THE DEVELOPER'S CONFERENCE

DevSecOps

Seu pipeline completo, com segurança!

Jaqueline Ramos

ESX | Microsoft MVP

Problemas? Todo mundo tem!

E se a situação complicar …

Simplesmente fechar os olhos


WORKED FINE IN DEV
OPS PROBLEM NOW
memegenerator.net


DEVOPS

Principais problemas

THE DEVELOPER'S CONFERENCE

1. Planejamento não condiz com a realidade
2. Pacotes sendo gerados localmente
3. Integração de códigos só quando vai para produção
4. Teste? Oi?
5. Processo de entrega manual (baixar pacote, limpar config, subir no ftp)
6. Muitas falhas, pacotes de hotfix no dia seguinte ao deploy
7. Muito tempo para a entrega de um ambiente
8. Não consigo monitorar meu ambiente

Principais problemas

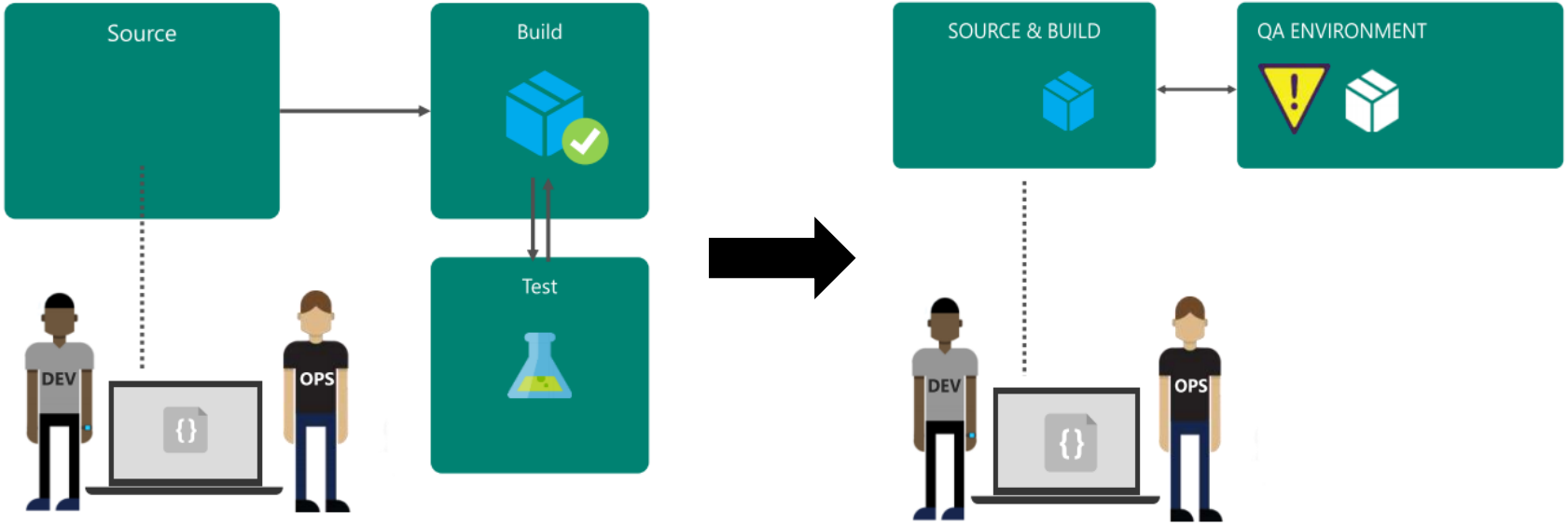
THE DEVELOPER'S CONFERENCE

- Falta de comunicação
- Falta de colaboração
- Sem automatização

Práticas

THE DEVELOPER'S CONFERENCE

- **CI: Continuous Integration**
  - A cada novo commit/check-in, realize testes individuais ou de integração
- **CD: Continuous Deployment**
  - Realize pequenas entregas a qualquer momento, em conjunto com CI


Source
Build
Test
DEV
OPS
SOURCE & BUILD
QA ENVIRONMENT
DEV
OPS

Segurança da informação

THE DEVELOPER'S CONFERENCE

- Qual é o momento em que sua empresa começa a se preocupar com a segurança?


4GIFs
.com

CVE-ID

CVE-2016-4800 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

The path normalization mechanism in PathResource class in Eclipse Jetty 9.3.x before 9.3.9 on Windows allows remote attackers to bypass protected resource restrictions and other security constraints via a URL with certain escaped characters, related to backslashes.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

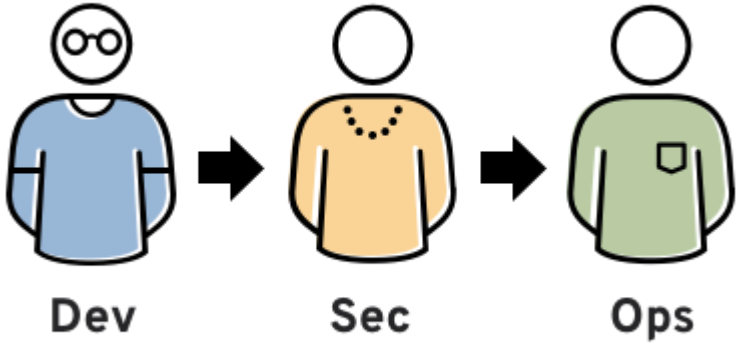
- MLIST:[jetty-announce] 20160531 [jetty-announce] Jetty 9.3.x/Windows Security Vulnerability CVE-2016-4800
- URL:http://dev.eclipse.org/mhonarc/lists/jetty-announce/msg00092.html
- MISC:http://www.ocert.org/advisories/ocert-2016-001.html
- MISC:http://www.zerodayinitiative.com/advisories/ZDI-16-362
- BID:90945
- URL:http://www.securityfocus.com/bid/90945

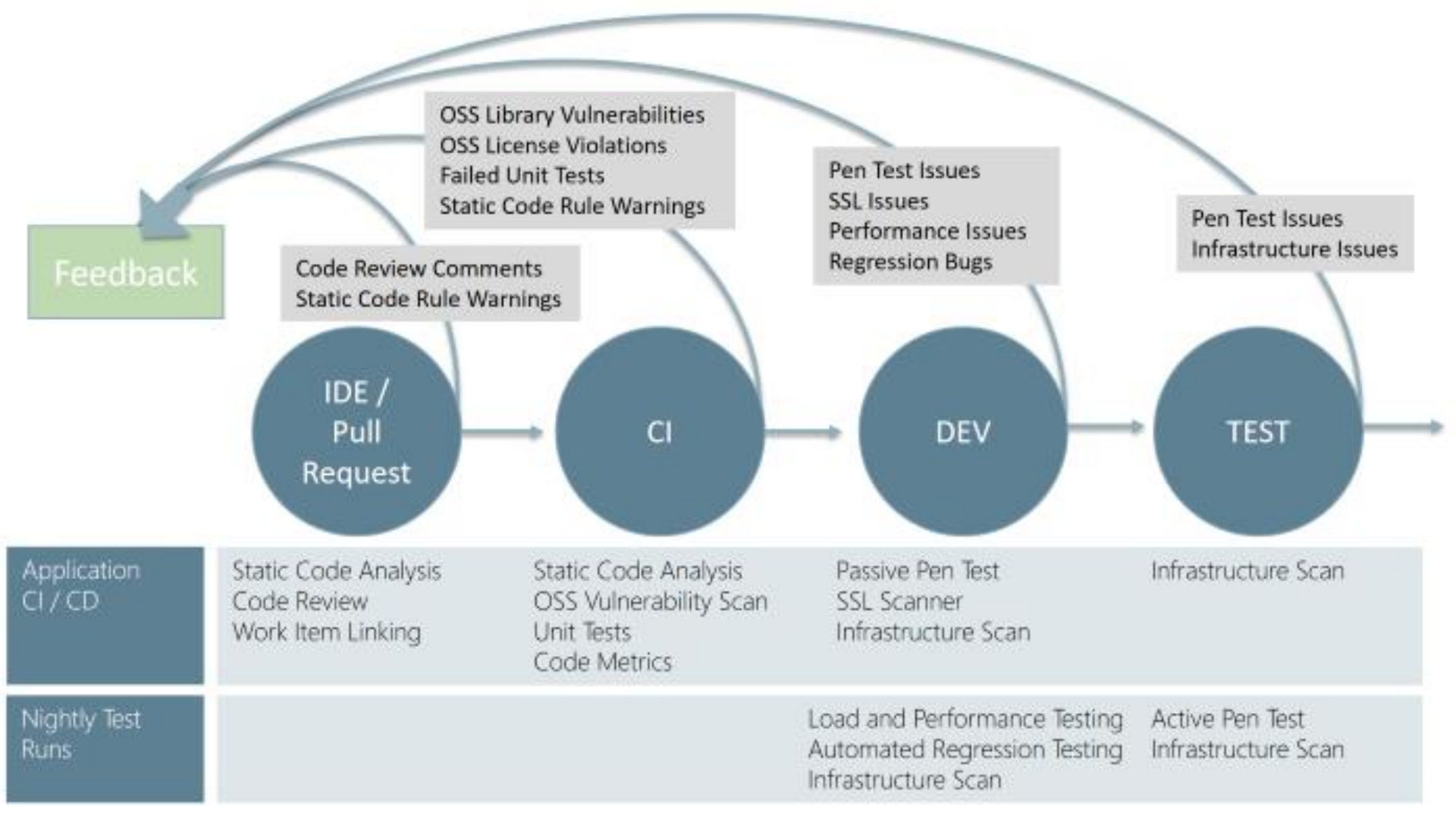
Assigning CNA

DevSecOps

THE DEVELOPER'S CONFERENCE

- **CS: Continuous Security**




Feedback
OSS Library Vulnerabilities
OSS License Violations
Failed Unit Tests
Static Code Rule Warnings
Code Review Comments
Static Code Rule Warnings
Pen Test Issues
SSL Issues
Performance Issues
Regression Bugs
Pen Test Issues
Infrastructure Issues
IDE / Pull Request
CI
DEV
TEST
Application CI / CD
Static Code Analysis
Code Review
Work Item Linking
Static Code Analysis
OSS Vulnerability Scan
Unit Tests
Code Metrics
Passive Pen Test
SSL Scanner
Infrastructure Scan
Infrastructure Scan
Nightly Test Runs
Load and Performance Testing
Automated Regression Testing
Infrastructure Scan
Active Pen Test
Infrastructure Scan

security

21 Results

Showing: Azure Pipelines | Hosted On: Any | Price: Any | Sort By: Relevance

Container Security
Aqua Security ↓250
Vulnerability scanner for container images
★★★★★ FREE

Codified Security
Codified Security ↓45
This step uploads your app to Codified Security for automated mobile app...
☆☆☆☆☆ FREE

Application Security T
HCL Technologies ↓10
Perform static and open source security tests for your applications built with VSTS
☆☆☆☆☆ FREE

SD Elements Integrati
Security Compass ↓4
Security Compass SD Elements Platform Integration
☆☆☆☆☆ FREE

Veracode
Veracode ↓2.3K
Find and fix security defects as part of your Azure DevOps pipeline - v2.4.0
★★★★☆ FREE

FOSSA
Fossa ↓17
Automatically analyze your code for open source license compliance and security...
☆☆☆☆☆ FREE

WhiteSource Bolt
WhiteSource ↓1.8K

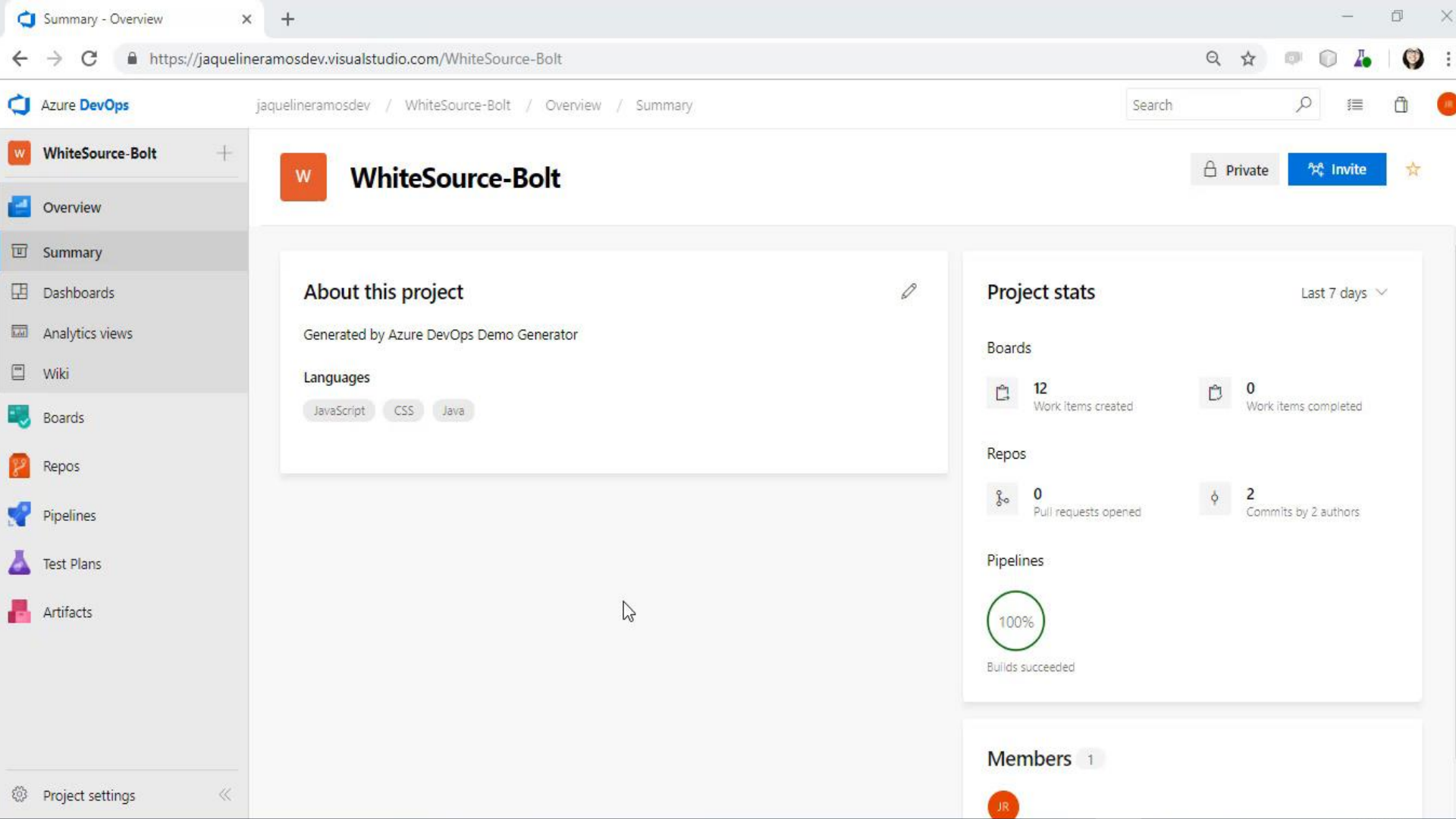
WhiteSource
WhiteSource ↓1.1K

OWASP Zed Attack Pr
Kasun Kodagoda ↓614

Kiuwan
Kiuwan Software ↓103

Secure DevOps Kit (Az
Microsoft DevLabs ↓918

Dotfuscator Commun
PreEmptive Solutio ↓540


Summary - Overview
https://jaquelineramosdev.visualstudio.com/WhiteSource-Bolt
Azure DevOps
jaquelineramosdev / WhiteSource-Bolt / Overview / Summary
Search
WhiteSource-Bolt
Overview
Summary
Dashboards
Analytics views
Wiki
Boards
Repos
Pipelines
Test Plans
Artifacts
Project settings
WhiteSource-Bolt
Private
Invite
About this project
Generated by Azure DevOps Demo Generator
Languages
JavaScript
CSS
Java
Project stats
Last 7 days
Boards
12
Work items created
0
Work items completed
Repos
0
Pull requests opened
2
Commits by 2 authors
Pipelines
100%
Builds succeeded
Members
1
JR

Links de apoio

THE DEVELOPER'S CONFERENCE

Maratona Azure DevOps

THE DEVELOPER'S CONFERENCE

bit.ly/MaratonaAzureDevOps

Obrigada!!

THE DEVELOPER'S CONFERENCE

bit.ly/2S19v2d

@JaqueCR2

bit.ly/2uhN28S

bit.ly/2yMPROF