OWASP London Chapter

The Iceberg: Your Attack Surface Just Got Bigger

(How to mitigate risks in your OSS projects)

Sonya Moisset | Sr. Security Advocate @ Snyk

What are we going to talk about

What is Open Source Software? 🤔

Christine Peterson coined the term “open source software” in 1998

It was a deliberate effort to make this field of endeavour more understandable to newcomers and to business

Source code that anyone can inspect, modify, and enhance

Authors make their source code available to others to view it, copy it, learn from it, change it or share it

Many people prefer using OSS for several reasons

Regarded as stable for long-term projects as they adhere to open standards and will not disappear if maintainers stop working on them

Considered more secure than proprietary software

Contributors can spot an error and raise a PR to propose some changes

Open Source Software attacks 💣

Typosquatting attacks

Bad actors push malicious packages to a registry with the hope of tricking users into installing them

```
$ npm install reeact
```

snyk.io/blog/typosquatting-attacks

Malicious packages

Inject malicious code into a software product in order to compromise dependent systems further down the chain

```
$ npm install fallguys
```

snyk.io/advisor/npm-package/fallguys

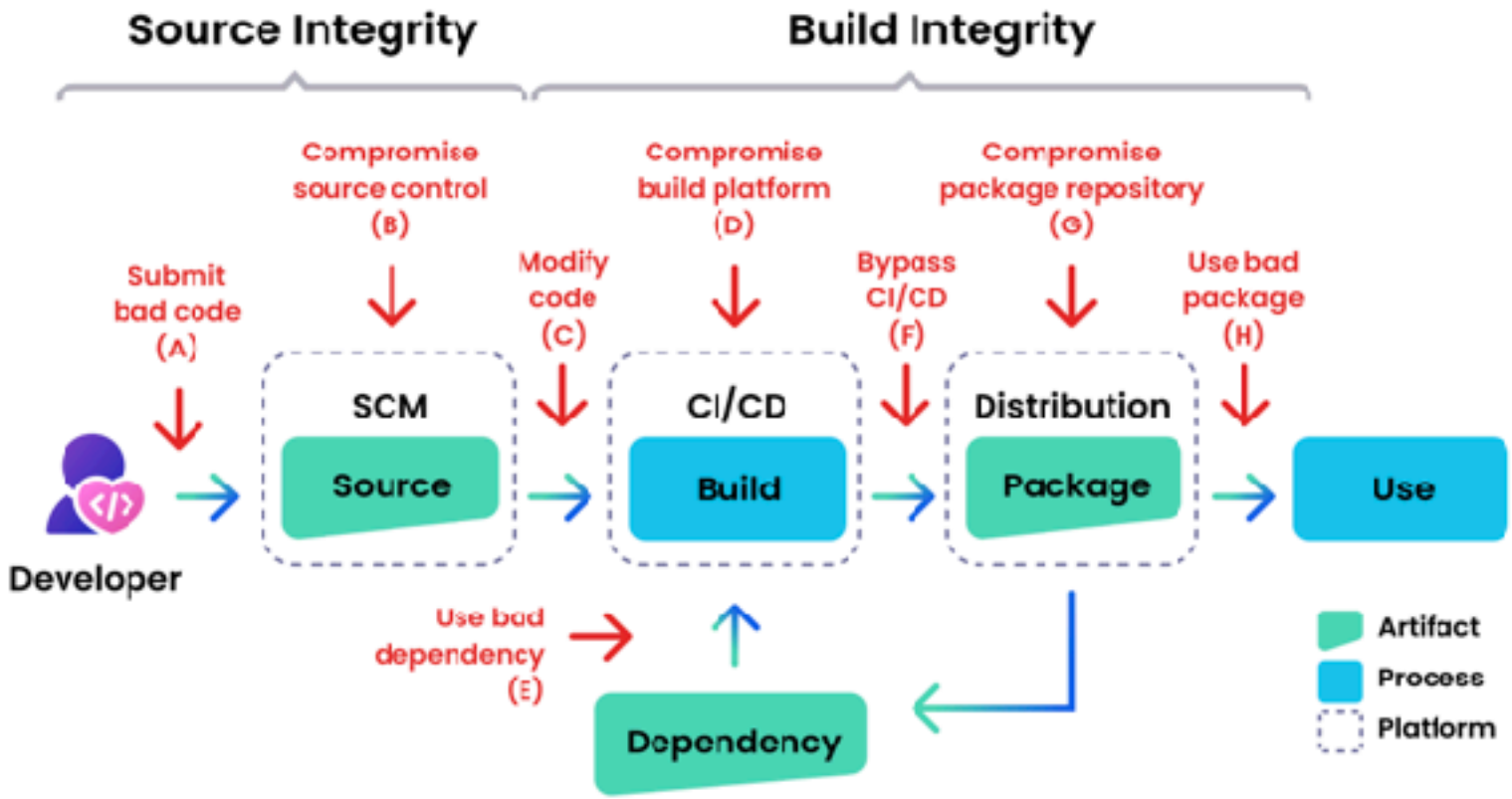
Compromised maintainers

Malicious actors will use social engineering methods to gain access to open source projects

```
$ npm install event-stream express react mailparser
```

snyk.io/blog/a-post-mortem-of-the-malicious-event-stream-backdoor

Supply Chain attacks affect all ecosystems


Source Integrity
Build Integrity
Compromise source control (B)
Compromise build platform (D)
Compromise package repository (G)
Submit bad code (A)
Modify code (C)
Bypass CI/CD (F)
Use bad package (H)
SCM
Source
CI/CD
Build
Distribution
Package
Use
Developer
Use bad dependency (E)
Dependency
Artifact
Process
Platform

Why Application Security is important?

Vulnerabilities can originate from many places

Organisations such as OWASP track vulnerabilities found, and provide a list that developers and security teams can use as a starting point

85k apps

83% At least 1 security flaw

20% 1 severe vulnerability

“

Say hi 👋 to the iceberg

”

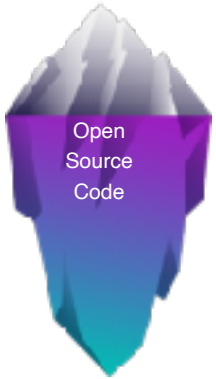
Sonya

Friendly Security 🥑

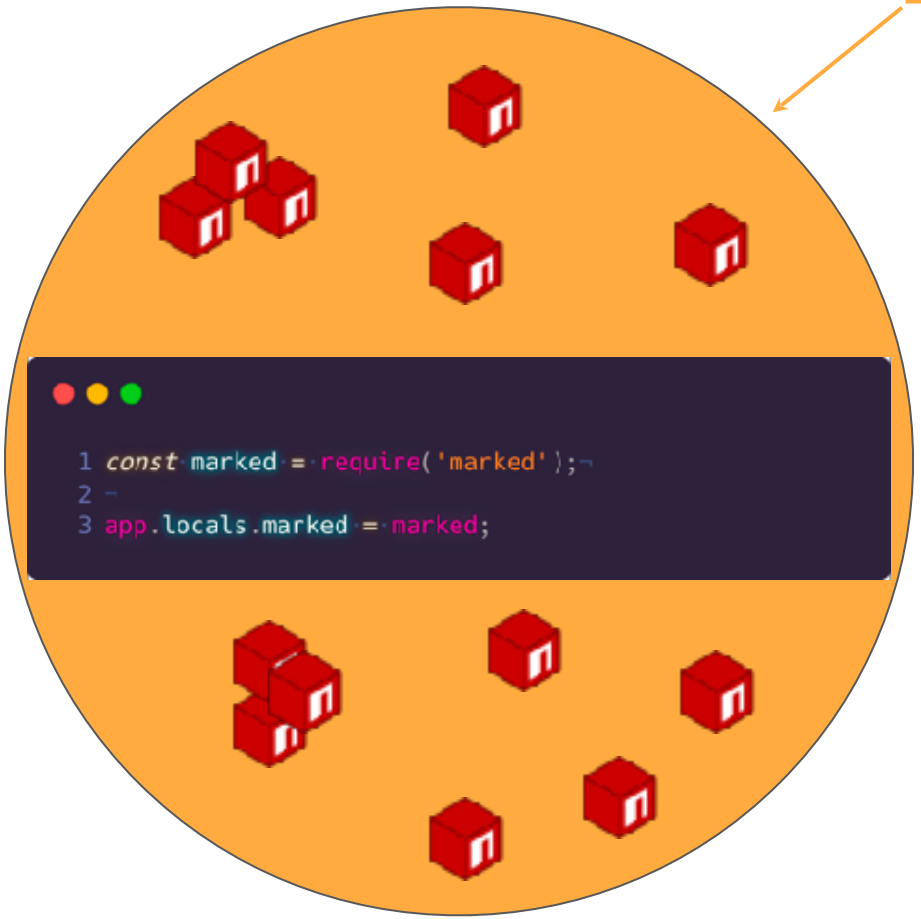
Your Code

```
1 const marked = require('marked');
2
3 app.locals.marked = marked;
```

snyk.io/advisor/npm-package/marked



Your App



```
const marked = require('marked');

app.locals.marked = marked;
```

Cybersecurity challenges in OSS

Average number of outstanding, critical vulnerabilities in an application
Ranges between 2.6 and 9.5 based on programming language

Average dependencies per project
Ranges between 25 and 174 based on programming language

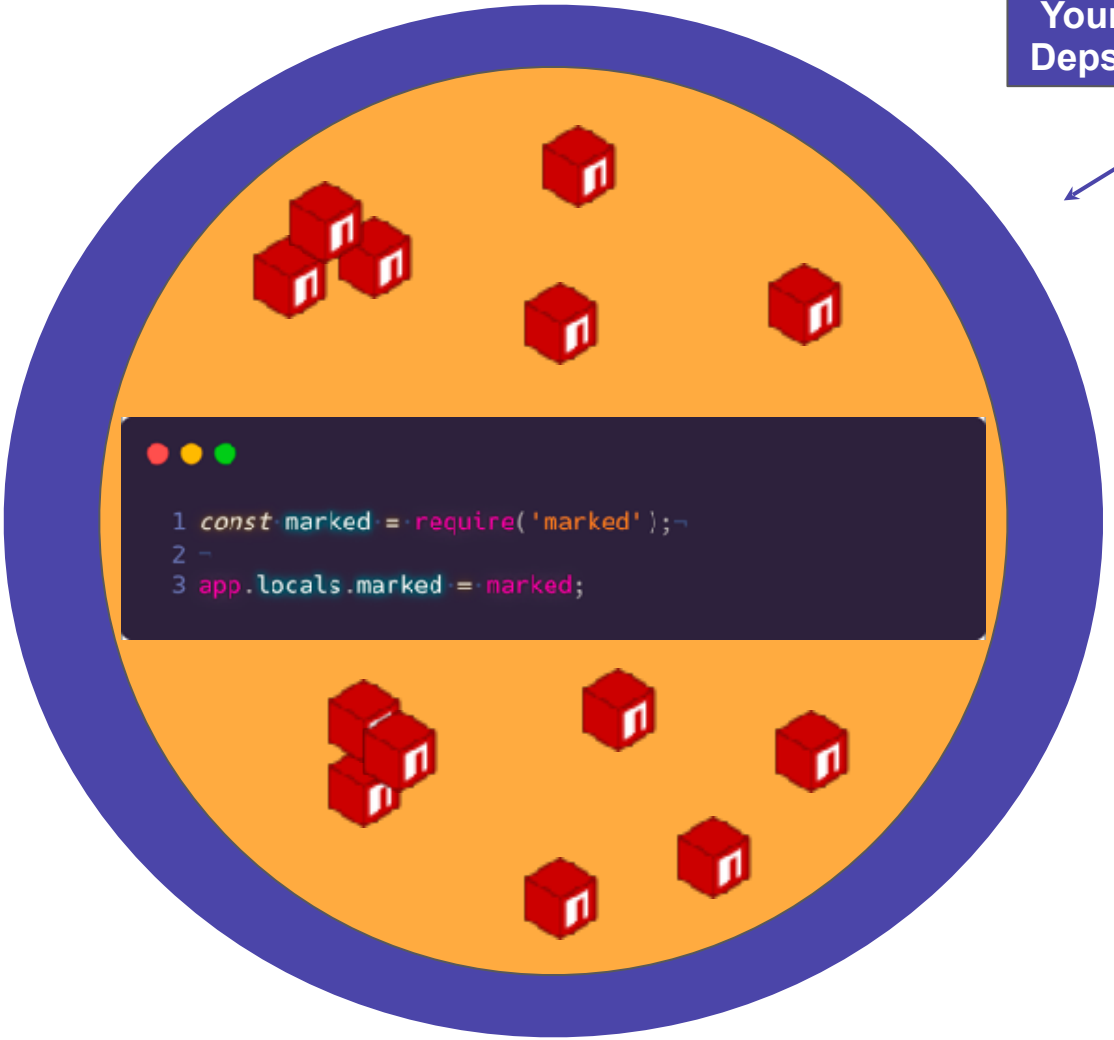
Average number of days it takes to fix a vulnerability

Let’s go back to our 

Vercel

AWS Lambda


Containers


Your Container
Deps & Runtime
1 const marked = require('marked');
2
3 app.locals.marked = marked;


```
FROM node

RUN apt-get update
RUN apt-get install -y imagemagick

COPY . /usr/src/goof
WORKDIR /usr/src/goof

RUN npm install

CMD ["npm", "start"]
```

XML Injection

Affecting imagemagick package, versions <8:6.9.7.4+dfsg-11+deb9u11

7.8
HIGH

How to fix?

NVD Description

ImageMagick before 6.9.11-40 and 7.x before 7.0.10-40 mishandles the -authenticate option, which allows setting a password for password-protected PDF files. The user-controlled password was not properly escaped/sanitized and it was therefore possible to inject additional shell commands via coders/pdf.c.

References:

- ADVISORY
- CENTOC
- MISC
- MLIST

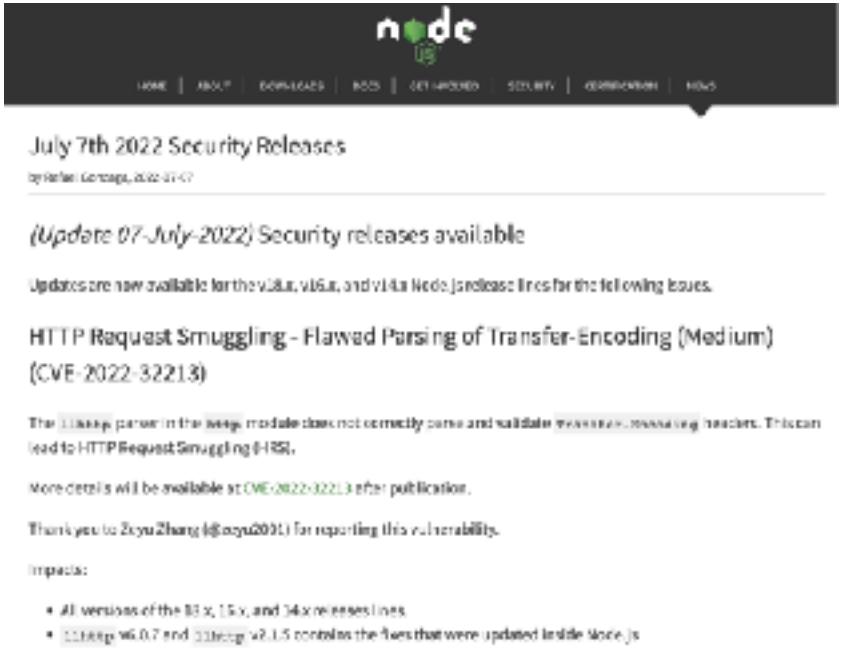
Attack Complexity: Low
User Interaction: Required
Confidentiality: High
Integrity: High
Availability: High
See more

```
FROM node

RUN apt-get update
RUN apt-get install -y imagemagick

COPY ./usr/src/goof
WORKDIR /usr/src/goof

RUN npm install

CMD ["npm", "start"]
```

Common software vulnerable?


```dockerfile
FROM node

RUN apt-get update
RUN apt-get install -y imagemagick

COPY . /usr/src/goof
WORKDIR /usr/src/goof

RUN npm install

CMD ["npm", "start"]
```

Dependencies vulnerable?



July 7th 2022 Security Releases

(Update 07-July-2022) Security releases available

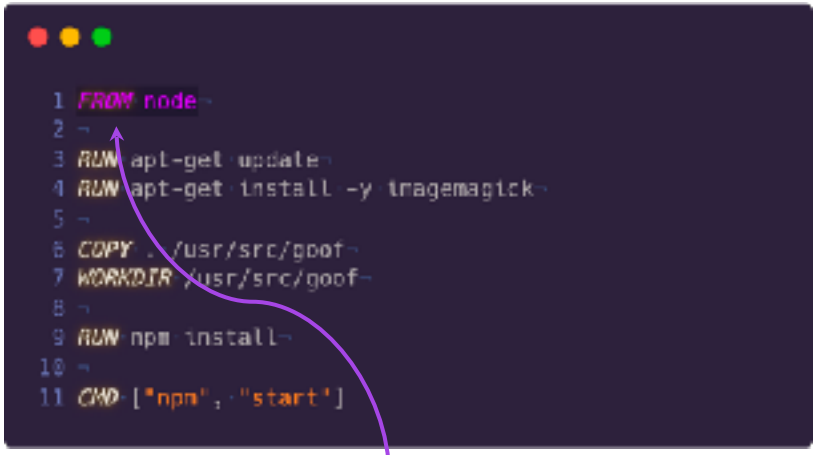
Updates are now available for the v18.x, v16.x, and v14.x Node.js release lines for the following issues.

HTTP Request Smuggling - Flawed Parsing of Transfer-Encoding (Medium) (CVE-2022-32213)

More details will be available at CVE-2022-32213 after publication.

Impacts:

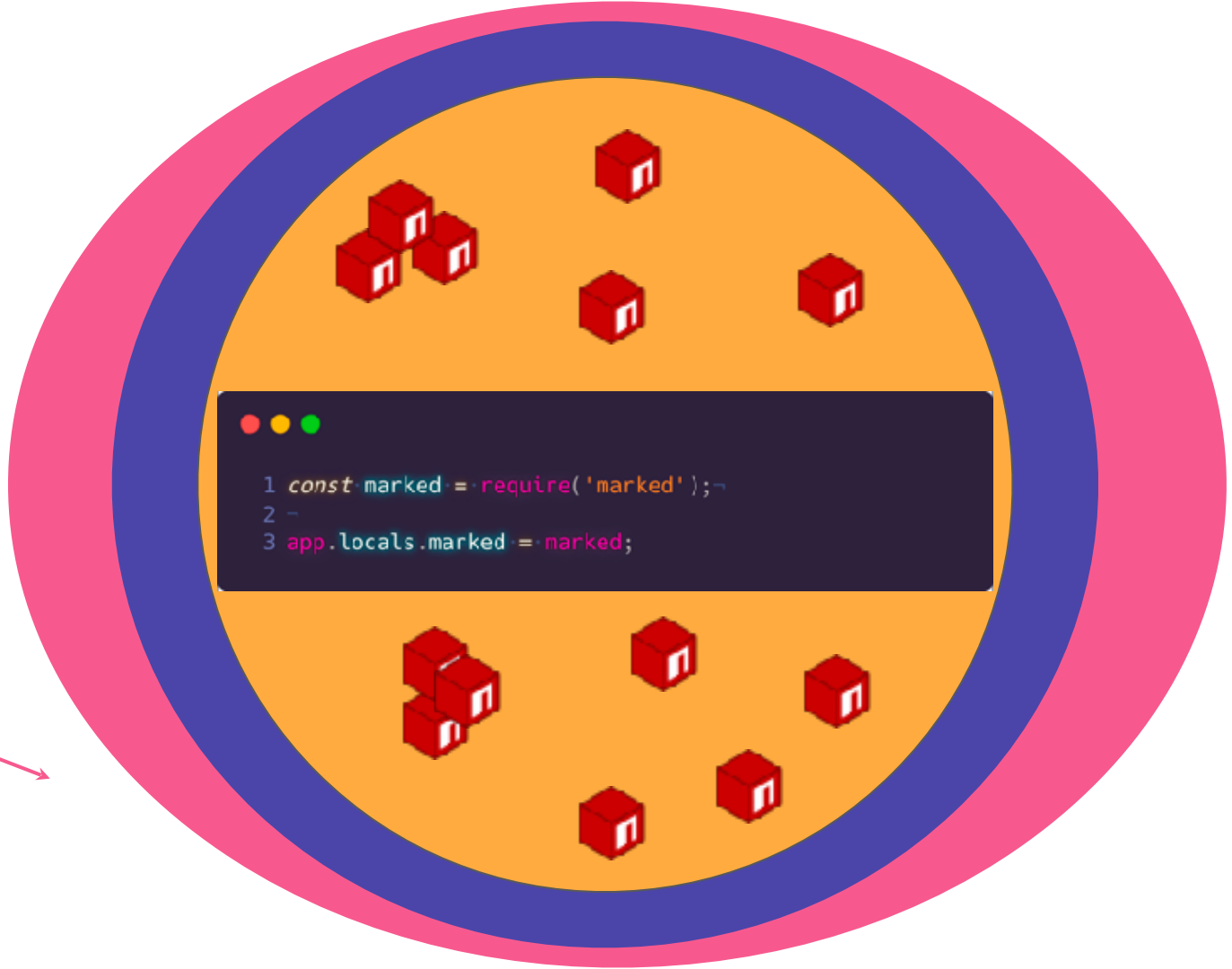
- All versions of the 18.x, 16.x, and 14.x release lines
- v6.0.7 and v2.1.5 contains the fixes that were updated inside Node.js



Runtime vulnerable?

What’s the last layer?

What else?



```
const marked = require('marked');

app.locals.marked = marked;
```

kubernetes

HELM

Terraform

#1 - Cloud Misconfiguration

Most common vulnerability organisations face

Refers to any glitches, gaps, or errors that could expose your environment to risk during cloud adoption

77M

PlayStation Network accounts hacked

57M

Customer & driver info breached via Uber's GHA/AWS creds

119k

Scanned docs in FedEx breach

The modern application

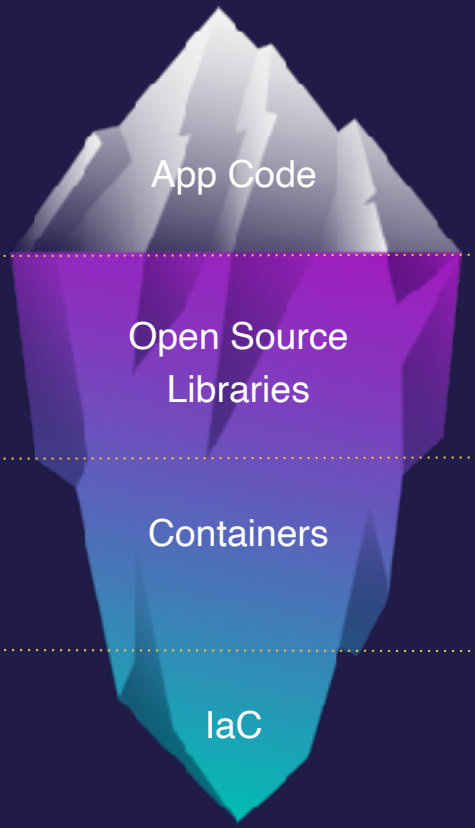
A New Risk Profile

Deployed daily - waterfall approach doesn't scale. Scans can't take hours.

80% of vulnerabilities found in indirect dependencies

100s of Linux packages, and their vulnerabilities, inherited with base images

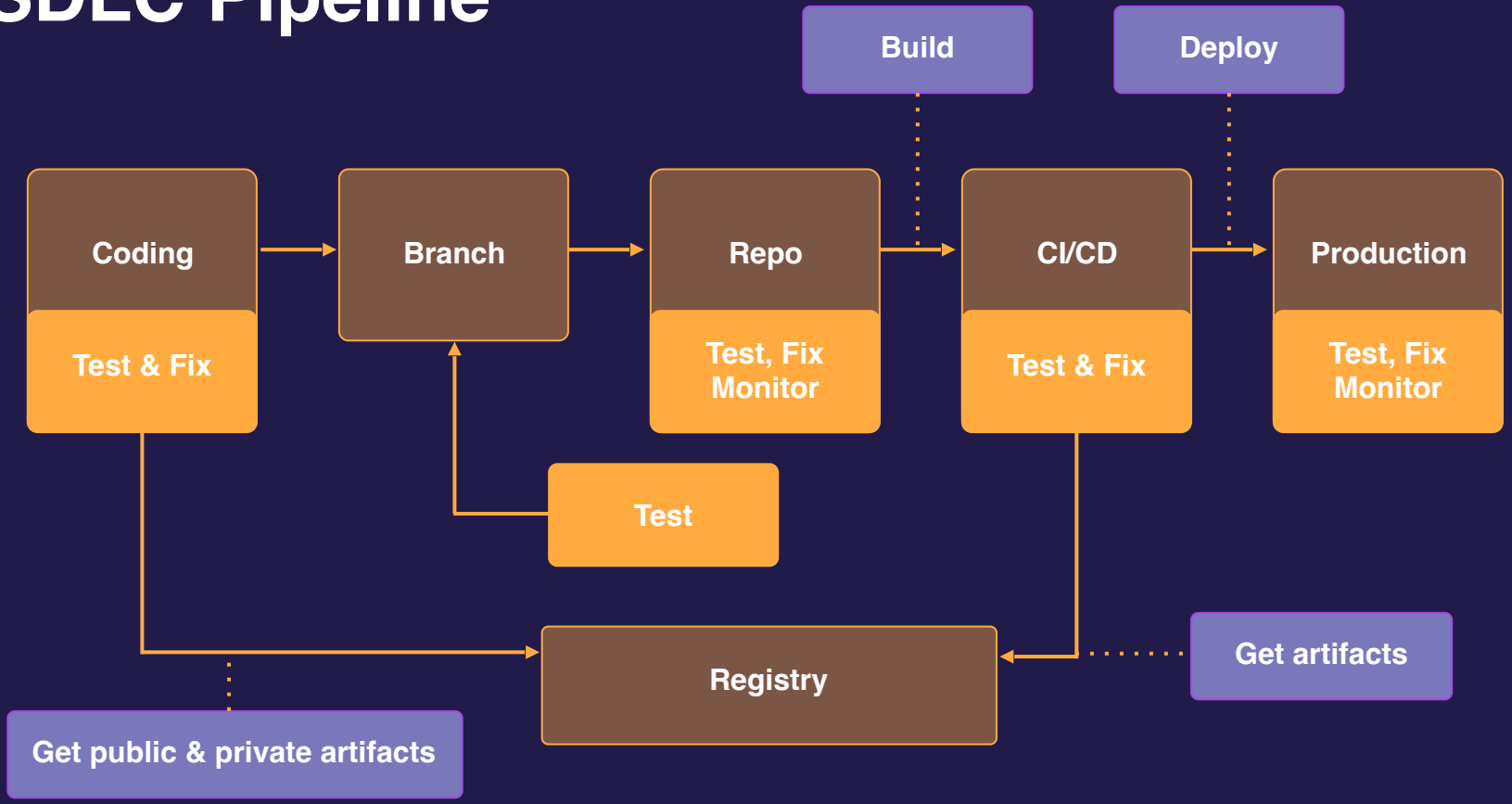
#1 cloud vulnerability is misconfiguration [NSA]



10-20% of codebase

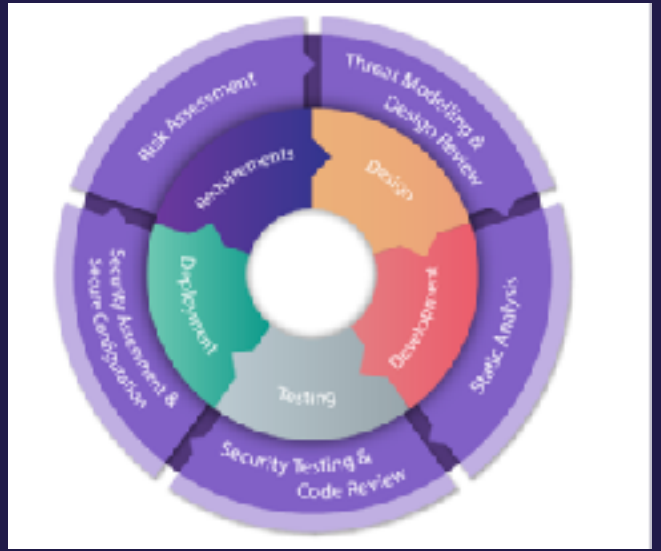
80-90% of codebase

SDLC Pipeline



Secure Software Development Lifecycle (SSDLC)

A secure SDLC process ensures that security assurance activities such as penetrating testing, code review, threat modelling sessions and architecture analysis are an integral part of the development effort



Secure Software Development Lifecycle (SSDLC)

.Security is a continuous concern

.Awareness of security considerations by stakeholders

.Early detection of flaws & cost reduction

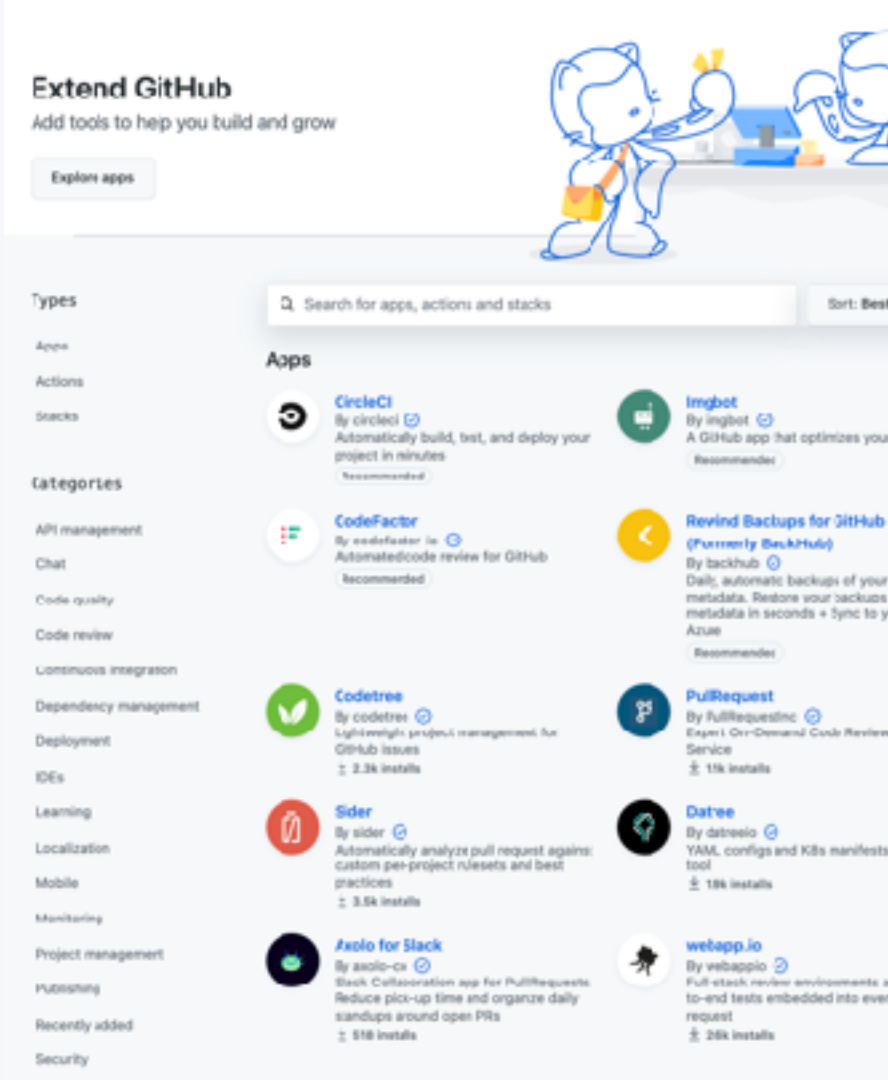
The GitHub Marketplace

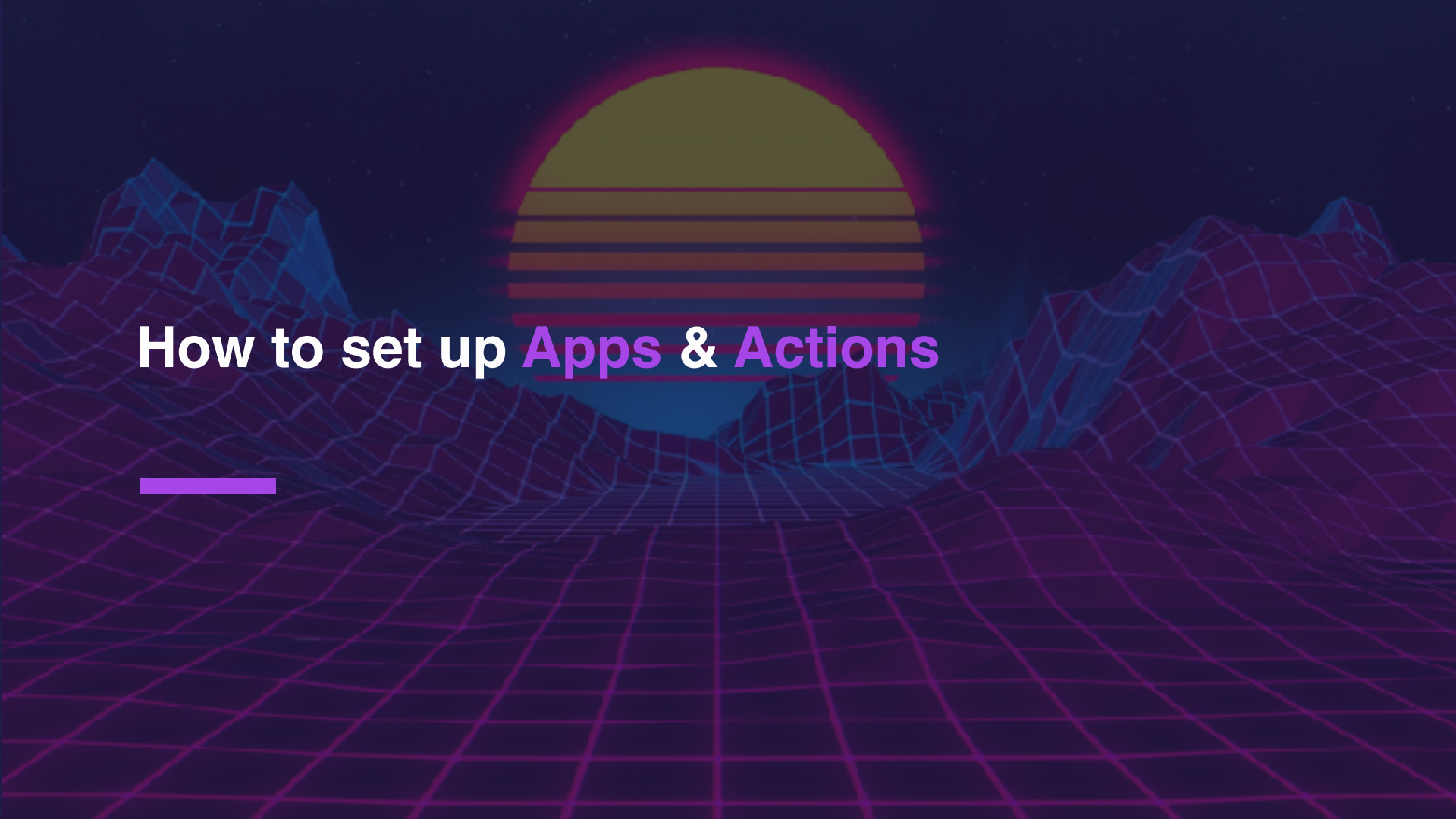
The GitHub Marketplace

.Introduced in 2016

.Makes it easier to customise your workflow with apps and actions

.Covers CI/CD tools, code review, security, compliance, dependency management, etc.




How to set up Apps & Actions

Apps

Actions

Stacks

Categories

API management

Chat

Code quality

Code review

Continuous integration

Container CI

Game CI

Mobile CI

Dependency management

Deployment

IDEs

Learning

Localization

Mobile

Monitoring

Project management

Publishing

Recently added

Security

Support

Testing

Utilities

Continuous integration

Automatically build and test your code as you push it to GitHub, preventing bugs from being deployed to production.

6196 results filtered by Continuous integration

Apps

CircleCI
By circleci
Automatically build, test, and deploy your project in minutes
Recommended

webapp.io
By webappio
Full-stack review environments and end-to-end tests embedded into every pull request
2.8k installs

Azure Pipelines
By AzurePipelines
Continuously build, test, and deploy to any platform and cloud
Recommended

Check Run Reporter
By check-run-reporter
See your test and style results without leaving GitHub. Works with any CI service. Supports JUnit, Checkstyle, and more
Not installs

GuardRails
By guardrailsio
GuardRails provides continuous security feedback for modern development teams
2.5k installs

Testspace.com
By testspace-com
Test Management software for DevOps, including CI Results Dashboard, Manual Test Case Management, and Exploratory testing
Not installs

AccessLint
By AccessLint
Find accessibility issues in your pull requests
4.6k installs

BuildPulse
By Workshop64
Automatically detect, track, and rank flaky tests so you can regain trust in your test suite
103 installs

abaplint
By tilobroichlabs
ABAP quality assurance and static analysis
376 installs

Percy
By percy
Automated visual review platform
4.2k installs

View all >

Application

CircleCI

You have already purchased this app on GitHub Marketplace

Set up a new plan | Edit your plan ▸ | Configure access

GitHub has verified that the publisher controls the domain and meets other requirements.

Categories

Continuous Integration | Mobile CI | GitHub Enterprise | Free

Supported Languages

C++, Clojure, Go
and 7 other languages supported

Customers

Developer

circleci

Verified domain

circleci.com

Developer Links

Support
Status
Documentation
Privacy Policy
Terms of Service

Organizations

About CircleCI

The world's best software teams deliver quality code, confidently, with CircleCI.

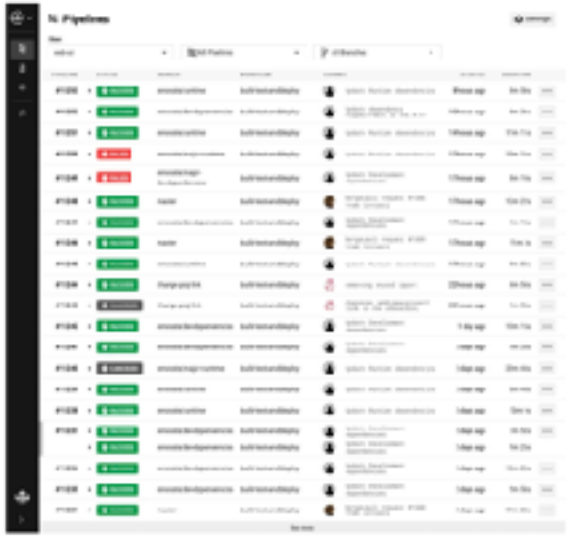
Get started in no time

CircleCI's free plan offers more build minutes than any free plan out there. Up to 6,000 build minutes/month and 30 jobs at a time.

Most customizable environments of any CI/CD provider

Widest choice to customize operating systems, CPUs, GPUs, memory and images for each job. Build for Docker, Windows, Linux, ARM and macOS or build on your own compute with runners.

Read more...



CircleCI pipeline dashboard shows all recent builds in one place. Apply filters to quickly find what you're looking for faster.

Pricing and setup

Free $0

Free for both open source and private projects

CircleCI

Free

Free for both open source and private projects

- ✓ Up to 6,000 build minutes per month
- ✓ Largest selection of Build for Docker, Windows, Linux, Arm, and macOS or on your own compute with self-hosted runners
- ✓ Build better: Choose the right resource class size (S–L) to go fast and maximize your build minutes
- ✓ Fast: Run up to 30 jobs at a time and run your tests in parallel using test splitting

Account: DevCI

Install it for free

Next: Confirm your installation location.

CircleCI is provided by a third-party and is governed by separate terms of service, privacy policy, and support documentation.

Review your order

CircleCI

Free

Free for both open source and private projects

- Up to 6,000 build minutes per month
- Largest selection: Build for Docker, Windows, Linux, Arm, and macOS or on your own compute with self-hosted runners
- Build better: Choose the right resource class size (S–L) to go fast and maximize your build minutes
- Fast: Run up to 30 jobs at a time and run your tests in parallel using test splitting

$0 /month

Order total $0.00
Free /month

Due today **$0.00**
Prorated for Sep 6th–Sep 7th

Billing information

iDevOI
Organization
Switch billing account

By clicking "Complete order and begin installation", you are agreeing to CircleCI's Terms of Service and the Privacy Policy. You previously agreed to the Marketplace Terms of Service.

The iDevOI organization has enabled OAuth App Access restrictions. You must grant CircleCI access to the iDevOI organization's data before you can begin the installation.

☐ Grant CircleCI access to iDevOI's private data.

Complete order and begin installation

Next: Authorize CircleCI to access your account.


What do you need to consider?

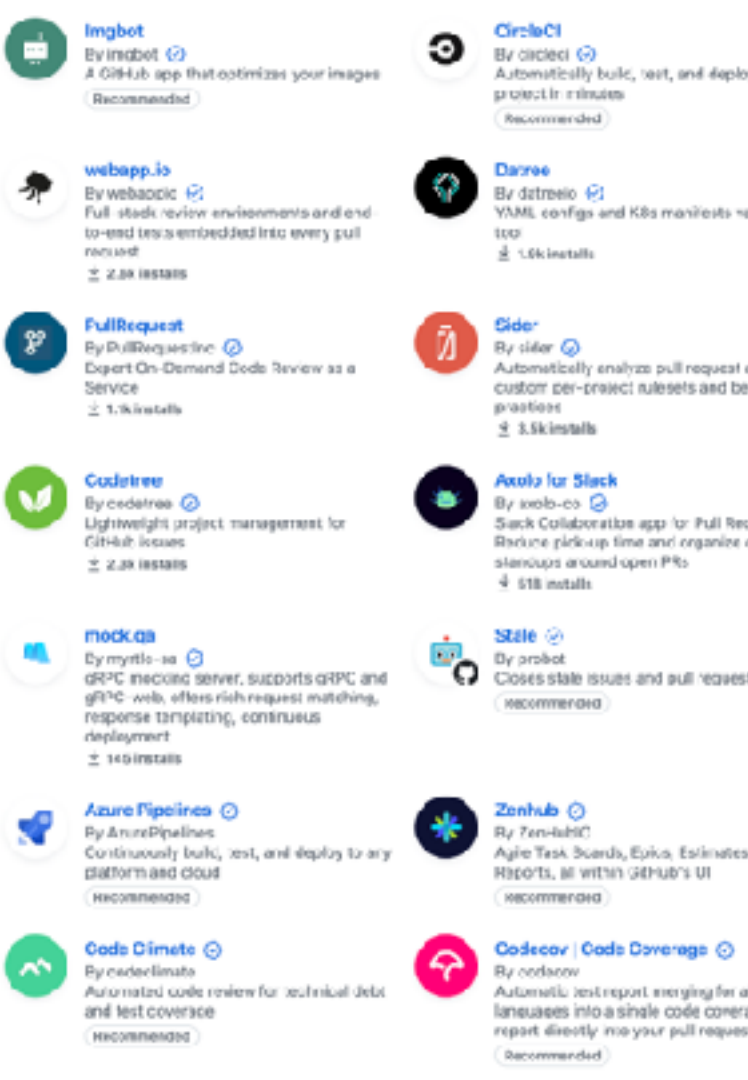
.Apps vs Actions

.Supported programming languages

.Publisher badge vs no publisher badge

.Implement at least one tool for each step in the DevOps pipeline (code review, code quality, dependencies, SAST…)

.Implement 2 tools for security (secrets, dependencies…)



“

Experiment!

”

Sonya

Friendly Security 🥑

“

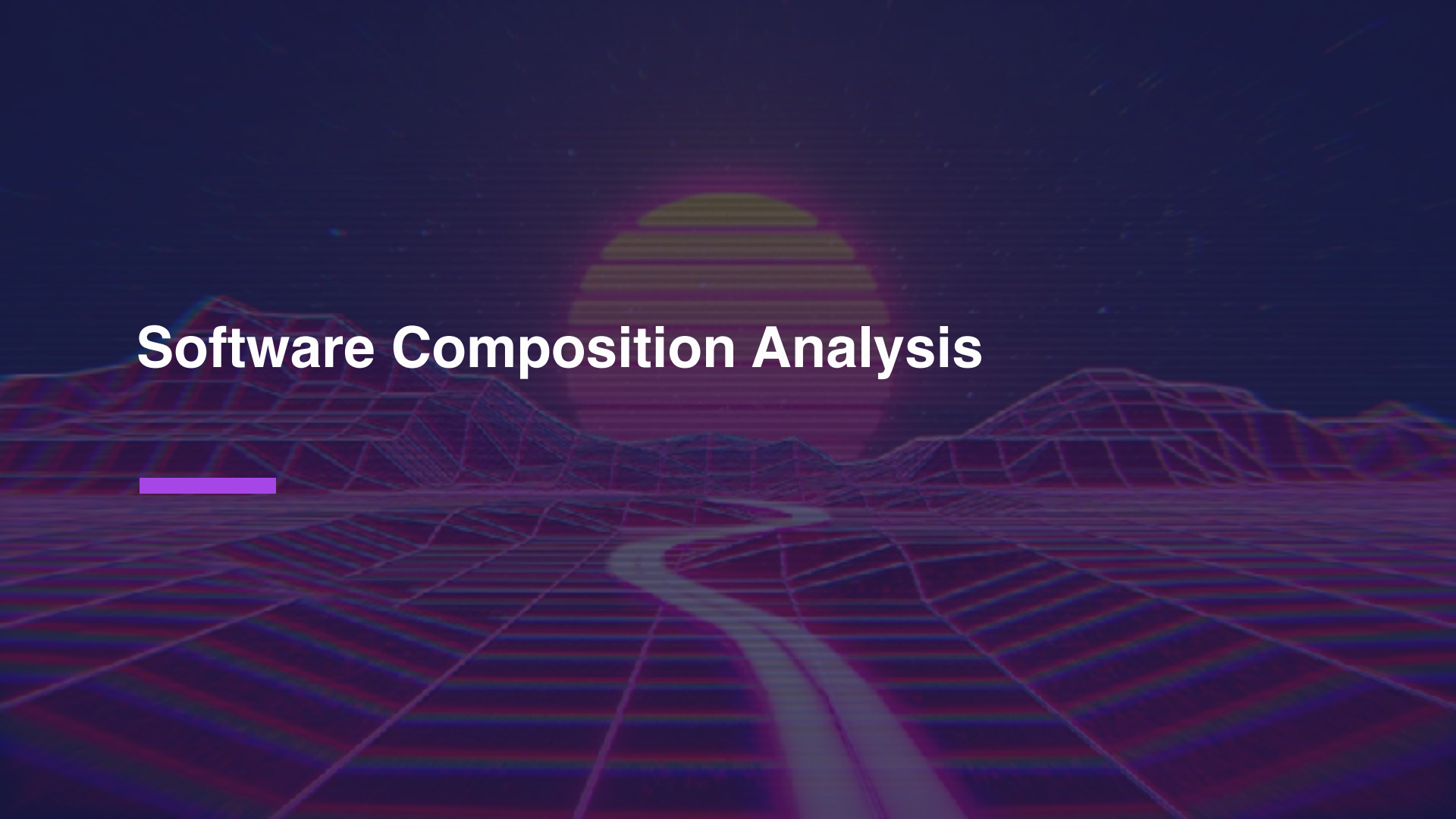
Get the right tools for your project!

”

Sonya

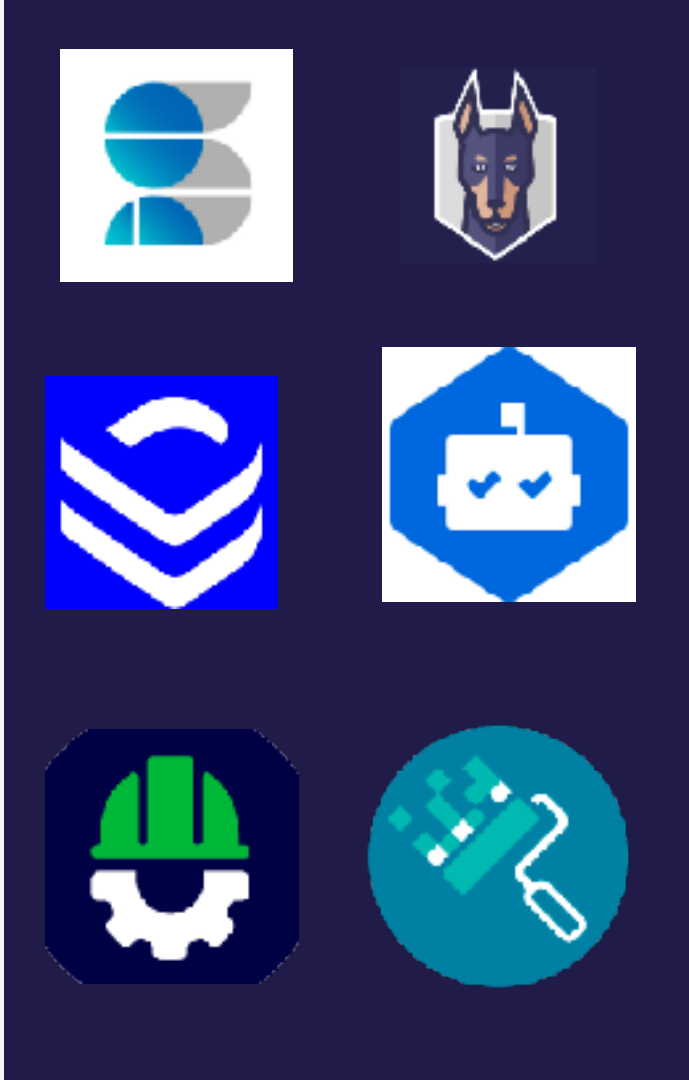
Friendly Security 🥑

Software Composition Analysis



| Synopsis

Software composition analysis (SCA) focuses on identifying the open source in a codebase so teams can manage their exposure to security and license compliance issues



Application

Renovate

You have already purchased this app on GitHub Marketplace

Set up a new plan | Edit your plan | Configure access

GitHub has verified that the application meets the requirements for listing.

Categories

Dependency management | Security | Free | GitHub Enterprise

Supported languages

Dockerfile, Go, Gradle and 7 other languages supported

Helm, Java, JavaScript, Maven POM, PHP, Python, and Ruby

Customers

Developer

renovatebot

Verified domains

renovatebot.com

Developer links

Support
Documentation
Privacy Policy
Terms of Service

Report abuse

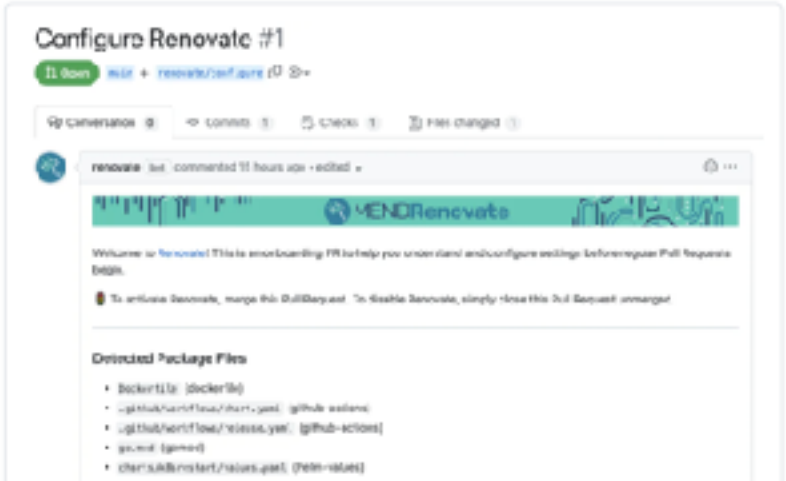
Mend Renovate | Dependency Update Automation

Renovate: an open-source tool which automatically creates pull requests for all types of dependency updates. Includes crowdsourced test and package adoption data are used to flag potentially risky updates and enable auto-merging for those that meet user-defined conditions.

How Renovate works:

- Scans your repos to detect dependencies (wide package manager support)
- Checks if any newer versions exist
- Raises PRs for available updates

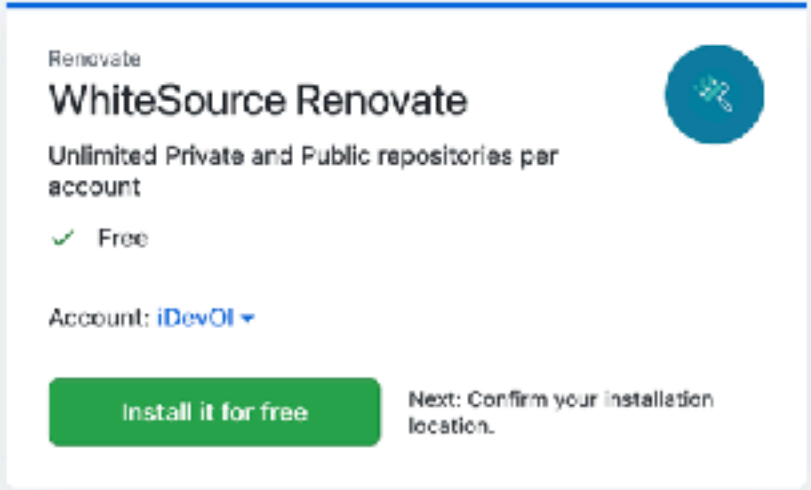
Read more...



Pricing and setup

WhiteSource Renovate $0

Unlimited Private and Public repositories per account



Renovate is provided by a third-party and is governed by separate terms of service, privacy policy, and support documentation.

Configure Renovate #12

Edit Code

Open renovate wants to merge 1 commit into `main` from `renovate/configure`

Conversation 2 · Commits 1 · Checks 8 · Files changed 1

renovate bot commented on 18 Oct 2021 • edited

MEND Renovate

Welcome to Renovate! This is an onboarding PR to help you understand and configure settings before regular Pull Requests begin.

To activate Renovate, merge this Pull Request. To disable Renovate, simply close this Pull Request unmerged.

Detected Package Files

- `docker-compose.test.yml` (docker-compose)
- `Dockerfile` (dockerfile)
- `.github/workflows/codacy-analysis.yml` (github-actions)
- `.github/workflows/codeql-analysis.yml` (github-actions)
- `.github/workflows/devskim-analysis.yml` (github-actions)
- `.github/workflows/main.yml` (github-actions)
- `.github/workflows/sfssca-analysis.yml` (github-actions)
- `.github/workflows/zap_scan.yml` (github-actions)
- `frontend/src/index.html` (html)
- `frontend/package.json` (npm)
- `package.json` (npm)

Configuration

Renovate has detected a custom config for this PR. Feel free to ask for help if you have any doubts and would like it reviewed.

Important: Now that this branch is edited, Renovate can't rebase it from the base branch any more. If you have changes to the base branch that could impact this onboarding PR, please merge them manually.

Reviewers

No reviews—at least 1 approving review is required.

Still in progress? Convert to draft.

Assignees

No one—assign yourself

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

Notifications Customize

Unsubscribe

You're receiving notifications because you're watching this repository.

0 participants

chore(deps): update dependency diff to v5.1.0 #15779

Merged · 2 hours ago

Conversation 0 · Commits 1 · Checks 0 · Files changed 2

renovate bot commented 2 hours ago · Contributor

MENDRenovate

This PR contains the following updates:

Package	Change	Age	Adoption	Passing	Confidence
diff	5.0.0 -> 5.1.0	2d	33%	102%	high

Release Notes

▸ kpdecker/jsdiff

Configuration

Schedule: At any time (no schedule defined).

Automerge: Enabled.

Rebasing: Whenever PR is behind base branch, or you tick the rebase/retry checkbox.

Ignore: Close this PR and you won't be reminded about this update again.

- [ ] If you want to rebase/retry this PR, click this checkbox.

This PR has been generated by Mend Renovate. View repository job log here.

Open **chore(deps): update dependency semantic-release to v17.3.0** #71

renovate wants to merge 1 commit into `master` from `renovate/semantic-release-…`

Package	Change	Age	Adoption	Passing	Confidence
semantic-release	`17.2.3` -> `17.3.0`	22d	43%	97%	high

Release Notes

▼ semantic-release/semantic-release

`v17.3.0`

Compare Source

Features

- **docs:** note that publish token is required (#1700) (885d87a)

`v17.2.4`

Compare Source

Bug Fixes

- escape uri encoded symbols (#1697) (f8f8fbc)

Application

Snyk

You have already purchased this app on GitHub Marketplace.

Set up a new plan | Edit your plan | Configure access

GitHub has verified that the application meets the requirements for listing.

Categories

Security | Dependency management | Free | GitHub Enterprise

Supported languages

Gradle, Java, Javascript and 4 other languages supported

More: PDM, Python, Ruby, and Scala

Developer

snyk

Verified domain

snyk.io

Developer links

Support
Status
Documentation
Privacy Policy
Terms of Service

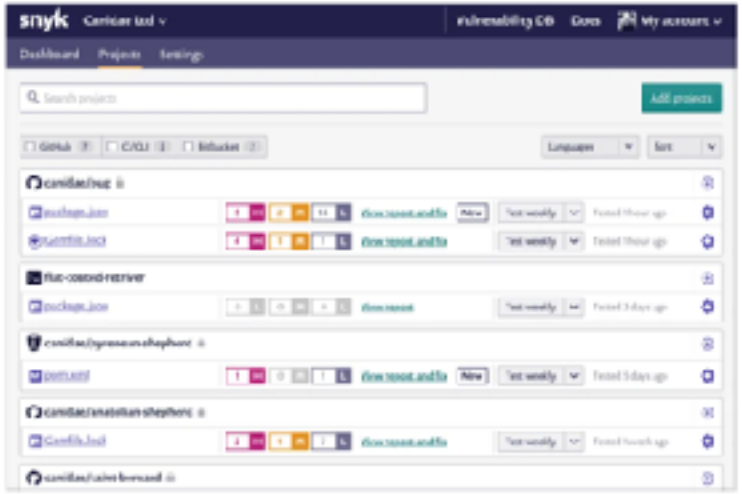
Report abuse

Snyk is on a mission to help developers use open source and stay secure.
Snyk helps find, fix & prevent known vulnerabilities in your Node.js, Java, Ruby, Python and Scala apps. Snyk is free for open source.

Snyk tracks vulnerabilities in over 800,000 open source packages, and helps protect over 25,000 applications.

83% of Snyk users found vulnerabilities in their applications, and new vulnerabilities are disclosed regularly, putting your application at risk.

Read more...



Find: Quickly scan all your repos and get a high level overview of the amount of known vulnerabilities

Pricing and setup

Free $0

For individuals and small organisations to stay secure.

Snyk

Free

For individuals and small organisations to stay secure.

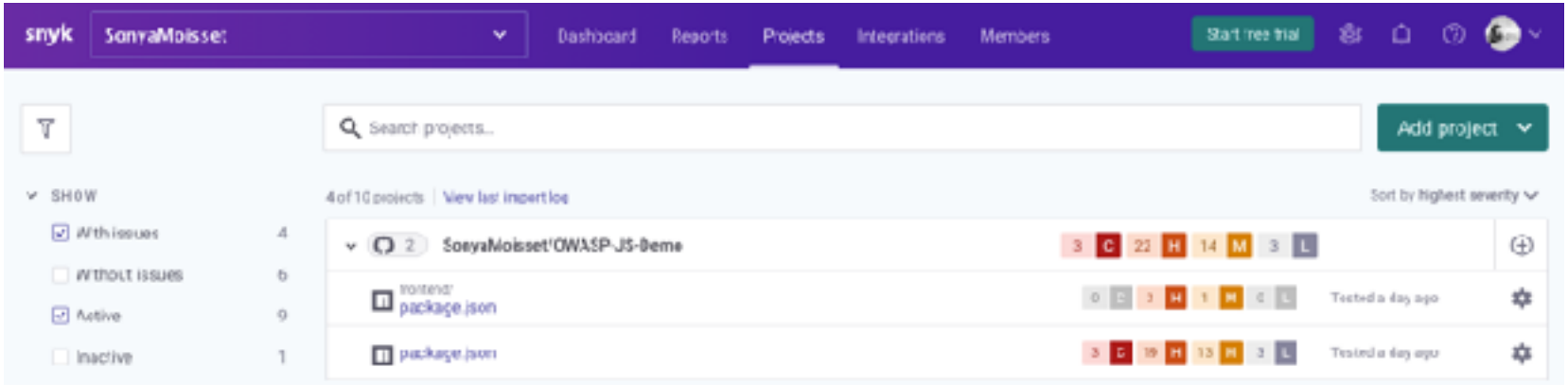
- ✓ Unlimited tests on open-source projects, 200 tests/month on private projects
- ✓ Single click remediation
- ✓ CI/CD pipeline integration
- ✓ Continuous monitoring

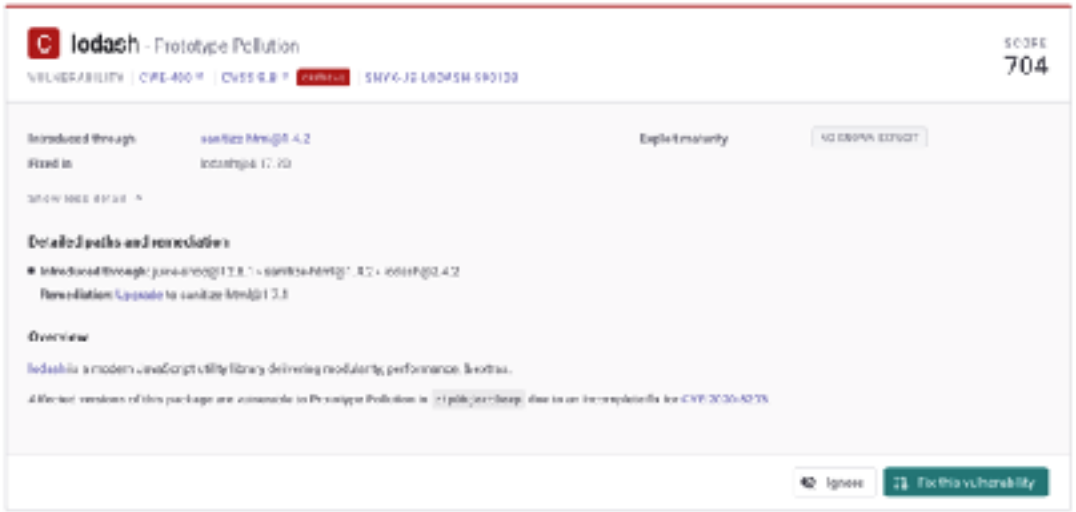
Account: iDevOI

Install it for free

Next: Confirm your installation location.

Snyk is provided by a third-party and is governed by separate terms of service, privacy policy, and support contact.


snyk
SonyaMoisset
Dashboard
Reports
Projects
Integrations
Members
Start free trial
Search projects...
Add project
SHOW
With issues 4
Without issues 6
Active 9
Inactive 1
4 of 10 projects
View last import log
Sort by highest severity
SonyaMoisset'OWASP-JS-Demo
3 C 22 H 14 M 3 L
frontend/
package.json
Tested a day ago
package.json


lodash - Prototype Pollution
SCORE
704
Introduced through
Fixed in
Exploit maturity
Detailed paths and remediation
Overview
Ignore
Fix this vulnerability

[Snyk] Security upgrade sanitize-html from 1.4.2 to 2.0.0 #7

Open snyk-bot wants to merge 1 commit into `main` from `snyk-fix-a2dfa597370c8e5eb2e4a7556bc9b110`

Conversation 0 Commits 1 Checks 9 Files changed 1

snyk-bot commented 3 minutes ago First-time contributor

Snyk has created this PR to fix one or more vulnerable packages in the `npm` dependencies of this project.

merge advice Review recommended

Changes included in this PR

- Changes to the following files to upgrade the vulnerable dependencies to a fixed version:
  - package.json

Vulnerabilities that will be fixed

With an upgrade:

Severity	Priority Score (*)	Issue	Breaking Change	Exploit Maturity
C	704/1000 Why? Has a fix available, CVSS 9.8	Prototype Pollution SNYK-JS-LODASH-590103	No	No Known Exploit
C	684/1000 Why? Has a fix available, CVSS 9.4	Arbitrary Code Execution SNYK-JS-SANITIZEHTML-585892	Yes	No Known Exploit

(*) Note that the real score may have changed since the PR was raised.

Check the changes in this PR to ensure they won't cause issues with your project.

GitHub security alert digest

SonyaMoisset's repository security updates from the week of **Sep 7 - Sep 14**

SonyaMoisset's personal acccunt

SonyaMoisset / CWASP-J8-Demo

Known security vulnerabilities detected

Dependency	vendor	upgrade to
jsonwebtoken	< 8.2.2	=> 8.2.2

Defined in
package.json

Vulnerabilities
CVE-2018-8231 Critical severity

Dependency	vendor	upgrade to
serialize-javascript	>= 2.1.1, < 2.1.2	>= 2.1.2

Defined in
package.json

Vulnerabilities
CVE-2019-16769 Moderate severity
CVE-2019-16768 Moderate severity
CVE-2020-7660 Moderate severity
CVE-2020-7660 Moderate severity

Dependency	vendor	upgrade to
express-jwt	>= 5.3.0, < 6.0.0	>= 6.0.0

Defined in
package.json

Vulnerabilities
CVE-2020-15084 High severity

Dependency	vendor
mongodb	>= 3.0.0, < 3.1.13

Defined in
package.json

Vulnerabilities

Review all vulnerable dependencies

New issues and remediations

Hello SonyaMoisset,
We found new vulnerabilities that affect 2 projects in the [redacted] organization

[redacted]

[redacted] package.json — view all project issues

H Prototype Pollution
Vulnerability in object-path: 2.11.4. No remediation available yet.

This issue can only be fixed manually or ignored

[redacted] — view all project issues

H Prototype Pollution
Vulnerability in object-path: 2.11.4. No remediation available yet.

This issue can be fixed via the CLI

Stay secure!
The Snyk team


Secret Sprawl

| Git Guardian

Secret Sprawl is the unwanted distribution of secrets like API Keys and credentials through multiple systems

Keep secrets out of your source code

SCAN YOUR SOURCE CODE TO DETECT API KEYS, PASSWORDS, CERTIFICATES, ENCRYPTION KEYS AND OTHER SENSITIVE DATA IN REAL-TIME

Start for free Book a demo

Application

GitGuardian

You have already purchased this app on GitHub Marketplace.

Set up a new plan | Edit your plan ▾ | Configure access

GitHub has verified that the publisher controls the domain and meets other requirements.

Categories

Security | Monitoring | Free

Developer

GitGuardian

Verified domains

gitguardian.com
www.gitguardian.com

Developer links

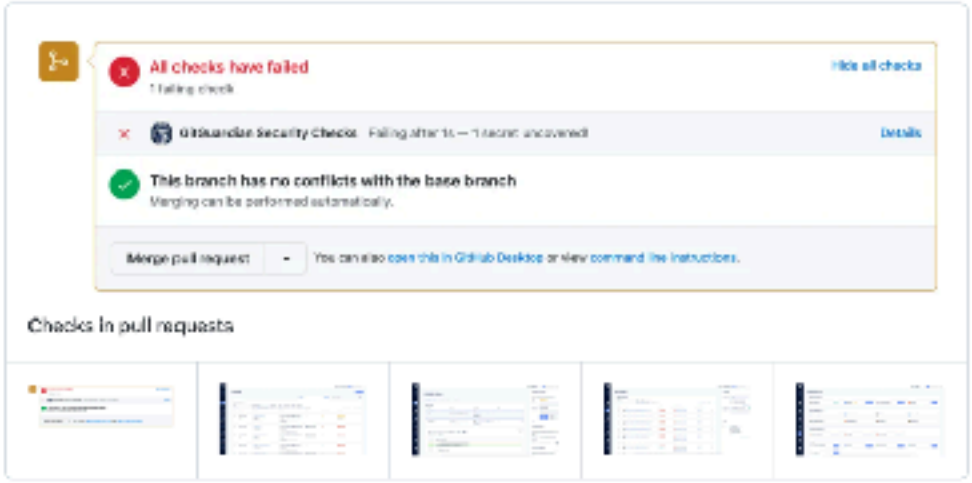
Support
Status
Documentation
Privacy Policy
Terms of Service

Report abuse

What is GitGuardian ?

GitGuardian is the ultimate security layer for developers.
We detect hard-coded secrets in commits and repositories, and help you with prevention and remediation.

Read more...

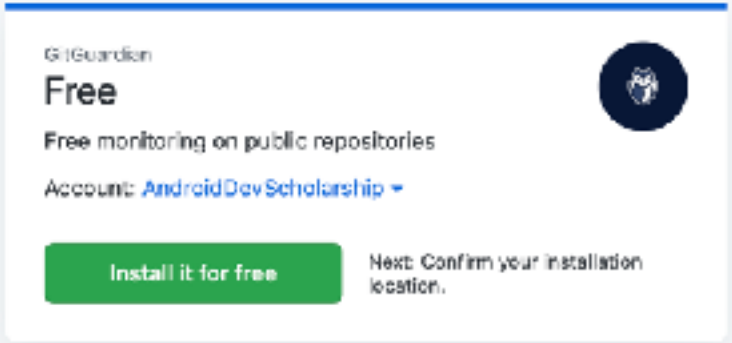


Checks in pull requests

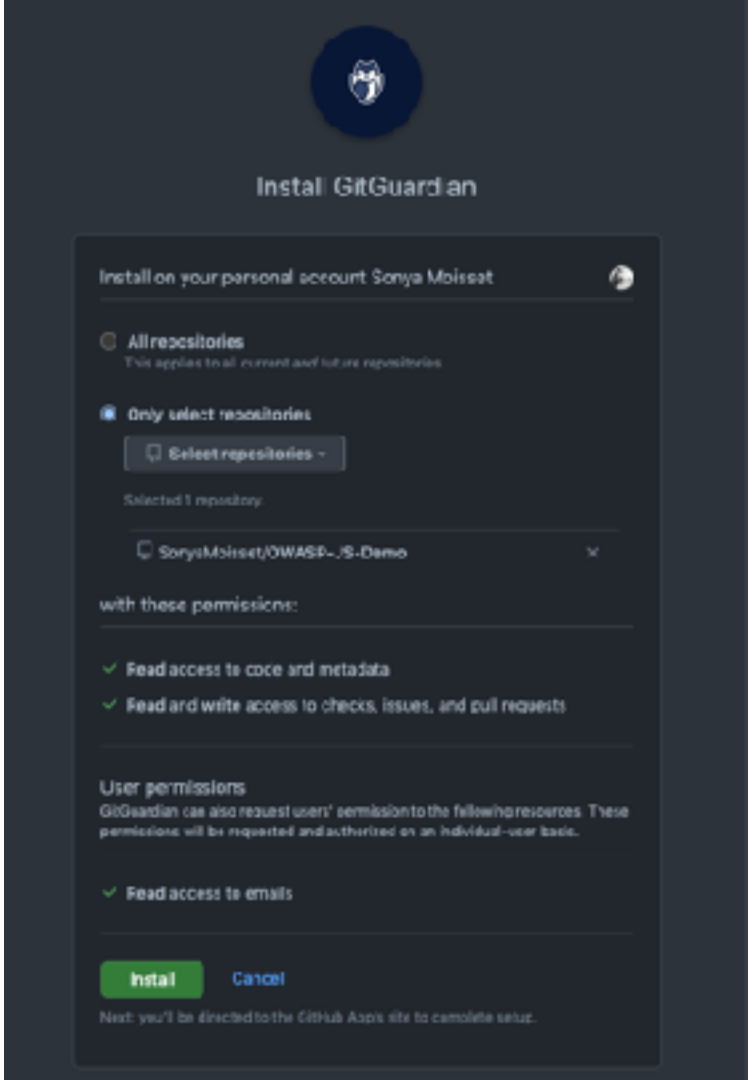
Pricing and setup

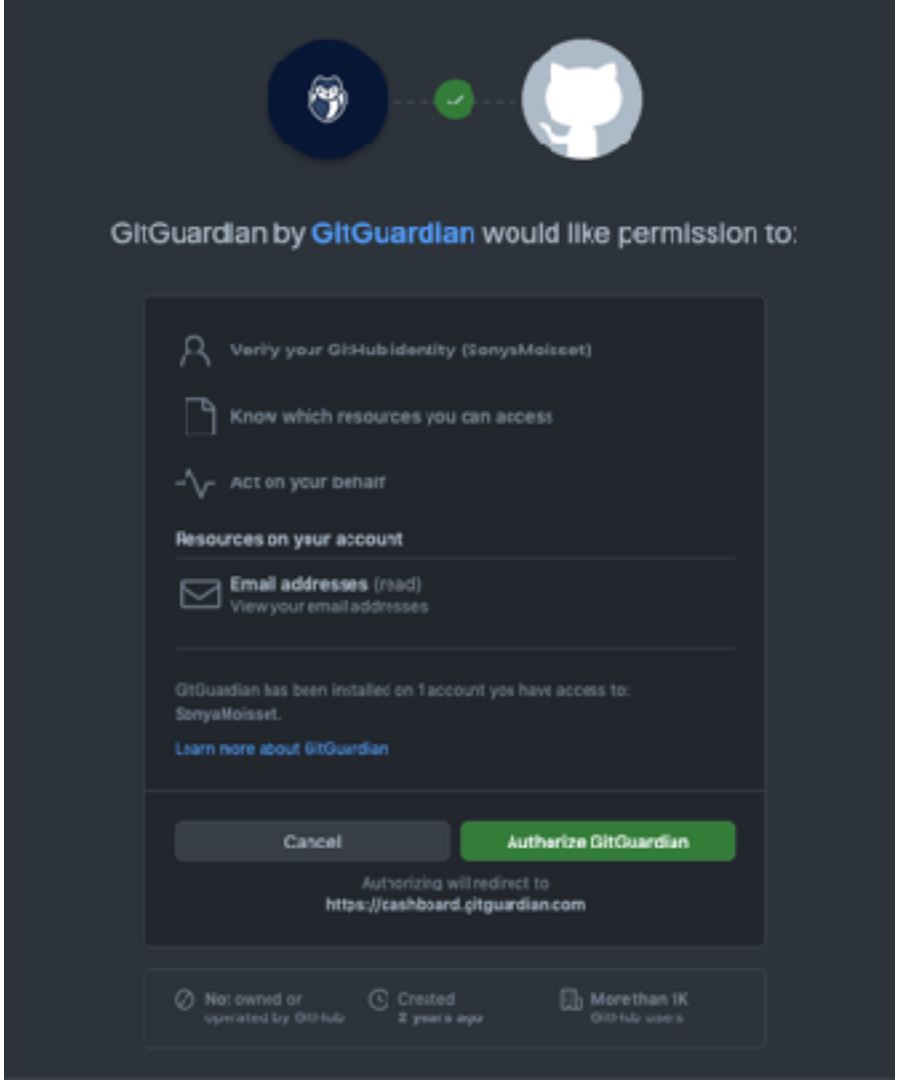
Free $0

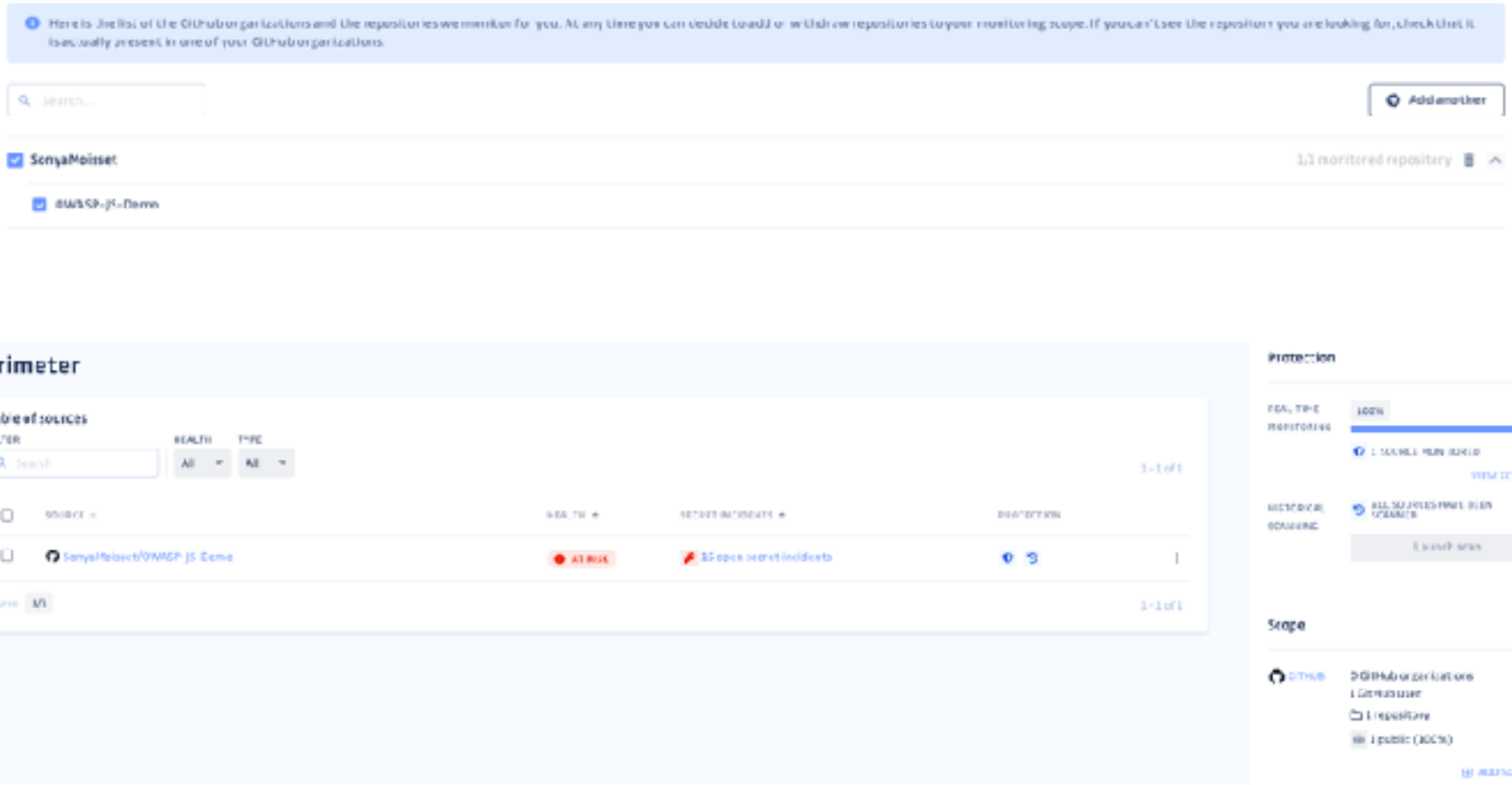
Free monitoring on public repositories



GitGuardian is provided by a third-party and is governed by separate terms of service, privacy policy, and support documentation.


Install GitGuardian
Install on your personal account Sonya Moisset
All repositories
This applies to all current and future repositories
Only select repositories
Select repositories
Selected 1 repository.
SonyaMoisset/OWASP-...S-Demo
with these permissions:
Read access to code and metadata
Read and write access to checks, issues, and pull requests
User permissions
GitGuardian can also request users' permission to the following resources. These permissions will be requested and authorized on an individual-user basis.
Read access to emails
Install
Cancel
Next: you'll be directed to the GitHub Apps site to complete setup.


GitGuardian by GitGuardian would like permission to:
Verify your GitHub identity (SonyaMoisset)
Know which resources you can access
Act on your behalf
Resources on your account
Email addresses (read)
View your email addresses
GitGuardian has been installed on 1 account you have access to:
SonyaMoisset.
Learn more about GitGuardian
Cancel
Authorize GitGuardian
Authorizing will redirect to
https://cashboard.gitguardian.com
Not owned or
operated by GitHub
Created
2 years ago
More than 1K
GitHub users


Here is the list of the GitHub organizations and the repositories we monitor for you. At any time you can double-load or unload new repositories to your monitoring scope. If you can't see the repository you are looking for, check that it is actually present in one of your GitHub organizations.
Search...
Add another
SonyaMoisset
1/1 monitored repository
OWASP-JS-Demo
Perimeter
Table of sources
FILTER
Search
HEALTH
All
TYPE
All
1 - 1 of 1
SOURCE
HEALTH
SECRET INCIDENTS
PROTECTION
SonyaMoisset/OWASP JS Demo
AT RISK
35 open secret incidents
Source 1/1
1 - 1 of 1
Protection
REAL-TIME MONITORING
100%
VIEW SETTINGS
HISTORICAL SCANNING
Launch scan
Scope
GITHUB
3 GitHub organizations
1 Contributor
1 repository
1 public (100%)

SECRET INCIDENTS > #3476676

Bearer Token

OCCURRENCES 3 FEEDBACK 0 TIMELINE

Occurrences

DATE	WHO	WHERE	PRESENCE	TAGS
March 17th, 2020 12:57	Bjoern Kimminich	Bkimminich/OWASP-JS-Demo client?? test/server/verifySpec.js		From historical scan Exposed publicly Test file
March 17th, 2020 12:57	Bjoern Kimminich	Bkimminich/OWASP-JS-Demo client?? test/server/verifySpec.js		From historical scan Exposed publicly Test file
February 20th, 2020 18:14	Scar26	Bkimminich/OWASP-JS-Demo [redacted] test/server/verifySpec.js		From historical scan Exposed publicly Test file

1 - 3 of 3


bkimminich/juice-shop
cfcd208
test/server/verifySpec.js
BEARER TOKEN
apikey
283 284
- it('"jwtForgedChallenge" is solved when forged token HMAC-signed with public RSA-key has email rsa_lord@juice-sh.op in the payload', () => {
- /*
- Header: { "alg": "HS256", "typ": "JWT" }
- Payload: { "data": { "email": "rsa_lord@juice-sh.op" }, "iat": 1508639612, "exp": 9999999999 }
- */
- this.req.headers = { authorization: 'Bearer eyJ0eXA10iJKV1QiLCJhbGci0iJIUzI1NiJ9.eyJkYXRhIjp7InNtYWlsIjoicmhhX2xvcmRAanVpY2Utc2hvcC5vcCJ9LCJpYXQiOjE1MDg2Mzk2MTIsImV4cCI6OTk5OTk5OTk5OX0.
+ if (!utils.disableOnWindowsHve()) {
+ it('"jwtForgedChallenge" is solved when forged token HMAC-signed with public RSA-key has email rsa_lord@juice-sh.op in the payload', () => {
+ /*
+ Header: { "alg": "HS256", "typ": "JWT" }
+ Payload: { "data": { "email": "rsa_lord@juice-sh.op" }, "iat": 1508639612, "exp": 9999999999 }
+ */
+ this.req.headers = { authorization: 'Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJkYXRhIjp7InNtYWlsIjoicnNhX2xvcmRAanVpY2Utc2hvcC5vcCJ9LCJpYXQiOjE1MDg2Mzk2MTIsImV4cCI6OTk5OTk5OTk5OX0.
290 292
- verify.jwtChallenges()(this.req, this.res, this.next)
+ verify.jwtChallenges()(this.req, this.res, this.next)
292 294
- expect(challenges.jwtForgedChallenge.solved).to.equal(true)
- })

Integrations

VCS integrations

- GitHub — INSTALLED
- Bitbucket — Install
- GitHub Enterprise — Install
- GitLab — Install

CI/CD integrations

- Azure pipelines
- Bitbucket pipelines
- CircleCI
- Drone CI
- GitHub actions
- GitLab pipelines
- Jenkins CI
- Travis CI

Git hooks integrations

- pre-commit — DOCUMENTATION
- pre-push — DOCUMENTATION
- pre-receive — DOCUMENTATION

Docker integrations

- Docker images — DOCUMENTATION

Alerting

- Custom Webhook — Install
- Discord — Install
- PagerDuty — Install
- Slack — Install
- Splunk — Install

Static Code Analysis

| Perforce

Static Code Analysis is a method of debugging by examining source code before a program is run. It’s done by analysing a set of code against a set of coding rules

sonarcloud

Features What we do What's new Pricing Explore Log in

Clean Code
Rockstar Status

Eliminate bugs and vulnerabilities.
Champion quality code in your projects.

Go ahead! Analyze your repo:

GitHub Bitbucket

Azure DevOps GitLab

Free for Open-Source Projects

GitHub Action

SonarCloud Scan

v1.0 Latest version

Use latest version

Scan your code with SonarCloud

Using this GitHub Action, scan your code with SonarCloud to detects bugs, vulnerabilities and code smells in more than 20 programming languages!

SonarCloud is the leading product for Continuous Code Quality & Code Security online, totally free for open-source projects. It supports all major programming languages, including Java, JavaScript, TypeScript, C#, C/C++ and many more. If your code is closed source, SonarCloud also offers a paid plan to run private analyses.

Requirements

- Have an account on SonarCloud. Sign up for free now if it's not already the case!
- The repository to analyze is set up on SonarCloud. Set it up in just one click.

Usage

Project metadata, including the location to the sources to be analyzed, must be declared in the file `sonar-project.properties` in the base directory:

```
sonar.organization=<replace with your sonarcloud organization key>
sonar.projectKey=<replace with the key generated when setting up the project on Son

# relative paths to source directories. More details and properties are described
# in https://sonarcloud.io/documentation/project-administration/narrowing-the-focus
sonar.sources=.
```

The workflow, usually declared in `.github/workflows/build.yml`, looks like

Verified creator

GitHub has verified that this action was created by **sonarsource**.

Learn more about verified Actions.

Stars

Star 205

Contributors

Categories

Code quality Security

Links

SonarSource/sonarcloud-github-action

Pull requests 9

Report abuse

SonarCloud Scan is not certified by GitHub. It is provided by a third-party and is governed by separate terms of service, privacy policy, and support documentation.

sonarcloud My Projects My Issues NEW WordPress plugins development... Explore Search for projects and files...

Sonya Moisset / OWASP-JS-Demo main

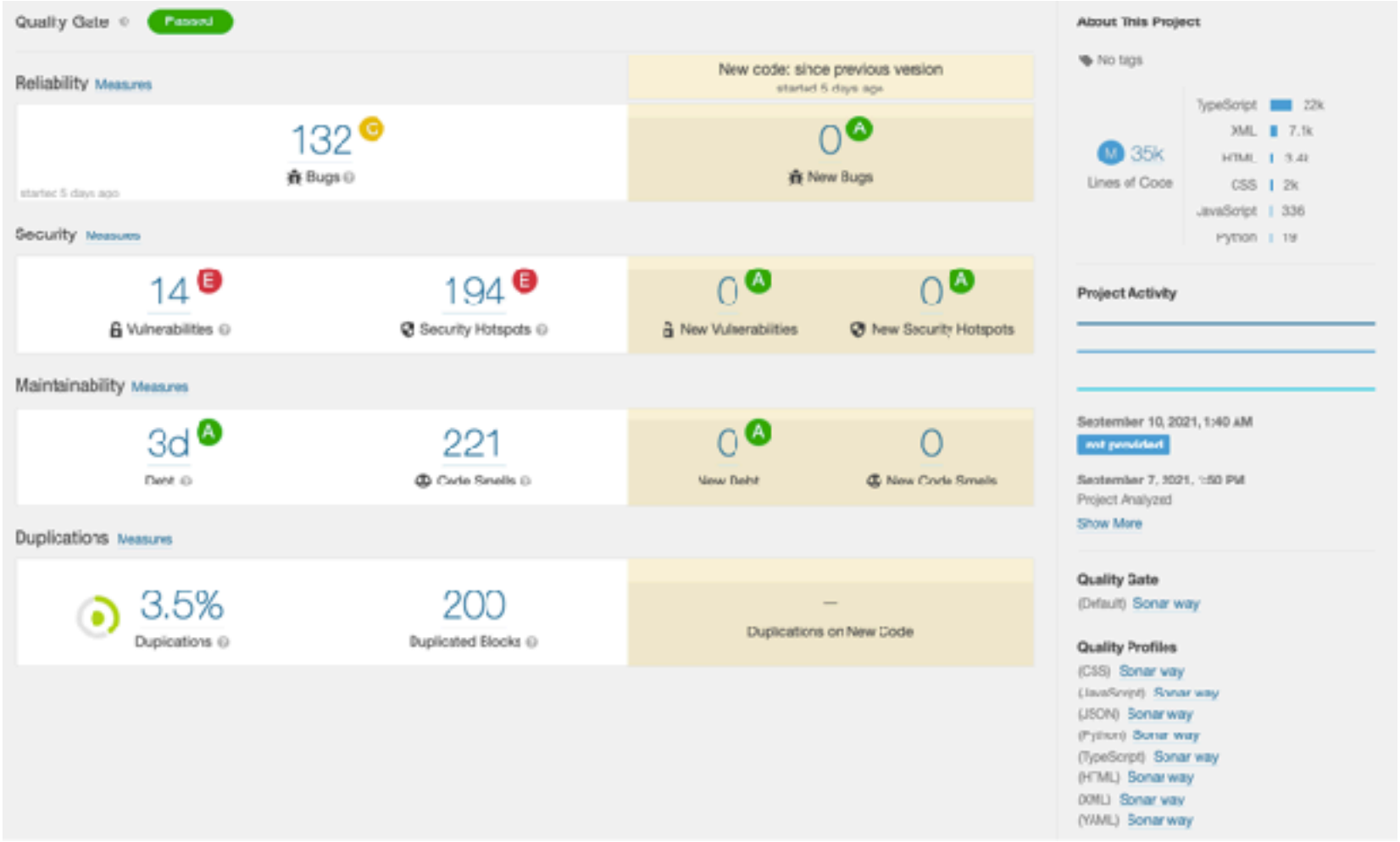
Configure Issues Security Hotspots Measures Code Activity Administration

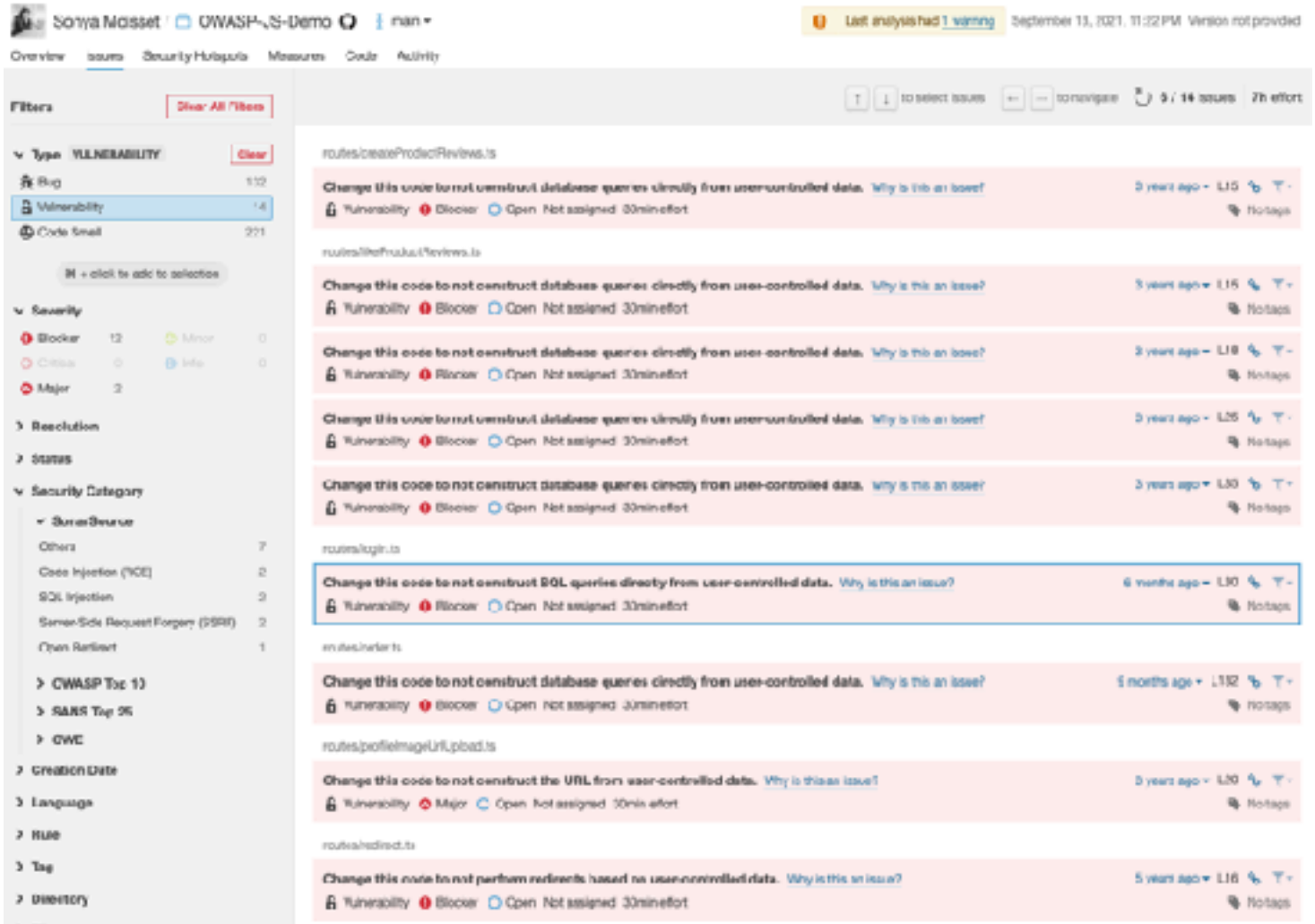
PUBLIC

We are analyzing your project.

You should see this page refresh in a few moments with your analysis results.

- You will get a first analysis of your default branch and the 5 most recently active Pull Requests.
- Each new push on your default branch will trigger a new analysis automatically.
- Each new push to a Pull Request will also trigger an analysis.


Quality Gate
Passed
Reliability Measures
New code: since previous version
started 5 days ago
132
C
Bugs
started 5 days ago
0
A
New Bugs
Security Measures
14
E
Vulnerabilities
194
E
Security Hotspots
0
A
New Vulnerabilities
0
A
New Security Hotspots
Maintainability Measures
3d
A
Debt
221
Code Smells
0
A
New Debt
0
New Code Smells
Duplications Measures
3.5%
Duplications
200
Duplicated Blocks
—
Duplications on New Code
About This Project
No tags
35k
Lines of Code
TypeScript 22k
XML 7.1k
HTML 3.4k
CSS 2k
JavaScript 336
Python 19
Project Activity
September 10, 2021, 1:40 AM
Project Analyzed
Show More
Quality Gate
(Default) Sonar way
Quality Profiles
(CSS) Sonar way
(JavaScript) Sonar way
(JSON) Sonar way
(Python) Sonar way
(TypeScript) Sonar way
(HTML) Sonar way
(XML) Sonar way
(YAML) Sonar way


Sonya Massat
main
Last analysis had 1 warning
September 13, 2021, 11:22 PM Version not provided
Overview
Issues
Security Hotspots
Measures
Code
Activity
Filters
Clear All Filters
Type VULNERABILITY
Clear
Bug 132
Vulnerability 14
Code Smell 221
⌘ + click to add to selection
Severity
Blocker 12
Minor 0
Critical 0
Info 0
Major 2
Resolution
Status
Security Category
SonarSource
Others 7
Code Injection (TCE) 2
SQL Injection 3
Server-Side Request Forgery (SSRF) 2
Cross-Site Request Forgery (CSRF) 1
OWASP Top 10
SANS Top 25
CWE
Creation Date
Language
Rule
Tag
Directory
to select issues
to navigate
3 / 14 issues
7h effort
routes/createProductReviews.ts
Change this code to not construct database queries directly from user-controlled data. Why is this an issue?
3 years ago L15
Vulnerability Blocker Open Not assigned 30min effort
No tags
routes/likeProductReviews.ts
Change this code to not construct database queries directly from user-controlled data. Why is this an issue?
3 years ago L16
Vulnerability Blocker Open Not assigned 30min effort
No tags
Change this code to not construct database queries directly from user-controlled data. Why is this an issue?
3 years ago L18
Vulnerability Blocker Open Not assigned 30min effort
No tags
Change this code to not construct database queries directly from user-controlled data. Why is this an issue?
3 years ago L26
Vulnerability Blocker Open Not assigned 30min effort
No tags
Change this code to not construct database queries directly from user-controlled data. Why is this an issue?
3 years ago L30
Vulnerability Blocker Open Not assigned 30min effort
No tags
routes/login.ts
Change this code to not construct SQL queries directly from user-controlled data. Why is this an issue?
6 months ago L30
Vulnerability Blocker Open Not assigned 30min effort
No tags
routes/order.ts
Change this code to not construct database queries directly from user-controlled data. Why is this an issue?
5 months ago L132
Vulnerability Blocker Open Not assigned 2min effort
No tags
routes/profileImageUrlUpload.ts
Change this code to not construct the URL from user-controlled data. Why is this an issue?
3 years ago L20
Vulnerability Major Open Not assigned 10min effort
No tags
routes/redirect.ts
Change this code to not perform redirects based on user-controlled data. Why is this an issue?
5 years ago L16
Vulnerability Blocker Open Not assigned 30min effort
No tags

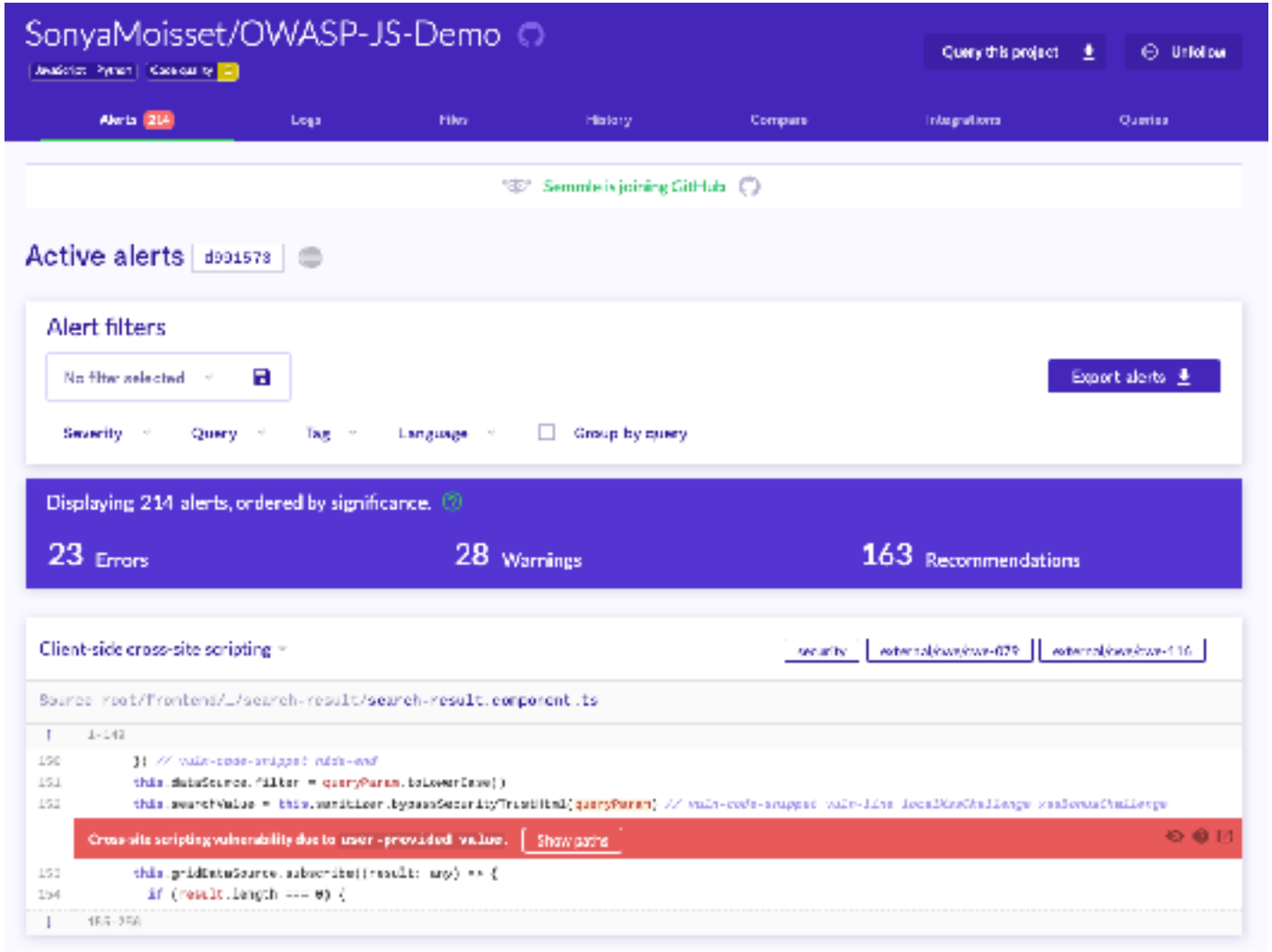
Sonya Moisset / OWASP-JS-Demo main

Last analysis had 1 warning September 10, 2021 11:22 PM Version not provided

Overview Issues Security Hotspots Measures Code Activity

	Lines of Code	Bugs	Vulnerabilities	Code Smells	Security Hotspots	Coverage	Duplications
config	–	0	0	0	0	–	0.0%
data	634	0	0	16	4	–	0.0%
frontend	3,239	132	0	14	15	–	0.8%
lib	–	0	0	0	0	–	0.0%
lib	1,046	0	0	17	6	–	0.0%
models	405	0	0	5	0	–	0.0%
monitoring	–	0	0	0	0	–	0.0%
routes	2,721	0	13	69	7	–	0.0%
test	5,848	0	1	90	156	–	14.4%
views/themes	51	0	0	0	0	–	64.2%
app.json	–	0	0	0	0	–	0.0%
app.ts	4	0	0	0	0	–	0.0%
config.schema.yml	–	0	0	0	0	–	0.0%
crowdin.yaml	–	0	0	0	0	–	0.0%
[illegible]	–	0	0	0	0	–	0.0%
Gruntfile.js	75	0	0	0	1	–	0.0%
package.json	–	0	0	0	0	–	0.0%
protractor.conf.js	54	0	0	0	0	–	0.0%
protractor.subproblem.conf.js	3	0	0	0	0	–	0.0%
server.ts	527	0	0	10	6	–	0.0%
swagger.yml	–	0	0	0	0	–	0.0%
threat-model.json	–	0	0	0	0	–	0.0%
tsconfig.json	–	0	0	0	0	–	0.0%


lgtm
Search LGTM
Help
Query console
Project lists
My alerts
Sonya Moisset
Semmle is joining GitHub
Continuous security analysis
A code analysis platform for finding zero-days and preventing critical vulnerabilities
Unparalleled security analysis
LGTM's security analysis is powered by findings from our dedicated team of security researchers, and by contributions from security teams at a number of top tech companies.
110+ CVEs disclosed by our security researchers
Automated code review
Prevent bugs from ever appearing in your project by automatically catching them in the review process before they get merged.
107,261 pull request analyses run
Free for open source
LGTM is completely free for open source projects. We integrate with GitHub and Bitbucket, and can analyze projects written in Java, Python, JavaScript, TypeScript, C#, Go, C and C++.
135,821 open source repos on LGTM.com
Deep semantic code search
All of our analyses are open source, and written as queries using CodeQL, our deep semantic code search engine. You can even write your own queries to find and prevent mistakes or issues that matter to you.
Plenty of results ready to explore
With over 39 million commits by more than 700000 developers analyzed for 135,821 open source projects (and counting!), you can dive right in to an wealth of results. Start exploring...
Start exploring...
by Semmle


SonyaMoisset/OWASP-JS-Demo
Query this project
Unfollow
Alerts 214
Logs
Files
History
Compare
Integrations
Queries
Semmle is joining GitHub
Active alerts
d931578
Alert filters
No filter selected
Export alerts
Severity
Query
Tag
Language
Group by query
Displaying 214 alerts, ordered by significance.
23 Errors
28 Warnings
163 Recommendations
Client-side cross-site scripting
security
external/cwe/cwe-079
external/cwe/cwe-116
Source: root/frontend/_/search-result/search-result.component.ts
1-143
190 }) // vuln-code-snippet vuln-end
191 this.dataSource.filter = queryParam.toLowerCase()
192 this.searchValue = this.sanitizer.bypassSecurityTrustHtml(queryParam) // vuln-code-snippet vuln-line localXssChallenge xssBonusChallenge
Cross-site scripting vulnerability due to user-provided value.
Show steps
1 / 1
193 this.gridDataSource.subscribe((result: any) => {
194 if (result.length === 0) {
195-350

Client-side cross-site scripting

Open in query console

Query help | Alerts

Semmle is joining GitHub

Writing user input directly to the DOM allows for a cross-site scripting vulnerability.

Query pack: com.lgtm/javascript-queries
Query ID: js/xss
Language: JavaScript
Severity: Error
Tags: security, external/cwe/cwe-079, external/owasp/owasp-a3
Displayed by default? Yes. Alerts for this query are visible by default, but can be hidden on a per-project basis. Learn how.

Directly writing user input (for example, a URL query parameter) to a webpage without properly sanitizing the input first, allows for a cross-site scripting vulnerability.

This kind of vulnerability is also called *DOM-based cross-site scripting*, to distinguish it from other types of cross-site scripting.

Recommendation

To guard against cross-site scripting, consider using contextual output encoding/escaping before writing user input to the page, or one of the other solutions that are mentioned in the references.

Example

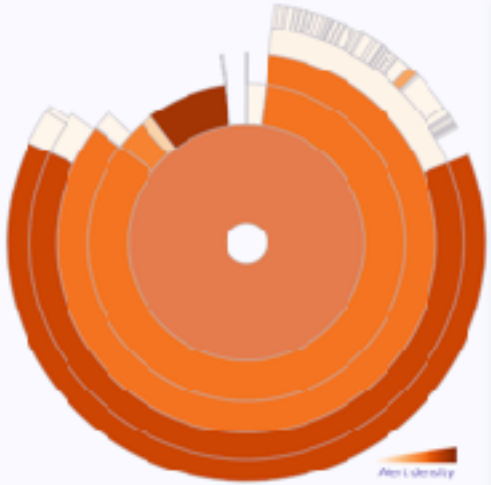
The following example shows part of the page URL being written directly to the document, leaving the website vulnerable to cross-site scripting.

```
function setLanguageOptions() {
    var href = document.location.href,
        deflt = href.substring(href.indexOf("default=")+8);
    document.write("<OPTION value1='+deflt+'>1</OPTION>");
    document.write("<OPTION value2=>English</OPTION>");
}
```

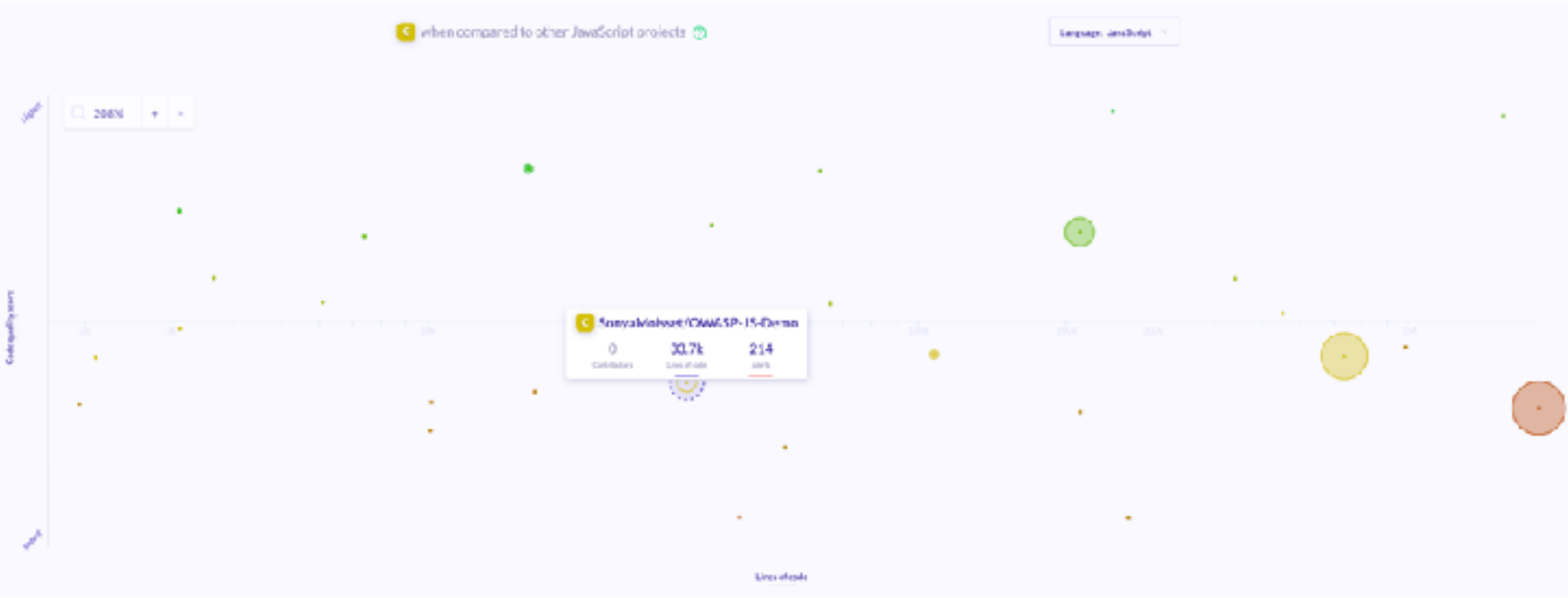
References

- OWASP: DOM based XSS Prevention Cheat Sheet.
- OWASP: XSS (Cross Site Scripting) Prevention Cheat Sheet.
- OWASP DOM Based XSS.
- OWASP Types of Cross-Site Scripting.
- Wikipedia: Cross-site scripting.
- Common Weakness Enumeration: CWE-79.
- Common Weakness Enumeration: CWE-116.

Source root/



Name	Alerts	Lines of code
.github	0	0
config	0	0
data	0	624
frontend	178	28.2k
ftp	0	0
lib	6	1k
models	1	405
routes	26	2.7k
test	0	0
views	0	55
.codeclimate.yml	0	0
.eslintrc.js	0	39
.gitlab-ci.yml	0	0
app.ts	0	4
config.schema.yml	0	0


when compared to other JavaScript projects
Language: JavaScript
200%
0
30.7k
214

CodeQL for research

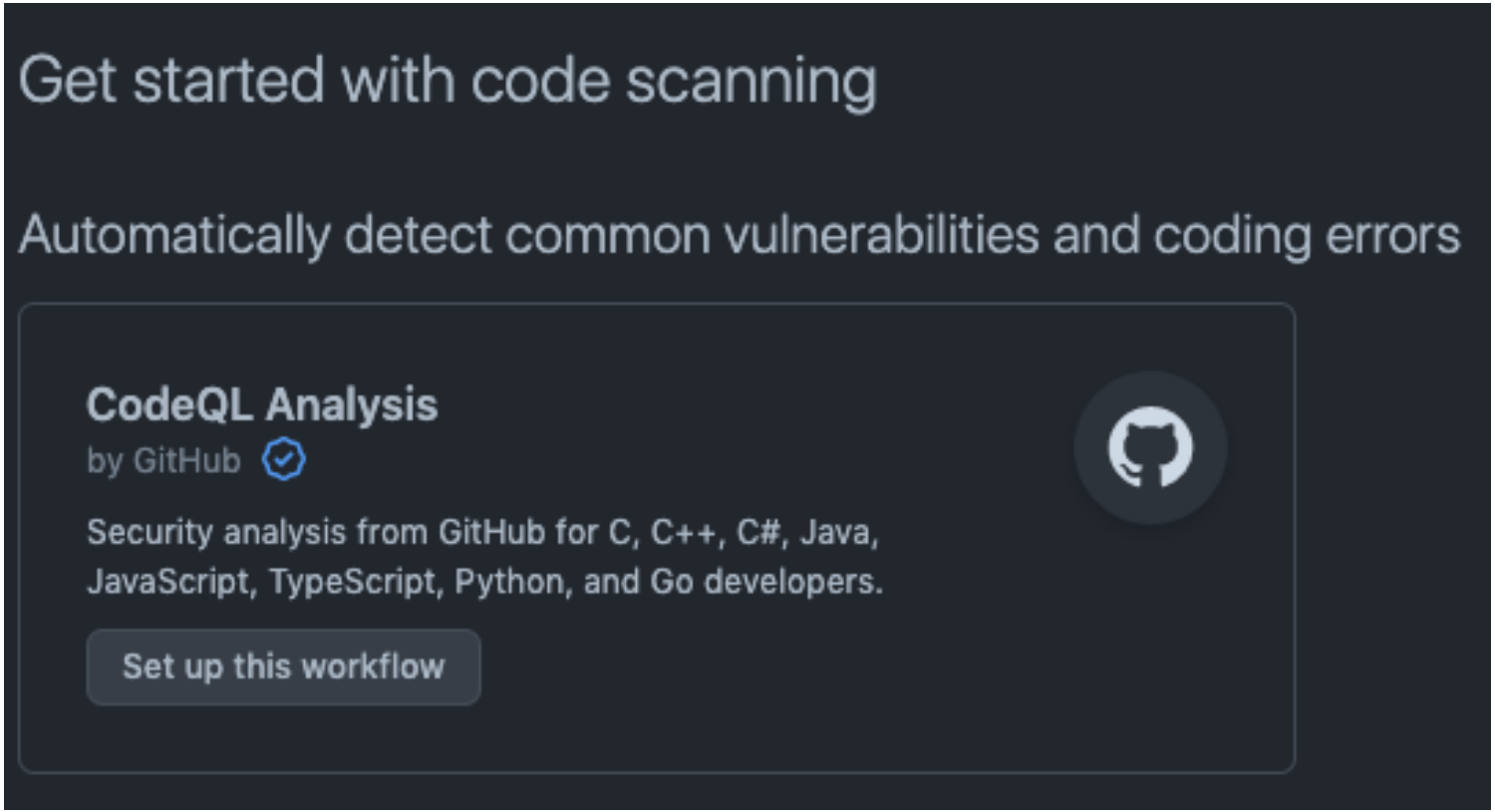
Discover vulnerabilities across a codebase with CodeQL, our industry-leading semantic code analysis engine. CodeQL lets you query code as though it were data. Write a query to find all variants of a vulnerability, eradicating it forever. Then share your query to help others do the same.

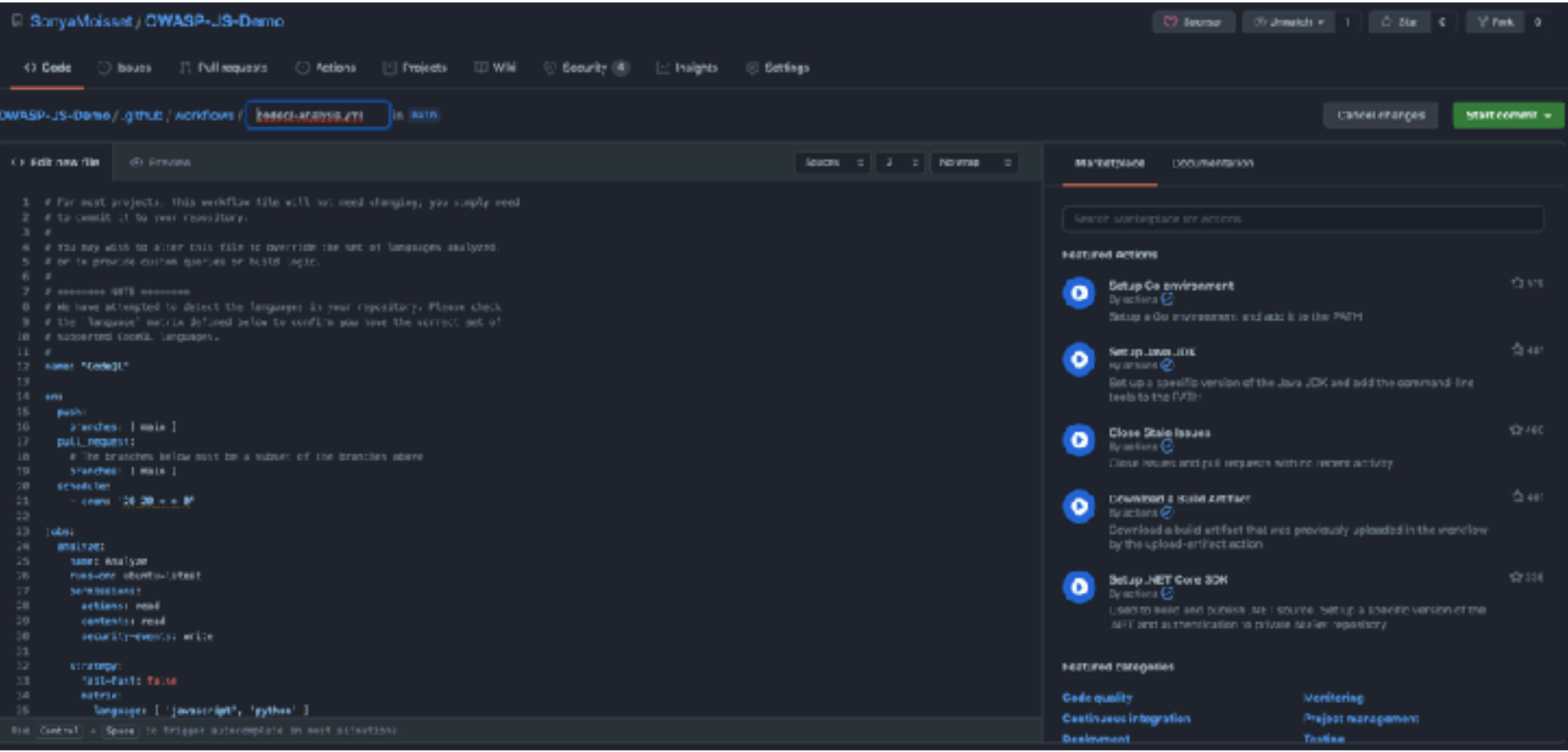
CodeQL is free for research and open source.

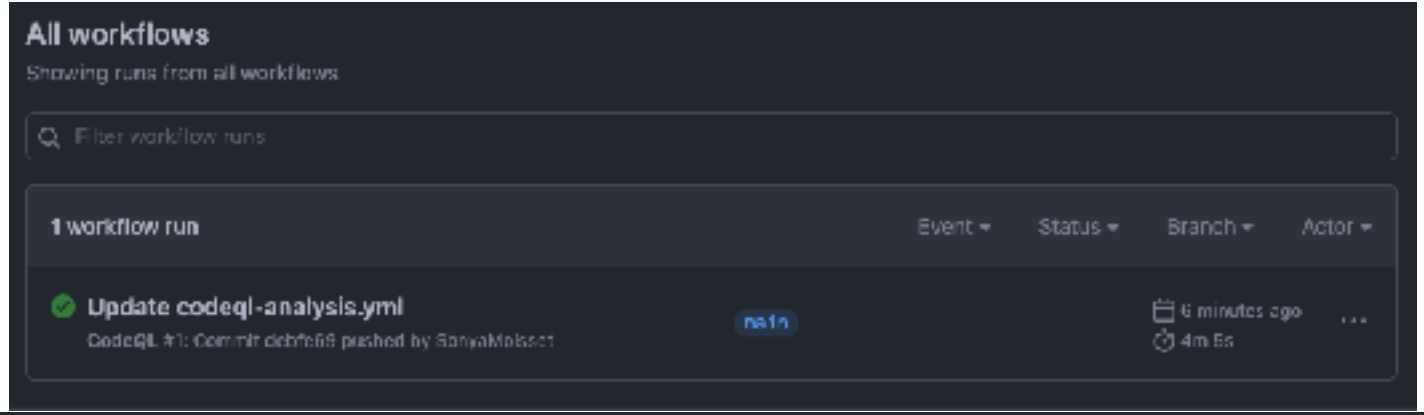
Try CodeQL on LGTM.com

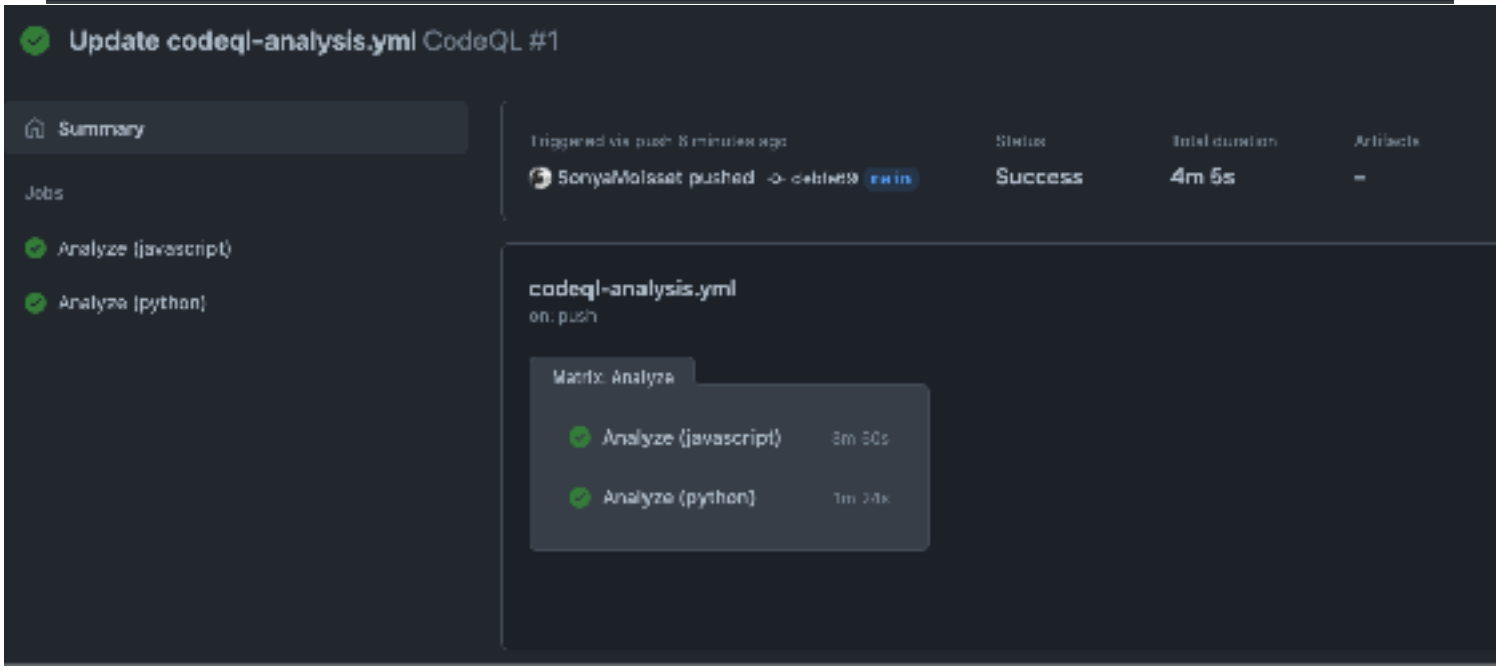
UnsafeDeserialization.ql

```
from DataFlow::PathNode source, DataFlow::PathNode sink, UnsafeDeserializationConfig conf

        where conf.hasFlowPath(source, sink)

        select sink.getNode().(UnsafeDeserializationSink).getMethodAccess(), source, sink,
    "Unsafe deserialization of $@.", source.getNode(), "user input"
```


Get started with code scanning
Automatically detect common vulnerabilities and coding errors
CodeQL Analysis
by GitHub
Security analysis from GitHub for C, C++, C#, Java, JavaScript, TypeScript, Python, and Go developers.
Set up this workflow


SanyaMoisset / OWASP-JS-Demo
Code
Issues
Pull requests
Actions
Projects
Wiki
Security
Insights
Settings
OWASP-JS-Demo / .github / workflows / codeql-analysis.yml in main
Cancel changes
Start commit
Edit new file
Preview
Spaces
2
No wrap
For most projects, this workflow file will not need changing; you simply need
to commit it to your repository.
#
You may wish to alter this file to override the set of languages analyzed,
or to provide custom queries or build logic.
#
******** NOTE ********
We have attempted to detect the languages in your repository. Please check
the `language` matrix defined below to confirm you have the correct set of
supported CodeQL languages.
#
name: "CodeQL"
on
push:
branches: [main]
pull_request:
The branches below must be a subset of the branches above
branches: [main]
schedule:
- cron: '24 20 * * 0'
jobs:
analyze:
name: Analyze
runs-on: ubuntu-latest
permissions:
actions: read
contents: read
security-events: write
strategy:
fail-fast: false
matrix:
language: ['javascript', 'python']
Use Control + Space to trigger autocomplete in most situations.
Marketplace
Documentation
Search Marketplace for Actions
Featured actions
Setup Go environment
By actions
Setup a Go environment, and add it to the PATH
Set up a specific version of the Java JDK and add the command-line tools to the PATH
Close Stale Issues
By actions
Close issues and pull requests with no recent activity
Download a build artifact
By actions
Download a build artifact that was previously uploaded in the workflow by the upload-artifact action
Setup .NET Core SDK
By actions
Featured categories
Code quality
Continuous integration
Deployment
Monitoring
Project management
Testing


All workflows
Showing runs from all workflows
Filter workflow runs
1 workflow run
Event
Status
Branch
Actor
Update codeql-analysis.yml
main
6 minutes ago
4m 6s


Update codeql-analysis.yml CodeQL #1
Summary
Jobs
Analyze (javascript)
Analyze (python)
Status
Success
Total duration
4m 5s
Artifacts
codeql-analysis.yml
on: push
Matrix: Analyze
Analyze (javascript)
Analyze (python)

Code scanning

Give feedback | Add more scanning tools

Latest scan	Pull request	Workflow	Lines scanned	Duration	Result
14 minutes ago	#6	CodeQL	50.6k / 49.7k	3m 55s	49 alerts

Filters | is:open branch:main

49 Open | 0 Closed | Tool | Rule | Branch | Severity | Sort

- Type confusion through parameter tampering — Critical
  routes/search.ts#L14 • Detected 6 days ago by CodeQL
- Type confusion through parameter tampering — Critical
  lib/insecurity.ts#L117 • Detected 6 days ago by CodeQL
- Hard-coded credentials — Critical
  (Test) test/server/verifySpec.ts#L303 • Detected 6 days ago by CodeQL
- Hard-coded credentials — Critical
  (Test) test/server/verifySpec.ts#L291 • Detected 6 days ago by CodeQL
- Hard-coded credentials — Critical
  (Test) test/server/verifySpec.ts#L260 • Detected 6 days ago by CodeQL
- Hard-coded credentials — Critical
  (Test) test/server/verifySpec.ts#L197 • Detected 6 days ago by CodeQL
- Hard-coded credentials — Critical
  (Test) test/server/verifySpec.ts#L60 • Detected 6 days ago by CodeQL
- Hard-coded credentials — Critical
  (Test) test/server/verifySpec.ts#L51 • Detected 6 days ago by CodeQL
- Hard-coded credentials — Critical
  (Test) test/server/verifySpec.ts#L42 • Detected 6 days ago by CodeQL
- Hard-coded credentials — Critical
  (Test) test/api/userApiSpec.ts#L262 • Detected 6 days ago by CodeQL
- Hard-coded credentials — Critical
  (Test) test/api/userApiSpec.ts#L253 • Detected 6 days ago by CodeQL
- Hard-coded credentials — Critical
  (Test) test/api/passwordApiSpec.ts#L81 • Detected 6 days ago by CodeQL

Hard-coded credentials

Hard-coding credentials in source code may enable an attacker to gain unauthorized access.

Open | Critical | CWE-259 | CWE-321 | CWE-798 | security

Branch: main | Dismiss

lib/insecurity.js

```
16
17  const publicKey = fs.readFileSync('encryptionkeys/jwt.pub', 'utf8')
18  module.exports.publicKey = publicKey
19  const privateKey = '-----BEGIN RSA PRIVATE KEY-----\r\nMIICXAIBAAKBgQDNwqLEe9wgTXCbC7+RPdDbBeqjdbs4kOPOIGzqLpXvJXlxxW8iMz
```

The hard-coded value "-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQDNwqLEe9wgTXCbC7+RPdDbBeqjdbs4kOPOIGzqLpXvJXlxxW8iMzHEaM40KUqYsIa+ndv3NAn2RxCd5ubVdJJcX43zO6Ko0TFEZx/65gY3BEO6s
-----END RSA PRIVATE KEY-----" is used as key.
The hard-coded value "-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQDNwqLEe9wgTXCbC7+RPdDbBeqjdbs4kOPOIGzqLpXvJXlxxW8iMzHEaM40KUqYsIa+ndv3NAn2RxCd5ubVdJJcX43zO6Ko0TFEZx/65gY3BEO6s
-----END RSA PRIVATE KEY-----" is used as key.

CodeQL Show paths

```
20
21  exports.hash = data => crypto.createHash('md5').update(data).digest('hex')
22  exports.hmac = data => crypto.createHmac('sha256', 'pa4qacea4VK9t9nGv7yZtwmj').update(data).digest('hex')
```

Tool	Rule ID	Query
CodeQL	js/hardcoded-credentials	View source

Including unencrypted hard-coded authentication credentials in source code is dangerous because the credentials may be easily discovered. For example, the code may be open source, or it may be leaked or accidentally revealed, making the credentials visible to an attacker. This, in turn, might enable them to gain unauthorized access, or to obtain privileged information.

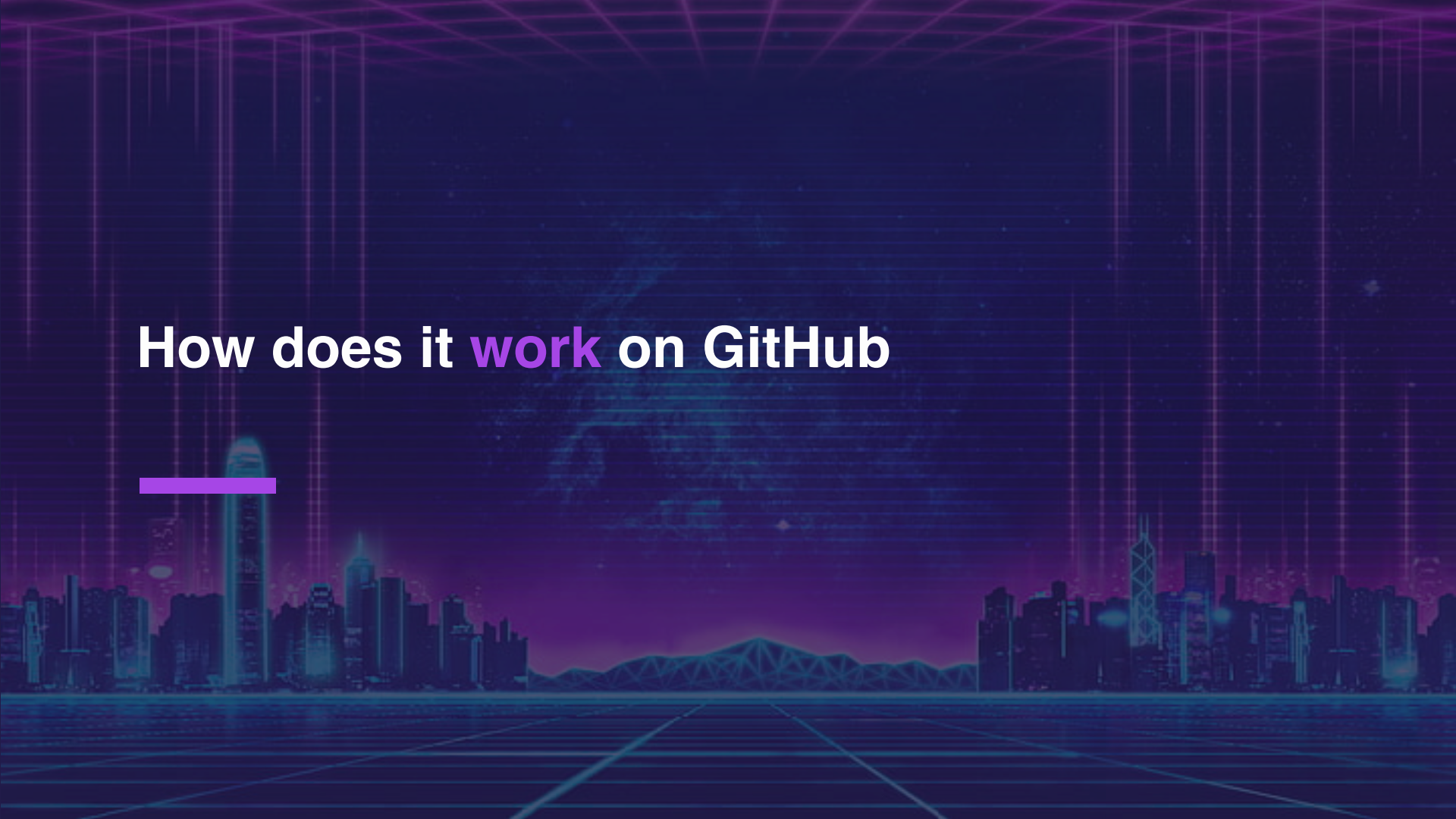
Show more

First detected in commit de3fe69 6 days ago

Update codeql-analysis.yml — Verified ✓ de3fe69

lib/insecurity.js#L19 on branch main

How does it work on GitHub



DSO-66 🔧 Contentful environment #1756

Merged SonyaMoisset merged 3 commits into master from DSO-66/contentful-env 14 days ago

Conversation 2 · Commits 3 · Checks 0 · Files changed 3 +21 −10

commented 14 days ago Member

Updated the Gatsby process to take in an optional `environment` option.

Cleaned over the current process to make things more readable and accessible.

added 2 commits 14 days ago

DSO-66 🔧 Updated config to work with new Contentful env e8b01e1

DSO-66 📝 Updated docs to reflect env var changes d5248ec

added Documentation Environment labels 14 days ago

added this to the **Environment** milestone 14 days ago

requested a review from **SonyaMoisset** 14 days ago

self-assigned this 14 days ago

added this to **In progress** in via automation 14 days ago

pull-request-size bot added the size/M label 14 days ago

changed the title **DSO-66-wrench-Contentful-environment** DSO-66 🔧 Contentful environment 14 days ago

Reviewers
SonyaMoisset

Assignees

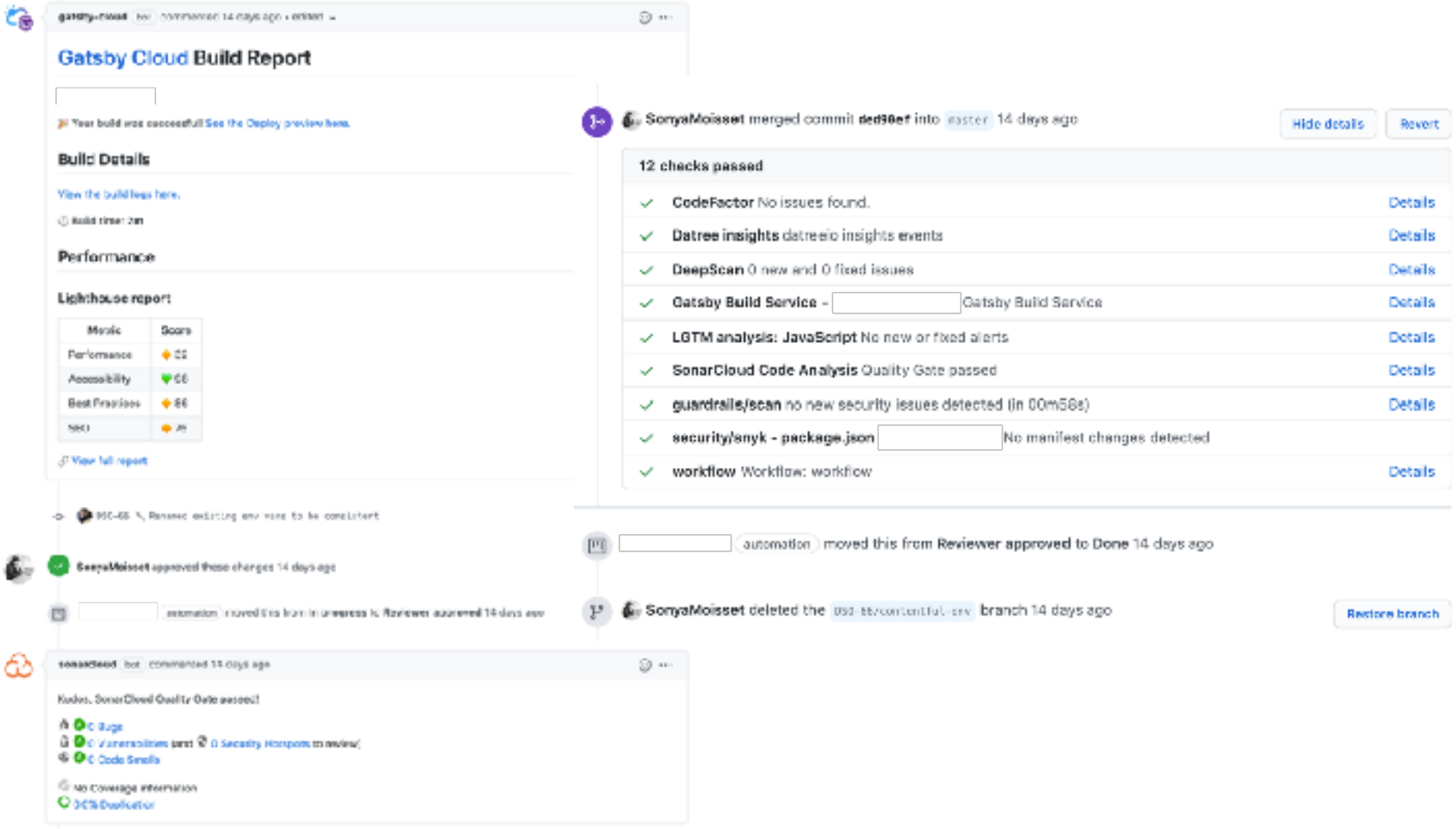
Labels
Documentation Environment size/M

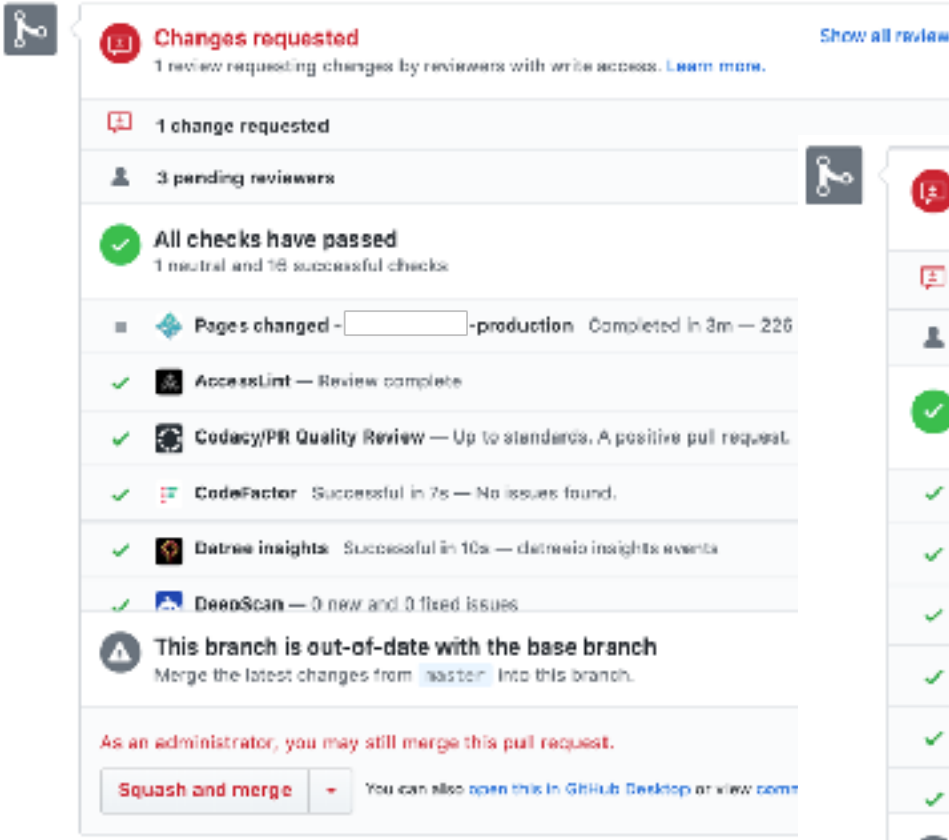
Projects
Done

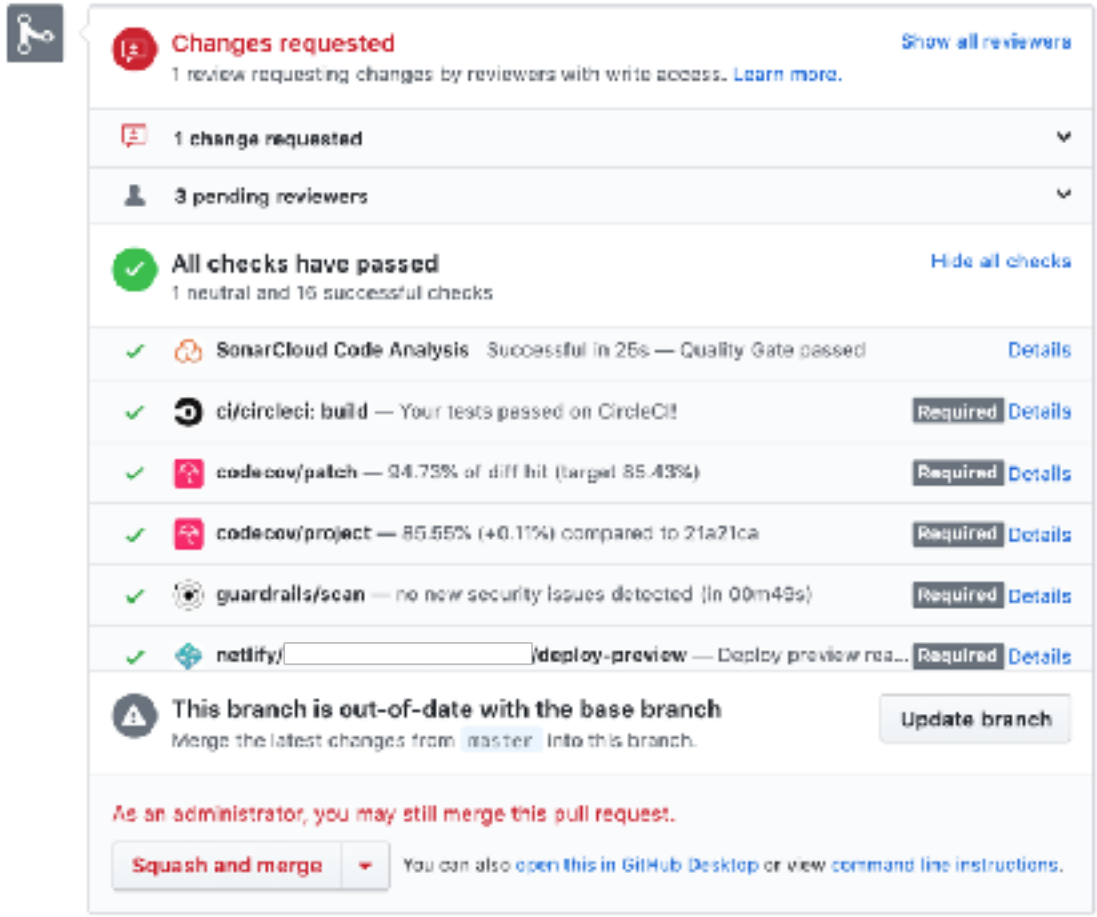
Milestone
environment

Linked issues
Successfully merging this pull request may close these issues.
None yet

Notifications Customize
Unsubscribe
You're receiving notifications because you're watching this repository.


Gatsby Cloud Build Report
Build Details
Performance
Lighthouse report
SonyaMoisset merged commit ded98ef into master 14 days ago
Hide details
Revert
12 checks passed
CodeFactor No issues found.
Datree insights datree/o insights events
DeepScan 0 new and 0 fixed issues
Gatsby Build Service – Gatsby Build Service
LGTM analysis: JavaScript No new or fixed alerts
SonarCloud Code Analysis Quality Gate passed
guardrails/scan no new security issues detected (in 00m56s)
security/snyk - package.json No manifest changes detected
workflow Workflow: workflow
automation moved this from Reviewer approved to Done 14 days ago
SonyaMoisset deleted the branch 14 days ago
Restore branch


Changes requested
1 review requesting changes by reviewers with write access. Learn more.
Show all reviewers
1 change requested
3 pending reviewers
All checks have passed
1 neutral and 16 successful checks
Pages changed - -production Completed in 3m — 226
AccessLint — Review complete
Codacy/PR Quality Review — Up to standards. A positive pull request.
CodeFactor Successful in 7s — No issues found.
Datree insights Successful in 10s — datree insights events
DeepScan — 0 new and 0 fixed issues
This branch is out-of-date with the base branch
Merge the latest changes from master into this branch.
As an administrator, you may still merge this pull request.
Squash and merge
You can also open this in GitHub Desktop or view comm


Changes requested
1 review requesting changes by reviewers with write access. Learn more.
Show all reviewers
1 change requested
3 pending reviewers
All checks have passed
1 neutral and 16 successful checks
Hide all checks
SonarCloud Code Analysis Successful in 26s — Quality Gate passed Details
ci/circleci: build — Your tests passed on CircleCI! Required Details
codecov/patch — 94.73% of diff hit (target 85.43%) Required Details
codecov/project — 85.55% (+0.11%) compared to 21a21ca Required Details
guardrails/scan — no new security issues detected (in 00m49s) Required Details
netlify/ /deploy-preview — Deploy preview rea... Required Details
This branch is out-of-date with the base branch
Merge the latest changes from master into this branch.
Update branch
As an administrator, you may still merge this pull request.
Squash and merge
You can also open this in GitHub Desktop or view command line instructions.

EVE-9: removal of flipmove #1209

Open wants to merge 8 commits into master from EVE-9/remove-flipmove

Conversation 2 · Commits 8 · Checks 8 · Files changed 12

add ternary to groupEventCards 7458428

- Netlify
  - Pages changed –
  - ✓ Header rules –
  - ✓ Mixed content –
  - ✓ Redirect rules –
- datreeio
  - ✓ Datree Insights
- LGTM.com
  - ✓ LGTM analysis: JavaScript
- codefactor.io
  - ✓ CodeFactor
- SonarCloud
  - ✓ SonarCloud Code Analy...

SonarCloud / SonarCloud Code Analysis
succeeded 2 days ago in 2m

Quality Gate passed

Passed

Additional information

The following metrics might not affect the Quality Gate status but improving them will improve your project code quality.

1 Issue

0 Bugs
0 Vulnerabilities (and 0 Security Hotspots to review)
1 Code Smell

Coverage and Duplications

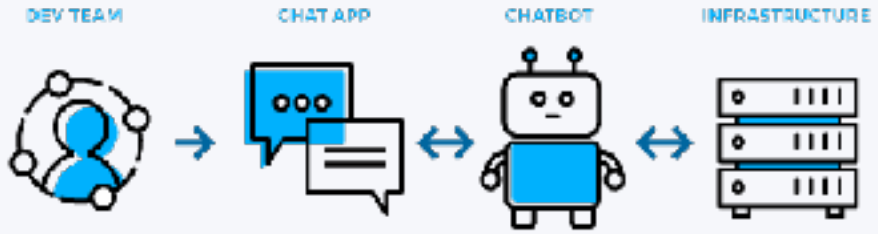
No Coverage information
0.0% Duplication (1.9% Estimated after merge)

View more details on SonarCloud


How to get value from ChatOps?

| ChatOps

ChatOps is a collaboration model that connects people, tools, process, and automation into a transparent workflow



CircleCI APP 9:08 PM

Success: SonyaMoisset's workflow (workflow) in [redacted] (improvement/security-headers) (739db7c)

Success: SonyaMoisset's workflow (workflow) in [redacted] (improvement/security-headers)
- Add Security headers (3dcd700 by SonyaMoisset)

CircleCI APP 9:22 PM

Success: SonyaMoisset's workflow (workflow) in [redacted] (improvement/security-headers)
- Fix typo in Security headers (4a0b9bb by SonyaMoisset)

Netlify APP 6:12 PM

There is a new deploy in process for [redacted]-production

Update Gatsby dependencies

Using git branch master, commit 739db7c85a6 · May 10th

Successful deploy of [redacted]-production

Update Gatsby dependencies

Or check out the build log

Using git branch master, commit 739db7c85a6 · May 10th

GuardRails APP 7:30 AM

Scan of bbaed78@[redacted]
no new security issues detected

Scan of 136ca09@[redacted]
no new security issues detected

Scan of 612a51d@[redacted]
no new security issues detected

Rollbar APP 11:35 AM

#10 10th error: Error: Missing resources for /

[redacted] in development

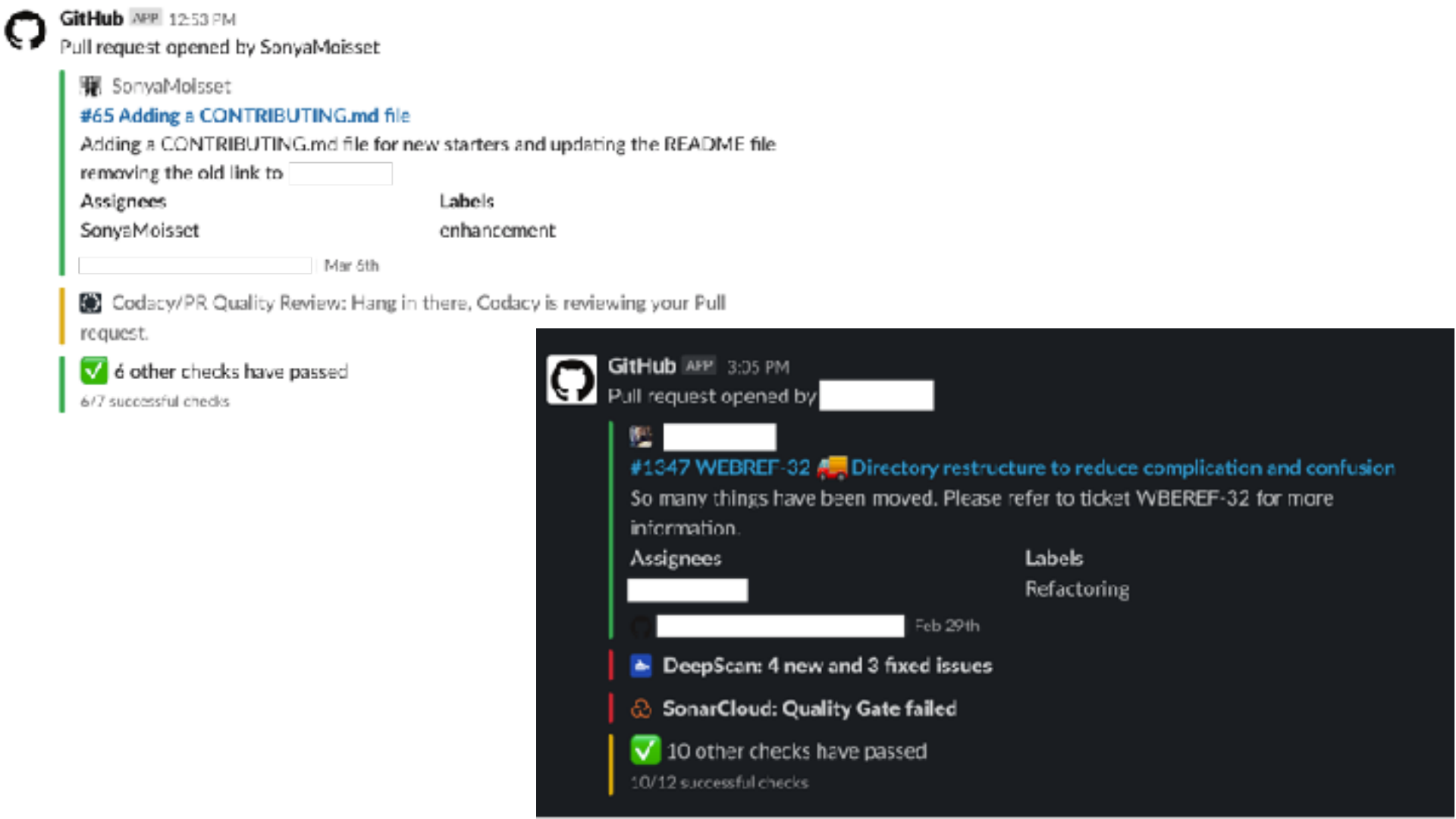
Resolve | Mute | error | Assign to user

Rollbar APP 5:40 PM

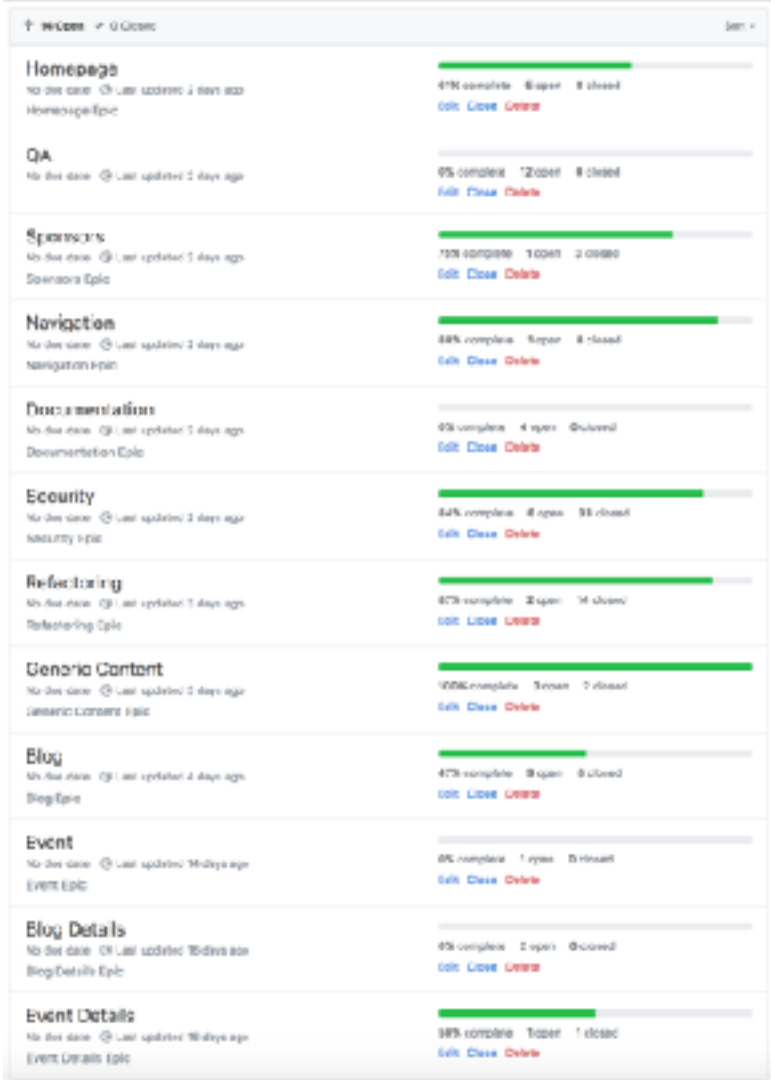
#17 New error: SyntaxError: The string did not match the expected pattern.

[redacted] in development

Resolve | Mute | error | Assign to user


GitHub APP 12:53 PM
Pull request opened by SonyaMoisset
SonyaMoisset
#65 Adding a CONTRIBUTING.md file
Adding a CONTRIBUTING.md file for new starters and updating the README file removing the old link to
Assignees
SonyaMoisset
Labels
enhancement
Mar 5th
Codacy/PR Quality Review: Hang in there, Codacy is reviewing your Pull request.
6 other checks have passed
6/7 successful checks
GitHub APP 3:05 PM
Pull request opened by
#1347 WEBREF-32 Directory restructure to reduce complication and confusion
So many things have been moved. Please refer to ticket WBEREF-32 for more information.
Assignees
Labels
Refactoring
Feb 29th
DeepScan: 4 new and 3 fixed issues
SonarCloud: Quality Gate failed
10 other checks have passed
10/12 successful checks

Any doc on GitHub?



Homepage

No due date **61%** complete

Homepage Epic

5 Open ✓ 8 Closed

- [QA] Volunteer Section - Replace pixelated images — Homepage, Improvement, QA
  #222 opened 2 days ago by SonyaMoisset
- [QA] Volunteer Section - Show more volunteers — Homepage, Improvement, QA
  #220 opened 2 days ago by SonyaMoisset
- Announcements — Homepage, New Component, New Feature, size/L
  #204 opened 2 days ago by codedev-exp • Review required
- Donate — Homepage, New Feature
  #108 opened 17 days ago by SonyaMoisset
- Announcements — Homepage, New Feature
  #107 opened 17 days ago by SonyaMoisset

Labels

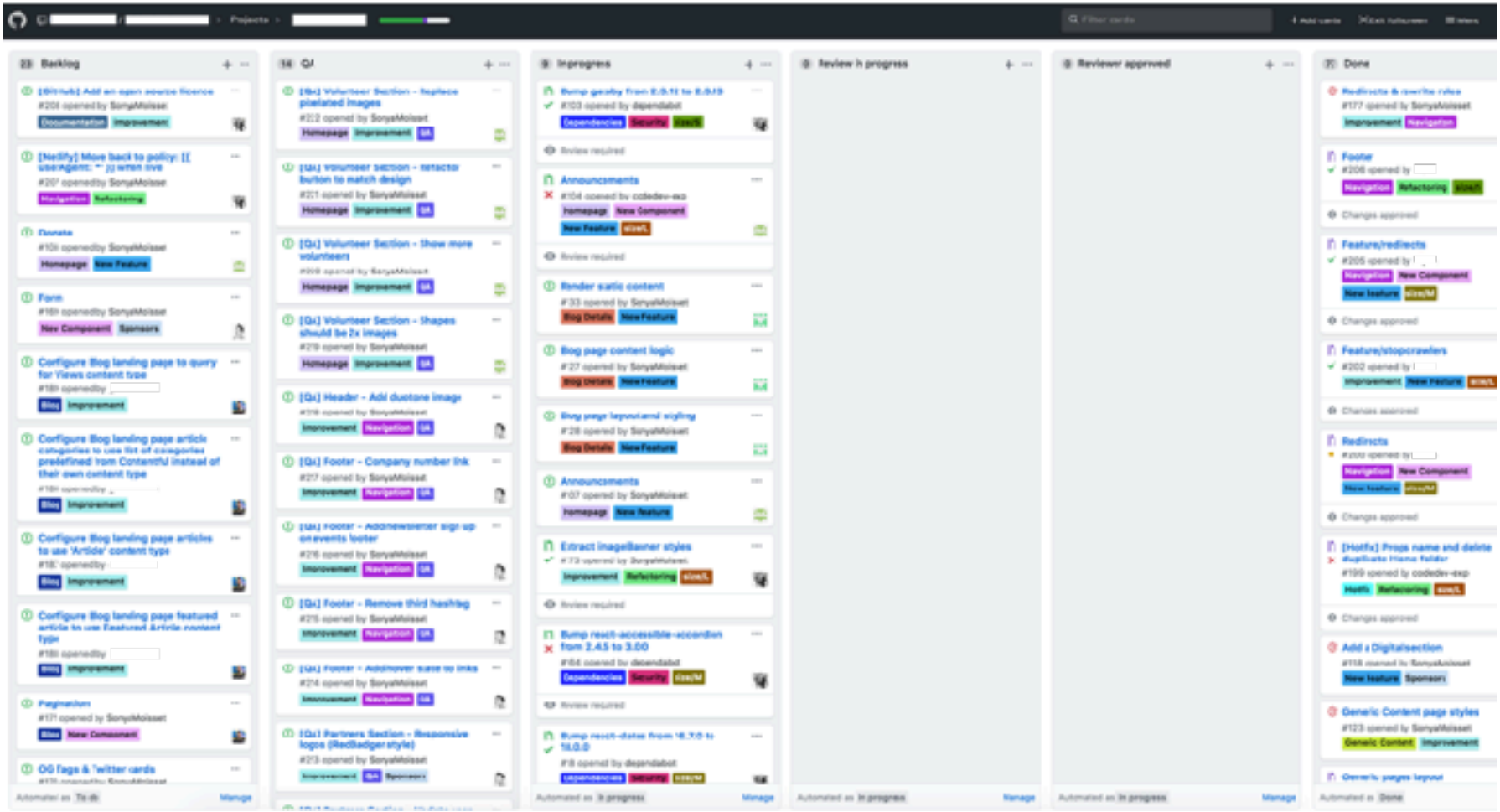
Documentation, Environment, size/M

Projects

Done

Milestone

Environment


Projects
Backlog
QA
In progress
Review in progress
Reviewer approved
Done
Footer
#206 opened by
Navigation
Refactoring
size/S
Changes approved
Feature/redirects
#205 opened by
Navigation
New Component
New feature
size/M
Changes approved
Feature/stopcrawlers
#202 opened by
Improvement
New feature
size/S
Changes approved
Redirects
Navigation
New Component
New feature
size/M
Changes approved
Add a Digital section
New feature
Sponsors
Generic Content page styles
#123 opened by SonyaMoisset
Generic Content
Improvement
Automated as Done


OSS Best Practices

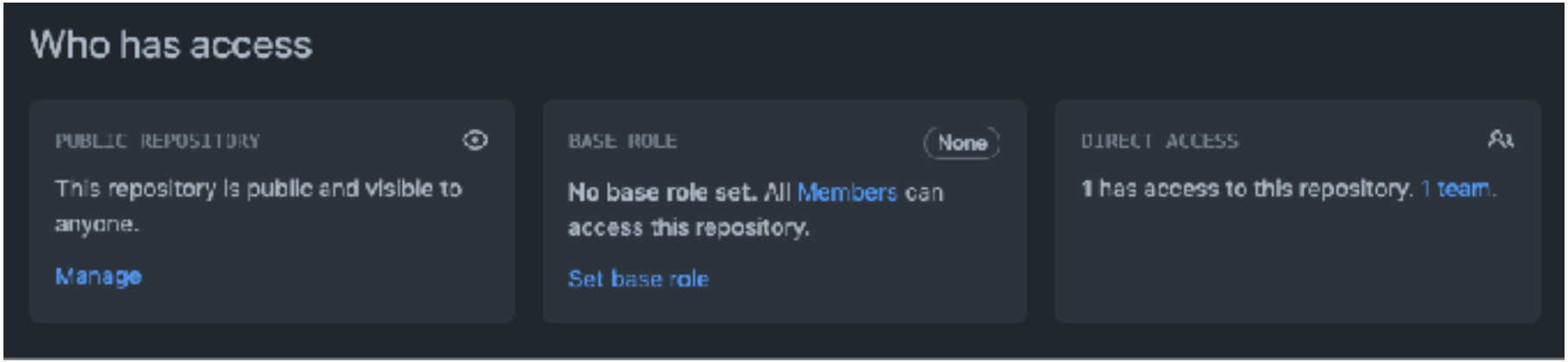
Apply the least privilege principle

Member repository permissions

Base permissions

Base permissions to the organization's repositories apply to all members and excludes outside collaborators. Since organization members can have permissions from multiple sources, members and collaborators who have been granted a higher level of access than the base permissions will retain their higher permission privileges.

No permission


Who has access
PUBLIC REPOSITORY
This repository is public and visible to anyone.
Manage
BASE ROLE
None
No base role set. All Members can access this repository.
Set base role
DIRECT ACCESS
1 has access to this repository. 1 team.

Make 2FA mandatory for all maintainers

Two-factor authentication

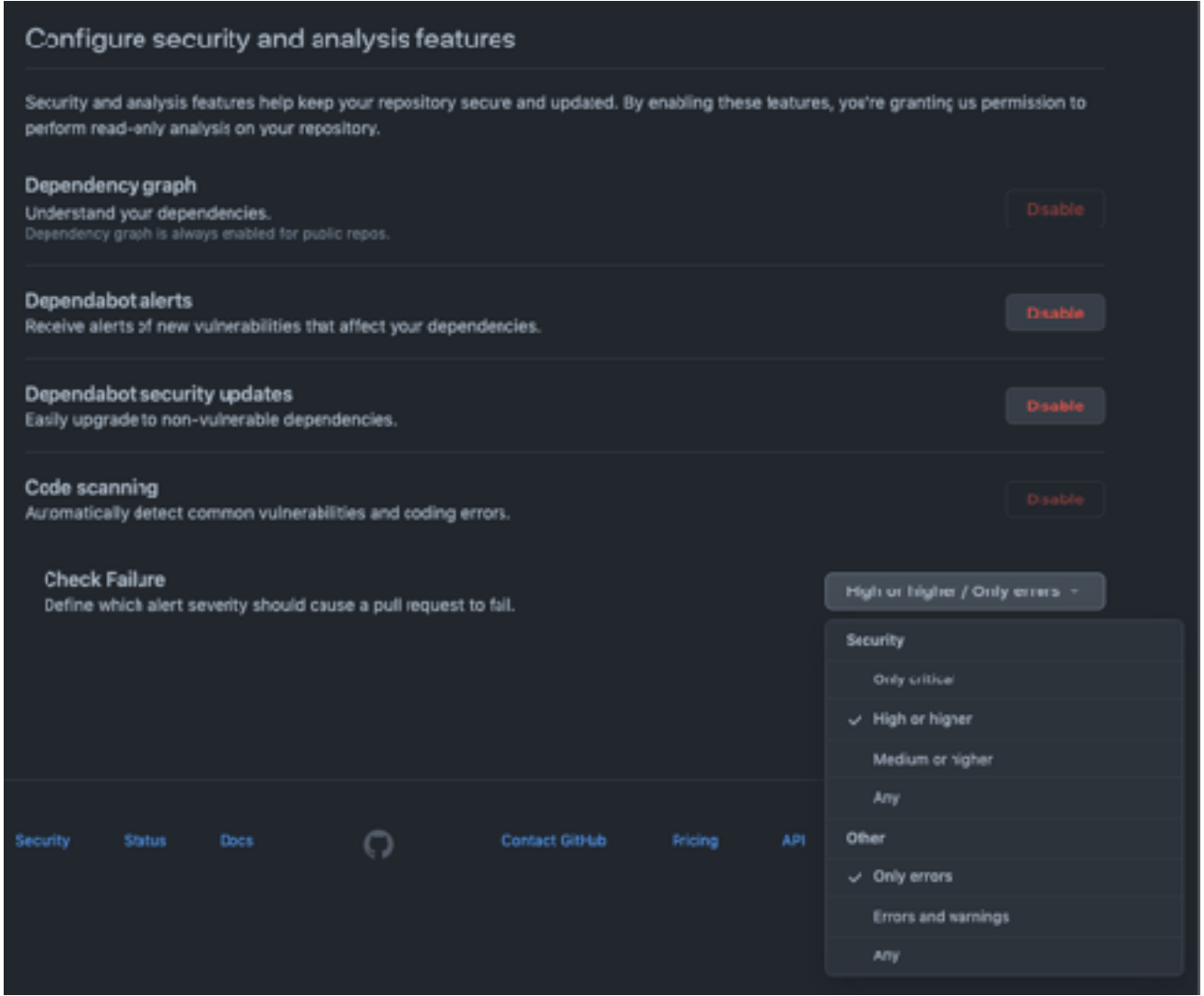
Requiring an additional authentication method adds another level of security for your organization.

☑ **Require two-factor authentication for everyone in the [redacted] organization.**

Members, billing managers, and outside collaborators who do not have two-factor authentication enabled for their personal account will be removed from the organization and will receive an email notifying them about the change. Learn more.

Save

Review your project controls


Configure security and analysis features
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.
Dependency graph is always enabled for public repos.
Disable
Dependabot alerts
Receive alerts of new vulnerabilities that affect your dependencies.
Disable
Dependabot security updates
Easily upgrade to non-vulnerable dependencies.
Disable
Code scanning
Automatically detect common vulnerabilities and coding errors.
Disable
Check Failure
Define which alert severity should cause a pull request to fail.
High or higher / Only errors
Security
High or higher
Medium or higher
Any
Other
Only errors
Errors and warnings
Any
Security
Status
Docs
Contact GitHub
Pricing
API

Actions permissions

Policies

Choose which repositories are permitted to use GitHub Actions.

All repositories ▾

- **Allow all actions**
  Any action can be used, regardless of who authored it or where it is defined.
- **Allow local actions only**
  Only actions defined in a repository within IDevOI can be used.
- **Allow select actions**
  Only actions that match specified criteria, plus actions defined in a repository within IDevOI, can be used. Learn more about allowing specific actions to run.

  - [x] Allow actions created by GitHub
  - [x] Allow Marketplace actions by verified creators

  Allow specified actions — Applies to public repositories only

  Enter a comma-separated list of actions

  Wildcards, tags, and SHAs are allowed. Examples: `monalisa/octocat@*`, `monalisa/octocat@v2`, `monalisa/*`

Save

Protect your main branch

Branch protection rules

Add rule

Define branch protection rules to disable force pushing, prevent branches from being deleted, and optionally require status checks before merging. New to branch protection rules? Learn more.

main

Currently applies to 1 branch

Edit Delete

Previous Next

☑ **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 branches to be up to date before merging**

This ensures pull requests targeting a matching branch have been tested with the latest code. This setting will not take effect unless at least one status check is enabled (see below).

Search for status checks in the last week for this repository

Status checks that are required.

- CodeFactor ×
- DeepScan ×
- LGTM analysis: JavaScript ×
- guardrails/scan ×
- security/snyk - package.json [redacted] ×
- SonarCloud Code Analysis ×
- Gatsby Build Service - [redacted] ×
- Analyze ×
- CodeQL ×
- workflow ×

Review required
At least 1 approving review is required by reviewers with write access. Learn more.

Add your review

Some checks haven't completed yet
2 expected, 2 in progress, and 4 successful checks

Hide all checks

- LGTM analysis: JavaScript — *In progress — Fetching git commits* — Details
- LGTM analysis: Python — *In progress — Fetching git commits* — Details
- GitGuardian Security Checks — Successful in 1s — No secrets detected ✅ — Required — Details
- guardrails/scan — no new security issues detected (in 00m17s) — Required — Details
- license/snyk (SonyaMoisset) — No license issues in 2 tests — Details
- security/snyk (SonyaMoisset) — No manifest changes detected in 2 projects — Details

Merging is blocked
Merging can be performed automatically with 1 approving review.

☐ Merge without waiting for requirements to be met (bypass branch protections)

Merge pull request ▾

You can also open this in GitHub Desktop or view command line instructions.

Enable notifications/alerts

Access to alerts

Admins, users, and teams in the list below have permission to view and manage Dependabot or secret scanning alerts. These users may be notified when a new vulnerability is found in one of this repository's dependencies and when a secret or key is checked in. They will also see additional details when viewing Dependabot security updates. Individuals can manage how they receive these alerts in their notification settings.

Choose the people or teams you would like to grant access

Search for people or teams

People and teams with access

Organization and repository administrators
These members always see Dependabot and secret scanning alerts.

Save changes

Notifications

Setup email addresses to receive notifications when push events are triggered.

Address *

one@example.com two@example.com

Whitespace separated email addresses (at most two).

Approved header

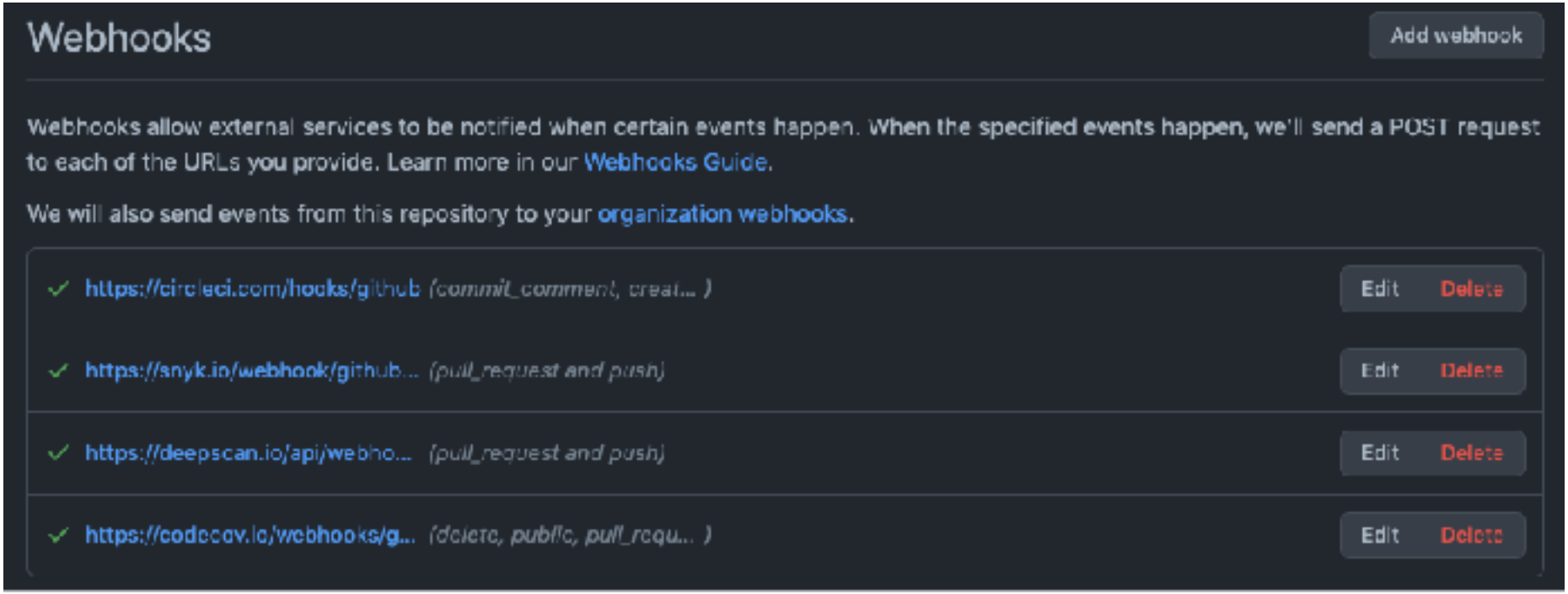
Sets the Approved header to automatically approve the message in a read-only or moderated mailing list.

Active

We will send notification emails to the listed addresses when a push event is triggered.

Setup notifications

Review webhooks


Webhooks
Add webhook
Webhooks allow external services to be notified when certain events happen. When the specified events happen, we'll send a POST request to each of the URLs you provide. Learn more in our Webhooks Guide.
We will also send events from this repository to your organization webhooks.
https://circleci.com/hooks/github (commit_comment, creat...)
Edit Delete
https://snyk.io/webhook/github... (pull_request and push)
Edit Delete
https://deepscan.io/api/webho... (pull_request and push)
Edit Delete
https://codecov.io/webhooks/g... (delete, public, pull_requ...)
Edit Delete

Third-party application access policy

Policy: Access restricted ✓

Only approved applications can access data in this organization. Applications owned by PrideInLondon always have access.

Remove restrictions

CircleCI	✓ Approved
Snyk	✓ Approved
LGTM	✓ Approved
Codecov	✓ Approved
codefactor.io	✓ Approved
GuardRails OAuth (Deprecated)	✓ Approved
CodeScene Authentication	✓ Approved
CodeScene repositories	✓ Approved
DeepSource	✓ Approved
restrict	✓ Approved
Atlassian Cloud	✓ Approved
Chromatic OAuth	✓ Approved
Travis CI for Open Source	✗ Denied
Greenkeeper	✗ Denied
Codacy Login	✗ Denied
Coveralls Pro	✗ Denied
codeclimate.io	✗ Denied
codebeat	✗ Denied
Percy	✗ Denied
Nightfall AI	✗ Denied
Test Quality	✗ Denied
Coverity Scan	✗ Denied
GitKraken	✗ Denied

Installed GitHub Apps

GitHub Apps augment and extend your workflows on GitHub with commercial, open source, and homegrown tools.

AccessLint

Configure

Chromatic.com

Configure

CircleCI Checks

Configure

Codecov

Configure

codefactor.io

Configure

dataeelo

Configure

Dependabot Preview

Configure

Gatsby Cloud

Configure

Guardrails

Configure

Permissions

✓ **Read** access to code and metadata

✓ **Read and write** access to commit statuses and pull requests

Repository access

◉ **All repositories**
This applies to all current and future repositories.

○ **Only select repositories**

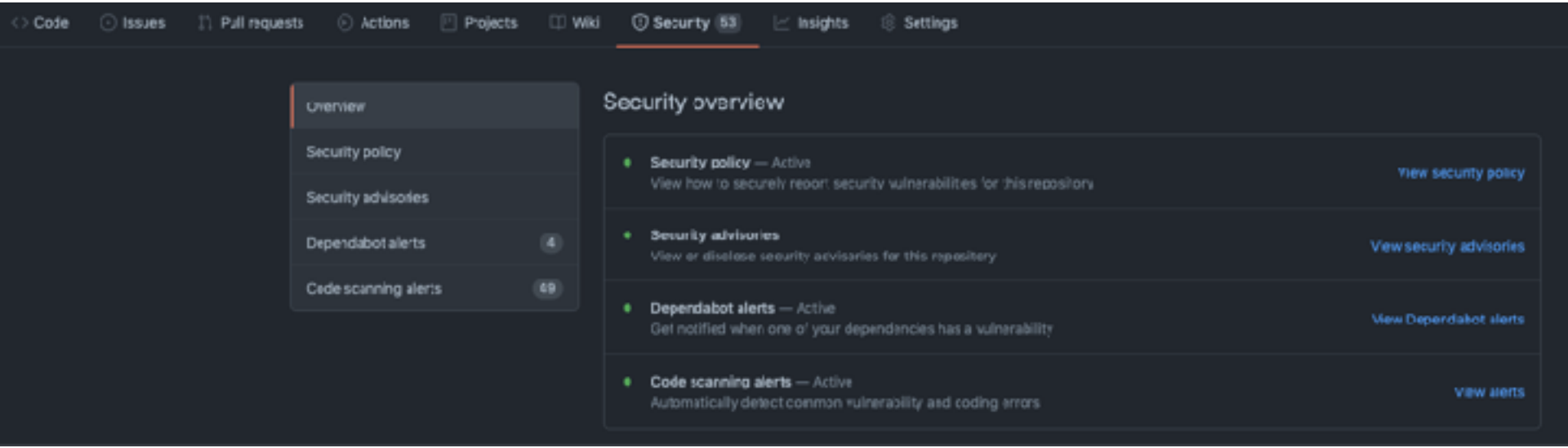
Save | Cancel

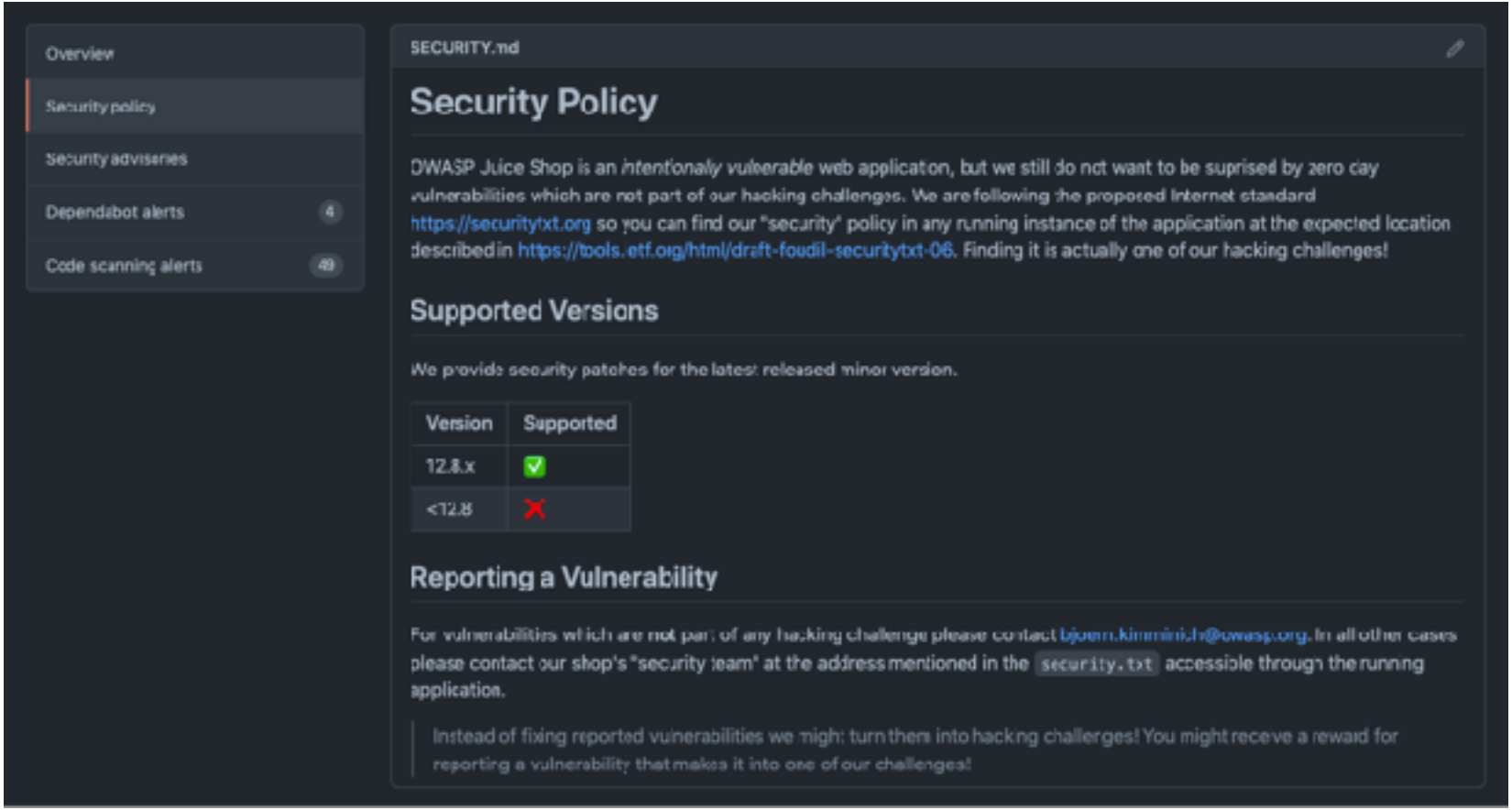
Danger zone

Suspend your installation
This will block the app access to your resources.
Suspend

Uninstall "AccessLint"
This will remove the app and revoke access to all resources.
Uninstall

Review Security Overview Checklist


Code
Issues
Pull requests
Actions
Projects
Wiki
Security 53
Insights
Settings
Overview
Security policy
Security advisories
Dependabot alerts 4
Code scanning alerts 49
Security overview
Security policy — Active
View how to securely report security vulnerabilities for this repository
View security policy
Security advisories
View or disclose security advisories for this repository
View security advisories
Dependabot alerts — Active
Get notified when one of your dependencies has a vulnerability
View Dependabot alerts
Code scanning alerts — Active
Automatically detect common vulnerability and coding errors
View alerts


Overview
Security policy
Security advisories
Dependabot alerts 4
Code scanning alerts 49
SECURITY.md
Security Policy
OWASP Juice Shop is an *intentionally vulnerable* web application, but we still do not want to be suprised by zero day vulnerabilities which are not part of our hacking challenges. We are following the proposed Internet standard https://securitytxt.org so you can find our "security" policy in any running instance of the application at the expected location described in https://tools.ietf.org/html/draft-foudil-securitytxt-06. Finding it is actually one of our hacking challenges!
Supported Versions
We provide security patches for the latest released minor version.
Version
Supported
12.8.x
<12.8
Reporting a Vulnerability
For vulnerabilities which are not part of any hacking challenge please contact bjoern.kimminich@owasp.org. In all other cases please contact our shop's "security team" at the address mentioned in the security.txt accessible through the running application.
Instead of fixing reported vulnerabilities we might turn them into hacking challenges! You might receive a reward for reporting a vulnerability that makes it into one of our challenges!

Open a draft security advisory

After the draft security advisory is open, you can privately discuss it with collaborators and create a temporary private fork where you can collaborate on a fix. If you've already fixed the vulnerability, just fill out the draft security advisory and then publish it.

Affected product

Ecosystem

Select an ecosystem

Package name

e.g. example.js

Affected versions

e.g. <1.2.3

Patched versions

e.g. 1.2.3

Severity

Select severity

Common weakness enumerator (CWE)

Search by CWE

CVE identifier

Request CVE ID later

Title

Description

Write Preview

Impact
What kind of vulnerability is it? Who is impacted?

Patches
Has the problem been patched? What versions should users upgrade to?

Workarounds
Is there a way for users to fix or remediate the vulnerability without upgrading?

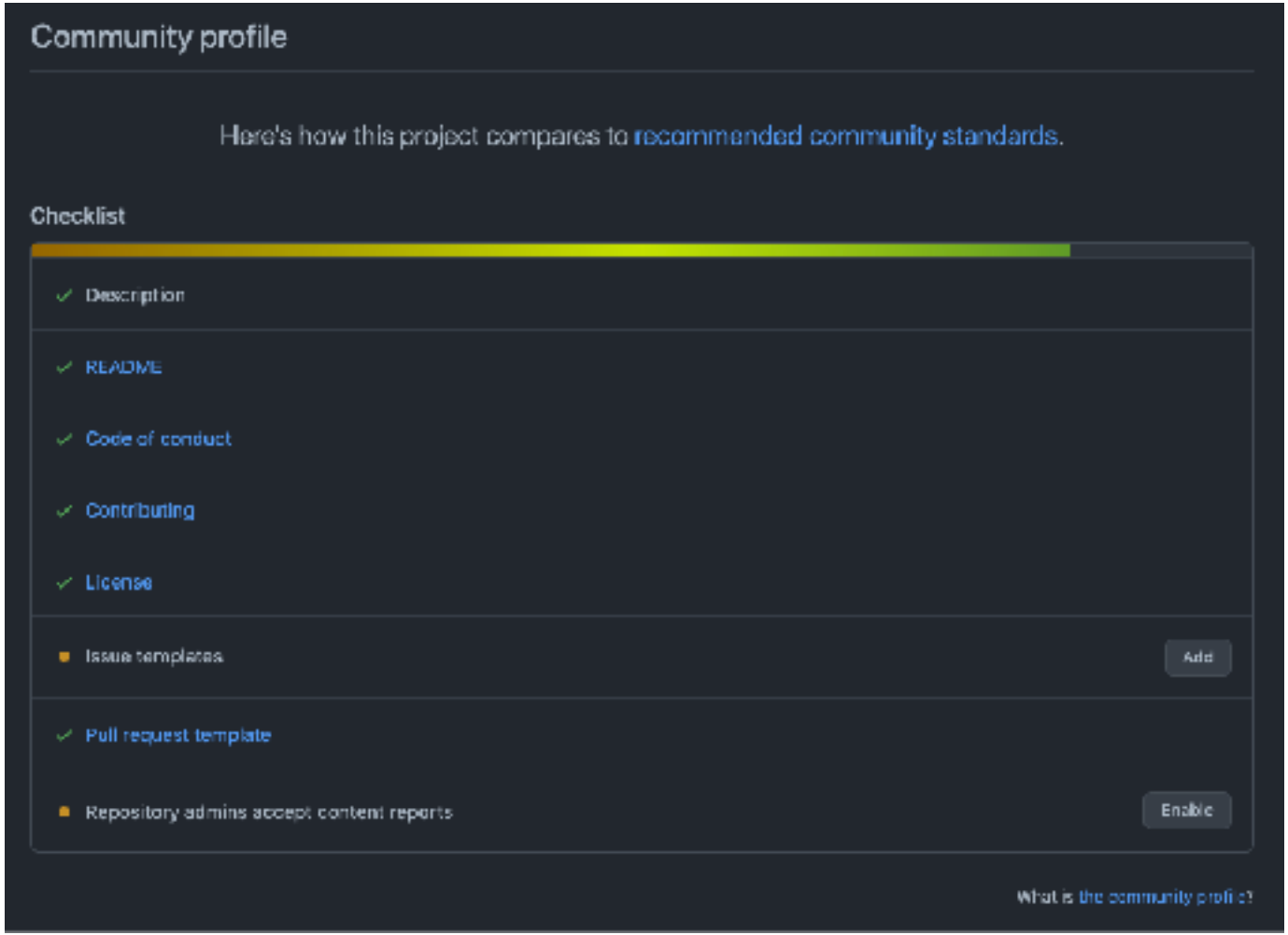
Access and visibility

Until it is published, this draft security advisory will only be visible to the owner of `fonyuAdviser/CVE-XP-IS-Demo`. Other users and teams may be added once the advisory is created.

Once published, security advisories on public repositories are visible to everyone.

Once reviewed by GitHub, security advisories may be broadcast on the GitHub advisory Database. They may also trigger Dependabot alerts to users that depend on this repository.

Review Open Source Checklist


Community profile
Here's how this project compares to recommended community standards.
Checklist
Description
README
Code of conduct
Contributing
License
Issue templates
Add
Pull request template
Repository admins accept content reports
Enable
What is the community profile?

Implement Open Source workflow

GitHub Action

First interaction

v1.1.0 Latest version

Use latest version

First Interaction

An action for filtering pull requests and issues from first-time contributors.

Usage

See action.yml

```
steps:
- uses: actions/first-interaction@v1
  with:
    repo-token: ${{ secrets.GITHUB_TOKEN }}
    issue-message: '# Message with markdown.\nThis is the message that will be disp
    pr-message: 'Message that will be displayed on users' first pr. Look, a `code b
```

License

The scripts and documentation in this project are released under the MIT License

Verified creator

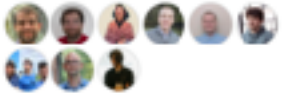
GitHub has verified that this action was created by **actions**.

Learn more about verified Actions.

Stars

☆ Star 340

Contributors



Categories

Utilities

Links

- actions/first-interaction
- Open issues 17
- Pull requests 14
- Report abuse

GitHub Action

Close Stale Issues

v4.0.0 Latest version

Use latest version

Close Stale Issues and PRs

Warns and then closes issues and PRs that have had no activity for a specified amount of time.

The configuration must be on the default branch and the default values are:

- Add a label 'Stale' on issues and pull requests after 60 days of inactivity
- Close the stale issues and pull requests after 7 days of inactivity
- If an update/comment occur on stale issues or pull requests, the stale label will be removed and the timer will restart

Recommended permissions

For the execution of this action, it must be able to fetch all issues and pull requests from your repository.
In addition, based on the provided configuration, the action could require more permission(s) (e.g.: add label, remove label, comment, close, etc.).
This can be achieved with the following configuration in the action if the permissions are restricted.

```
permissions:
  issues: write
  pull-requests: write
```

You can find more information about the required permissions under the corresponding options that you wish to use.

Verified creator

GitHub has verified that this action was created by actions.

Learn more about verified Actions.

Stars

Star 469

Contributors

Categories

Utilities

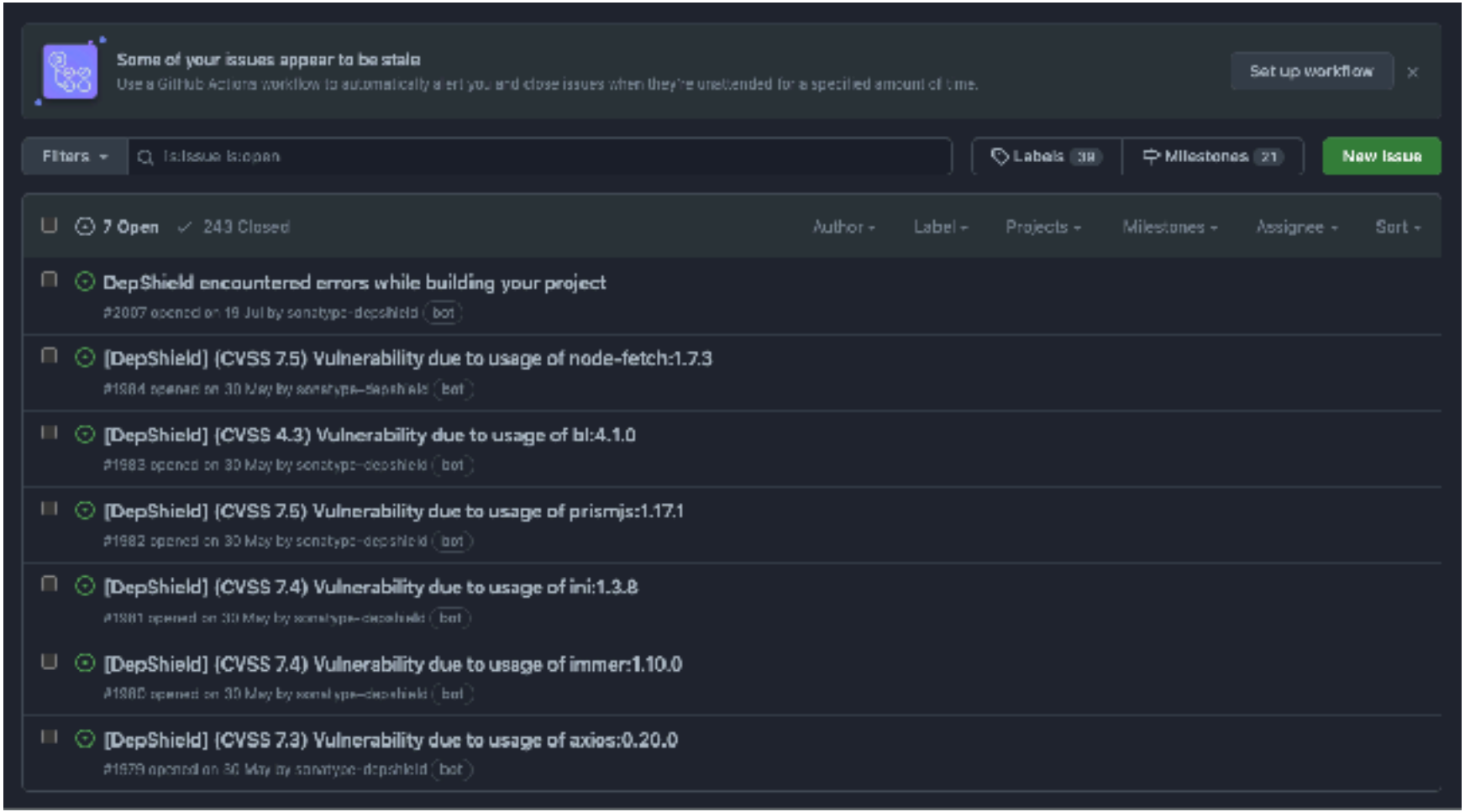
Links

actions/stale

Open issues 18

Pull requests 11

Report abuse

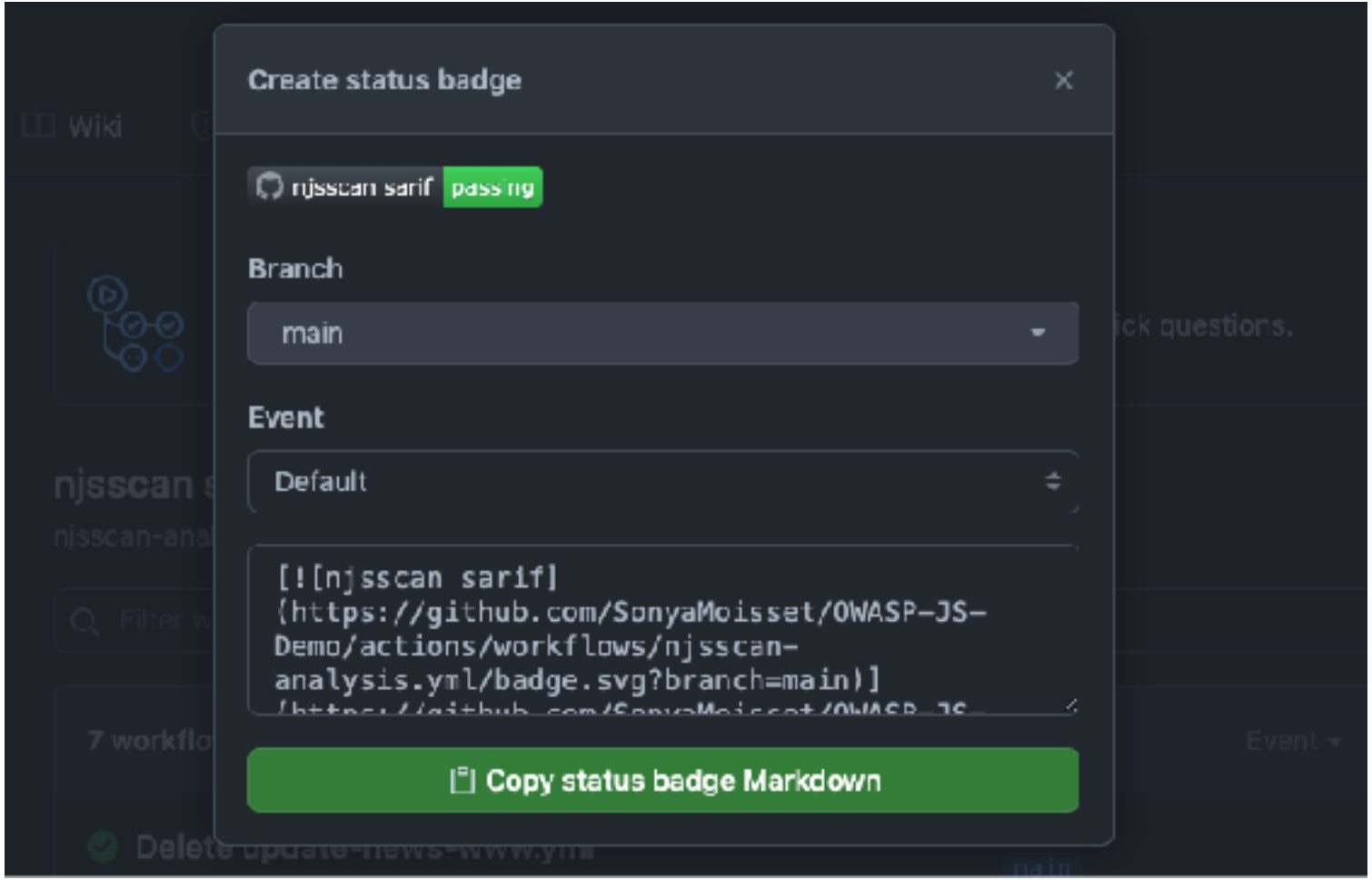

Some of your issues appear to be stale
Use a GitHub Actions workflow to automatically alert you and close issues when they're unattended for a specified amount of time.
Set up workflow
Filters
is:issue is:open
Labels 38
Milestones 21
New issue
7 Open
243 Closed
Author
Label
Projects
Milestones
Assignee
Sort
DepShield encountered errors while building your project
#2007 opened on 19 Jul by sonatype-depshield bot
[DepShield] (CVSS 7.5) Vulnerability due to usage of node-fetch:1.7.3
#1984 opened on 30 May by sonatype-depshield bot
[DepShield] (CVSS 4.3) Vulnerability due to usage of bl:4.1.0
#1983 opened on 30 May by sonatype-depshield bot
[DepShield] (CVSS 7.5) Vulnerability due to usage of prismjs:1.17.1
#1982 opened on 30 May by sonatype-depshield bot
[DepShield] (CVSS 7.4) Vulnerability due to usage of ini:1.3.8
#1981 opened on 30 May by sonatype-depshield bot
[DepShield] (CVSS 7.4) Vulnerability due to usage of immer:1.10.0
#1980 opened on 30 May by sonatype-depshield bot
[DepShield] (CVSS 7.3) Vulnerability due to usage of axios:0.20.0
#1979 opened on 30 May by sonatype-depshield bot

Showcase your Open Source Project Status

README.md

website

This project is a community effort to provide the website. The project is written in JavaScript/TypeScript and leverages the Gatsby and React web frameworks.


Create status badge
njsscan sarif passing
Branch
main
Event
Default
[![njsscan sarif]
(https://github.com/SonyaMoisset/OWASP-JS-
Demo/actions/workflows/njsscan-
analysis.yml/badge.svg?branch=main)]
Copy status badge Markdown

OWASP-JS-Demo / README.md in main

Cancel changes

<> Edit file Preview Spaces 2 Soft wrap

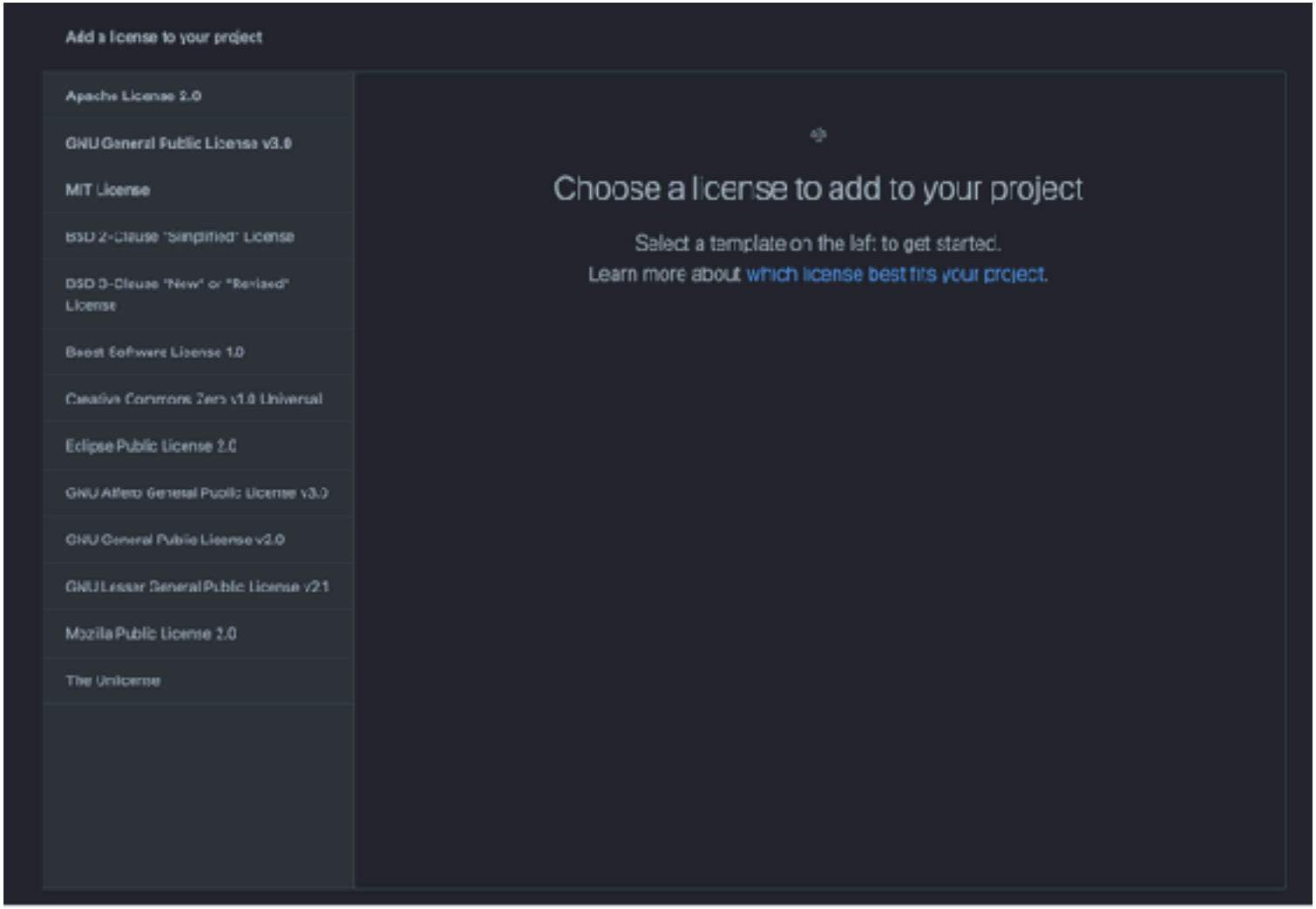
```
1  # OWASP JS Demo - Whitesource
2
3
4  |[Codacy Security Scan](https://github.com/SonyaMoisset/OWASP-JS-Demo/actions/workflows/codacy-analysis.yml/badge.svg?branch=main)|
   (https://github.com/SonyaMoisset/OWASP-JS-Demo/actions/workflows/codacy-analysis.yml)
5  |[CodeQL](https://github.com/SonyaMoisset/OWASP-JS-Demo/actions/workflows/codeql-analysis.yml/badge.svg?branch=main)|(https://github.com/SonyaMoisset/OWASP-JS-
   Demo/actions/workflows/codeql-analysis.yml)
6  |[njsscan sarif](https://github.com/SonyaMoisset/OWASP-JS-Demo/actions/workflows/njsscan-analysis.yml/badge.svg?branch=main)|
   (https://github.com/SonyaMoisset/OWASP-JS-Demo/actions/workflows/njsscan-analysis.yml)
```

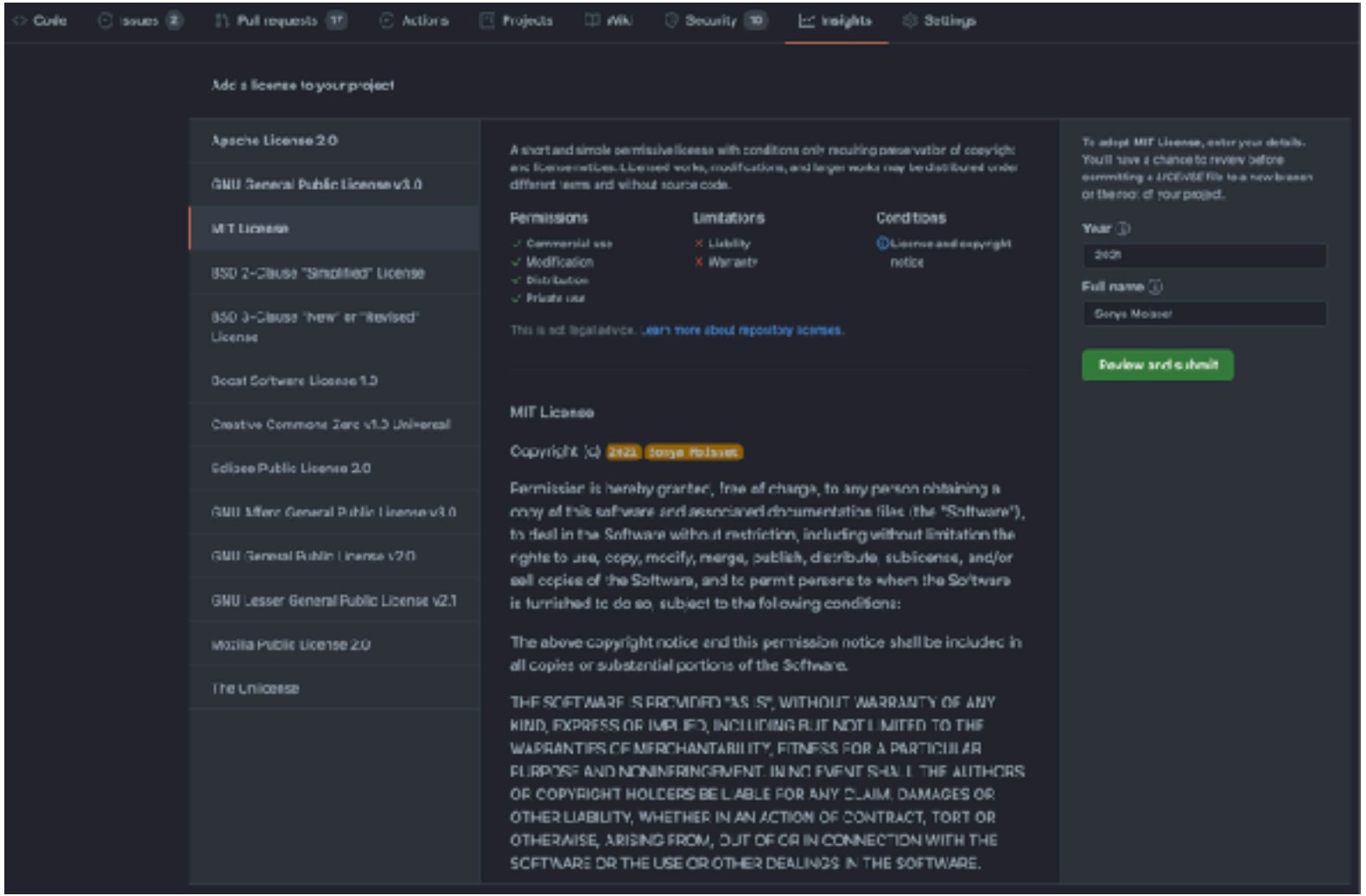
<> Edit file Preview Show diff

OWASP JS Demo - Whitesource

Codacy Security Scan passing CodeQL passing njsscan sarif passing

Check/Add licence


Add a license to your project
Apache License 2.0
GNU General Public License v3.0
MIT License
BSD 2-Clause "Simplified" License
BSD 3-Clause "New" or "Revised" License
Boost Software License 1.0
Creative Commons Zero v1.0 Universal
Eclipse Public License 2.0
GNU Affero General Public License v3.0
GNU General Public License v2.0
GNU Lesser General Public License v2.1
Mozilla Public License 2.0
The Unlicense
Choose a license to add to your project
Select a template on the left to get started.
Learn more about which license best fits your project.


Code
Issues 2
Pull requests 17
Actions
Projects
Wiki
Security 10
Insights
Settings
Add a license to your project
Apache License 2.0
GNU General Public License v3.0
MIT License
BSD 2-Clause "Simplified" License
BSD 3-Clause "New" or "Revised" License
Boost Software License 1.0
Creative Commons Zero v1.0 Universal
Eclipse Public License 2.0
GNU Affero General Public License v3.0
GNU General Public License v2.0
GNU Lesser General Public License v2.1
Mozilla Public License 2.0
The Unlicense
A short and simple permissive license with conditions only requiring preservation of copyright and license notices. Licensed works, modifications, and larger works may be distributed under different terms and without source code.
Permissions
Commercial use
Modification
Distribution
Private use
Limitations
Liability
Warranty
Conditions
License and copyright notice
This is not legal advice. Learn more about repository licenses.
MIT License
Copyright (c) 2021 Sonya Moisset
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
To adopt MIT License, enter your details. You'll have a chance to review before committing a LICENSE file to a new branch or the root of your project.
Year
2021
Full name
Sonya Moisset
Review and submit

Check Website Score

Google
Lighthouse

Google

PageSpeed Insights

“Adopt a
Dev{Sec}Ops approach”

Sonya

Friendly Security 🥑

“

Address
Open-Source Vulnerabilities

”

Sonya

Friendly Security 🥑

“

Automate simple Security tasks

”

Sonya

Friendly Security 🥑

“

Be aware of your own assets

”

Sonya

Friendly Security 🥑

“

Security training for developers

”

Sonya

Friendly Security 🥑

| KEY TAKEAWAYS

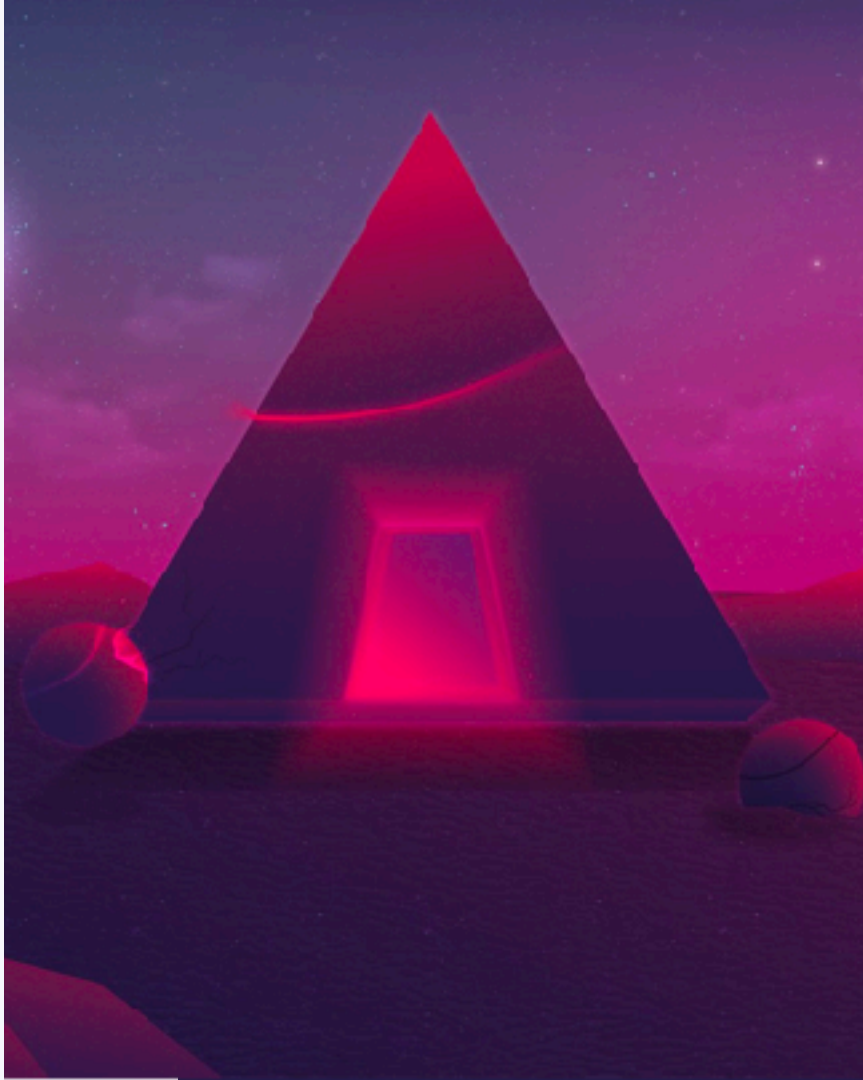
_+ Open source can be a vector for large scale cyber attacks

_+ Leverage the applications available on GitHub marketplace

_+ Create a small pipeline and harden the security of the projects for your collaborators

_+ Experiment

_+ Don’t push your keys on GitHub! 😡 😡 😡



Sonya Moisset

Senior Security 🥑 @ Snyk

💖 Passionate about Dev{Sec}Ops, Open Source & Cloud Security

🌟 GitHub Star

☁️ OpenUK Security Advisory Board Member

💻 Founder Epic Women in Cyber

✍️ Writer for FreeCodeCamp

🏆 30 Top Female Cybersecurity Leaders 2022

😀🌍🇫🇷🌈🦄🎛️✈️💻☕🎧🎬📷🕹️

@SonyaMoisset

snyk

Thank you!

Stay safe in your journey to OSS Contributions 😄