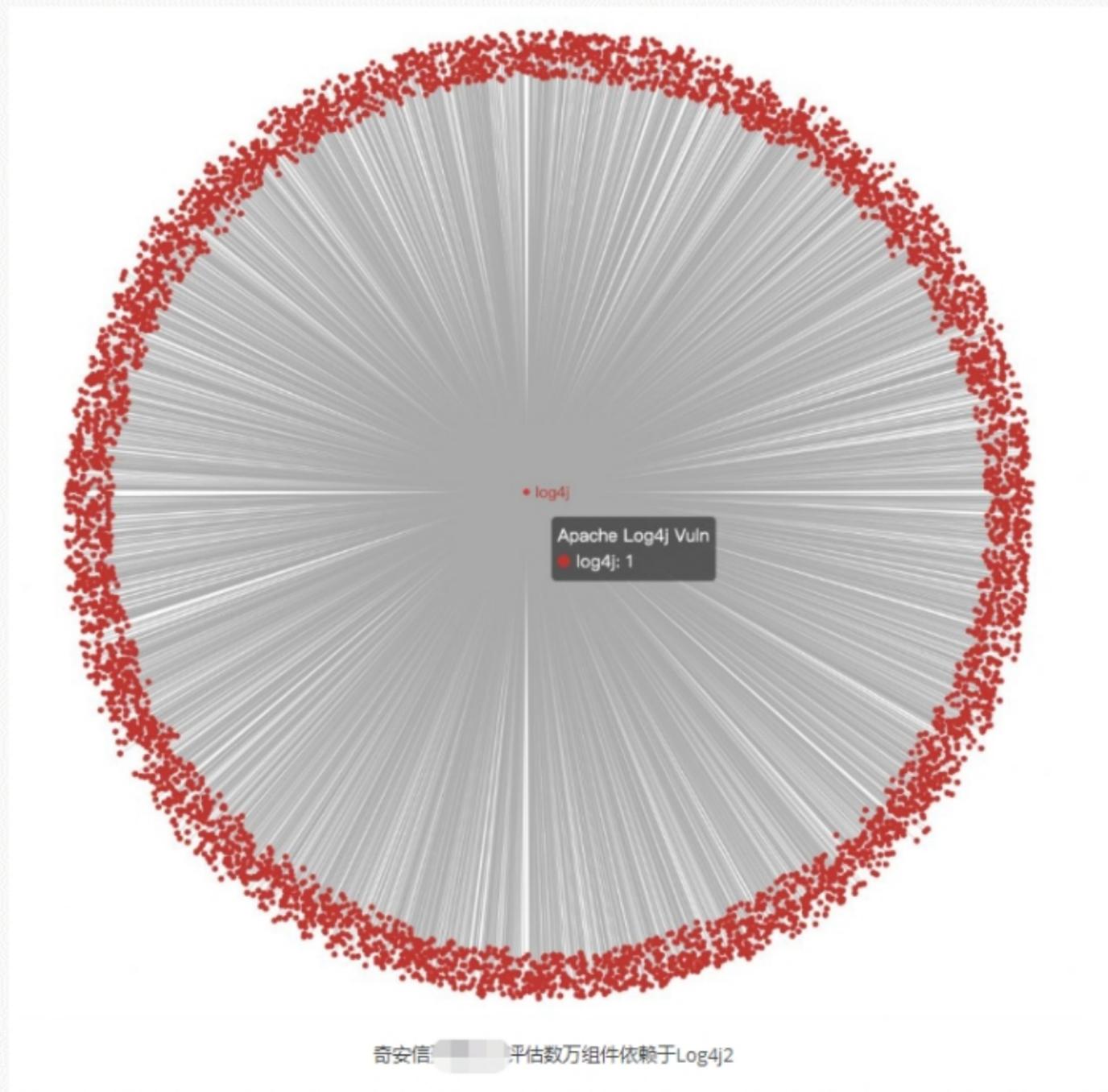
# 先从吃瓜开始

- ❖ 微信可被远程执行命令
- ❖ 贡献者是一位中学生



# log4j2漏洞事件

- 影响6万+流行开源软件
- 影响互联网70%以上的企业系统
- 官方发布漏洞修复补丁后依旧被黑客多次绕过
- 几乎所有互联网大厂都通宵加急处理漏洞



# 大型银行与中小银行对比

类型	银行名称	金融科技投入 (亿元)	同比增速	占营收比重	金融科技 员工数	占员工总 数比重
六大行	工商银行	262.24	0.91%	2.86%	3.6万	8.30%
	建设银行	232.90	-1.21%	2.83%	18511	4.20%
	农业银行	232.11	13.05%	3.20%	10021	2.20%
	中国银行	215.41	15.70%	3.49%	13318	4.35%
	交通银行	116.31	32.93%	5.26%	5862	6.38%
	邮储银行	106.52	6.20%	3.18%	6373	3.27%
股份行	招商银行	141.68	6.60%	4.11%	10846	9.60%
	中信银行	87.49	16.08%	4.14%	4762	8.40%
	兴业银行	82.51	29.65%	3.71%	6699	11.87%
	平安银行	73.83	-6.15%	4.10%		
	浦发银行	70.07	4.49%	3.71%	6447	10.47%
	光大银行	61.27	5.89%	4.04%	3212	6.75%
	民生银行	47.07	22.48%	3.57%	-	-
	华夏银行	38.63	16.39%	4.12%	-	-
	浙商银行	-	-	-	1615	9.60%
城农商行	北京银行	24.52	5.72%	3.70%	783	4.74%
	上海银行	21.32	15.06%	4.18%	1232	10.14%
	沪农商行	9.95	12.68%	3.88%	715	7.86%
	重庆银行	3.84	14.29%	2.85%	-	-
	贵阳银行	3.58	17.03%	2.29%	253	4.30%
	厦门银行	3.25	35.98%	5.51%	-	-
	常熟银行	3.14	25.00%	3.56%	-	-
	渝农商行	-	-	-	522	3.54%
	南京银行	-	-	-	726	4.88%

数据来源：银行年报

资产规模分布



来源：中国银行业协会:中小银行数据安全治理研究报告



立法、监管助力金融科技安全风险管控

 7部法律

 42部行政法规条例

 450余部国家及行业标准

## 没有网络安全就没有国家安全



关于  
**网络安全**  
习近平总书记  
的这些话  
要牢记!

共产党员网 | 同学

网络安全事关国家安全和国家发展、事关广大人民群众工作生活，深刻影响政治、经济、文化、社会、军事等各领域安全。习近平总书记说过，“没有网络安全就没有国家安全”。共产党员网《同学》工作室摘录总书记关于网络安全的部分重要论述，与大家共同学习。让我们树立网络安全意识，筑牢网络安全防线。

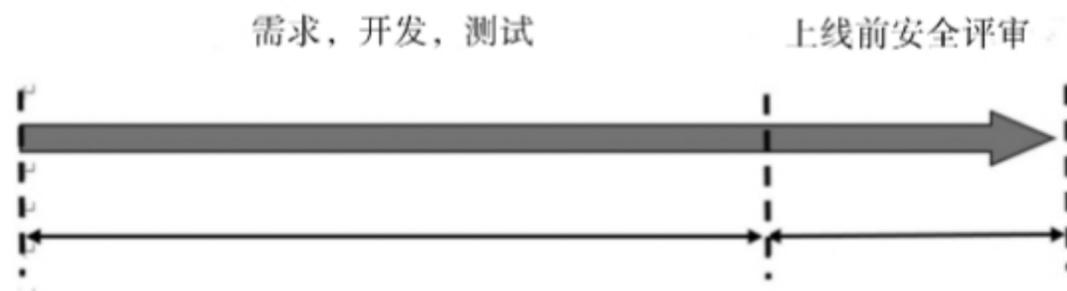


## 2.DevSecOps介绍

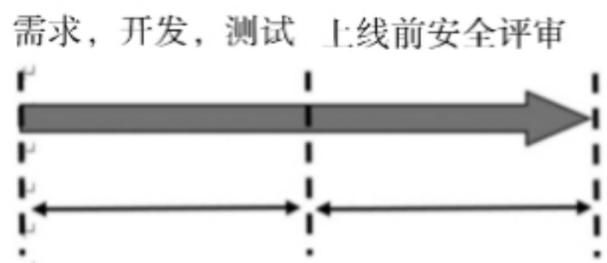


# 安全左移

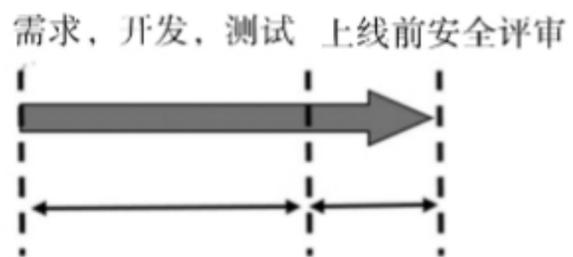
传统模式



DevOps 模式



DevSecOps 模式

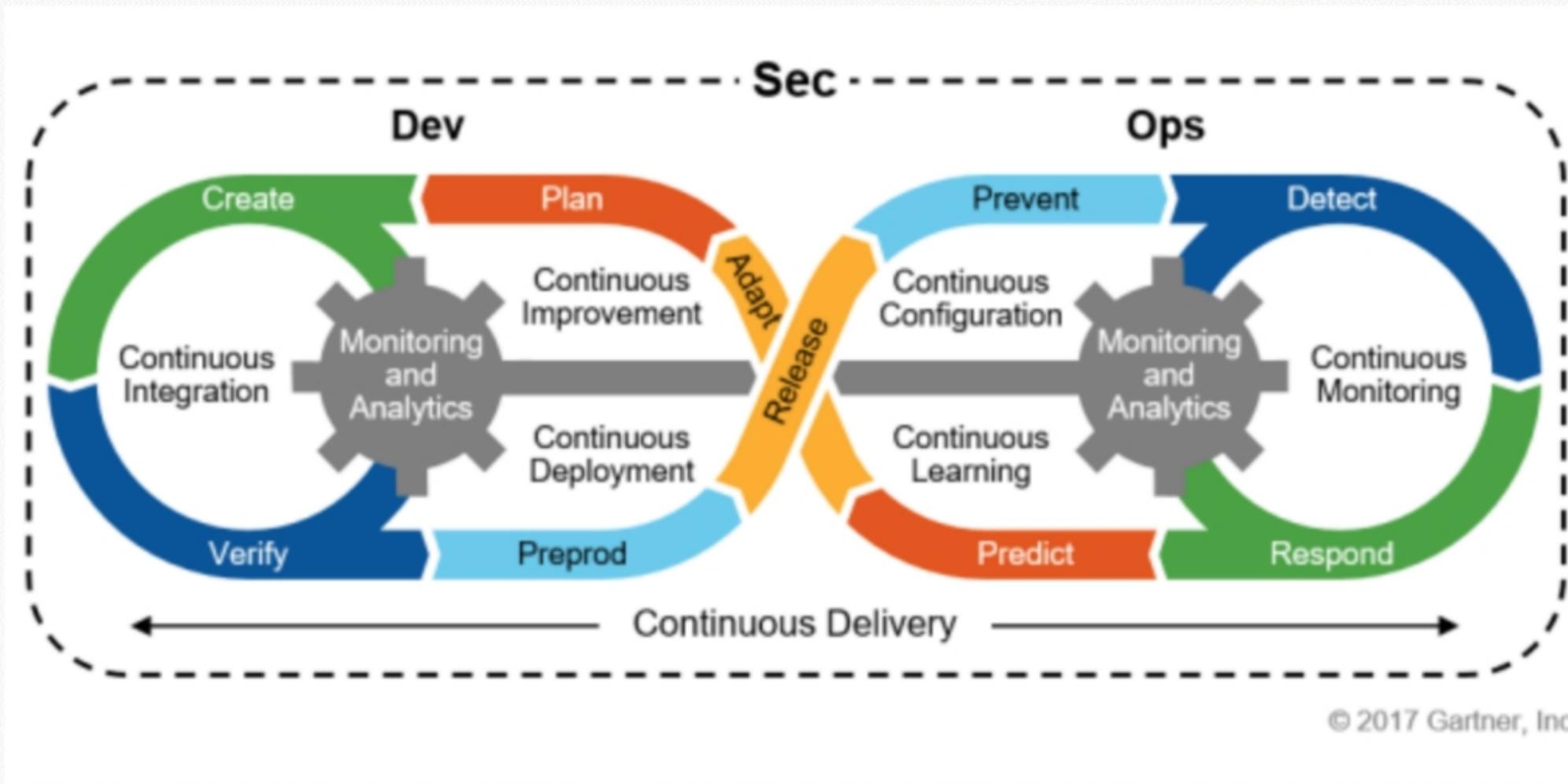


图片来源: 周纪海老师



# DevSecOps核心理念

安全是整个IT团队(包括开发、测试运维及安全团队)所有成员的责任,需要贯穿整个业务生命周期的每一个环节。“每个人都对安全负责”安全工作前置,柔和嵌入现有开发流程体系。



# DevSecOps价值

在软件生命周期的不同阶段引入适合的安全检测工具实现**自动化**安全风险分析、质量管控，优化工作流程，提升系统应用安全的管理效率和运营能力，降低漏洞修复所带来的成本，保障安全风险的高效治理。

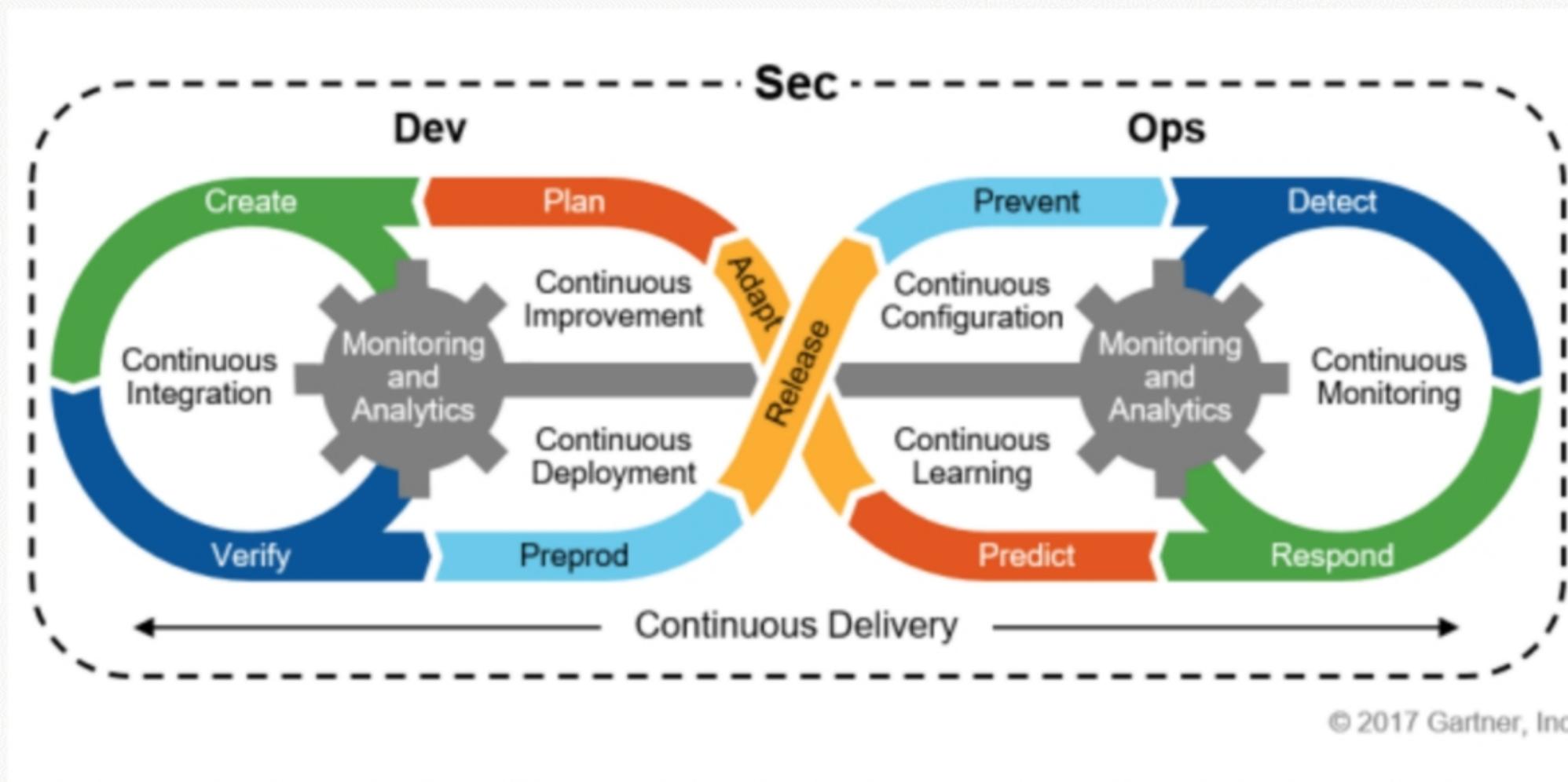




# 浅谈DevSecOps在中小银行落地方式



- 1.制度和流程
- 2.工具链
- 3.安全运营
- 4.度量



# 制度和流程规范

## 自上而下

信息安全需要高度重视

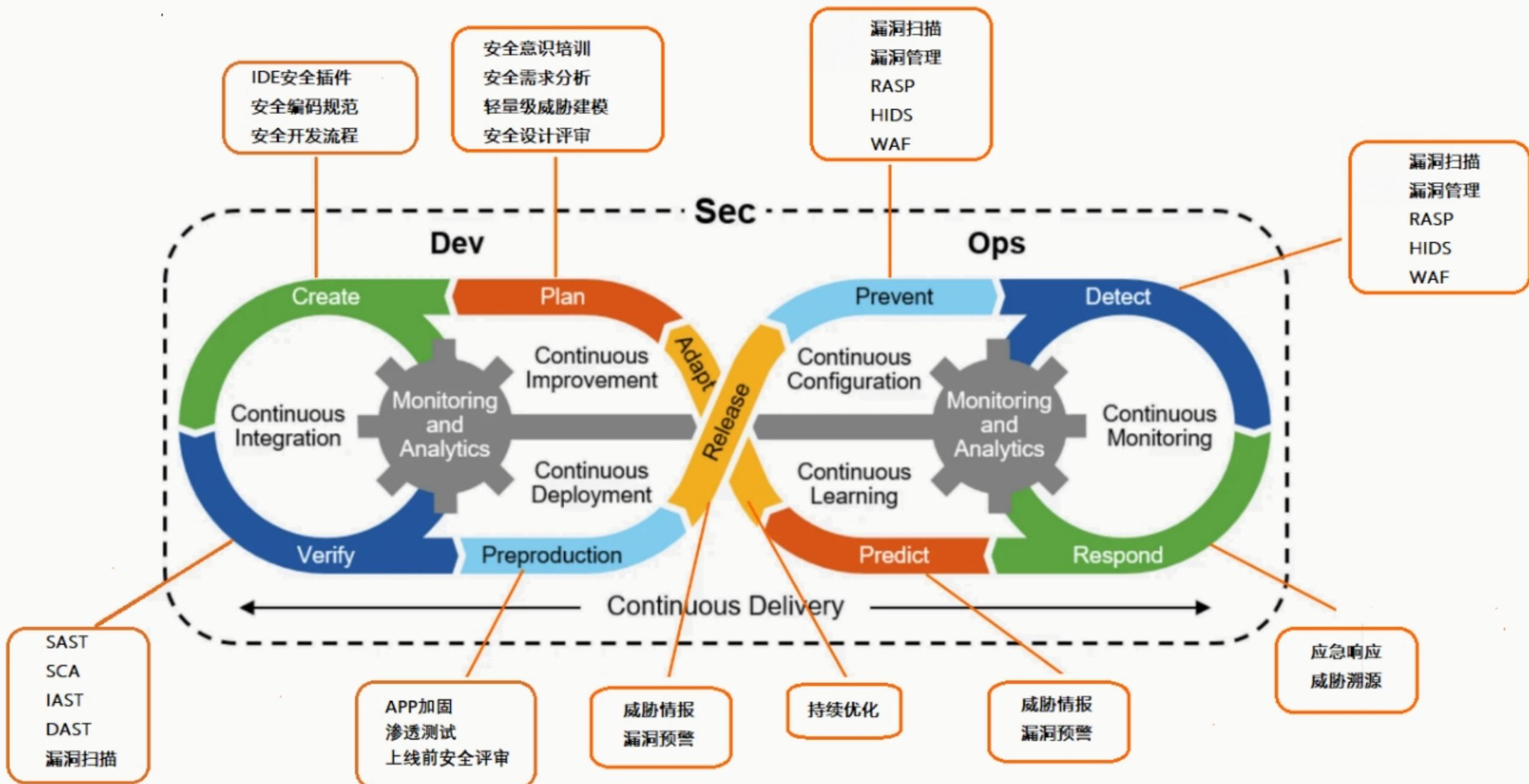
信息安全需要持续投入

安全与业务发展需要找到平衡

综合保障与重点防护需要找到  
平衡



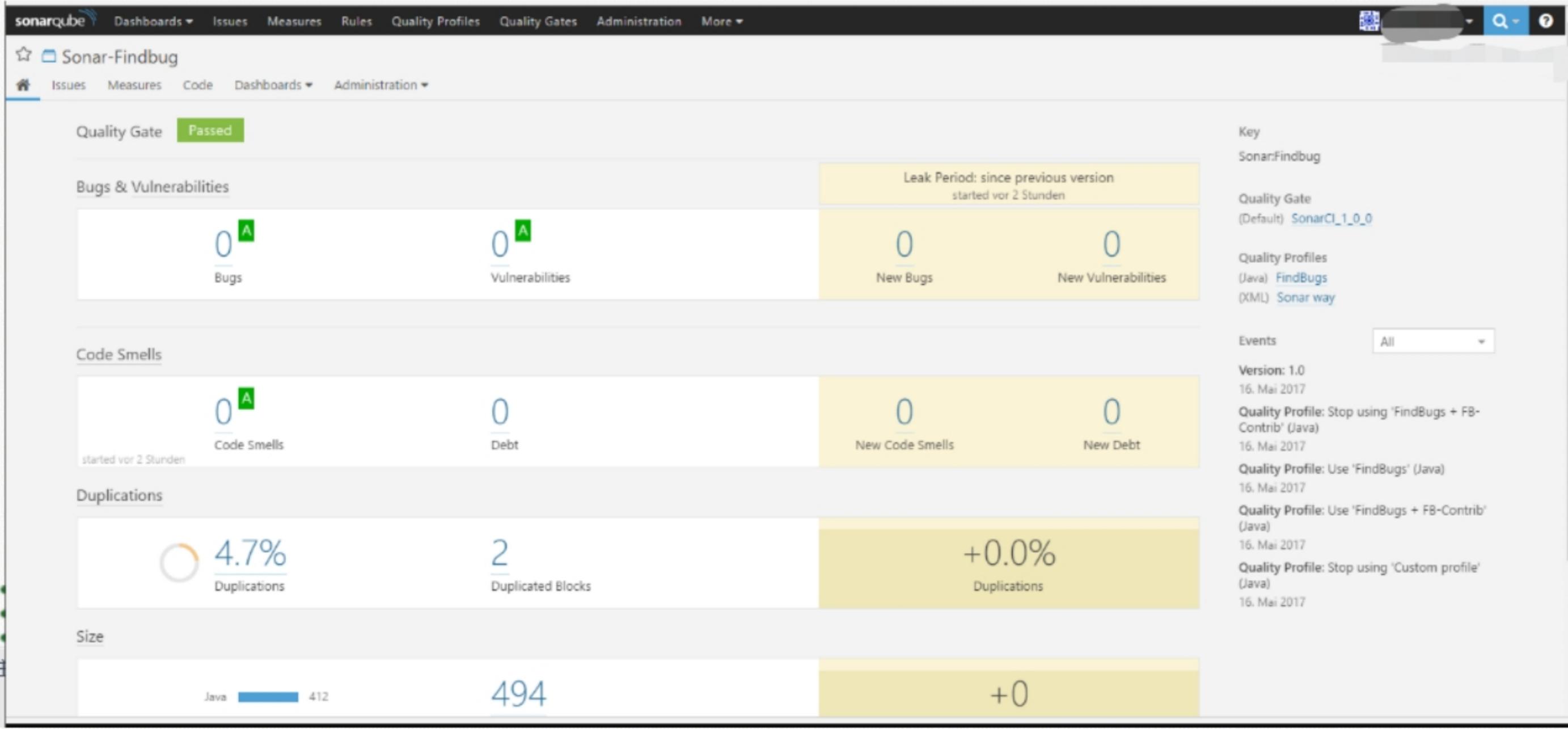
# 流程和工具链建设



# 威胁建模checklist

2	功能场景	安全需求	需求描述	安全设计	设计描述	安全测试	测试用例	监管条例	监管条例
3	Android客户端通用场景	反编译	对源码进行混淆保护防止反编译。	防代码反编译	给应用做安全防护能给出有效较低APP被反编译	代码反编译测试	1、解压apk文件到A文件夹2、在cmd窗口	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M9-逆向工
4	Android客户端通用场景	反编译	对源码进行混淆保护防止反编译。	防代码反编译	给应用做安全防护能给出有效较低APP被反编译	代码反编译测试	1、解压apk文件到A文件夹2、在cmd窗口	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M9-逆向工
5	Android客户端通用场景	程序完整性保护	Android系统通过应用程序的签名来追踪程序完整性	程序安全性	Android系统通过应用程序的签名来追踪程序完整性	系统完整性测试	1、在cmd窗口使用jarsigner工具对apk文件	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M7-客户端
6	Android客户端通用场景	程序完整性保护	Android系统通过应用程序的签名来追踪程序完整性	程序安全性	Android系统通过应用程序的签名来追踪程序完整性	系统完整性测试	1、在cmd窗口使用jarsigner工具对apk文件	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M7-客户端
7	Android客户端通用场景	登录限制	系统应避免同一账号在多处同时登录	账户安全策略	首先多点登录的原理: ![image.png](/account-security-test)	账户安全测试	1、在IOS客户端登录系统2、在Android端	《网上银行系统信息安全	6.1.4.4应用安全->访问控制->应
8	Android客户端通用场景	信息泄露	需要统一错误页面,例如无论出现任何报错信息提示安	系统应当避免向用户提示过多的技术细节	提示信息安全测试	提示信息安全测试	1、对登录后的某个url后缀进行部分删	《网上银行系统信息安全	6.1.4.4应用安全->软件容错->应
9	Android客户端通用场景	登录限制	系统应避免同一账号在多处同时登录	账户安全策略	首先多点登录的原理: ![image.png](/account-security-test)	账户安全测试	1、在IOS客户端登录系统2、在Android端	《网上银行系统信息安全	6.1.4.4应用安全->访问控制->应
10	Android客户端通用场景	安全退出	交互界面提供安全退出和自动超时退出	会话安全	定义一个全局变量time获取当前时间,会话安全测试	会话安全测试	1、点击查看个人信息,使用burpsuite	《网上银行系统信息安全	6.1.4.4应用安全->访问控制->应
11	Android客户端通用场景	信息泄露	需要统一错误页面,例如无论出现任何报错信息提示安	系统应当避免向用户提示过多的技术细节	提示信息安全测试	提示信息安全测试	1、对登录后的某个url后缀进行部分删	《网上银行系统信息安全	6.1.4.4应用安全->软件容错->应
12	Android客户端通用场景	手势安全	需要满足手势密码的复杂度、点判	手势认证密码安	客户端手势密码复杂度,观察是否有点	认证安全测试	1、进行手势密码修改2、分别只连接1、	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M4 -不安
13	Android客户端通用场景	安全退出	交互界面提供安全退出和自动超时退出	会话安全	定义一个全局变量time获取当前时间,会话安全测试	会话安全测试	1、点击查看个人信息,使用burpsuite	《网上银行系统信息安全	6.1.4.4应用安全->访问控制->应
14	Android客户端通用场景	Activity权限控制	应用程序外部调用Activity时,应严	Activity接口访	应用程序外部调用Activity时,应严格	接口访问安全测试	1、查看Manifest.xml2、查看activity属	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M6 -不安
15	Android客户端通用场景	手势安全	需要满足手势密码的复杂度、点判	手势认证密码安	客户端手势密码复杂度,观察是否有点	认证安全测试	1、进行手势密码修改2、分别只连接1、	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M4 -不安
16	Android客户端通用场景	service权限控制	应用程序需要外部调用Service时,应	Service接口访	应用程序需要外部调用Service时,应	接口访问安全测试	1、查看Manifest.xml2、查看Service属	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M6 -不安
17	Android客户端通用场景	Activity权限控制	应用程序外部调用Activity时,应严	Activity接口访	应用程序外部调用Activity时,应严格	接口访问安全测试	1、查看Manifest.xml2、查看activity属	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M6 -不安
18	Android客户端通用场景	Broadcast Receiver权限	应用程序使用Broadcast Receiver时	Broadcast Rece	应用程序使用Broadcast Receiver时,接	接口访问安全测试	1、查看Manifest.xml2、查看Broadcast	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M6 -不安
19	Android客户端通用场景	service权限控制	应用程序需要外部调用Service时,应	Service接口访	应用程序需要外部调用Service时,应	接口访问安全测试	1、查看Manifest.xml2、查看Service属	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M6 -不安
20	Android客户端通用场景	Content Provider权限控	应用程序使用Content Provider向外	Content Provid	应用程序使用Content Provider向外	接口访问安全测试	1、查看Manifest.xml2、查看Content P	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M6 -不安
21	Android客户端通用场景	Broadcast Receiver权限	应用程序使用Broadcast Receiver时	Broadcast Rece	应用程序使用Broadcast Receiver时,接	接口访问安全测试	1、查看Manifest.xml2、查看Broadcast	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M6 -不安
22	Android客户端通用场景	异常捕获	应对需要捕获的异常进行处理,禁止	异常处理安全	捕获异常的步骤1.定义一个类,该类继	异常处理安全检查	对代码进行查看审计	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M10: 无
23	Android客户端通用场景	Content Provider权限控	应用程序使用Content Provider向外	Content Provid	应用程序使用Content Provider向外	接口访问安全测试	1、查看Manifest.xml2、查看Content P	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M6 -不安
24	Android客户端通用场景	异常信息泄露	应对出现的异常进行处理,避免直接	异常处理安全	在Android中有的未知的Bug可能在测试	异常处理安全检查	1、对登录后的某个url后缀进行部分删	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M10: 无
25	Android客户端通用场景	异常捕获	应对需要捕获的异常进行处理,禁止	异常处理安全	捕获异常的步骤1.定义一个类,该类继	异常处理安全检查	对代码进行查看审计	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M10: 无
26	Android客户端通用场景	敏感信息安全	应按要求进行敏感信息确认,并将敏	信息存储安全	对敏感信息进行加密,访问时进行验证	信息存储安全检查	查看数据库存储的敏感信息。	《银行卡信息泄露风险一、银行卡信息的管理安全->支付	
27	Android客户端通用场景	异常信息泄露	应对出现的异常进行处理,避免直接	异常处理安全	在Android中有的未知的Bug可能在测试	异常处理安全检查	1、对登录后的某个url后缀进行部分删	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M10: 无
28	Android客户端通用场景	日志记录功能开启	应开启日志记录功能,保证用户操作	日志记录安全	Android系统开启日志记录功能设计样	日志功能检查	查看应用日志。	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M7-客户端
29	Android客户端通用场景	敏感信息安全	应按要求进行敏感信息确认,并将敏	信息存储安全	对敏感信息进行加密,访问时进行验证	信息存储安全检查	查看数据库存储的敏感信息。	《银行卡信息泄露风险一、银行卡信息的管理安全->支付	
30	Android客户端通用场景	日志类型记录	确保在重要行为发生时能有相应的记录	异常处理安全	在Android中有的未知的Bug可能在测试	异常处理检查	对代码进行查看审计。	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M7-客户端
31	Android客户端通用场景	日志记录功能开启	应开启日志记录功能,保证用户操作	日志记录安全	Android系统开启日志记录功能设计样	日志功能检查	查看应用日志。	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M7-客户端
32	Android客户端通用场景	时间戳要求	必须明确的把时间戳包含在日志文件	日志记录安全	必须明确的把时间戳包含在日志文件内	日志安全检查	查看服务端应用日志。	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M7-客户端
33	Android客户端通用场景	日志类型记录	确保在重要行为发生时能有相应的记录	异常处理安全	在Android中有的未知的Bug可能在测试	异常处理检查	对代码进行查看审计。	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M7-客户端
34	Android客户端通用场景	客户端日志记录要求	客户端打印日志应避免输出明文密码	日志内容安全	本地输出的日志要求不包含敏感信息、	日志记录安全测试	1、使用adb连接上手机命令: adb conne	《网上银行系统信息安全	6.1.4.4应用安全->身份鉴别->禁
35	Android客户端通用场景	时间戳要求	必须明确的把时间戳包含在日志文件	日志记录安全	必须明确的把时间戳包含在日志文件内	日志安全检查	查看服务端应用日志。	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M7-客户端
36	Android客户端通用场景	日志访问权限控制	控制其他应用程序对日志的访问权限	日志访问安全	控制其他应用程序对日志的访问权限。	日志访问安全测试	1、使用adb shell命令连接手机2、使用	《网上银行系统信息安全	6.1.4.4应用安全->访问控制->应
37	Android客户端通用场景	客户端日志记录要求	客户端打印日志应避免输出明文密码	日志内容安全	本地输出的日志要求不包含敏感信息、	日志记录安全测试	1、使用adb连接上手机命令: adb conne	《网上银行系统信息安全	6.1.4.4应用安全->身份鉴别->禁
38	Android客户端通用场景	软件更新	支持安全更新。	更新升级安全	1.更新程序进行签名,保证应用程序完	更新升级安全检查	进入应用程序,查看程序更新	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M7-客户端
39	Android客户端通用场景	日志访问权限控制	控制其他应用程序对日志的访问权限	日志访问安全	控制其他应用程序对日志的访问权限。	日志访问安全测试	1、使用adb shell命令连接手机2、使用	《网上银行系统信息安全	6.1.4.4应用安全->访问控制->应
40	Android客户端通用场景	动态更新	采用动态加载更新补丁的方式,需校	更新升级安全	1.采用动态加载更新补丁的方式,需校	更新升级安全检查	下载最新的apk文件使用jarsigner进行	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M7-客户端
41	Android客户端通用场景	第三方组件安全	调用第三方代码或库文件,应确保其	第三方组件安全	调用第三方代码或库文件,应确保其来	第三方组件安全检查	1、使用md5摘要工具对第三方库进行md5	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M7-客户端
42	Android客户端通用场景	软件更新	支持安全更新。	更新升级安全	1.更新程序进行签名,保证应用程序完	更新升级安全检查	进入应用程序,查看程序更新	OWASP Mobile TOP 10	OWASP Mobile TOP 10: M7-客户端

# SAST: SonarQube



The screenshot shows the SonarQube dashboard for a project named 'Sonar-Findbug'. The interface includes a navigation menu at the top with options like Dashboards, Issues, Measures, Rules, Quality Profiles, Quality Gates, Administration, and More. The main content area is divided into several sections:

- Quality Gate:** A green badge indicates the gate has 'Passed'.
- Bugs & Vulnerabilities:** This section shows 0 Bugs and 0 Vulnerabilities, both with an 'A' grade. It also displays 'Leak Period: since previous version started vor 2 Stunden' and 0 New Bugs and 0 New Vulnerabilities.
- Code Smells:** Shows 0 Code Smells and 0 Debt, both with an 'A' grade. It also displays 'Leak Period: since previous version started vor 2 Stunden' and 0 New Code Smells and 0 New Debt.
- Duplications:** Shows 4.7% Duplications and 2 Duplicated Blocks. The change in duplications is +0.0%.
- Size:** Shows the total size of the project as 494, with a breakdown for Java (412).

On the right side, there is a sidebar with additional information:

- Key:** SonarFindbug
- Quality Gate:** (Default) SonarCI\_1\_0\_0
- Quality Profiles:** (Java) FindBugs, (XML) Sonar way
- Events:** All
- Version:** 1.0, 16. Mai 2017
- Quality Profile:** Stop using 'FindBugs + FB-Contrib' (Java), 16. Mai 2017
- Quality Profile:** Use 'FindBugs' (Java), 16. Mai 2017
- Quality Profile:** Use 'FindBugs + FB-Contrib' (Java), 16. Mai 2017
- Quality Profile:** Stop using 'Custom profile' (Java), 16. Mai 2017



# IAST: openrasp-iaast

当前应用  PHP示例应用 添加主机 openrasp 管理员权限

安全总览 [漏洞列表](#) [攻击事件](#) [安全基线](#) [主机管理](#) [插件管理](#) [异常日志](#) [系统设置](#) [帮助文档](#)

你还没有修改默认的后台密码, 可前往 [登录认证](#) 设置

## 漏洞列表

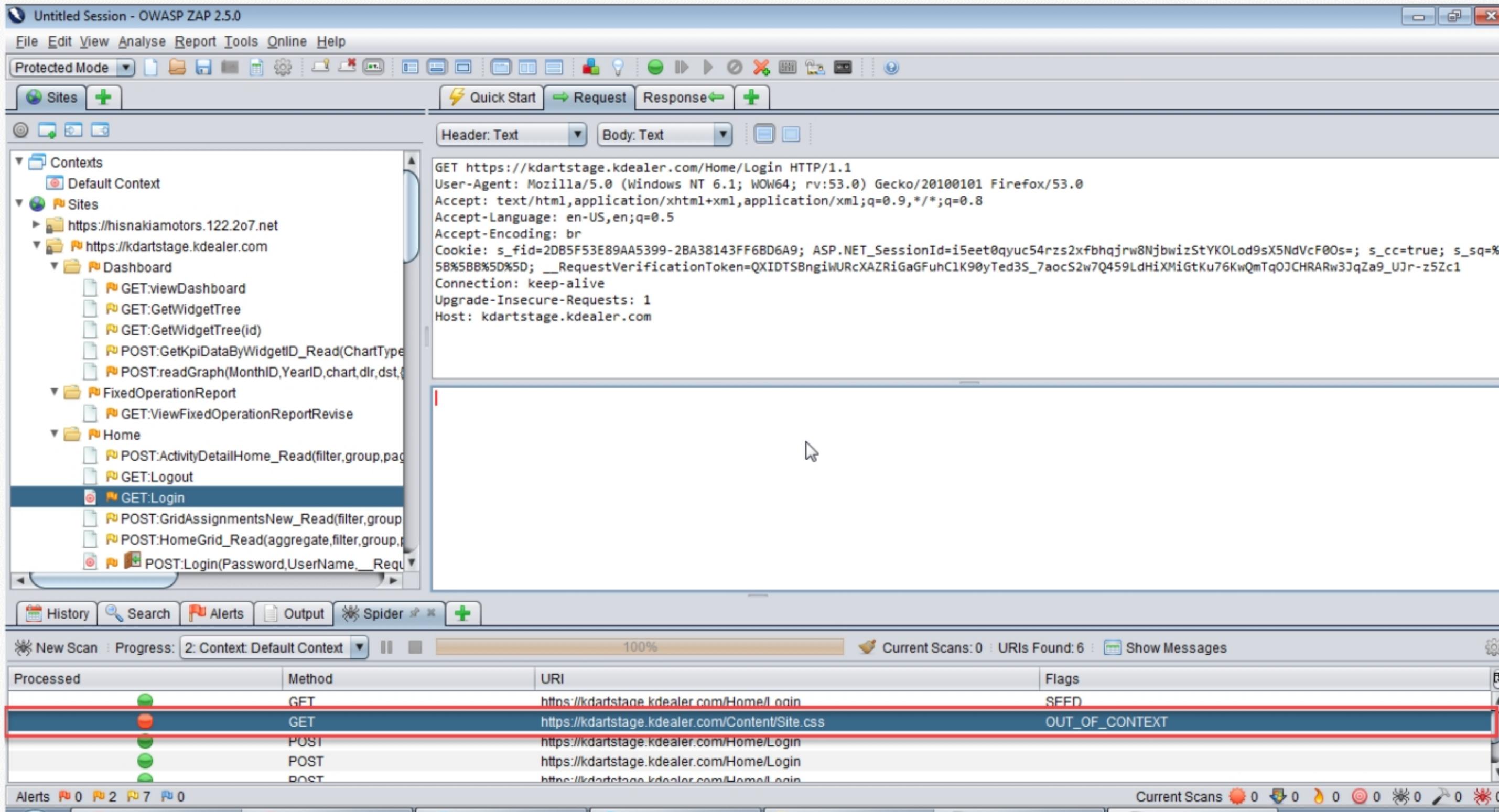
12/09/2019 - 01/09/2020 拦截状态 - 漏洞类型 - 目标URL 搜索

4 结果, 显示 1/1 页

最后发现	URL	攻击来源	最后状态	漏洞类型	报警消息	操作
2020-01-09 14:11:00	<a href="http://[redacted]/vulnerabilities/brute/?user_name=1'openrasp&amp;password=122&amp;Login=Login">http://[redacted]/vulnerabilities/brute/?user_name=1'openrasp&amp;password=122&amp;Login=Login</a>	[redacted] 利用 1 次	记录日志	SQL注入	OpenRASP-IAST漏洞扫描 - sql语句逻辑 可被用户输入控制	<a href="#">查看详情</a>
2020-01-09 14:07:33	<a href="http://[redacted]erabilities/upload/">http://[redacted]erabilities/upload/</a>	[redacted] 利用 1 次	记录日志	任意文件上传	OpenRASP-IAST漏洞扫描 - 用户可上传 脚本文件至web目录	<a href="#">查看详情</a>
2020-01-09 14:00:23	<a href="http://[redacted]ulnerabilities/sql_i_blind/?id=1'openrasp&amp;Submit=Submit">http://[redacted]ulnerabilities/sql_i_blind/?id=1'openrasp&amp;Submit=Submit</a>	[redacted] 利用 1 次	记录日志	SQL注入	OpenRASP-IAST漏洞扫描 - sql语句逻辑 可被用户输入控制	<a href="#">查看详情</a>
2020-01-09 13:57:27	<a href="http://[redacted]es/sql_i/?id=1'openrasp&amp;Submit=Submit">http://[redacted]es/sql_i/?id=1'openrasp&amp;Submit=Submit</a>	[redacted] 利用 1 次	记录日志	SQL注入	OpenRASP-IAST漏洞扫描 - sql语句逻辑 可被用户输入控制	<a href="#">查看详情</a>



# DAST: owasp-zap



Header: Text

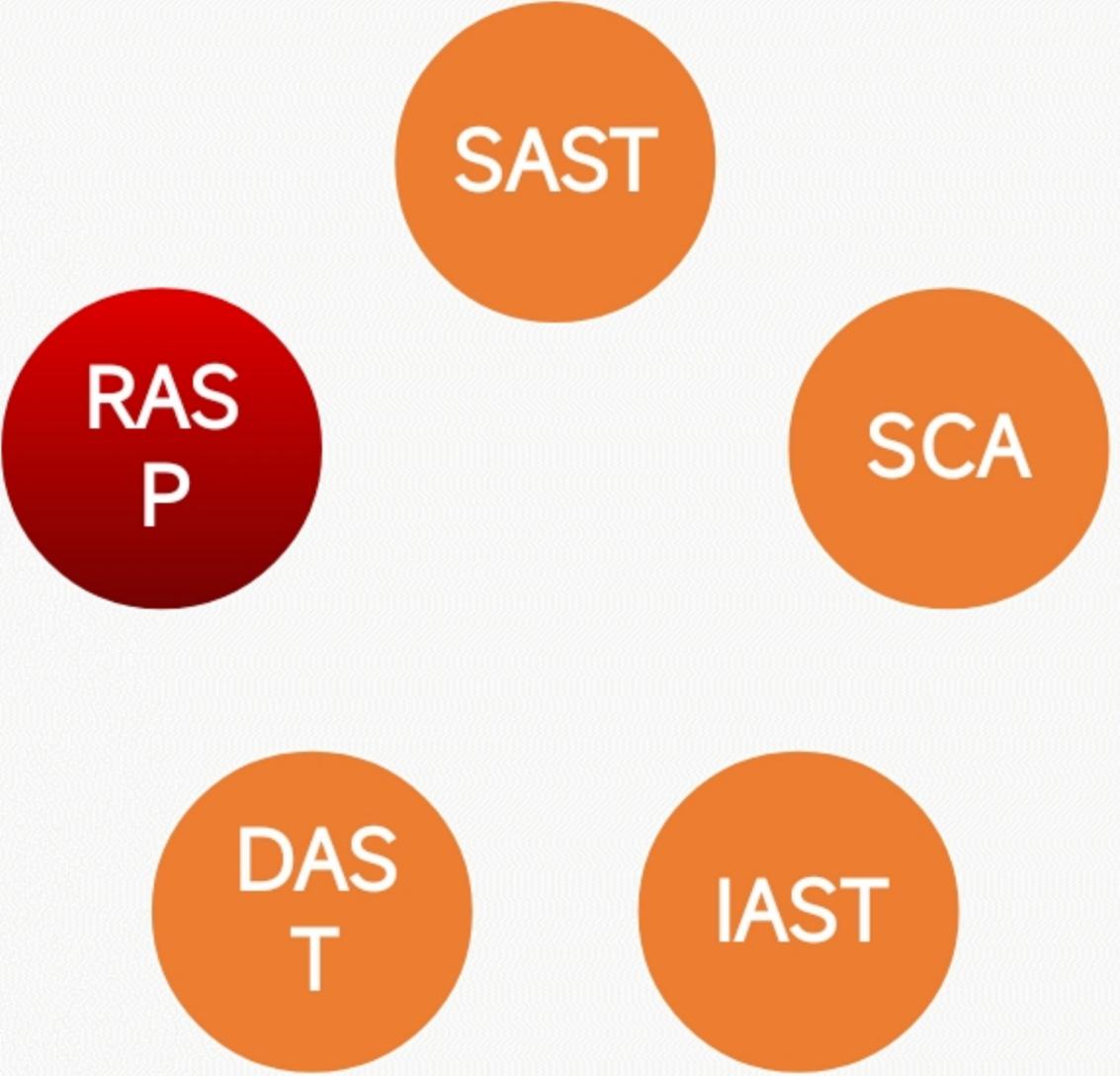
```
GET https://kdartstage.kdealer.com/Home/Login HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:53.0) Gecko/20100101 Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: br
Cookie: s_fid=2DB5F53E89AA5399-2BA38143FF6BD6A9; ASP.NET_SessionId=i5eet0qyuc54rzs2xfbhqjrw8NjbwizStYKOLod9sX5NdVcF00s=; s_cc=true; s_sq=%5B%5BB%5D%5D; __RequestVerificationToken=QXIDTSBngiWURcXAZRiGaGFuhC1K90yTed3S_7aocS2w7Q459LdHiXMiGtKu76KwQmTqOJCHRARw3JqZa9_UJr-z5Zc1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: kdartstage.kdealer.com
```

Processed	Method	URI	Flags
	GET	https://kdartstage.kdealer.com/Home/Login	SEED
	GET	https://kdartstage.kdealer.com/Content/Site.css	OUT_OF_CONTEXT
	POST	https://kdartstage.kdealer.com/Home/Login	
	POST	https://kdartstage.kdealer.com/Home/Login	
	POST	https://kdartstage.kdealer.com/Home/Login	

Alerts 0 2 7 0

Current Scans 0 0 0 0 0 0 0 0

# DevSecOps主要工具链



AST技术对比分析

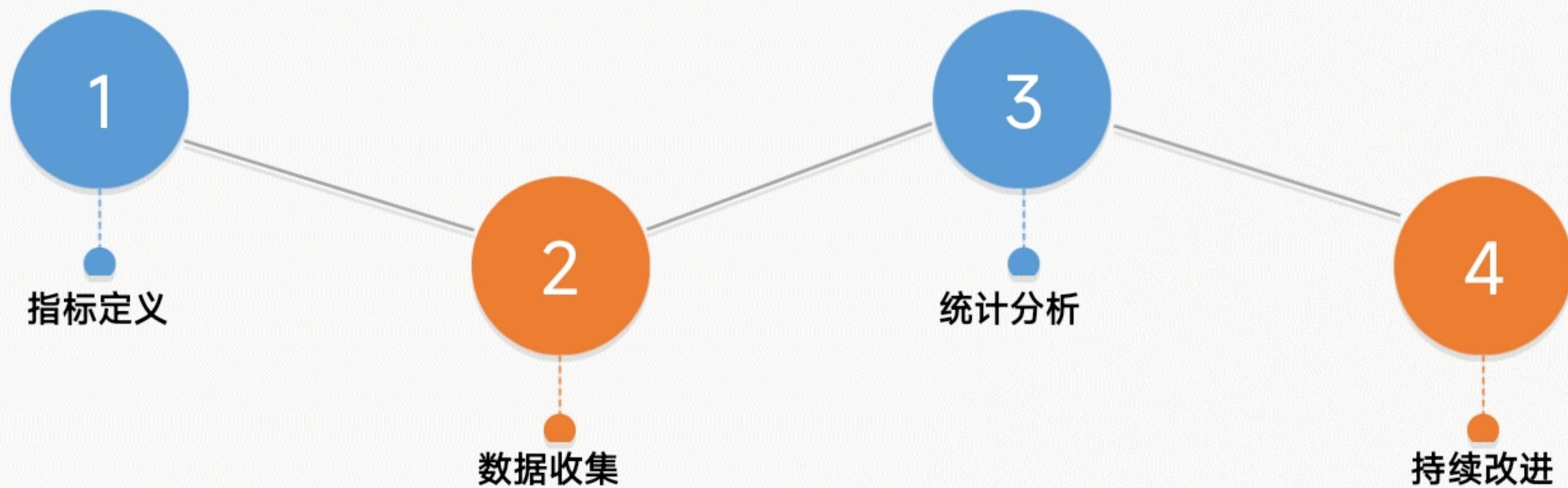
AST技术系	SAST白盒	IAST灰盒	DAST黑盒
误报率	高	极低	低
检出率	高	高	中
检测速度	随代码量	依点击流量实时检测	随URL、payload数量
SCA成分分析	静态扫描支持	运行时支持	依赖payload、指纹
API识别分析	深度支持	深度支持	一般支持
敏感数据追踪	无法支持	深度支持	一般支持
语言支持	区分不同语言	区分不同的语言	不区分语言
框架支持	一定程度区分	一定程度区分	不区分框架
漏洞验证利用	很难验证利用	可验证利用	可验证利用
使用成本	高，人工排查误报	低，基本没有误报	较低
漏洞详情	代码行数、执行流	请求响应、代码行数、数据流、调用堆栈等	参数、请求响应
DevOps CI/CD支持	较高	高	低
漏洞种类覆盖	更偏向应用代码漏洞和编码规范缺陷	更偏向应用本身漏洞，难以回显带外也可发现	可发现配置、运维、运行时层面漏洞



## 应用安全编排和关联



# 度量



# 信通院DevOps成熟度模型：第六部分



来源：信通院DevOps成熟度模型\_第六部分说明



# GB/T 42560-2023



**SAC** 全国标准信息公共服务平台  
National public service platform for standards information

标准信息一网打尽

首页 国家标准 行业标准 地方标准 团体标准 企业标准 国际标准 国外标准 示范试点 技术委员会

## 系统与软件工程 开发运维一体化 能力成熟度模型

System and software engineering—Development and operations—Capability maturity model

国家标准 推荐性 即将实施

国家标准《系统与软件工程 开发运维一体化 能力成熟度模型》由TC28（全国信息技术标准化技术委员会）归口，TC28SC7（全国信息技术标准化技术委员会软件与系统工程分会）执行，主管部门为国家标准化管理委员会。

主要起草单位 北斗天地股份有限公司、中国电子技术标准化研究院、南京大学、华为技术有限公司、网易（杭州）网络有限公司、中兴通讯股份有限公司、工银科技有限公司、中国航天系统科学与工程研究院、中国商用飞机有限责任公司北京民用飞机技术研究中心、腾讯科技（深圳）有限公司、杭州朗和科技有限公司、南京中兴软件有限责任公司、广东益安人防工程科技有限公司、航天中认软件测评科技（北京）有限责任公司、爱捷软件开发（深圳）有限公司、震兑工业智能科技有限公司、北京高质系统科技有限公司、北京软件和信息服务交易所有限公司、山东正中信息技术股份有限公司、上海计算机软件技术开发中心、云南电网有限责任公司信息中心、神州数码系统集成服务有限公司、普元信息技术股份有限公司、中国电子科技集团公司第五十四研究所、成都信息工程大学、中国人民解放军军事科学院国防科技创新研究院、北方民族大学、北京邮电大学、云南南天电子信息产业股份有限公司、联通数字科技有限公司、内蒙古东润能源科技有限公司、成都新希望金融信息有限公司、深圳市海德森科技股份有限公司、江苏汤谷智能科技有限公司。

主要起草人 张旻旻、荣国平、冯建、张文渊、徐毅、陈谔、胡继东、钱湘隆、郭栋、袁玉宇、朱少凡、王芹、殷柱伟、翁扬慧、王公韬、赵国亮、吴穹、姚炳雄、严亮、庄园、张建成、沈颖、李玲璠、赵一博、王晓朋、钱淑丽、舒红平、史殿习、韩强、刘亚、张贺、李强、冯常健、周天才、温建波、董冠涛、汪皓、陈晓敏、张晔、周长怀、周启平、雷晓宝、代东洋、张玉良、许志国、蔡立志、马文、沈伟、王茹、薛超、丁静、李杉杉、匡宏宇、陈杰、张小燕、苏春山、于长钺、熊辉、宋雨伦、刘全东、赵永亮、张华山、刘丹。

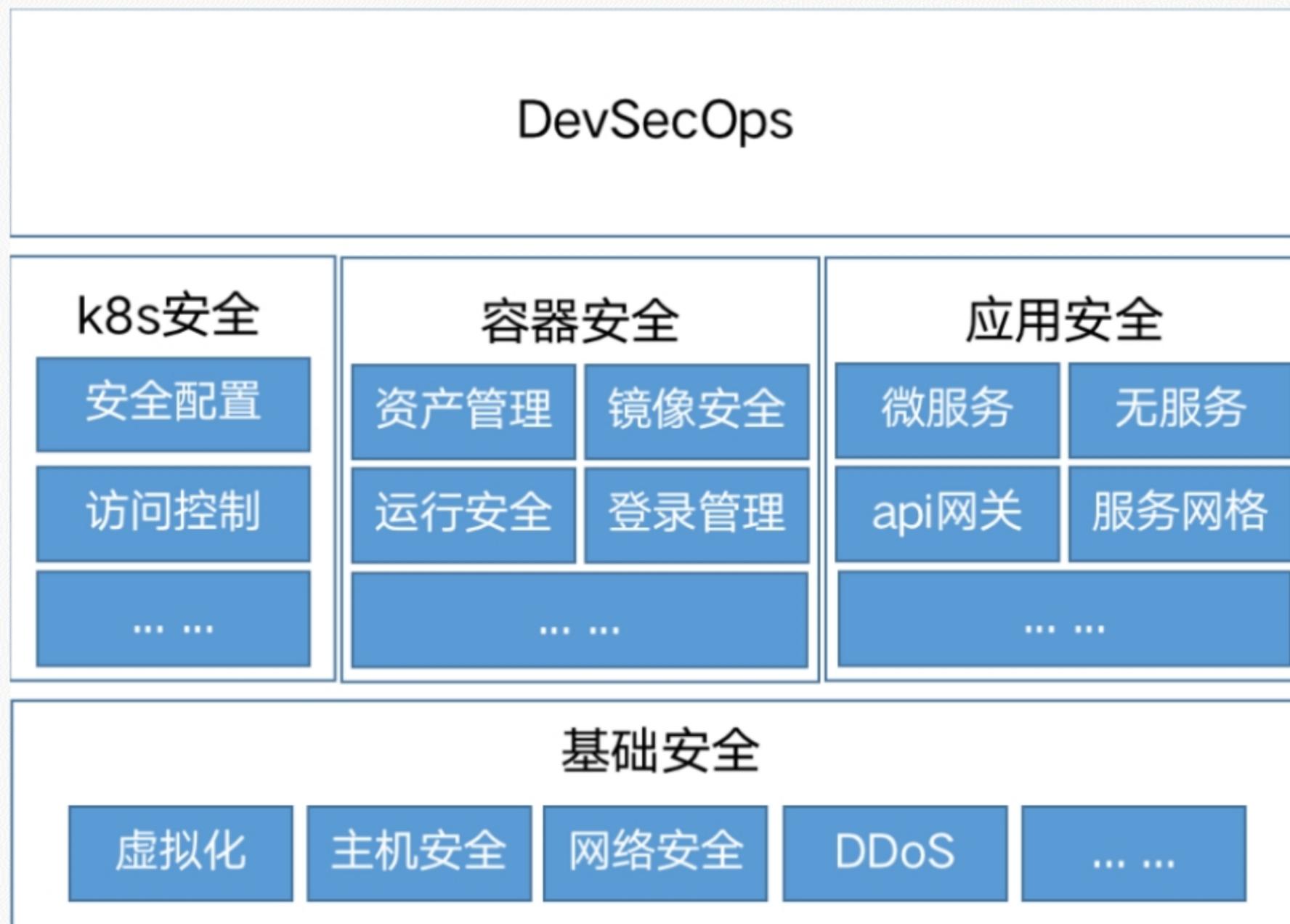




# 云原生时代安全思考



# 云原生时代安全何去何从



来源：腾讯应急响应中心博客





# 提问时间

谢谢大家





关注社区公众号  
了解更多活动

