SECURITY IN THE DELIVERY PIPELINE

JAMES WICKETT
SIGNAL SCIENCES

GOTO; Amsterdam 2017

@WICKETT

Want the slides?

james@signalsciences.com

@WICKETT

- HEAD OF RESEARCH AT SIGNAL SCIENCES
- ORGANIZER OF DEVOPS DAYS AUSTIN
- LYNDA.COM AUTHOR ON DEVOPS
- RECOVERING FROM YEARS OF OPS AND SECURITY

SUMMARY

- SECURITY IS STILL MAKING THE JOURNEY OF DEVOPS
- SECURITY SEES NEW OPPORTUNITIES TO AUTOMATE AND ADD VALUE
- THE DELIVERY PIPELINE EXTENDS FARTHER THAN WE USUALLY CONSIDER

MORE SUMMARY

- CULTURE AND TOOLING NEED TO ALIGN FOR US TO MAKE THIS WORK
- COVERAGE OF SECURITY TOOLS FOR THREE PIPELINE AREAS: INHERIT, BUILD AND RUNTIME
- ADVICE FOR DEALING WITH THE AUDITORS AND OTHER BLOCKERS

CI/CD JOURNEY

GOTO; Amsterdam 2017

@WICKETT

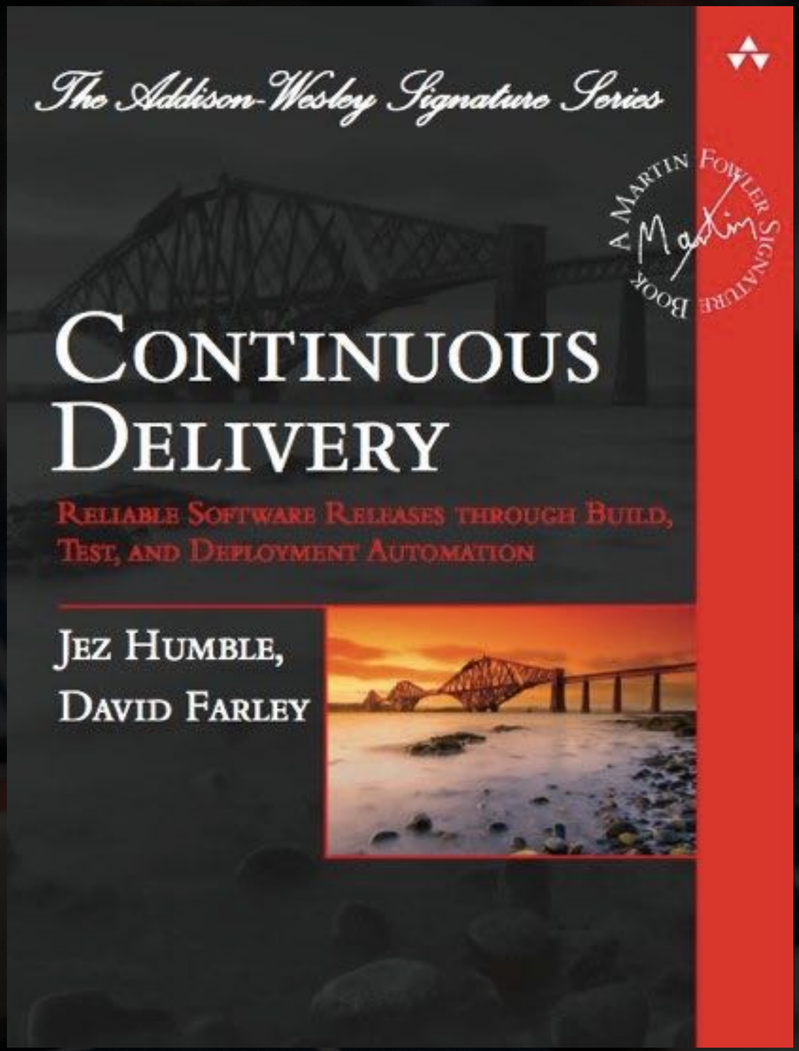
CI/CD at three companies

GOTO; Amsterdam 2017

@WICKETT

Currently, at Signal Sciences we do about 15 deploys per day

Roughly 10,000 deploys in the last 2.5 yrs



GOTO; Amsterdam 2017

@WICKETT

CD is how little you can deploy at a time

We optimized for cycle time—the time from code commit to production

Gave power to the team to deploy

Signal Sciences is a software as a service company and a security company

Security had to be part of CI/CD and the overall delivery pipeline

Before Signal Sciences

Rugged Software circa 2010

GOTO; Amsterdam 2017

@WICKETT

Rugged Software Development

Joshua Corman, David Rice, Jeff Williams
2010

Security vs. Rugged

- Absence of Events
- Cost
- Negative
- FUD
- Toxic

- Verification of quality
- Benefit
- Positive
- Known values
- Affirming

Started Gauntlt
4 years ago

Security is different in CI/CD

GOTO; Amsterdam 2017

@WICKETT

SECURITY'S DILEMMA

GOTO; Amsterdam 2017

@WICKETT

Security Epistemology is difficult to assess

GOTO; Amsterdam 2017

@WICKETT

Early days of the industry created a binary approach to security

Breached or Secure

GOTO; Amsterdam 2017

@WICKETT

This creates a false dichotomy

Complexity Reductionism falsely propagates this type of thinking

Breached or secure?
This is not the question we should ask

Where can security add value?

AN OPINIONATED VIEW OF HOW WE GOT HERE

GOTO; Amsterdam 2017

@WICKETT

Agile

Agile attempted to remove epistemological gaps in software development

GOTO; Amsterdam 2017

@WICKETT

Largely it worked and created a new culture of rapid delivery and feedback loops

GOTO; Amsterdam 2017

@WICKETT

Operations didn’t ride the first wave of Agile

Continuation of Agile to Ops

DEVOPS IS THE APPLICATION OF AGILE METHODOLOGY TO SYSTEM ADMINISTRATION

– THE PRACTICE OF CLOUD SYSTEM ADMINISTRATION BOOK

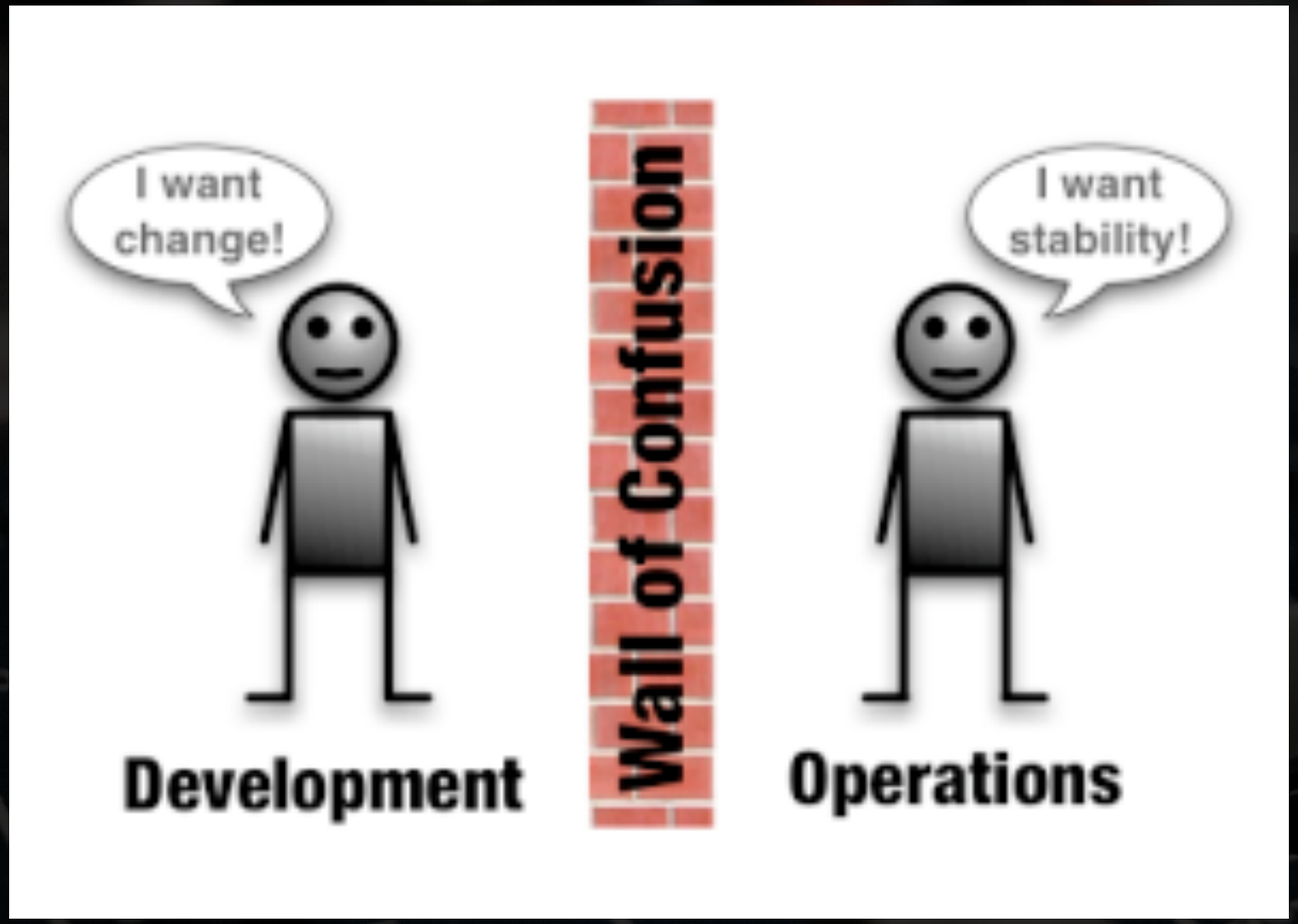
GOTO; Amsterdam 2017

@WICKETT

10 deploys per day

Dev & ops cooperation at Flickr

John Allspaw & Paul Hammond
Velocity 2009


I want change!
I want stability!
Wall of Confusion
Development
Operations


WORKED FINE IN DEV
OPS PROBLEM NOW
memegenerator.net

DEV : OPS

10 : 1

CULTURE IS THE MOST IMPORTANT ASPECT TO DEVOPS SUCCEEDING IN THE ENTERPRISE

- PATRICK DEBOIS

4 KEYS TO CULTURE

- MUTUAL UNDERSTANDING
- SHARED LANGUAGE
- SHARED VIEWS
- COLLABORATIVE TOOLING

SECURITY WAS LEFT OUT OF THE STORY

GOTO; Amsterdam 2017

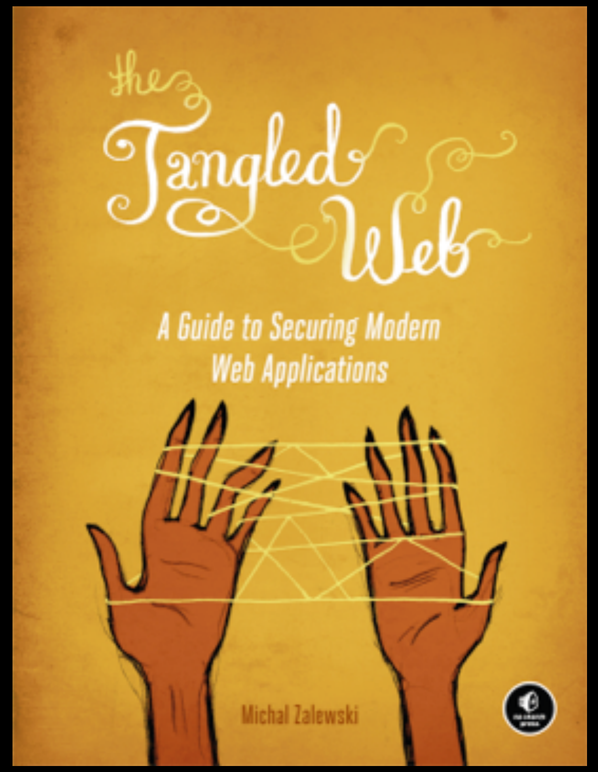
@WICKETT

Why?

Compliance Driven Security

GOTO; Amsterdam 2017

@WICKETT



[Security by risk assessment] introduces a dangerous fallacy: that structured inadequacy is almost as good as adequacy and that underfunded security efforts plus risk management are about as good as properly funded security work

Dev : Ops : Sec
100 : 10 : 1

Security as the cultural outlier in an organization

GOTO; Amsterdam 2017

@WICKETT

“SECURITY PREFERS A SYSTEM POWERED OFF AND UNPLUGGED”

- DEVELOPER

“…THOSE STUPID DEVELOPERS”

- SECURITY PERSON

“every aspect of managing WAFs is an ongoing process. This is the antithesis of set it and forget it technology. That is the real point of this research. To maximize value from your WAF you need to go in with everyone’s eyes open to the effort required to get and keep the WAF running productively.”

- WHITEPAPER FROM AN UNDISCLOSED WAF VENDOR

Bottleneck Approach

THE AVERAGE TIME TO DELIVER CORPORATE IT PROJECTS HAS INCREASED FROM ~8.5 MONTHS TO OVER 10 MONTHS IN THE LAST 5 YEARS

Revving up your Corporate RPMs, Fortune Magazine, Feb 1, 2016

THE GROWTH OF [SECURITY] FUNCTIONS WHICH IS TOO OFTEN POORLY COORDINATED... [RESULTING IN] A PROLIFERATION OF NEW TASKS IN THE AREAS OF COMPLIANCE, PRIVACY AND DATA PROTECTION.

Revving up your Corporate RPMs, Fortune Magazine, Feb 1, 2016

IT IS 30 TIMES CHEAPER TO FIX SECURITY DEFECTS IN DEV VS. PROD

NIST, 2002, The Economic Impacts of Inadequate Infra for Software Testing

NIST, 2002, The Economic Impacts of Inadequate Infra for Software Testing

Security is ineffective

GOTO; Amsterdam 2017

@WICKETT

SECURITY KNOWS IT MUST CHANGE OR DIE

GOTO; Amsterdam 2017

@WICKETT

Companies are spending a great deal on security, but we read of massive computer-related attacks. Clearly something is wrong.

The root of the problem is twofold: we're **protecting the wrong things**, and **we're hurting productivity** in the process.

THINKING SECURITY, STEVEN M. BELLOVIN 2015

AVERAGE INCIDENT COST IS $5.4 MILLION IN THE U.S.

Poneman Institute, 2013, Cost of Data Breach Report

High performers spend 50 percent less time remediating security issues than low performers. By better integrating information security objectives into daily work, teams achieve higher levels of IT performance and build more secure systems.

2016 State of DevOps Report

High performing orgs achieve quality by incorporating security (and security teams) into the delivery process

2016 State of DevOps Report

A large percentage of the companies on the expo floor will not there in 5 years @rmogull #RSAC2017

5:51 PM - 14 Feb 2017

2

http://www.youtube.com/watch?v=jQbIKuMuS0Y

A CI/CD PIPELINE

GOTO; Amsterdam 2017

@WICKETT

Pipelines look different for different people

PIPELINE PHASES

- DESIGN
- BUILD
- DEPLOY
- OPERATE

PIPELINE PHASES

- DESIGN
- INHERIT
- BUILD
- DEPLOY
- OPERATE

WE WILL FOCUS HERE

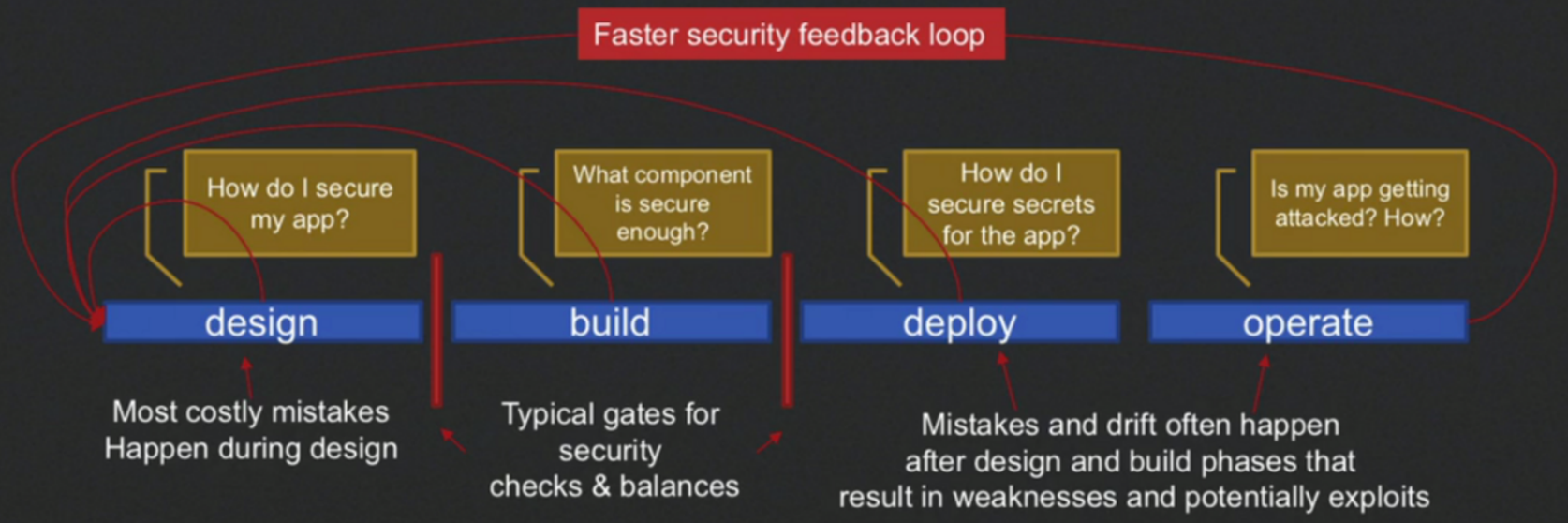
- DESIGN
- INHERIT
- BUILD
- DEPLOY
- OPERATE

SECURITY CONSIDERATIONS

- INHERIT — What have I bundled into my app that leaves me vulnerable?
- BUILD — Do my build acceptance tests and integration tests catch security issues before release?
- OPERATE — Am I being attacked right now? Is it working?

Secure Software Supply Chain

1. Gating processes are not Deming-like
2. Security is a design constraint
3. Decisions made by engineering teams
4. It's hard to avoid business catastrophes by applying one-size-fits-all strategies
5. Security defects is more like a *security "recall"*



Secure Software Supply Chain presented by Shannon Leitz at DevOps Days Austin 2016.

SECURITY IN THE DELIVERY PIPELINE

GOTO; Amsterdam 2017

@WICKETT

INHERIT

OpenSSL

GOTO; Amsterdam 2017

@WICKETT

Shellshock

GOTO; Amsterdam 2017

@WICKETT

Speaker Deck

Published on Feb 6, 2017

What's Inside That Container?

Containers and config management in the real world

Gareth Rushgrove
Puppet

puppet

share

What's Inside That Container? by Gareth Rushgrove

Published February 6, 2017 in Technology

Gareth Rush...
61 Presentations

Star this Talk 9 Stars

Published in Technology

Stats 2,203 Views

Share

Twitter, Facebook

Embed

Direct Link

Download PDF

OVER 30% OF OFFICIAL IMAGES IN DOCKER HUB CONTAIN HIGH PRIORITY SECURITY VULNERABILITIES

https://banyanops.com/blog/analyzing-docker-hub/

bundler-audit for ruby

GOTO; Amsterdam 2017

@WICKETT

Lynis

https://cisofy.com/lynis/

snyk

serverless dep checks

Docker Bench for Security

script that checks for dozens of common best-practices around deploying Docker containers in production
https://dockerbench.com

Retire.js

http://retirejs.github.io/retire.js/

@webtonull

Lots more...

Instrument your CI system with checks for all the things you inherit

Twistlock
Aqua
Sonatype
BlackDuck

BUILD

Security is a function of Quality

GOTO; Amsterdam 2017

@WICKETT

Vulnerable code in all Languages

Vulnerability percentage class by language

	ASP	Coldfusion	.NET	Java	Perl	PHP	Ruby
Cross-Site Scripting	49	46	35	57	67	56	29
Information Leakage	29	24	44	15	11	17	55
Content Spoofing	5	4	5	8	6	7	3
SQL Injection	8	11	6	1	3	6	-
Cross-Site Request Forgery	2	2	2	4	4	2	-
Insufficient Transport Layer Protection	0.8	1	0.9	1	0.3	4	0.7
Abuse of Functionality	0.3	6	0.3	0.9	0.5	0.2	-
HTTP Response Splitting	0.9	3	0.8	2	0.8	0.3	-
Predictable Resource Location	0.1	0.1	0.0	0.2	0.1	1	6
Brute Force	0.7	0.3	1	2	0.8	1	-
URL Redirector Abuse	0.7	0.4	0.5	1	1	0.9	-
Insufficient Authorization	0.2	0.3	0.5	0.9	1	0.2	0.7
Fingerprinting	0.3	0.1	0.5	0.6	0.3	0.1	0.7
Session Fixation	0.2	0.3	0.2	0.6	0.1	0.3	-
Directory Indexing	-	-	0.0	0.0	-	0.3	

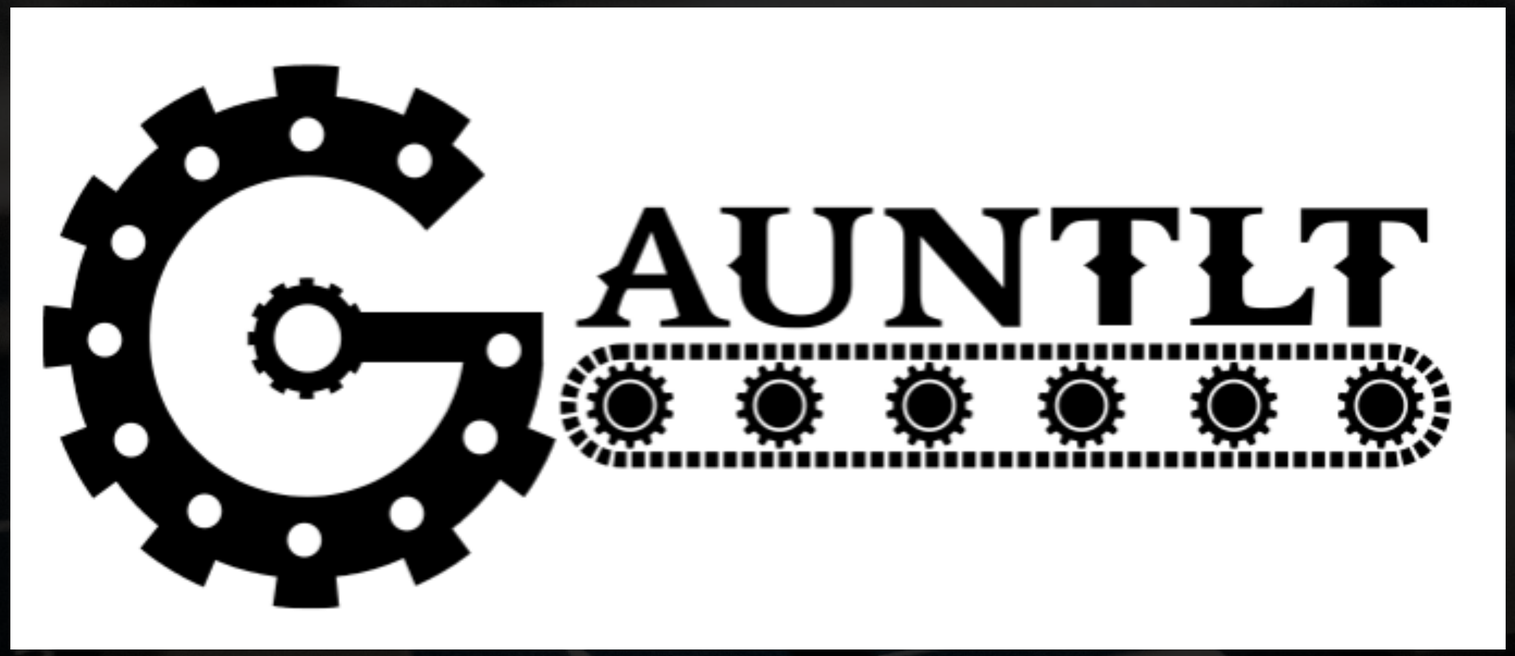
* Limited amount of data available

WhiteHat Security Report (2015)

Security tools are intractably noisy and difficult to use

A method of collaboration was needed for devs, ops and security eng.

There needed to be a new language to span the parties



GOTO; Amsterdam 2017

@WICKETT

Open source, MIT License

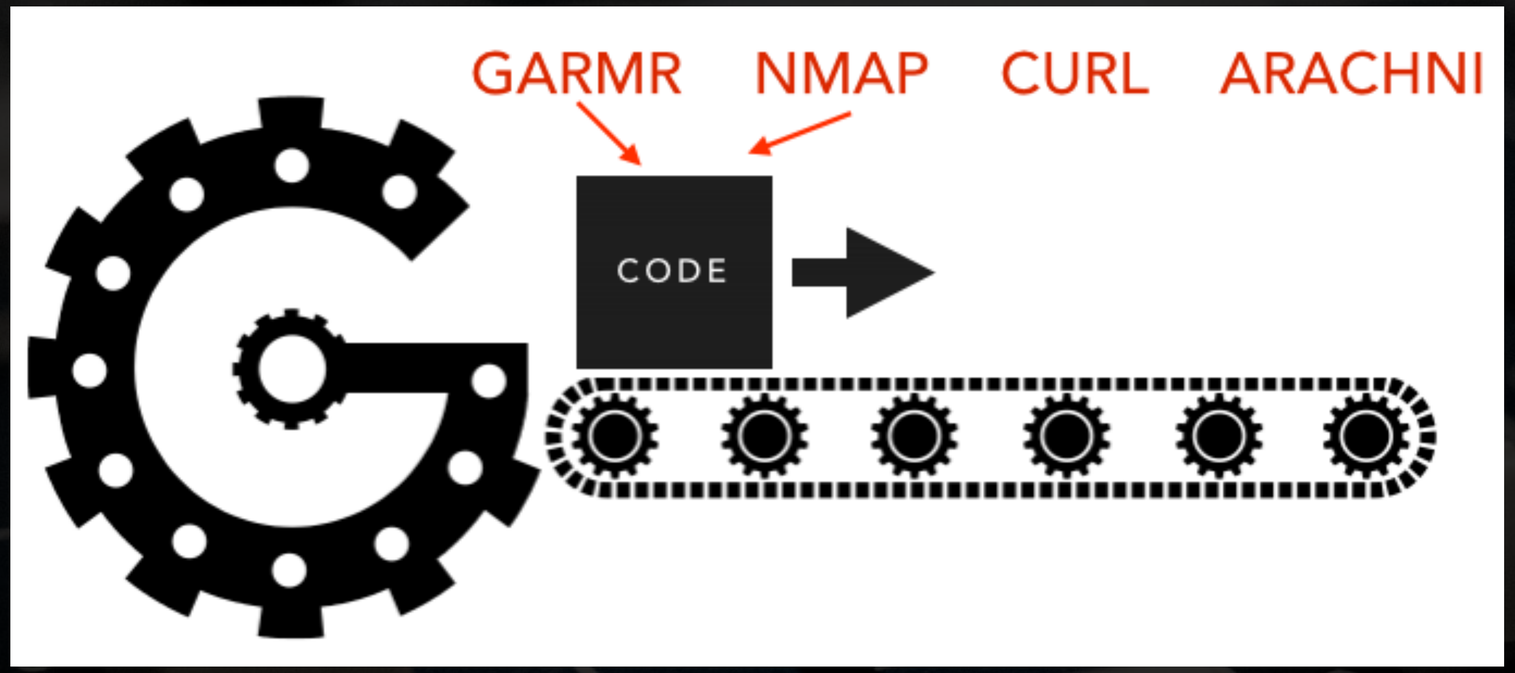
Gauntlt comes with pre-canned steps that hook security testing tools

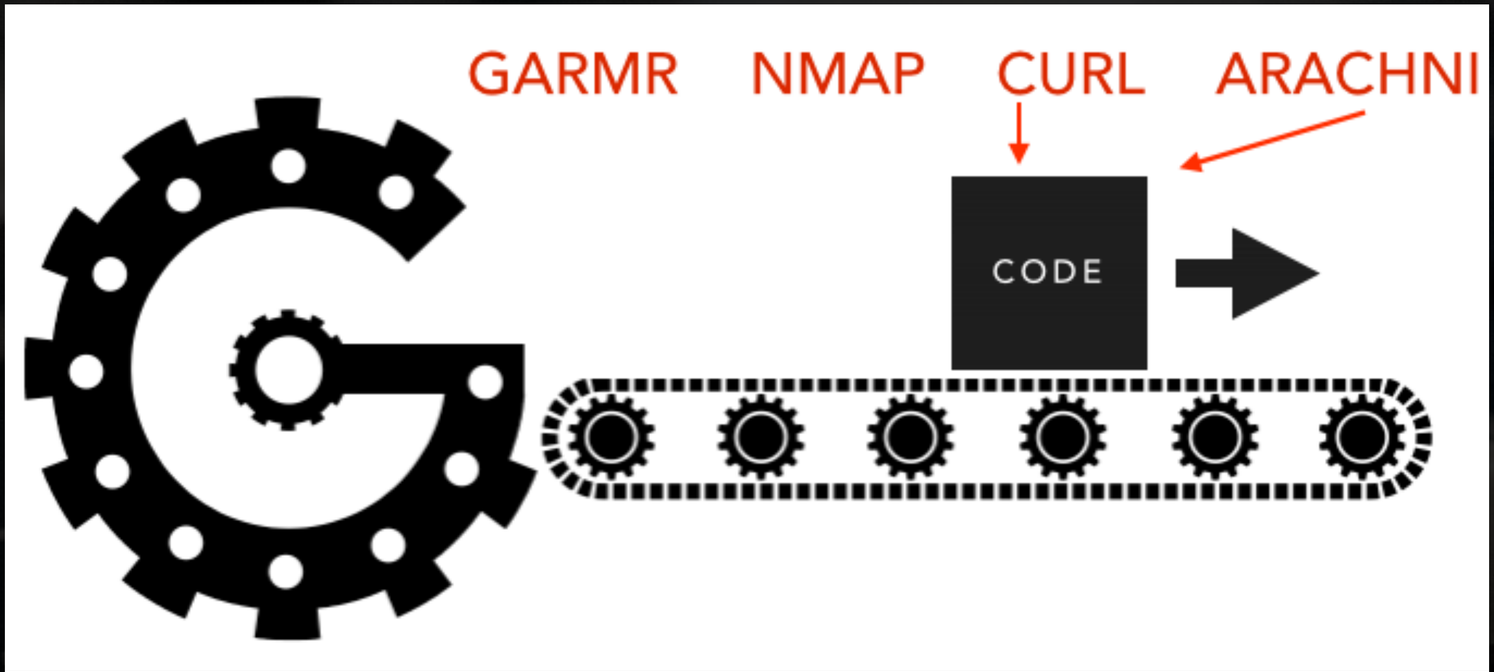
Gauntlt does not install tools

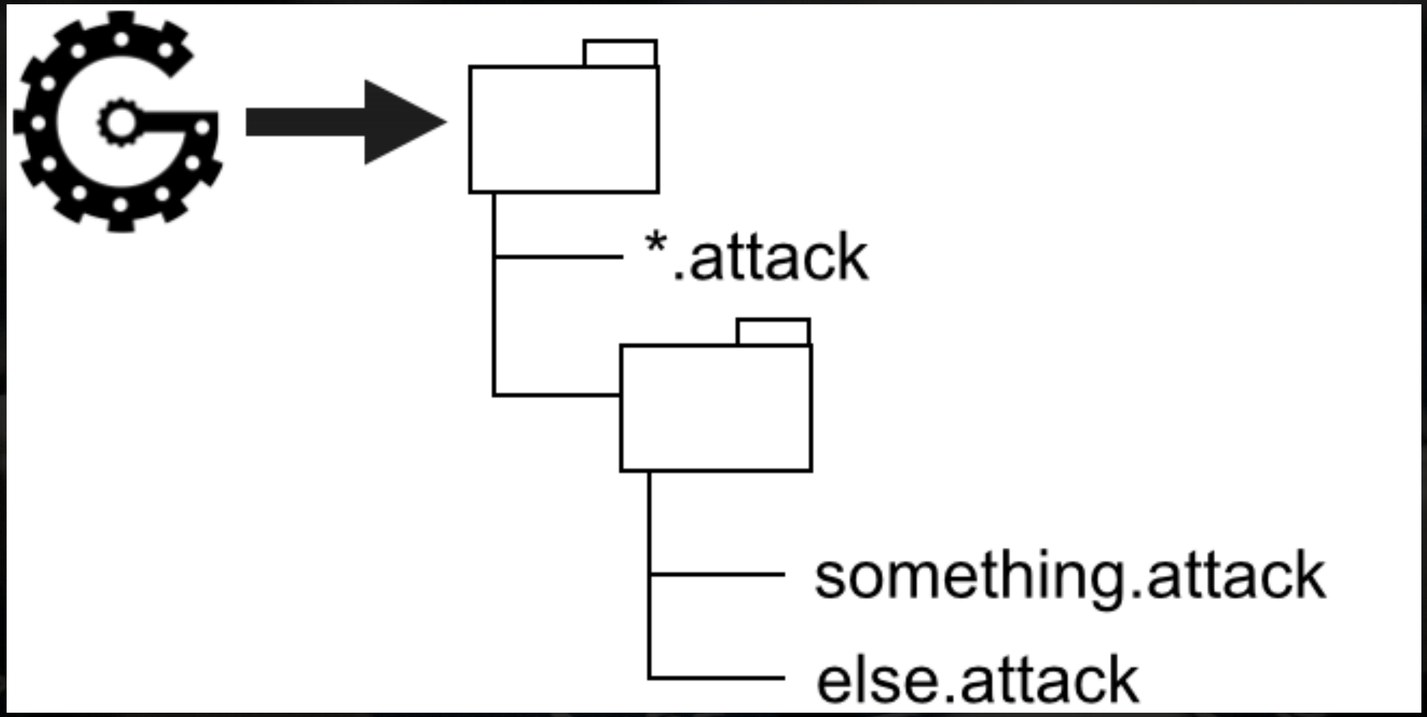
Gauntlt wants to be part of the CI/CD pipeline

Be a good citizen of exit status and stdout/stderr

gauntlt.org


GARMR
NMAP
CURL
ARACHNI
CODE


GARMR
NMAP
CURL
ARACHNI
CODE


*.attack
something.attack
else.attack

```
$ gem install gauntlt

# download example attacks from github
# customize the example attacks
# now you can run gauntlt

$ gauntlt
```

What?

```
@slow @final
Feature: Look for cross site scripting (xss) using arachni
against a URL

Scenario: Using arachni, look for cross site scripting and verify
no issues are found
  Given "arachni" is installed
  And the following profile:
      | name                | value                          |
      | url                 | http://localhost:8008          |
  When I launch an "arachni" attack with:
  """
  arachni –check=xss* <url>
  """
  Then the output should contain "0 issues were detected."
```

Given

When

Then

“We have saved millions of dollars using GauntIt for the largest healthcare industry project.”

- Aaron Rinehart, UnitedHealthCare

http://bit.ly/2s8P1LI

WORKSHOP INCLUDES:

- 8 LABS FOR GAUNTLT
- HOW TO USE GAUNTLT FOR NETWORK CHECKS
- GAUNTLT FOR XSS, SQLI, OTHER APSES
- HANDLING REPORTING
- USING ENV VARS
- CI SYSTEM SETUP

http://bit.ly/2s8P1LI

Gauntlt Demo

This is a demo set of attacks that can be used to demo gauntlt and learn how to implement it. Each directory in `./examples` contains a specific type of attack that you might want to run. Inside each example you will find a README.md which will have a challenge and some hints on how to solve it. We recommend reading that first and then try to create an attack to solve the challenge.

Installation

```
$ git clone https://github.com/secure-pipeline/gauntlt-demo
$ cd ./gauntlt-demo
$ git submodule update --init --recursive
$ bundle
```

Start targets

This includes gruyere and railsgoat as a target to pratice against and in the future we will bundle other services. To start the default targets run the following.

```
$ bundle exec start_services

# For some reason railsgoat doesnt exit cleanly from a Ctl-C with service manager so yo
# will have to stop it manually
# ps -ef | grep rails
# kill -9 <PID>
# Please send a pull request if you know how to fix this
```

You can also run the following to start individual targets which include: railsgoat and gruyere

github.com/gauntlt/gauntlt-demo

Gauntlt Starter Kit

In the Gauntlt Starter Kit, you'll find scripts, examples, and some other great stuff to help you get started with Gauntlt.

How to use

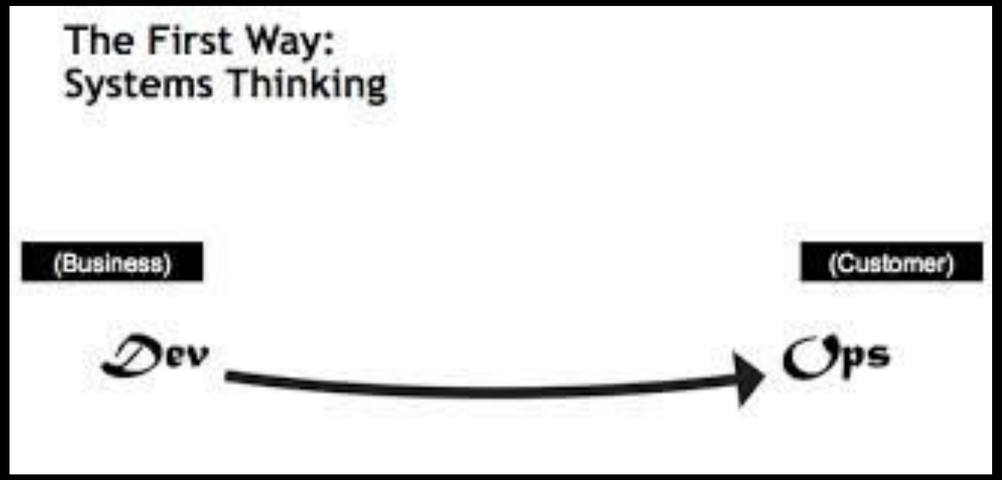
Start with a git clone of `git clone git@github.com:gauntlt/gauntlt-starter-kit` and run the following:

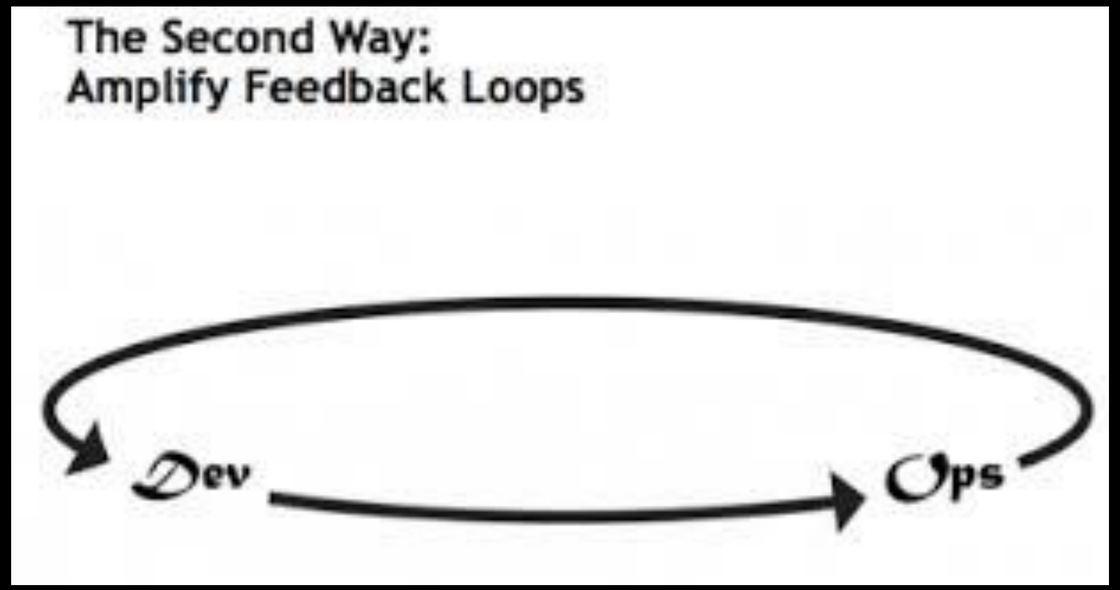
```
$ cd ./gauntlt-starter-kit/vagrant/gauntlt
$ vagrant up
$ vagrant ssh
```

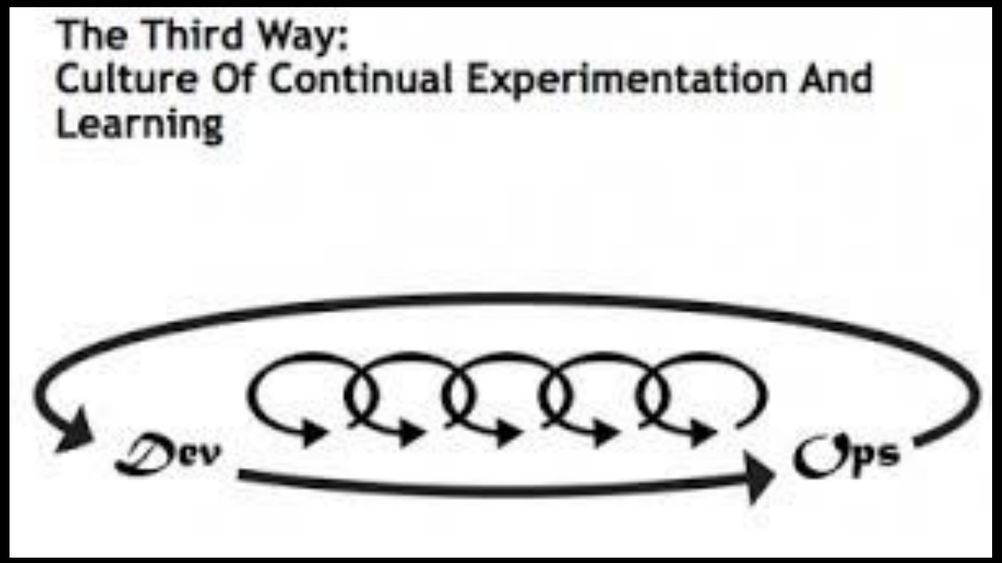
Pre-requisites

- Virtual Box
- Vagrant

github.com/gauntlt/gauntlt-starter-kit







SOURCE: THE THREE WAYS OF DEVOPS, GENE KIM

gauntlt/gauntlt-demo

build passing

this is a demo set of attacks that can be used to get started with gauntlt

Current | Build History | Pull Requests | Branch Summary

Build	51	Commit	a1e38a0 (master)
State	Passed	Compare	5c96e71da2fe...a1e38a0b1a6b
Finished	about 2 hours ago	Author	James Wickett
Duration	5 min 4 sec	Committer	James Wickett
Message	reorganizing these		

```
1   Using worker: worker-linux-10-1.bb.travis-ci.org:travis-linux-1
2
3   $ git clone --depth=50 --branch=master git://github.com/gauntlt/gauntlt-demo.git gauntlt/gauntlt-demo        git.1
11  $ cd gauntlt/gauntlt-demo
12  $ git checkout -qf a1e38a0b1a6b896265af8e21708f34ebfa1087bc                                               git.3
13  $ git submodule init                                                                                       git.4
18  $ git submodule update                                                                                     git.5
50  $ rvm use 1.9.3 --install --binary --fuzzy
51  Using /home/travis/.rvm/gems/ruby-1.9.3-p484
52  $ export BUNDLE_GEMFILE=$PWD/Gemfile
53  $ ruby --version
54  ruby 1.9.3p484 (2013-11-22 revision 43786) [x86_64-linux]
55  $ rvm --version
56
57  rvm 1.25.14 (version) by Wayne E. Seguin <wayneeseguin@gmail.com>, Michal Papis <mpapis@gmail.com> [https://rvm.io/]
58
59  $ gem --version
60  2.2.2
61  $ bundle --version
62  Bundler version 1.5.3
63  Applying fix for NPM certificates
64  $ git submodule update --init --recursive                                                                  before_install
65  $ bundle install                                                                                           install
133 $ sudo apt-get install nmap                                                                                before_script.1
161 $ sudo apt-get install wget                                                                                before_script.2
167 $ sudo apt-get install libcurl4-openssl-dev                                                               before_script.3
173 $ pwd                                                                                                      before_script.4
175 $ export SSLYZE_PATH="/home/travis/build/gauntlt/gauntlt-demo/vendor/sslyze/sslyze.py"                     before_script.5
176 $ export SQLMAP_PATH="/home/travis/build/gauntlt/gauntlt-demo/vendor/sqlmap/sqlmap.py"                     before_script.6
177 $ cd vendor/Garmr && sudo python setup.py install && cd ../..                                              before_script.7
256 $ cd vendor && wget http://downloads.sourceforge.net/project/dirb/dirb/2.03/dirb203.tar.gz && tar xvfz dirb203.tar.gz && cd dirb &&  before_script.8
```

```
$ export DIRB_WORDLISTS="/home/travis/build/gauntlt/gauntlt/vendor/dirb/wordlists"
$ bundle exec rake
cd ./vendor/gruyere && ./manual_launch.sh && cd ../..
Gruyere started at 20097 PID and is available at localhost:8008
cd ./examples && bundle exec gauntlt --tags @final && cd ..
Using the default profile...
@final
Feature: hello world with gauntlt using the generic command line attack

  Scenario:                                # ./hello_world/hello_world.attack:3
    When I launch a "generic" attack with: # gauntlt-1.0.8/lib/gauntlt/attack_adapters/generic.rb:1
      """
      cat /etc/passwd
      """
    Then the output should contain:        # aruba-0.5.4/lib/aruba/cucumber.rb:147
      """
      root
      """

@slow @final
Feature: Look for cross site scripting (xss) using arachni against a URL

  Scenario: Using arachni, look for cross site scripting and verify no issues are found # ./arachni-xss/final_arachni-xss.attack:4
    Given "arachni" is installed                                                         # gauntlt-1.0.8/lib/gauntlt/attack_adapters/arachni.rb:1
    And the following profile:                                                           # gauntlt-1.0.8/lib/gauntlt/attack_adapters/gauntlt.rb:9
      | name | value                |
      | url  | http://localhost:8008 |
    When I launch an "arachni" attack with:                                              # gauntlt-1.0.8/lib/gauntlt/attack_adapters/arachni.rb:5
      """
      arachni --modules=xss --depth=1 --link-count=10 --auto-redundant=2 <url>
      """
    Then the output should contain "0 issues were detected."                             # aruba-0.5.4/lib/aruba/cucumber.rb:131

  Scenario: Using arachni, look for cross site scripting and verify no issues are found # ./arachni-xss/final_arachni-xss.attack:15
    Given "arachni" is installed                                                         # gauntlt-1.0.8/lib/gauntlt/attack_adapters/arachni.rb:1
    And the following profile:                                                           # gauntlt-1.0.8/lib/gauntlt/attack_adapters/gauntlt.rb:9
      | name | value                |
      | url  | http://localhost:8008 |
Running a arachni-simple_xss attack. This attack has this description:
 This is a scan for cross site scripting (xss) that only runs the base xss module in arachni.  The scan only crawls one level deep which makes it
faster.  For more depth, run the gauntlt attack alias 'arachni-simple_xss_with_depth' and specifiy depth.
The arachni-simple_xss attack requires the following to be set in the profile:
 ["<url>"]
    When I launch an "arachni-simple_xss" attack                                         # gauntlt-1.0.8/lib/gauntlt/attack_adapters/arachni.rb:9
    Then the output should contain "0 issues were detected."                             # aruba-0.5.4/lib/aruba/cucumber.rb:131
```

Most teams use Gauntlt in Docker containers

https://github.com/gauntlt/gauntlt-docker

ZAP

https://github.com/zaproxy/zaproxy

Static Code Analysis e.g. Brakeman

GOTO; Amsterdam 2017

@WICKETT

OPERATE

Configuration and Runtime

Configuration

Chef Inspec

Audit and CIS benchmarks on machines

GOTO; Amsterdam 2017

@WICKETT

evident.io
Threatstack
AlienVault

Runtime


VAYAGIF.COM

Runtime is arguably the most important place to instrument

Are you under attack?

Where?

ModSecurity pumped to ELK

GOTO; Amsterdam 2017

@WICKETT

RASP and NGWAF and Web Protection Platform

GOTO; Amsterdam 2017

@WICKETT

This one is the best! [n.b. I work here, but it really is]

Signal Sciences
Immunio
Contrast

DETECT WHAT MATTERS

- ACCOUNT TAKEOVER ATTEMPTS
- AREAS OF THE SITE UNDER ATTACK
- MOST LIKELY VECTORS OF ATTACK
- BUSINESS LOGIC FLOWS

Runtime instrumentation also helps prioritize backlog

Bug Bounties

GOTO; Amsterdam 2017

@WICKETT

HackerOne
BugCrowd

GOTO; Amsterdam 2017

@WICKETT

A SIDE JOURNEY ON COMPLIANCE

GOTO; Amsterdam 2017

@WICKETT

Separation of Duties Considered Harmful

Win over the auditors and lawyers with the DevOps Audit Defense Toolkit

https://cdn2.hubspot.net/hubfs/228391/Corporate/DevOps_Audit_Defense_Toolkit_v1.0.pdf

3 LESSONS LEARNED ALONG THE JOURNEY

GOTO; Amsterdam 2017

@WICKETT

Security is not a binary event; embrace feedback loops

Attack Driven Defense beats Compliance Driven Defense

GOTO; Amsterdam 2017

@WICKETT

Don’t be a blocker, be an enabler of the business

SUMMARY

- SECURITY IS STILL MAKING THE JOURNEY OF DEVOPS
- SECURITY SEES NEW OPPORTUNITIES TO AUTOMATE AND ADD VALUE
- THE DELIVERY PIPELINE EXTENDS FARTHER THAN WE USUALLY CONSIDER

MORE SUMMARY

- CULTURE AND TOOLING NEED TO ALIGN FOR US TO MAKE THIS WORK
- COVERAGE OF SECURITY TOOLS FOR THREE PIPELINE AREAS: INHERIT, BUILD AND RUNTIME
- ADVICE FOR DEALING WITH THE AUDITORS AND OTHER BLOCKERS

Want the slides?

james@signalsciences.com

Questions?