
GitHub Advanced Security Demo



Agenda

What is GitHub Advanced Security (GHAS)

Why GHAS

Live Demo

Questions

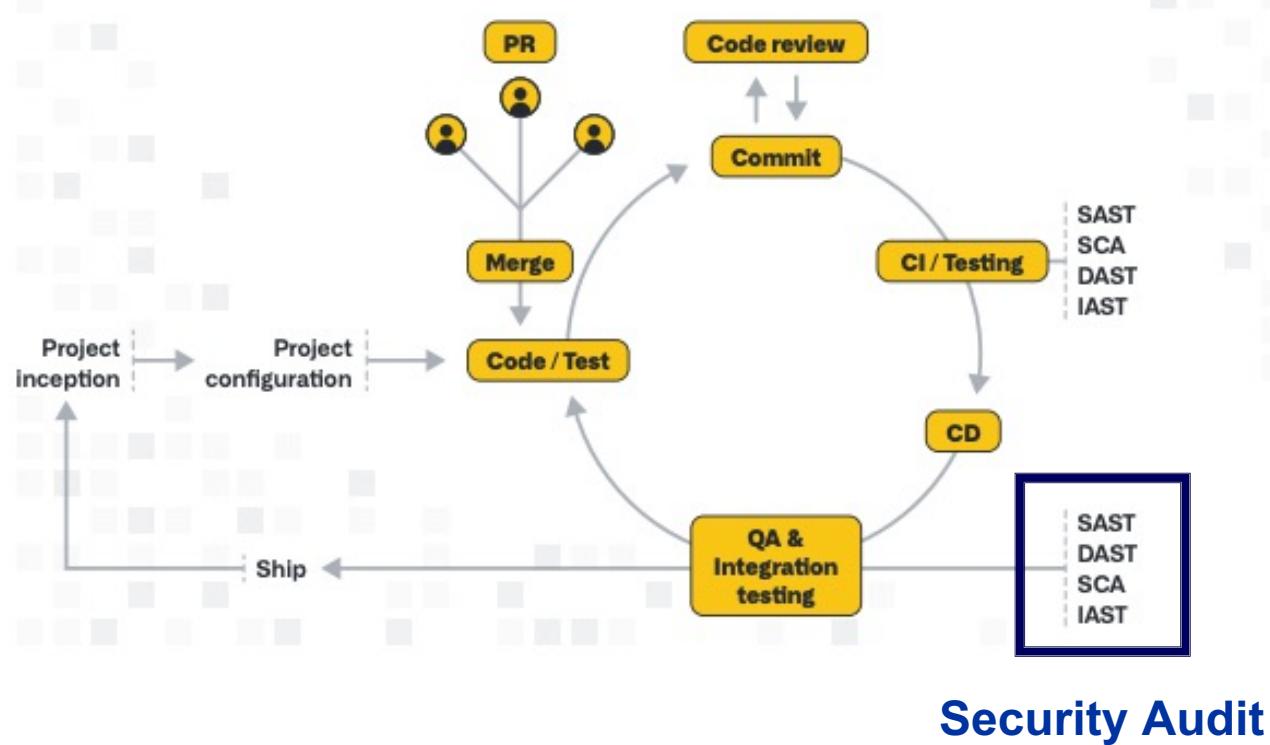


What is GitHub Advanced Security

Traditional Approach

Issues

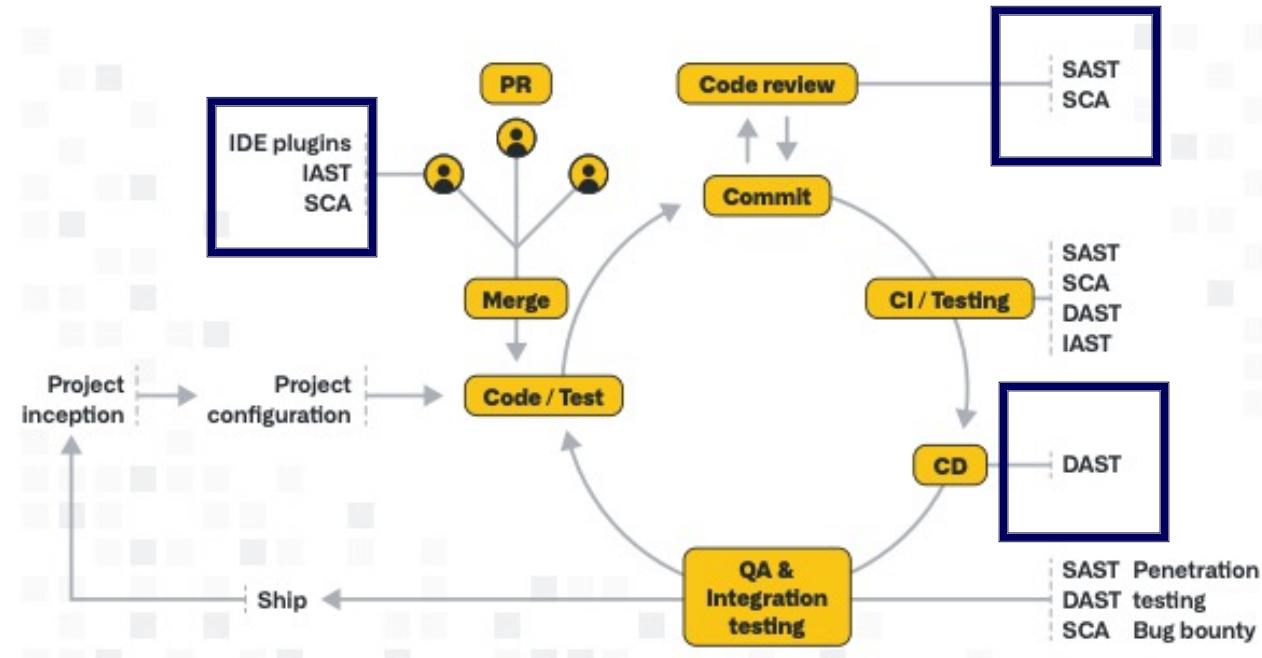
- Security comes too late in the development process
- Scan results, if any, often have a high noise-to-signal ratio
- Manual reviews cause bottlenecks



Targeted End to End Approach

Issues

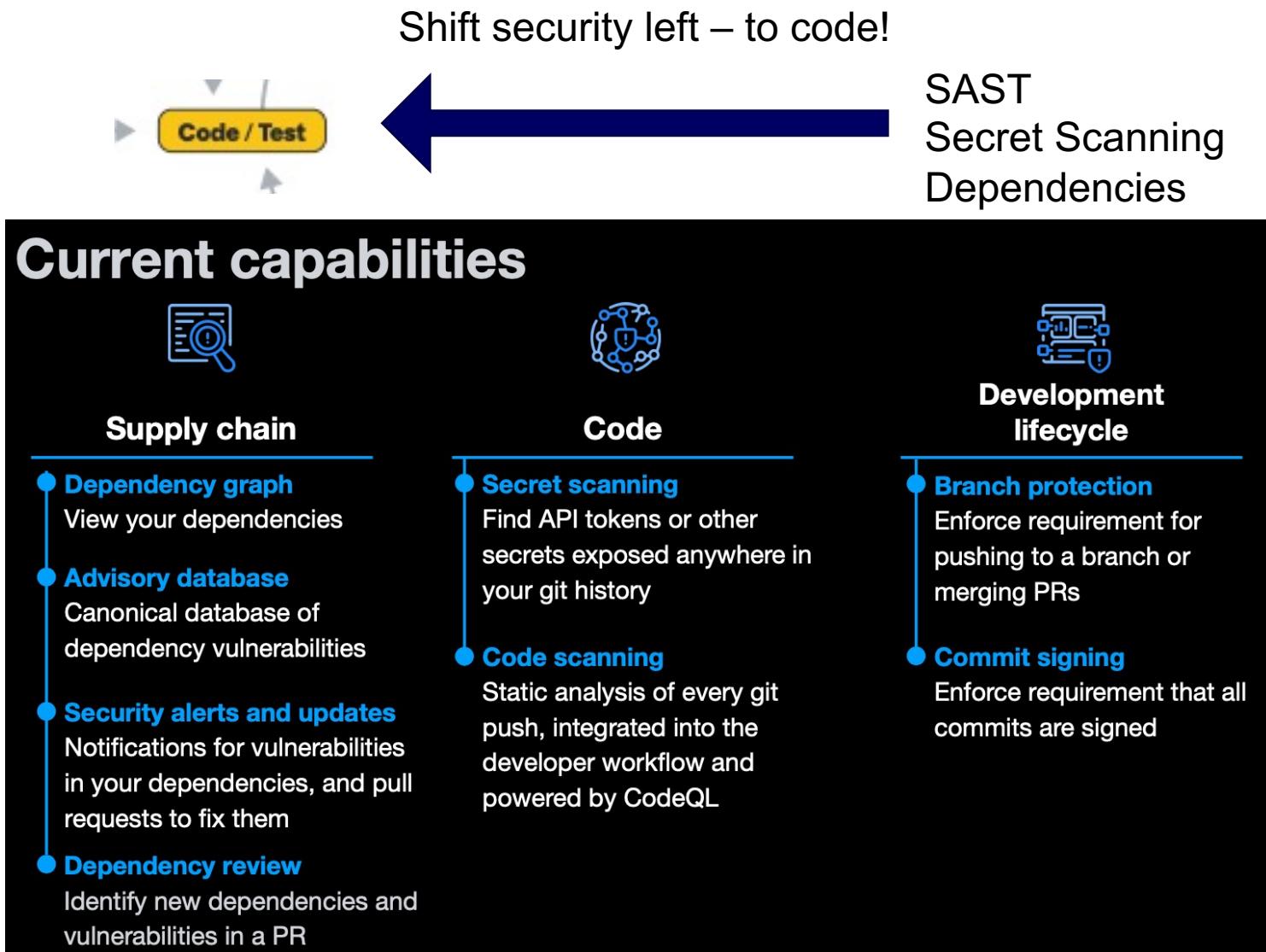
- Integrations require a lot of upkeep
- Several disparate systems tracking results
- Security and Dev teams continue to work in silos
- Still have false positive issues
- Traditional tools fail to keep pace with the software ecosystem



Solution?

GitHub Advanced Security Selling Points

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



Demo

Demo Overview

Demo overview

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

Current capabilities



Supply chain

- **Dependency graph**
View your dependencies
- **Advisory database**
Canonical database of dependency vulnerabilities
- **Security alerts and updates**
Notifications for vulnerabilities in your dependencies, and pull requests to fix them
- **Dependency review**
Identify new dependencies and vulnerabilities in a PR



Code

- **Secret scanning**
Find API tokens or other secrets exposed anywhere in your git history
- **Code scanning**
Static analysis of every git push, integrated into the developer workflow and powered by CodeQL



Development lifecycle

- **Branch protection**
Enforce requirement for pushing to a branch or merging PRs
- **Commit signing**
Enforce requirement that all commits are signed

GitHub Advanced Security – GitHub.com

The screenshot shows the GitHub Advanced Security settings page. The left sidebar has a dark background with white text and a vertical red bar highlighting the 'Security & analysis' section. The main content area has a light gray background with a blue header bar containing navigation links: requests (1), Actions, Projects, Wiki, Security (16), Insights, and Settings (which is underlined). The main title is 'Configure security and analysis features'. Below it, a paragraph explains that security and analysis features help keep the repository secure and updated by granting permission for read-only analysis. Three features are listed with 'Disable' buttons: 'Dependency graph' (understood to be always enabled for public repos), 'Dependabot alerts' (receive alerts of new vulnerabilities), and 'Dependabot security updates' (easily upgrade to non-vulnerable dependencies).

Options

Manage access

Security & analysis

Branches

Webhooks

Notifications

Integrations

Deploy keys

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

GitHub Advanced Security – Enterprise Cloud

Options

Manage access

Security & analysis

Branches

Webhooks

Notifications

Integrations

Deploy keys

Autolink references

Actions

Environments

Secrets

Pages

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.

Disable

Dependabot alerts

Receive alerts of new vulnerabilities that affect your dependencies.

Disable

Dependabot security updates

Easily upgrade to non-vulnerable dependencies.

Disable

GitHub Advanced Security

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

Go to code scanning

Disable

Code scanning

Automatically detect common vulnerability and coding errors.

Secret scanning

Receive alerts when secrets or keys are checked in.

Access to alerts

Dependabot and secret scanning alerts are only visible to people and teams that are given access by admins. These users will 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

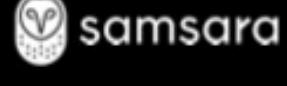
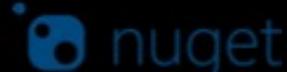
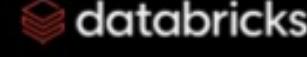
Organization and repository administrators

These members always see Dependabot and secret scanning alerts.

Secret Scanning

Partners

Secret Scanning partners



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

Secret Scanning

Email Notification

Disabled Public API Key ➔

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

11:10 AM (0 minutes ago)



Hey Joshua --

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

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

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

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

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

Thanks,

-- The Mailchimp API Team

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

Secret Scanning

Mailchimp integration – Rolled Secret

Your API keys

API keys provide full access to your Mailchimp account, so keep them safe. [Tips on keeping API keys secure.](#)

Created	User	Label	API key	QR Code	Status
May 10, 2021 12:07 pm Disabled on 05/10/2021	Joshua Johanning (owner)	Posted in public, do not enable	eee82088dde8d20f5a165f533e4e726e-us1		<input type="checkbox"/>

[Create A Key](#)

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

Secret Scanning

GitHub Enterprise Cloud – Secret Scanning Alerts

The screenshot shows the GitHub Enterprise Cloud interface with the 'Secret scanning' tab selected in the navigation bar. On the left, a sidebar lists various security-related sections, with 'Secret scanning alerts' highlighted and a white border around it. The main content area displays a single alert for a 'Doppler Personal Token' found in 'appsettings.json#L10'. The alert was detected on Jan 5. The code snippet shows lines 9, 10, and 11 of the JSON file. To the right of the alert, there is a dropdown menu with options: Open (disabled), Revoked (selected and highlighted in blue), False positive, Used in tests, and Won't fix.

Code Issues Pull requests Actions Projects Wiki Security 1 Insights Settings

Overview

Security policy

Security advisories 0

Dependabot alerts

Code scanning alerts

Secret scanning alerts 1

Secret scanning

1 selected

 **Doppler Personal Token**
appsettings.json#L10 • Detected on Jan 5

```
9     {"value": "Close", "onclick": "CloseDoc()"}  
10    {"value": "Doppler", "onclick": "dp.pt.howInPzsd8wbx9kC7SkItjq1VSRCU47Z5MHyfTdQ"}  
11 ]
```

Mark as ▾

Open

Revoked

False positive

Used in tests

Won't fix

Secret Scanning

GitHub Enterprise Cloud – Custom Patterns!

Secret scanning

Receive alerts when secrets or keys are checked in.

Custom patterns

There are no custom patterns in this repository

 Add a secret scanning custom pattern

Security & analysis / New custom pattern

Custom pattern name

test

Secret format

The pattern for the secret, specified as a regular expression. [Learn more.](#)

`octocat_token_[a-zA-Z0-9]{15}`

More options ▾

Test string - 1 match

`octocat_token_1234567890abcde`

not a token

Code Scanning

CodeQL

CodeQL analysis consists of three steps:

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

Code Scanning

Open Alerts

The screenshot shows the GitHub interface for a repository named 'emo'. The top navigation bar includes 'Pull requests' (7), 'Actions', 'Projects', 'Wiki', a highlighted 'Security' tab with 30 alerts, 'Insights', and 'Settings'. A sidebar on the left lists 'Overview', 'Security policy', 'Security advisories' (0), 'Dependabot alerts' (17), and 'Code scanning alerts' (13, which is selected). The main content area is titled 'Code scanning' and displays a summary: 'Last scanned PR #7 33 minutes ago' and '13 alerts found >'. Below this is a search bar with filters set to 'is:open'. A table lists the first seven alerts:

Alert Type	Description	File	Line	Tool	Rule	Branch	Severity	Sort
Disabled Spring CSRF protection	...e-service/src/main/java/com/github/advancedsecurity/storageservice/WebSecurityConfig.java#L46	...e-service/src/main/java/com/github/advancedsecurity/storageservice/WebSecurityConfig.java	L46	CodeQL		main	Medium	
Deserialization of user-controlled data	.../src/main/java/com/github/advancedsecurity/storageservice/controllers/BlobController.java#L45	.../src/main/java/com/github/advancedsecurity/storageservice/controllers/BlobController.java	L45	CodeQL		main	Medium	
Clear-text logging of sensitive information	gallery-service/main.go#L663	gallery-service/main.go	L663	CodeQL		main	Medium	
Clear-text logging of sensitive information	gallery-service/main.go#L644	gallery-service/main.go	L644	CodeQL		main	Medium	
Database query built from user-controlled sources	gallery-service/main.go#L200	gallery-service/main.go	L200	CodeQL		main	Medium	
Client-side cross-site scripting	frontend/src/components/Login.vue#L5	frontend/src/components/Login.vue	L5	CodeQL		main	Medium	
Missing JWT signature method validation	gallery-service/main.go#L645	gallery-service/main.go	L645	CodeQL		main	Medium	

Code Scanning

Example Alert

Clear-text logging of sensitive information

Logging sensitive information without encryption or hashing can expose it to an attacker.

[Open](#) [Error](#) [CWE-312](#) [CWE-315](#) [CWE-359](#) [security](#)

Branch: main [Dismiss](#)

gallery-service/main.go

```
660
661
662     if claims, ok := token.Claims.(*OctoClaims); ok && token.Valid {
663         log.Printf("AuthN: Received valid token %s", authz)
664
665         log.Printf("AuthN: Adding %s %s", GitHubLoginHeader, claims.Profile.Login)
666         r.Header.Add(GitHubLoginHeader.String(), claims.Profile.Login)
```

Sensitive data returned by HTTP request headers is logged here.

CodeQL [Show paths](#)

Tool	Rule ID	Query
CodeQL	go/clear-text-logging	View source

Sensitive information that is logged unencrypted is accessible to an attacker who gains access to the logs.

Show more ▾

First appeared in commit 7b68985 44 minutes ago

Update codeql-analysis.yml

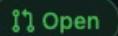
gallery-service/main.go#L663 on branch main

Verified ✓ 7b68985

Code Scanning

Pull Request

Create vulnerable-code.js #8

 Open

soccerjoshj07 wants to merge 1 commit into `main` from `vulnerable-code` 

 Conversation 0

 Commits 1

 Checks 5

 Files changed 1



soccerjoshj07 commented 11 minutes ago

Owner  Tip ...

No description provided.

 Create vulnerable-code.js

 c3d9d3d

Add more commits by pushing to the `vulnerable-code` branch on [soccerjoshj07/ghas-demo](#).



 Some checks were not successful

4 successful and 1 failing checks

[Hide all checks](#)

  [CodeQL / Analyze \(go\) \(pull_request\)](#) Successful in 2m [Details](#)

  [CodeQL / Analyze \(java\) \(pull_request\)](#) Successful in 2m [Details](#)

  [CodeQL / Analyze \(javascript\) \(pull_request\)](#) Successful in 2m [Details](#)

  [CodeQL / Analyze \(python\) \(pull_request\)](#) Successful in 5m [Details](#)

  [Code scanning results / CodeQL](#) Failing after 2s — 1 new error, 1 new note [Required](#) [Details](#)

 **Required statuses must pass before merging**

All required [statuses](#) and check runs on this pull request must run successfully to enable automatic merging.

Dependabot – Security Alerts

Supported package ecosystems

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

Dependabot – Security Alerts

Open Alerts

The screenshot shows the GitHub interface for Dependabot alerts. The top navigation bar includes 'Pull requests 7', 'Actions', 'Projects', 'Wiki', 'Security 30' (which is highlighted), 'Insights', and 'Settings'. On the left, a sidebar lists 'Overview', 'Security policy', 'Security advisories 0', 'Dependabot alerts 17' (which is selected), and 'Code scanning alerts 13'. The main content area is titled 'Dependabot alerts' and contains a message: 'We are changing how you subscribe to Dependabot alerts. Learn more at github.com/watching'. Below this, it shows '17 Open' alerts, '0 Closed', and buttons for 'Manifest ▾' and 'Sort ▾'. The alerts are listed as follows:

- hosted-git-info** (moderate severity): 1 hour ago by GitHub, frontend/package-lock.json, #4
- postcss** (moderate severity): 1 hour ago by GitHub, frontend/package-lock.json
- ssri** (high severity): 1 hour ago by GitHub, frontend/package-lock.json, #7
- lodash** (high severity): 1 hour ago by GitHub, frontend/package-lock.json, #1
- url-parse** (high severity): 1 hour ago by GitHub, frontend/package-lock.json, #3

Dependabot – Security Alerts

Remediation

Dismiss ▾

lodash

⚠️ Open GitHub opened this alert 1 hour ago

⚠️ **Bump lodash from 4.17.20 to 4.17.21 in /frontend** ✓ dependencies

#1 opened 1 hour ago by dependabot bot

1 lodash vulnerability found in frontend/package-lock.json 1 hour ago

Remediation

Upgrade lodash to version 4.17.21 or later. For example:

```
"dependencies": {  
  "lodash": ">=4.17.21"  
}  
  
or...  
  
"devDependencies": {  
  "lodash": ">=4.17.21"  
}
```

Always verify the validity and compatibility of suggestions with your codebase.

Details

CVE-2021-23337 high severity

Vulnerable versions: < 4.17.21
Patched version: 4.17.21

lodash versions prior to 4.17.21 are vulnerable to Command Injection via the template function.

Dependabot – Security Updates

Pull Request

The screenshot shows a GitHub Pull Request page for a repository. The title of the pull request is "Bump lodash from 4.17.20 to 4.17.21 in /frontend #1". A green button labeled "Open" is visible. A prominent message box states: "This automated pull request fixes a **security vulnerability**". It includes a link to learn more about Dependabot security updates, opt out, or give feedback. The message is marked as "high severity".

The pull request has 0 conversations, 1 commit, 5 checks, and 1 file changed. The commit summary is "Bumps lodash from 4.17.20 to 4.17.21." The commit is 95% compatible. Dependabot will resolve any conflicts if altered manually by commenting "@dependabot rebase".

On the right side, there are sections for Reviewers, Assignees, Labels, Projects, Milestone, and Linked issues. The "Labels" section shows a "dependencies" label. The "Projects" section indicates "None yet". The "Milestone" section indicates "No milestone". The "Linked issues" section is currently empty.

At the bottom, a message from dependabot adds the "dependencies" label 1 hour ago. The pull request was verified 207d193 ago.

Dependabot – Security Updates

Pull Request – Introducing a vulnerable package version

The screenshot shows a GitHub pull request page for a repository named "07/zero-to-hero-codeql-test". The pull request is titled "adding axios #14" and is open, with 9 commits. The "Security" tab is active, showing 20 vulnerabilities. A red arrow points to the "Review changes" button, which is highlighted in green. Below the commit list, a specific dependency update for "axios" is circled in red, showing it was updated from version 0.18.0 to 0.21.1. A callout bubble over this section says "Display the rich diff".

Issues Pull requests 9 Actions Projects Wiki Security 20 Insights Settings

adding axios #14

Open soccerjosh07 wants to merge 1 commit into main from adding-axios

Conversation 0 Commits 1 Checks 2 Files changed 1

Changes from all commits ▾ File filter ▾ Jump to ▾

0 / 1 files viewed Review changes

1 package.json

axios 0.18.0 released 3 years ago

Server-Side Request Forgery in Axios (GHSA-4w2v-q235-vp99)
high severity Patched version: 0.21.1

Denial of Service in axios (GHSA-42xw-2xvc-qx8m)
moderate severity Patched version: 0.18.1

Give feedback on dependency review Beta

Display the rich diff

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

Dependabot – Dependency Graph

The screenshot shows the Dependabot interface on a GitHub repository page. The top navigation bar includes links for Pull requests (7), Actions, Projects, Wiki, Security (30), Insights (selected), and Settings.

The left sidebar menu lists Pulse, Contributors, Community, Traffic, Commits, Code frequency, Dependency graph (selected), Network, and Forks.

The main content area is titled "Dependency graph". It features three tabs: Dependencies (selected), Dependents, and Dependabot.

A prominent alert message states: "⚠ We found potential security vulnerabilities in your dependencies. Dependencies defined in these manifest files have known security vulnerabilities and should be updated: authn-service/requirements.txt 10 vulnerabilities found frontend/package-lock.json 12 vulnerabilities found". A "View Dependabot alerts" button is available.

Text below the alert says: "Only the owner of this repository can see this message."

Below the alert, a note states: "These dependencies are defined in ghas-demo's manifest files, such as [frontend/package-lock.json](#), [frontend/package.json](#), and [authn-service/requirements.txt](#)".

The "Dependencies defined in frontend/package-lock.json 1,009" section lists the following dependencies:

- axios / axios: Known security vulnerability in 0.18.0
- indutny / elliptic: Known security vulnerability in 6.5.3
- highlightjs / highlight.js: Known security vulnerability in 9.18.3
- petkaantonov / bluebird: ^ 3.5.5
- acornjs / acorn: ^ 6.0.2
- acornjs / acorn-walk: ^ 6.1.0

Dependabot – Dependency Updates

Supported Manifests

Bundler

Cargo

Composer

Docker

Hex

elm-package

git submodule

GitHub Actions

Go modules

Gradle

Maven

npm

NuGet

pip

pipenv

pip-compile

poetry

Terraform

yarn

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

Dependabot – Dependency Updates

Packages that need to be updated – not necessarily security vulnerabilities

- ↑↑ pip: bump chardet from 3.0.4 to 4.0.0 in /authn-service ✓ triage-required**
#15 opened 37 minutes ago by dependabot [bot](#)
- ↑↑ pip: bump six from 1.12.0 to 1.16.0 in /authn-service ✓ triage-required**
#14 opened 37 minutes ago by dependabot [bot](#)
- ↑↑ pip: bump keyrings-alt from 3.1.1 to 4.0.2 in /authn-service ✓ triage-required**
#13 opened 37 minutes ago by dependabot [bot](#)
- ↑↑ pip: bump pygobject from 3.30.4 to 3.40.1 in /authn-service ✓ triage-required**
#12 opened 37 minutes ago by dependabot [bot](#)
- ↑↑ pip: bump python-dotenv from 0.15.0 to 0.17.1 in /authn-service ✓ triage-required**
#11 opened 37 minutes ago by dependabot [bot](#)

GitHub – Dependency Vulnerabilities shown in local Git output

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

GitHub – Advisory Database

The screenshot shows the GitHub Advisory Database homepage. At the top center is a blue icon of a document with a lock and the text "GitHub Advisory Database". Below the icon is a search bar with the placeholder "Search by CVE/GHSA ID, package, severity, ecosystem, credit...". To the left of the search bar, it says "3,799 advisories". To the right are dropdown menus for "Ecosystem", "Severity", "CWE", and "Sort". The main content area displays a list of seven recent vulnerabilities:

- Command injection in get-git-data**
CVE-2020-7619 (High severity) was published 6 hours ago • [get-git-data \(npm\)](#)
- Prototype Pollution in tiny-conf**
CVE-2020-7724 (Critical severity) was published 6 hours ago • [tiny-conf \(npm\)](#)
- Command Injection in geojson2kml**
CVE-2020-28429 (Critical severity) was published 6 hours ago • [geojson2kml \(npm\)](#)
- Incorrect Authorization in Spring Cloud Netflix Zuul**
CVE-2021-22113 (Moderate severity) was published 6 hours ago • [org.springframework.cloud:spring-cloud-netflix-zuul \(Maven\)](#)
- Injection in pomelo-monitor**
CVE-2020-7620 (High severity) was published 3 hours ago • [pomelo-monitor \(npm\)](#)
- Cross-site Scripting in quill**
CVE-2021-3163 (Moderate severity) was published 6 hours ago • [quill \(npm\)](#)

GitHub Advanced Security – Feature Compare

Feature	GitHub Enterprise (Cloud)	GitHub Enterprise (Cloud) w/ GitHub Advanced Security	Public Repos
Dependency Graph	X	X	X
Dependency Review in Pull Request (beta)		X	X
GHAS Code Scanning		X	X
GitHub Security Advisories	X	X	X
Dependabot Alerts / Security Updates	X	X	X
Security Policies	X	X	X
Secret Scanning		X	X (note that you won't see a secret scanning menu, you will just get an email when a secret was committed to the repo and the secret will likely be rolled)
Secret Scanning - Custom Patterns		X	

Questions?