# Security as Code (SaC) a DevSecOps approach



Joseph Katsioloudes

@GHSecurityLab

securitylab.github.com


# Joseph Katsioloudes

@jkcso

**GitHub** @github · 21h

Stay secure when using third-party GitHub Actions. Check out these tips from @jkcso!

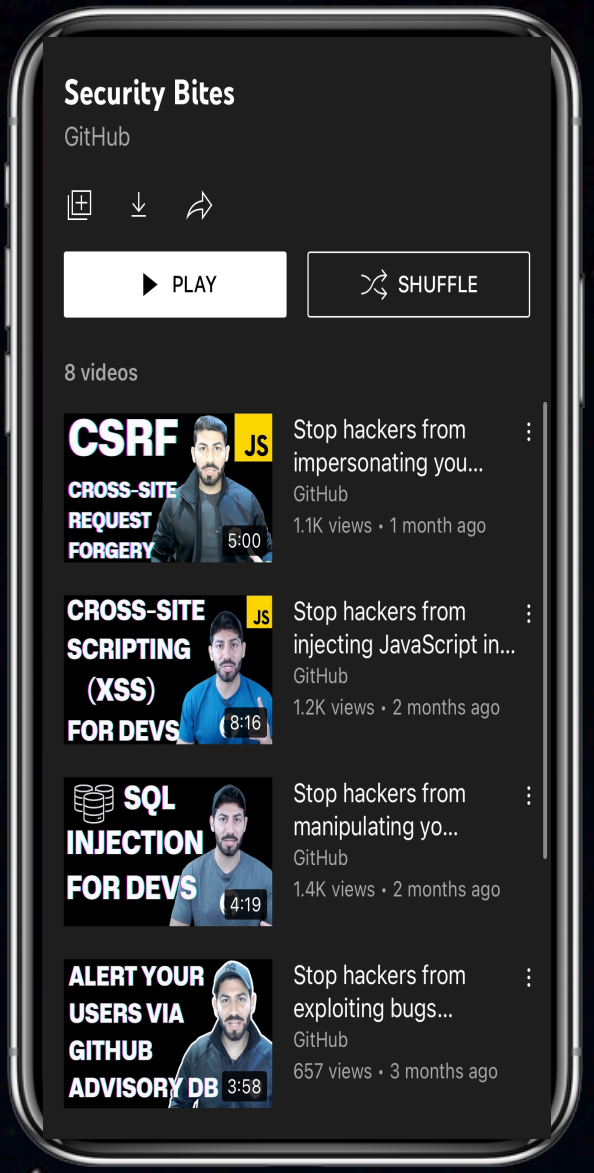

2 18 101

**GitHub Security Lab** @GHSecurityLab · Aug 9

How to avoid injection in GitHub Actions, in ⏱ 45 seconds


11 36

# Security Bites
# at GitHub's Channel

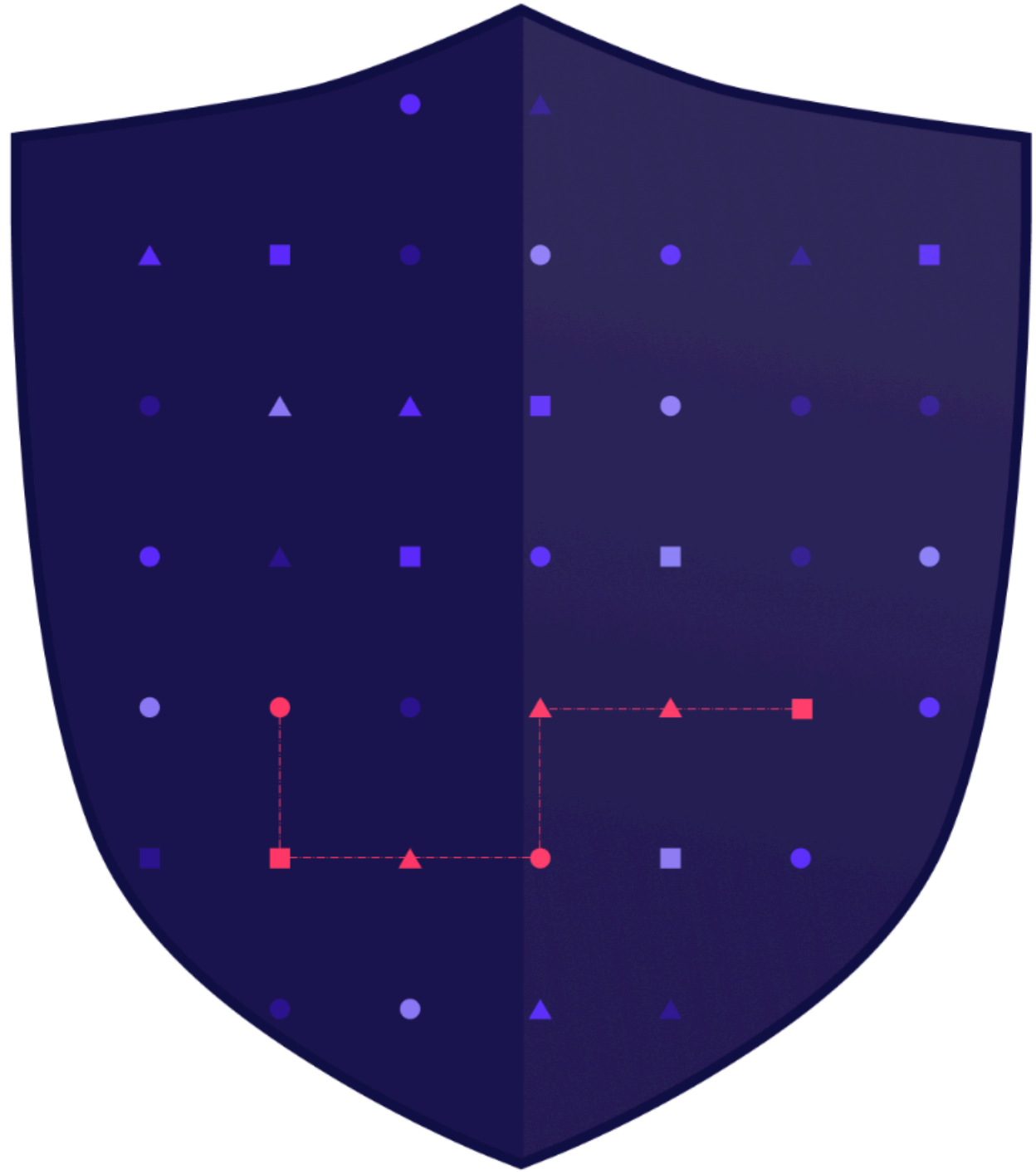


GitHub Security Lab

# Securing the world's software, together

GitHub Security Lab's mission is to inspire and enable the community to secure the open source software we all depend on.

Follow @GHSecurityLab



# Vulnerabilities we've disclosed so far

**Remote Code Execution (RCE) in the Chrome renderer - CVE-2022-1869**
GHSL-2022-043 • CVE-2022-1869 • published 20 days ago • discovered by Man Yue Mo

**XSS in Toast UI Grid - CVE-2022-23458**
GHSL-2022-029 • CVE-2022-23458 • published 20 days ago • discovered by team

**Regular Expression Denial of Service (ReDoS) in the Azure SDK for Java.**
GHSL-2022-024 • published 20 days ago • discovered by team

**Regular Expression Denial of Service (ReDoS) in Apache Ignite**
GHSL-2022-023 • published 20 days ago • discovered by team

**Regular Expression Denial of Service (ReDoS) in Tapestry - CVE-2022-31781**
GHSL-2022-022 • CVE-2022-31781 • published 20 days ago • discovered by team

See all disclosures →

??? CVEs found

by Security Lab researchers

221 since March 2020

# Vulnerabilities we've disclosed so far

**Remote Code Execution (RCE) in the Chrome renderer - CVE-2022-1869**
GHSL-2022-043 • CVE-2022-1869 • published 20 days ago • discovered by Man Yue Mo

**XSS in Toast UI Grid - CVE-2022-23458**
GHSL-2022-029 • CVE-2022-23458 • published 20 days ago • discovered by team

**Regular Expression Denial of Service (ReDoS) in the Azure SDK for Java.**
GHSL-2022-024 • published 20 days ago • discovered by team

**Regular Expression Denial of Service (ReDoS) in Apache Ignite**
GHSL-2022-023 • published 20 days ago • discovered by team

**Regular Expression Denial of Service (ReDoS) in Tapestry - CVE-2022-31781**
GHSL-2022-022 • CVE-2022-31781 • published 20 days ago • discovered by team

See all disclosures →

## 344 CVEs found

by Security Lab researchers

221 since March 2020

```
void fire_thrusters(double vectors[12]) {
  for (int i = 0; i < 12; i++) {
     ... vectors[i] ...
  }
}

double thruster[3] = ... ;
fire_thrusters(thruster);
```


Curiosity Rover
@MarsCuriosity
I'm safely on the surface of Mars.

**Nat Friedman**
@natfriedman

Honored that @NASA is using GitHub, Actions, and CodeQL for the Mars drone flight software: github.com/nasa/fprime

If anyone working on this needs GitHub support, please feel free to DM me directly!

Traduire le Tweet

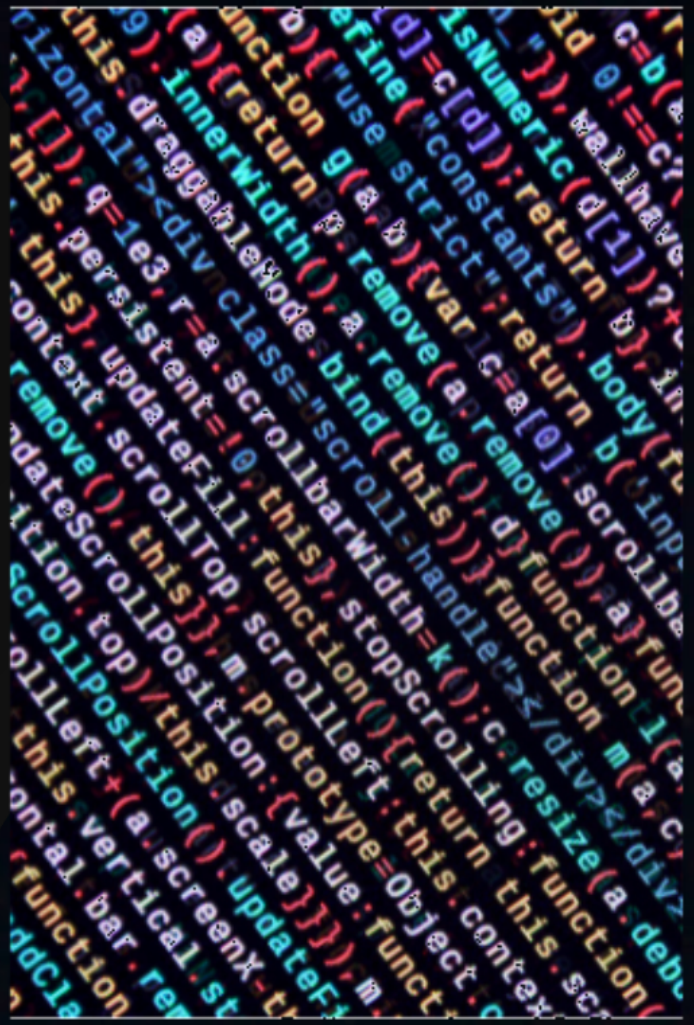
GitHub

Community

Hunters

# Security as Code (SaC)

+



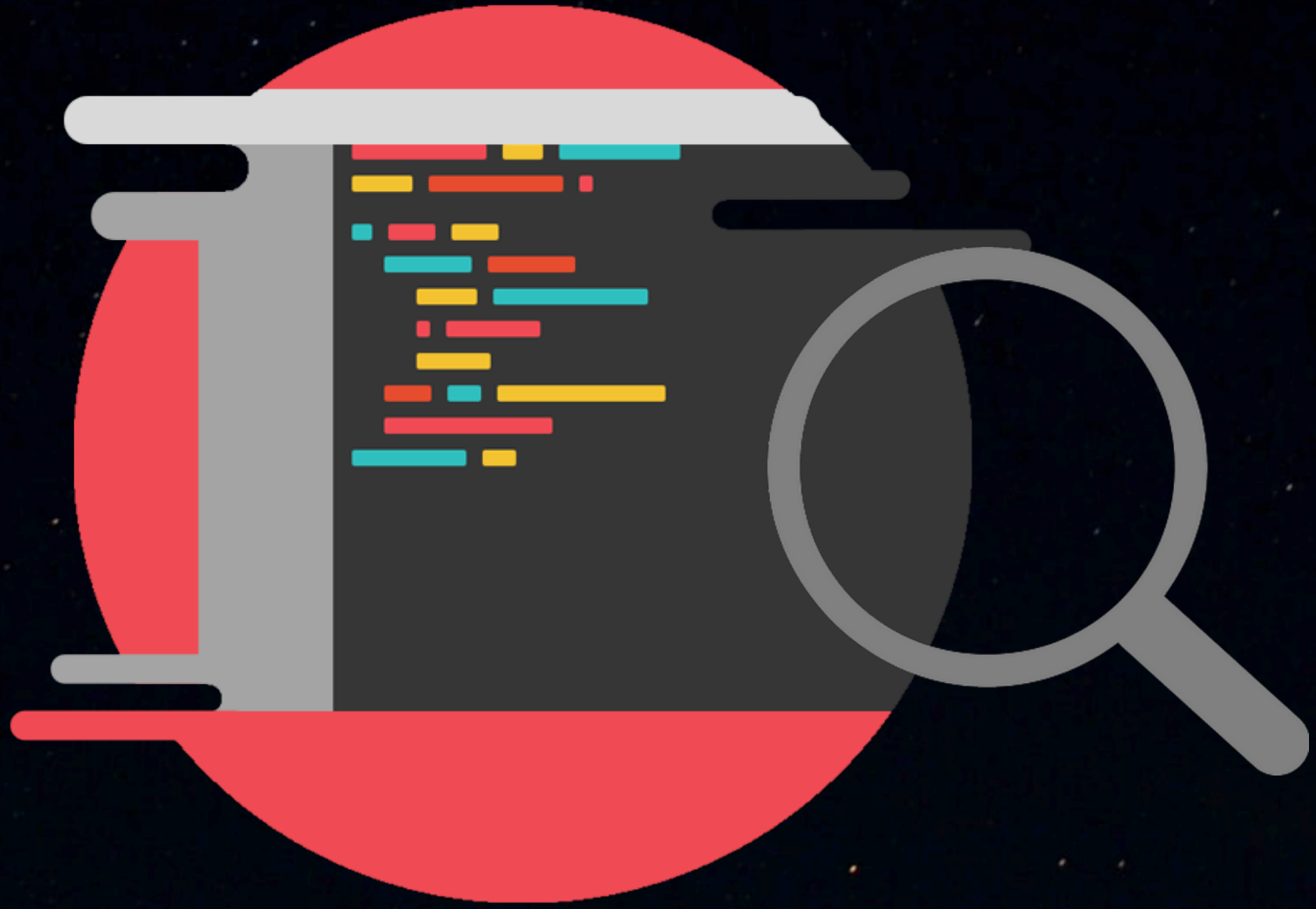
# Security as Code

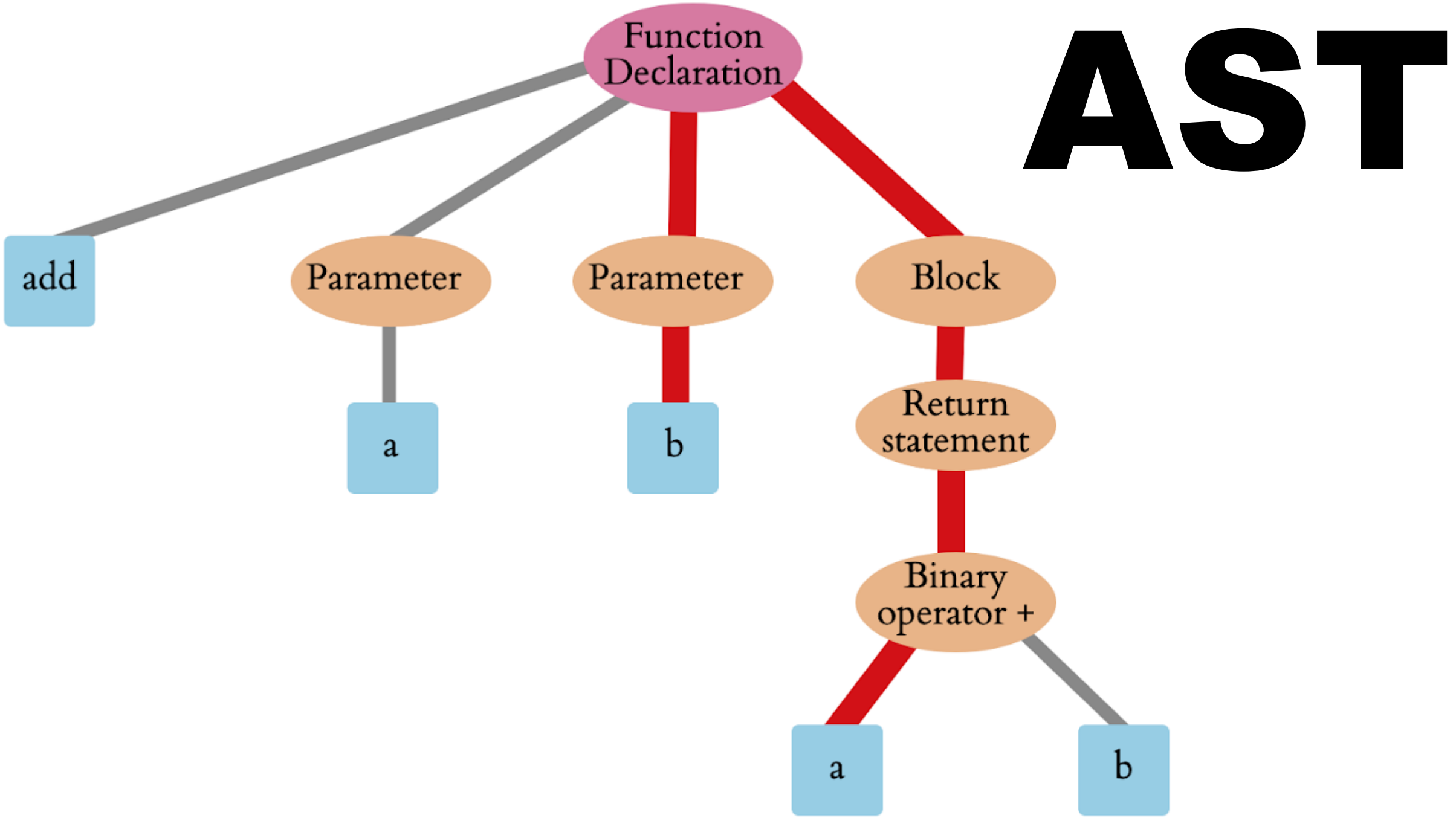
The methodology of codifying security decisions that are then shared with other teams

# CodeQL

Query code as if it was data by describing what you want to find, not how to find it

# Query Code




AST
Function Declaration
add
Parameter
a
Parameter
b
Block
Return statement
Binary operator +
a
b




Java


JS


SAST
VS
DAST

# Passive user


# Active user

# Passive user


# Active user

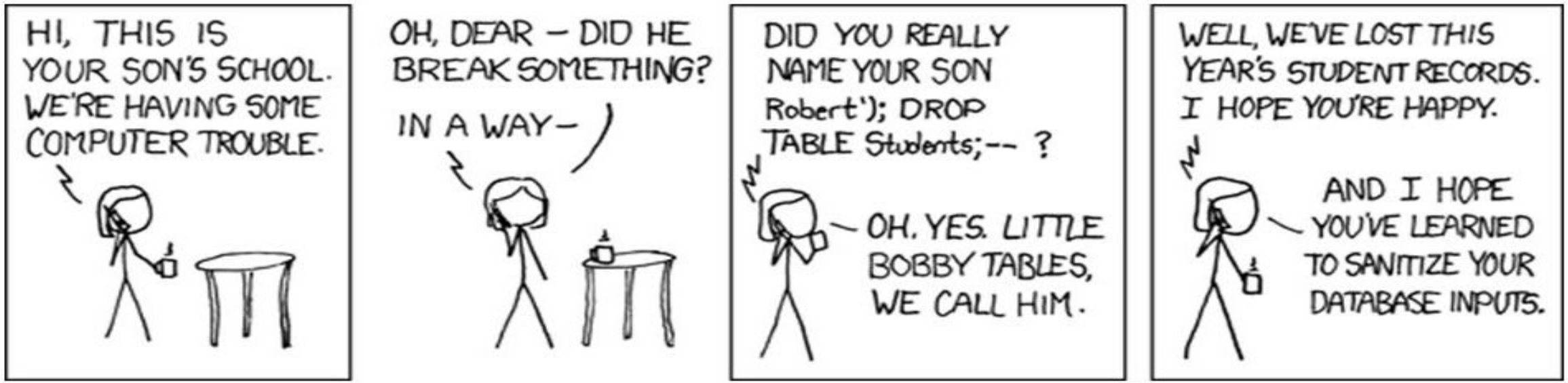
# How to enable CodeQL for your OS project

# Security Alerts

# Passive user


# Active user

# SQL Injection




Did you really name your son

*Robert'); DROP TABLE Students;--?*

Image source: XKCD, http://xkcd.com/327/

```
INSERT INTO students (name) VALUES ('Cleo');
```

```
INSERT INTO students (name) VALUES ('Cleo');
DROP TABLE students;
--');
```


Source


```
INSERT INTO students (name)
VALUES ('Cleo');
```


Source


Sink

Type: > query.Execute
& hit enter key


Source
Data Flow
Sink

# CodeQL in action

Source

# getText()

# ALL Methods


filter

# getText()

rawQuery(arg1, arg2)

# ALL Methods

filter

rawQuery()

get 1st arg

rawQuery(arg1, arg2)


Source
Data Flow
Sink

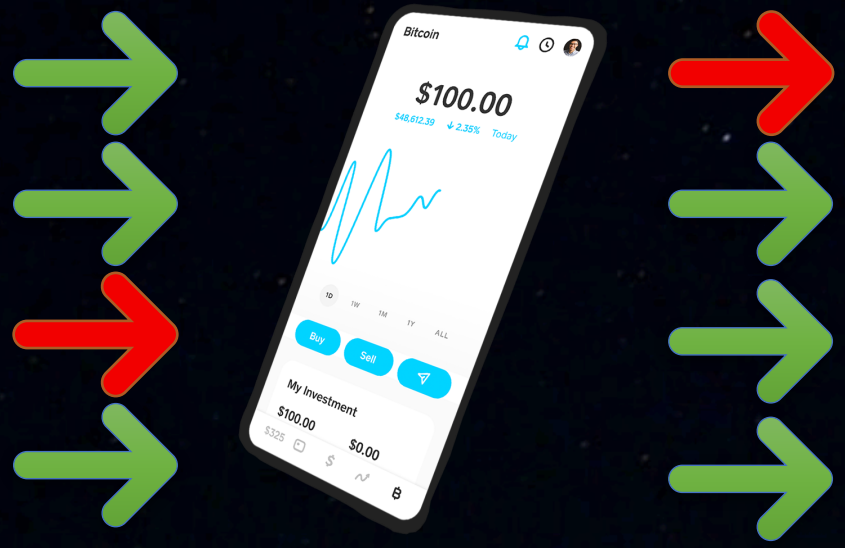

NODE
(expression)
Data Flow
NODE
(expression)

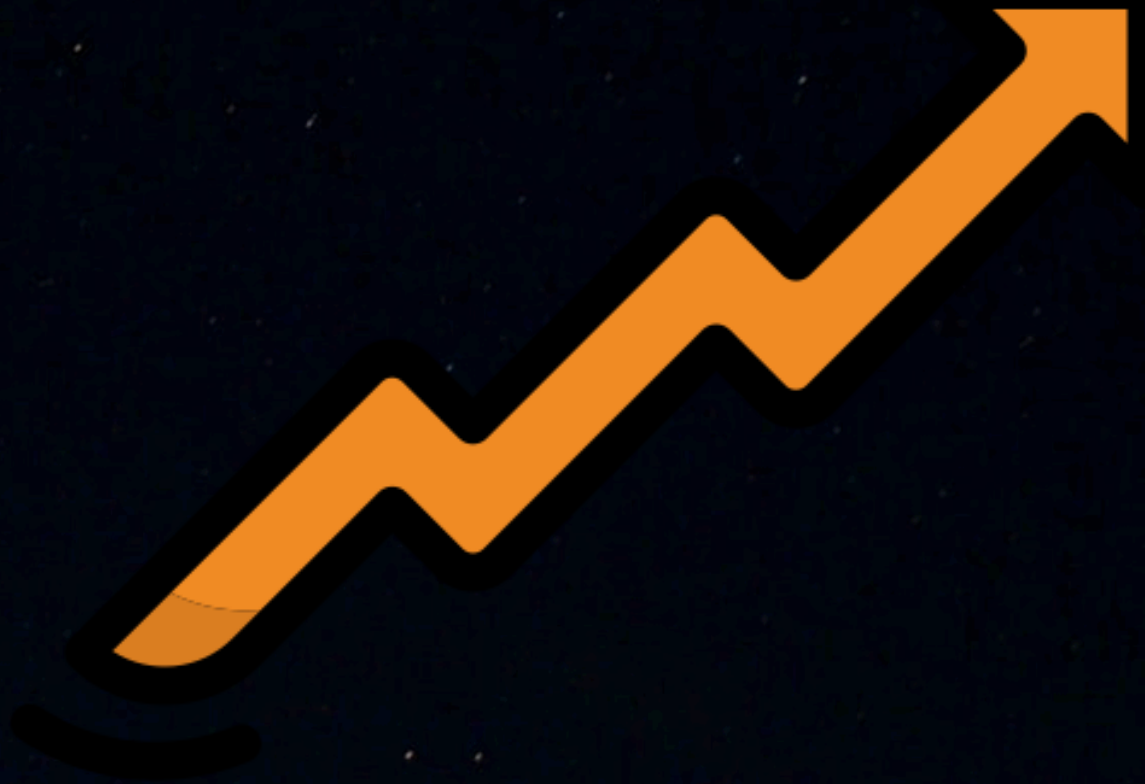
# Taint Tracking

# Extensibility & Flexibility

input

output



GitHub

Community

Hunters

# Start your CodeQL journey

1. codeql.com
2. securitylab.github.com/get-involved
3. securitylab.github.com/ctf
4. github.co/codeql-ci

Universe 2022

# Let’s build from here

November 9–10, San Francisco, CA
Streaming on githubuniverse.com

**GitHub Security Lab**
@GHSecurityLab

The pleasure was ours, @lukaseder
Happy to talk to more OSS maintainers and help secure OSS together.

> **Lukas Eder** @lukaseder · 14/04/2022
> Just had a really pleasant chat with folks from @ghsecuritylab to help better secure @JavaOOQ. 10/10 can recommend to all OSS maintainers: github.com/github/securit...

18:05 · 14/04/2022 · Twitter Web App

**@GHSecurityLab**

# Thank You

# Vienna!

@jkcso @GHSecurityLab