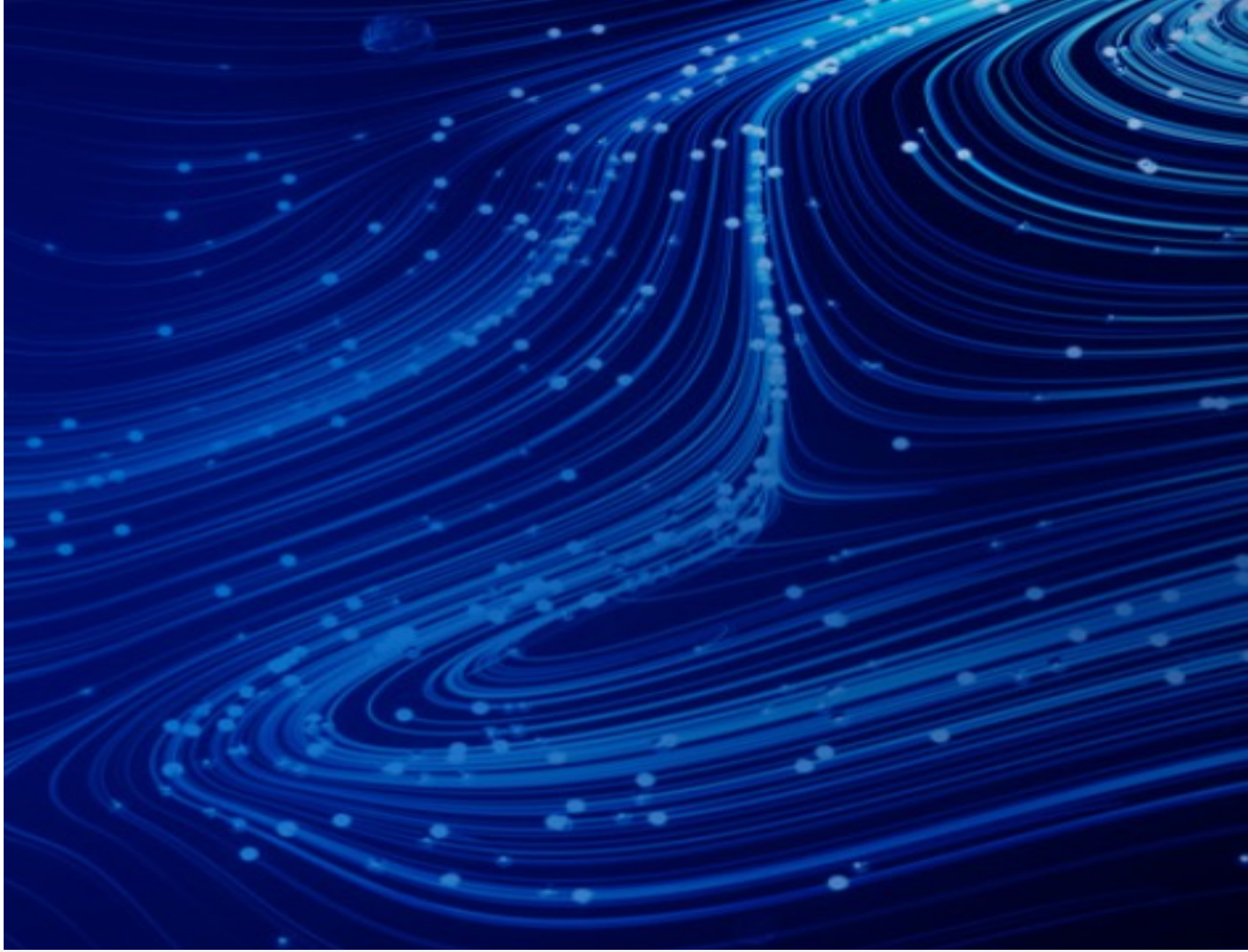
Cognizant
Microsoft Business Group

GitHub Advanced Security Demo

Josh Johanning | 5/11/21

Agenda

- What is GitHub Advanced Security (GHAS)
- Why GHAS
- Live Demo
- Questions

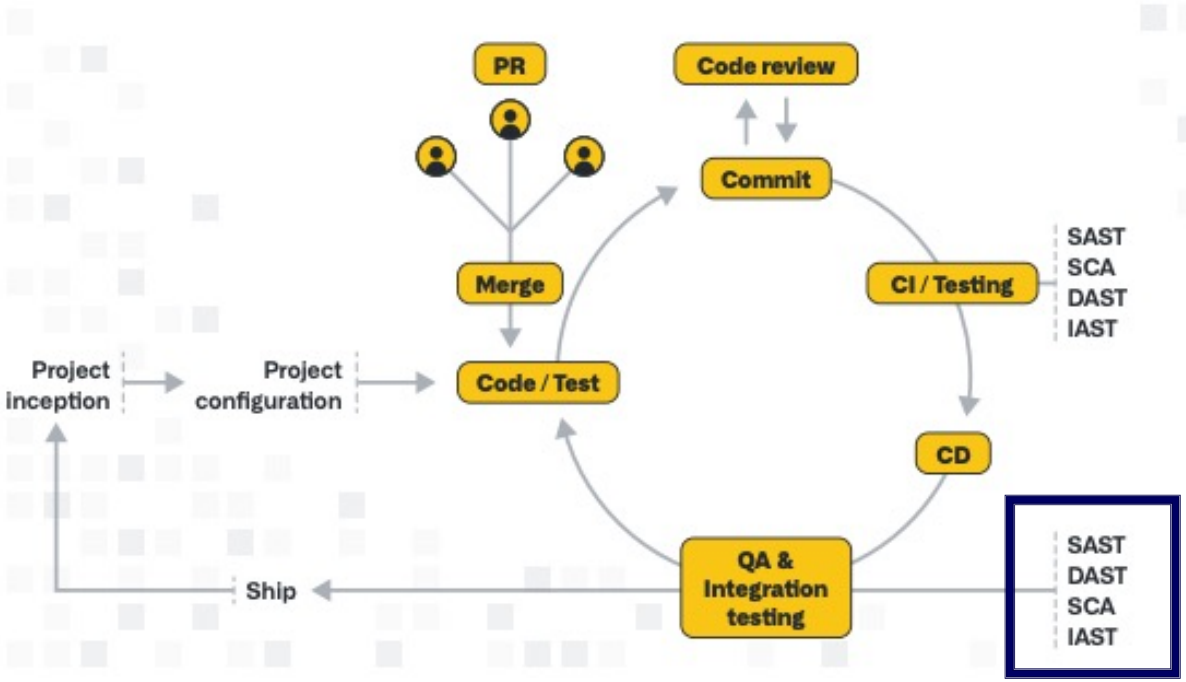


What is GitHub Advanced Security

Traditional Approach

Issues

- Security comes too late in the development process
- Scan results, if any, often have a high noise-to-signal ratio
- Manual reviews cause bottlenecks

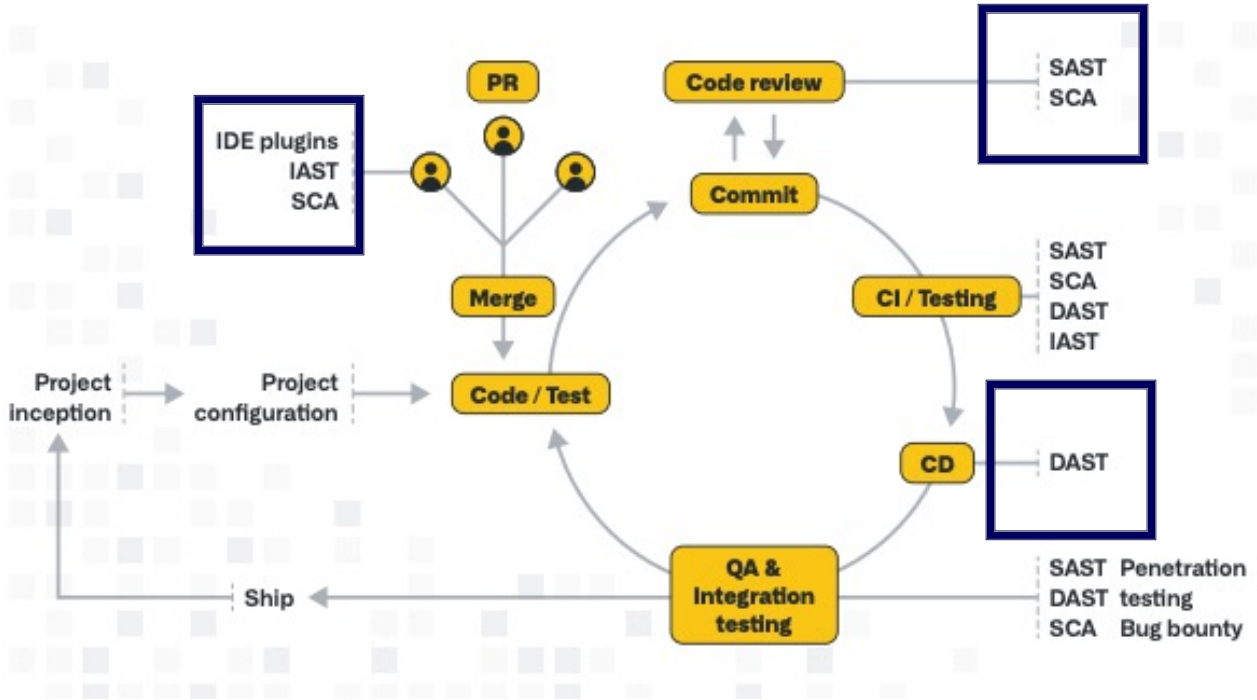


Security Audit

Targeted End to End Approach

Issues

- Integrations require a lot of upkeep
- Several disparate systems tracking results
- Security and Dev teams continue to work in solos
- Still have false positive issues
- Traditional tools fail to keep pace with the software ecosystem



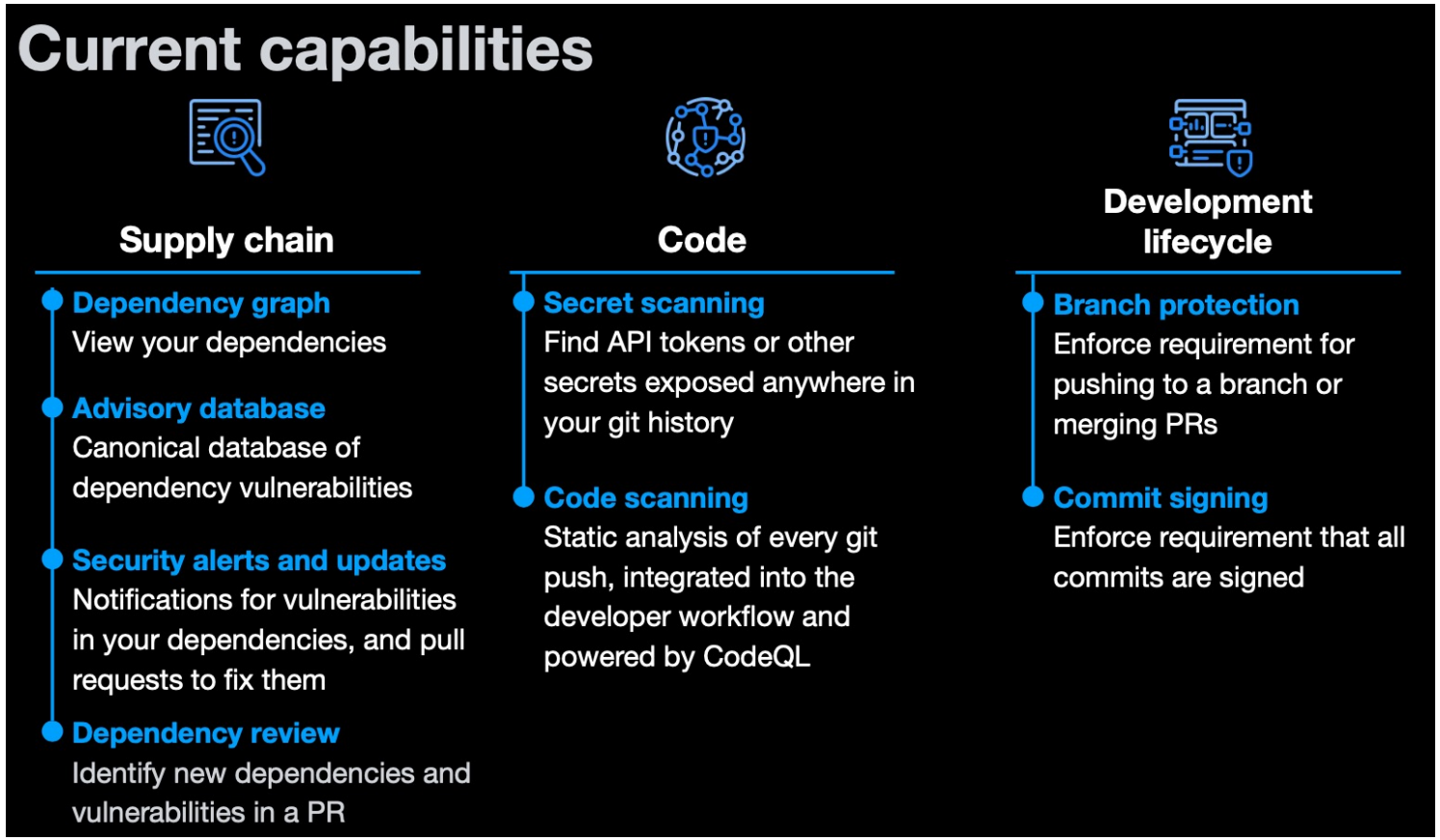
Solution?

GitHub Advanced Security Selling Points

- **Single view to track/manage security issues**
- **Find out new vulnerabilities faster – instead of finding out in CI pipeline, vulnerabilities will show even if no changes/builds are queued**
- **Security issues visible in GitHub pull requests**
- **Minimizes noise**

Shift security left – to code!

SAST
Secret Scanning
Dependencies

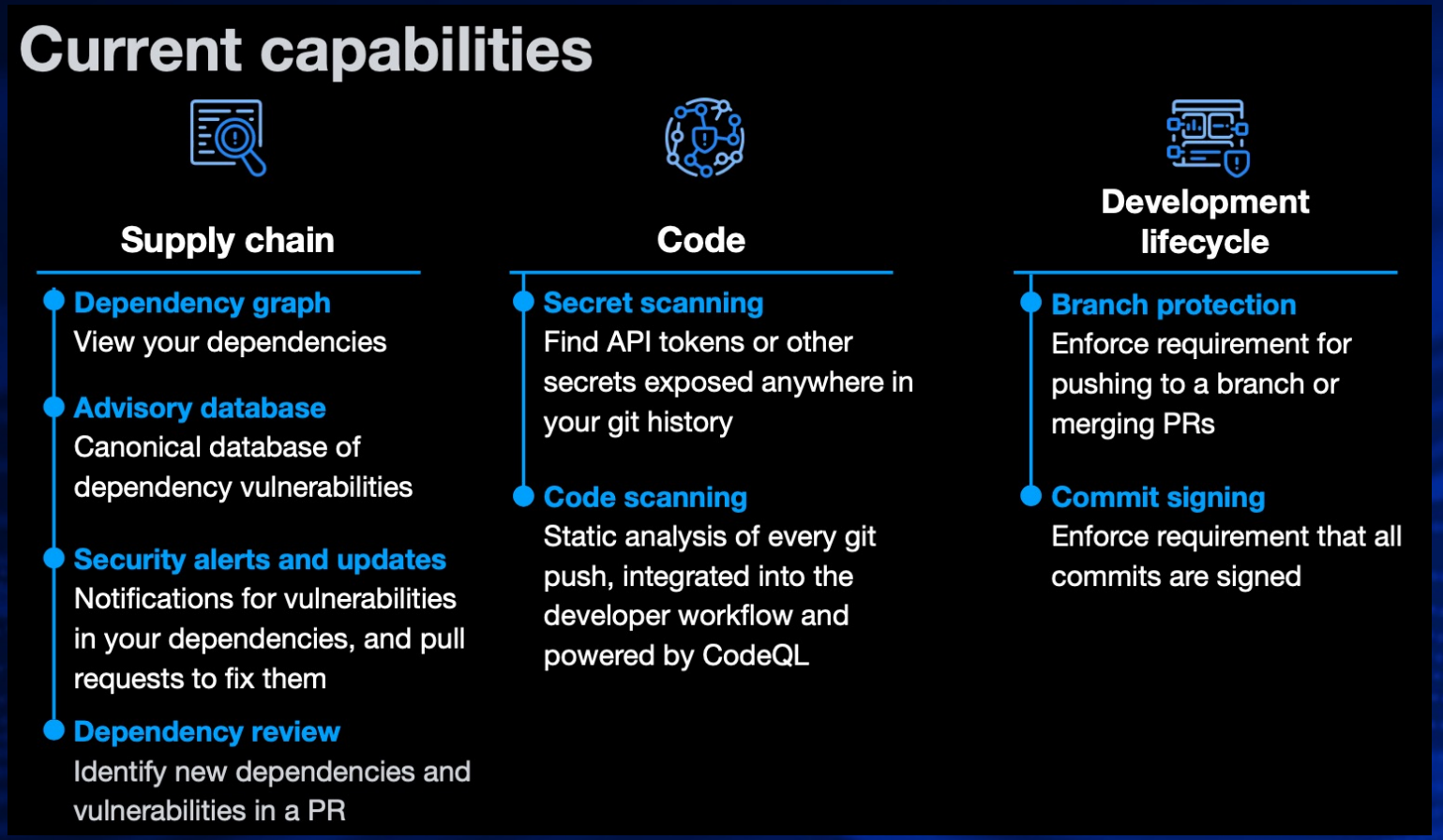


Demo

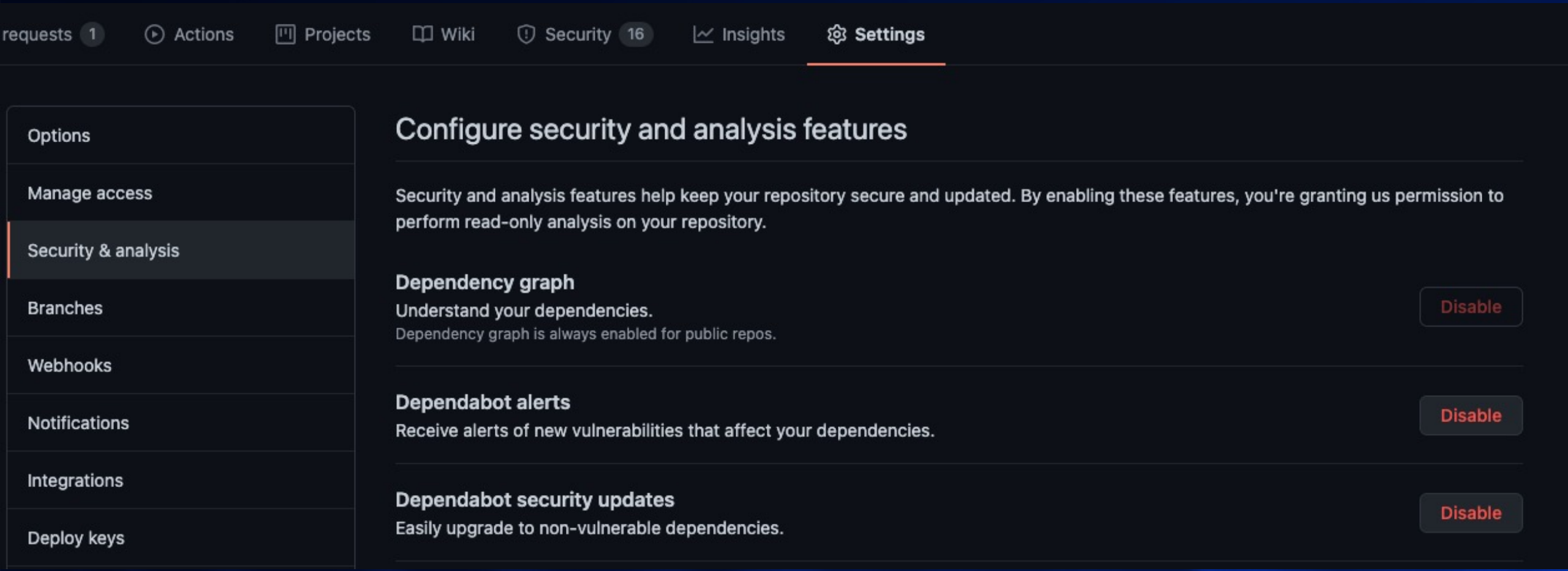
Demo Overview

Demo overview

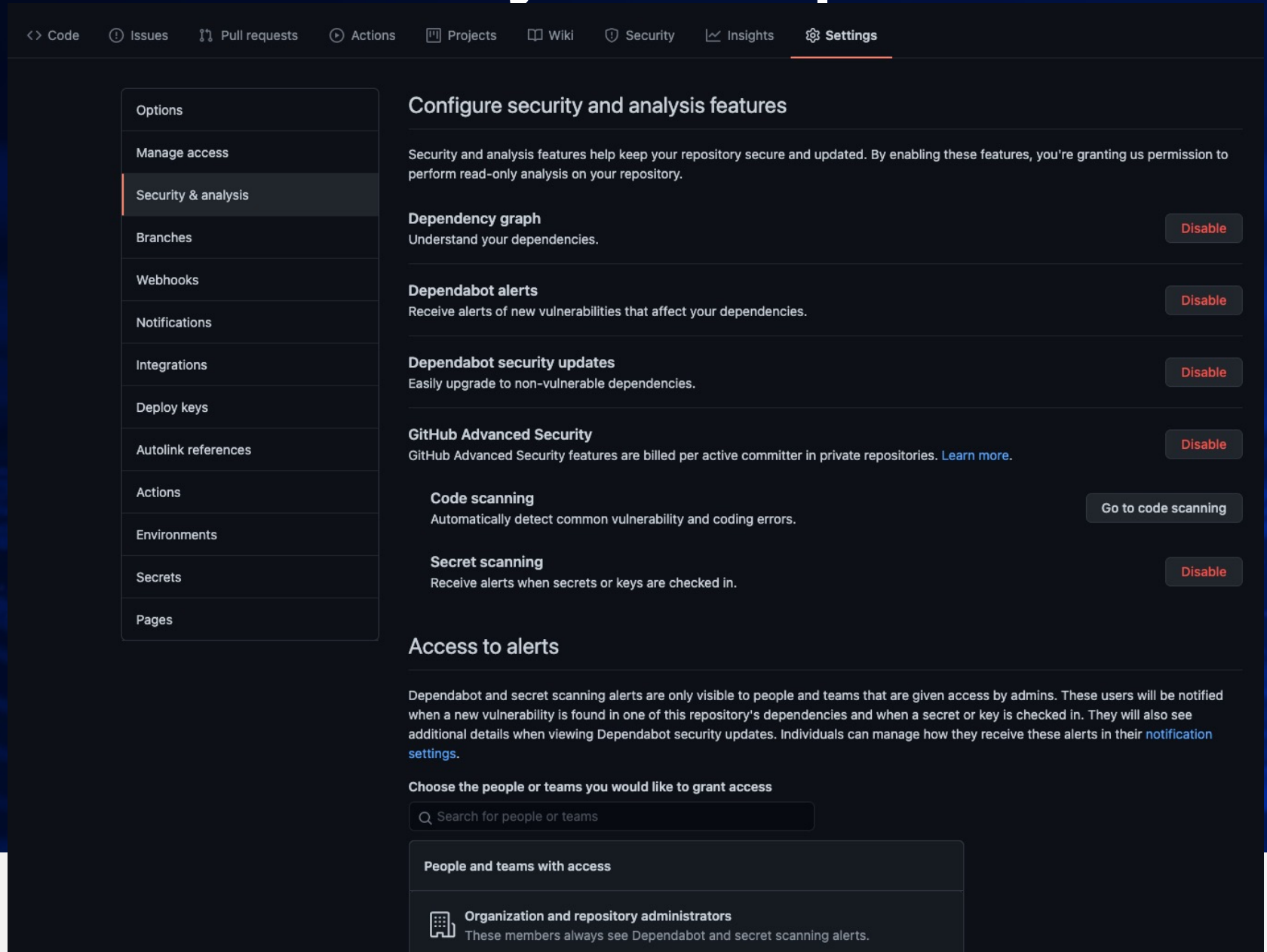
- Configure on .com public repo / Enterprise Cloud
- Secret Scanning
  - Committing code to source
  - Email and Mailchimp dashboard
  - GHEC – how it looks in there
- CodeQL
  - Existing alerts
  - Creating workflow and my workflow
  - Other partners (ie: IaaC scans)
- Dependabot
  - Security Alerts and Updates
  - Dependency Graph
  - Version Updates
  - Vulnerability Database



GitHub Advanced Security – GitHub.com

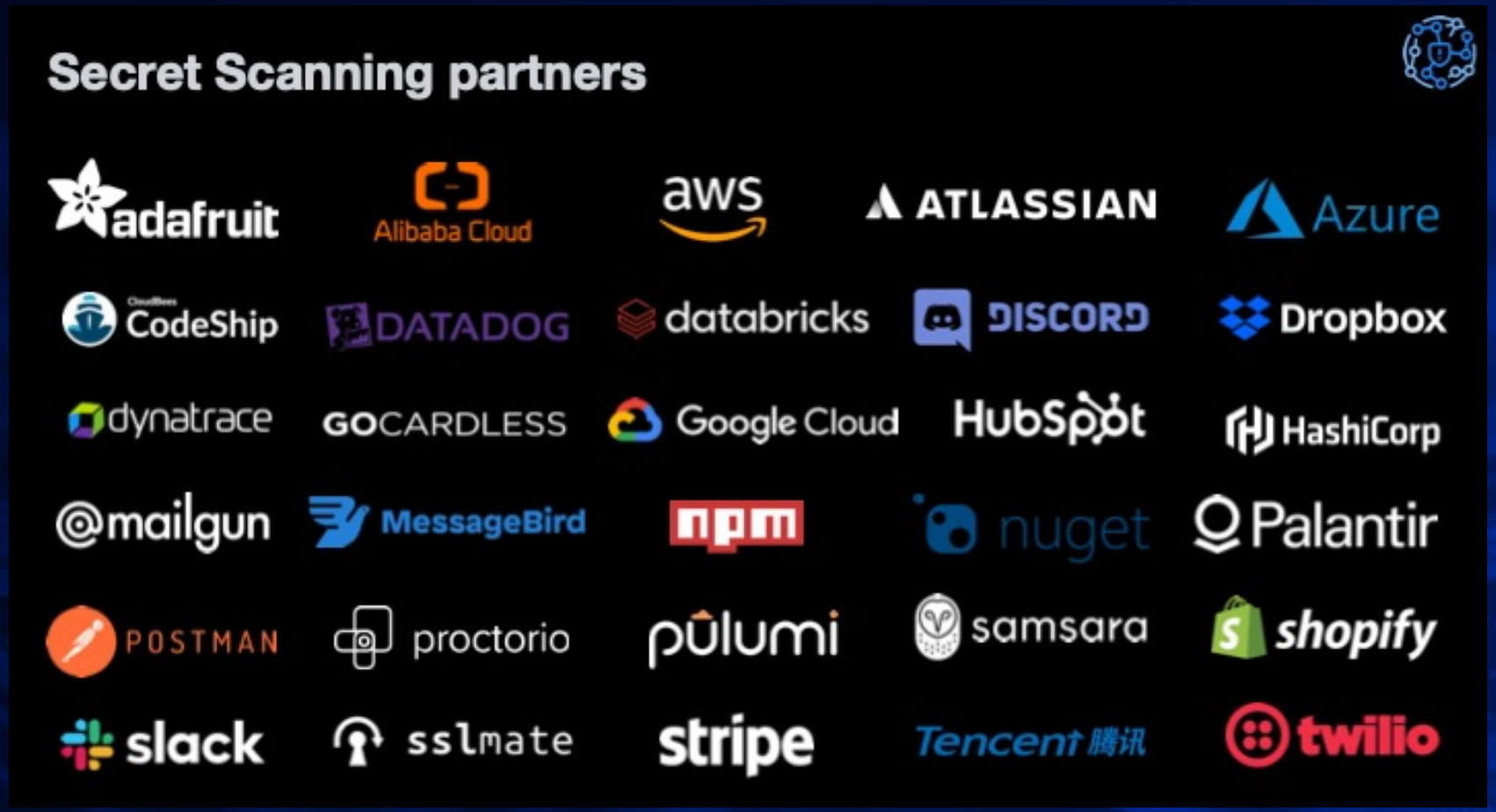


GitHub Advanced Security – Enterprise Cloud



Secret Scanning

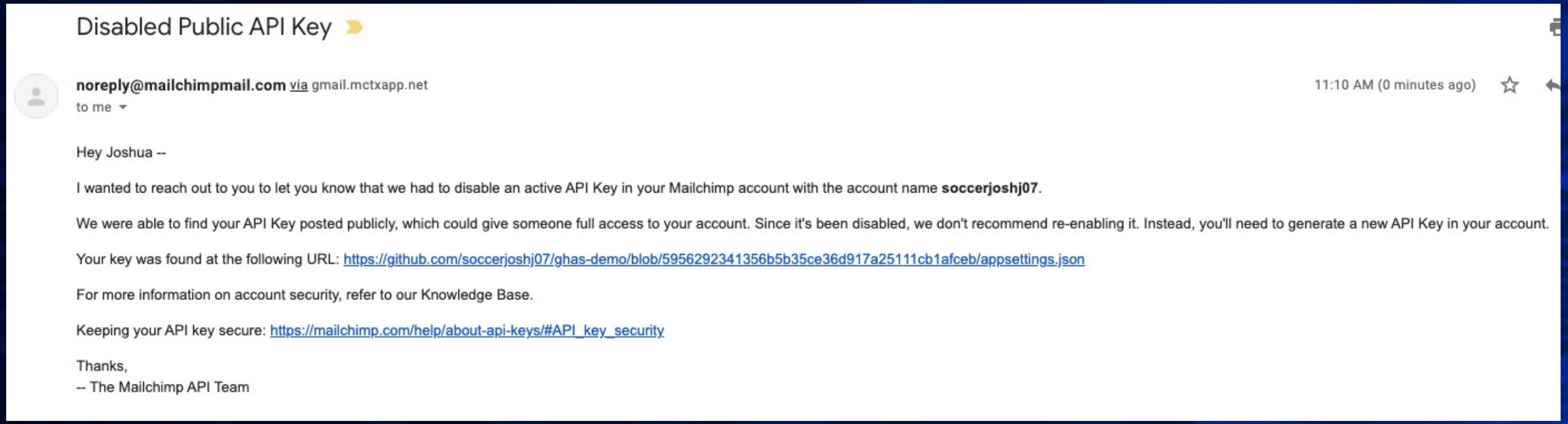
Partners



https://docs.github.com/en/enterprise-server@3.0/code-security/secret-security/about-secret-scanning

Secret Scanning

Email Notification



Disabled Public API Key

noreply@mailchimpmail.com via gmail.mctxapp.net
to me

11:10 AM (0 minutes ago)

Hey Joshua --

I wanted to reach out to you to let you know that we had to disable an active API Key in your Mailchimp account with the account name **soccerjoshj07**.

We were able to find your API Key posted publicly, which could give someone full access to your account. Since it's been disabled, we don't recommend re-enabling it. Instead, you'll need to generate a new API Key in your account.

Your key was found at the following URL: https://github.com/soccerjoshj07/ghas-demo/blob/5956292341356b5b35ce36d917a25111cb1afceb/appsettings.json

For more information on account security, refer to our Knowledge Base.

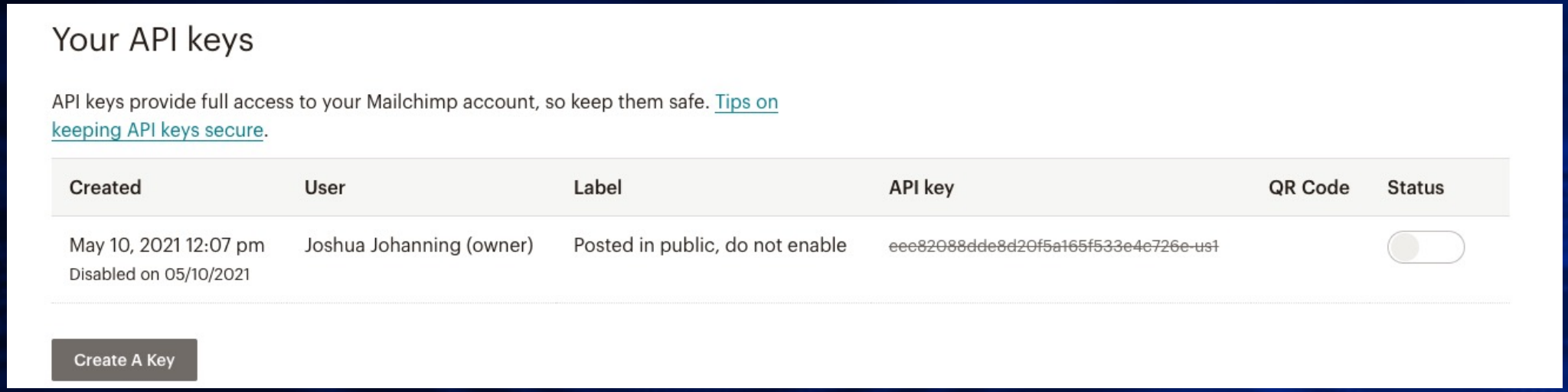
Keeping your API key secure: https://mailchimp.com/help/about-api-keys/#API_key_security

Thanks,
-- The Mailchimp API Team

https://mail.google.com/mail/u/0/#search/Disabled+Public+API+Key+in%3Aall

Secret Scanning

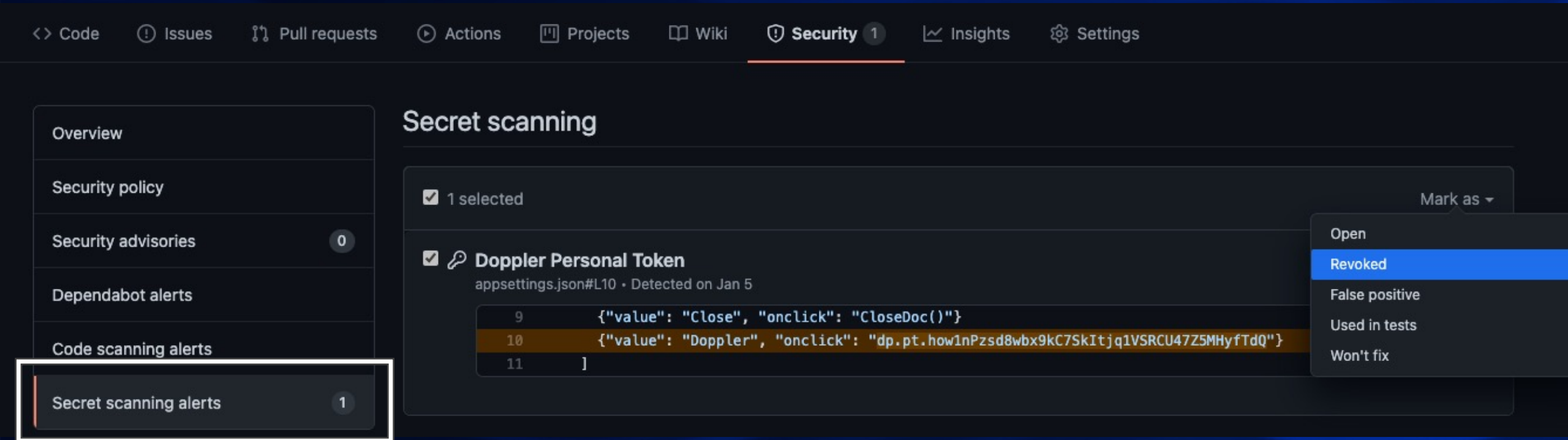
Mailchimp integration



https://us1.admin.mailchimp.com/account/api/

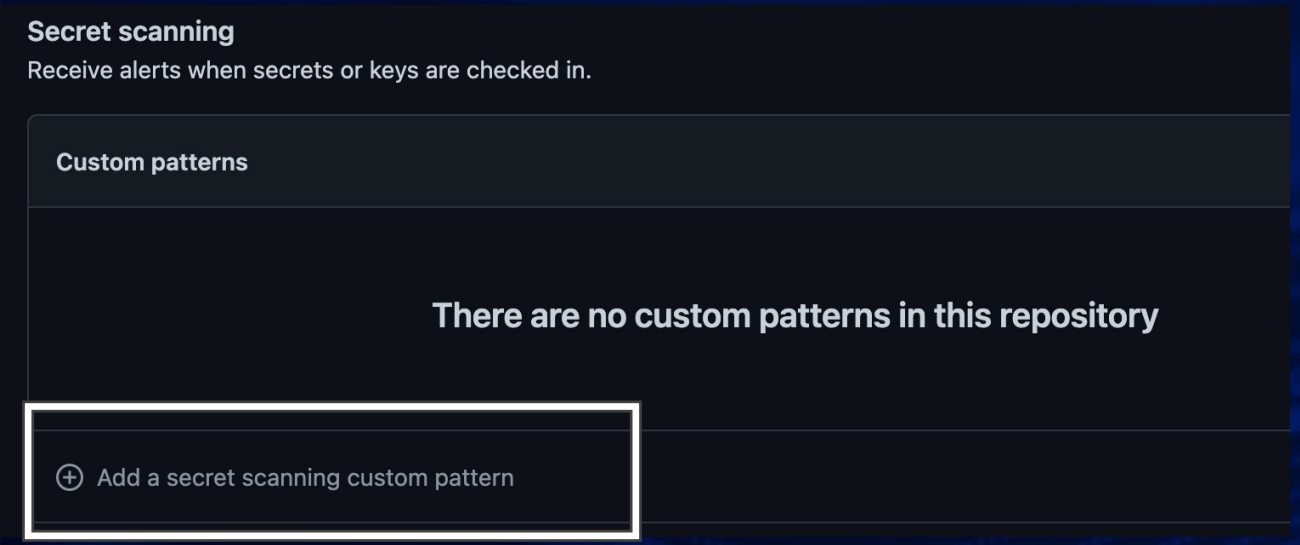
Secret Scanning

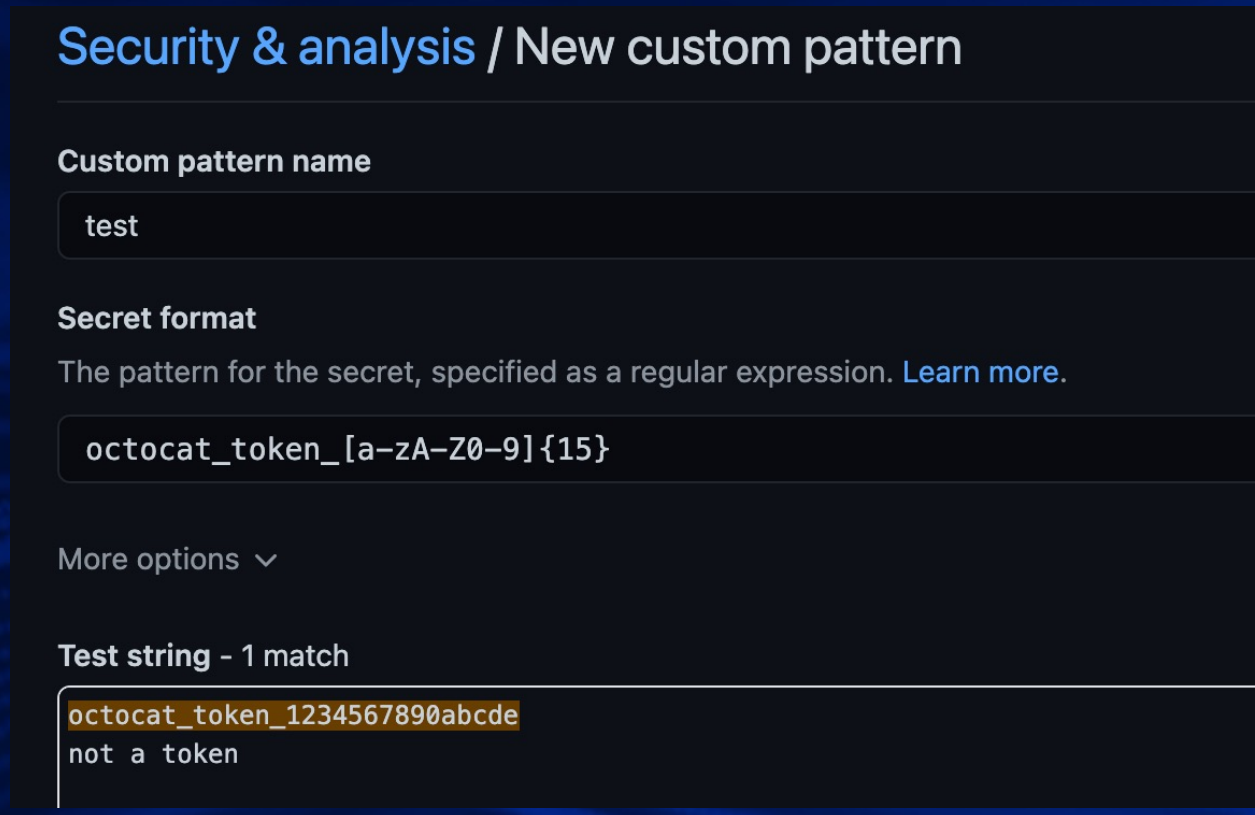
GitHub Enterprise Cloud – Secret Scanning Alerts



Secret Scanning

GitHub Enterprise Cloud – Custom Patterns!





Code Scanning

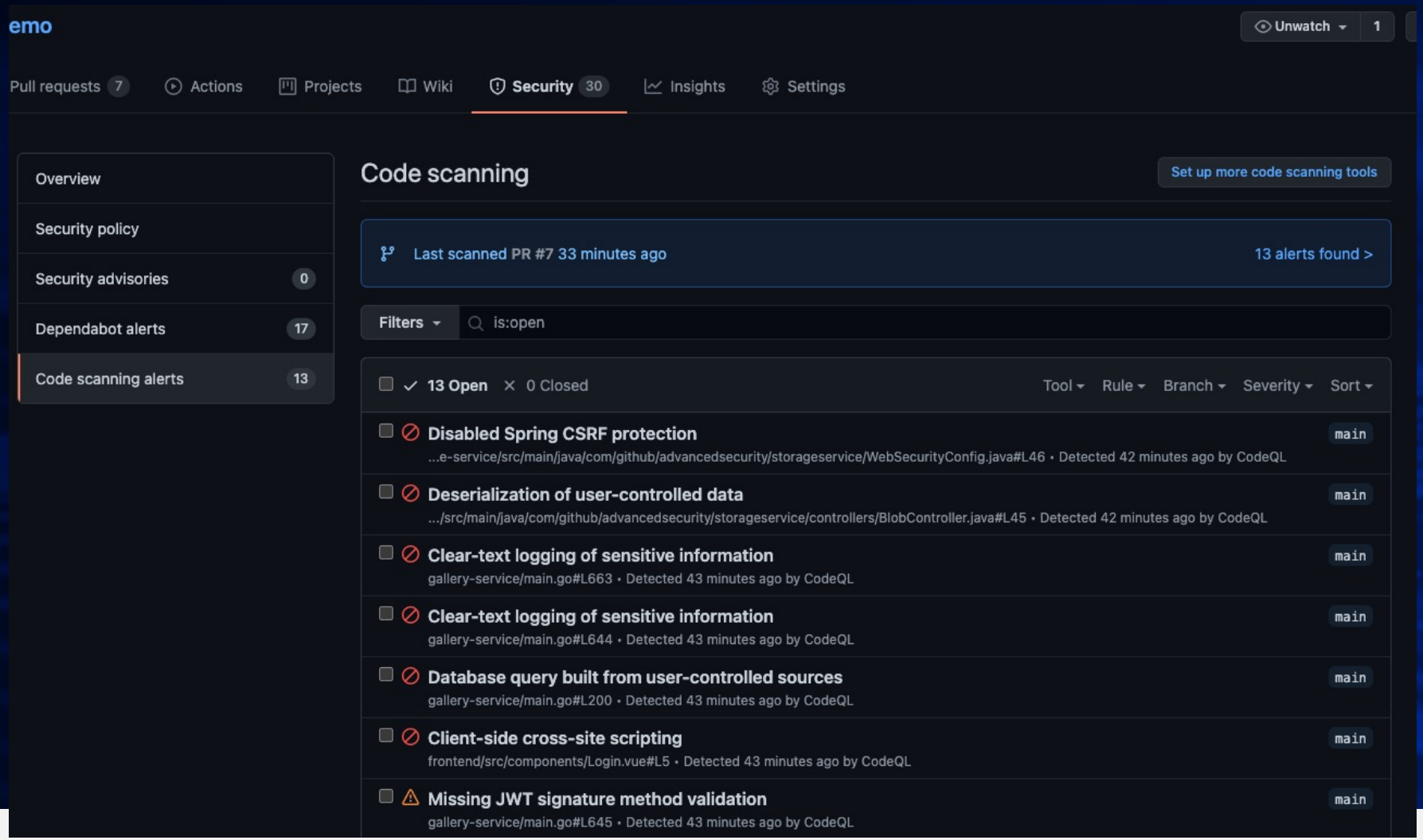
CodeQL

CodeQL analysis consists of three steps:

1. Preparing the code, by creating a CodeQL database
2. Running CodeQL queries against the database
3. Interpreting the query results

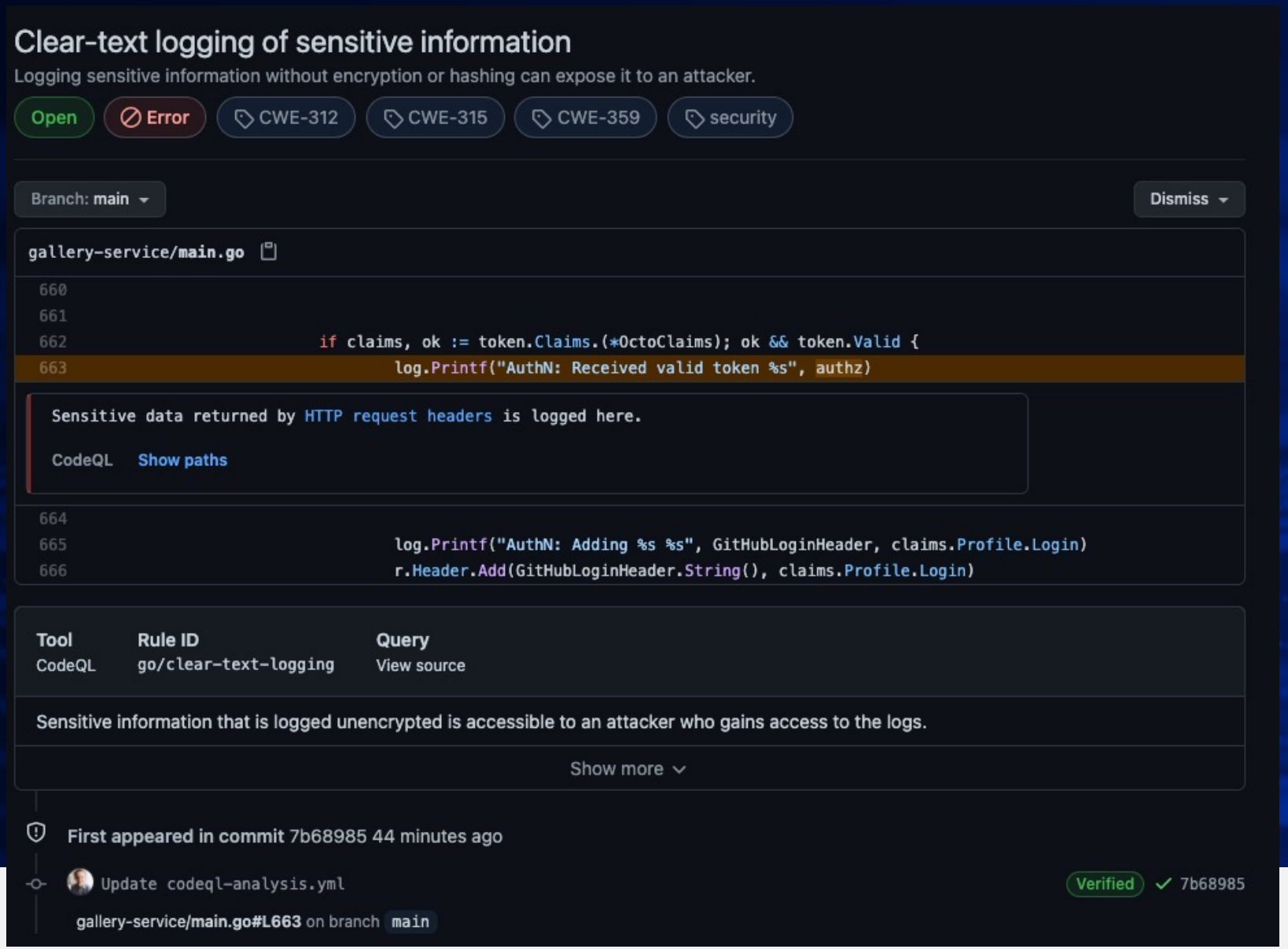
Code Scanning

Open Alerts



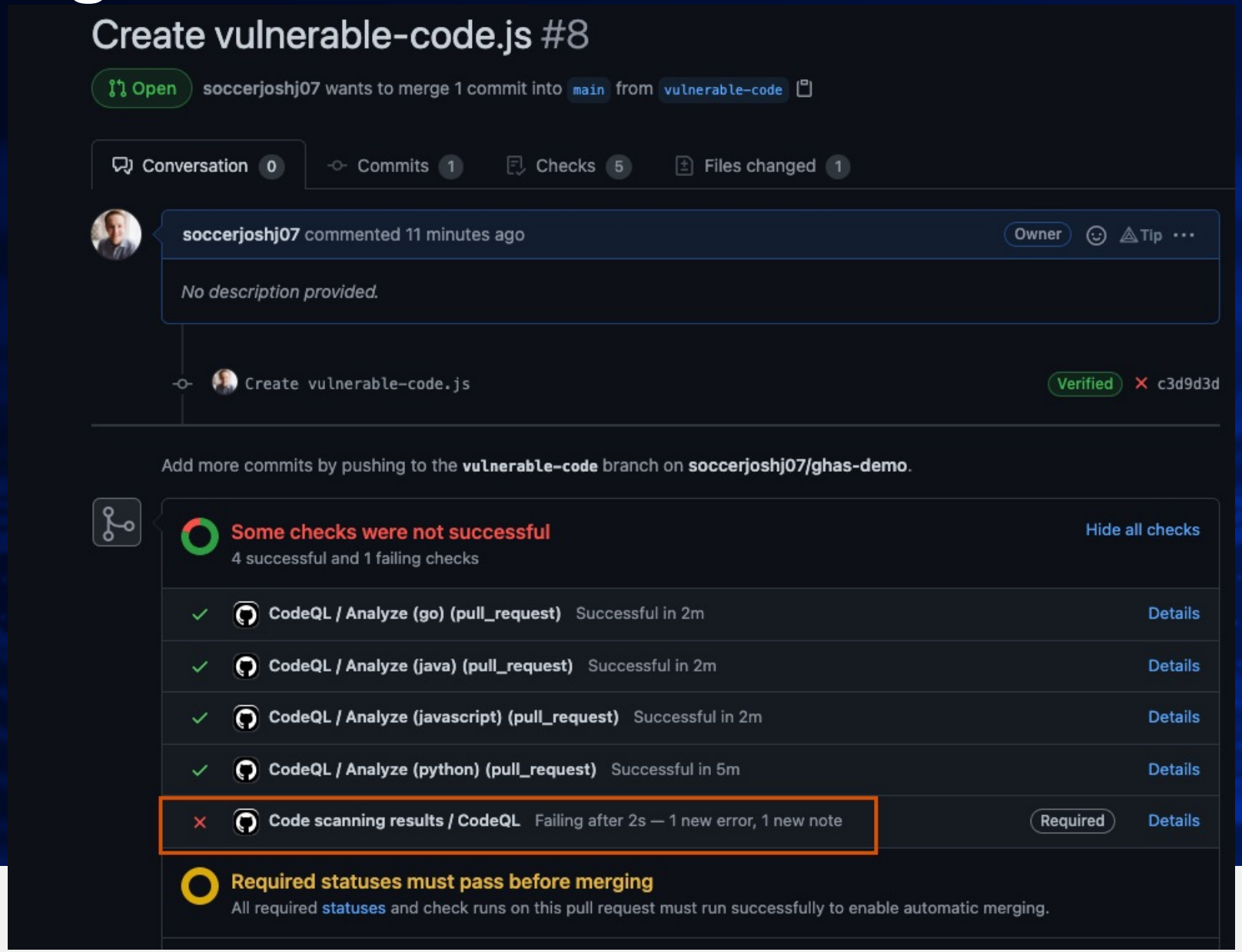
Code Scanning

Example Alert



Code Scanning

Pull Request



Dependabot – Security Alerts

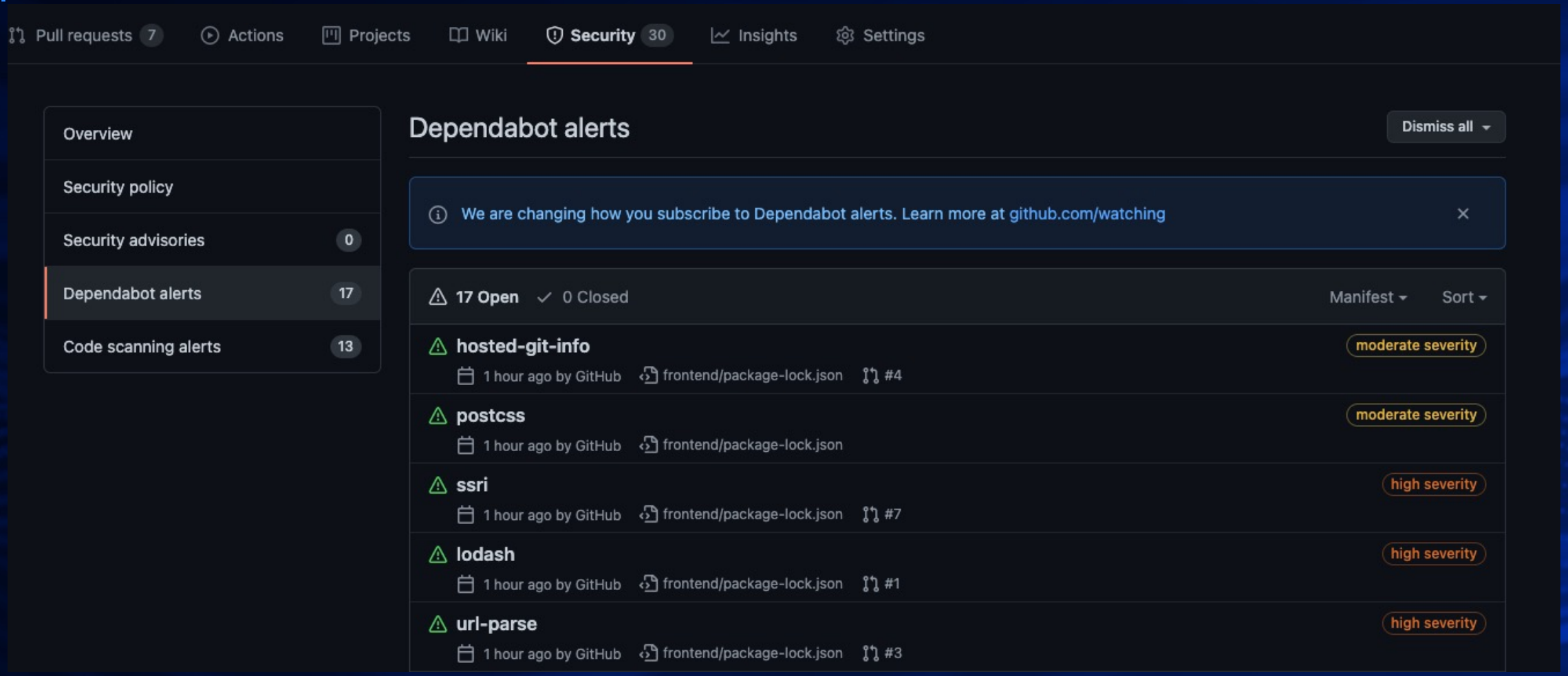
Supported package ecosystems

Package manager	Languages	Recommended formats	All supported formats
Composer	PHP	`composer.lock`	`composer.json`, `composer.lock`
`dotnet` CLI	.NET languages (C#, C++, F#, VB)	`.csproj`, `.vbproj`, `.nuspec`, `.vcxproj`, `.fsproj`	`.csproj`, `.vbproj`, `.nuspec`, `.vcxproj`, `.fsproj`, `packages.config`
Maven	Java, Scala	`pom.xml`	`pom.xml`
npm	JavaScript	`package-lock.json`	`package-lock.json`, `package.json`
Python PIP	Python	`requirements.txt`, `pipfile.lock`	`requirements.txt`, `pipfile`, `pipfile.lock`, `setup.py` *
RubyGems	Ruby	`Gemfile.lock`	`Gemfile.lock`, `Gemfile`, `*.gemspec`
Yarn	JavaScript	`yarn.lock`	`package.json`, `yarn.lock`

https://docs.github.com/en/code-security/supply-chain-security/about-the-dependency-graph#supported-package-ecosystems

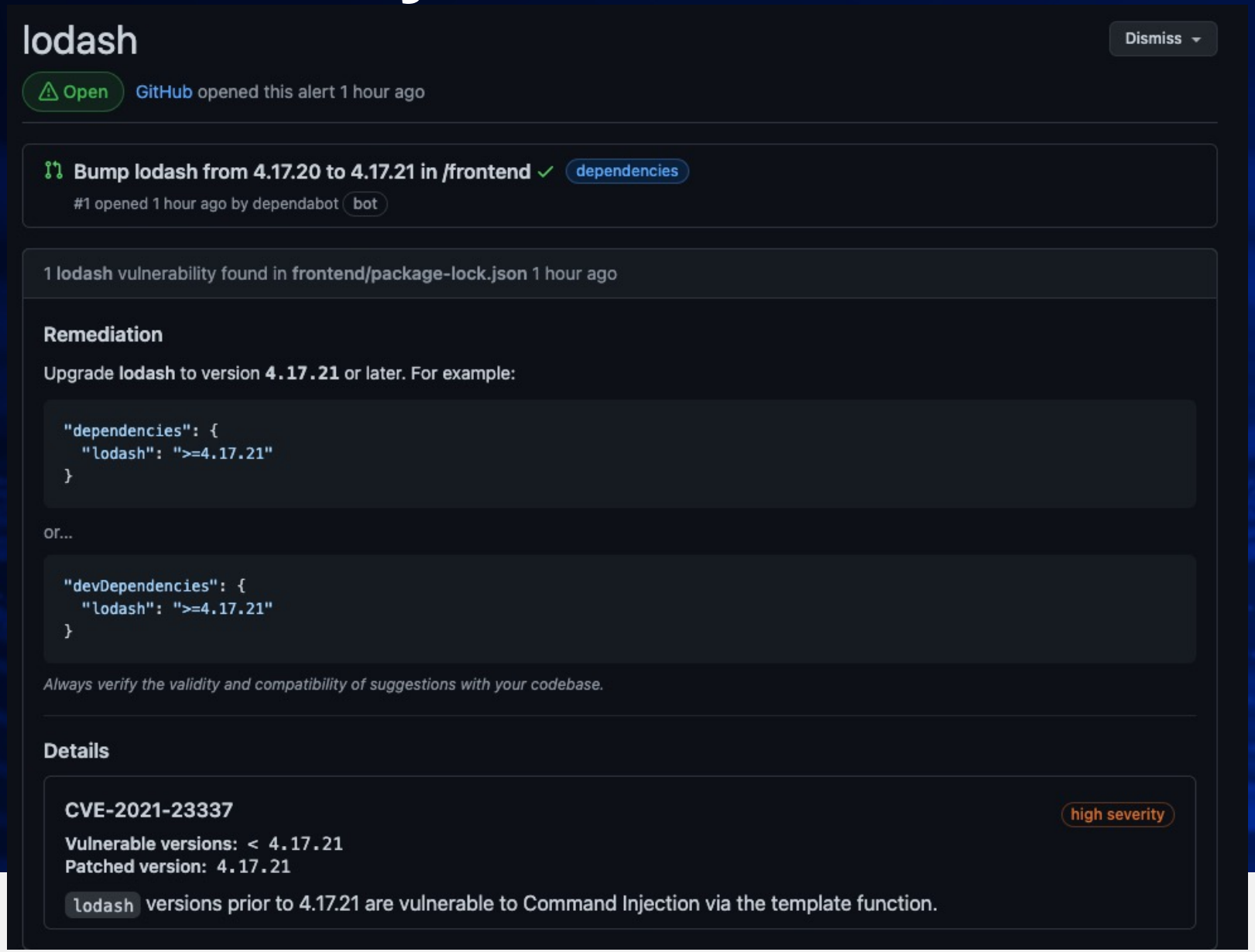
Dependabot – Security Alerts

Open Alerts



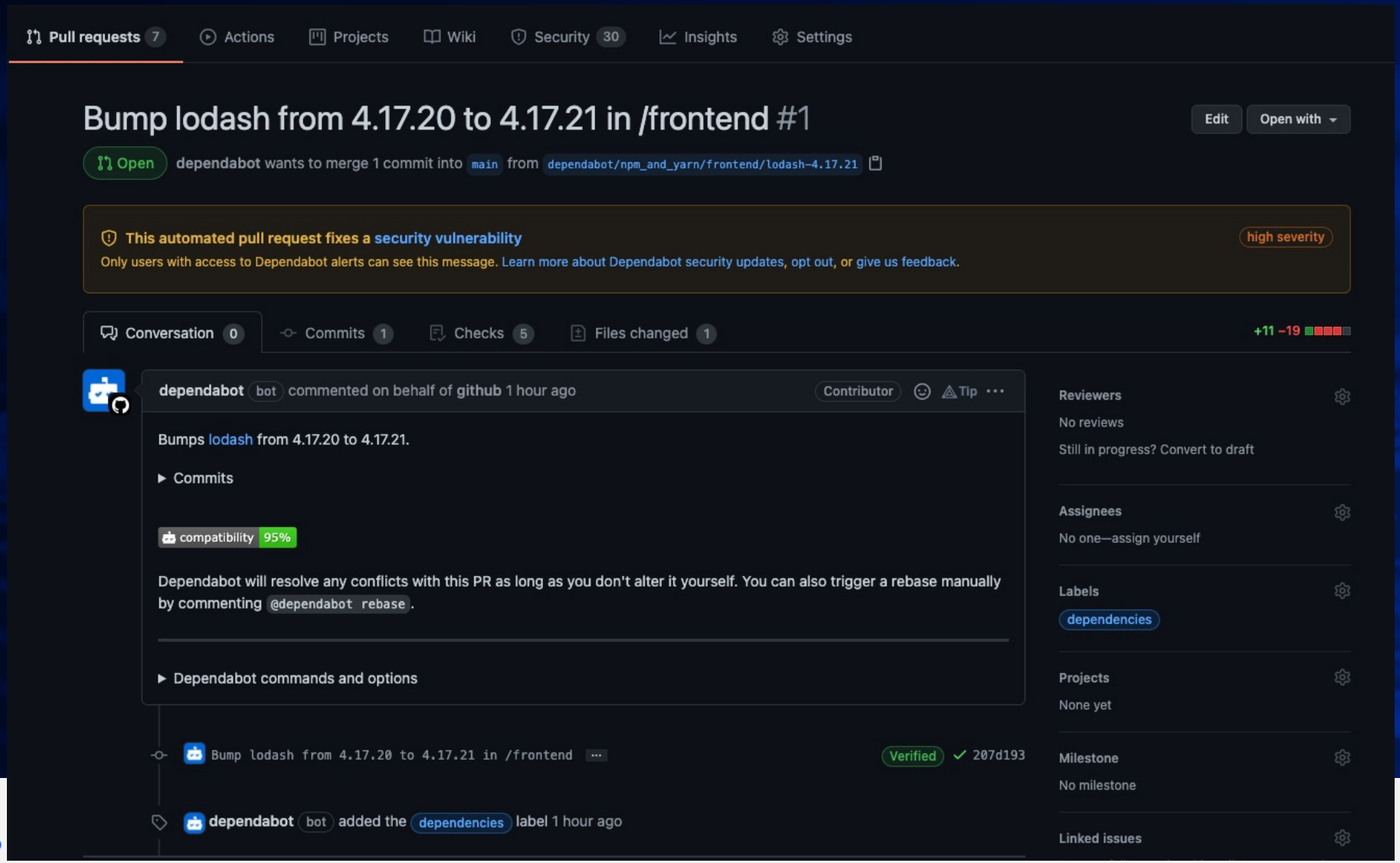
Dependabot – Security Alerts

Remediation



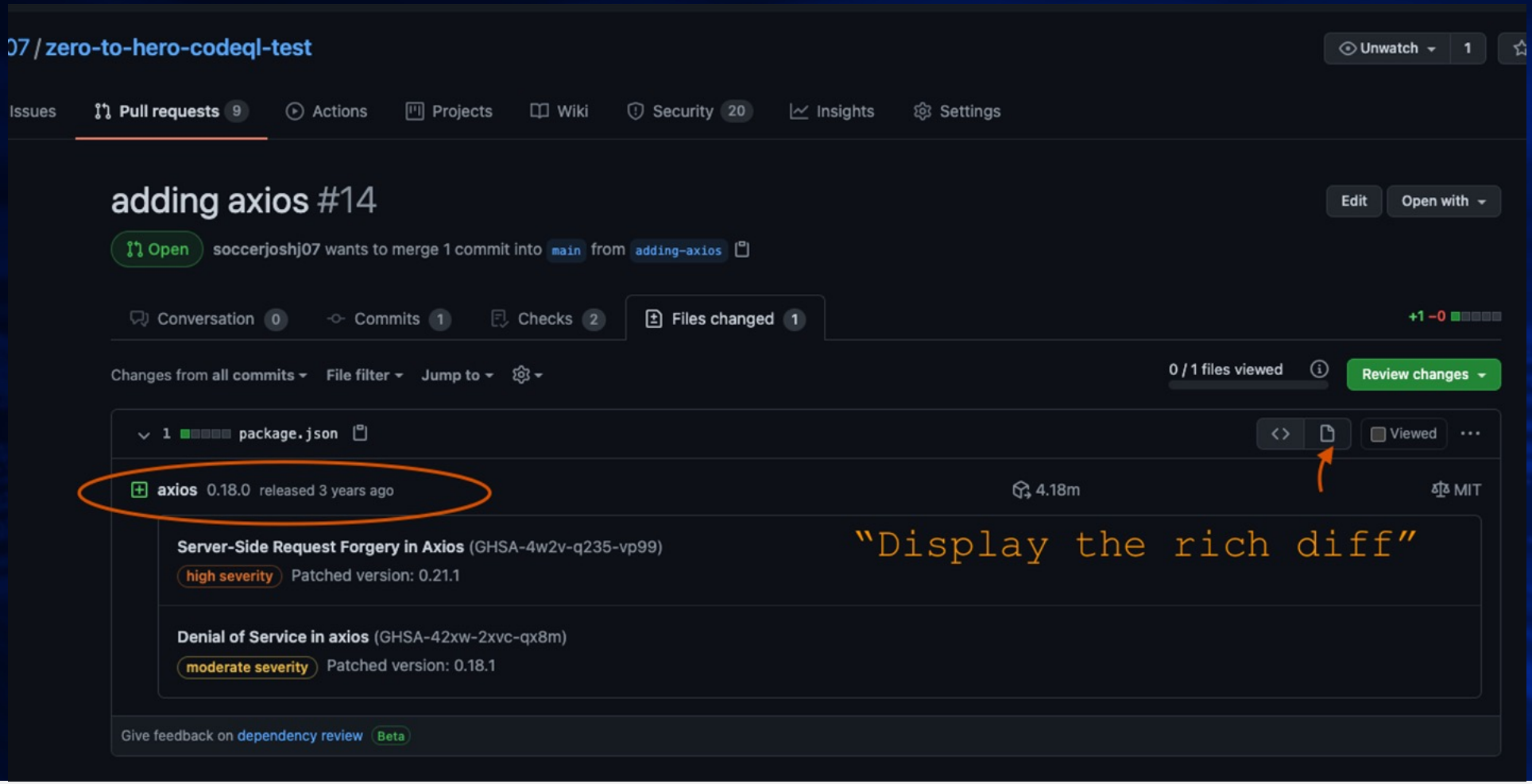
Dependabot – Security Updates

Pull Request



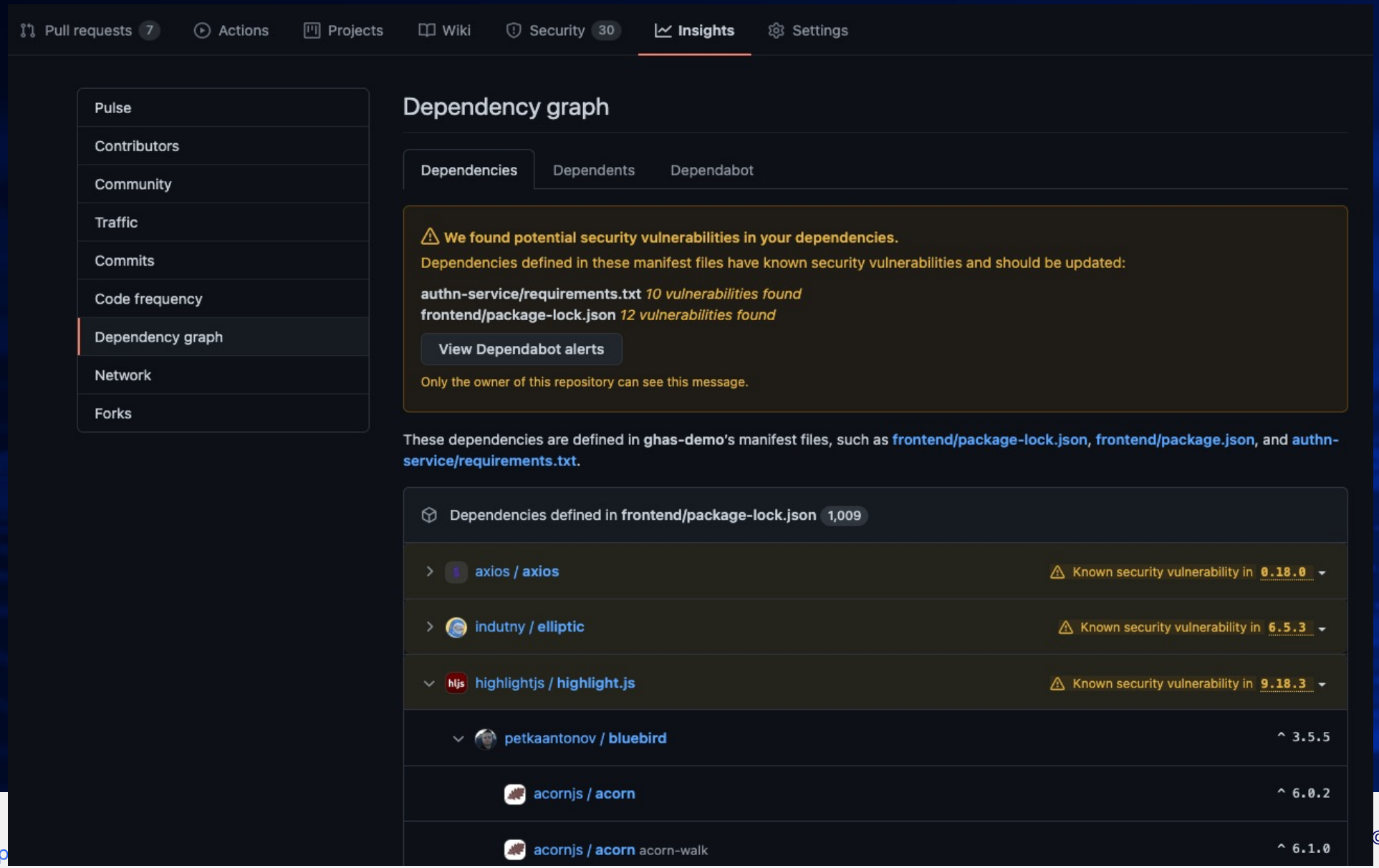
Dependabot – Security Updates

Pull Request – Introducing a vulnerable package version



https://github.com/soccerjoshj07/zero-to-hero-codeql-test/pull/14/files?short_path=7ae45ad#diff-7ae45ad102eab3b6d7e7896acd08c427a9b25b346470d7bc6507b6481575d519

Dependabot – Dependency Graph



Dependabot – Dependency Updates

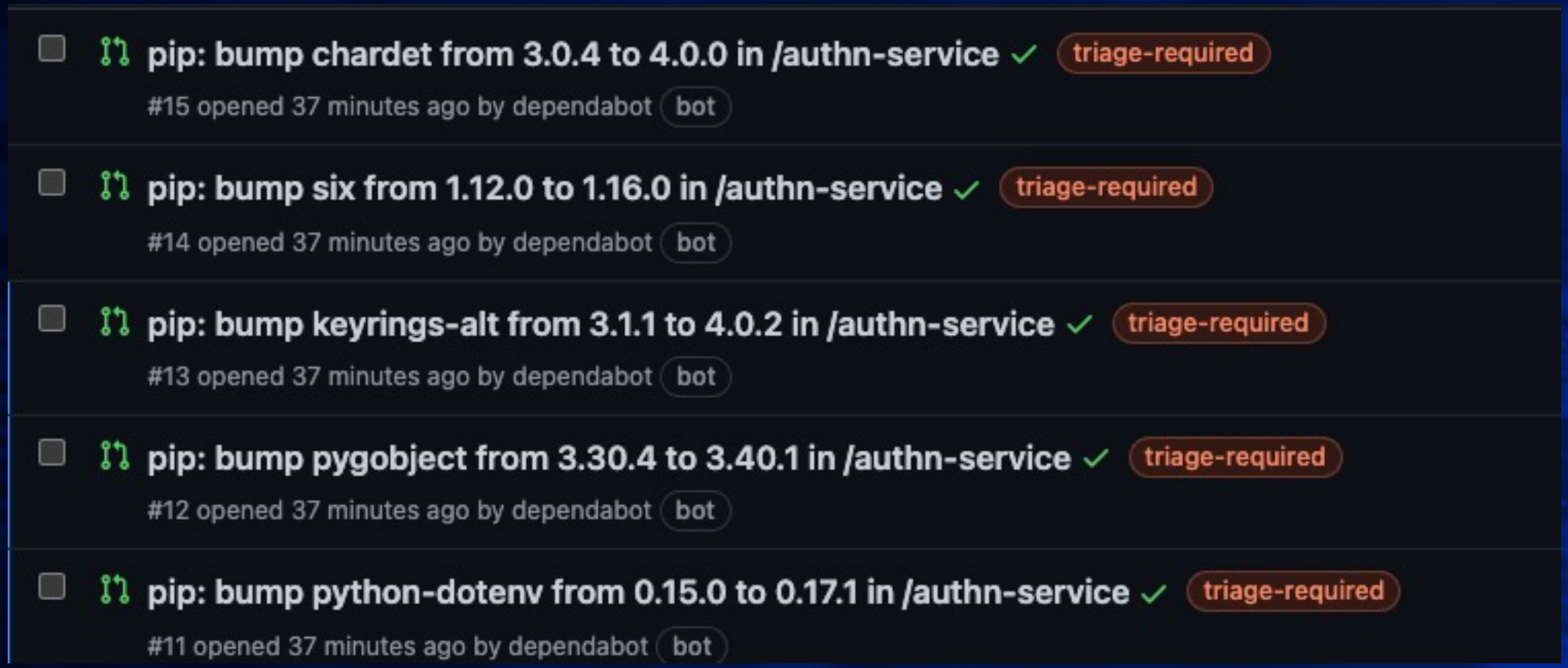
Supported Manifests

- Bundler
- Cargo
- Composer
- Docker
- Hex
- elm-package
- git submodule
- GitHub Actions
- Go modules
- Gradle
- Maven
- npm
- NuGet
- pip
- pipenv
- pip-compile
- poetry
- Terraform
- yarn

https://docs.github.com/en/code-security/supply-chain-security/configuration-options-for-dependency-updates#package-ecosystem

Dependabot – Dependency Updates

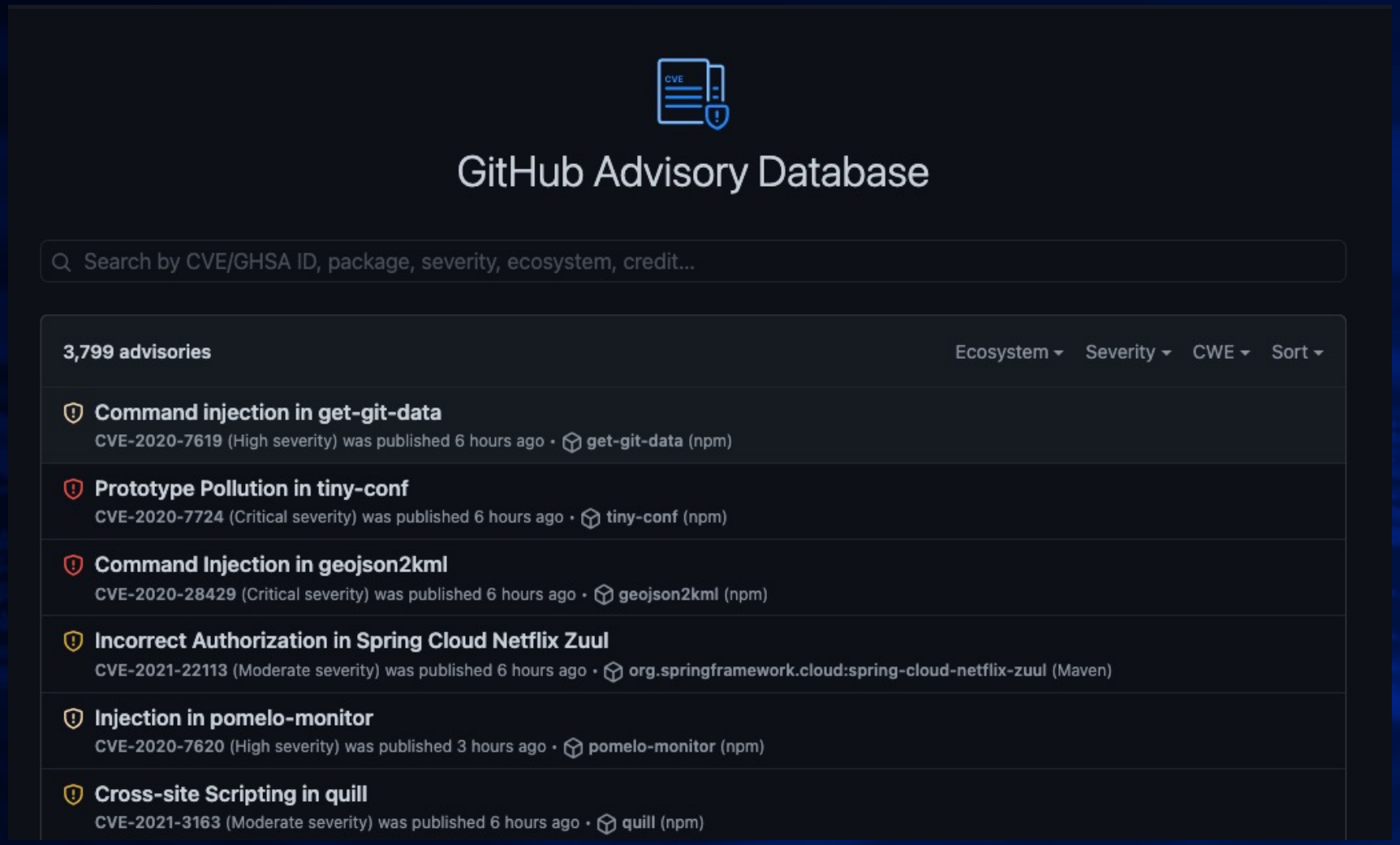
Packages that need to be updated – not necessarily security vulnerabilities



GitHub – Dependency Vulnerabilities shown in local Git output

```
joshuajohanning@10M-MAC-JJHANNING ~/Repos/AzDO/test-gh-scripts main git push
Enumerating objects: 4, done.
Counting objects: 100% (4/4), done.
Delta compression using up to 12 threads
Compressing objects: 100% (2/2), done.
Writing objects: 100% (3/3), 275 bytes | 275.00 KiB/s, done.
Total 3 (delta 1), reused 0 (delta 0), pack-reused 0
remote: Resolving deltas: 100% (1/1), completed with 1 local object.
remote:
remote: GitHub found 3 vulnerabilities on soccerjoshj07/test-github's default branch (3 moderate). To find out more, visit:
remote:      https://github.com/soccerjoshj07/test-github/security/dependabot
remote:
To https://github.com/soccerjoshj07/test-github.git
   34ab7b7..19d2f98  main -> main
```

GitHub – Advisory Database



https://github.com/advisories

Questions?