Security as Code, a DevSecOps Approach

Xavier René-Corail

@xcorail

Security Lab

Security Lab

Bounties Research Advisories Get Involved Events

What we do

Find vulnerabilities

Our researchers find and report new vulnerabilities in the open source projects everyone relies on.

Educate the community

We share our research through proof-of-concepts, articles, tutorials, conferences and community events.

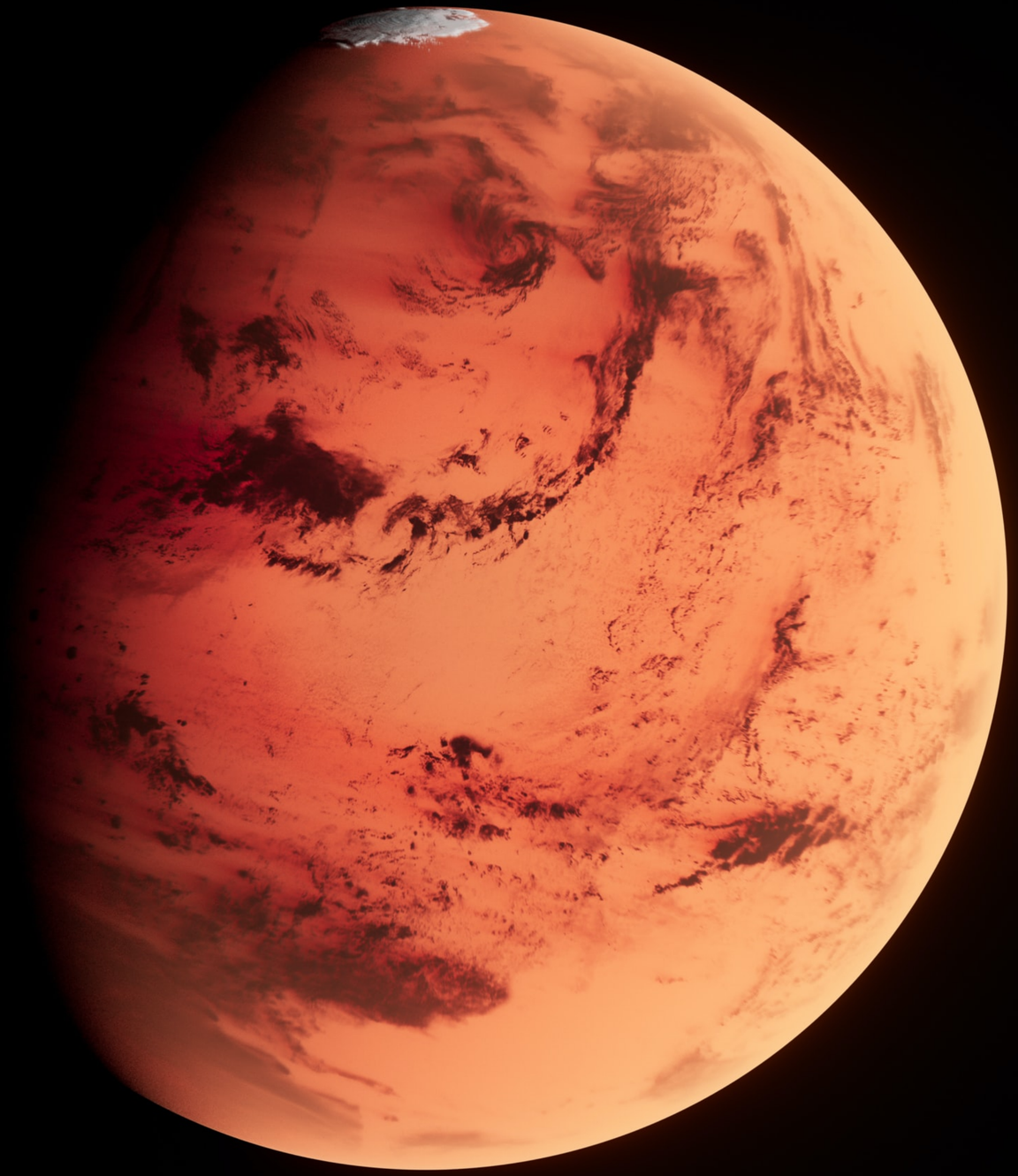
Amplify security research

We scale the security research of our community by performing Variants Analysis for open source projects with CodeQL.

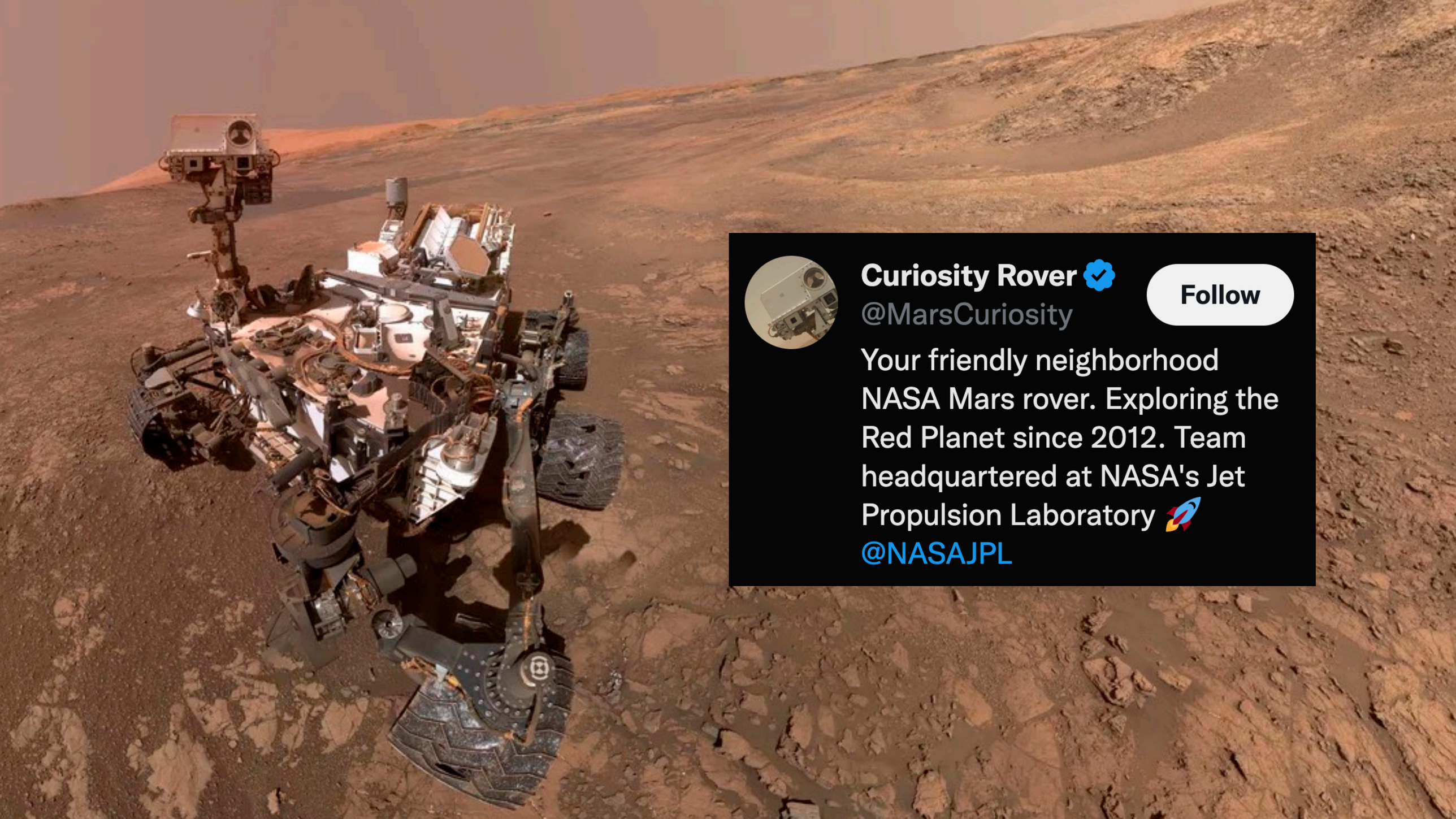
Notify the ecosystem

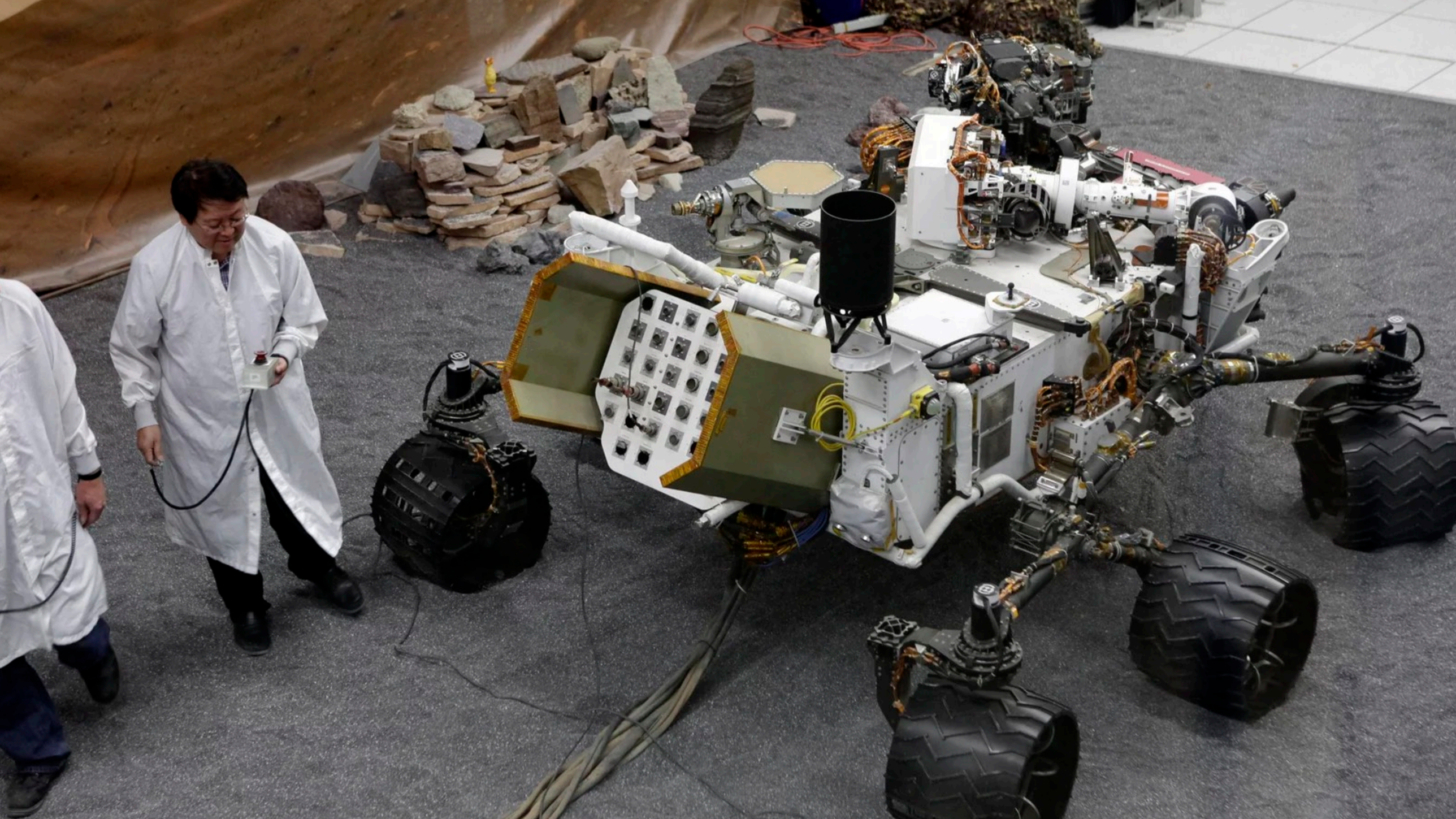
We curate a database of CVEs and security advisories to notify open source developers and maintainers.

https://securitylab.github.com

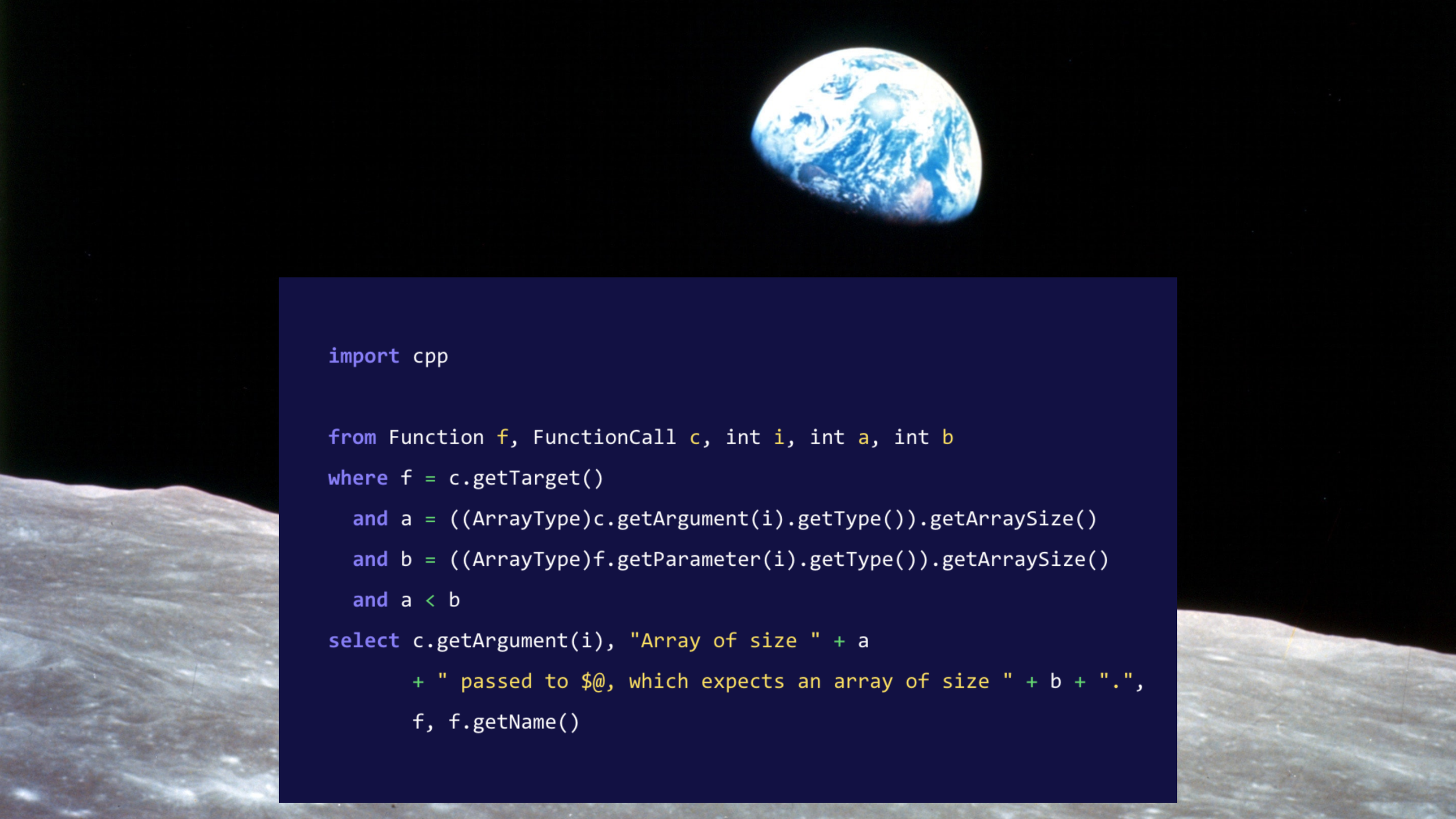


Planet Mars


Curiosity Rover
@MarsCuriosity
Follow
Your friendly neighborhood NASA Mars rover. Exploring the Red Planet since 2012. Team headquartered at NASA's Jet Propulsion Laboratory 🚀
@NASAJPL



```
1 void open_parachute(double vectors[12])
2 { for (int i = 0; i < 12; i++) {
3     ... vectors[i] ...
4   }
5 }
6
7 double thrusters[3] = ...;
8 open_parachute(thrusters);
```



```
import cpp

from Function f, FunctionCall c, int i, int a, int b
where f = c.getTarget()
  and a = ((ArrayType)c.getArgument(i).getType()).getArraySize()
  and b = ((ArrayType)f.getParameter(i).getType()).getArraySize()
  and a < b
select c.getArgument(i), "Array of size " + a
       + " passed to $@, which expects an array of size " + b + ".",
       f, f.getName()
```

Curiosity Rover
@MarsCuriosity

I'm safely on the surface of Mars. GALE CRATER I AM IN YOU!!! #MSL

8:32 AM · Aug 6, 2012

53.5K Retweets **53** Quote Tweets **12K** Likes

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!

6:23 AM · Feb 19, 2021

276 Retweets **40** Quote Tweets **2,131** Likes

What is different 9 years later?
Inclusion in the SDLC

How can we play it all like NASA?

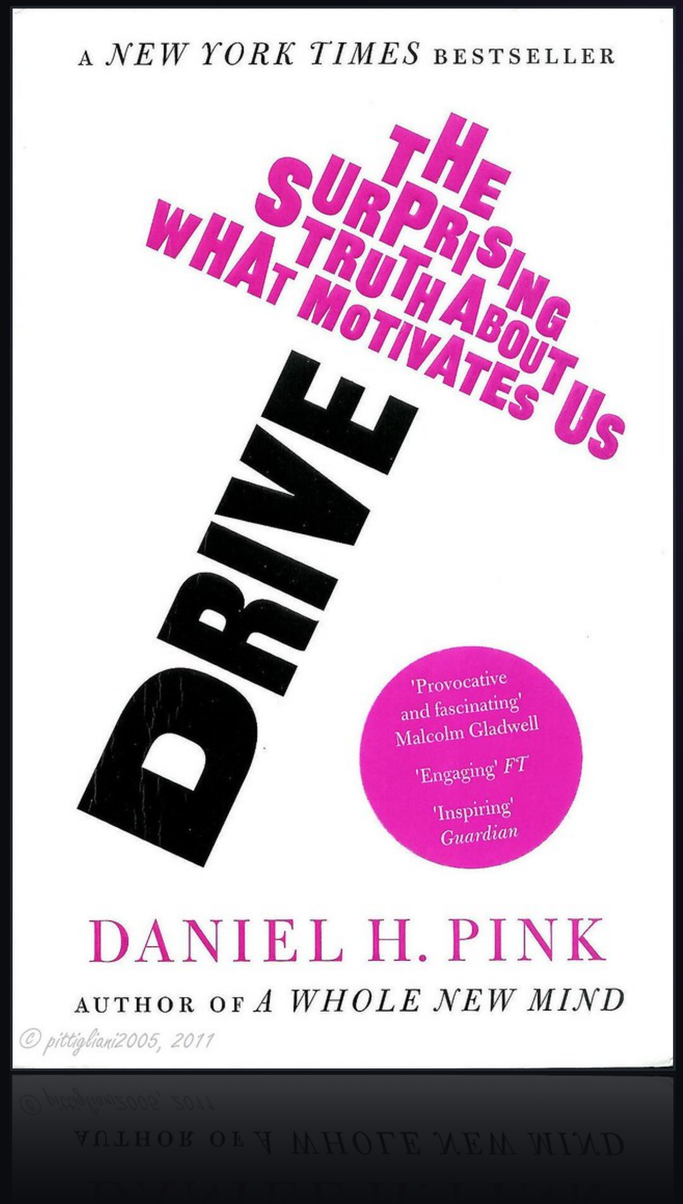
43%

Frustrated that security testing is done late in the SDLC

https://www.cshub.com/security-strategy/articles/how-devops-teams-embracing-new-ways-to-achieve-devsecops

Lessons learned from DevOps?

We need to Empower developers



What motivates developers?

Autonomy, Mastery, Purpose

Autonomy

You are in control

You receive a list of issues …

Mastery

You are learning and mastering a new skill

… from the experts …

Purpose

You know why you're doing what you're doing

… and you just do what you're told.

Giv’em code!

```
(function repeat() {
    eat();
    sleep();
    coffeeLoader();
    code();
    repeat();
})();
```


Security as Code

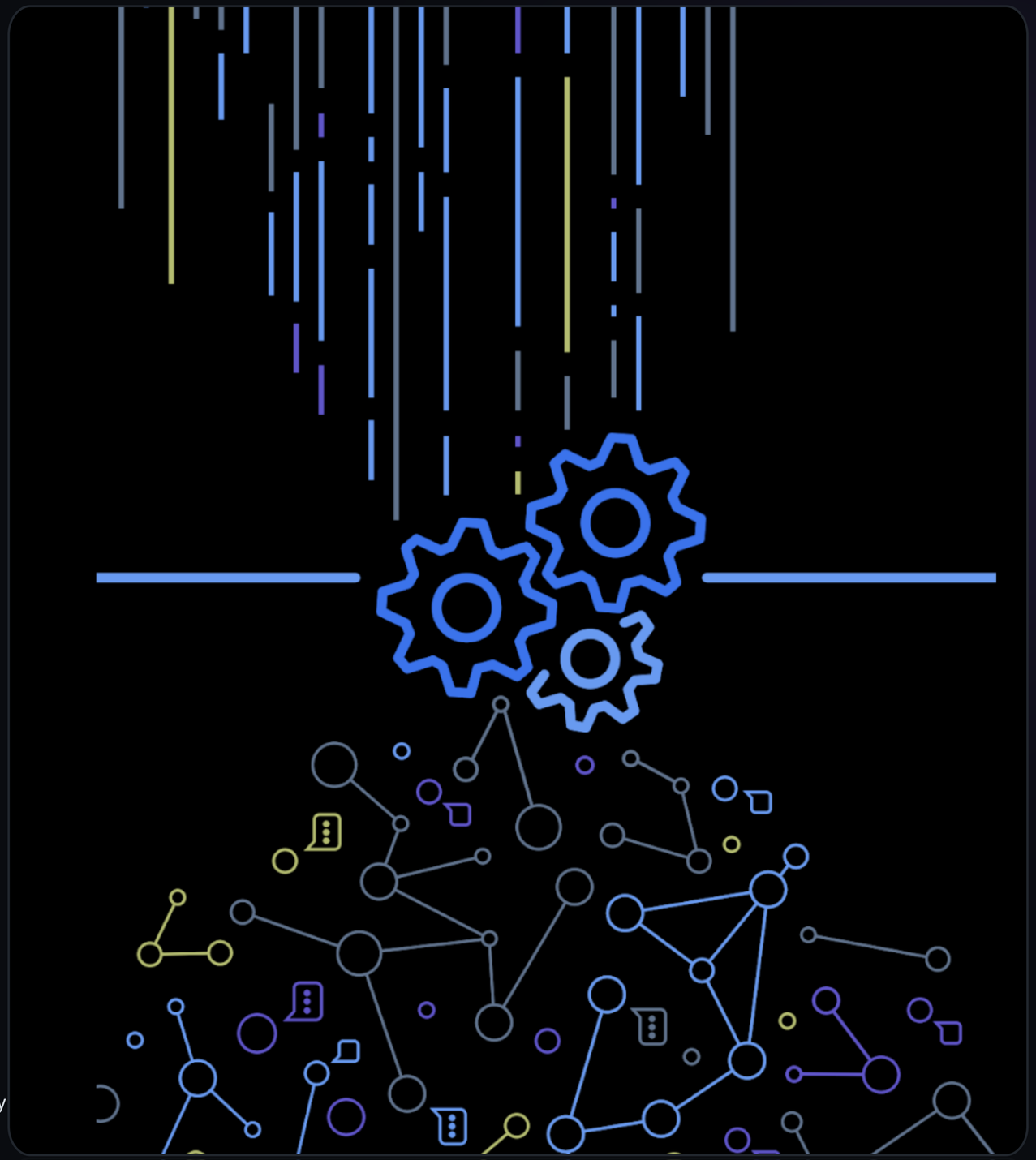
“

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

Security as Code (SaC)

CodeQL

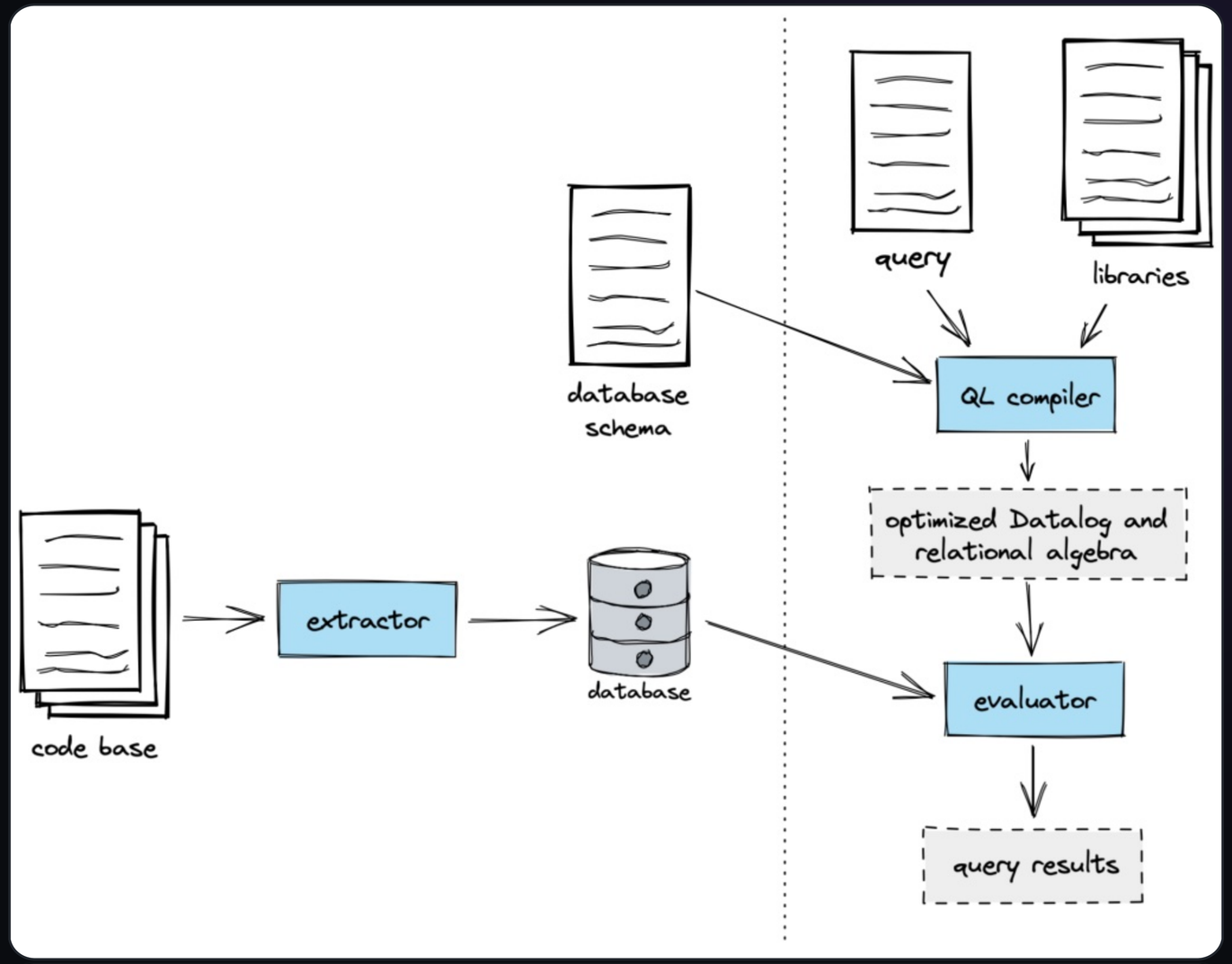
- SAST (Static Analysis Security Testing)
- Query code as if it’s data
- Describe what to find, not how to find it
- Logical, Declarative, Object-Oriented



CodeQL **extracts** your code into a **database**

AST, Semantics, Control Flow Graph

Optimized OO language to query this DB




```
from Function f
where f.getName() = "MyFunction"
select f
```

```
from Function f, FunctionCall c
where f.getName() = "MyFunction"
    and c.getTarget() = f
select c.getArgument(0)
```


Java


GO


JS

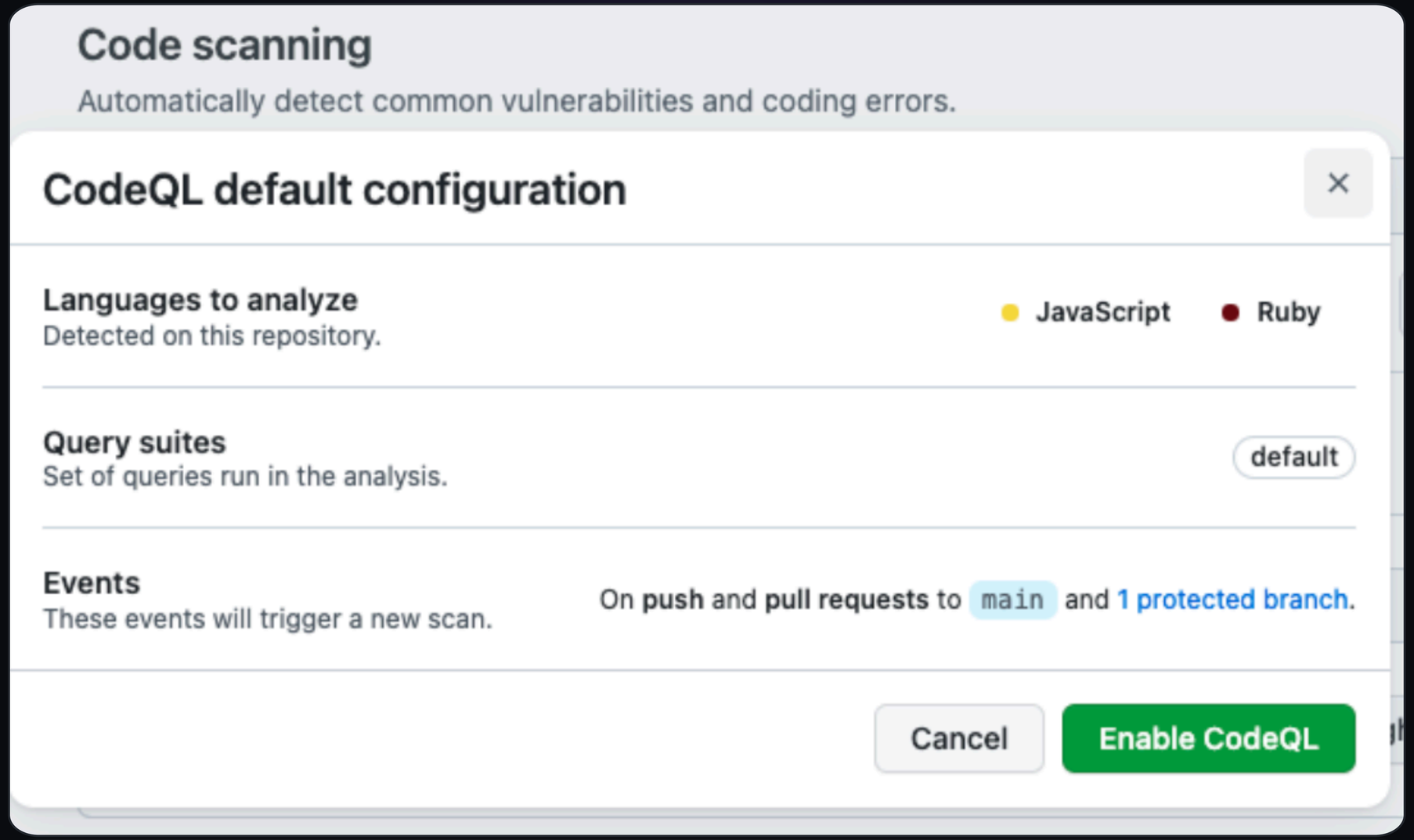

C++

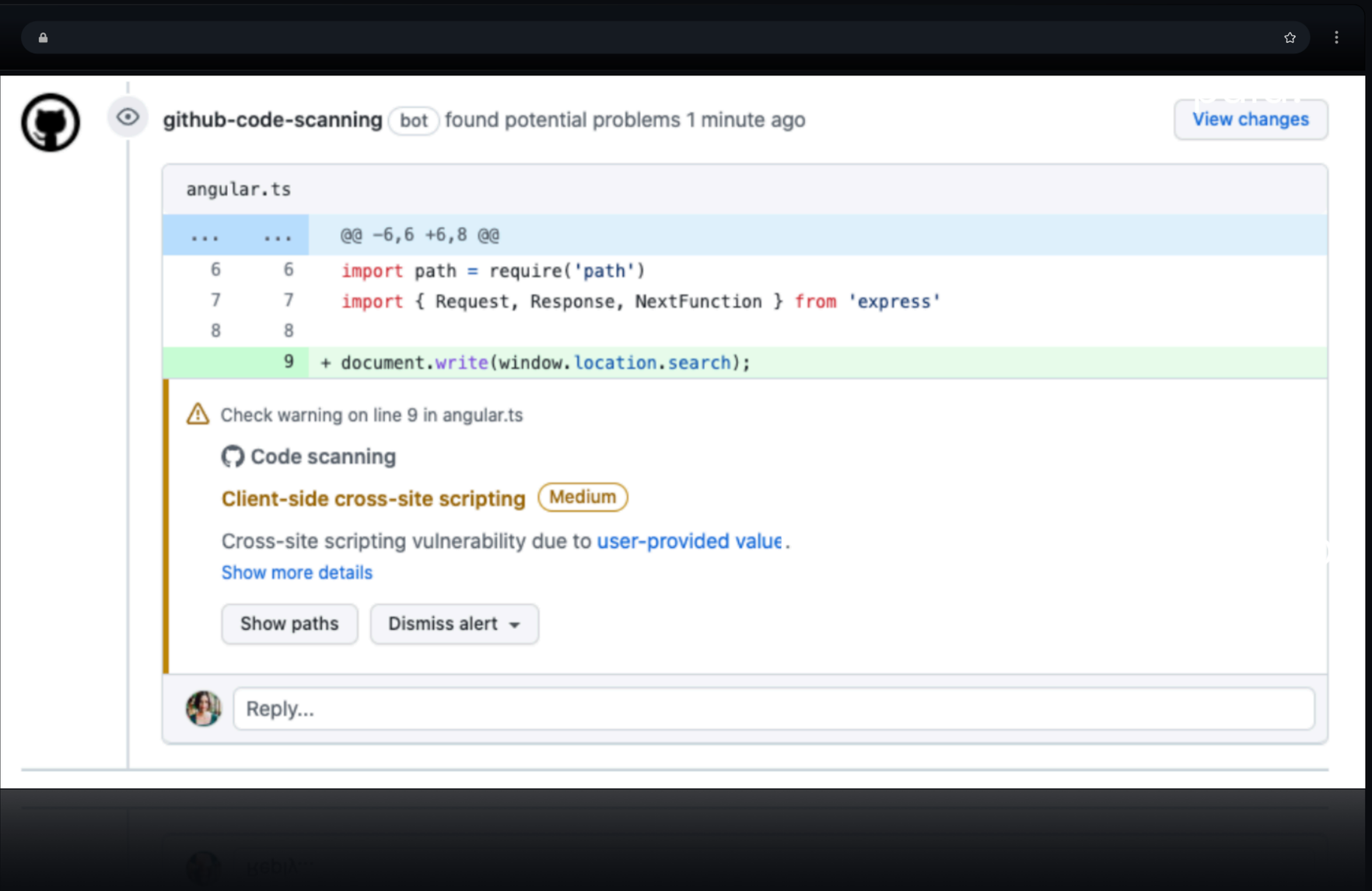

TS

Consumers

Writers

Consumers


Code scanning
Automatically detect common vulnerabilities and coding errors.
CodeQL default configuration
Languages to analyze
Detected on this repository.
JavaScript
Ruby
Query suites
Set of queries run in the analysis.
default
Events
These events will trigger a new scan.
On push and pull requests to main and 1 protected branch.
Cancel
Enable CodeQL



- Comments in your PR
- Integrated in your existing SDLC
- Act just as your usual peer reviewer
- Documentation attached with remediation advice

Writers

Conclusion

- Automated, repeatable
- Included in my SDLC
- I can read it, I can learn
- Bonus: Community-driven

To know more

- codeql.com
- securitylab.github.com
- booth #G17

Thank you