

Protect your code with GitHub security features

Rob Bos

DevOps Consultant – Xebia | Xpirit

The Netherlands



<https://myoctocat.com>

Security features

Commit signing

Dependabot

Security alerts on dependencies

Secret scanning

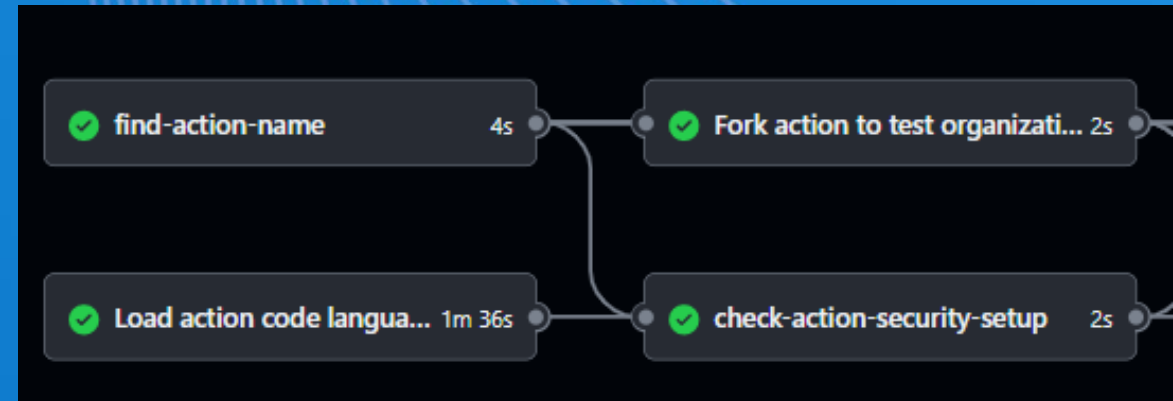
CodeQL

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



<https://owasp.org/Top10>

Who can push code?

The screenshot shows the GitHub repository settings page for 'rajbos / github-actions-requests'. The 'Settings' tab is highlighted in the top navigation bar. In the left sidebar, the 'Access' section is highlighted, and 'Collaborators' is selected. The main content area is divided into two sections: 'Who has access' and 'Manage access'. The 'Who has access' section shows 'PUBLIC REPOSITORY' (visible to anyone) and 'DIRECT ACCESS' (1 collaborator). The 'Manage access' section includes a search bar for collaborators and a list of current collaborators, with 'Hindrik Bruinsma | DevOps Consultant' listed as a collaborator. An orange arrow points from the 'DIRECT ACCESS' section to the 'Manage access' section.

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!

Search or jump to... / 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 Delete

Subkeys: 05B8A873485710EA

Added on Feb 27, 2021

You have your private key to sign with  GitHub has public key to verify the commit with

Commit signing

- GPG keys (most common)  Works on Windows with Vs Code
- S/MIME
- SSH keys (since September 2022)  Issue with passphrase on Windows with Vs Code

Always configure commit signing

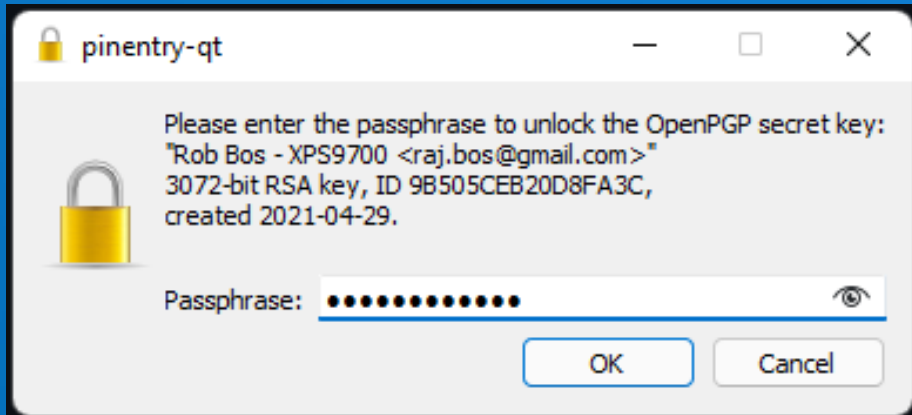
```
git commit -S -m "your commit message"
```

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


Demo / example

Demo – Commit signing

```
git commit -m 'my commit'
```



Commit signing

The screenshot shows the GitHub interface for the `npm/cli` repository. The commit history for March 2, 2022, is displayed. The first three commits are highlighted with an orange box, and an orange arrow points to the second commit.

Commit Message	Author	Time	SHA-1
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

Commit signing


The screenshot shows a GitHub pull request interface. At the top, there's a search bar and navigation links for Pull requests, Issues, Marketplace, and Explore. Below that, the repository 'npm/cli' is identified as 'Public', with 'Watch 178' and 'Fork 1.5k' buttons. The main navigation bar includes 'Code', 'Issues 462', 'Pull requests 27', 'Actions', 'Wiki', 'Security 4', and 'Insights'. The pull request title is 'docs: standardize changelog heading #4510', and it shows 'wraithgar wants to merge 1 commit into release-next from gar/changelogs'. Below the title, there are tabs for 'Conversation 1', 'Commits 1', 'Checks 192', and 'Files changed 9'. A comment from 'wraithgar' is visible, stating 'This will allow for release-please to update them appropriately'. To the right of the comment, a 'Verified' badge is highlighted with an orange box, and an orange arrow points to it from the right. Below the comment, a commit entry shows 'docs: standardize changelog heading' with a 'Verified' badge and the commit hash '48f7612'. At the bottom, it says 'wraithgar requested a review from as a code owner yesterday'. On the right side, there are sections for 'Reviewers' (listing 'nlf'), 'Assignees' (stating 'No one assigned'), and 'Labels'.

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.

 **Email addresses:** raj.bos+gpg@gmail.com raj.bos@gmail.com

Key ID: 9329ACE0943AF0DE Delete

Subkeys: 05B8A873485710EA

Added on Feb 27, 2021

 **Email address:** raj.bos@gmail.com

Key ID: 9B505CEB20D8FA3C Delete

Subkeys: 577ECBC1D3DADEAF

Added on Apr 29, 2021

[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. beta

[Learn about vigilant mode.](#)

Vigilant mode

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

main ▾

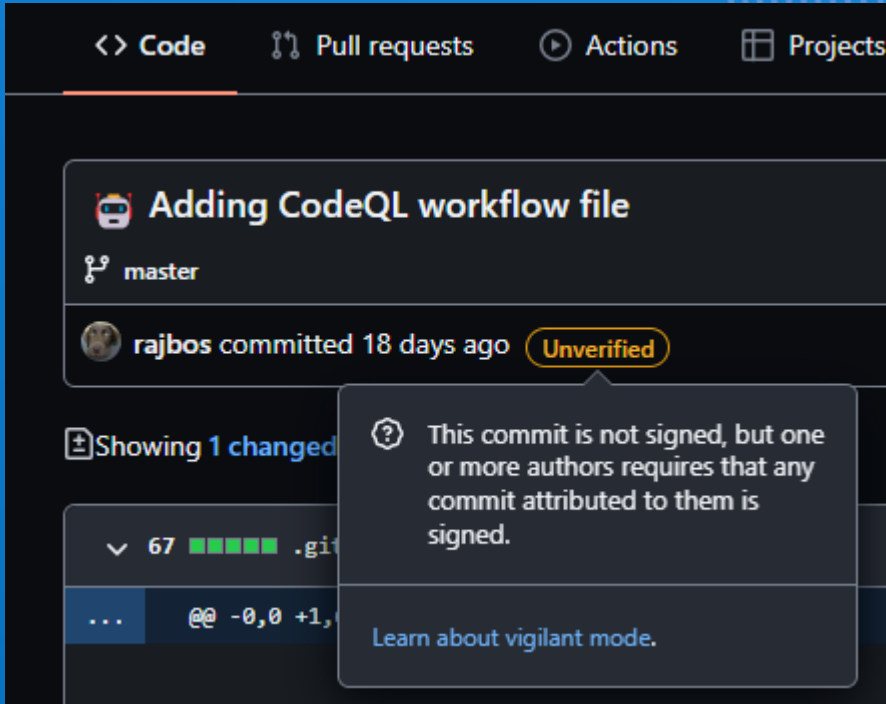
Commits on Apr 27, 2021

Signed and signature verified hubwriter committed 3 hours ago ✓	Verified	2ce6deb	<>
Signature verified but has co-author with vigilant mode enabled John Doe authored and hubwriter committed 4 hours ago ✓	Partially verified	f514ac0	<>
Not signed but committer has vigilant mode enabled octocat committed 6 hours ago ✓	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"/>	X
Unverified	<input checked="" type="checkbox"/>	X	
	X		

Vigilant mode



Next step:

The screenshot displays the GitHub repository settings interface. The left sidebar contains a navigation menu with categories: General, Access, Code and automation, Security, and Integrations. The 'Branches' option under 'Code and automation' is highlighted with an orange box. The main content area is titled 'Branch protection rule' and is also highlighted with an orange box. It contains the following configuration options:

- Branch name pattern ***: A text input field containing 'main'.
- Protect matching branches**: A section with several checkboxes:
 - 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.

An orange arrow points from the 'Secrets' option in the sidebar to the 'Require signed commits' checkbox.

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

Signed commits – recommendation

- Use either a Yubikey or a signing key with a pass phrase!
- No way to enforce / check for this unfortunately

Security features

> Commit signing

Dependabot

Security alerts on dependencies

Secret scanning

CodeQL

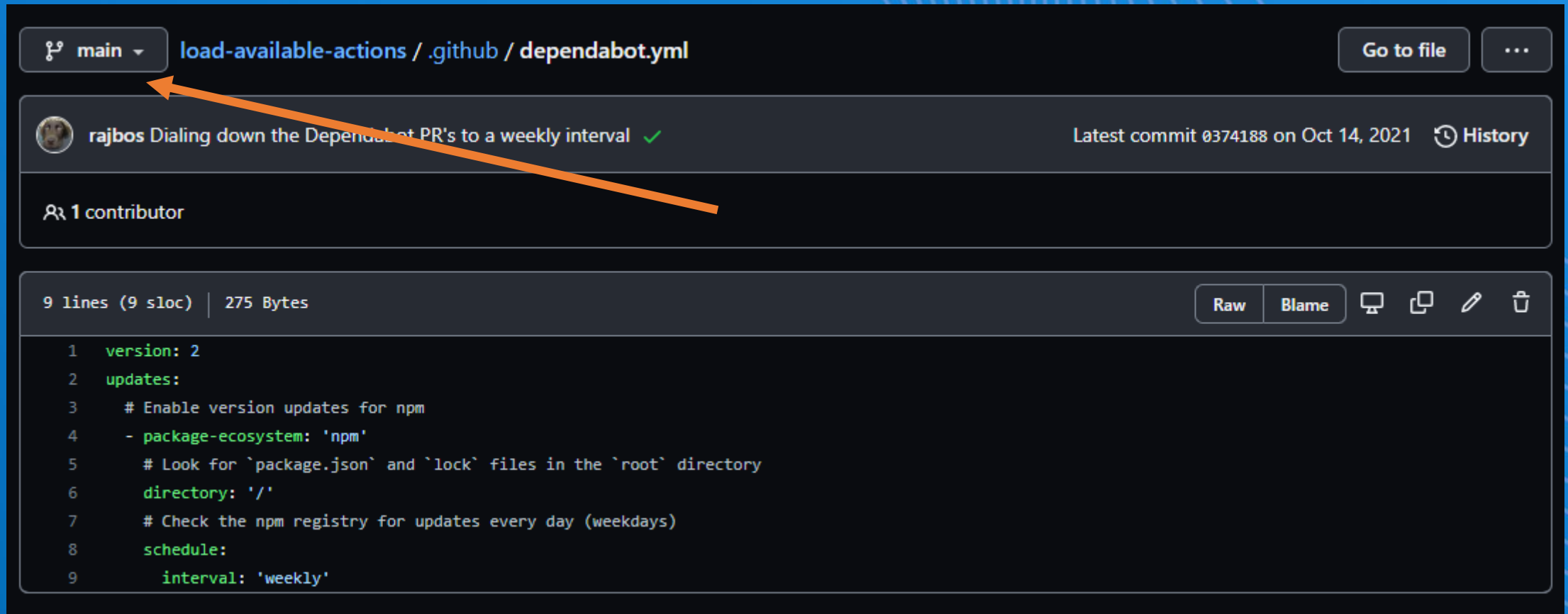


Stay up to date

- 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/307>



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



 Open 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? Convert

Assignees
No one—assign yourself

Labels
`dependencies` `.NET`

Projects
None yet

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
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"]
```


Bump @typescript-eslint/parser from 5.20.0 to 5.23.0 #98

Closed dependabot wants to merge 1 commit into `main` from `dependabot/npm_and_yarn/typescript-eslint/parser-5.23.0`

Conversation 1 Commits 1 Checks 2 Files changed 2

dependabot bot commented 11 days ago Contributor

Bumps @typescript-eslint/parser from 5.20.0 to 5.23.0.

- ▶ Release notes
- ▶ 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

Newer version available

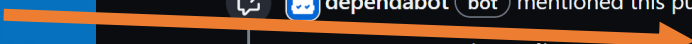


Bump @typescript-eslint/parser from 5.20.0 to 5.23.0 Verified ✓ 086145f

dependabot bot added dependencies javascript labels 11 days ago

dependabot bot mentioned this pull request 11 days ago

Bump @typescript-eslint/parser from 5.20.0 to 5.22.0 #92 Closed



dependabot bot commented on behalf of github 4 days ago Contributor Author

Superseded by #102.

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

rob-demo / security-demo Private

Watch 0 Fork 0 Star 0

Code Issues Pull requests Actions Projects Wiki Security Insights Settings

General

Access

Collaborators and teams

Team and member roles

Code and automation

Branches

Actions

Webhooks

Environments

Codespaces

Pages

Security

Code security and analysis

Deploy keys

Secrets

Integrations

GitHub apps

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 **Enable**

GitHub Advanced Security features are billed per active committer in private repositories. [Learn more.](#)

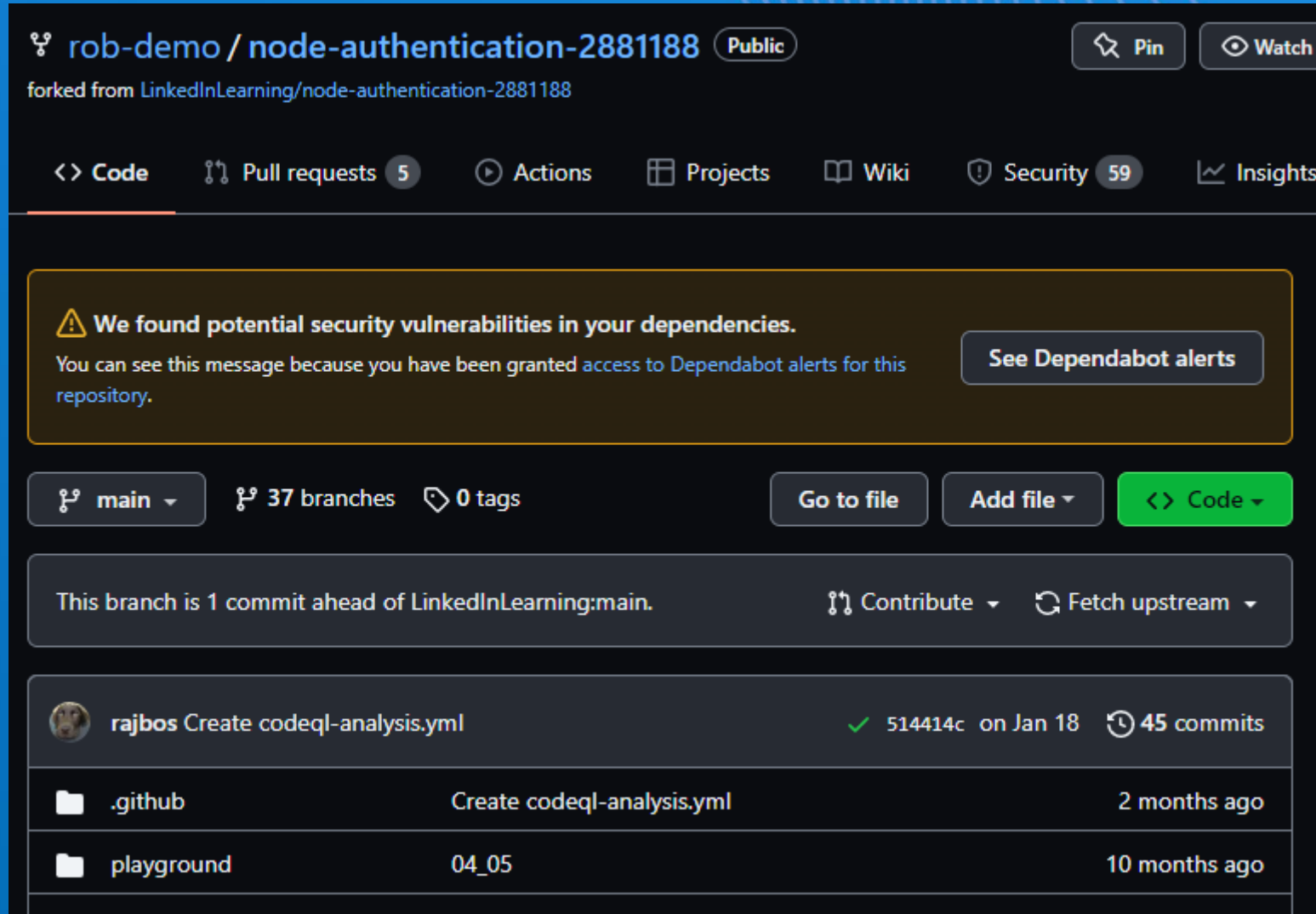
Code scanning Automatically detect common vulnerabilities and coding errors. **Set up**

Secret scanning **Enable**

Demo

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

DEMO: Security alerts on dependencies



The screenshot shows a GitHub repository page for 'rob-demo / node-authentication-2881188'. The repository is public and forked from 'LinkedInLearning/node-authentication-2881188'. The navigation bar includes 'Code', 'Pull requests 5', 'Actions', 'Projects', 'Wiki', 'Security 59', and 'Insights'. A prominent yellow warning box with a triangle icon contains the text: '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.' A button labeled 'See Dependabot alerts' is located to the right of the text. Below the warning box, the repository's main branch is 'main', with 37 branches and 0 tags. The current branch is 1 commit ahead of the upstream 'main' branch. The commit history shows a commit by 'rajbos' titled 'Create codeql-analysis.yml' on Jan 18, with 45 commits. The file list includes '.github' (created 2 months ago) and 'playground' (created 10 months ago).

rob-demo / node-authentication-2881188 Public Pin Watch


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

The screenshot shows the GitHub interface for a repository named 'rob-demo / node-authentication-2881188'. The 'Security' tab is active, displaying 59 alerts. A sidebar on the left lists navigation options: Overview, Security policy, Security advisories, Dependabot alerts (49), Code scanning alerts (10), and Secret scanning alerts. The main content area is titled 'Dependabot alerts' and includes a search bar with the text 'is:open'. Below the search bar, there are filters for '49 Open' and '1 Closed', and dropdown menus for 'Severity', 'Package', 'Ecosystem', 'Manifest', and 'Sort'. The alert list contains three entries, all for the package 'url-parse (npm) · todolist/package-lock.json'. The first two are 'Moderate' severity and the third is 'Critical'. Each entry includes a green bug icon, a '#6' identifier, and a timestamp indicating when the alert was opened.

rob-demo / node-authentication-2881188 Public Pin Watch 0 Fork 16 Star 0

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

is:open

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. The 'Dependency graph' is enabled. 'Dependabot alerts' are enabled. 'Dependabot security updates' are highlighted with an orange box and are enabled. 'GitHub Advanced Security' is also highlighted with an orange box and is enabled. The 'Code scanning' feature is set to 'Set up', and 'Secret scanning' is enabled. The left sidebar shows the 'Security' section is selected, with 'Code security and analysis' highlighted.

rob-demo / security-demo Private

Watch 0 Fork 0 Star 0

Code Issues Pull requests Actions Projects Wiki Security Insights Settings

General

Access

Collaborators and teams

Team and member roles

Code and automation

Branches

Actions

Webhooks

Environments

Codespaces

Pages

Security

Code security and analysis

Deploy keys

Secrets

Integrations

GitHub apps

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 **Enable**

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: Security alerts on dependencies

The screenshot shows a GitHub pull request titled "Bump url-parse from 1.4.7 to 1.5.10 in /todolist #6". At the top right, there are "Edit" and "Code" buttons. Below the title, a green "Open" button is followed by the text "dependabot wants to merge 1 commit into main from dependabot/npm_and_yarn/todolist/url-parse-1.5.10".

A prominent yellow warning box contains the message: "This automated pull request fixes a security vulnerability" with a "Critical severity" label. Below this, it states: "Only users with access to Dependabot alerts can see this message. Learn more about Dependabot security updates, opt out, or give us feedback."

The PR navigation bar shows: Conversation (0), Commits (1), Checks (2), and Files changed (1). On the right, a status bar indicates "+6 -6" with a color-coded progress indicator.

The main content area shows a comment from the "dependabot" bot, dated "5 days ago". The comment text is: "Bumps url-parse from 1.4.7 to 1.5.10." Below this, there is a "Commits" section and a "compatibility 75%" badge. The comment continues: "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." At the bottom of the comment, there is a "Dependabot commands and options" section.

On the right side of the PR, there are sections for "Reviewers" (No reviews, "Still in progress? Convert to draft"), "Assignees" (No one—assign yourself), "Labels" (dependencies), and "Projects" (None yet).

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>
- [unshiftdio/url-parse#197](https://unshiftdio.com/issue/unshiftio/url-parse#197)
- [unshiftdio/url-parse@d1e7e88](https://unshiftdio.com/issue/unshiftio/url-parse@d1e7e88)
- [unshiftdio/url-parse@1.4.7...1.5.0](https://unshiftdio.com/issue/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

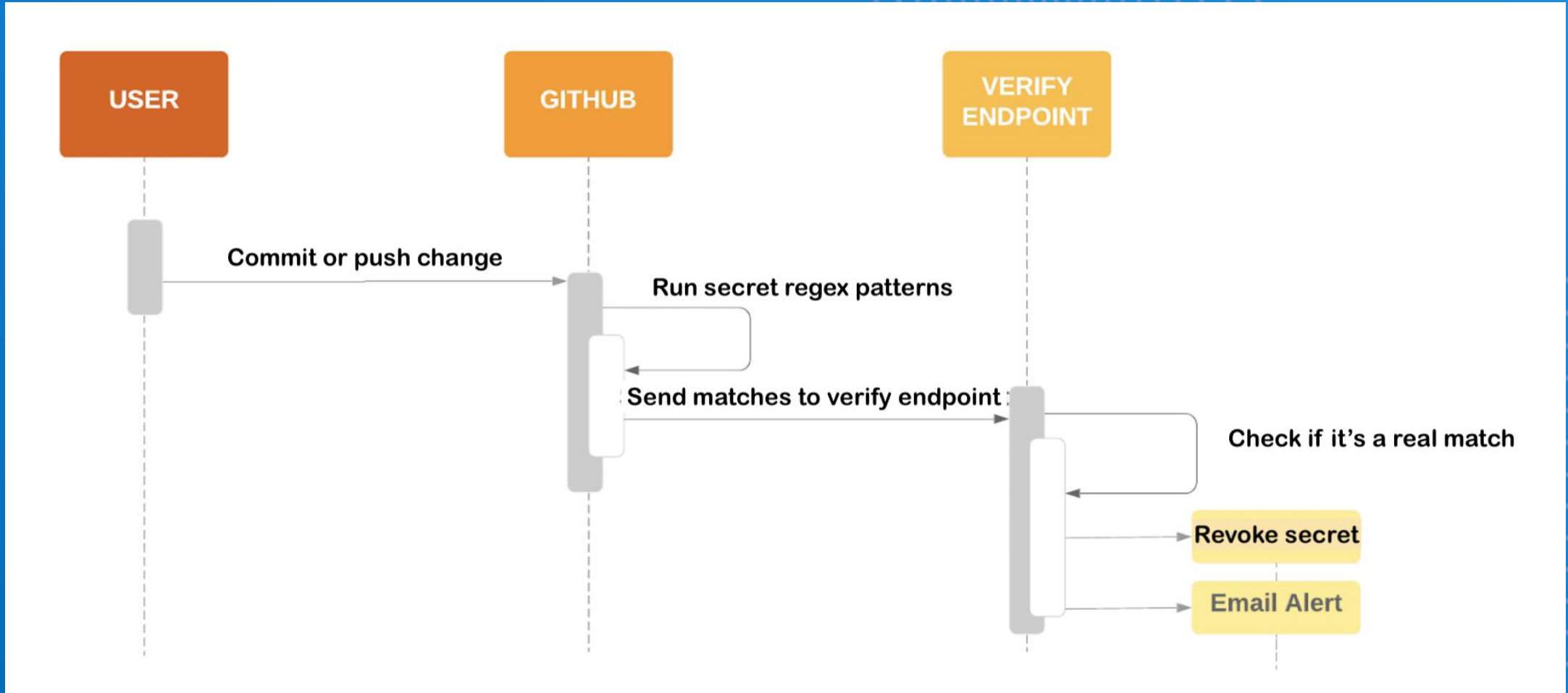
Secrets have a high risk!

Enabled by default on public repos

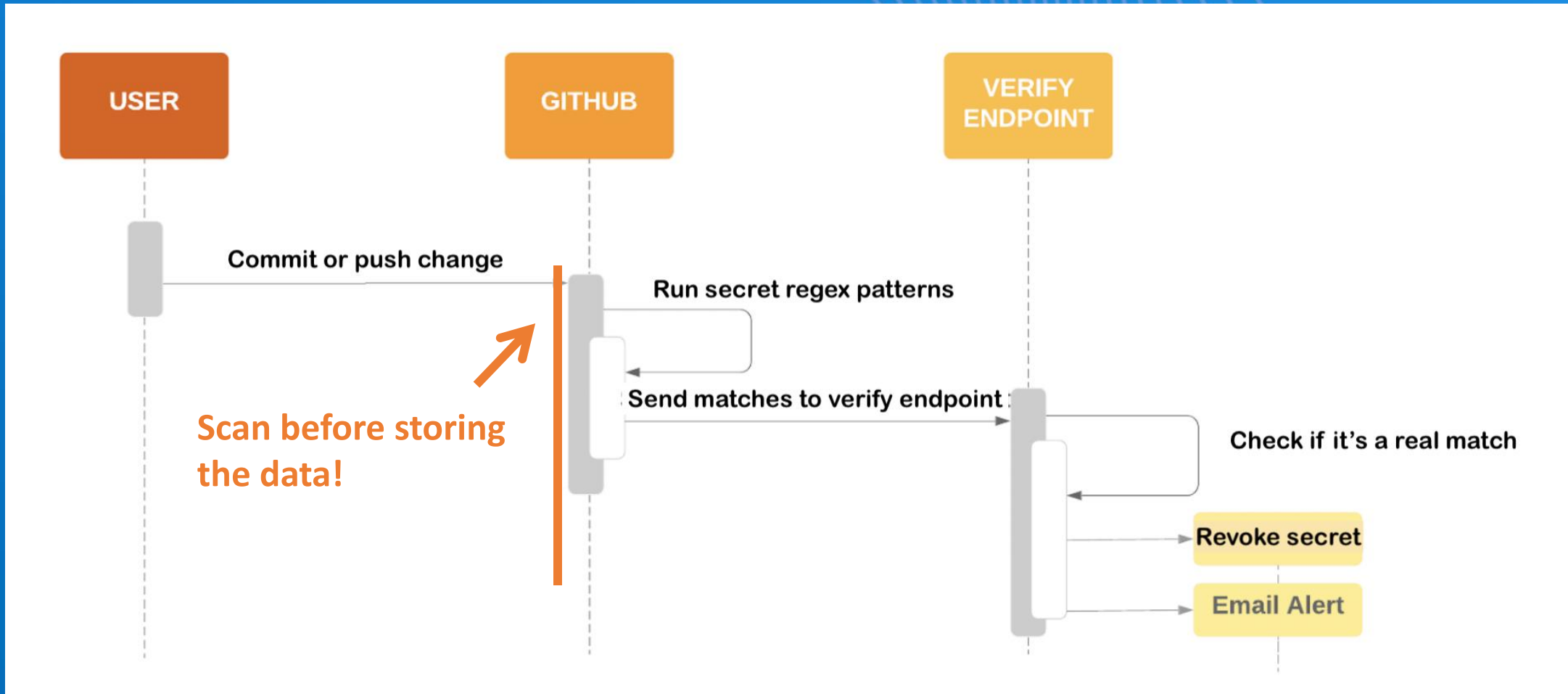
120+ secret scanning partners

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

Secret scanning



Secret scanning – push protection



Enable push protection for your account

- https://github.com/settings/security_analysis

The screenshot displays the GitHub account settings page for security analysis. On the left, a sidebar lists various settings categories: Code, planning, and automation; Repositories; Codespaces; Packages; Copilot; Pages; Saved replies; Security; Integrations; Applications; and Scheduled reminders. The 'Security' category is selected, and 'Code security and analysis' is highlighted with an orange box and an arrow pointing to the main content area.

Code, planning, and automation

- Repositories
- Codespaces
- Packages
- Copilot
- Pages
- Saved replies

Security

- Code security and analysis**

Integrations

- Applications
- Scheduled reminders

Dependabot pull requests to resolve these vulnerabilities. [Configure alert notifications.](#)

- Automatically enable for new repositories

Dependabot security updates Disable all Enable all

Allow Dependabot to open pull requests automatically to resolve Dependabot alerts.

- Automatically enable for new repositories

Secret scanning Disable all Enable all

Receive alerts on GitHub for detected secrets, keys, or other tokens.

- Automatically enable for new public repositories

Push protection Disable all Enable all

Block commits that contain [supported secrets](#).

- Automatically enable for repositories added to 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>

Security features

Commit signing

Dependabot

Security alerts on dependencies

Secret scanning

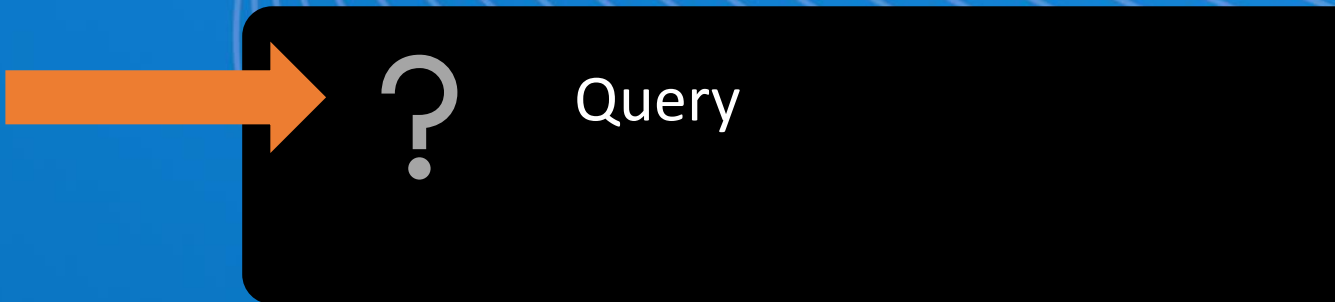
CodeQL

CodeQL – What is it?

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



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



Using CodeQL

Free for public repos, uses your own Action minutes

CLI support

Open-source queries

Support for:

javascript

c#

java

c++

go

python

ruby

kotlin

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 Actions workflow named "CodeQL" (ID #78) in the repository "rajbos / dotnetcore-webapp". The workflow is in a "Success" state, triggered via a schedule 2 days ago. The total duration of the workflow is 2m 41s. The workflow consists of two jobs: "Analyze (csharp)" and "Analyze (javascript)". A matrix named "Matrix: Analyze" is used to run these jobs in parallel. The "Analyze (csharp)" job took 2m 27s, and the "Analyze (javascript)" job took 1m 31s. The workflow is triggered via a schedule.

rajbos / dotnetcore-webapp Public Pin Unwatch 2 Fork 136 Star 6

[Code](#) [Issues](#) [Pull requests](#) **Actions** [Projects](#) [Wiki](#) [Security 6](#) [Insights](#) [Settings](#)

CodeQL CodeQL #78 Re-run all jobs

Summary

Triggered via schedule 2 days ago	Status	Total duration	Artifacts
rajbos <small>1ac525d</small>	Success	2m 41s	—

Jobs

- Analyze (csharp)
- Analyze (javascript)

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	Branch	Workflow	Lines scanned	Duration	Result
2 days ago	main	CodeQL	143 / 269 ⓘ	2m 19s	0 alerts

Filters

6 Open 0 Closed Tool Branch Rule Severity Sort

- Inefficient regular expression** High main
dotnet-core-webapp/.../dist/jquery.validate.js:1394 • Detected on Feb 4, 2021 by CodeQL
- Inefficient regular expression** High main
dotnet-core-webapp/.../dist/additional-methods.js:1092 • Detected on Feb 4, 2021 by CodeQL
- Inefficient regular expression** High main
dotnet-core-webapp/.../dist/additional-methods.js:1092 • Detected on Feb 4, 2021 by CodeQL
- Unsafe expansion of self-closing HTML tag** Medium main
dotnet-core-webapp/.../dist/jquery.js:5796 • Detected on Nov 12, 2020 by CodeQL
- DOM text reinterpreted as HTML** Medium main
dotnet-core-webapp/.../js/bootstrap.bundle.js:1076 • Detected on Nov 12, 2020 by CodeQL
- DOM text reinterpreted as HTML** Medium main
dotnet-core-webapp/.../js/bootstrap.js:1077 • Detected on Nov 12, 2020 by CodeQL

Security features – overview

Commit signing

Dependabot

Security alerts on dependencies

Secret scanning

CodeQL

Don't forget to
vote for this session
in the **GOTO Guide app**

Protect your code with GitHub security features



Rob Bos
DevOps Consultant – Xebia | Xpirit
The Netherlands

