Satellite

INDIA 2021

From Right to Left

Security and Secure Development

Nickolas Means

Director of Engineering, Supply Chain Security

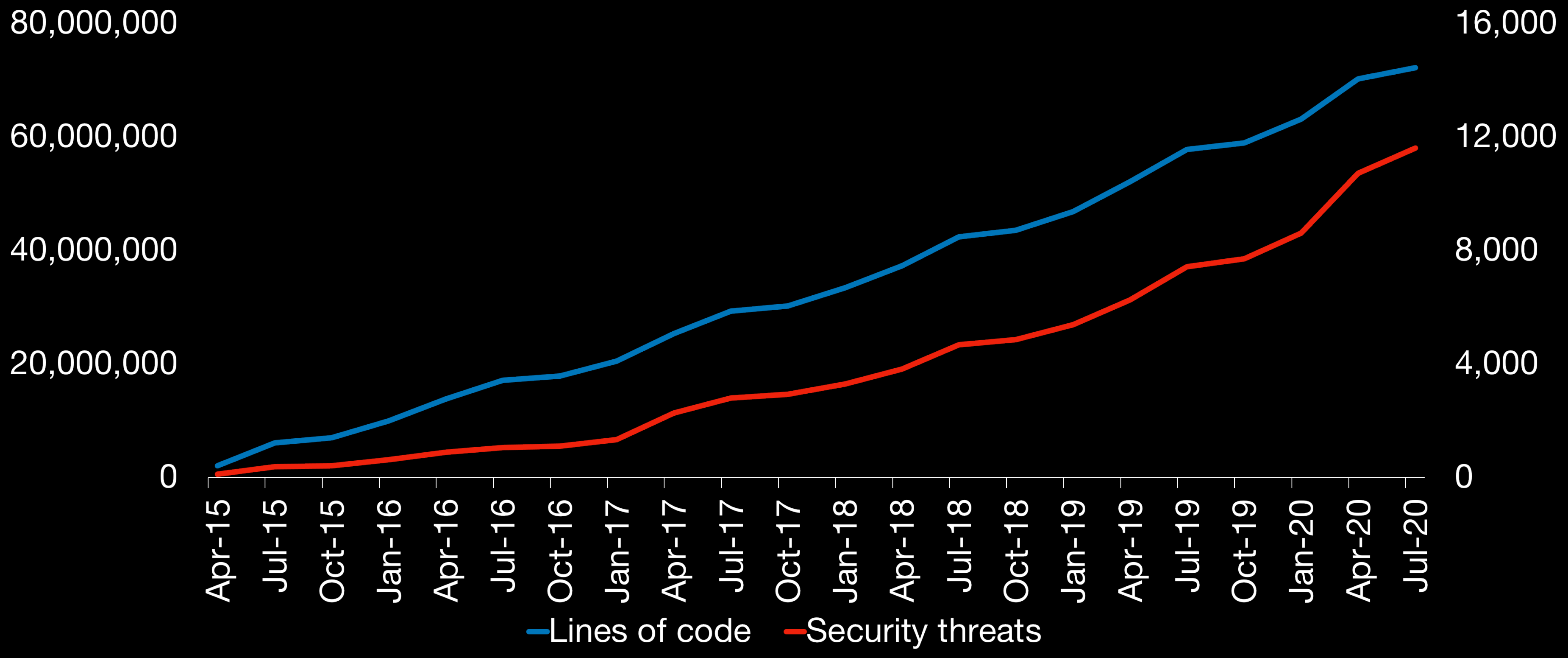
Solorigate

83%

Of applications have at least one security vulnerability.

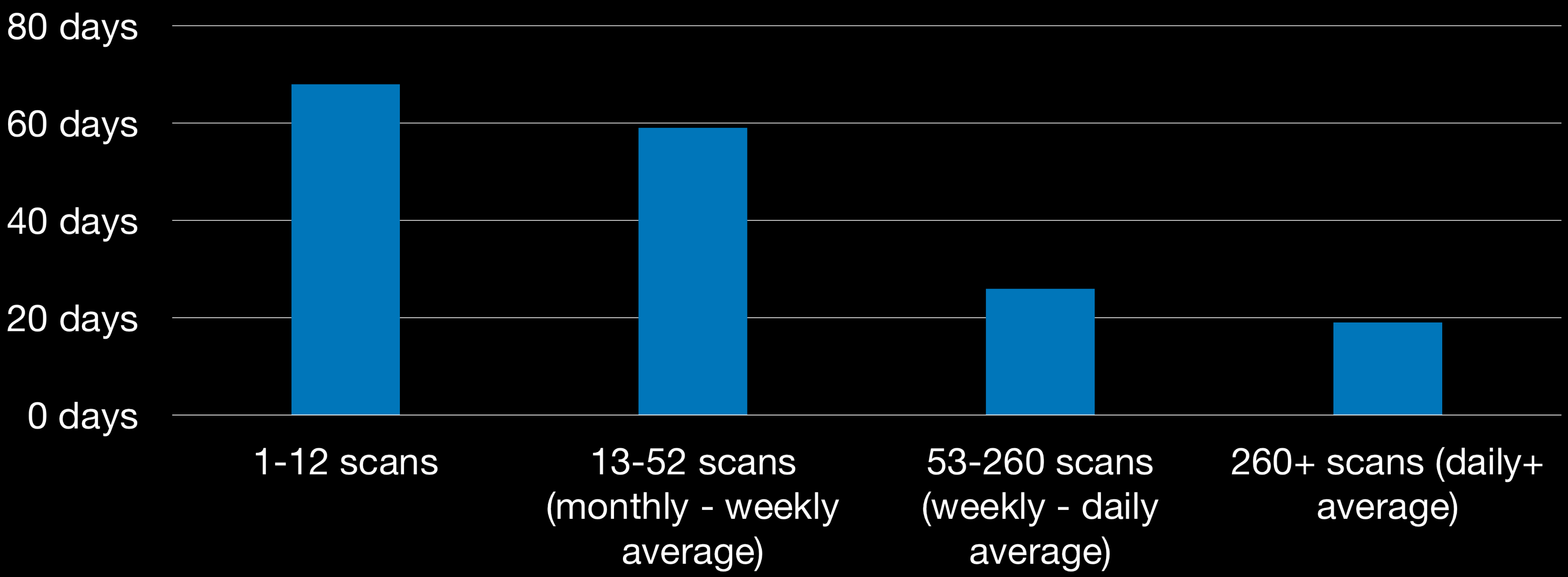
Source: Veracode State of Software Security Vol 10

Potential vulnerabilities found in source code scales with lines of code written



Source: State of the Octoverse 2020

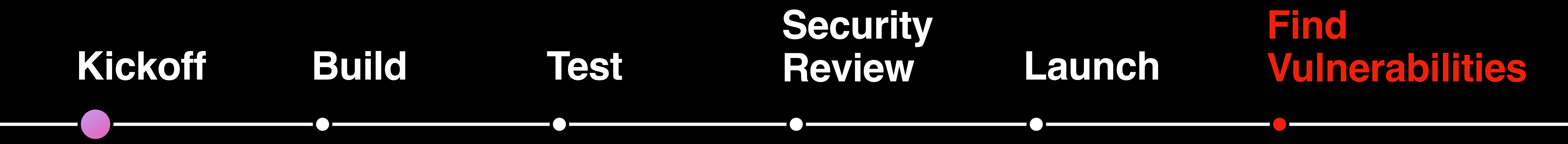
Mean time to remediate goes down when you adopt DevSecOps practices and scan more frequently



Source: State of the Octoverse 2020

Shift Left on Security

Feature Timeline



Kickoff

Build

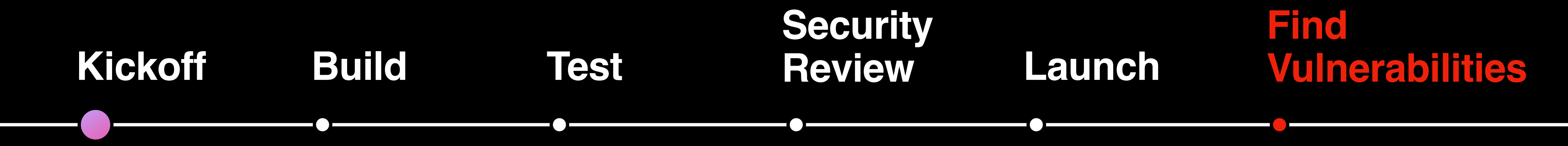
Test

Security Review

Launch

Find Vulnerabilities

Shifted Left Timeline



Kickoff

Build

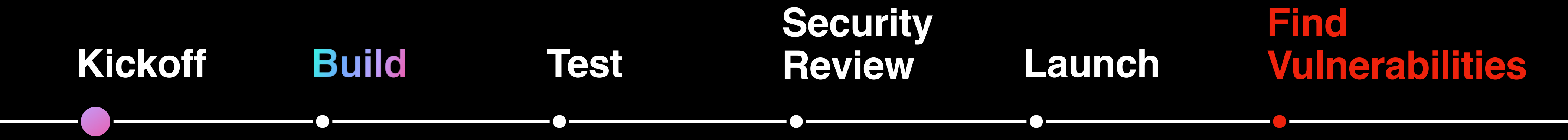
Test

Security Review

Launch

Find Vulnerabilities

Shifted Left Timeline



Kickoff

Build

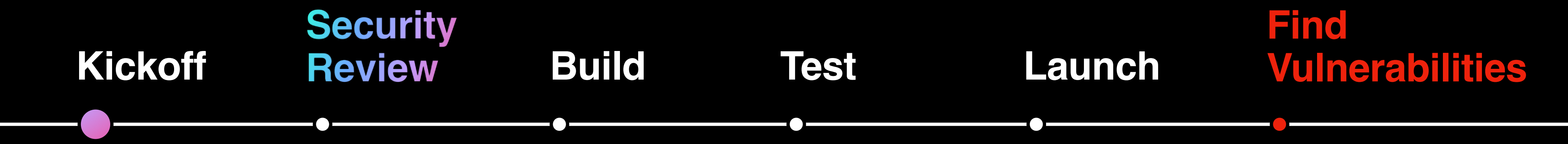
Test

Security Review

Launch

Find Vulnerabilities

Shifted Left Timeline



Kickoff

Security Review

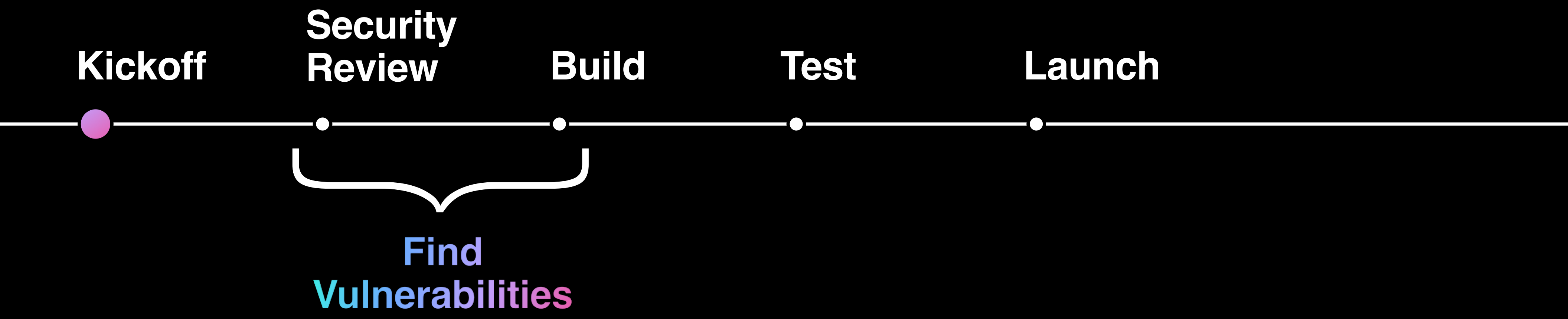
Build

Test

Launch

Find Vulnerabilities

Shifted Left Timeline



Kickoff

Security Review

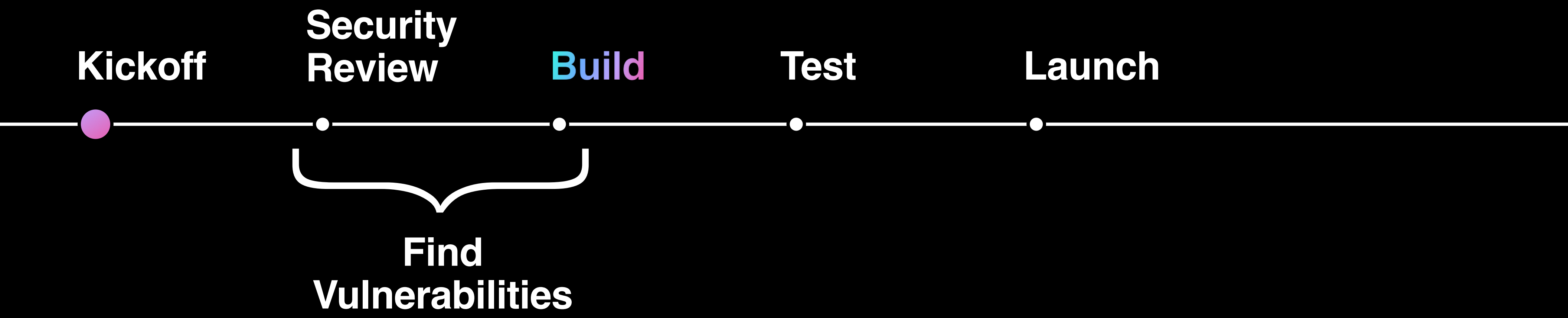
Build

Test

Launch

Find Vulnerabilities

Shifted Left Timeline



GitHub Advanced Security

Secure
Dependencies

Secure
Code

Secure
Secrets

GitHub Advanced Security

Secure Dependencies

Secure Code

Secure Secrets

Secure Dependencies

Dependabot

Keep your dependencies up to date with automated pull requests

Dependency Review

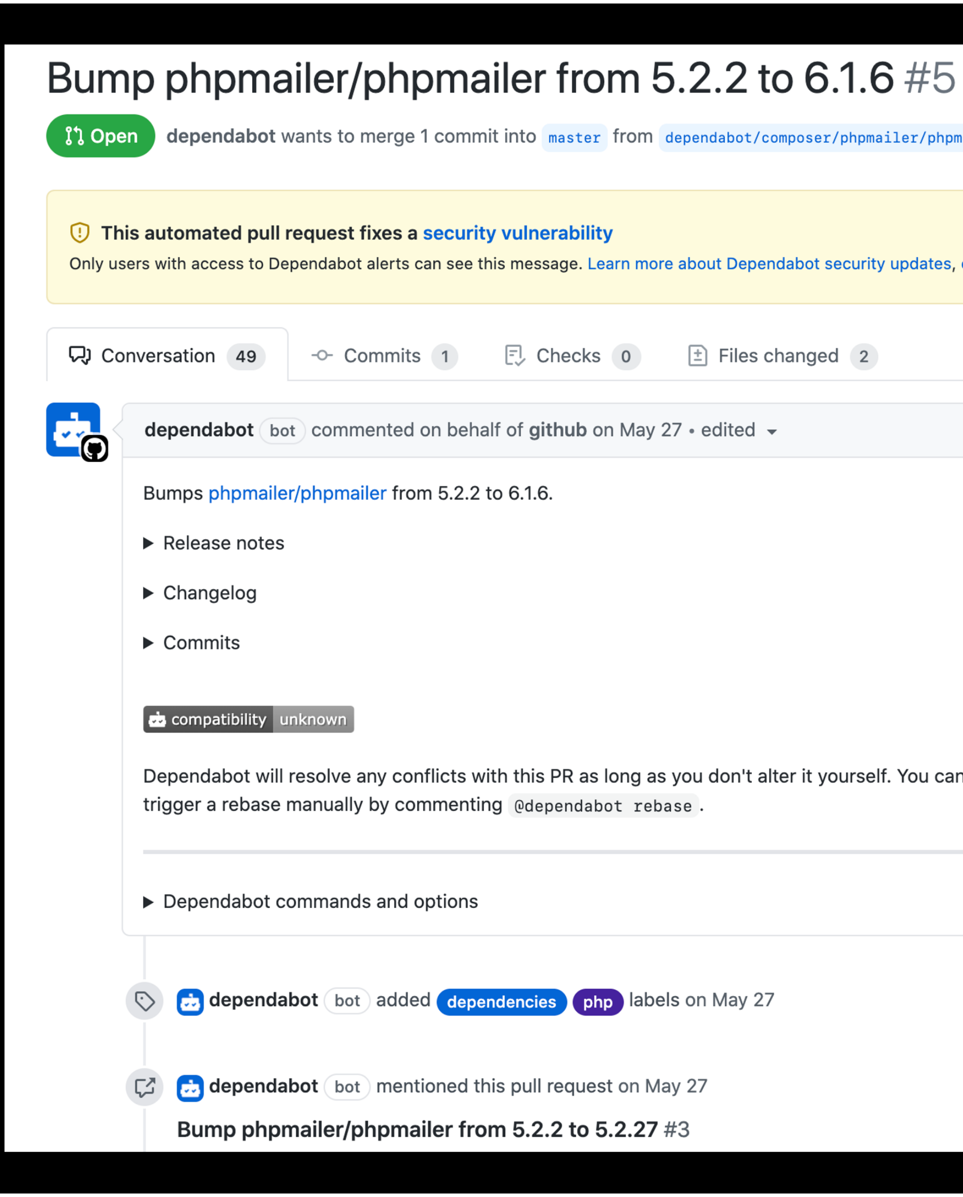
Empower code reviewers with insights on dependency changes in a pull request

Dependency Graph

Understand what software you depend on

Dependabot

- Alerts you to vulnerable dependencies
- Generates automatic pull requests to fix vulnerable or out of date dependencies
- Repositories w/ Dependabot enabled fix vulnerabilities 1.4x faster



Bump phpmailer/phpmailer from 5.2.2 to 6.1.6 #5

Open dependabot wants to merge 1 commit into `master` from `dependabot/composer/phpmailer/phpm`

This automated pull request fixes a security vulnerability

Only users with access to Dependabot alerts can see this message. Learn more about Dependabot security updates,

dependabot bot commented on behalf of github on May 27 • edited

Bumps phpmailer/phpmailer from 5.2.2 to 6.1.6.

- ▶ Release notes
- ▶ Changelog
- ▶ Commits

Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can trigger a rebase manually by commenting `@dependabot rebase`.

- ▶ Dependabot commands and options

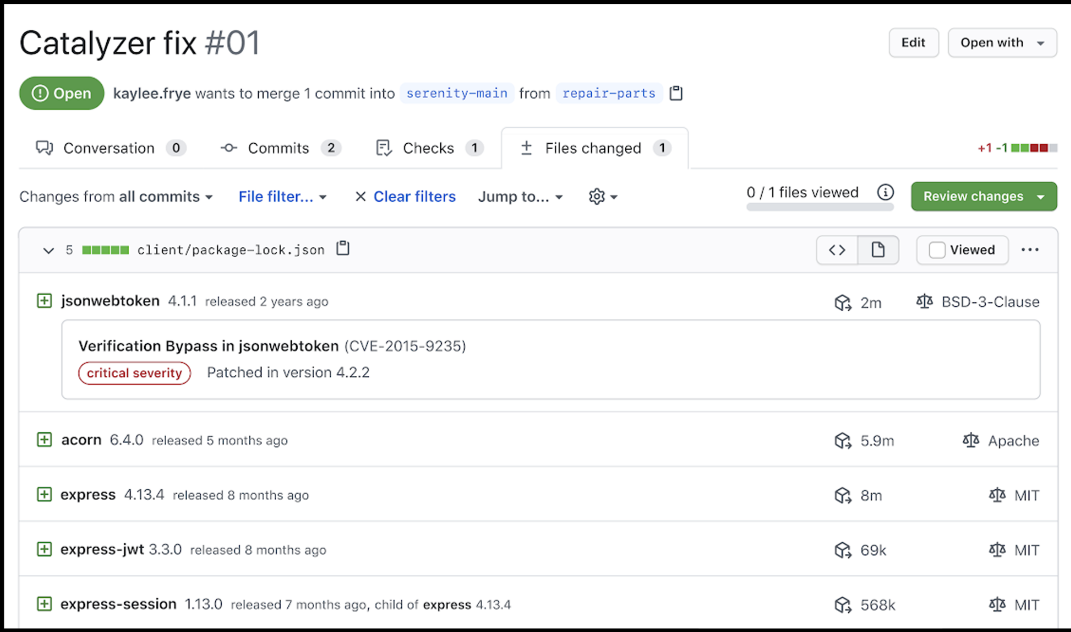
dependabot bot added dependencies php labels on May 27

dependabot bot mentioned this pull request on May 27

Bump phpmailer/phpmailer from 5.2.2 to 5.2.27 #3

Dependency Review

- Helps code reviewers visualize dependency changes and prevents vulnerable dependencies from hitting production



Catalyzer fix #01

Open kaylee.frye wants to merge 1 commit into `serenity-main` from `repair-parts`

5 `client/package-lock.json`

jsonwebtoken 4.1.1 released 2 years ago — 2m — BSD-3-Clause

Verification Bypass in jsonwebtoken (CVE-2015-9235)
critical severity — Patched in version 4.2.2

acorn 6.4.0 released 5 months ago — 5.9m — Apache

express 4.13.4 released 8 months ago — 8m — MIT

express-jwt 3.3.0 released 8 months ago — 69k — MIT

express-session 1.13.0 released 7 months ago, child of express 4.13.4 — 568k — MIT

Dependency Graph

Supports common package managers for .NET, Java, JavaScript, PHP, Python, and Ruby

GitHub Advanced Security

Secure Dependencies

Secure Code

Secure Secrets

Secure Code

Code Scanning

Developer experience for running static analysis security tests (SAST)

CodeQL

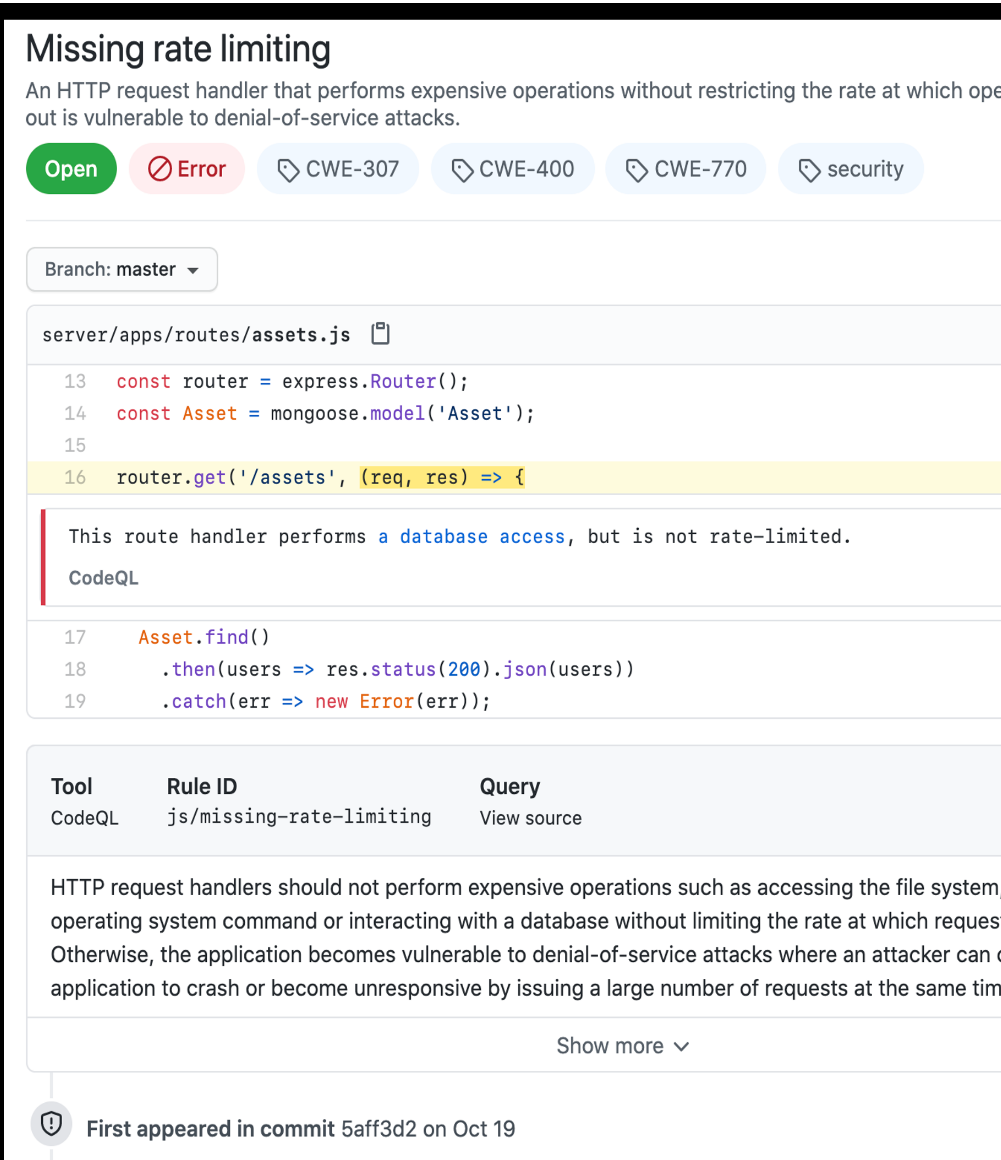
GitHub's semantic code engine finds security vulnerabilities

3rd Party Analyzers

Extend the built-in analysis with any standards compliant SAST tooling

Code Scanning

- Surfaces code vulnerabilities in developer workflows like pull requests
- Lowest friction way to harness the power of CodeQL and 3rd party analysis tools
- Integrates with Actions and 3rd party CI/CD systems



Missing rate limiting

An HTTP request handler that performs expensive operations without restricting the rate at which ope
out is vulnerable to denial-of-service attacks.

server/apps/routes/assets.js

```
const router = express.Router();
const Asset = mongoose.model('Asset');

router.get('/assets', (req, res) => {
```

This route handler performs a database access, but is not rate-limited.

CodeQL

```
  Asset.find()
    .then(users => res.status(200).json(users))
    .catch(err => new Error(err));
```

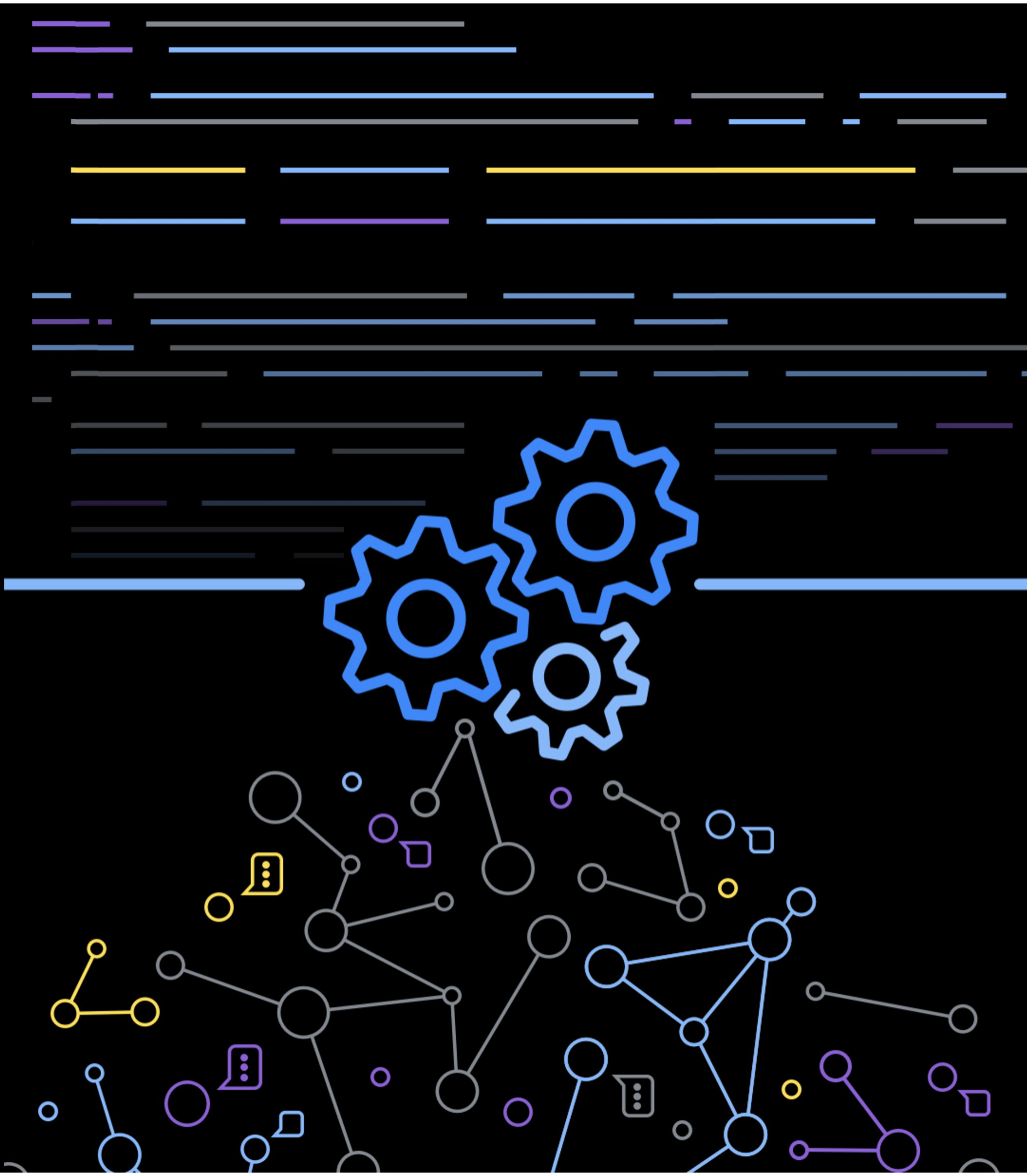
Tool	Rule ID	Query
CodeQL	js/missing-rate-limiting	View source

HTTP request handlers should not perform expensive operations such as accessing the file system
operating system command or interacting with a database without limiting the rate at which reques
Otherwise, the application becomes vulnerable to denial-of-service attacks where an attacker can
application to crash or become unresponsive by issuing a large number of requests at the same tim

First appeared in commit 5aff3d2 on Oct 19

CodeQL

- Revolutionary semantic analysis engine by GitHub
- Powered by more than 2000 open-source queries
- 24% of recent JS CVEs would have been caught



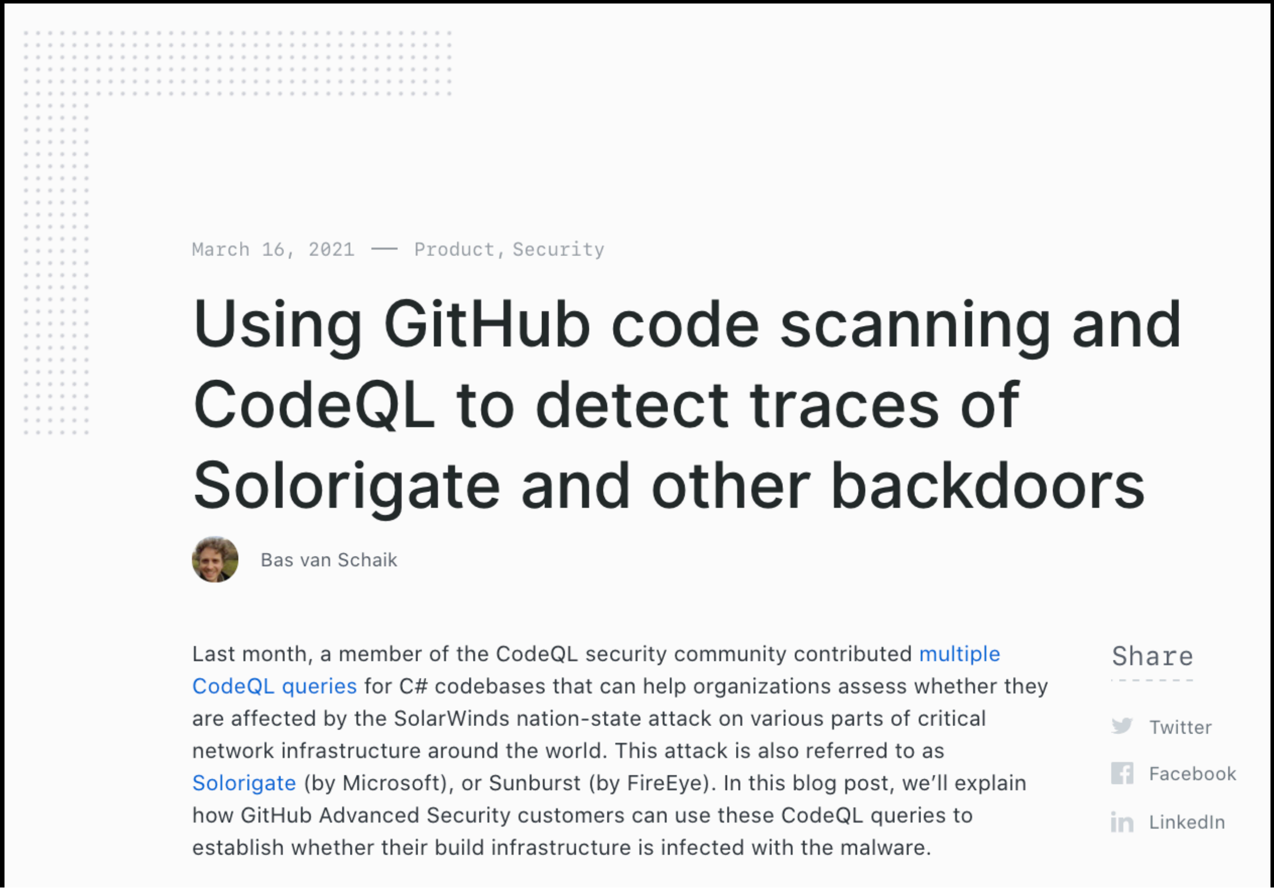
CodeQL Languages

- C
- C++
- C#
- Go
- JavaScript
- Java
- Python
- TypeScript

Queries detect 160+ CWEs

- Improper input validation
- Cross site scripting
- Improper encoding or escaping of input
- Integer overflow
- Denial of service
- Uncontrolled resource consumption

CodeQL and Solorigate



March 16, 2021 — Product, Security

Using GitHub code scanning and CodeQL to detect traces of Solorigate and other backdoors

Bas van Schaik

Last month, a member of the CodeQL security community contributed multiple CodeQL queries for C# codebases that can help organizations assess whether they are affected by the SolarWinds nation-state attack on various parts of critical network infrastructure around the world. This attack is also referred to as Solorigate (by Microsoft), or Sunburst (by FireEye). In this blog post, we'll explain how GitHub Advanced Security customers can use these CodeQL queries to establish whether their build infrastructure is infected with the malware.

3rd Party Analyzers

- Scan code, Docker containers, and configuration for security issues
- View results in Code Scanning, alongside results from CodeQL

42crunch

anchore

BRAKEMAN

CHECKMARX

{/code.scan}®

CODACY

FORTIFY®

ShiftLeft

snyk

trivy

VERACODE

XANITIZER
... because security matters

GitHub Advanced Security

Secure Dependencies

Secure Code

Secure Secrets

Secure Secrets

Secret Scanning for Public Repositories

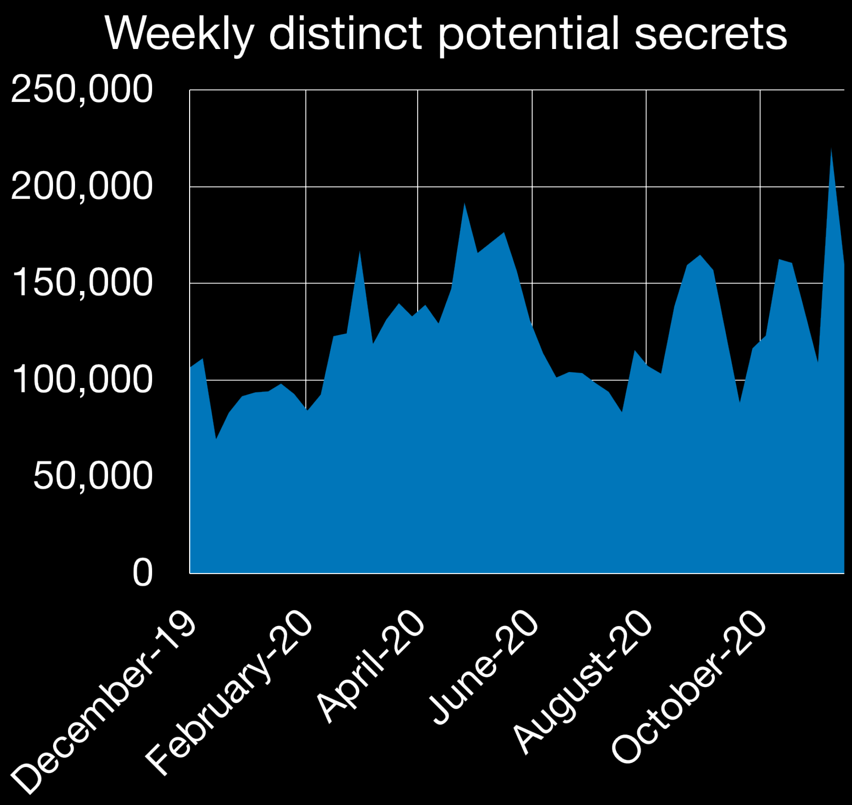
Detects secrets in open-source code and gets them reviewed/ revoked automatically

Secret Scanning for Private Repositories

Detects secrets in private code and helps developers review and revoke manually

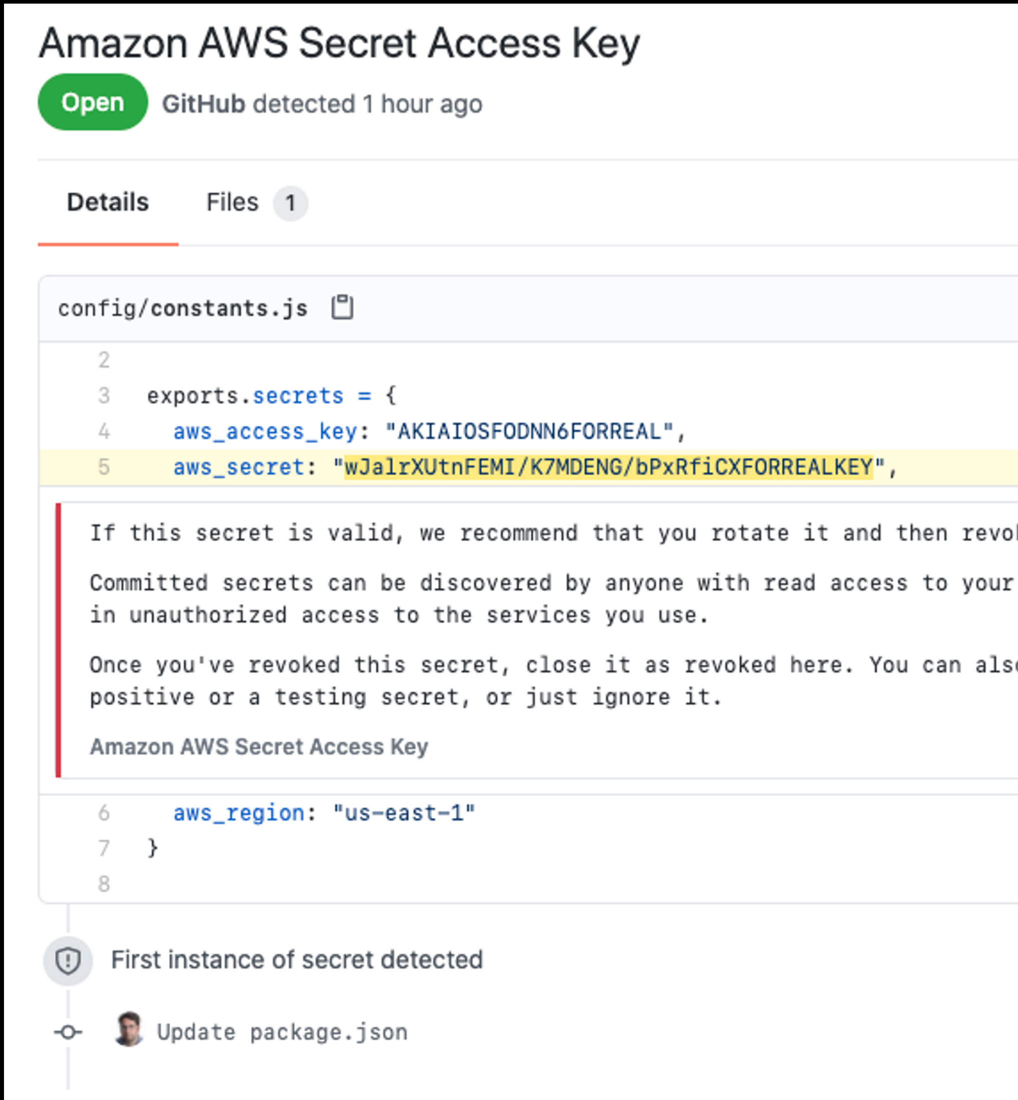
Secret Scanning (public)

- Free: enabled by default for all public repositories
- Scans incoming commits to open source for potential secrets
- Sends results to partners for automatic remediation



Secret Scanning (Private)

- Scans full repository history for potential security leaks
- Allows you to review and triage them right on GitHub



Amazon AWS Secret Access Key

GitHub detected 1 hour ago

config/constants.js

```

exports.secrets = {
  aws_access_key: "AKIAIOSFODNN6FORREAL",
  aws_secret: "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",
```

```
If this secret is valid, we recommend that you rotate it and then revol

Committed secrets can be discovered by anyone with read access to your
in unauthorized access to the services you use.

Once you've revoked this secret, close it as revoked here. You can als
positive or a testing secret, or just ignore it.
```

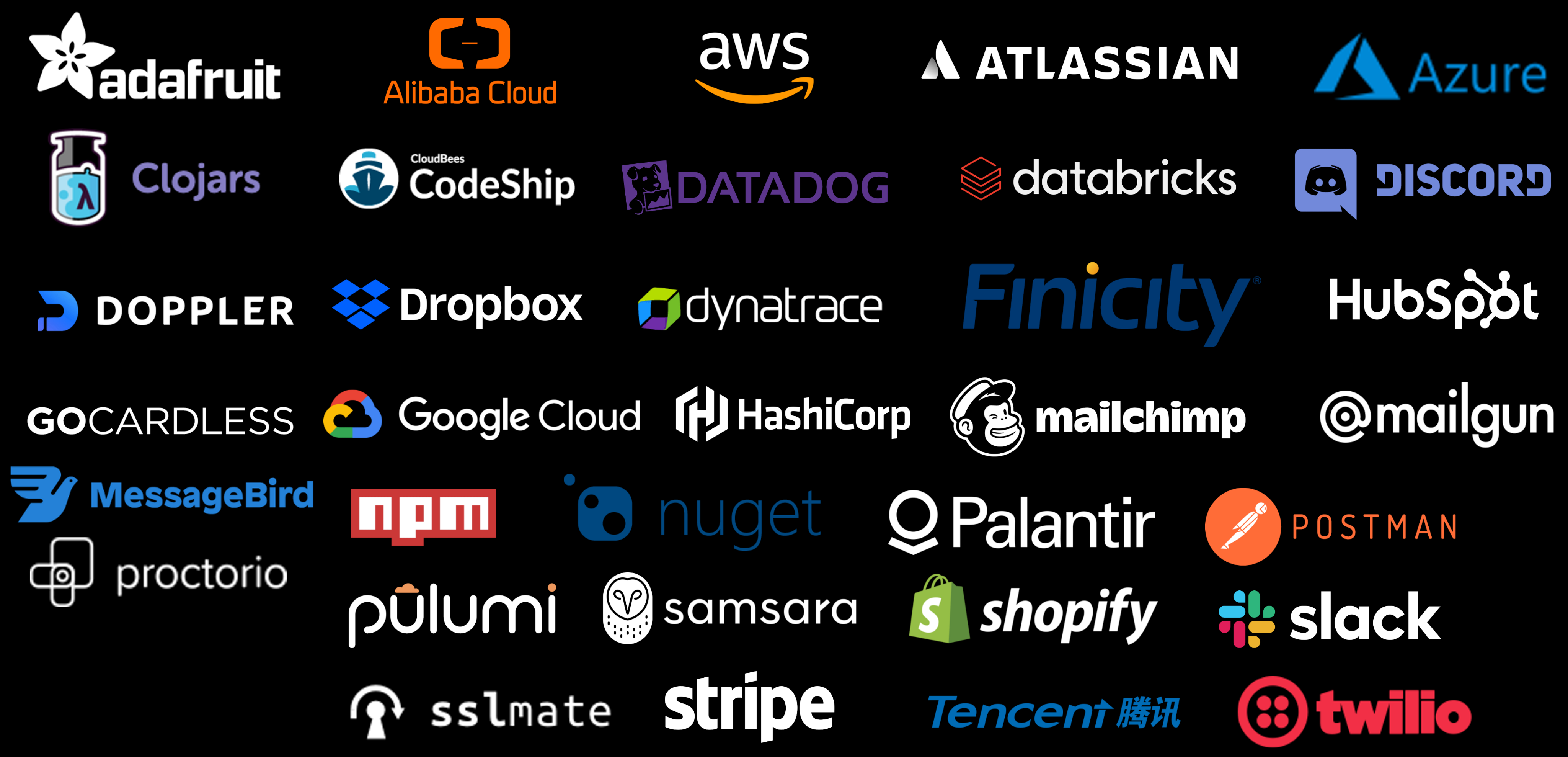
Amazon AWS Secret Access Key

```
  aws_region: "us-east-1"
}

```

First instance of secret detected

Update package.json


adafruit
Alibaba Cloud
aws
ATLASSIAN
Azure
Clojars
CloudBees
CodeShip
DATADOG
databricks
DISCORD
DOPPLER
Dropbox
dynatrace
Finicity
HubSpot
GOCARDLESS
Google Cloud
HashiCorp
mailchimp
@mailgun
MessageBird
npm
nuget
Palantir
POSTMAN
proctorio
pulumi
samsara
shopify
slack
sslmate
stripe
Tencent 腾讯
twilio

GitHub Advanced Security

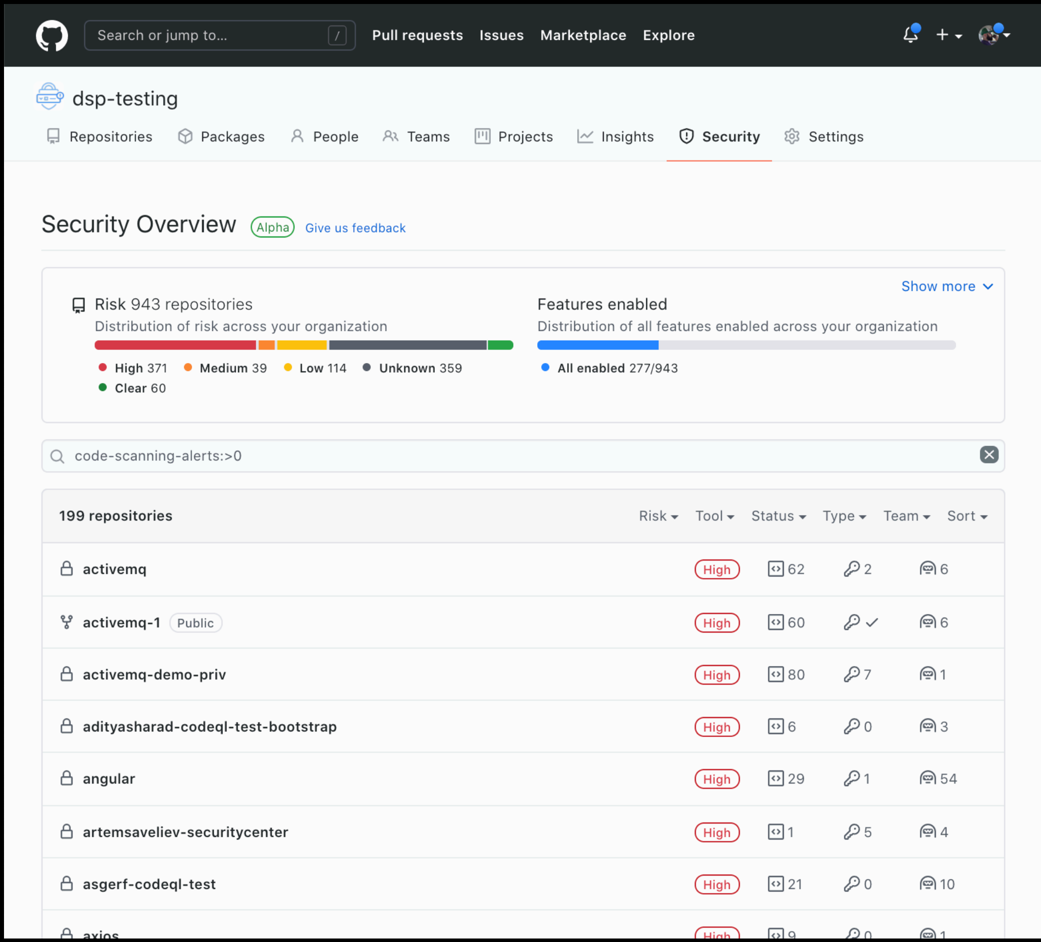
Secure Dependencies

Secure Code

Secure Secrets

Security Overview

- Displays security feature enablement and alert counts across Secure Dependencies, Code, and Secrets
- Available in Beta on GitHub Enterprise Cloud accounts



dsp-testing

Security Overview Alpha Give us feedback

Risk 943 repositories
Distribution of risk across your organization

● High 371 ● Medium 39 ● Low 114 ● Unknown 359 ● Clear 60

Features enabled
Distribution of all features enabled across your organization

● All enabled 277/943

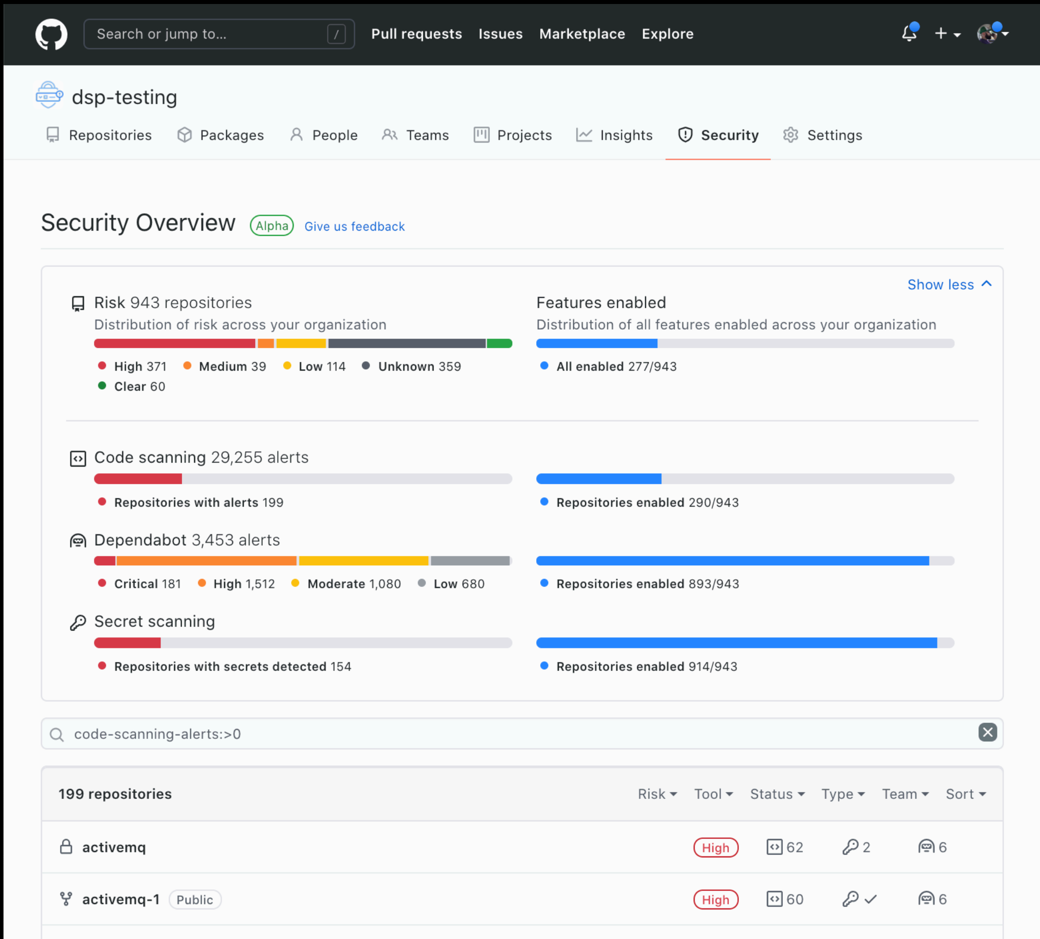
code-scanning-alerts:>0

199 repositories

activemq	High	62	2	6
activemq-1 Public	High	60	✓	6
activemq-demo-priv	High	80	7	1
adityasharad-codeql-test-bootstrap	High	6	0	3
angular	High	29	1	54
artemsaveliev-securitycenter	High	1	5	4
asgerf-codeql-test	High	21	0	10
axios	High	9	0	1

Security Overview

- Displays security feature enablement and alert counts across Secure Dependencies, Code, and Secrets
- Available in Beta on GitHub Enterprise Cloud accounts



Security Overview Alpha Give us feedback

Show less

Risk 943 repositories

Distribution of risk across your organization

● High 371 ● Medium 39 ● Low 114 ● Unknown 359 ● Clear 60

Features enabled

Distribution of all features enabled across your organization

● All enabled 277/943

Code scanning 29,255 alerts

● Repositories with alerts 199

● Repositories enabled 290/943

Dependabot 3,453 alerts

● Critical 181 ● High 1,512 ● Moderate 1,080 ● Low 680

● Repositories enabled 893/943

Secret scanning

● Repositories with secrets detected 154

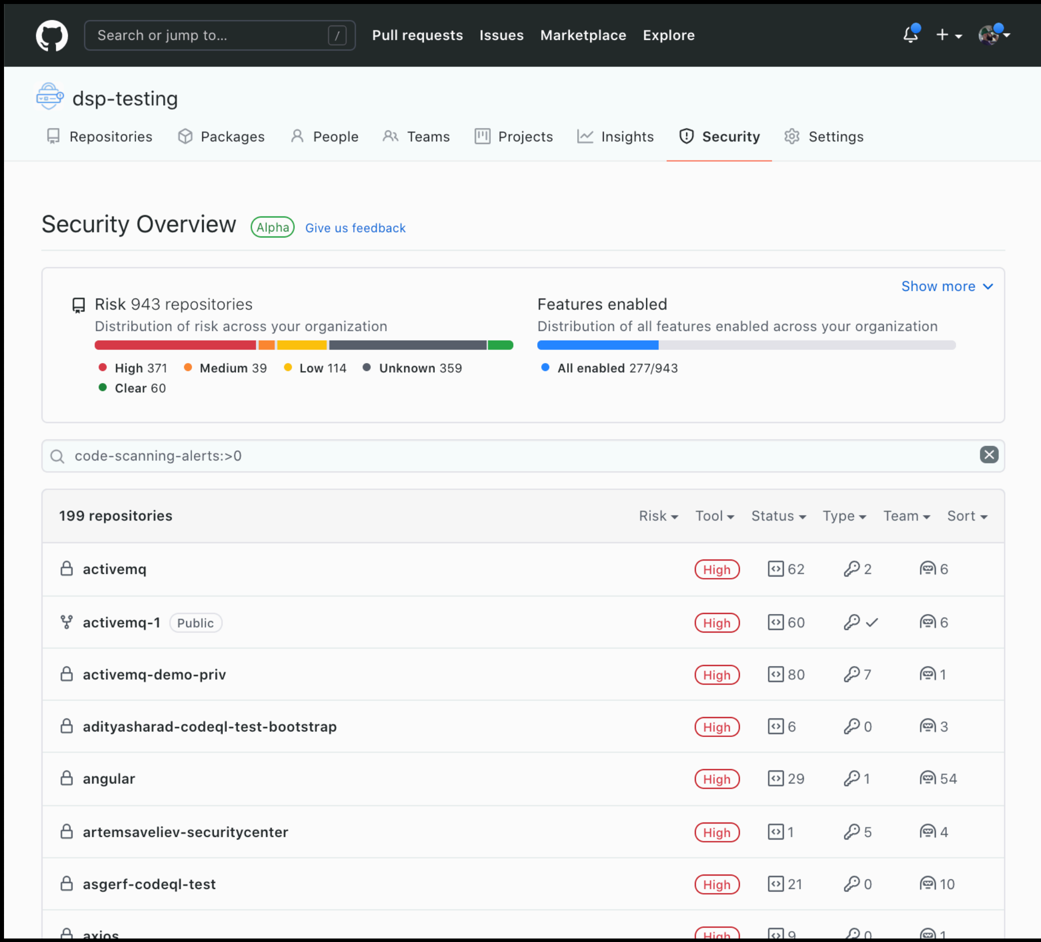
● Repositories enabled 914/943

code-scanning-alerts:>0

199 repositories	Risk	Tool	Status	Type	Team	Sort
activemq	High	62	2	6		
activemq-1 Public	High	60	✓	6		

Security Overview

- Displays security feature enablement and alert counts across Secure Dependencies, Code, and Secrets
- Available in Beta on GitHub Enterprise Cloud accounts



Security Overview

Alpha Give us feedback

Show more

Risk 943 repositories
Distribution of risk across your organization

● High 371 ● Medium 39 ● Low 114 ● Unknown 359
● Clear 60

Features enabled
Distribution of all features enabled across your organization

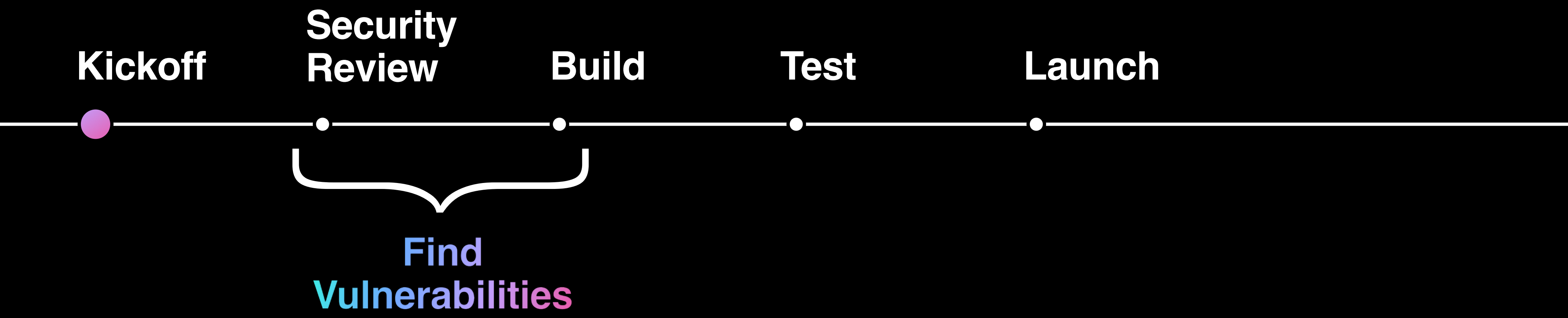
● All enabled 277/943

code-scanning-alerts:>0

199 repositories — Risk ▾ Tool ▾ Status ▾ Type ▾ Team ▾ Sort ▾

activemq	High	62	2	6
activemq-1 Public	High	60	✓	6
activemq-demo-priv	High	80	7	1
adityasharad-codeql-test-bootstrap	High	6	0	3
angular	High	29	1	54
artemsaveliev-securitycenter	High	1	5	4
asgerf-codeql-test	High	21	0	10
axios	High	9	0	1

How to Shift Left?



Kickoff

Security Review

Build

Test

Launch

Find Vulnerabilities

Want to learn more?

https://github.com/features/security