

Protect your code with GitHub security features



<https://myoctocat.com>

Protect your code with GitHub security features



Rob Bos

DevOps Consultant – Xpirit

The Netherlands

<https://devopsjournal.io>

@robbos81



<https://myoctocat.com>

Security features

Commit signing

Dependabot

Security alerts on dependencies

Secret scanning

CodeQL

Why? Attack vectors!

your code

```
26 // if npm is called as "npgm" or "npm_g", then
27 // run in global mode.
28 if (process.argv[1][process.argv[1].length - 1] === 'g') {
29   process.argv.splice(1, 1, 'npm', '-g')
30 }
31
32 const log = require('./utils/log-shim.js')
33 const replaceInfo = require('./utils/replace-info.js')
34 log.verbose('cli', replaceInfo(process.argv))
35
36 log.info('using', 'npm@%s', npm.version)
37 log.info('using', 'node@%s', process.version)
38
39 const updateNotifier = require('./utils/update-notifier.js')
40
```

your pipelines



Who can push code?

Search or jump to... / Pull requests Issues Marketplace Explore

rajbos / github-actions-requests Public Pin Unwatch 2 Fork 8 Star 5

<> Code Issues 14 Pull requests Actions Wiki Security Insights **Settings**

General

Access

Collaborators

Moderation options

Code and automation

Branches

Actions

Webhooks

Environments

Pages

Security

Code security and analysis

Deploy keys

Secrets

Who has access

PUBLIC REPOSITORY

This repository is public and visible to anyone.

[Manage](#)

DIRECT ACCESS

1 has access to this repository. 1 collaborator.

Manage access

☐ Select all Type

Find a collaborator...

☐ **Hindrik Bruinsma | DevOps Consultant**
cloudcosmonaut • Collaborator

[Add people](#)

Who can push code?

Direct: users with write access

- https
- ssh

Deploy keys

Machine users

GitHub Apps

GITHUB_TOKEN

Indirect (public repo):

– anyone can send in a Pull Request

How do you push code?


```
$ git config --global user.name "Some name"
```

```
$ git config --global user.email some-name@example.com
```







GitHub uses **this** info to match the user!

Not the authentication method!



[Pulls](#) [Issues](#) [Marketplace](#) [Explore](#)



















 **npm / cli** Public

[Watch](#) 178 [Fork](#) 1.5k [Star](#) 5.6k

[Code](#) [Issues](#) 462 [Pull requests](#) 27 [Actions](#) [Wiki](#) [Security](#) 4

latest

Commits on Mar 2, 2022

fix: ignore implicit workspace for whoami (#4493)  nlf committed 3 days ago ✓	 9e43de8 
fix: set proper workspace repo urls in package.json (#4476)  ljharb committed 3 days ago ✓	 0cfc155 
chore: @npmcli/template-oss@2.9.2 (#4491) ...  wraithgar committed 3 days ago ✓	 2b8f51e 
deps: lru-cache@7.4.0  wraithgar committed 3 days ago ✗	 10e1326 
minimatch@3.1.2  wraithgar committed 3 days ago	 236e3b4 
deps: socks@2.6.2  wraithgar committed 3 days ago	 1dd2f7e 

What's so bad?

- I can automate your commits!
- Default setup (Linux/Windows/https/ssh):



```
git add .  
git commit -m 'doing the commit for you'  
git push
```

Commit signing

GPG keys

[New GPG key](#)

This is a list of GPG keys associated with your account. Remove any keys that you do not recognize.

Email addresses: [raj.bos+gpg@gmail.com](#) [raj.bos@gmail.com](#)

Key ID: 9329ACE0943AF0DE

Subkeys: 05B8A873485710EA

Added on Feb 27, 2021

[Delete](#)

Always configure commit signing

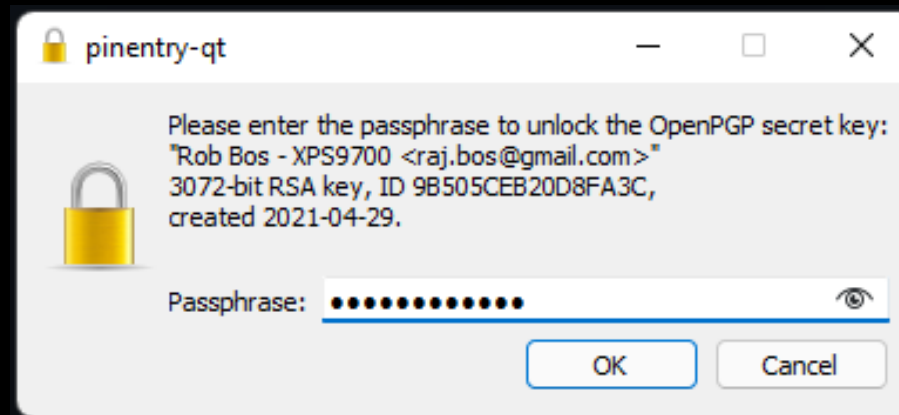
```
git commit -S -m "your commit message"
```

```
git config commit.gpgsign true
```

Demo / example

Demo – Commit signing

`git commit -m 'my commit'`



Commit signing

The screenshot shows the GitHub repository page for `npm/cli`. The repository is public and has 178 watches, 1.5k forks, and 5.6k stars. The commit history is filtered to show commits from March 2, 2022. The following table summarizes the commits shown:

Commit Message	Author	Status	Commit Hash
fix: ignore implicit workspace for whoami (#4493)	nlf	✓	9e43de8
fix: set proper workspace repo urls in package.json (#4476)	ljharb	✓	0cfc155
chore: @npmcli/template-oss@2.9.2 (#4491)	wraithgar	✓	2b8f51e
deps: lru-cache@7.4.0	wraithgar	✗	10e1326
minimatch@3.1.2	wraithgar		236e3b4
deps: socks@2.6.2	wraithgar		1dd2f7e

An orange box highlights the commit messages, and an orange arrow points from the highlighted area to the commit hash `10e1326`.

Commit signing

The screenshot shows a GitHub pull request interface. At the top, the repository is 'npm / cli' (Public). The pull request title is 'docs: standardize changelog heading #4510'. It shows 'wraithgar' wants to merge 1 commit into 'release-next' from 'gar/changelogs'. The interface includes tabs for Conversation (1), Commits (1), Checks (192), and Files changed (9). The conversation history shows: 'wraithgar' commented 'This will allow for release-please to update them appropriately'; 'wraithgar' requested a review; 'nlf' approved the changes; and 'npm-robot' commented 'no statistically significant performance changes detected'. A commit 'docs: standardize changelog heading' is shown with a 'Verified' status and a red 'X' icon, which is highlighted by an orange box. The right sidebar shows 'Reviewers' (nlf), 'Assignees' (None), 'Labels' (None), 'Projects' (None), 'Milestone' (None), and 'Development' status.

Search or jump to... Pull requests Issues Marketplace Explore

npm / cli Public Watch 178 Fork 1.5k

<> Code Issues 462 Pull requests 27 Actions Wiki Security 4 Insights

docs: standardize changelog heading #4510

Open wraithgar wants to merge 1 commit into release-next from gar/changelogs

Conversation 1 Commits 1 Checks 192 Files changed 9

wraithgar commented yesterday Contributor

This will allow for release-please to update them appropriately

docs: standardize changelog heading Verified X 48f7612

wraithgar requested a review from as a code owner yesterday

nlf approved these changes yesterday View changes

npm-robot commented yesterday

no statistically significant performance changes detected

► timing results

Reviewers: nlf

Assignees: No one assigned

Labels: None yet

Projects: None yet

Milestone: No milestone

Development: Successfully merging this p

Vigilant mode

GPG keys

[New GPG key](#)

This is a list of GPG keys associated with your account. Remove any keys that you do not recognize.



GPG

Email addresses: [raj.bos+gpg@gmail.com](#) [raj.bos@gmail.com](#)

Key ID: 9329ACE0943AF0DE

Subkeys: 05B8A873485710EA

Added on Feb 27, 2021

[Delete](#)

GPG

Email address: [raj.bos@gmail.com](#)

Key ID: 9B505CEB20D8FA3C

Subkeys: 577ECBC1D3DADEAF

Added on Apr 29, 2021

[Delete](#)

[Learn how to generate a GPG key and add it to your account .](#)

Vigilant mode

☒ **Flag unsigned commits as unverified**

This will include any commit attributed to your account but not signed with your GPG or S/MIME key.
Note that this will include your existing unsigned commits.

[Learn about vigilant mode.](#)

beta

Vigilant mode

<> Code Issues Pull requests 8 Actions Projects Wiki Security 1 ...

main ▾

Commits on Apr 27, 2021

Signed and signature verified

 hubwriter committed 3 hours ago ✓

Signature verified but has co-author with vigilant mode enabled

 John Doe authored and hubwriter committed 4 hours ago ✓

Not signed but committer has vigilant mode enabled

 octocat committed 6 hours ago ✓

Verified



2ce6deb

<>

Partially verified



f514ac0

<>

Unverified



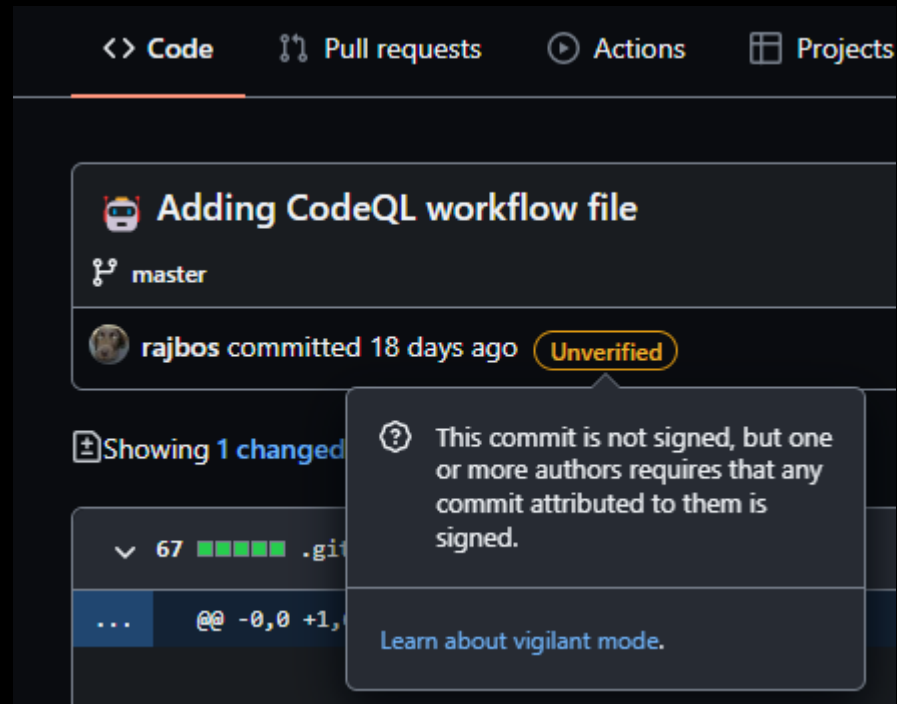
c83b4fd

<>

Vigilant mode

Status	Commit signed?	Signature verified?	Commit matches author?
Verified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Partially verified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	✗
Unverified	<input checked="" type="checkbox"/>	✗	
	✗		

Vigilant mode



Next step:

The screenshot displays the GitHub repository settings interface. On the left sidebar, the 'Code and automation' section is expanded, and the 'Branches' option is selected. The main content area is titled 'Branch protection rule'. It includes a 'Branch name pattern' field with the value 'main'. Below this, the 'Protect matching branches' section contains several checkboxes: 'Require a pull request before merging' (unchecked), 'Require status checks to pass before merging' (unchecked), 'Require conversation resolution before merging' (unchecked), 'Require signed commits' (checked), and 'Require linear history' (unchecked). An orange arrow points from the 'Secrets' option in the sidebar to the 'Require signed commits' checkbox.

Branch protection rule

Branch name pattern *

main

Protect matching branches

- ☐ **Require a pull request before merging**
When enabled, all commits must be made to a non-protected branch and submitted via a pull request before they can be merged into a branch that matches this rule.
- ☐ **Require status checks to pass before merging**
Choose which [status checks](#) must pass before branches can be merged into a branch that matches this rule. When enabled, commits must first be pushed to another branch, then merged or pushed directly to a branch that matches this rule after status checks have passed.
- ☐ **Require conversation resolution before merging**
When enabled, all conversations on code must be resolved before a pull request can be merged into a branch that matches this rule. [Learn more.](#)
- ☒ **Require signed commits**
Commits pushed to matching branches must have verified signatures.
- ☐ **Require linear history**
Prevent merge commits from being pushed to matching branches.

Require signed commits – impact

Users' setup: needs to install/configure tools

Automation:

- Dependabot – will sign automatically
- GitHub Apps
- Personal Access Tokens

Codespaces



GPG verification

Codespaces created from the following repositories can have GPG capabilities and sign commits that they come from a trusted source. Only enable this for repositories that you trust.

- ☐ Disabled
GPG will not be available in Codespaces
- ☒ All repositories
GPG will be available for Codespaces for all repositories
- ☐ Selected repositories
GPG will be available for Codespaces from the selected repositories

Security features

Commit signing

Dependabot

Security alerts on dependencies

Secret scanning

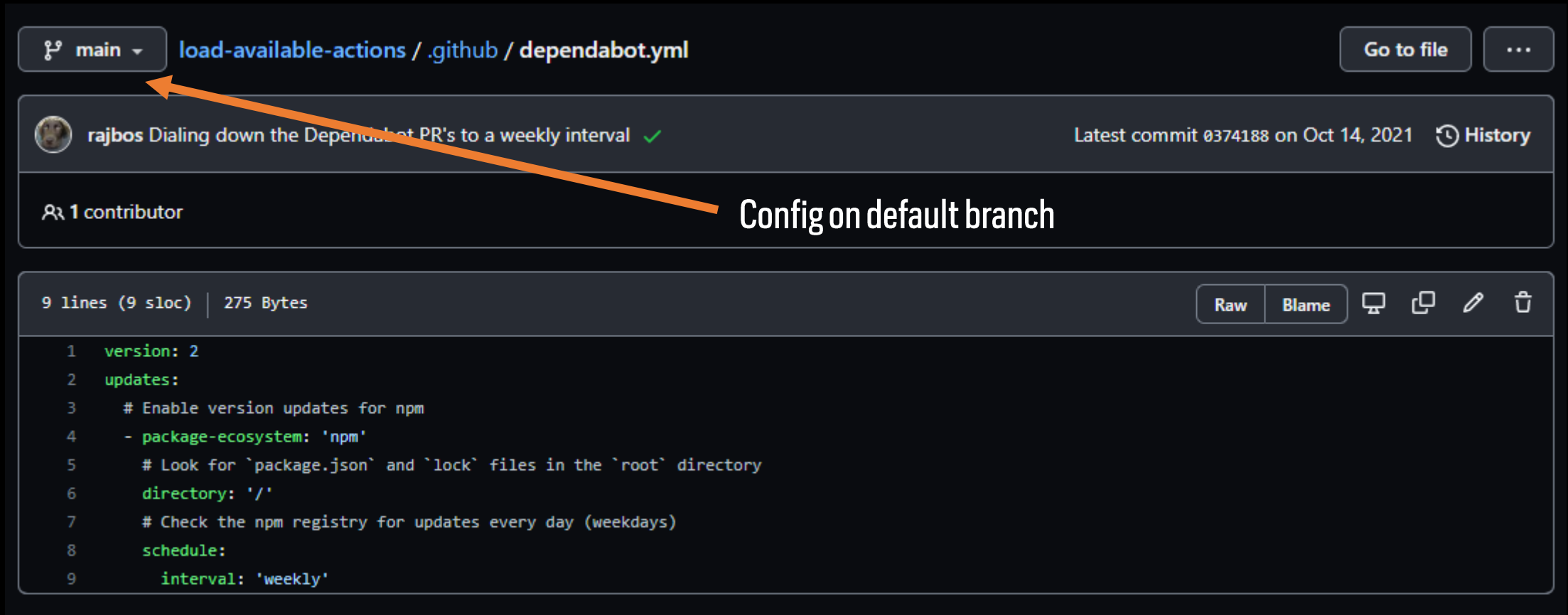
CodeQL

Stay up to date


- Dependabot + updates
 - Why
 - What to do
 - How
- Free for public repos



Dependabot config



main **load-available-actions / .github / dependabot.yml** Go to file ...

 **rajbos** Dialing down the Dependabot PR's to a weekly interval ✓ Latest commit 0374188 on Oct 14, 2021 History

1 contributor

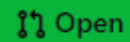
9 lines (9 sloc) | 275 Bytes Raw Blame

```
1 version: 2
2 updates:
3   # Enable version updates for npm
4   - package-ecosystem: 'npm'
5     # Look for `package.json` and `lock` files in the `root` directory
6     directory: '/'
7     # Check the npm registry for updates every day (weekdays)
8     schedule:
9       interval: 'weekly'
```


Dependabot demo

<https://github.com/devops-actions/load-runner-info/pull/98>

Bump Selenium.WebDriver.ChromeDriver from 97.0.4692.7100 to 98.0.4758.10200 #45



dependabot wants to merge 1 commit into `main` from `dependabot/nuget/Selenium.WebDriver.ChromeDriver-98.0.4758.10200`



Conversation 0



Commits 1



Checks 7



Files changed 1



dependabot bot commented 17 days ago

Contributor



Bumps `Selenium.WebDriver.ChromeDriver` from 97.0.4692.7100 to 98.0.4758.10200.

► Changelog



► Commits



compatibility unknown



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

► Dependabot commands and options

Reviewers

No reviews

Still in progress? Conve

Assignees

No one—assign yourse

Labels

dependencies

.NE

Projects

None yet



dependabot bot commented 17 days ago

Contributor



Bumps [Selenium.WebDriver.ChromeDriver](#) from 97.0.4692.7100 to 98.0.4758.10200.

▼ Changelog

Sourced from [Selenium.WebDriver.ChromeDriver's changelog](#).

98.0.4758.10200

- Chrome Driver 98.0.4758.102 release 98.0.4758.8000
- Chrome Driver 98.0.4758.80 release 98.0.4758.4800
- Chrome Driver 98.0.4758.48 release

▼ Commits

- [0733b78](#) Upgrade to 98.0.4758.102
- [3d7b7cc](#) Upgrade to 98.0.4758.80
- [dabd9e2](#) refine unit tests
- [ea396b9](#) modernize unit tests
- [9d4bdcf](#) v.98.0.4758.4800 release
- [d68a57d](#) Merge branch 'v98'
- [dd8278c](#) Upgrade to 98.0.4758.48
- See full diff in [compare view](#)

compatibility unknown

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

► Dependabot commands and options

▼ Dependabot commands and options

You can trigger Dependabot actions by commenting on this PR:

- `@dependabot rebase` will rebase this PR
- `@dependabot recreate` will recreate this PR, overwriting any edits that have been made to it
- `@dependabot merge` will merge this PR after your CI passes on it
- `@dependabot squash and merge` will squash and merge this PR after your CI passes on it
- `@dependabot cancel merge` will cancel a previously requested merge and block automerging
- `@dependabot reopen` will reopen this PR if it is closed
- `@dependabot close` will close this PR and stop Dependabot recreating it. You can achieve the same result by closing it manually
- `@dependabot ignore this major version` will close this PR and stop Dependabot creating any more for this major version (unless you reopen the PR or upgrade to it yourself)
- `@dependabot ignore this minor version` will close this PR and stop Dependabot creating any more for this minor version (unless you reopen the PR or upgrade to it yourself)
- `@dependabot ignore this dependency` will close this PR and stop Dependabot creating any more for this dependency (unless you reopen the PR or upgrade to it yourself)

```
# Use `ignore` to specify dependencies that should not be updated
```

```
version: 2
```

```
updates:
```

```
- package-ecosystem: "npm"
```

```
  directory: "/"
```

```
  schedule:
```

```
    interval: "daily"
```

```
  ignore:
```

```
- dependency-name: "express"
```

```
  # For Express, ignore all updates for version 4 and 5
```

```
  versions: ["4.x", "5.x"]
```

```
# Use `ignore` to specify dependencies that should not be updated
```

```
version: 2
```

```
updates:
```

- package-ecosystem: "npm"
 - directory: "/"
 - schedule:
 - interval: "daily"
 - ignore:

```
# For Lodash, ignore all updates
```

- dependency-name: "lodash"

```
# Use `ignore` to specify dependencies that should not be updated
```

```
version: 2
```

```
updates:
```

- package-ecosystem: "npm"
 directory: "/"
 schedule:
 interval: "daily"
 ignore:

```
  # For AWS SDK, ignore all patch updates  
  - dependency-name: "aws-sdk"  
    update-types: ["version-update:semver-patch"]
```

Security features

Commit signing

Dependabot

Security alerts on dependencies

Secret scanning

CodeQL

Security alerts on dependencies

Security updates from Dependabot

Free for public repos

Dependabot knows your dependency graph

Dependency has vulnerability? Alert!

Alerts on dependencies

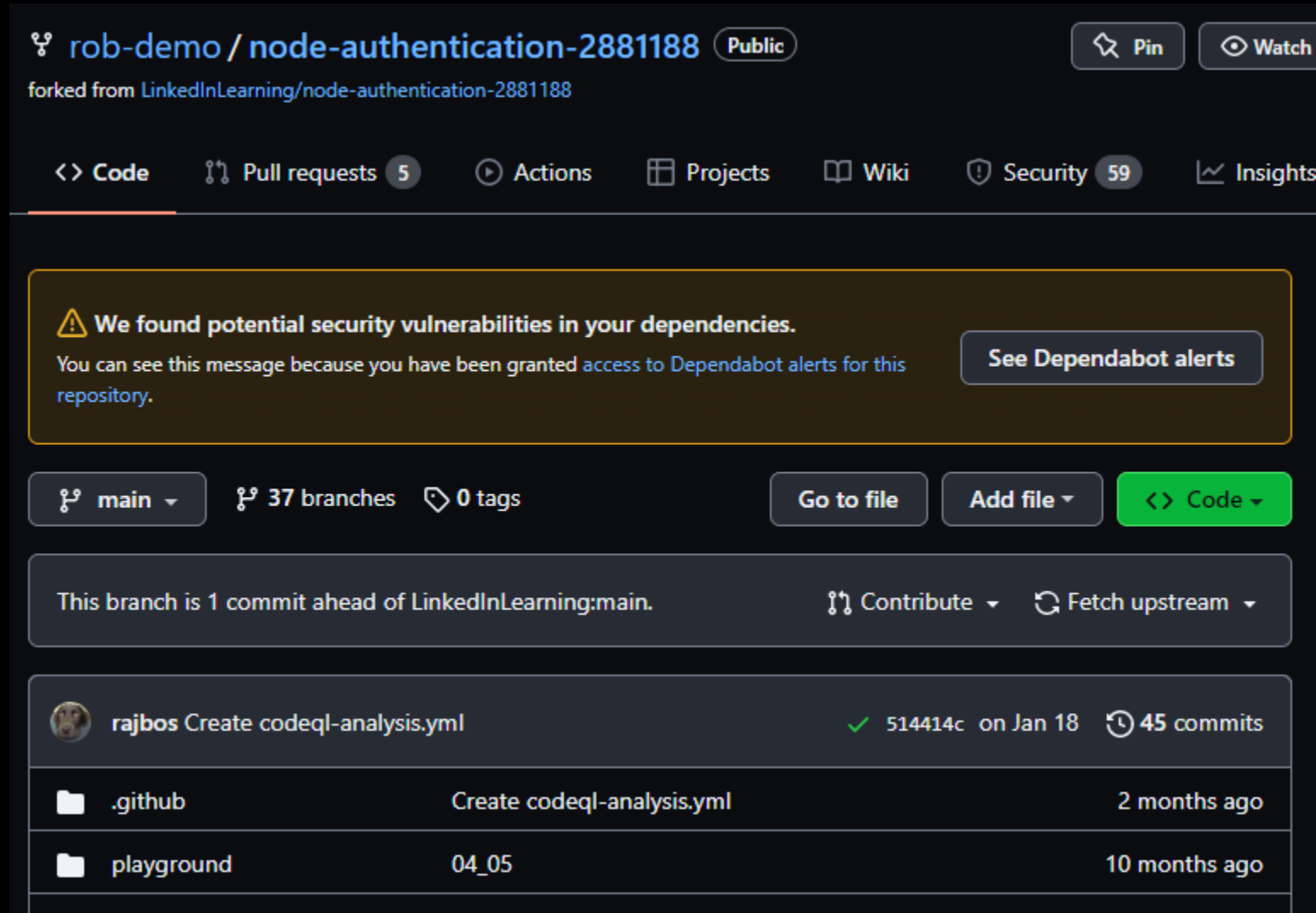
The screenshot shows the GitHub repository settings for 'rob-demo/security-demo' (Private). The 'Settings' tab is selected, and the 'Code security and analysis' section is highlighted in the left sidebar. The main content area shows the following settings:

- Code security and analysis**
 - Security and analysis features help keep your repository secure and updated. By enabling these features, you're granting us permission to perform read-only analysis on your repository.
 - Dependency graph**
 - Understand your dependencies.
 - Enable**
 - Dependabot alerts**
 - Receive alerts of new vulnerabilities that affect your dependencies.
 - Enable**
 - Dependabot security updates**
 - Easily upgrade to non-vulnerable dependencies.
 - Enable**
 - GitHub Advanced Security**
 - GitHub Advanced Security features are billed per active committer in private repositories. [Learn more.](#)
 - Code scanning**
 - Automatically detect common vulnerabilities and coding errors.
 - Set up**
 - Secret scanning**
 - Enable**

Demo

<https://github.com/rob-demo/node-authentication-2881188>

DEMO: Security alerts on dependencies



rob-demo / node-authentication-2881188 Public

forked from LinkedInLearning/node-authentication-2881188

<> Code Pull requests 5 Actions Projects Wiki Security 59 Insights

⚠️ We found potential security vulnerabilities in your dependencies.
You can see this message because you have been granted [access to Dependabot alerts](#) for this repository. [See Dependabot alerts](#)

main 37 branches 0 tags Go to file Add file <> Code

This branch is 1 commit ahead of LinkedInLearning:main. Contribute Fetch upstream

rajbos Create codeql-analysis.yml ✓ 514414c on Jan 18 ⌚ 45 commits

📁 .github	Create codeql-analysis.yml	2 months ago
📁 playground	04_05	10 months ago

DEMO: Security alerts on dependencies

🔑 rob-demo / node-authentication-2881188 Public

forked from LinkedInLearning/node-authentication-2881188

<> Code

🔗 Pull requests 5

🔄 Actions

📁 Projects

📖 Wiki

🛡️ Security 59

📈 Insights

⚙️ Settings

Overview

Security policy

Security advisories

Dependabot alerts 49

Code scanning alerts 10

Secret scanning alerts

Dependabot alerts Dismiss all

🛡️ 49 Open ✓ 1 Closed

Severity ▾ Package ▾ Ecosystem ▾ Manifest ▾ Sort ▾

🛡️	Authorization Bypass Through User-Controlled Key in url-parse Moderate	🔗 #6
url-parse (npm) · todolist/package-lock.json · #51 opened yesterday		
🛡️	Authorization Bypass Through User-Controlled Key in url-parse Moderate	🔗 #6
url-parse (npm) · todolist/package-lock.json · #50 opened 5 days ago		
🛡️	Authorization Bypass Through User-Controlled Key in url-parse Critical	🔗 #6
url-parse (npm) · todolist/package-lock.json · #49 opened 5 days ago		

DEMO: Security alerts on dependencies

The screenshot shows the GitHub repository settings for 'rob-demo/security-demo' (Private). The 'Settings' tab is selected, and the 'Code security and analysis' section is highlighted in the left sidebar. The main content area shows the following settings:

- Code security and analysis**: Security and analysis features help keep your repository secure and updated. By enabling these features, you're granting us permission to perform read-only analysis on your repository.
- Dependency graph**: Understand your dependencies. **Enable**
- Dependabot alerts**: Receive alerts of new vulnerabilities that affect your dependencies. **Enable**
- Dependabot security updates**: Easily upgrade to non-vulnerable dependencies. **Enable**
- GitHub Advanced Security**: GitHub Advanced Security features are billed per active committer in private repositories. **Learn more.** **Enable**
- Code scanning**: Automatically detect common vulnerabilities and coding errors. **Set up**
- Secret scanning**: **Enable**

DEMO: Security alerts on dependencies

Bump url-parse from 1.4.7 to 1.5.10 in /todolist #6

[Open](#) dependabot wants to merge 1 commit into `main` from `dependabot/npm_and_yarn/todolist/url-parse-1.5.10`

This automated pull request fixes a [security vulnerability](#)

Critical severity

Only users with access to Dependabot alerts can see this message. [Learn more about Dependabot security updates](#), [opt out](#), or [give us feedback](#).

Conversation 0

Commits 1

Checks 2

Files changed 1

+6 -6

dependabot bot commented 5 days ago

Bumps `url-parse` from 1.4.7 to 1.5.10.

► Commits

compatibility 75%

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

► Dependabot commands and options

Reviewers

No reviews

Still in progress? [Convert to draft](#)

Assignees

No one—[assign yourself](#)

Labels

`dependencies`

Projects

None yet

@robbos81

43


DEMO: Security alerts on dependencies

GitHub Advisory Database / GitHub Reviewed / CVE-2021-27515

Path traversal in url-parse

High severity **GitHub Reviewed** Published on May 6, 2021 • Updated on May 6, 2021

Vulnerability details Dependabot alerts **81**

Package	Affected versions	Patched versions
 url-parse (npm)	< 1.5.0	1.5.0

Description

url-parse before 1.5.0 mishandles certain uses of backslash such as http:/ and interprets the URI as a relative path.

References

- <https://nvd.nist.gov/vuln/detail/CVE-2021-27515>
- [unshiftio/url-parse#197](#)
- [unshiftio/url-parse@d1e7e88](#)
- [unshiftio/url-parse@1.4.7...1.5.0](#)
- <https://advisory.checkmarx.net/advisory/CX-2021-4306>

CVE ID

CVE-2021-27515

GHSA ID

GHSA-9m6j-fcg5-2442

CWEs

CWE-23

CVSS Score

5.3 Moderate
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

See something to contribute? [Suggest improvements for this vulnerability](#)

Security features

Commit signing

Dependabot

Security alerts on dependencies

Secret scanning

CodeQL

Secret scanning

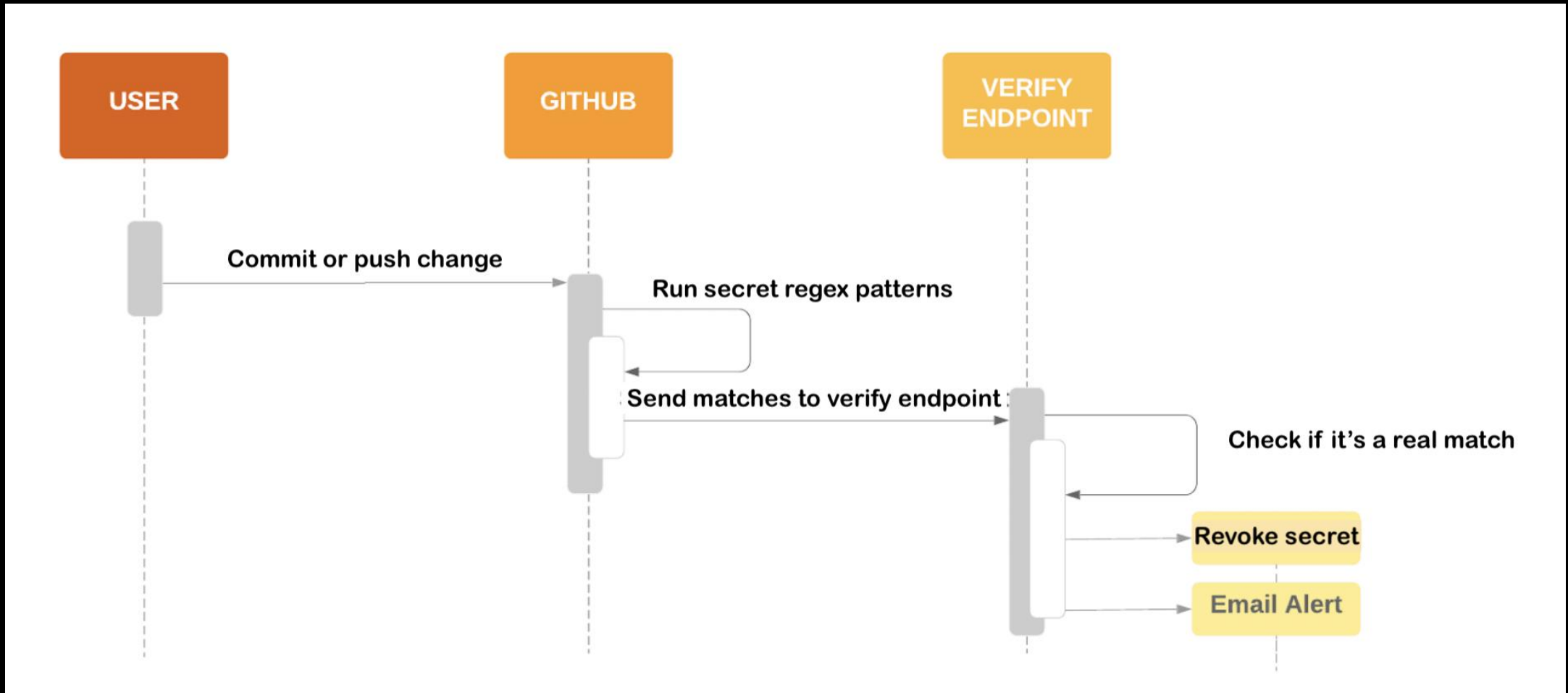
Secrets have a high risk!

Enabled by default on public repos

70+ secret scanning partners

- AWS / GCP/ Azure
- Discord
- npm
- NuGet
- Postman
- Twillio

Secret scanning



Secret scanning

Runs after a push event (scanning issues/ PR's is on the roadmap)

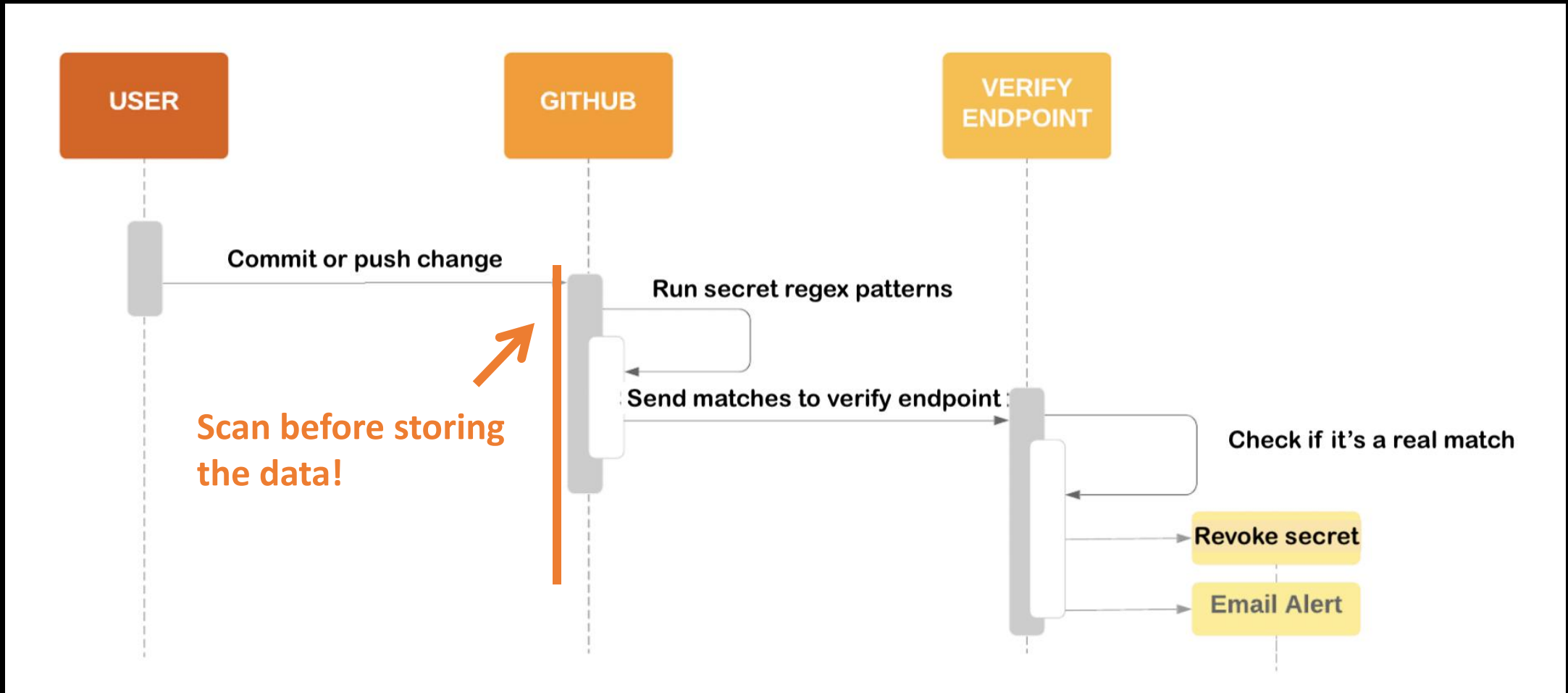
Scans the entire history of the repo as well

Public repo + actionable secret = high probability of revoking

Demo with an example repository:

- <https://github.com/Microsoft-Bootcamp/attendee-rajbos>

Secret scanning – push protection



Security features

Commit signing

Dependabot

Security alerts on dependencies

Secret scanning

CodeQL

CodeQL – What is it?

```
- name: Initialize CodeQL
  uses: github/codeql-action/init@v1
  with:
    languages: ${{ matrix.language }}
    config-file: ./.github/codeql/codeql-config.yml
```



Database

```
- name: Perform CodeQL Analysis
  uses: github/codeql-action/analyze@v1
```



Query

Using CodeQL

Free for public repos, uses your own Action minutes

CLI support

Open-source queries

Support for:

javascript

c++

ruby

c#

go

java

python

CodeQL – demo

a: <https://github.com/rajbos/TailwindTraders-Website>

b: <https://github.com/github/codeql>

c: <https://sarifweb.azurewebsites.net/>

CodeQL – demo

The screenshot shows a GitHub repository named `rajbos / dotnetcore-webapp` with a public status. The `Actions` tab is selected, displaying a workflow named `CodeQL` with run ID `CodeQL #78`. The workflow status is `Success`, triggered via schedule 2 days ago. The total duration is `2m 41s`. The workflow consists of two jobs: `Analyze (csharp)` and `Analyze (javascript)`, both of which are successful. The `codeql-analysis.yml` file is shown, configured to run on a schedule. A matrix named `Analyze` is defined, containing the two analysis jobs. The `Analyze (csharp)` job took `2m 27s` and the `Analyze (javascript)` job took `1m 31s`. The interface includes navigation links for Code, Issues, Pull requests, Actions, Projects, Wiki, Security, Insights, and Settings. A `Re-run all jobs` button is also visible.

rajbos / dotnetcore-webapp Public

<> Code Issues Pull requests **Actions** Projects Wiki Security 6 Insights Settings

✓ **CodeQL** CodeQL #78 Re-run all jobs ...

Summary

Jobs

- ✓ Analyze (csharp)
- ✓ Analyze (javascript)

Triggered via schedule 2 days ago	Status	Total duration	Artifacts
rajbos -O- 1ac525d	Success	2m 41s	–

codeql-analysis.yml
on: schedule

Matrix: Analyze

✓ Analyze (csharp)	2m 27s
✓ Analyze (javascript)	1m 31s

CodeQL – demo

rajbos / dotnetcore-webapp Public

Pin Unwatch 2 Fork 136 Star 6

<> Code Issues Pull requests Actions Projects Wiki Security 6 Insights Settings

Overview

Security policy

Security advisories

Dependabot alerts

Code scanning alerts 6

Code scanning

Add scanning tool

Latest scan 2 days ago

Branch main

Workflow CodeQL

Lines scanned 143 / 269

Duration 2m 19s

Result 0 alerts

Filters

is:open branch:main

6 Open 0 Closed

Tool Branch Rule Severity Sort

☐

Inefficient regular expression High

dotnet-core-webapp/.../dist/jquery.validate.js:1394 • Detected on Feb 4, 2021 by CodeQL

main

☐

Inefficient regular expression High

dotnet-core-webapp/.../dist/additional-methods.js:1092 • Detected on Feb 4, 2021 by CodeQL

main

☐

Inefficient regular expression High

dotnet-core-webapp/.../dist/additional-methods.js:1092 • Detected on Feb 4, 2021 by CodeQL

main

☐

Unsafe expansion of self-closing HTML tag Medium

dotnet-core-webapp/.../dist/jquery.js:5796 • Detected on Nov 12, 2020 by CodeQL

main

☐

DOM text reinterpreted as HTML Medium

dotnet-core-webapp/.../js/bootstrap.bundle.js:1076 • Detected on Nov 12, 2020 by CodeQL

main

☐

DOM text reinterpreted as HTML Medium

dotnet-core-webapp/.../js/bootstrap.js:1077 • Detected on Nov 12, 2020 by CodeQL

main

@robbos81

ProTip! The libraries and queries that power CodeQL are open-source. [Learn more](#)

Security features – overview

Commit signing

Dependabot

Security alerts on dependencies

Secret scanning

CodeQL

Protect your code with GitHub security features



Rob Bos

DevOps Consultant – Xpirit

The Netherlands

<https://devopsjournal.io>

@robbos81



<https://myoctocat.com>