

How to effect change in the Epistemological Wasteland of Application Security

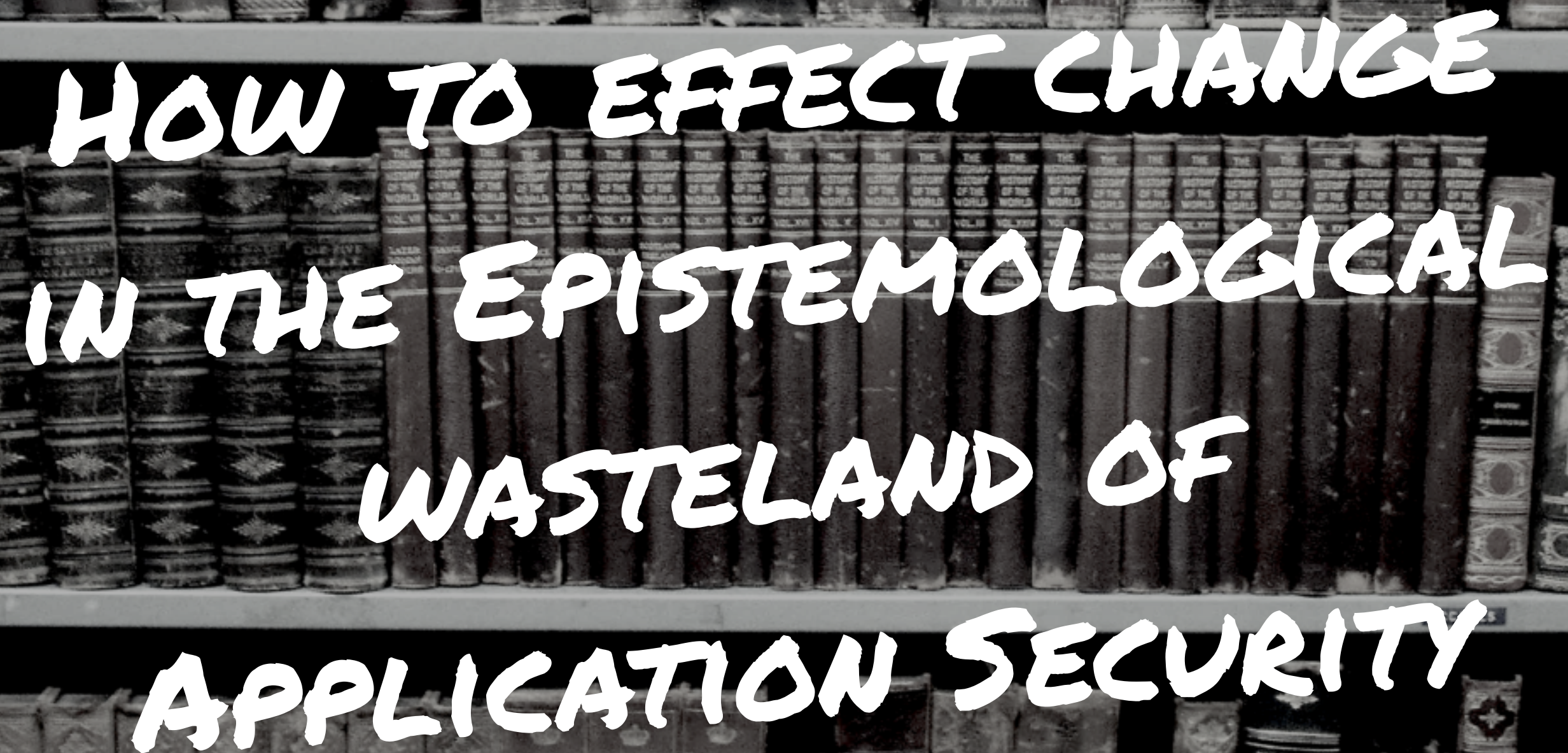
James Wickett





Click 'engage' to rate session.

Rate **12** sessions to get the supercool GOTO reward



HOW TO EFFECT CHANGE IN THE EPISTEMOLOGICAL WASTELAND OF APPLICATION SECURITY

- @WICKETT

JAMES WICKETT

SR. ENGINEER, SIGNAL SCIENCES

AUSTIN, TX

HANDS-ON GAUNTLT BOOK

DEVOPS DAYS GLOBAL ORGANIZER

LASCON ORGANIZER



@WICKETT

#RUGGEDDEVOPS



Application Security Monitoring and Instrumentation

Application Security you can use!

An approach that integrates with devops organizations

Productizing the Etsy security approach



Make security visible.

Prioritize your defensive efforts where your applications are actually targeted.

[LEARN MORE](#)

[REQUEST MORE INFO](#)

signalsciences.com

SUMMARY


Software development has been a constant experiment in how we know anything

Application Security abdicated runtime responsibility and effectively abdicated development responsibility through incoherent philosophical approaches and fostering organizational silos

DevOps is here to stay, and security can actually be a part of it

Ops found a way to add value, security needs to find that same path

There are three ways we can add value: at development, at deploy, at runtime



A STUDY IN HOW WE KNOW ANYTHING IN APPLICATION SECURITY

SPOILER ALERT:
WE DON'T!

ONCE UPON A TIME...

EPISTEMOLOGICAL PROBLEM OF SOFTWARE DEVELOPMENT

WE OPTIMIZE FOR THE
PROBABLE

UNIT TESTING

@WICKETT

#RUGGEDDEVOPS

INTEGRATION TESTING

HAPPY PATH ENGINEERING

@WICKETT

#RUGGEDDEVOPS

WE ALSO OPTIMIZE
FOR THE POSSIBLE

OVER ENGINEERING

@WICKETT

#RUGGEDDEVOPS

THE SCALING ALGO
THAT NEVER GOT USED...

THERE IS TOO MUCH TO
CHOOSE FROM IN THE
REALM OF POSSIBLE

ACTUALLY, WE OPTIMIZE FOR
THE PERCEIVED PROBABLE

HOW DO WE KNOW
WHAT TO CREATE?

THIS IS THE PROBLEM

EPISTEMOLOGICAL PROBLEM OF SOFTWARE DEVELOPMENT

WE GATHER DATA AND
RHETORIC TO SUPPORT
OUR THEORIES

THERE ARE 3 MAJOR
ARCS IN THE HISTORY OF
SOFTWARE DEVELOPMENT



FIRST ARC: AGILE

@WICKETT

#RUGGEDDEVOPS

AGILE AVOIDS THE
PROBLEM

AGILE REMINDS THAT
WE DONT KNOW WHAT
WE ARE BUILDING



@WICKETT

#RUGGEDDEVOPS

BEHAVIOR DRIVEN DEVELOPMENT

@WICKETT

#RUGGEDDEVOPS

**BDD = AGILE +
FEEDBACK**

Behavior Driven Development is a second-generation, outside-in, pull-based, multiple-stakeholder, multiple-scale, high-automation, agile methodology. It describes a cycle of interactions with well-defined outputs, resulting in the delivery of working, tested software that matters.

Dan North , 2009



AMPLIFY FEEDBACK LOOP

@WICKETT

#RUGGEDDEVOPS

AGILE EMPHASIZES
FEEDBACK TO DEVELOPERS
FROM THEIR OVERLORDS AND
SOMETIMES EVEN CUSTOMERS

TLDR;
RAPID ITERATIONS WIN



AGILE IS
OUR GUIDING
LIGHT

@WICKETT

#RUGGEDDEVOPS

THE WORLD HAS
CHANGED SINCE AGILE



WE DON'T SELL
CD'S ANYMORE

@WICKETT

#RUGGEDDEVOPS

SOFTWARE AS A SERVICE

THE LAST FIFTEEN YEARS HAVE
BROUGHT A COMPLETE CHANGE IN
OUR DELIVERY CADENCE,
DISTRIBUTION MECHANISMS AND
REVENUE MODELS



SECOND ARC: DEVOPS

@WICKETT

#RUGGEDDEVOPS

DEVOPS IS THE APPLICATION OF AGILE METHODOLOGY TO SYSTEM ADMINISTRATION

– THE PRACTICE OF CLOUD SYSTEM ADMINISTRATION BOOK



AGILE INFRASTRUCTURE

10 deploys per day

Dev & ops cooperation at Flickr

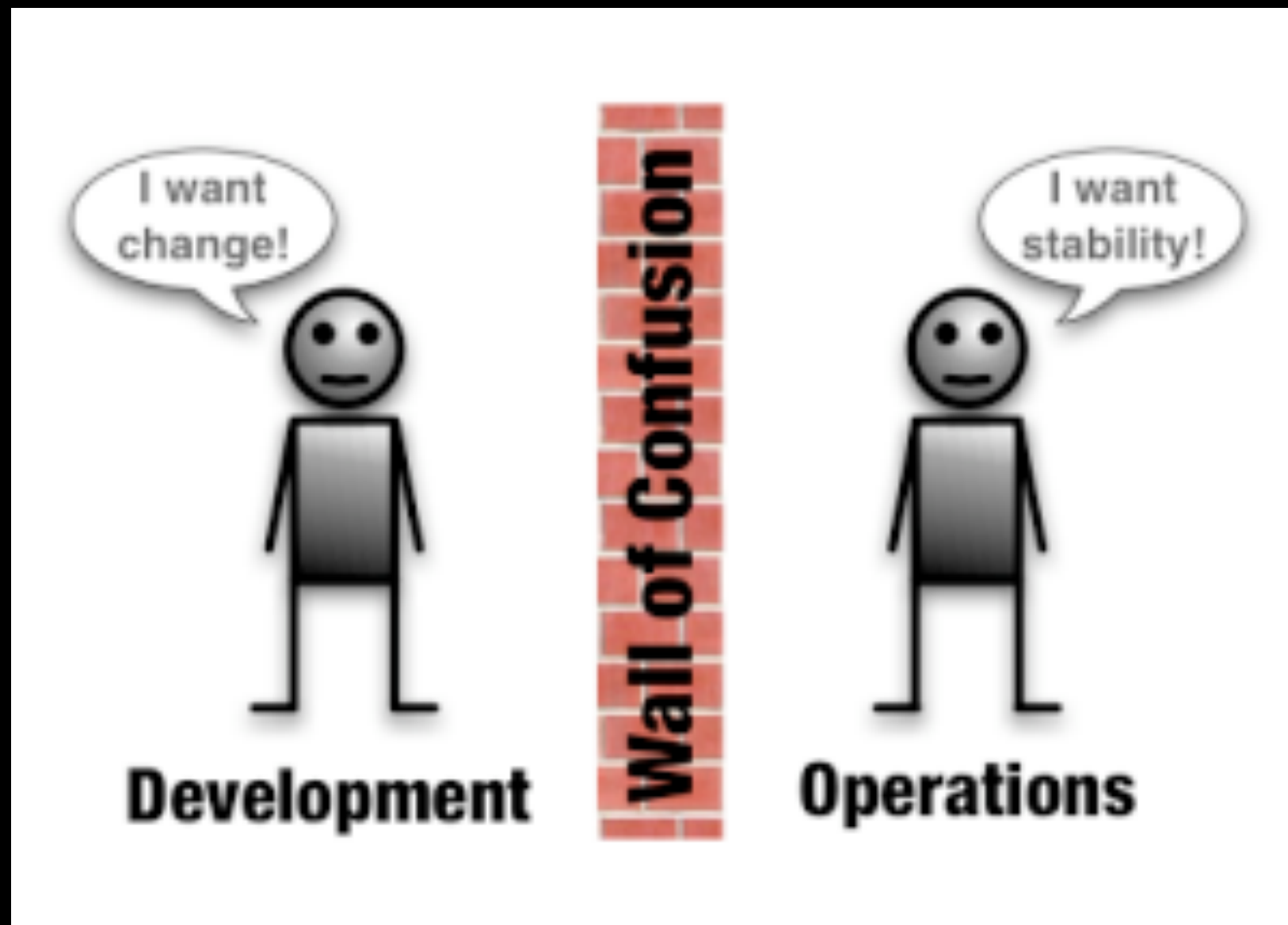
John Allspaw & Paul Hammond
Velocity 2009

<http://www.slideshare.net/jallspaw/10-deploys-per-day-dev-and-ops-cooperation-at-flickr>

LESS WIP
LESS TECHNICAL DEBT

CUSTOMERS ACTUALLY USING
THE FEATURE WHILE THE
DEVELOPER IS WORKING ON IT

**GREAT SIDE EFFECT:
PRODUCES HAPPY DEVELOPERS**





@WICKETT

#RUGGEDDEVOPS

DEVOPS REALIZED THAT OPS
DOESN'T KNOW WHAT DEVS
KNOW AND VICE VERSA

DEV : OPS

10 : 1

DEVOPS IS AN EPISTEMOLOGICAL
BREAKTHROUGH JOINING PEOPLE
AROUND A COMMON PROBLEM

CULTURE IS THE MOST
IMPORTANT ASPECT TO DEVOPS
SUCCEEDING IN THE ENTERPRISE
- PATRICK DEBOIS

CULTURE IS SHAPED IN
PART BY VALUES



@WICKETT

#RUGGEDDEVOPS

MUTUAL UNDERSTANDING

SHARED LANGUAGE

SHARED VIEWS

COLLABORATIVE TOOLING

**DEVOPS IS THE INEVITABLE RESULT OF NEEDING
TO DO EFFICIENT OPERATIONS IN A [DISTRIBUTED
COMPUTING AND CLOUD] ENVIRONMENT.
– TOM LIMONCELLI**



<https://puppetlabs.com/sites/default/files/2015-state-of-devops-report.pdf>

@WICKETT

#RUGGEDDEVOPS

TLDR;

HIGH-PERFORMING IT
ORGANIZATIONS EXPERIENCE 60X
FEWER FAILURES AND RECOVER FROM
FAILURE 168X FASTER THAN THEIR
LOWER-PERFORMING PEERS. THEY
ALSO DEPLOY 30X MORE FREQUENTLY
WITH 200X SHORTER LEAD TIMES.

CULTURE
AUTOMATION
MEASUREMENT
SHARING

- @DAMONEDWARDS, @BOTCHAGALUPE

DEVOPS GONE WRONG



@WICKETT

#RUGGEDDEVOPS

**“THAT THE WORD #DEVOPS GETS REDUCED
TO TECHNOLOGY IS A MANIFESTATION OF
HOW BADLY WE NEED A CULTURAL SHIFT”
– @PATRICKDEBOIS**

<http://www.slideshare.net/cm6051/london-devops-31-5-years-of-devops>

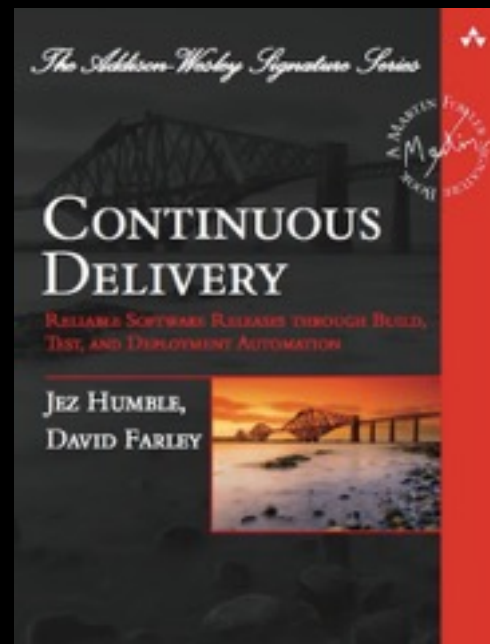


THIRD ARC: CONTINUOUS DELIVERY

@WICKETT

#RUGGEDDEVOPS

CONTINUOUS DELIVERY IS NOT
MERELY HOW OFTEN YOU
DELIVER BUT HOW LITTLE
YOU CAN DELIVER AT A TIME



@WICKETT

#RUGGEDDEVOPS



**DELIVERY
PIPELINES
ARE RAD!**

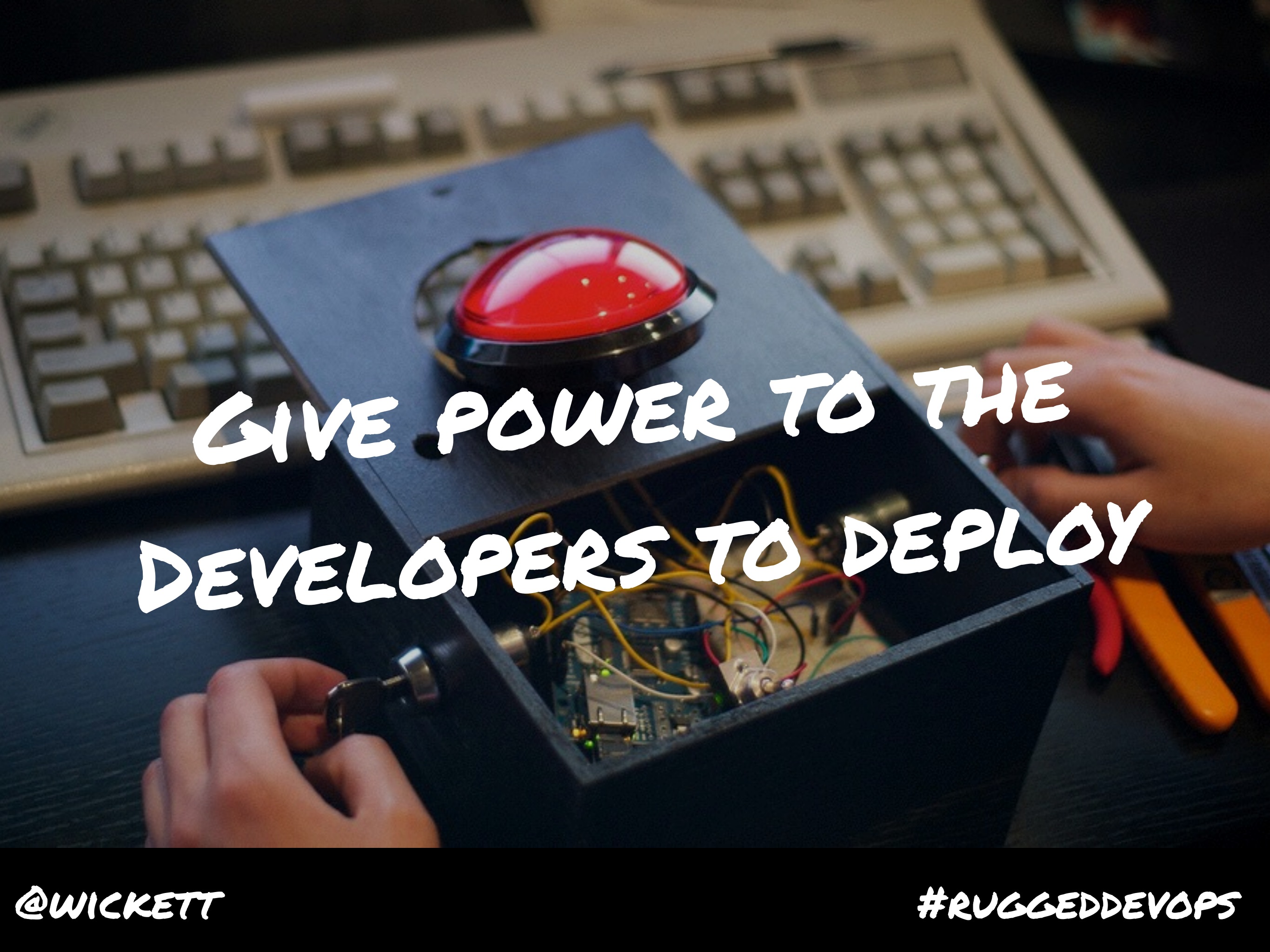
@WICKETT

#RUGGEDDEVOPS

BATCH SIZE OF 1



SEPARATION OF DUTIES
CONSIDERED HARMFUL

A close-up photograph of a person's hands working on a custom-built electronic device. The device is housed in a dark, rectangular enclosure. On top of the enclosure is a large, prominent red push-button. The front panel of the enclosure is open, revealing the internal components, which include a printed circuit board (PCB) with various electronic components and a complex network of colorful jumper wires. One hand is visible on the left, holding a small metal component, while another hand is on the right, holding a pair of orange-handled pliers. The background is slightly blurred, showing a computer keyboard and a dark desk surface.

GIVE POWER TO THE
DEVELOPERS TO DEPLOY

@WICKETT

#RUGGEDDEVOPS

REDUCE CODE LATENCY
INCREASE CODE VELOCITY

3 ARCS:
AGILE
DEVOPS
CONTINUOUS DELIVERY

THE NEXT ARC: SECURITY RUGGED

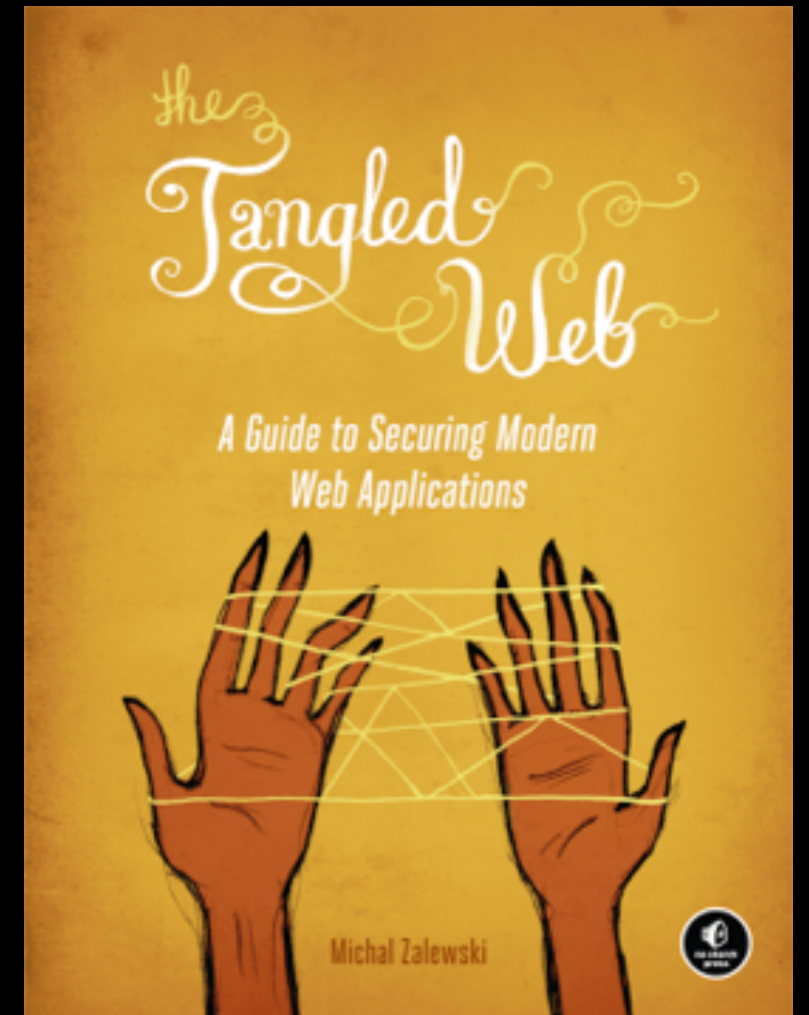
"...THOSE STUPID DEVELOPERS"
- SECURITY PERSON

"SECURITY PREFERS A SYSTEM
POWERED OFF AND UNPLUGGED"
- DEVELOPER

CULTURAL UNREST
WITH SECURITY IN
MOST ORGANIZATIONS

COMPLIANCE DRIVEN CULTURE

“[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”



SECURITY IS WHERE OPS
WAS 5 YEARS AGO...

DEV : OPS : SEC

100 : 10 : 1

UNDERSTAFFING MEANS
NO ONE THINKS SECURITY
HELPS THE BUSINESS WIN

DEVOPS CHANGED THAT
FOR OPS, SECURITY CAN
CHANGE TOO



**NETFLIX
DEMONSTRATED
THAT PEOPLE
CARE ABOUT
RESILIENCY**



**DOUBLE
ZIPPER**

30 BAGS • 7 IN X 8 IN (17.8 cm X 20.3 cm)

**New &
Improved**

JUMBO SANDWICH

**30
BAGS**

7" x 8"

**MADE IN
USA**

INNATELY, WE ALL CARE

@WICKETT

#RUGGEDDEVOPS



Rugged Software Development

Joshua Corman, David Rice, Jeff Williams
2010

RUGGED SOFTWARE MOVEMENT

@WICKETT

#RUGGEDDEVOPS

#RUGGEDDEVOPS

Put Your Robots to Work: Security Automation at Twitter



Speakers: Justin Collins, Security Engineer, Twitter
Neil Matatall, Information Security Engineer, Twitter
Alex Smolen, Security Engineer, Twitter



38:22



<https://vimeo.com/54250716>

@WICKETT

#RUGGEDDEVOPS

O'REILLY®

Velocity

Web Performance
and Operations

CONFERENCE

📍 NEW YORK, NEW YORK

📅 OCTOBER 14-16, 2013

VELOCITYCONF.COM

#VELOCITYCONF

Delivering Security: Faster, Better, Cheaper

Zane Lackey,
Etsy

Dan Kaminsky,
dankaminsky.com

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

@WICKETT

#RUGGEDDEVOPS

SECURITY'S WAY FORWARD IS TO
HELP DEVELOPERS AND HELP
OPERATIONS

START THERE

LET'S REVIEW SECURITY'S
APPROACH THUS FAR

BADIDEA #1
APPLICATIONS CAN'T BE
DEFENDED—WEB APP
FIREWALLS SUCK!
LETS DO DEVELOPER TRAINING





THEY SEE ME ROLLIN'
THEY PATCHIN'

@WICKETT

#RUGGEDDEVOPS

AWARENESS CAMPAIGN

OWASP TOP TEN

WE ABANDONED KNOWING
ANYTHING USEFUL ABOUT
THE RUNTIME

INSTEAD ADD DEFENSE
BASED ON BEHAVIORS

BADIDEA #2

DEVELOPERS CAN'T FIGURE IT OUT.
LETS SCAN FOR VULNERABILITIES
INSTEAD


"HERE IS A 400 PAGE PDF OF
OUR FINDINGS TO PROVE YOUR
DEVELOPERS DON'T GET IT!"
- THE PEN TESTER

EVEN WITH THE EMPHASIS
ON APPSEC TRAINING, IN
PRACTICE WE MADE IT A
DARK ART

INTEGRATED RUGGED
TESTING SHOULD SIT
INSIDE THE PIPELINE

BADIDEA #3

WITH THE NEW ALIGNMENT
TO VULNERABILITY SCANNING,
THERE IS A TENDENCY TO FIX
THE LOW-HANGING FRUIT



What if when we swat flies,

We're killing only slow ones...

**So there's only fast ones to
breed?**

WE STILL DON'T KNOW
WHO IS ATTACKING US

WE STILL DON'T
ACTUALLY KNOW WHAT
THEY ARE ATTACKING

REAL THREATS GO UNKNOWN
SO DEVELOPERS FIX WHAT THE
AUTOMATED TOOLING DETECTED
AT A CERTAIN POINT IN TIME

ADD APPLICATION
SECURITY TELEMETRY

BADIDEA #4

PUT IN TOOLING THAT NO
ONE OUTSIDE OF SECURITY
CAN UNDERSTAND

USUALLY IN THE NAME
OF COMPLIANCE

"GET A WEB APP FIREWALL
DUDE!"

- PCI-DSS REQ 6.6



@WICKETT

#RUGGEDDEVOPS

CHOOSE YOUR OWN
ADVENTURE...

SMALLEST POSSIBLE
SOLUTION YOU CAN
CONSIDER A WAF...

OUR CDN ADDED
MODSECURITY RULESET
HUZZAH!

AN APPLIANCE THAT
BLOCKS ALL THE THINGS

AND NOW YOU WONDER
WHY NO ONE EATS LUNCH
WITH YOU ANYMORE

"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."

- A WHITEPAPER FROM A WAF VENDOR



@WICKETT

#RUGGEDDEVOPS

OK, SECURITY HAS TO CHANGE...
HOW DO WE ADD VALUE
ALREADY?

TWO WAYS!

ADD VALUE TO DEVS

ADD VALUE TO OPS

PRAY THAT SOMEONE
NOTICES

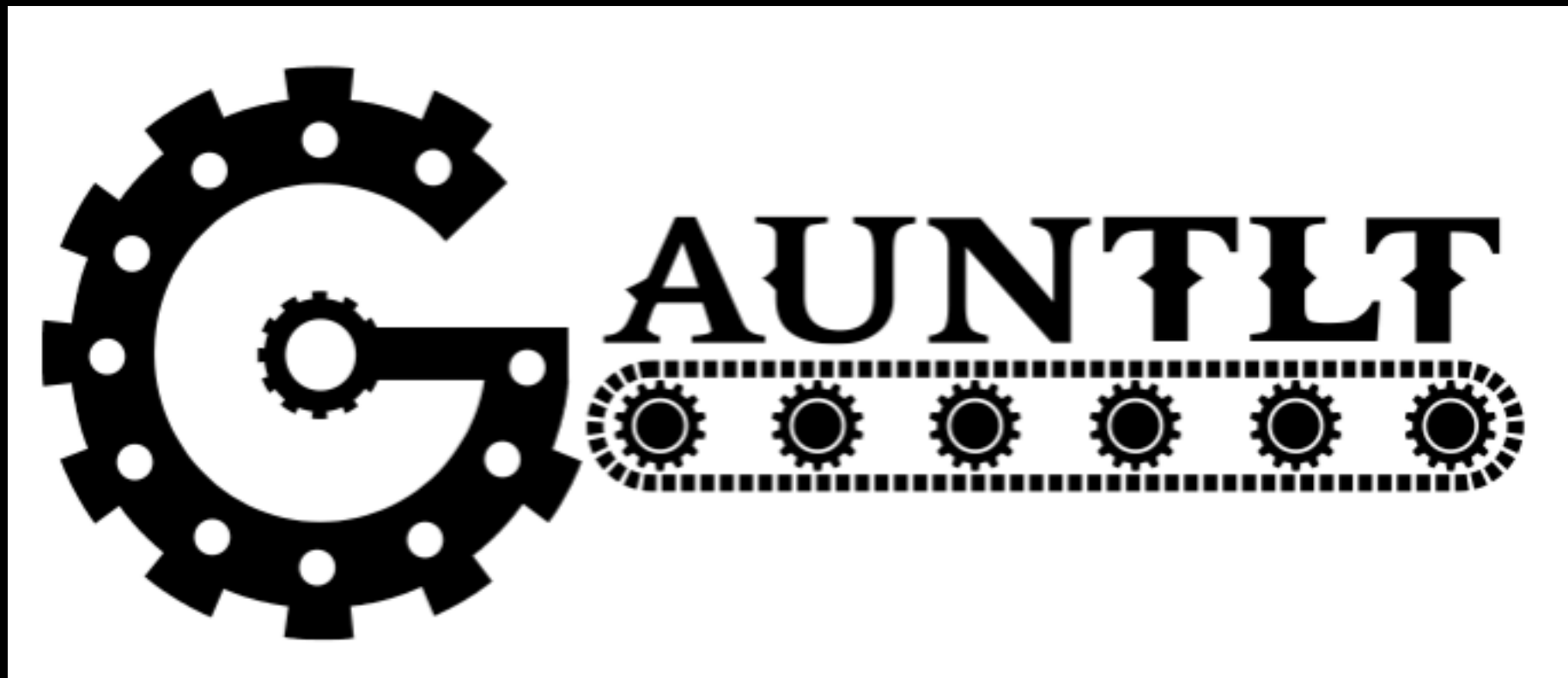


@WICKETT

#RUGGEDDEVOPS

PRO-TIP #1
AUTOMATE SECURITY TOOLING
TO RUN IN TESTING

START WITH ADDING JUST ONE
TEST FOR XSS ON A FEW PAGES
IN YOUR APP



@WICKETT

#RUGGEDDEVOPS

GAUNTLT AUTOMATES SECURITY TOOLS

GAUNTLT

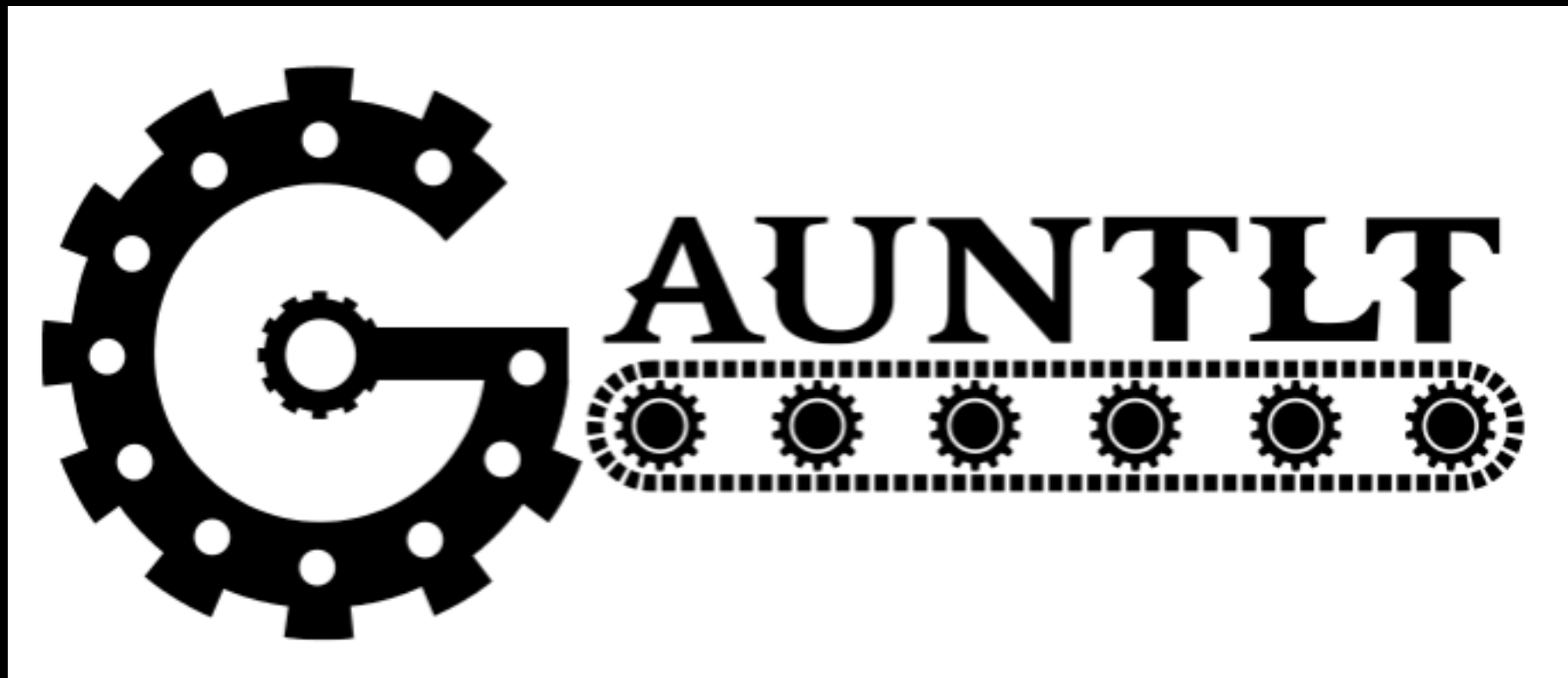
Open source, MIT License

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

GauntIt does not install tools

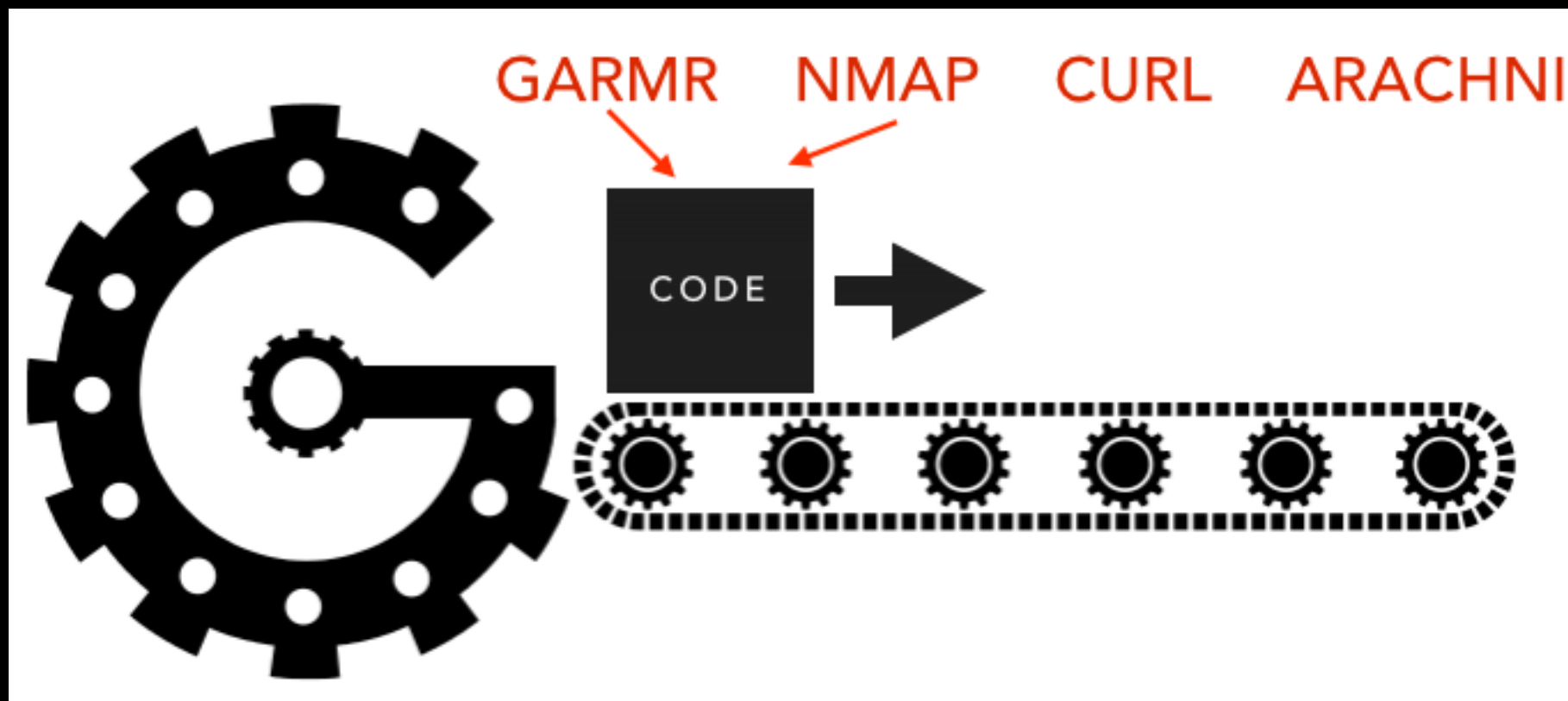
GauntIt wants to be part of the CI/CD pipeline

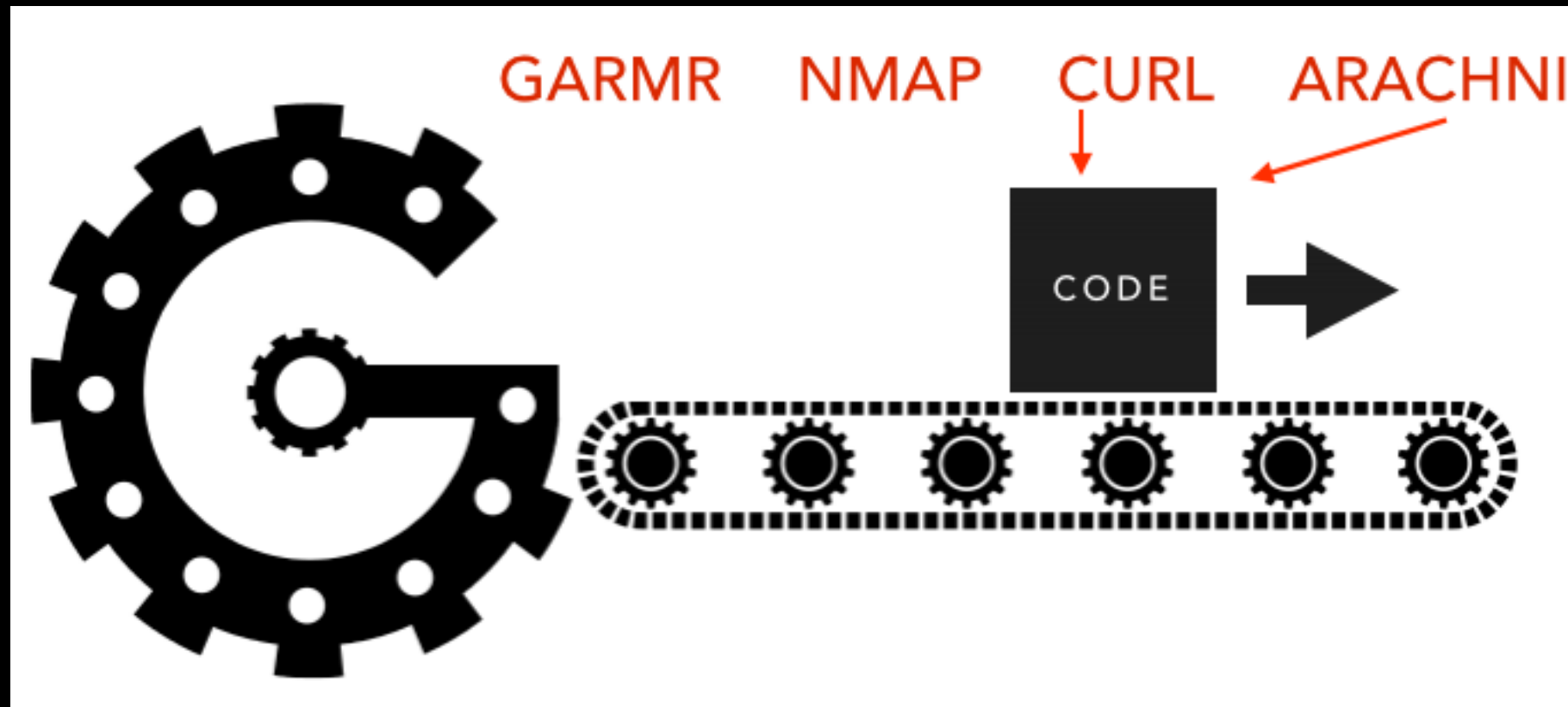
Be a good citizen of exit status and stdout/stderr

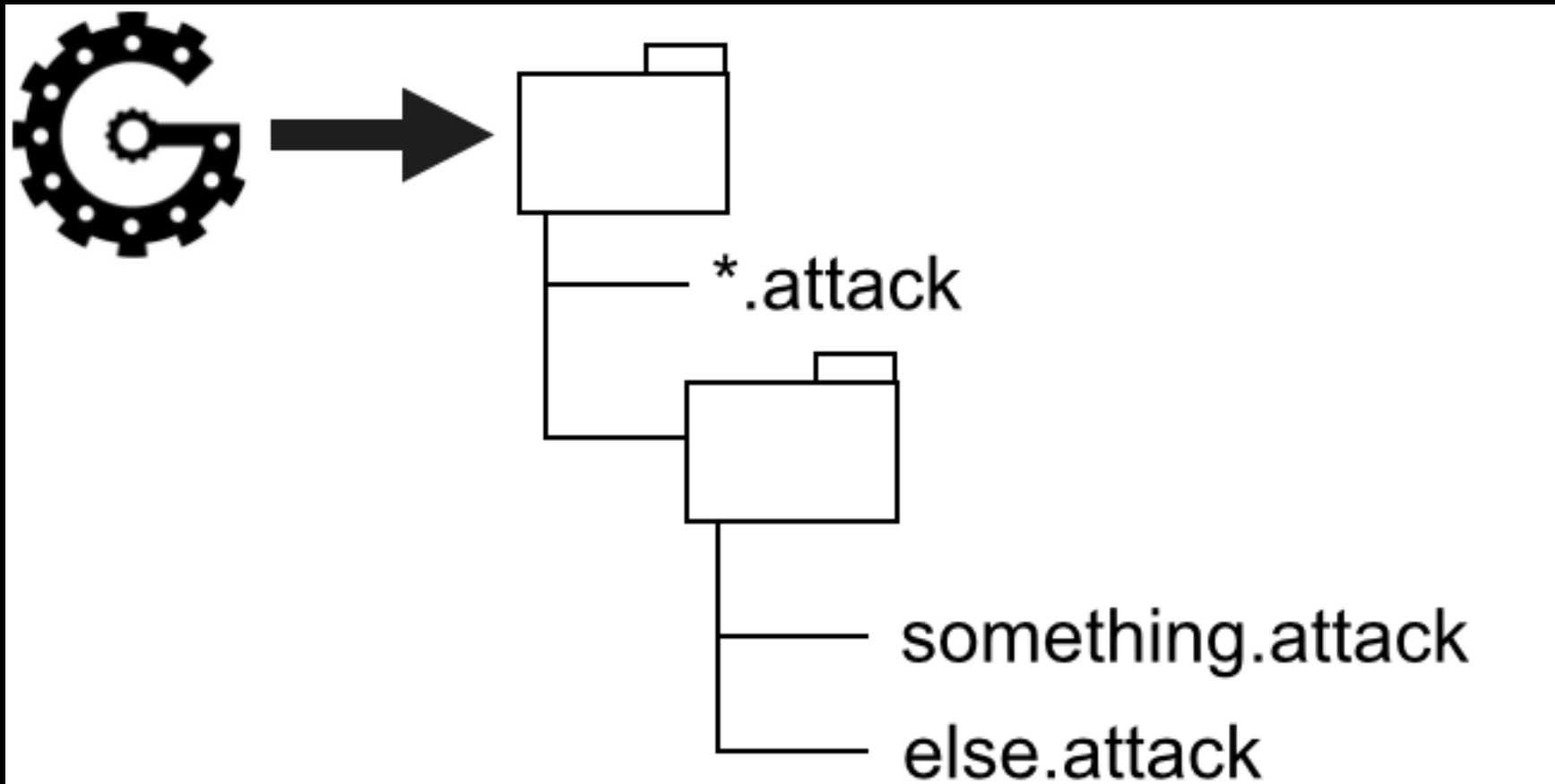


@WICKETT

#RUGGEDDEVOPS







Feature: nmap attacks for example.com

Given

Background:

Given "nmap" is installed
And the following profile:

name	value	
hostname	example.com	

Scenario: Verify server is open on expected ports

When

When I launch an "nmap" attack with:

~~~~~

nmap -F <hostname>

~~~~~

Then

Then the output should contain:

~~~~~

80/tcp open http

~~~~~

Scenario: Verify that there are no unexpected ports open

When

When I launch an "nmap" attack with:

~~~~~

nmap -F <hostname>

~~~~~

Then

Then the output should not contain:

~~~~~

25/tcp

~~~~~

HERE'S AN XSS ATTACK
YOU CAN USE

@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 --modules=xss --depth=1 --link-count=10 --auto-redundant=2 <url>

"""

Then the output should contain "0 issues were detected."



<http://theagileadmin.com/2015/06/09/pragmatic-security-and-rugged-devops/>

@WICKETT

#RUGGEDDEVOPS

github.com/gauntlt/gauntlt-demo

@WICKETT

#RUGGEDDEVOPS

HANDS-ON GAUNTLT BOOK FOR GOTO ATTENDEES

Email book@gauntlt.org
before the end of the day
for a review copy



@WICKETT

#RUGGEDDEVOPS

PRO-TIP #2
PUT SECURITY TESTING IN
YOUR CONTINUOUS
INTEGRATION SYSTEM

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 <wayneesequin@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

```

459 $ export DIRB_WORDLISTS="/home/travis/build/gauntlt/gauntlt/vendor/dirb/wordlists"
460 $ bundle exec rake
461 cd ./vendor/gruyere && ./manual_launch.sh && cd ../..
462 Gruyere started at 20097 PID and is available at localhost:8008
463 cd ./examples && bundle exec gauntlt --tags @final && cd ..
464 Using the default profile...
465 @final
466 Feature: hello world with gauntlt using the generic command line attack
467
468   Scenario:                               # ./hello_world/hello_world.attack:3
469     When I launch a "generic" attack with: # gauntlt-1.0.8/lib/gauntlt/attack_adapters/generic.rb:1
470       """
471       cat /etc/passwd
472       """
473     Then the output should contain:        # aruba-0.5.4/lib/aruba/cucumber.rb:147
474       """
475       root
476       """
477
478 @slow @final
479 Feature: Look for cross site scripting (xss) using arachni against a URL
480
481   Scenario: Using arachni, look for cross site scripting and verify no issues are found # ./arachni-xss/final_arachni-xss.attack:4
482     Given "arachni" is installed                                                         # gauntlt-1.0.8/lib/gauntlt/attack_adapters/arachni.rb:1
483     And the following profile:                                                           # gauntlt-1.0.8/lib/gauntlt/attack_adapters/gauntlt.rb:9
484       | name | value |
485       | url  | http://localhost:8008 |
486     When I launch an "arachni" attack with:                                           # gauntlt-1.0.8/lib/gauntlt/attack_adapters/arachni.rb:5
487       """
488       arachni --modules=xss --depth=1 --link-count=10 --auto-redundant=2 <url>
489       """
490     Then the output should contain "0 issues were detected."                          # aruba-0.5.4/lib/aruba/cucumber.rb:131
491
492   Scenario: Using arachni, look for cross site scripting and verify no issues are found # ./arachni-xss/final_arachni-xss.attack:15
493     Given "arachni" is installed                                                         # gauntlt-1.0.8/lib/gauntlt/attack_adapters/arachni.rb:1
494     And the following profile:                                                           # gauntlt-1.0.8/lib/gauntlt/attack_adapters/gauntlt.rb:9
495       | name | value |
496       | url  | http://localhost:8008 |
497   Running a arachni-simple_xss attack. This attack has this description:
498   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
499   faster. For more depth, run the gauntlt attack alias 'arachni-simple_xss_with_depth' and specify depth.
500   The arachni-simple_xss attack requires the following to be set in the profile:
501   ["<url>"]
502   When I launch an "arachni-simple_xss" attack                                         # gauntlt-1.0.8/lib/gauntlt/attack_adapters/arachni.rb:9
503   Then the output should contain "0 issues were detected."                          # aruba-0.5.4/lib/aruba/cucumber.rb:131

```

BATTLE-TESTED CODE WITHOUT THE BATTLE

SECURITY TESTING AND CONTINUOUS INTEGRATION

James Wickett and Gareth Rushgrove

Velocity 2014



share

Battle-tested code without the battle by Gareth Rushgrove

Published June 24, 2014 in Technology

<https://speakerdeck.com/garethr/battle-tested-code-without-the-battle>

@WICKETT

#RUGGEDDEVOPS

PRO-TIP #3

ADD APPLICATION SECURITY
TELEMETRY TO DEVS AND OPS

CONVERT APP SECURITY
LOGS INTO METRICS IN THE
SYSTEMS DEV AND OPS USE



logstash

StatsD

RUNTIME CORRELATION BETWEEN BIZ, OPS, DEV, SEC

SQLI ATTEMPTS + HTTP 500's
OR
LOGIN SPIKES + TRANSACTION
DECREASE

RUNTIME INSTRUMENTATION FOR APPLICATION SECURITY



Signal Sciences

PRO-TIP #4
GET HUGS FROM THE
AUDITORS AND ADD
HARDENING AND AUDIT USING
CONFIG MANAGEMENT

OPEN SOURCE HARDENING FRAMEWORK CHEF/PUPPET/ANSIBLE

<http://hardening.io/>

@WICKETT

#RUGGEDDEVOPS

RUN NIGHTLY AUDITS OF YOUR HARDENING USING CONFIG MANAGEMENT (CHEF AUDIT MODE)

<https://www.chef.io/blog/2015/04/09/chef-audit-mode-cis-benchmarks/>

OS AND CONFIG MANAGEMENT



REVERSE THE TREND
ADD VALUE TO DEVS
ADD VALUE TO OPS

SUMMARY

Software development has been a constant experiment in how we know anything

Application Security abdicated runtime responsibility and effectively abdicated development responsibility through incoherent philosophical approaches and fostering organizational silos

DevOps is here to stay, and security can actually be a part of it

Ops found a way to add value, security needs to find that same path

There are three ways we can add value: at development, at deploy, at runtime



Please

**Remember to
rate this session**

Thank you!

Thanks !