Protect your code with GitHub security features

NDC { Security }

https://myoctocat.com

@robbos81

Protect your code with GitHub security features

NDC { Security }

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 "npmg" 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?

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!

@robbos81   10

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

https://xpir.it/commit-signing

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

Commit signing

Vigilant mode

https://xpir.it/vigilant-mode

Vigilant mode

Vigilant mode

Status	Commit signed?	Signature verified?	Commit matches author?
Verified	☑	☑	☑
Partially verified	☑	☑	✘
Unverified	☑	✘	
	✘		
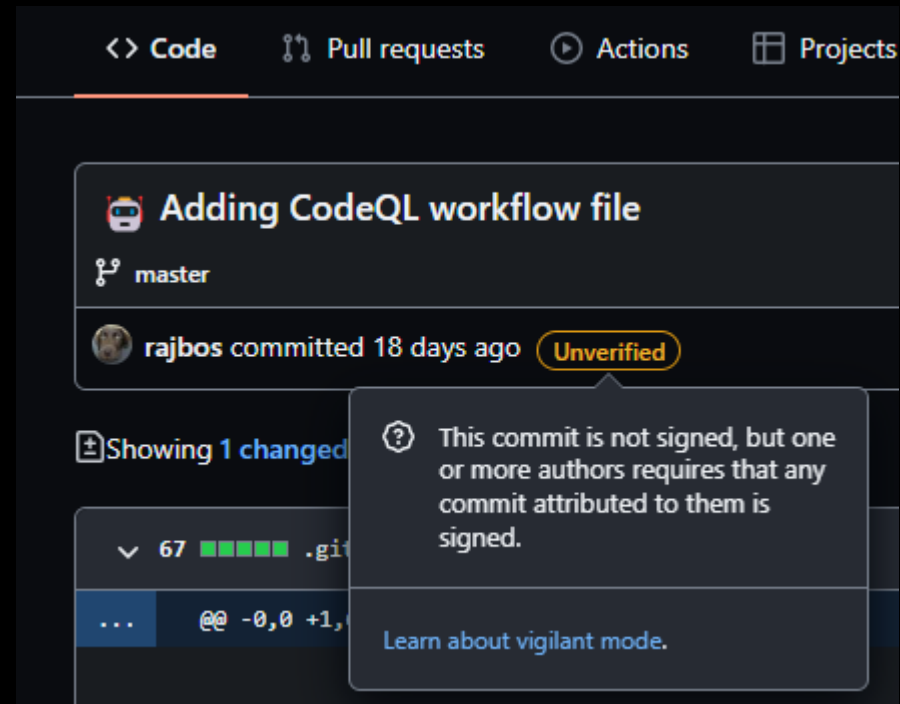
Vigilant mode

Next step:

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.

General

Access

Collaborators

Moderation options

Code and automation

Branches

Actions

Webhooks

Environments

Pages

Security

Code security and analysis

Deploy keys

Secrets

Integrations

GitHub apps

Email notifications

Autolink references

@robbos81

22

Require signed commits – impact

Users' setup – needs to install 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
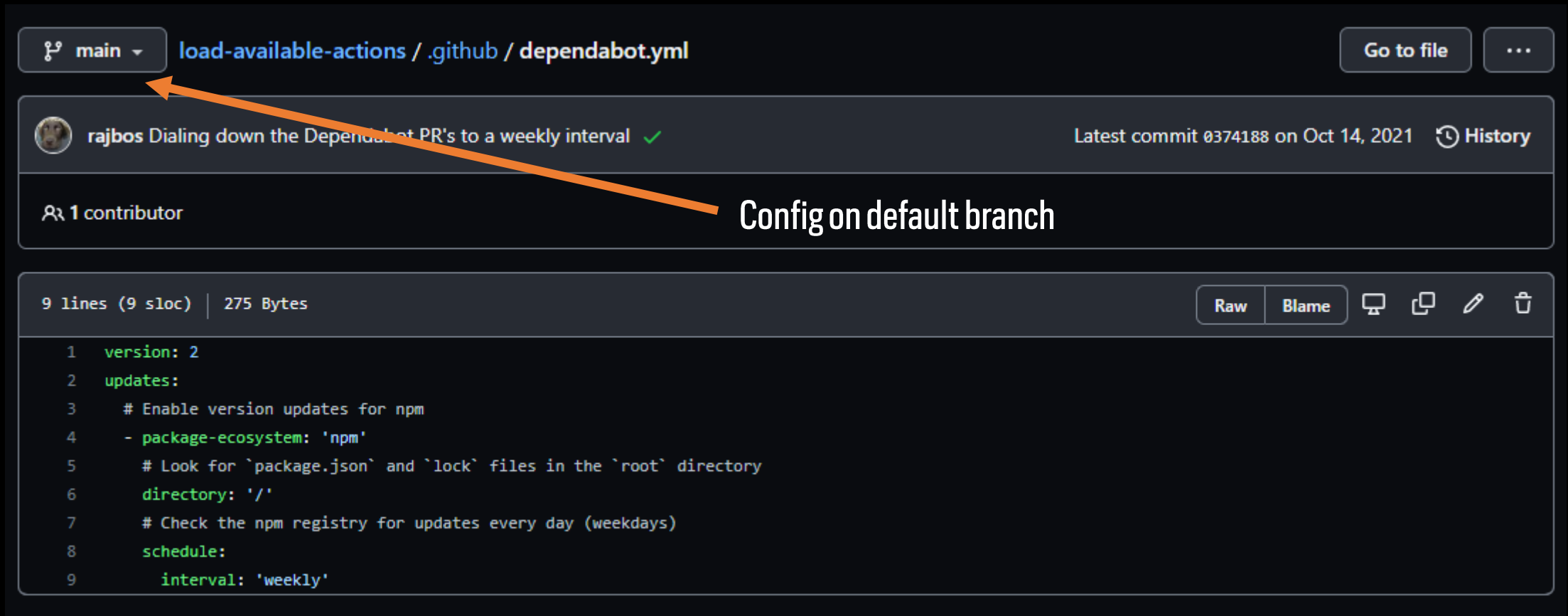
Commit signing
Dependabot
Security alerts on dependencies
Secret scanning
CodeQL

Stay up to date

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

Dependabot config

Config on default branch

Dependabot demo

https://github.com/devops-actions/load-available-actions/pull/151

▼ 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)

```yaml
# 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"]
```

```yaml
# 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"
```

```yaml
# 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

@robbos81

Demo

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

DEMO: Security alerts on dependencies

DEMO: Security alerts on dependencies

DEMO: Security alerts on dependencies

DEMO: Security alerts on dependencies

DEMO: Security alerts on dependencies

Security features

Commit signing

Dependabot

Security alerts on dependencies
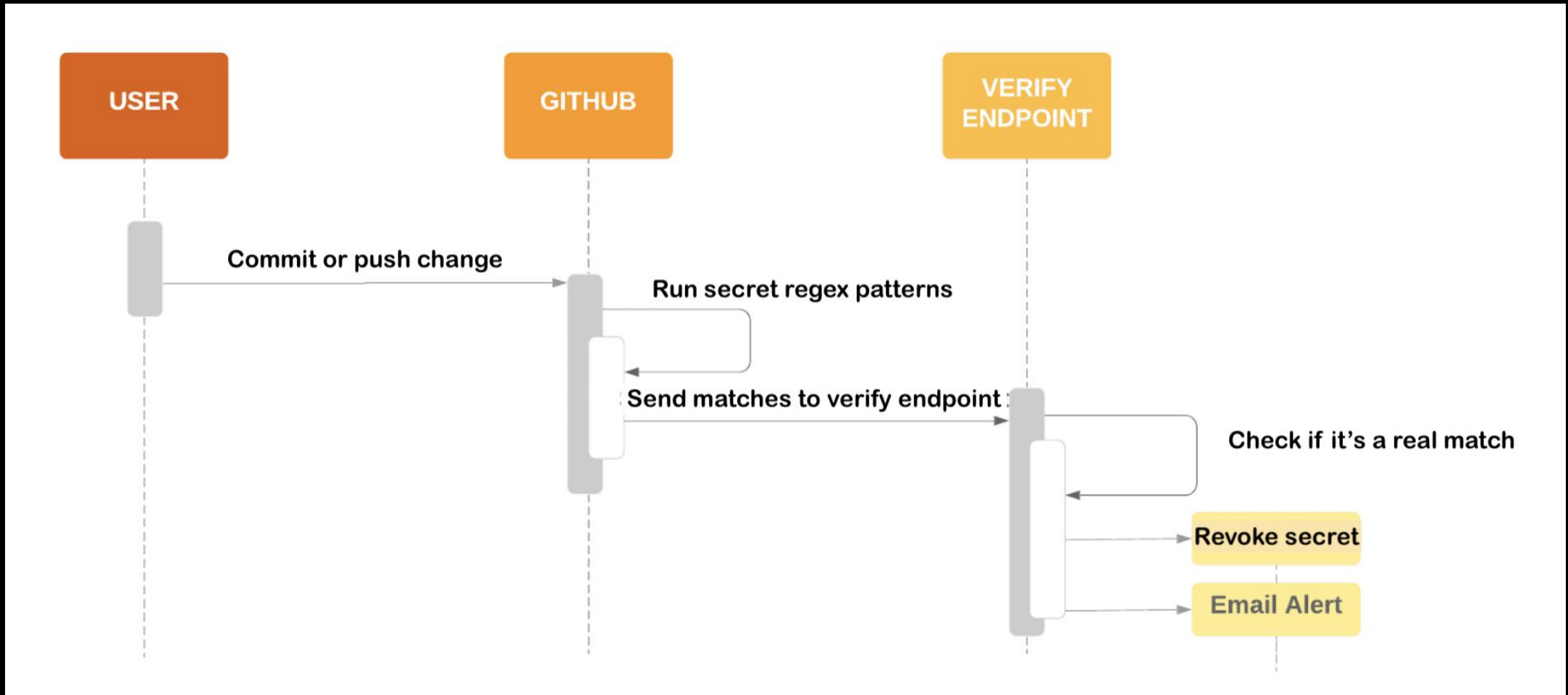
Secret scanning

CodeQL

Secret scanning

Secrets have a high risk!

Enabled by default on public repos

50+ 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

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

CodeQL – demo

Security features – overview

Commit signing

Dependabot

Security alerts on dependencies

Secret scanning

CodeQL

Protect your code with GitHub security features

NDC { Security }

Rob Bos

DevOps Consultant – Xpirit

The Netherlands

https://devopsjournal.io

@robbos81

https://myoctocat.com