Automating Almost All Application Security Things with CI/CD

Even Honeypots!

Mick Douglas and Andy Douglas

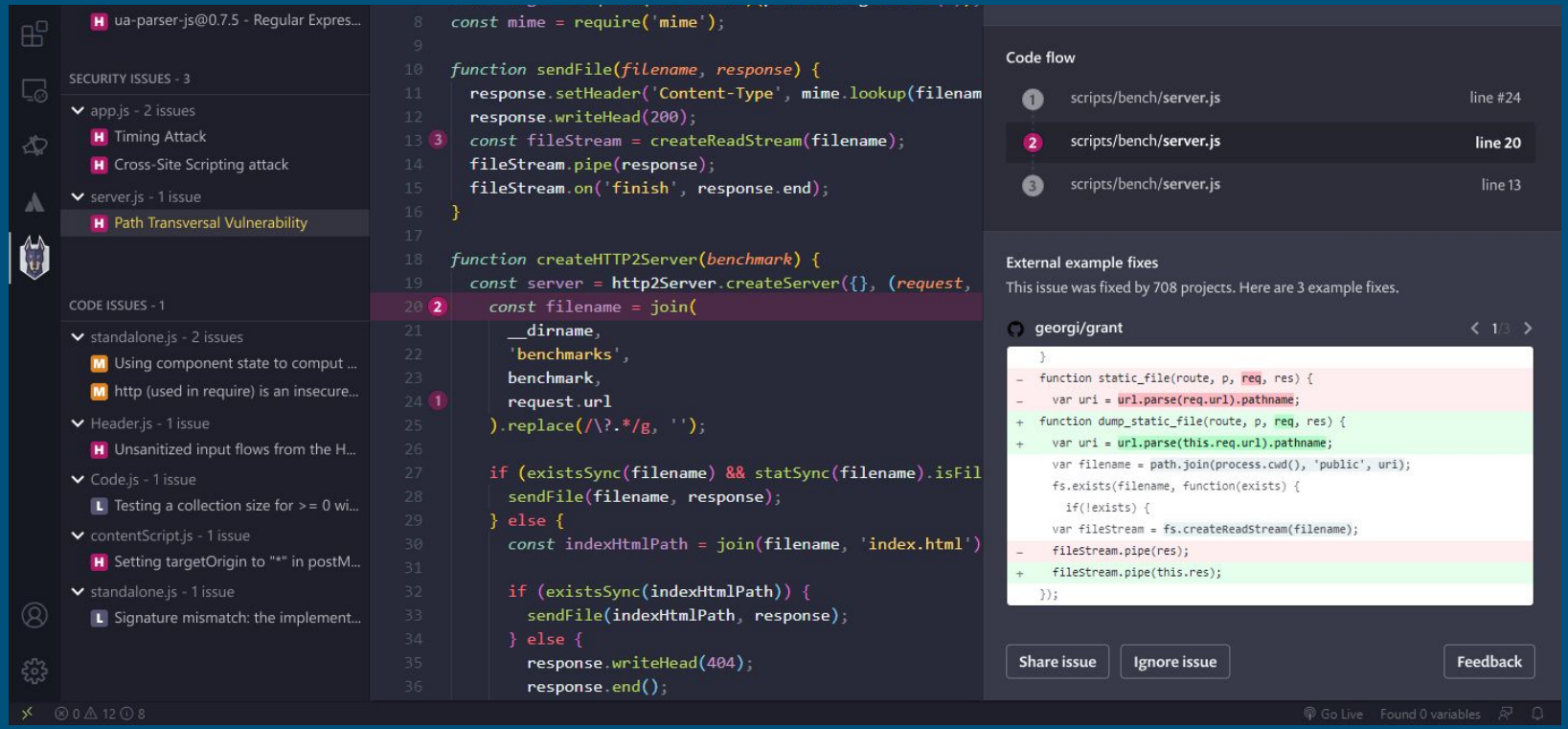
Link to slides+resources at end!


Development
Continuous Integration
Continuous Delivery or Deployment

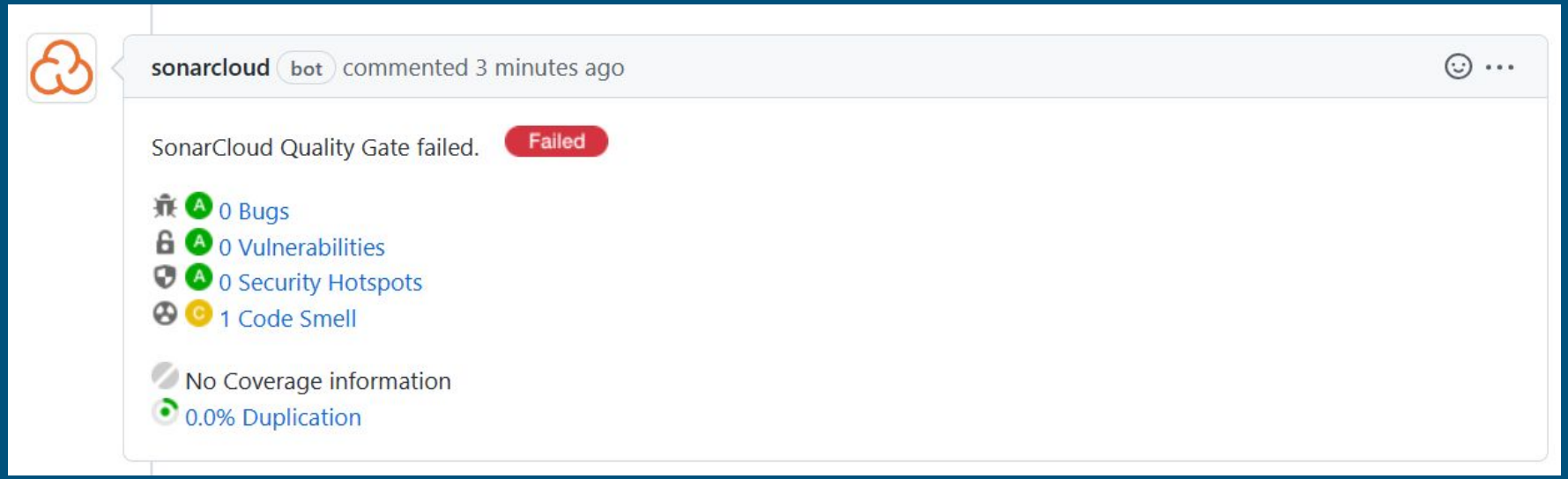
Development

Continuous Integration

Continuous Delivery or Deployment



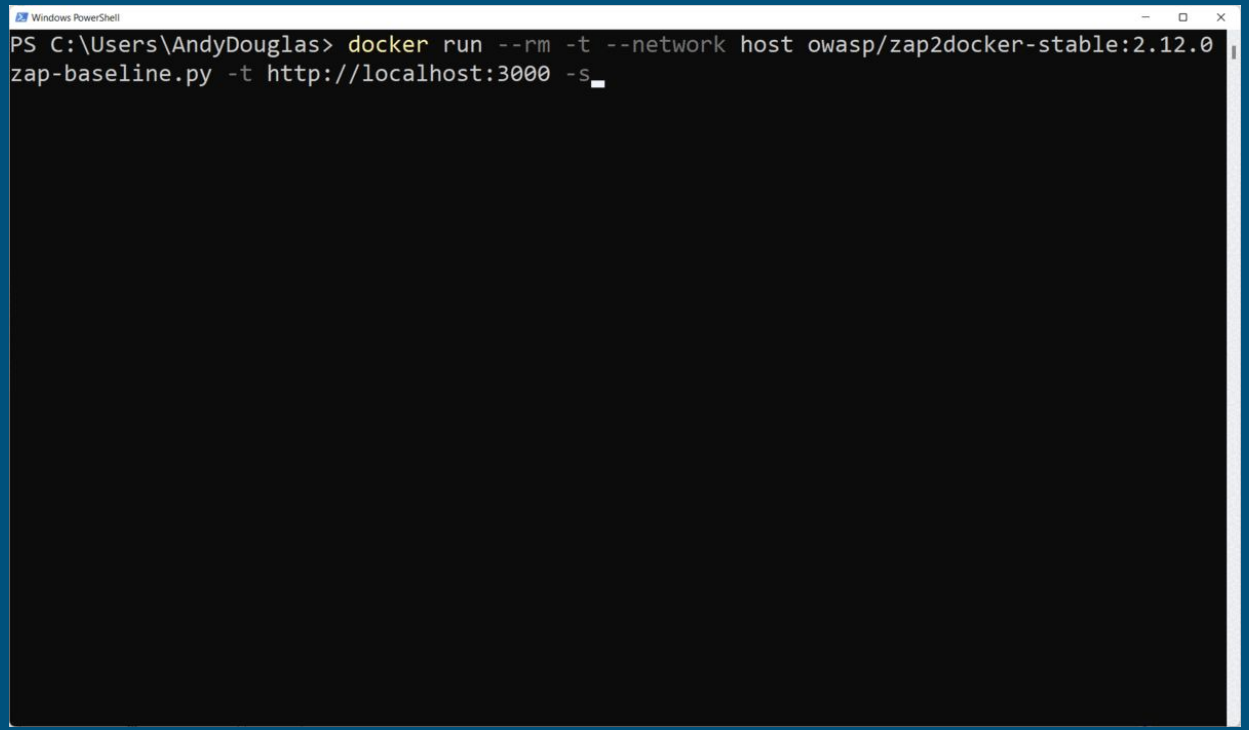
Development → Continuous Integration → Continuous Delivery or Deployment



Development

Continuous Integration

Continuous Delivery or Deployment



Active Defense

Automate Application Security with CI/CD

Part 1: Dynamic Scans for prevention

Part 2: Active Defense for detection

Goal: Actionable Security Improvement

Hi, my name is Andy Douglas

- Long-time CodeMash attendee, first-time speaking
- Full Stack Software Dev/Engineer > Architect > Engineering Manager
- Security…meh

Hi, my name is Mick Douglas

- First time CodeMash attendee
- Passionate about security
- Infosec Innovations, SANS Principle Instructor, IANS Research Faculty

Part 1: Dynamic Scans for prevention

SAST - quick word

Recommendation:

Integrate SAST w/ IDE + CI

Popular Tools: Snyk, Checkmarx, SonarQube/SonarCloud

Dynamic Application Security Testing (DAST)


Merge into main
CI build runs
(hopefully with SAST)
CD build runs
to deploy to env X
Smoke tests
and DAST

4 Labs

DAST Lab

DAST Lab: deploy vulnerable web app

DAST Lab: Automate a leading DAST tool

DAST Lab: Learn how to include DAST in your pipelines

DAST Strengths

DAST Weaknesses

Recommendation:

DAST: CD and/or scheduled

Popular Tools: ZAP, StackHawk, Burp Suite, Astra Pentest, etc.

Part 2: Active Defense for detection

Part 2: Active Defense ~~for detection~~ FTW!!

WAF

Traditional Defense == Passive

Traditional Defense == KNOWN

Active Defense == Passive & Active

Shift focus/effort to higher reward

Attackers have predictable paths

Active Defence at each phase

Recon: Ports

Honey Port

DEMO: Honey Port

Privilege Escalation: session tokens

Honey Tokens

Demo: Honey Tokens

Strategy: Defense Options

Watch and learn?

Random error response?

Firewall

QoS

Demo response options

Security != Hard/Expensive

Security as Functional Requirement

Security + CI/CD is good

LAB IT UP!!