

Secure Development Sharing

Date: Jun 2019

Prepared by: 周继海 / 杨伟强



目录



1

自我介绍

2

DevSecOps介绍

3

DevSecOps实现和运作模型

4

DevSecOps工具

5

DevSecOps文化的建立

目录

1 自我介绍

➔ **2** DevSecOps介绍

3 DevSecOps实现和运作模型

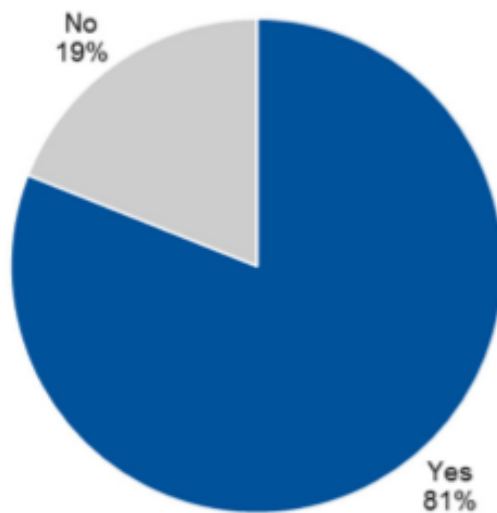
4 DevSecOps工具

5 DevSecOps文化的建立

为什么需要DevSecOps?

- DevOps 让开发团队的产品交付更快、协作更好。传统的信息安全交付模式和现代的快速持续交付理念形成冲突，从而使信息安全成为快速交付的瓶颈
- 如果没有考虑到信息安全的DevOps，反而让产品更加容易存在信息安全漏洞的风险

Figure 2. IT Operations Professionals: Do You Believe Your Information Security Policies/Teams Are Slowing IT Down?

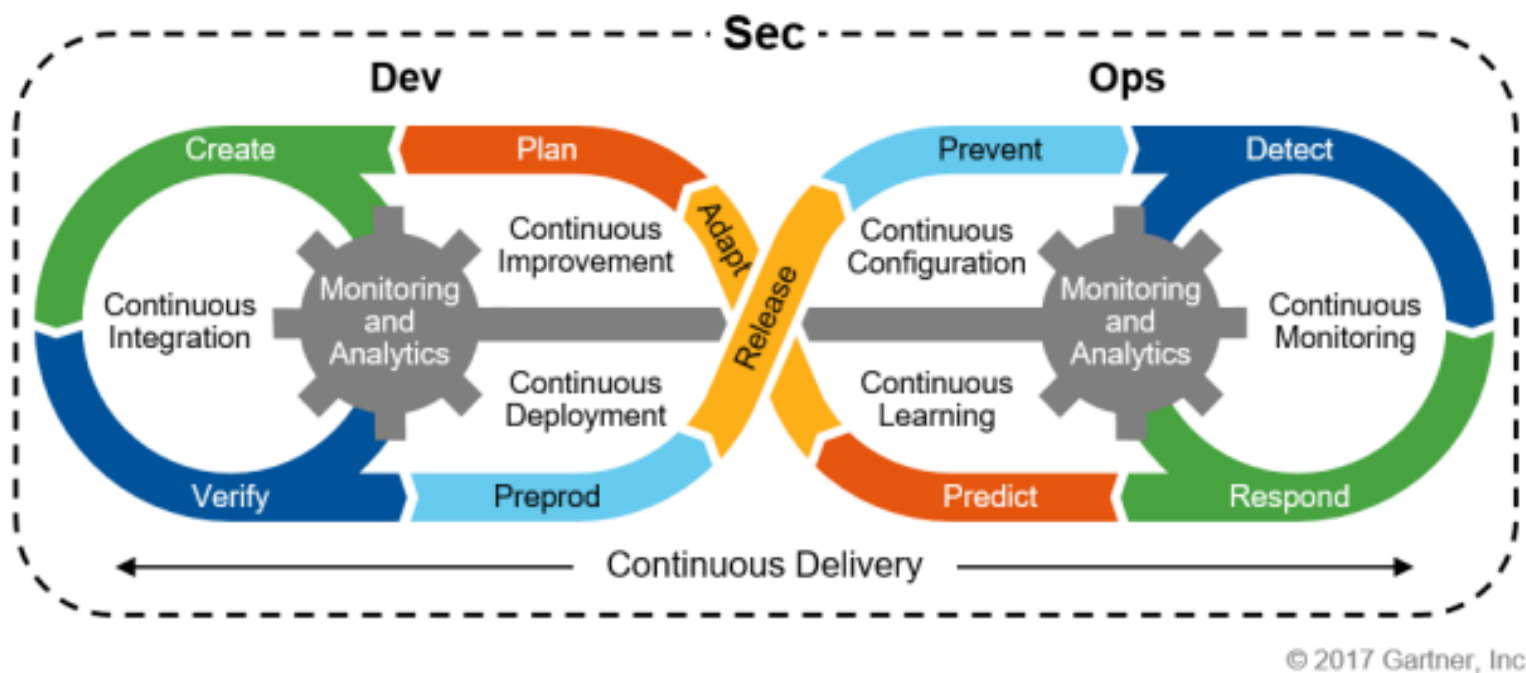


n = 93

Source: Gartner (September 2016)

什么是DevSecOps

2012年，Gartner 提出了DevSecOps的概念 (初始称为DevOpsSec)。
自从2017起，DevSecOps 开始成为一个全球热门话题。



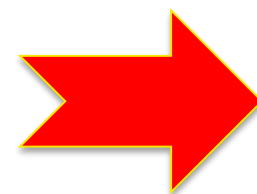
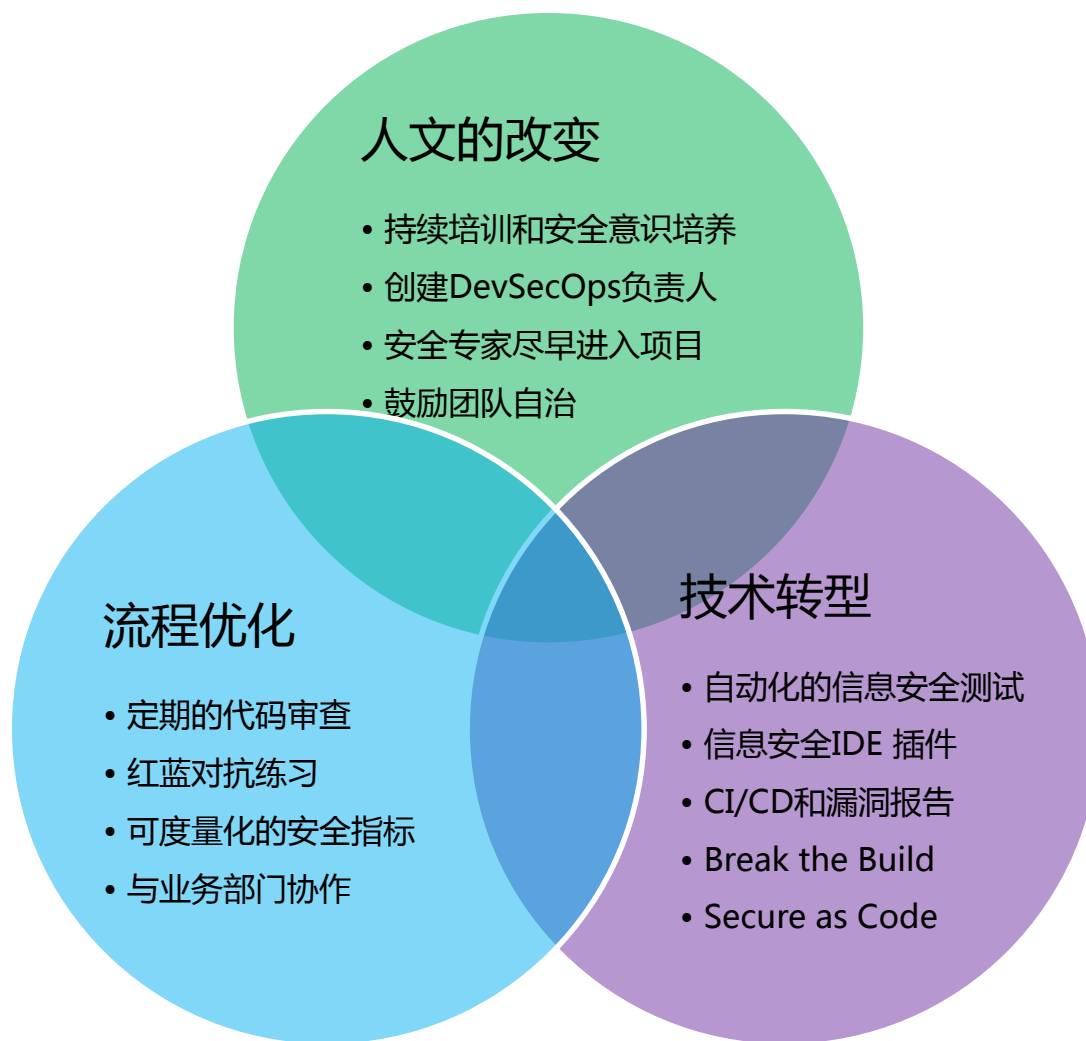
DevSecOps的好处



DevSecOps的挑战



DevSecOps的最佳实践



DevSecOps的最终目标是引入一套框架，解决持续快速交付和信息安全之间的矛盾

目录

1 自我介绍

2 DevSecOps介绍

 **3** DevSecOps实现和运作模型

4 DevSecOps工具

5 DevSecOps文化的建立

DevSecOps的实现模型

1. 信息安全的工具应用

- 将DevSecOps工具嵌入到CI/CD流水线中，实现自动化安全漏洞扫描
- 生成公开的信息安全漏洞报表
- 根据团队情况定制信息安全规则

2. 信息安全培训

- 信息安全工具中的学习材料
- 在线培训 – Secure Code Warrior
- 信息安全咨询

3. 信息安全意识和“专家”

- 建立信息安全意识和文化
- 培养开发团队中的“信息安全专家”

DevSecOps的运作模型



DevSecOps负责人

- 负责推广DevSecOps文化和帮助开发团队建立DevSecOps意识
- 连接开发团队和信息安全团队
- 将从开发团队收集到的问题反馈给信息安全团队, 并将信息安全团队提供的方案传递给开发团队形成一条健康的回路



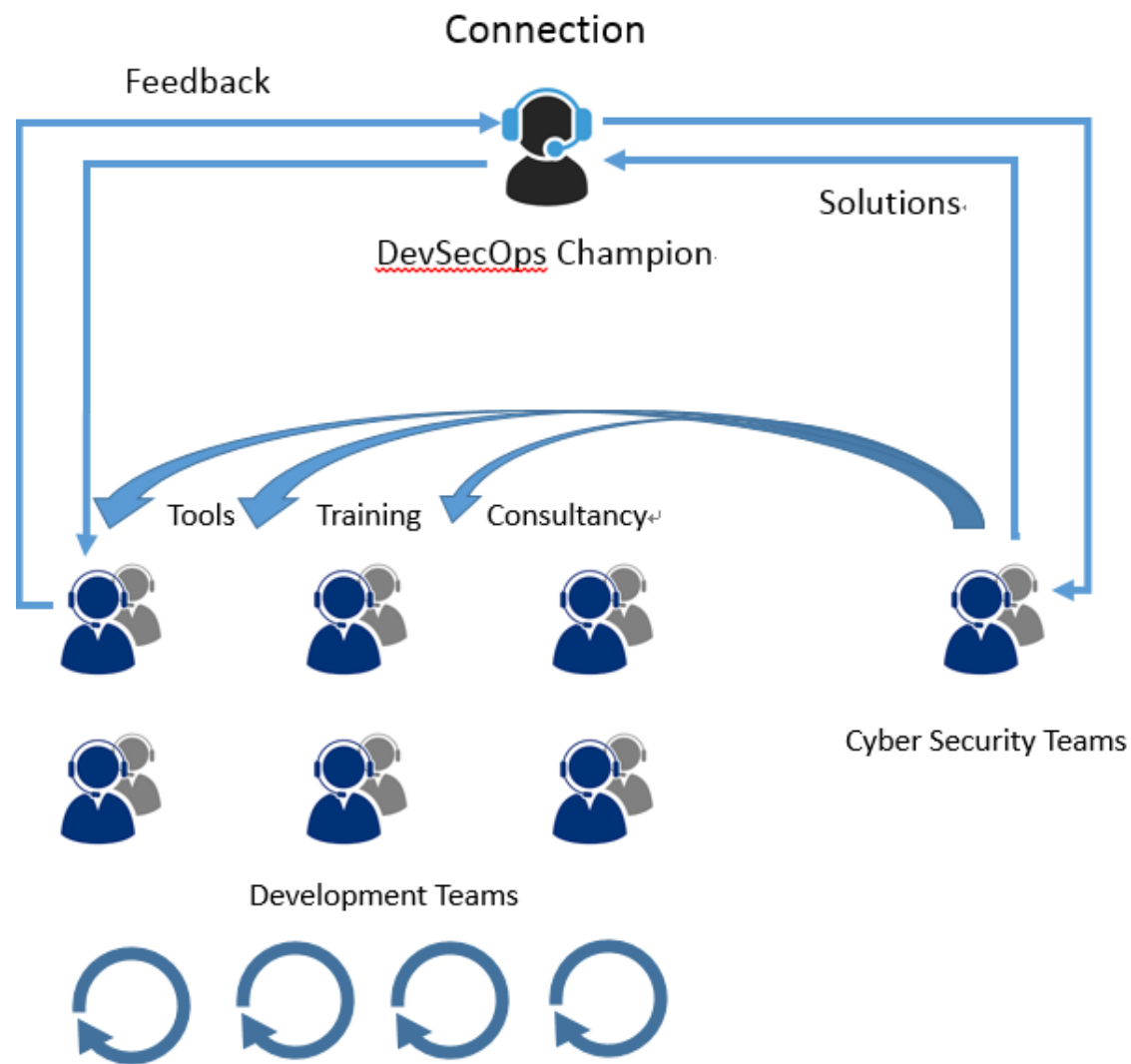
开发团队

- 将DevSecOps工具集成到CI/CD流水线中自动生成安全漏洞扫描报表
- 接受DevSecOps培训从而掌握足够的信息安全知识去修补扫描出来的信息安全漏洞
- 和DevSecOps负责人合作建立DevSecOps文化和意识



信息安全团队

- 向开发团队提供DevSecOps工具支持
- 向开发团队提供DevSecOps培训的支持
- 向开发团队提供信息安全咨询



目录

1 自我介绍

2 DevSecOps介绍

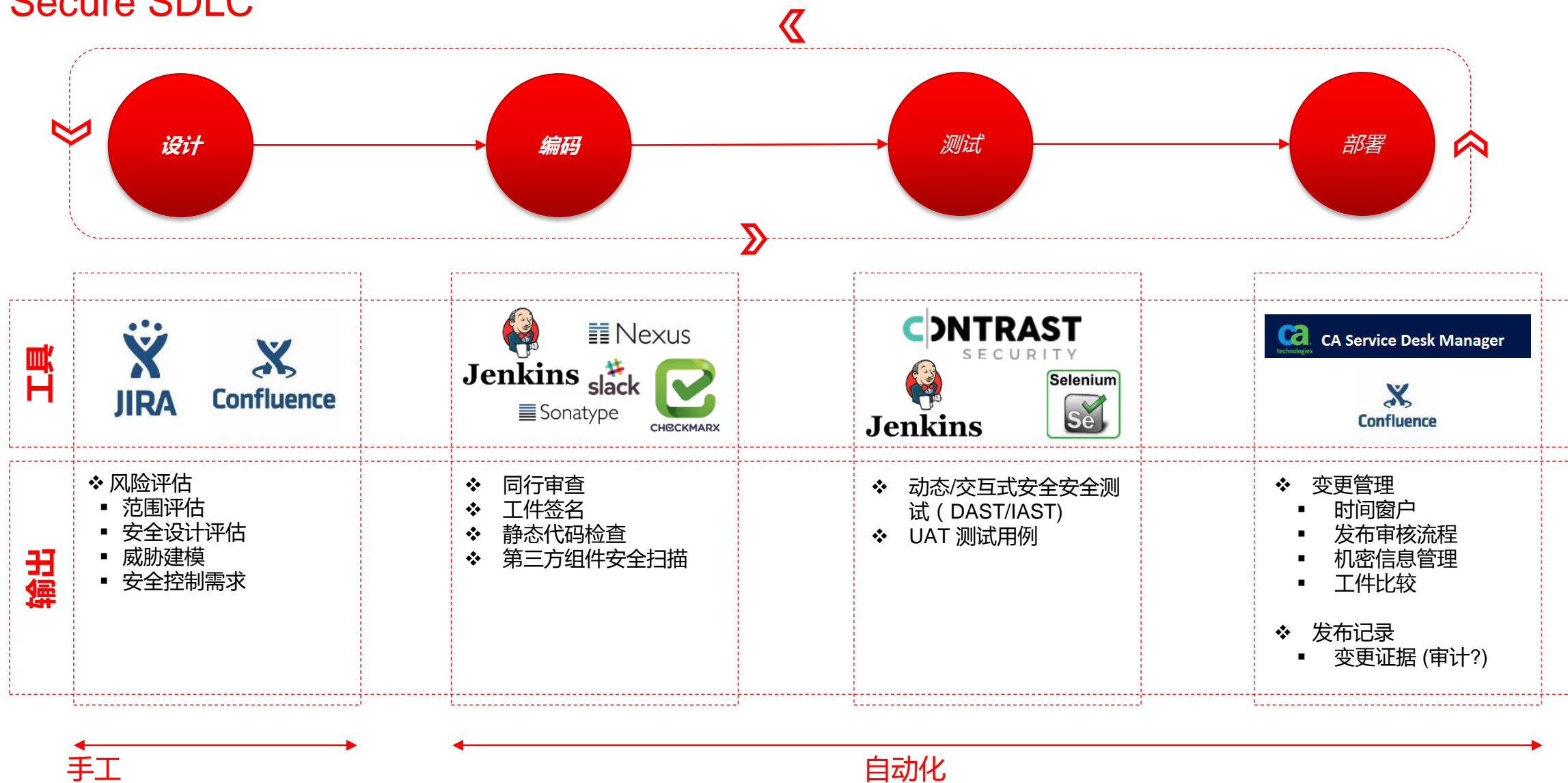
3 DevSecOps实现和运作模型



4 DevSecOps工具

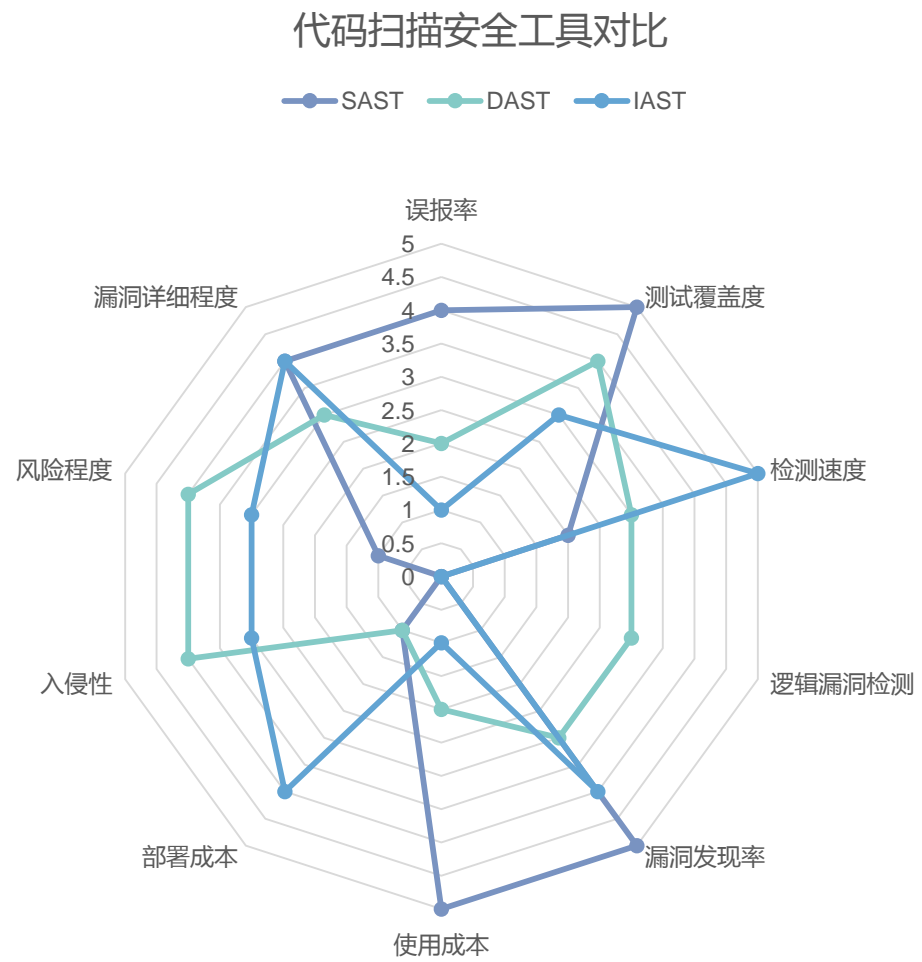
5 DevSecOps文化的建立

Secure SDLC





工具特点和选择的比较



SAST

SAST原理：基于源代码进行检测，可支持多种语言，检出率高，但误报率也高

使用于研发阶段

SAST的优势：

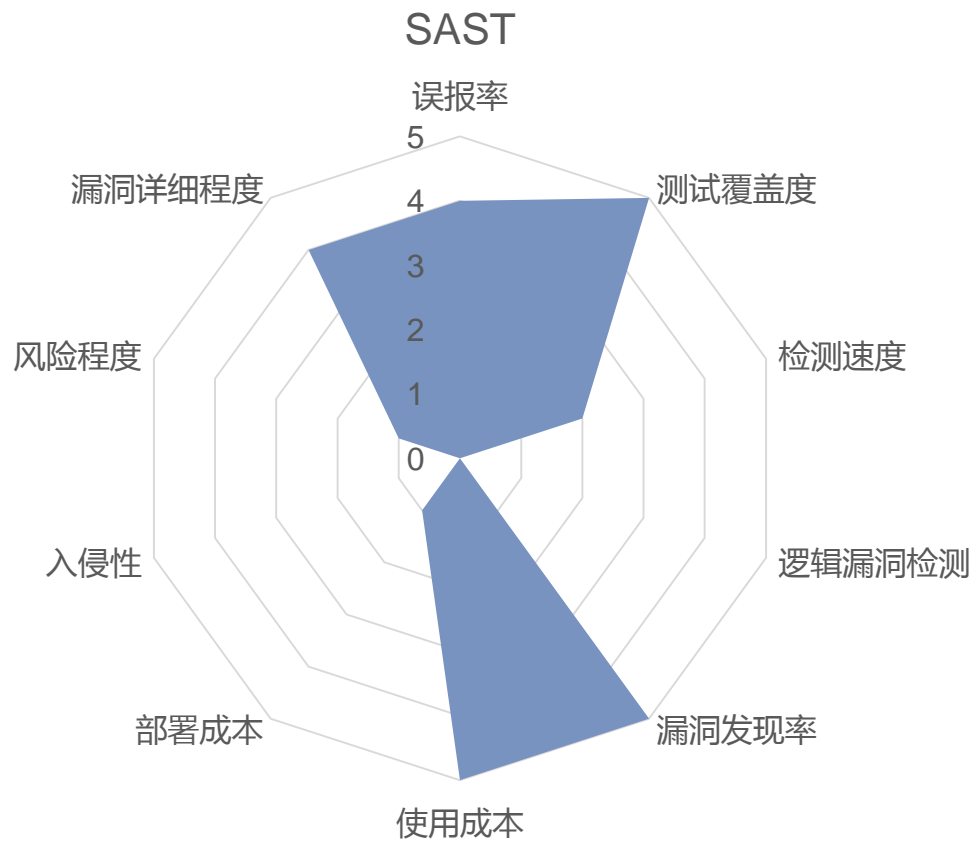
漏洞检测：检出率，覆盖度高

部署使用：侵入性小，风险程度低

SAST的劣势：

漏洞检测：误报高，耗时久

部署使用：人工成本



IAST

IAST原理：与webserver集成，基于扩展获取到的数据流，对语言 and 平台要求高（当前：java/php），检出率高，误报率极低

适用于测试阶段

IAST的优势:

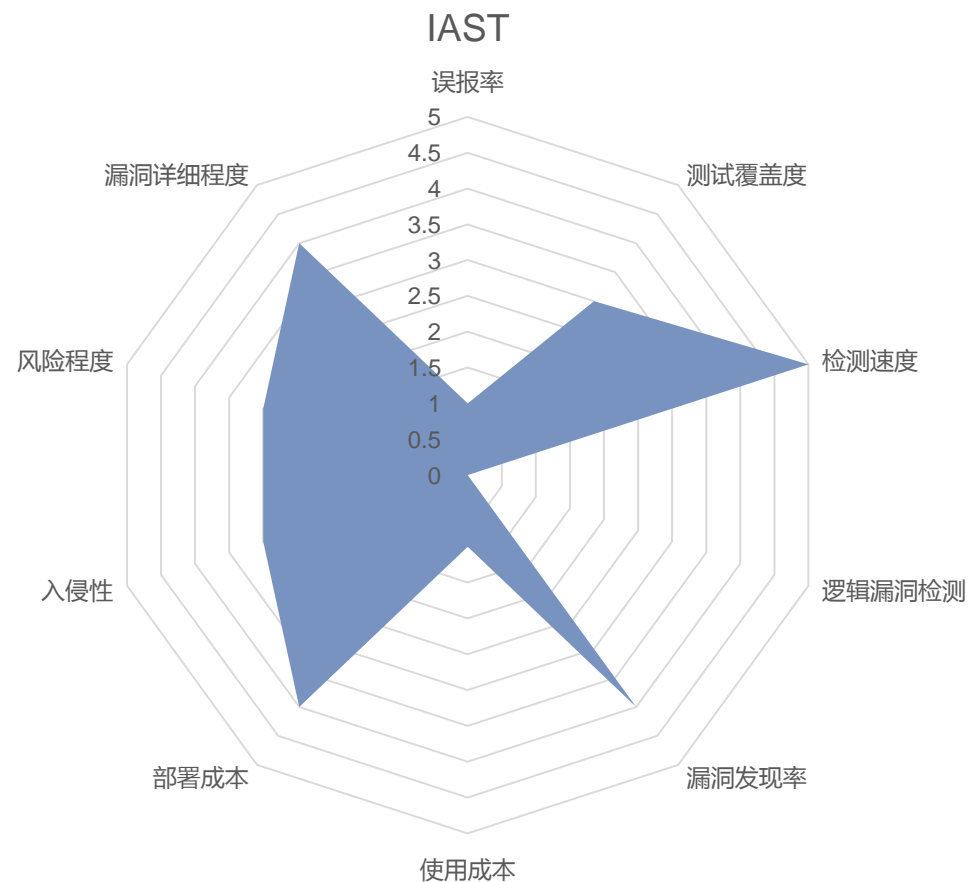
漏洞检测：误报率低，检测速度快，漏洞详细度高

部署使用：人工成本低

IAST的劣势:

漏洞检测：覆盖度难以保证

部署使用：部署成本高（需要集成Web Server，支持的语言和框架较少，价格高昂）



DevSecOps工具

静态应用安全工具

- Fortify
- Checkmarx



动态/交互式应用安全工具

- IBM AppScan
- Contrast



开源软件安全工具

- Sonatype IQ
- Dependencies Check (内部开发)



基础设施安全工具

- Nessus



漏洞管理工具

- Kenna

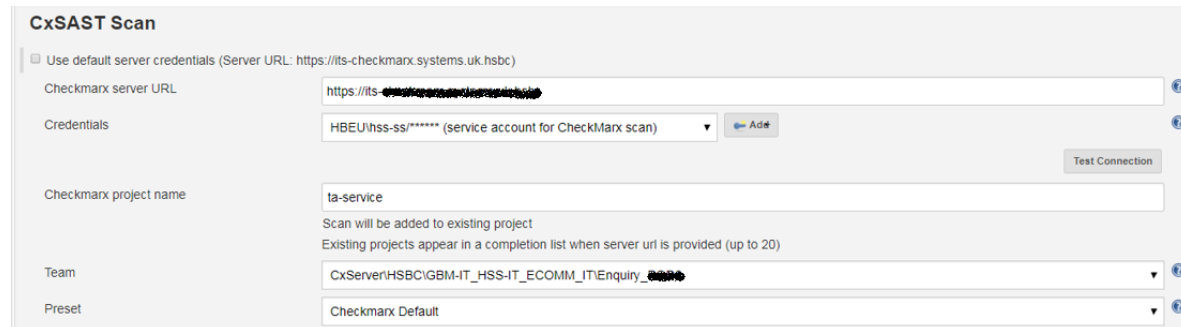
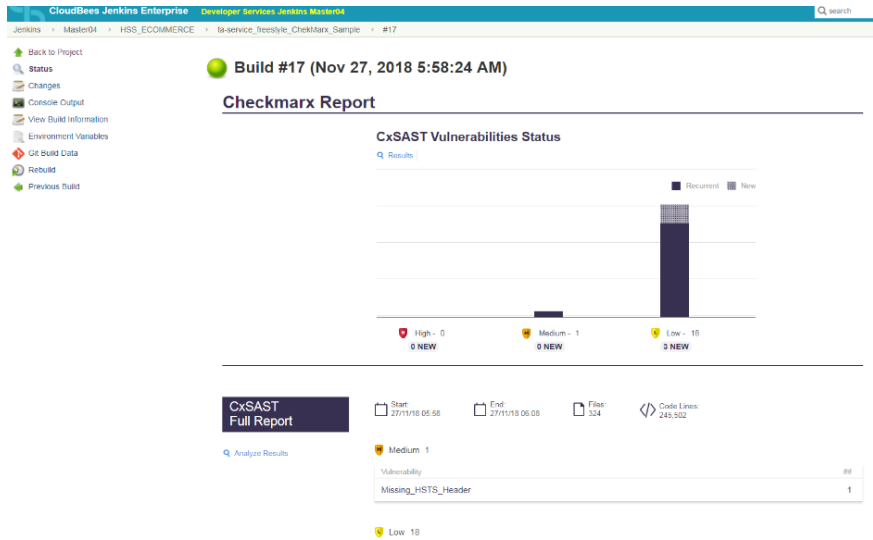
将DevSecOps工具集成到CI/CD流水线

首先, 相关插件需要在Jenkins服务器上安装, 比如Checkmarx Jenkins插件
有两种方法可以在Jenkins上配置Checkmarx扫描

- Freestyle job:
 - 在 “Build”部分选择 “Execute Checkmarx Scan项
 - 配置Checkmarx 服务器URL, 权限和源代码路径

- Pipeline job

Checkmarx 扫描结果报表可以在Jenkins界面上显示出来



CxSAST Scan

☐ Use default server credentials (Server URL: https://its-checkmarx.systems.uk.hsbc)

Checkmarx server URL: https://its-checkmarx.systems.uk.hsbc

Credentials: HBEU/hss-ss/***** (service account for CheckMarx scan) [Add]

Test Connection

Checkmarx project name: ta-service

Scan will be added to existing project

Existing projects appear in a completion list when server uri is provided (up to 20)

Team: CxServerHSBC\GBM-IT_HSS-IT_ECOMM_ITEnquiry_*****

Preset: Checkmarx Default

静态应用安全工具 – Checkmarx

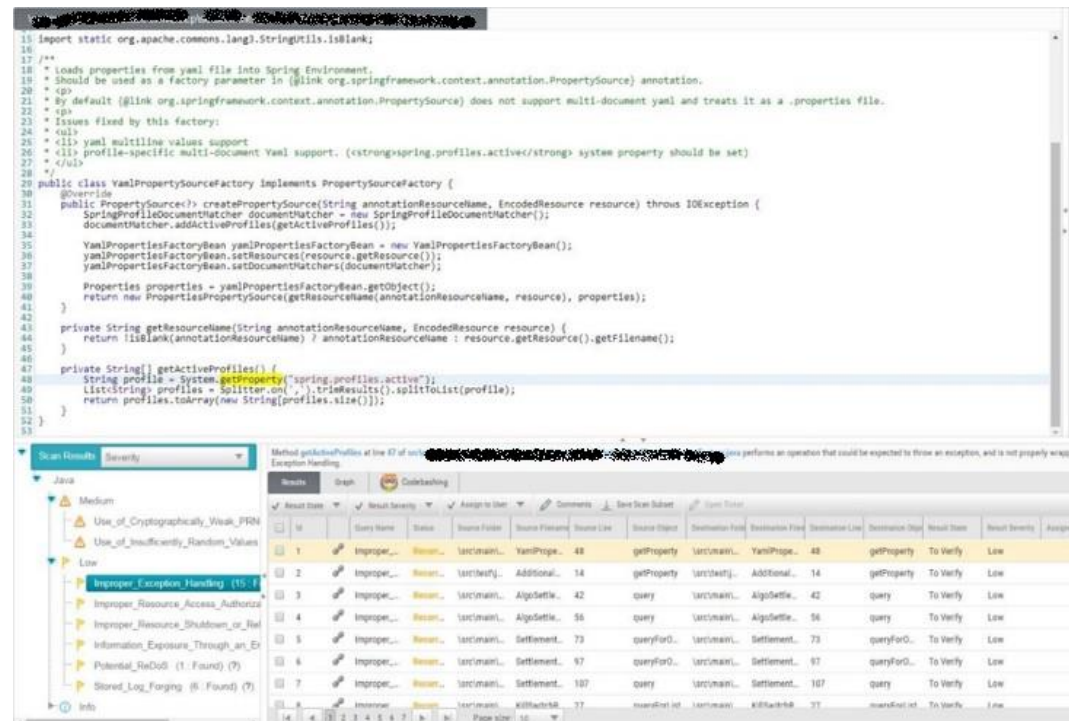
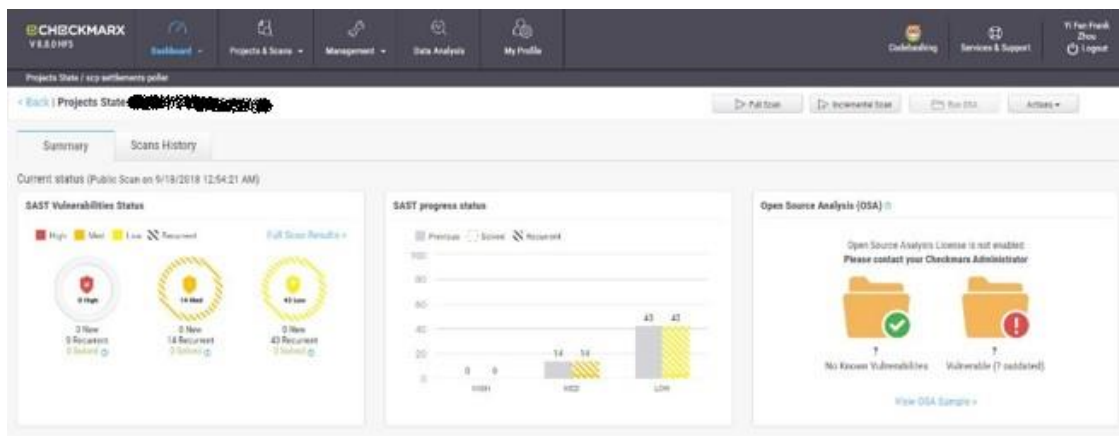
CheckMarx 可以很容易地集成到CICD流水线里自动化安全漏洞扫描和报表流程

CheckMarx 可以生成基于源代码中已发现的安全漏洞的报表

CheckMarx Server 将安全漏洞分类为三个等级 – 高级, 中级和低级

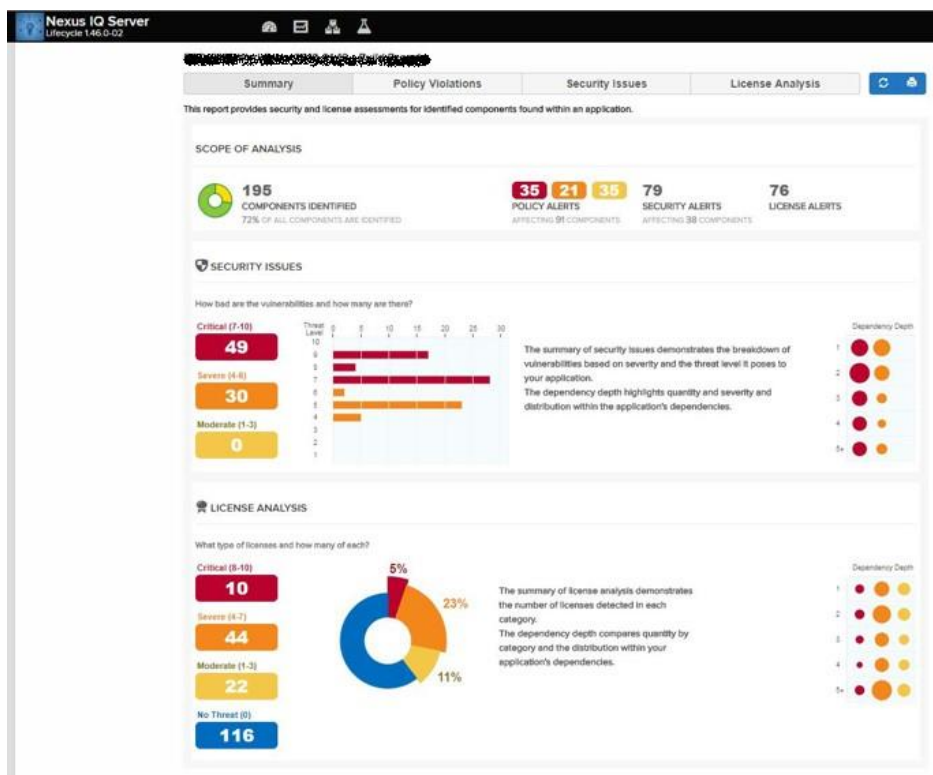
CheckMarx让程序员可以可以发现哪一行代码存在安全漏洞, 这可以帮助程序员很容易和快速的追踪安全漏洞的出处

CheckMarx自带基于已发现的安全漏洞的学习资料帮助程序员去修补安全漏洞



开源软件开源工具 – Sonatype Nexus IQ Server

Nexus IQ Server 可以很容易地被集成到CICD流水线中去自动化安全漏洞扫描和报表流程
Nexus IQ Server 产生的报表, 用于展示开源代码和插件中已经存在的信息安全和执照问题
Nexus IQ Server 有一个可以把所有系统里的相关安全漏洞都能展示的全方位的中央报表
Nexus IQ Server 将安全漏洞分类为三个等级 – 严重, 中等, 没有威胁



Application Name	Build Violations	Stage Release Violations	Release Violations	Contact	Organization
MyApplication	28 159 3 1 minute ago	28 159 3 1 minute ago			My Organization
My Application 4			6 5 1 month ago		My Organization 3
My Application 3	6 11 1 5 months ago				My Organization 7
My Application 2	6 11 1 5 months ago	6 11 1 1 month ago	6 11 1 6 months ago	John Smith	My Organization 4

目录

1 自我介绍

2 DevSecOps介绍

3 DevSecOps实现和运作模型

4 DevSecOps工具

 **5** DevSecOps文化的建立

The screenshot displays a security scan tool interface. On the left, a tree view shows 'Scan Results' with a 'Severity' dropdown. Under 'Java', there is a 'Medium' severity section containing 'Missing_HSTS_Header (1 : Found) (?)'. Below this, a 'Low' severity section lists several other findings: 'Improper_Exception_Handling (1 : Found) (?)', 'Improper_Resource_Access_Authorization (5 : Found) (?)', 'Improper_Resource_Shutdown_or_Release (2 : Found) (?)', and 'Incorrect_Permission_Assignment_For_Critical_Resources (1 : Found) (?)'. On the right, a detailed view for the 'Missing_HSTS_Header' finding is shown. It includes a description: 'Method apiExecute, at line 112 of ... handling code, the application exposes the exception details to error, in method apiExecute of ta-service-war/src/w... 112.' Below this is a table with columns: 'Results', 'Graph', 'Codebashing', 'Result State', 'Result Severity', 'Assign to User', 'Comments', and 'Save Scan Subset'. The table lists four results (Id 11, 12, 13, 14) all marked as 'New' with a severity of 'ex'. The source folder for all is '\ta-service-wa...' and the source filename is 'AbstractTACo...'. The source lines are 133, 136, 140, and 199 respectively.

Id	Direct	Status	Source Folder	Source Filename	Source Line	Source Object
11		New	\ta-service-wa...	AbstractTACo...	133	ex
12		New	\ta-service-wa...	AbstractTACo...	136	ex
13		New	\ta-service-wa...	AbstractTACo...	140	ex
14		New	\ta-service-wa...	AbstractTACo...	199	ex

Missing_HSTS_Header

Risk

What might happen


Failure to set an HSTS header and provide it with a reasonable "max-age" value of at least one year may leave users vulnerable to Man-in-the-Middle attacks.

Cause

How does it happen


Many users browse to websites by simply typing the domain name into the address bar, without the protocol prefix. The browser will automatically assume that the user's intended protocol is HTTP, instead of the encrypted HTTPS protocol.

DevSecOps培训 – 注册自学课程



Fundamentals of Application Security
ELEARNING [REDACTED] ENROLL

START COURSE ▾




REQUIRED

Fundamentals of the PCI-DSS - Assessment
ASSESSMENT [REDACTED] ENROLL

■ Part of Fundamentals of the PCI-DSS

START COURSE >




REQUIRED

How to Create an Application Security Threat Model
ELEARNING [REDACTED] ENROLL

■ Part of How to Create an Application Security Threat Model

START COURSE >



REQUIRED

YOU HAVE UNMET PR...

How to Create an Application Security Threat Model - Assessment
ASSESSMENT [REDACTED] ENROLL

■ Part of How to Create an Application Security Threat Model

DevSecOps在线培训 – Secure Code Warrior [1]

Level 1
0 points

Most Critical Weaknesses
Accuracy
Security Maturity

Leaderboard

Developer names have been anonymised for privacy

Rank	Name	points
1031	Multicoloured Cony	0
1032	Cardiologic Woodborer	0
1033	Nonliving Alaskankleekai	0
1034	Dreamy Pintall	0
1035	Taphophobic Genet	0
1036	David Du Pre	0
1037	Statesmanlike Alleycat	0
1038	Guessable Galapagostortoise	0
1039	Felt Northernseahorse	0
1040	Underqualified Schnauzer	0

Active Missions
Proof of Concept Challenges: A **Hacktivist** from **Brazil** is attacking the **AngularJS Version 1.x Code Snippets** application [View](#)

© Secure Code Warrior 2017

[Tutorial](#) [Feedback](#) [Support](#)

Ref : [1] <https://securecodewarrior.com/training.html>

DevSecOps在线培训 – Secure Code Warrior [2]

The screenshot displays the Secure Code Warrior training interface. The top navigation bar includes links for Learning, Tournaments, Training, Sensei, Assessments, Metrics, and Administration. The main content area is titled "Select Vulnerability Category" and shows a progress bar with a "Challenge Complete" status. Below this, there are four categories of vulnerabilities: Cross-Site Scripting (XSS) - Stored Cross-Site Scripting, Cross-Site Scripting (XSS) - Reflected Cross-Site Scripting, Injection Flaws - HTTP Injection, and Memory Corruption - Stack Overflow. A "Hint" button and a "Submit" button are visible. The "Debug Information" section shows the challenge ID: 580e88240413719554de48eb. The file explorer on the right shows the project structure, with the "public" directory selected. The code editor on the right shows the following code:

```
1 'use strict';
2
3 // filter to make texts bold
4 angular.module('MiniPastebin').filter('boldText', function($sce) {
5   return function(text) {
6     return $sce.trustAsHtml('<b>' + text + '</b>');
7   }
8 });
```

[2] <https://securecodewarrior.com/training.html>

治理：合规和标准，教育与引导，指标设计

实施：安全需要，威胁评估，安全架构

验证：设计审查，安全测试，部署审查

运行管理：加固，事件管理，应急响应等

