How To Build An Application Security Program

BSides San Francisco 2019

Jerry Gamblin

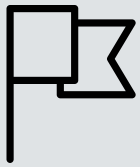
Kenna Security

@jgamblin

JerryGamblin.com

HandsOnHacking.org

Internal.dev



MY APPLICATION SECURITY JOURNEY

A Journey of A Thousand Miles Begins With A Single Step.

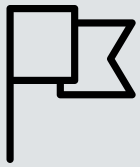
1 The Government

2

CarFax

3

Kenna Security



Lessons Learned

"Wow, There Are A Lot"

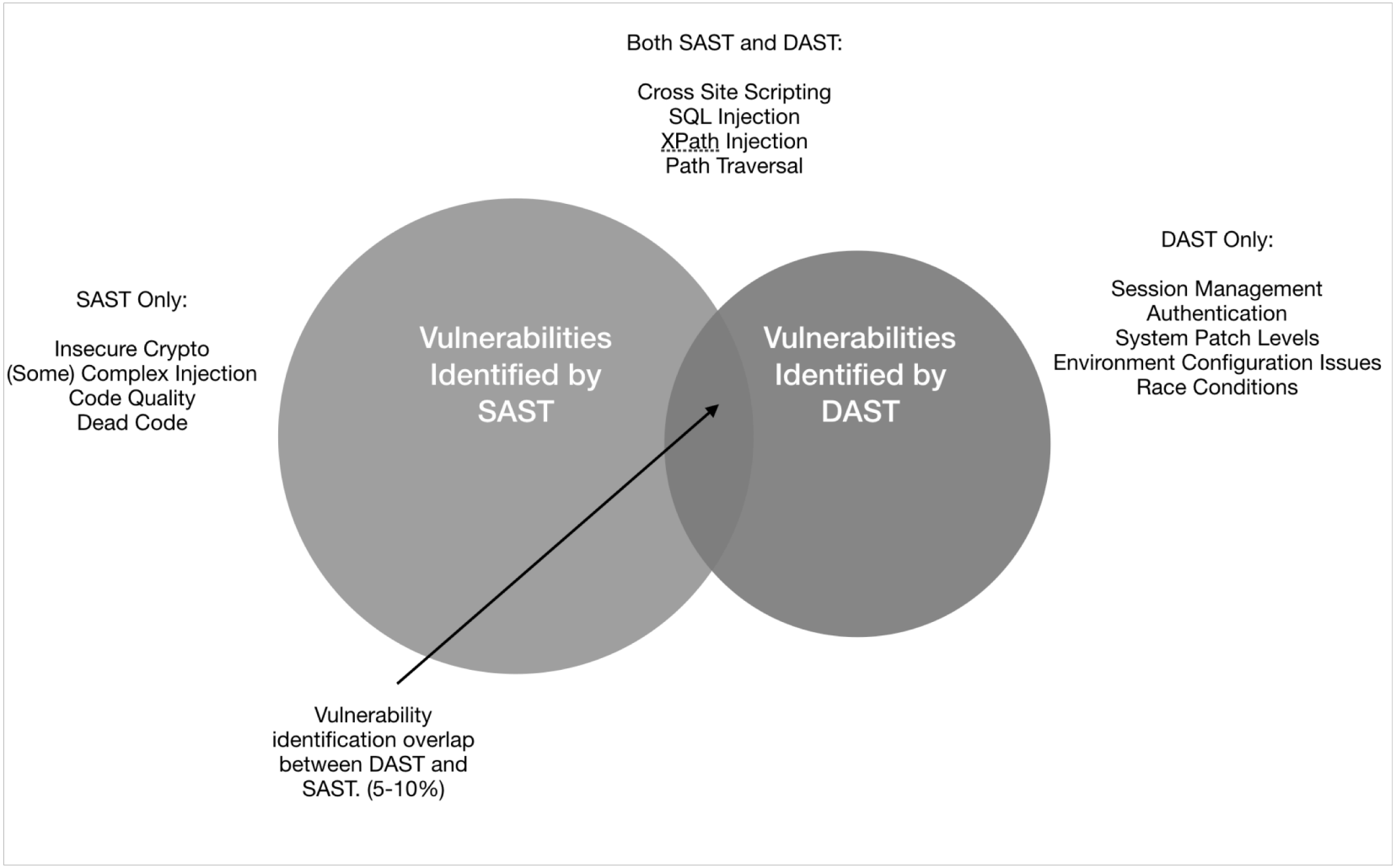
THERE IS NO PREFECT TOOL

“If Application Security was easy the security team would just do it.”

- [redacted]

…and there are so many.

PHASE	VULNERABILITY DATA TYPE	VULNERABILITY SOURCES
Develop	• Threat Modelling • IDE (Static Analysis) • Software Composition Analysis (SCA)	IDE, JSON, CSV, API
Monitor	• Software Composition Analysis	BLACKDUCK HUB, Sonatype
Build	• Static Analysis • Software Composition Analysis	CHECKMARX, MICRO FOCUS, VERACODE API, VERACODE XML, WhiteHat SECURITY.
Deploy	• DAST • "Classic" Vulnerability Management	Trustwave Hailstorm, MICRO FOCUS WebInspect, IBM AppScan, netsparker, appspider, ZAP, Burp Suite, Qualys WAS, w3af, WhiteHat Sentinel, BETA bugcrowd, IMPERVA WAF
Operate	• Discovery • DAST • Bug Bounty • Penetration Testing	


Both SAST and DAST:
Cross Site Scripting
SQL Injection
XPath Injection
Path Traversal
SAST Only:
Insecure Crypto
(Some) Complex Injection
Code Quality
Dead Code
Vulnerabilities Identified by SAST
Vulnerabilities Identified by DAST
DAST Only:
Session Management
Authentication
System Patch Levels
Environment Configuration Issues
Race Conditions
Vulnerability identification overlap between DAST and SAST. (5-10%)

AUTOMATION IS HARD

Move Application Quality And Security Closer To The Developer.

All Configurations Should Be Static, Scripted, and Immutable.

Testing Continuously At Every Stage Of Deployment, Including Production.

Build Dashboards and Reports Tailored To Security Considerations For The Developer.

Block Code From Production If It’s Found Insecure.

MANAGEMENT MANAGEMENT

Everyone wants security, without the burden of security.

If you want to learn how to deal with upper management get a cat, most of the time they want you to leave them alone unless you have something for them, or they need something.

- Tell Them What You Know.
- Tell Them What You Don’t Know.
- Tell Them What You Think Is Likely To Happen.

PRODUCT MANAGEMENT

No Better Friend, No Worse Enemy.

Product Management

✓ The Roadmap

- Manages The Direction Of The Product.

✓ Day to Day Work Management

- High Level Overview of Major Work

✓ Break Fix

- Interrupts
  - Break/Fix
  - *Security Findings*.

Product Management Is ***EASILY*** The Hardest

Job In Any Technical Organization.

DEVELOPER RELATIONS

I like to build cool stuff too.

Programmers don’t burn out on hard work, they burn out on change-with-the-wind directives and not ‘shipping’.

Mark Berry

- Host Dev Security Training.
- Host A CTF For Your Dev Teams.
- Teach Them Basic Threat Modeling.

TIME MANAGMENT

“I hope you like going to meetings, because Application Security is 50% meetings, 50% documentation/email/JIRA/Snow and 50% hacking.”

- **Me**

Time Management

"Sure, I Can Make That Meeting,"

Meetings

If you have 4 development teams and they have 2 hours of planning meetings a week (they will have more) that is 20% of your time.

Written Communications

Responding to email, slack messages and JIRA tickets can easily take up 2-4 hours a day.

"Hacking"

Anytime left over you will get to do "the fun part" of your job, hopefully.

BUDGET MANAGMENT

You can not run a successful application security program on handouts.

Application Budgeting

"Show Me The Money"

Static Tools

Surprisingly, these are normally the cheapest and usually start in the sub $5,000 range.

Dynamic Tools

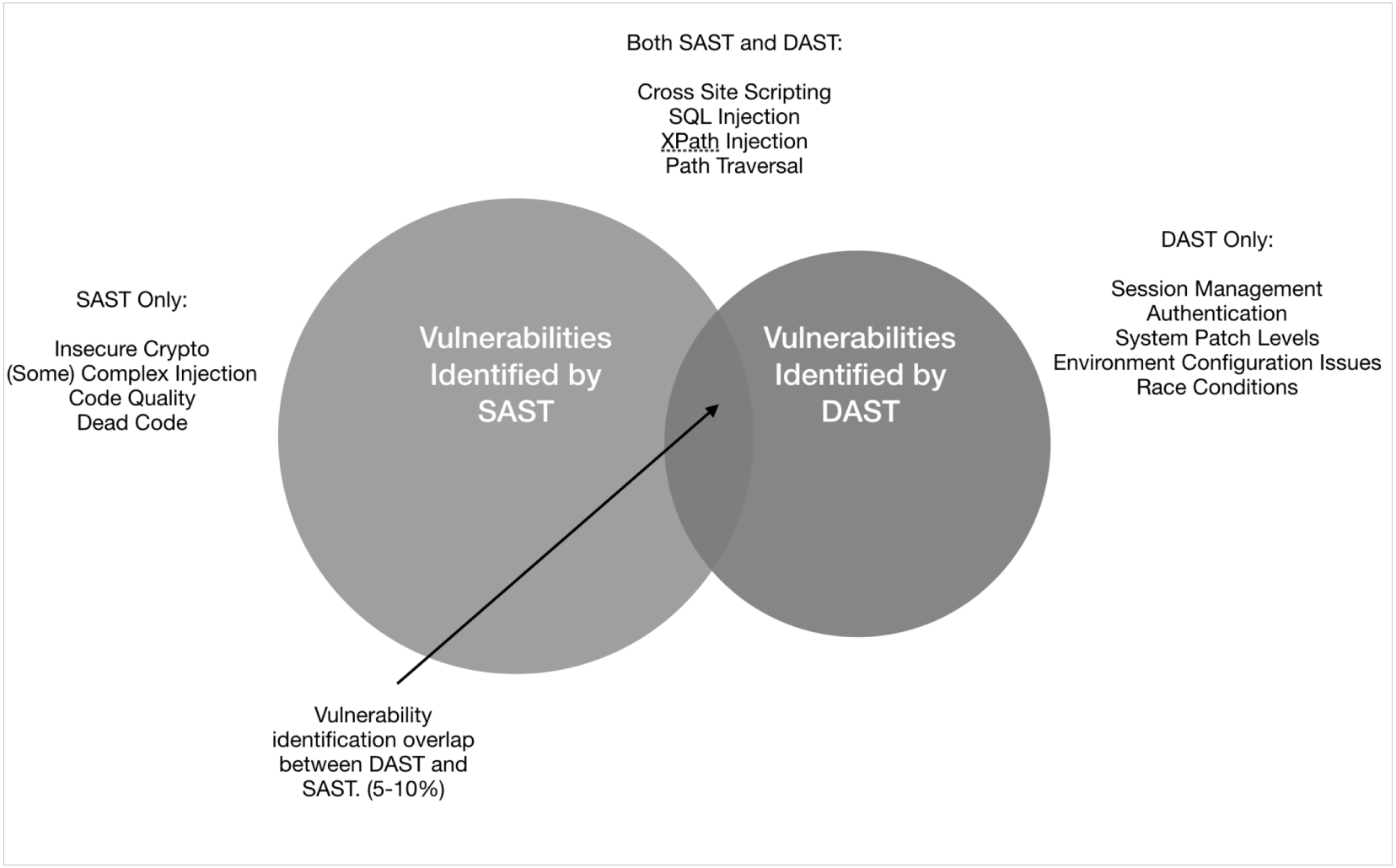
This group of tools is normally a SaaS offering and can run from $10,000 to $TEXAS

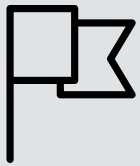
Consulting

Hiring an application security consultant is a great way to test your applications but normally start $20,000 a week.

Growth Management

New Team or Product, You need More Budget.


Both SAST and DAST:
Cross Site Scripting
SQL Injection
XPath Injection
Path Traversal
SAST Only:
Insecure Crypto
(Some) Complex Injection
Code Quality
Dead Code
Vulnerabilities Identified by SAST
Vulnerabilities Identified by DAST
DAST Only:
Session Management
Authentication
System Patch Levels
Environment Configuration Issues
Race Conditions
Vulnerability identification overlap between DAST and SAST. (5-10%)



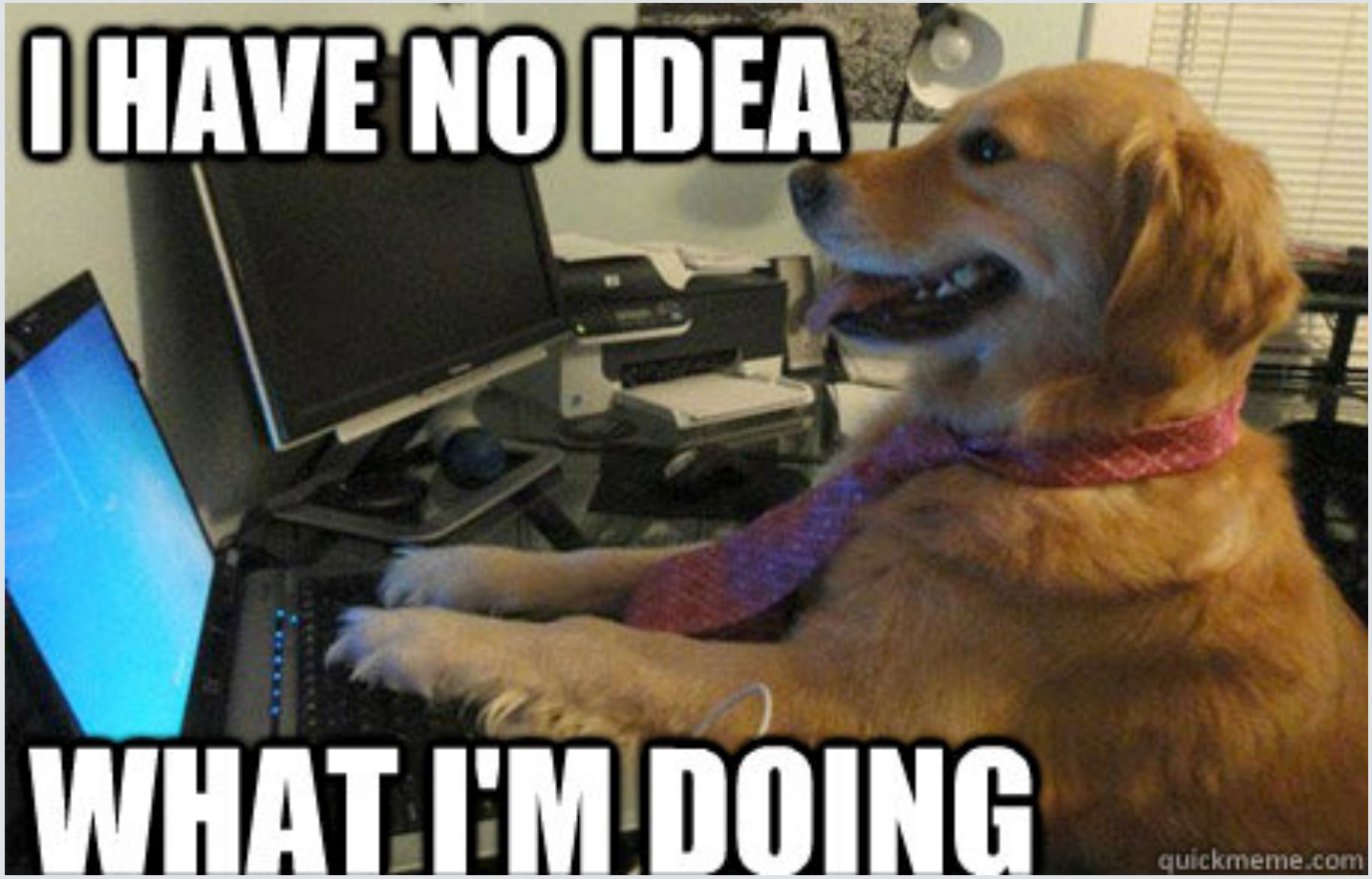
My Failures

"Trust Me, There Are A Lot"

"SUCCESS IS WALKING FROM FAILURE TO FAILURE WITH NO LOSS OF ENTHUSIASM."

WINSTON CHURCHILL

NOT LEARNING TO PROGRAM


I HAVE NO IDEA
WHAT I'M DOING
quickmeme.com

NOT UNDERSTANDING THE BUSINESS

“Having a kid is like having a tiny drunk friend who thinks you are incredibly rich.”

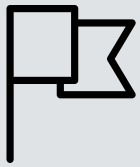
NO BUDGET? NO PROGRAM.

TITLES MATTER

COMMUNICATION


I WILL
PUT THAT
THANG ON!!
ANTLERS
ANTLERS
ANTLERS
ANTLERS


MIZZOU
32
MIZZOU
10
BARNETT
21
ROBERTSON



Quick Review

Quick Review

- ✓ Communicate.
- ✓ There Is No Perfect Tool
  - ✓ You NEED A DAST & SAST tool.
- ✓ Product Management Is Your Friend.
- ✓ Automation Is Hard, Do It Anyway.
- ✓ Understand Your Business.
- ✓ Titles Matter.
- ✓ Budgets Matter More.
- ✓ Communicate.

THERE IS NO “RIGHT” WAY.

“You have your way. I have my way. As for the right way, the correct way, and the only way, it does not exist.”

- **Nietzsche**

Jerry Gamblin

@jgamblin

JerryGamblin.com

THANK YOU!