Being Mean To Your Code: Integrating Security Tools into Your DevOps Pipeline

Boston Code Camp 26
November 19, 2016

Robert Hurlbut

RobertHurlbut.com • @RobertHurlbut

Boston Code Camp 26 - Thanks to our Sponsors!

- Platinum

- Gold

- Silver

- Bronze

- In-Kind Donations

Robert Hurlbut

Software Security Consultant, Architect, and Trainer

- Owner / President of Robert Hurlbut Consulting Services
- Microsoft MVP – Developer Technologies and Security 2005-2009, 2015, 2016
- (ISC)2 CSSLP 2014-2017
- Co-host with Chris Romeo – App Sec Podcast (https://appsecpodcast.org)

Contacts

Web Site: https://roberthurlbut.com

Twitter: @RobertHurlbut, @AppSecPodcast

ROBERT HURLBUT CONSULTING SERVICES

securedevelop.NET

Who is this for?

Developers

QA

Operations

Security

Consultants

(Managers)

Whomever is involved in automation!

What are trying to solve?

Find security issues as early as possible

Integration into the DevOps (CI/CD) pipeline

What are we **not** trying to solve?

Finding all possible vulnerabilities

Putting pentesters out of a job ☺

What can you get out of this?

A way to quickly evaluate your apps

Options for more thorough scanning

Introduction to Gauntlt

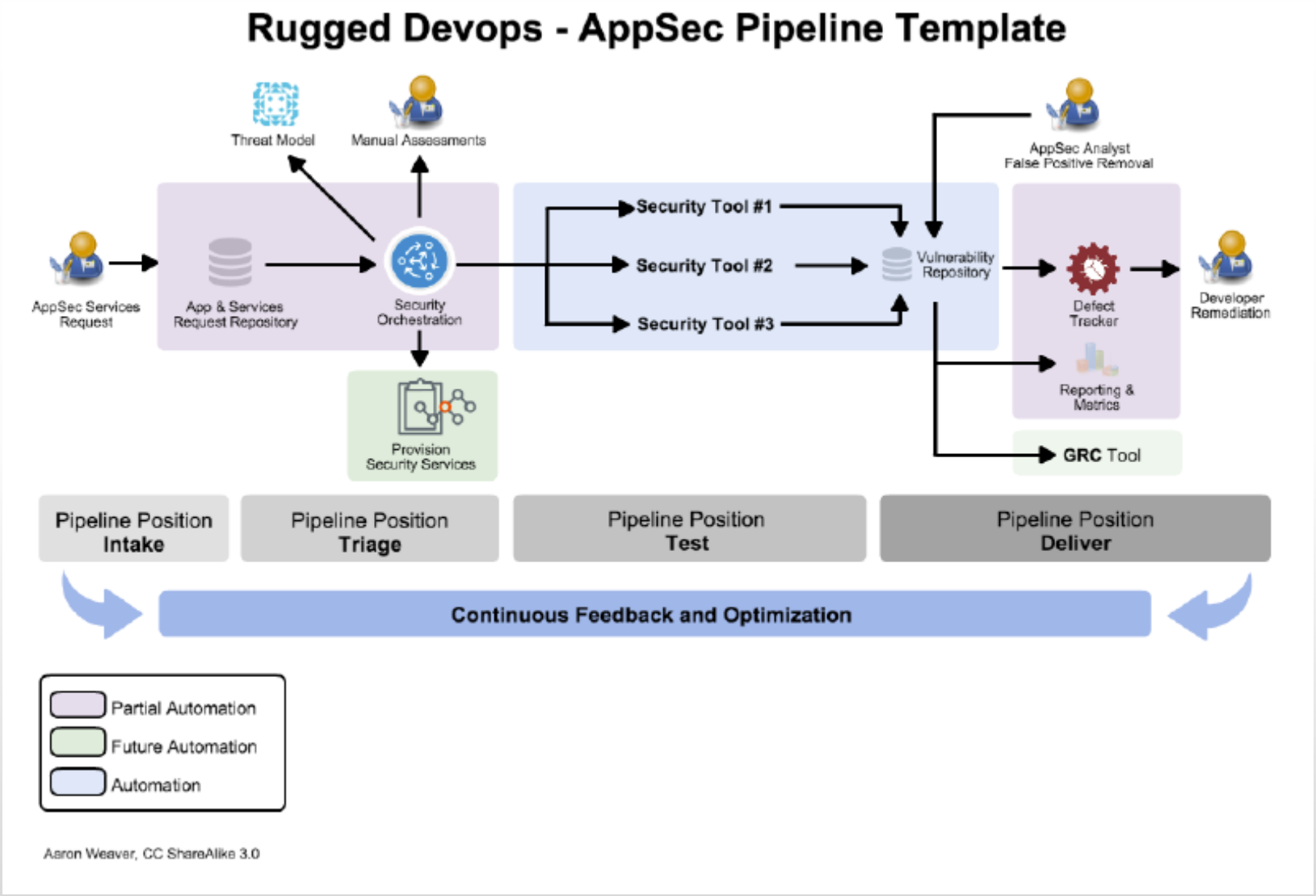
Introduction to ZAP API

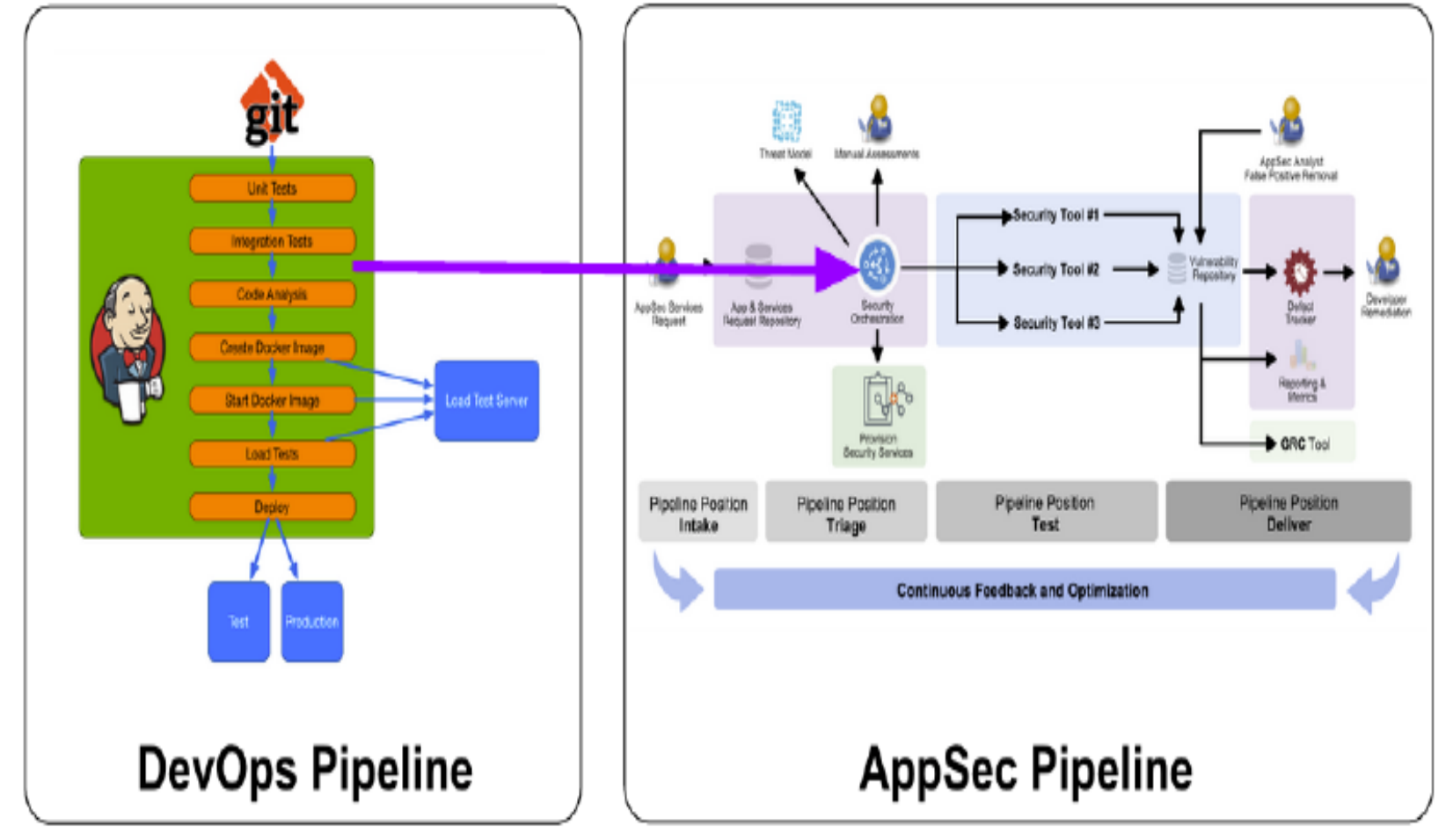
Integrating results

What is DevOps?

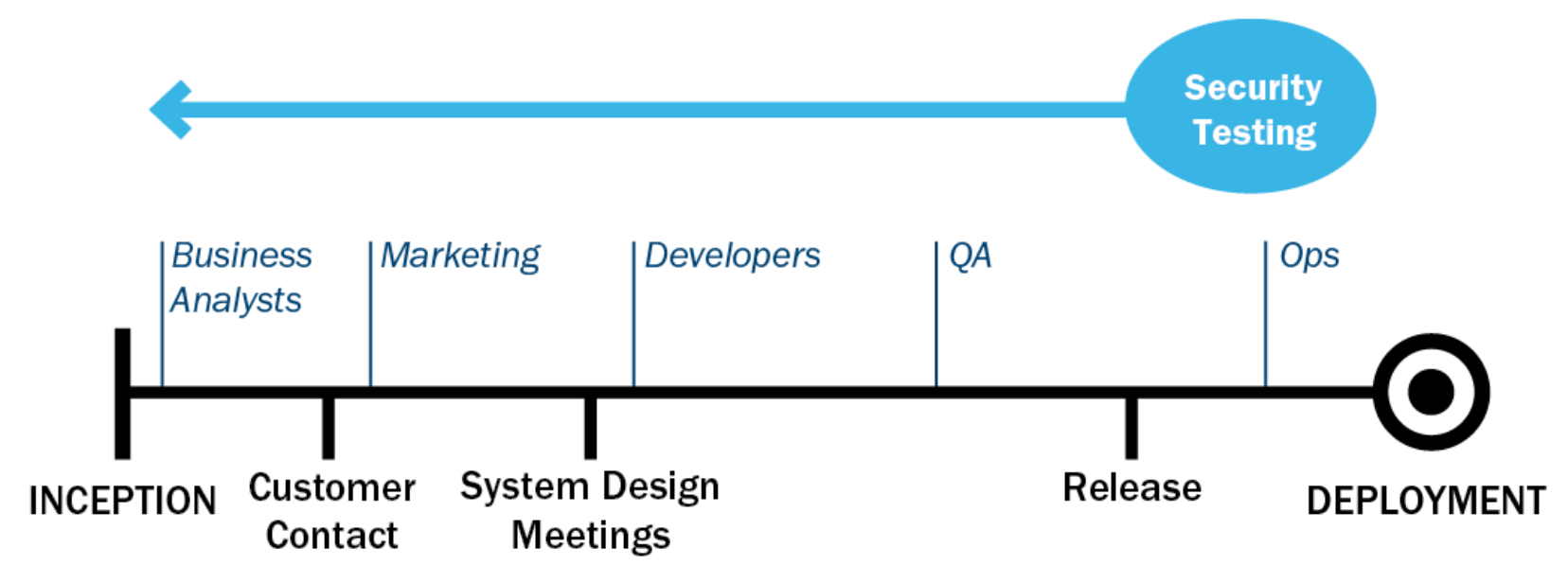
DevOps (development and operations) - a type of agile relationship between Development and IT Operations.

Goal: Change and improve relationship by advocating better communication and collaboration between the two business units.





Moving security testing to the left



DevOps or not, automate/integrate security in

Even if no DevOps, think about automating security tests

Integrate tests into your pipeline, either for deployment (continuous or not) or build integration (continuous or not)

Use test results to drive vulnerability management (bug fixes, etc.)

Automate Testing with Security Tools

Gauntlt

Open source, MIT License

Gauntlt comes with pre-canned steps that hook security testing tools

Gauntlt does not install tools

Gauntlt wants to be part of the CI/CD pipeline

Be a good citizen of exit status and stdout/stderr

Gauntlt

Gauntlt comes packaged with a set of pre-canned attacks using a pre-defined set of "attack adapters" that map the steps to the security tools that can run each type of attack:

- Arachni (testing for XSS)
- Garmr (testing for new login pages or insecure references in login flows)
- SQLmap (testing for SQL injection attacks)
- dirb (testing for misconfigured web objects)
- SSlyze (testing for misconfigured SSL servers)
- NMap (testing for unexpected open ports)

Gauntlt reporting

bundle exec gauntlt --format html > out.html

BDD/Gerkhin Security Assertion

Scenario: Lock the user account out after 4 incorrect authentication attempts

Meta: @id auth_lockout

Given the default username from: users.table

And an incorrect password

And the user logs in from a fresh login page 4 times

When the default password is used from: users.table

And the user logs in from a fresh login page

Then the user is not logged in

Gauntlt - Cucumber syntax

```
Feature: nmap attacks for example.com
  Background:
    Given "nmap" is installed
    And the following profile:
    | name     | value       |
    | hostname | example.com |
  Scenario: Verify that there are no unexpected ports open
    When I launch an "nmap" attack with:
      """
      nmap -F <hostname>
      """
    Then the output should not contain:
      """
```

Gauntlt - example

```
@slow

Feature: nmap robots attack

Background:
Given "nmap" is installed
And the following profile:
| name | value |
| hostname | www.cert.org |

Scenario: Detects robots.txt files on this host.
When I launch an "nmap" attack with:
"""
nmap --script http-robots.txt <hostname>
"""
Then the output should contain:
"""
| http-robots.txt:
"""
```

OWASP Zed Attack Proxy (ZAP)

ZAP is used to test for the most common vulnerabilities that accompany web applications

For instance, SQL Injection and cross-site scripting (XSS) are two types of attacks that can be prevented with the use of ZAP

Ideal for beginners

Checks for security headers, other requirements

ZAP Features

Swing based UI for desktop mode
Comprehensive API for daemon mode
Plugin architecture (add-ons)
Online ‘marketplace’ (all free)
Release, beta, and alpha quality add-ons
Traditional and ajax spiders
Passive and active scanning
Highly configurable, eg scan policies
Highly scriptable

Some ZAP use cases

Point and shoot – the Quick Start tab

Proxying via ZAP, and then scanning

Manual pentesting

Automated security regression tests

Debugging

Part of a larger security program

ZAP Install Options

Windows .exe

Linux .tar .gz

Mac OS .dmg

Docker Images

Distros like Kali

Run ZAP UI

Simplest way to run

But, basic results

Run ZAP through API

Command line with the -daemon flag.

This option allows for easy integration into your CI server because you will be able to run ZAP by including a post-build step specifically for ZAP.

If using Jenkins as your CI server, there is a ZAP plug-in specifically for Jenkins.

All you have to do is download the plug-in from the Jenkins plug-in manager and add a post-build step.

ZAP API Command Line

Options:

-cmd	Runs ZAP 'inline', ie without starting the UI or a daemon
-config	Overrides the specified key=value pair in the configuration file
-daemon	Starts ZAP in 'daemon' mode, ie without a UI
-dir	Uses the specified directory instead of the default one
-installdir	Overrides the code that detects where ZAP has been installed with the specified directory
-h	Shows all of the command line options available, including those added by add-ons
-help	The same as -h
-host	Overrides the host used for proxying specified in the configuration file
-port	Overrides the port used for proxying specified in the configuration file
-version	Reports the ZAP version
-newsession	Creates a new session at the given location
-session	Opens the given session after starting ZAP

ZAP API Command Line Examples

Start ZAP in 'daemon' mode with a new session created at a given path:

-daemon -newsession session

Create a report of the last scan of an existing session and exit ZAP once finished:

-last_scan_report /path/to/save/report.xml -session /path/to/existing/session -cmd

Use zapr

Command-line wrapper around ZAP

https://github.com/garethr/zapr

ZAP Report

	Application Error Disclosure
	This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This info launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.
	http://128.237.191.24:8080/docs/manager-howto.html
	N/A
	java.lang.NumberFormatException: For input string:
	http://128.237.191.24:8080/docs/jndi-resources-howto.html
	N/A
	JDBC Driver
	http://128.237.191.24:8080/docs/jndi-datasource-examples-howto.html
	N/A
	JDBC Driver
	http://128.237.191.24:8080/docs/config/listeners.html
	N/A
	JDBC Driver
	http://128.237.191.24:8080/examples/jsp/error/err.jsp?name=bmw328i&submit=Submit
	N/A
	HTTP 500 Internal server error

ThreadFix

Automates matching and merging of report results from dynamic, static, and interactive application scanners.

Integrates with with report results from: OWASP ZAP, Burp Suite, Veracode, Contrast Security, and on and on

Summary

Automate all the things

Add security testing as part of your CI/CD pipeline

Take a look at Gauntlt and ZAP as two possible open / free tools

Integrate results from security tools to manage vulnerabilities

Resources - Books

The DevOps Handbook: How to Create World-Class Agility, Reliability, & Security in Technology Organizations

Gene Kim, Jez Humble, Patrick Debois, John Willis

Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation

Jez Humble, David Farley

Resources - Tools

Gauntlt

http://gauntlt.org/index.html#getting-started

Owasp ZAP

https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

ThreadFix (from Denim Group)

https://www.threadfix.it

Questions?

Contacts

Web Site: https://roberthurlbut.com

Twitter: @RobertHurlbut, @AppSecPodcast

Email: robert at roberthurlbut.com

ROBERT HURLBUT CONSULTING SERVICES

securedevelop.NET