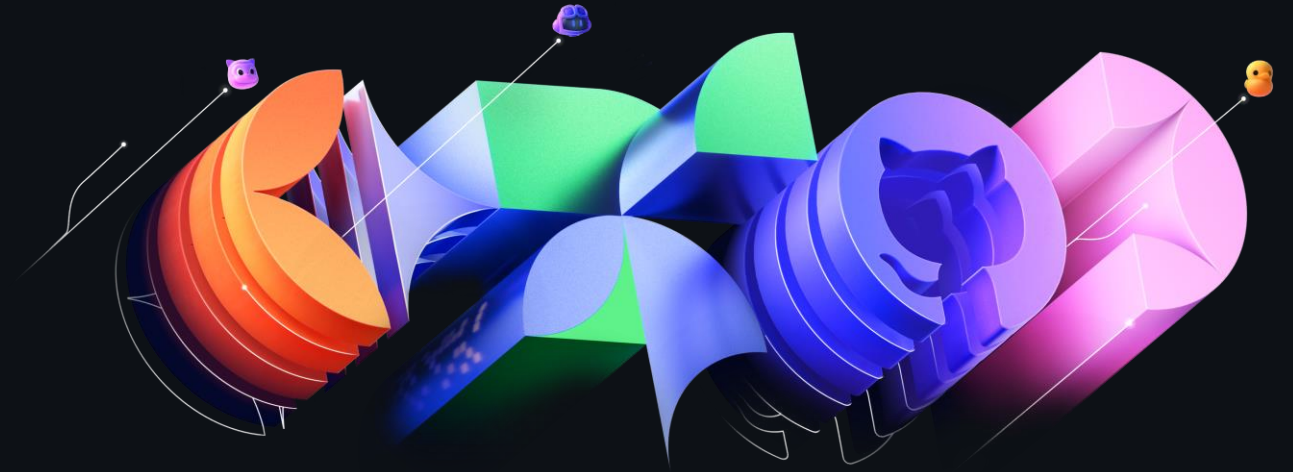


UNIVERSE'24



脆弱性、お前はすでに修正されている...
AIでコードをセキキュアに☒



Kenta Nakase / @parroty
Senior Solutions Engineer, GitHub

Octoverse 2024 Report

(<https://github.blog/news-insights/octoverse/octoverse-2024/>)



The image shows a browser window with a dark theme. The address bar contains the URL <https://github.blog/news-insights/octoverse/octoverse-2024/>. The main content area features the following text:

Octoverse: AI leads Python to top language as the number of global developers surges

In this year's Octoverse report, we study how public and open source activity on GitHub shows how AI is expanding as the global developer community surges in size.



The graphic consists of several glowing lines in shades of blue, green, and orange, with small circular nodes at their ends. The lines are set against a dark blue background with a subtle grid pattern. The overall aesthetic is futuristic and tech-oriented.

 Octoverse 2024

Octoverse 2024 Report

(<https://github.blog/news-insights/octoverse/octoverse-2024/>)

In 2024, developers across GitHub used secret scanning to detect more than 39 million secret leaks. We also saw developers and open-source communities respond more quickly to security incidents through new generative AI security tools, automated alerts, and proactive measures. This isn't just helping make software more secure—it's leading to faster fixes, too.

The most common security vulnerabilities in 2024. Injection, an admittedly large category of security issues, was the most common type of vulnerability found across public and private repositories via CodeQL, a code analysis engine developed by GitHub to automate security checks. Meanwhile, Security Logging and Monitoring Failures vulnerabilities were found more often in private repositories.

3900万以上のシークレット検知
A global community of developers that's growing fast
The state of open source

The state of generative AI in 2024

The state of security and automation in 2024
The rise of AI-powered languages
The state of the open source ecosystem

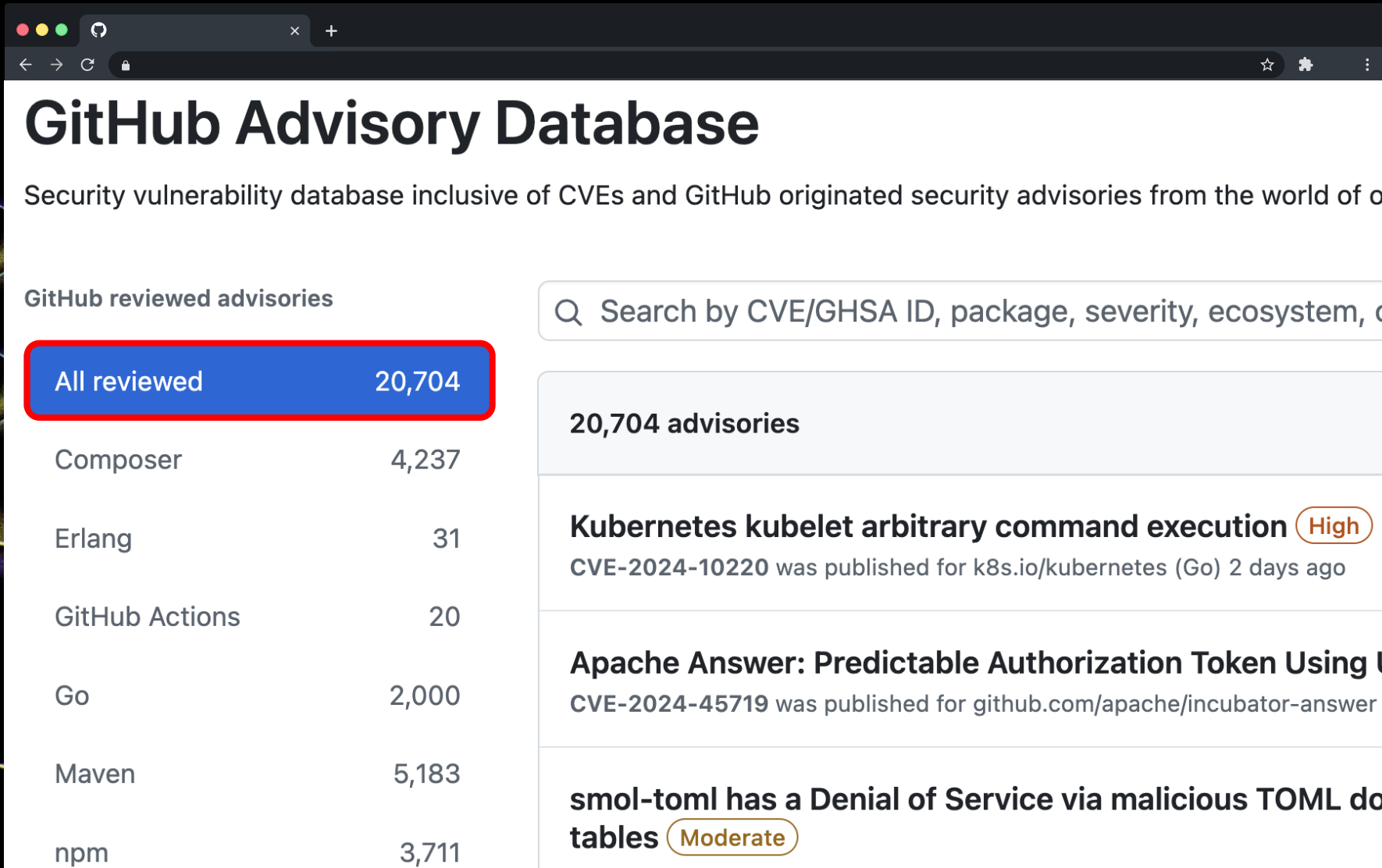
Injectionの脆弱性がトップ

Most common types of vulnerabilities found by CodeQL in 2024

Vulnerability Type	Frequency
Injection	High
Broken access control	Medium

GitHub Advisory Database

(<https://github.com/advisories>)



Security vulnerability database inclusive of CVEs and GitHub originated security advisories from the world of open source

GitHub reviewed advisories

Search by CVE/GHSA ID, package, severity, ecosystem, or ecosystem

All reviewed	20,704
Composer	4,237
Erlang	31
GitHub Actions	20
Go	2,000
Maven	5,183
npm	3,711

20,704 advisories

Kubernetes kubelet arbitrary command execution High
CVE-2024-10220 was published for k8s.io/kubernetes (Go) 2 days ago

Apache Answer: Predictable Authorization Token Using U
CVE-2024-45719 was published for github.com/apache/incubator-answer (Go) 2 days ago

smol-toml has a Denial of Service via malicious TOML do
tables Moderate



アプリケーションセキュリティの現状

セキュリティリスク

アプリケーションに含まれる脆弱性が一番の攻撃対象

80%の情報漏洩は、ウェブアプリケーションの脆弱性を悪用した攻撃によって発生

Source: [Verizon Data Breach Investigations Reports 2023](#)

停滞するプロセス

検出された脆弱性の87%は9ヶ月後も修復されずに存在

脆弱性のうち、発見され修正されるものは最初の271日間でわずか13%に過ぎない

Source: [Mend Open Source Risk Report 2022](#)

効率を高める手段

AIを活用したセキュリティツールへの期待

84%のエグゼクティブが、生成AIを活用したセキュリティソリューションを優先

Source: [IBM CEO's Guide to Generative AI, 2023](#)



検出するだけでは
十分ではない

組織には、検出したものの
まだ修復できていない
脆弱性がバツタログに
何千もある。

```
Step 3 jsonProjection
Step 2 jsonQuery
Step 1 req.query.query Source

lib/routes/collection.js
34 var key = req.query.key;
35 var value = req.query.value;
36 var type = req.query.type && req.query.type.toUpperCase();
37 var jsonQuery = req.query.query;
38
39 if (key && value) {
40 // if it is a simple query,
```



Found means fixed

GitHub Advanced SecurityはCopilotの技術を活用して、コード解析によって検出された脆弱性に対して、**修正の提案**を作成し、脆弱性の解消を促進



リスクの低減

- 既存の脆弱性に対してキャンペーンを設定し、優先する対象を明確化
- セキュリティ負債を減らし脆弱性が悪用される可能性を低減

開発者の生産性の確保

- 開発フローに自然に統合された形で脆弱性の説明と修正提案を提示。開発者のスキル向上にも効果的
- 開発スピードを犠牲にすることなくリスクを低減

セキュリティと開発の調和

- セキュリティチームの要件を満たすと同時に、開発者の革新とスピードをサポート
- セキュリティ負債の増加を抑制し、新たなリスクを削減する

GitHub Advanced Security

Dependabot

脆弱性を含んだ古い依存ライブラリを自動的に更新

Code Scanning

アプリケーションに含まれる脆弱性を検出・修正

Secret Scanning

ハードコードされたシークレットの検出・管理

Security Overview

セキュリティ機能のアラートをダッシュボードで集約

Dependabot

脆弱性を含んだ古い依存
ライブラリを自動的に更新

- 問題点検知の簡略化
- 更新作業の効率化



Dependabot Security Updates

The screenshot shows a GitHub interface with a navigation bar at the top containing 'Code', 'Issues 2', 'Pull requests 7', 'Actions', 'Projects', 'Wiki', 'Security 19', and 'Insights'. Below the navigation bar, the page title is 'Dependabot alerts / #7'. The main heading is 'semver vulnerable to Regular Expression Denial of Service #7'. A 'Dismiss alert' button is in the top right. A green 'Open' button with a shield icon is on the left, followed by the text 'Opened last year on semver (npm) · yarn.lock'. A pull request card is shown with the title 'Bump semver from 5.7.1 to 5.7.2' and a 'Review security update' button. Below this is a table with columns 'Package', 'Affected versions', and 'Patched version'. The table shows 'semver (npm)' with affected versions '< 5.7.2' and patched version '5.7.2'. A descriptive paragraph follows, stating that versions of semver before 7.5.2 on the 7.x branch, before 6.3.1 on the 6.x branch, and all other versions before 5.7.2 are vulnerable to Regular Expression Denial of Service (ReDoS) via the function new Range, when untrusted user data is provided as a range. On the right side, there is a 'Severity' section showing 'High' (7.5 / 10) and a 'CVSS v3 base metrics' table with the following data: Attack vector: Network, Attack complexity: Low, Privileges required: None, User interaction: None, Scope: Unchanged, Confidentiality: None, Integrity: None, Availability: High.

Code Issues 2 Pull requests 7 Actions Projects Wiki Security 19 Insights

Dependabot alerts / #7

semver vulnerable to Regular Expression Denial of Service #7

Dismiss alert

Open Opened last year on semver (npm) · yarn.lock

Bump semver from 5.7.1 to 5.7.2 [Review security update](#)

Merging this pull request would fix 2 Dependabot alerts on semver in yarn.lock.

Package	Affected versions	Patched version
semver (npm)	<u>< 5.7.2</u>	<u>5.7.2</u>

Versions of the package semver before 7.5.2 on the 7.x branch, before 6.3.1 on the 6.x branch, and all other versions before 5.7.2 are vulnerable to Regular Expression Denial of Service (ReDoS) via the function new Range, when untrusted user data is provided as a range

Severity **High** 7.5 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	High

Dependency Graph

The screenshot shows a web browser window with a navigation bar at the top containing links for Code, Issues (3), Pull requests (9), Actions, Projects, Wiki, and Security (14). On the left side, there is a sidebar menu with options: Pulse, Contributors, Community, Traffic, Commits, Code frequency, **Dependency graph** (highlighted), Network, Forks, Actions Usage Metrics, and Actions Performance Metrics. The main content area is titled "Dependency graph" and has two tabs: "Dependencies" and "Dependabot". An "Export SBOM" button is visible in the top right of the main area. A search bar contains the text "express". Below the search bar, a summary shows "7 Total" dependencies. The first dependency listed is "@types/express ^ 4.17.21", which is underlined in red. Below it is "express ^ 4.19.2", and at the bottom is "express-openid-connect 2.7.2".

Code Issues 3 Pull requests 9 Actions Projects Wiki Security 14

Pulse

Contributors

Community

Traffic

Commits

Code frequency

Dependency graph

Network

Forks

Actions Usage Metrics

Actions Performance Metrics

Dependency graph

Dependencies Dependabot [Export SBOM](#)

Search: express

7 Total

@types/express ^ 4.17.21
npm · package.json · Detected automatically on Nov 23, 2024

express ^ 4.19.2
npm · package.json · Detected automatically on Nov 23, 2024

express-openid-connect 2.7.2
npm · package.json · Detected automatically on Nov 23, 2024 · MIT

Dependabot Version Updates (with Group)

The screenshot shows a GitHub pull request titled "Bump the npm_and_yarn group with 4 updates #291". The pull request is open and originates from a branch named "dependabot/npm_and_yarn/npm_and_yarn-bef8bfe7f" on the "main" branch. The navigation bar at the top shows "Pull requests" with a count of 9. Below the title, there are tabs for "Conversation" (1), "Commits" (1), "Checks" (6), and "Files changed" (2). A comment from the "dependabot" bot, posted on Sep 24, is highlighted with a red box. The comment text is: "Bumps the npm_and_yarn group with 4 updates: [express](#), [body-parser](#), [path-to-regexp](#) and [serve-static](#)." Below the comment, it lists the updates: "Updates `express` from 4.19.2 to 4.20.0". There are also expandable sections for "Release notes", "Changelog", and "Commits".

Code Issues 3 Pull requests 9 Actions Projects Wiki Security 14

Bump the npm_and_yarn group with 4 updates #291

Open dependabot wants to merge 1 commit into main from dependabot/npm_and_yarn/npm_and_yarn-bef8bfe7f

Conversation 1 Commits 1 Checks 6 Files changed 2

dependabot bot commented on behalf of github on Sep 24 • edited

Bumps the npm_and_yarn group with 4 updates: [express](#), [body-parser](#), [path-to-regexp](#) and [serve-static](#).

Updates `express` from 4.19.2 to 4.20.0

- ▶ Release notes
- ▶ Changelog
- ▶ Commits

Pull Request Checks - with Dependency Review

The screenshot shows a GitHub pull request interface. At the top, the title is "Bump the npm_and_yarn group with 4 updates #291" and the description says "dependabot wants to merge 1 commit into main from dependabot/npm_and_yarn...". Below the title, a green box indicates "All checks have passed" with "8 successful checks" and a "Hide all checks" link. A list of checks follows, each with a green checkmark, a GitHub logo, a name, a status, and a "Details" link. The "Dependency Review / dependency-review (pull_request)" check is highlighted with a red underline. Below the list, a green box states "This branch has no conflicts with the base branch" and "Merging can be performed automatically." At the bottom left, there is a green "Merge pull request" button. On the right side, there are sections for "Labels" (None yet), "Projects" (None yet), "Milestone" (No milestone), "Development" (Successfully merging this pull request may close these issues.), and "Notifications" (Unsubscribe button).

pen Bump the npm_and_yarn group with 4 updates #291
dependabot wants to merge 1 commit into `main` from `dependabot/npm_and_yarn...`

All checks have passed [Hide all checks](#)
8 successful checks

- ✓ CodeQL / Analyze (pull_request) Successful in 1m [Details](#)
- ✓ Dependency Review / dependency-review (pull_request) S... [Details](#)
- ✓ ESLint / Run eslint scanning (pull_request) Successful in 39s [Details](#)
- ✓ End to End Tests (Playwright) / test (pull_request) Success... [Details](#)
- ✓ Unit Tests (Jest) / test (pull_request) Successful in 34s [Details](#)
- ✓ Unit Tests (Jest) / test (push) Successful in 26s [Details](#)

This branch has no conflicts with the base branch
Merging can be performed automatically.

[Merge pull request](#)

Labels
None yet

Projects
None yet

Milestone
No milestone

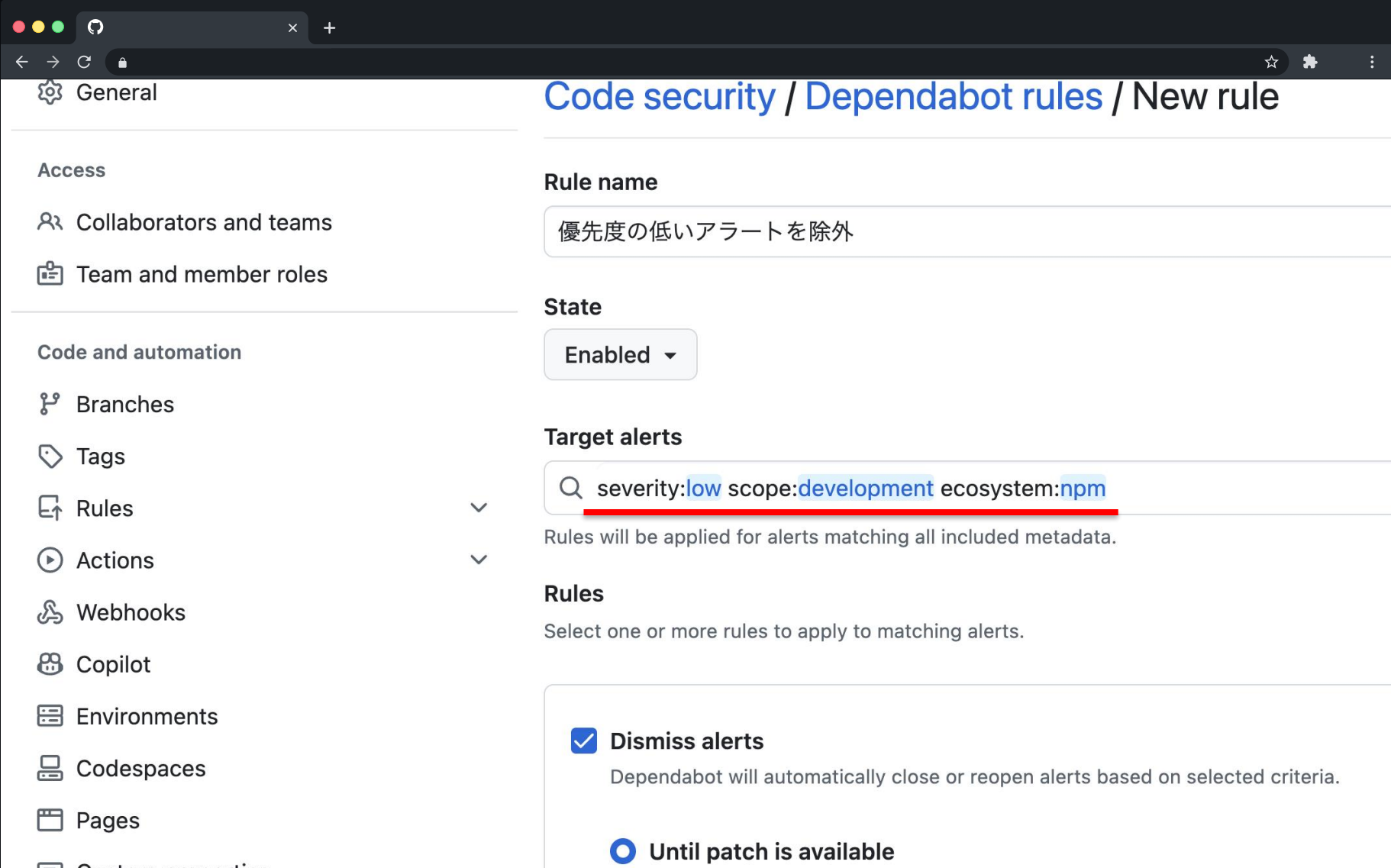
Development
Successfully merging this pull request may close these issues.

None yet

Notifications Cus
[Unsubscribe](#)

You're receiving notifications because you are...

Dependabot Rules (Custom Auto Triage Rule)



Copilot Autofix for Dependabot

The screenshot shows a GitHub pull request interface. At the top, there's a navigation bar with tabs for Code, Issues, Pull requests (1), Actions, Projects, Wiki, Security (7), and Insights. The main title of the pull request is "Bump lodash and @types/lodash #23". Below the title, it says "dependabot wants to merge 1 commit into main from dependabot/npm_and_yarn/multi-a2dacc6af4". There are buttons for "Open", "Edit", and "Code". Below the title, there are statistics: Conversation (1), Commits (1), Checks (2), and Files changed (2). A color-coded progress bar shows +11 and -12 changes. A comment from the dependabot bot is visible, stating it bumped lodash and @types/lodash. The right sidebar shows the "Reviewers" section with a suggestion from landongrindheim and a "Request" button. Below that, it says "Still in progress? Convert to draft". The "Assignees" section shows "No one—assign yourself".



dependabot bot commented on behalf of github 2 weeks ago

Bumps [lodash](#) and [@types/lodash](#). These dependencies needed to be updated together.

Updates `lodash` from 3.10.1 to 4.17.21

- ▶ Release notes
- ▶ Commits
- ▶ Maintainer changes

Reviewers ⚙️

Suggestions

landongrindheim Request

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

Assignees ⚙️

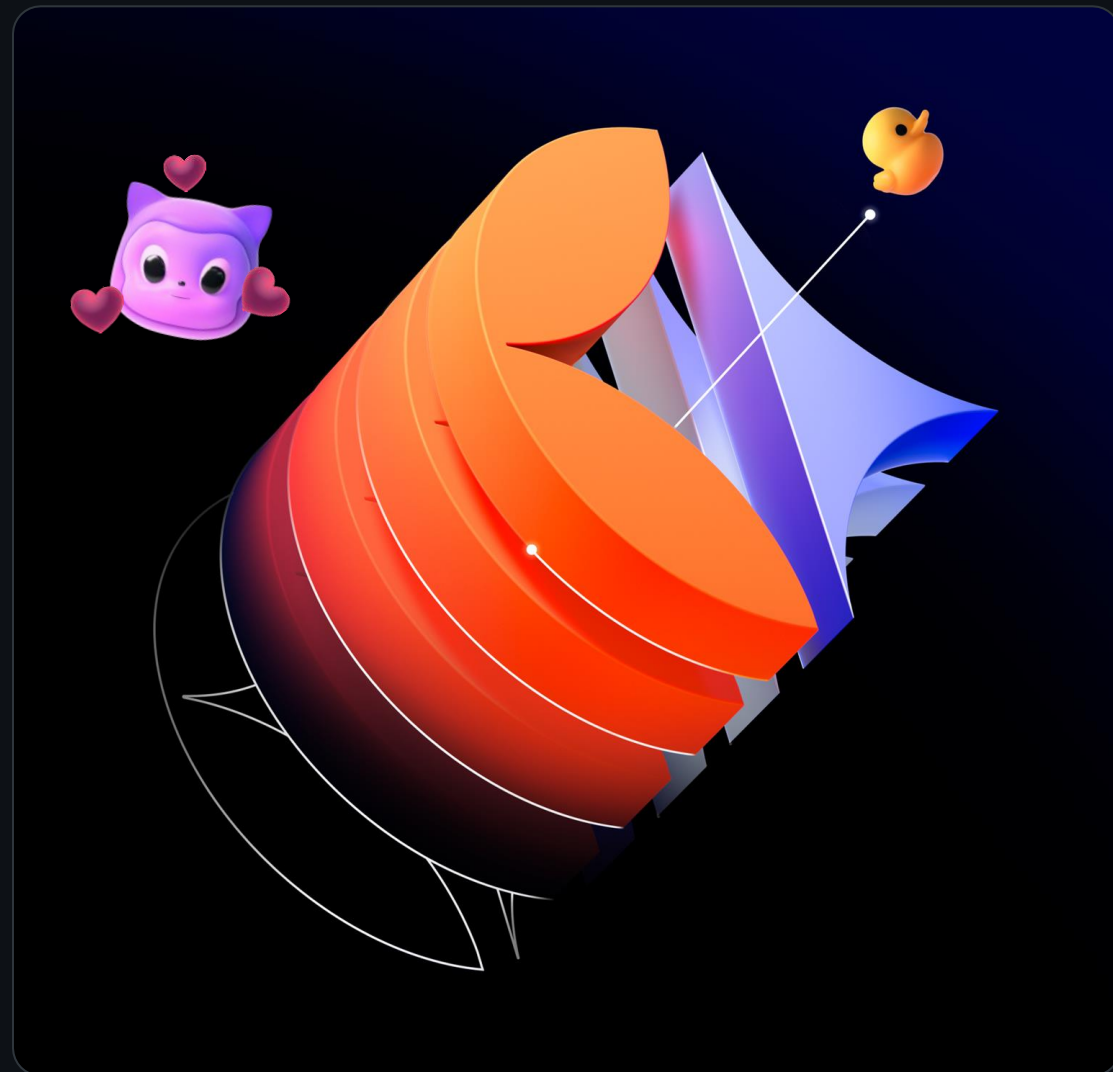
No one—[assign yourself](#)



Code Scanning

アプリケーションに含まれる脆弱性を検出・修正

- 開発ワークフローとの整合性
- 問題点・修正方法の理解支援



Code Scanning Alerts

The screenshot shows a GitHub repository page for 'parrotly-demo / bookstore-demo-javascript'. The 'Security' tab is active, showing 18 alerts. A specific alert is highlighted: 'Reflected cross-site scripting' (Severity: High), located in the 'main' branch on July 2. The alert is marked as 'Open'. A 'Generate fix' button is available, along with a link to 'Copilot Autofix for CodeQL'. The code snippet shows a JavaScript function 'app.get' that uses 'res.send' to output 'Hello \${message}', where the user-provided value is not properly escaped. The affected branches list shows 'main' is impacted. A video player is visible in the bottom right corner.

Code scanning alerts / #11

Reflected cross-site scripting

Dismiss alert ▼ Create issue

Open in main on Jul 2

Speed up the remediation of this alert with [Copilot Autofix for CodeQL](#) Generate fix

src/index.js:30

```
27
28 app.get('/echo/:message', (req, res) => {
29     const message = req.params.message;
30     res.send(`Hello ${message}`)
```

Cross-site scripting vulnerability due to a [user-provided value](#)

Severity: High

Affected branches: main

Security campaigns: No campaign is currently tracking

Copilot Autofix (CodeQL)

The screenshot shows a GitHub Code Scanning alert for a 'Reflected cross-site scripting' vulnerability. The alert is located in the 'main' branch and was detected yesterday. It is categorized as 'High' severity. The code snippet shows a Node.js Express route at 'src/index.js:30' where user input is directly concatenated into an HTML response string. A 'Generate fix' button is available, which is linked to 'Copilot Autofix for CodeQL'. The alert is associated with the 'security' tag and is tracked by the CWE-79 and CWE-116 weaknesses. The description explains that directly writing user input to an HTTP response without sanitization allows for a cross-site scripting vulnerability.

Code scanning alerts / #11

Reflected cross-site scripting

Open in main yesterday

Speed up the remediation of this alert with [Copilot Autofix for CodeQL](#) Generate fix

```
src/index.js:30
27
28 app.get('/echo/:message', (req, res) => {
29     const message = req.params.message;
30     res.send(`Hello ${message}`)
31 });
32
33 app.get('/users', (req, res) => {
```

Cross-site scripting vulnerability due to a user-provided value

CodeQL [Show paths](#)

Tool	Rule ID	Query
CodeQL	js/reflected-xss	View source

Directly writing user input (for example, an HTTP request parameter) to an HTTP response without properly sanitizing the input first, allows for a cross-site scripting vulnerability.

Dismiss alert Create issue

Severity: High

Affected branches: main (2)

Security campaigns: No campaign is currently tracking this alert.

Tags: security

Weaknesses: CWE-79, CWE-116

Copilot Autofix (CodeQL)

Code scanning alerts / #5011

Reflected cross-site scripting

Dismiss alert Create issue

Open in `main` 24 minutes ago

Copilot Autofix AI generated a fix less than a minute ago

To fix the problem, we need to sanitize the user input before incorporating it into the response. This can be achieved by using a library that provides HTML escaping functionality. The `escape-html` library is a good choice for this purpose.

The best way to fix the problem without changing existing functionality is to import the `escape-html` library and use it to escape the `message` parameter before including it in the response. This ensures that any potentially malicious input is rendered harmless by converting special characters to their HTML-escaped equivalents.

src/index.ts:28 Autofix

...	@@ -2,2 +2,3 @@	
2	<code>import { listBooks } from './query-</code>	2 <code>import { listBooks } from './query-</code>
	<code>handler'</code>	<code>handler'</code>
		3 <code>import escapeHtml = require('escape-html')</code>
3		4
...	@@ -26,3 +27,3 @@	
26	<code>app.get('/echo/:message', (req, res) => {</code>	27 <code>app.get('/echo/:message', (req, res) => {</code>
27	<code>const message = req.params.message</code>	28 <code>const message =</code>

Severity: High

Affected branches: main

Security campaigns: No campaign is currently tracking this alert.

Tags: security

Weaknesses: CWE-79, CWE-116



Reading Alerts with Copilot

The screenshot shows a GitHub Code Scanning alert for "Reflected cross-site scripting" in the "main" branch. A Copilot Autofix has been generated. A comment from user "parroty" asks for a Japanese explanation of the alert, which Copilot has provided. The Copilot response includes a summary and recommended mitigation strategies.

Code Scanning Alerts / #11

Reflected cross-site scripting

Open in main yesterday

Copilot Autofix (AI) generated a fix less than a minute ago

To fix the problem, we need to sanitize the user input before i
The best way to do this is by using a library that provides HTM
ensure that any potentially malicious scripts in the user input

We will use the `escape-html` library to escape the user-provi
the response. This change will be made in the `src/index.js`

`src/index.js:30` **Autofix**

```
... @@ -27,4 +27,6 @@  
27
```

反射型クロスサイトスクリプティング

parroty 1 minute ago

このアラートの概要を日本語で解説して

Copilot now

このアラートは「反射型クロスサイトスクリプティング (Reflected Cross-Site Scripting)」に関するものです。

概要:

- ユーザー入力を適切にサニタイズせずにHTTPレスポンスに直接書き込むことで、クロスサイトスクリプティングの脆弱性が発生します。
- この脆弱性により、悪意のあるスクリプトがユーザーのブラウザで実行される可能性があります。

推奨対策:

- ユーザー入力をレスポンスに書き込む前に、コンテキストに応じたエンコードやエスケープ処理を行います。

Copilot Autofix for Partner Tools

The screenshot shows a GitHub pull request interface. At the top, the navigation bar includes 'Code', 'Issues', 'Pull requests' (with a count of 5), 'Actions', 'Projects', 'Wiki', 'Security' (with a count of 13), and 'Insights'. The main heading is 'Update application.js #6', with 'Edit' and '<> Code' buttons to the right. Below the heading, a green 'Open' button is followed by the text 'rvermeulen wants to merge 2 commits into master from rvermeulen-patch-6'. A progress bar shows '+3 -1' changes. The left sidebar has tabs for 'Conversation' (1), 'Commits' (2), 'Checks' (51), and 'Files changed' (2). The main content area shows a comment from 'rvermeulen' on Sep 7 with the text 'No description provided.' and a smiley face emoji. Below the comment, a commit history shows 'rvermeulen added 2 commits 2 months ago'. The commit list includes 'Update application.js' (Verified, 436d2a2) and 'Update .eslintrc.yml' (Verified, c087527). On the right, the 'Reviewers' section shows 'No reviews' and a 'Convert to draft' link. The 'Assignees' section shows 'No one—assign yourself'. The 'Labels' section shows 'None yet'. A play button icon is visible in the bottom right corner.

Secret Scanning

ハードコードされた
シークレットの検出・管理

- 未然の検知・防止
- 検知の網羅性・精度



Secret Scanning Alerts

Overview

Reporting

Policy

Requests

Push protection bypass

Vulnerability alerts

- Dependabot 11
- Code scanning 1
- Secret scanning 6
- Default 6
- Experimental

Secret scanning alerts

is:open

Default Experimental 0

6 Open 2 Closed

Bypassed Validity Secret type Provider Sort

- GitHub Personal Access Token** `github_pat_11AW4L3WY0qP...`
#6 opened on 2022年12月1... • Detected secret in issue #8
- Azure Storage Account Access Key** `4DZa7PkfkI0gB3L7xw+`
#5 opened on 2022年11月2... • Detected secret in src/config.js:10
- Amazon AWS Secret Access Key** `lDjW2nYM85mlvZ7mZK5L/M`
#4 opened on 2022年11月2... • Detected secret in src/config.js:4

Push Protection

The screenshot shows a web browser window displaying the GitHub interface for a repository named 'parroty-demo / bookstore-demo-javascript'. The browser's address bar shows the repository URL. The navigation bar includes tabs for 'Code', 'Issues' (with a count of 2), 'Pull requests' (with a count of 7), 'Actions', 'Projects', 'Wiki', and 'Security' (with a count of 18). The main content area shows the file 'config.yaml' selected in the 'main' branch. There are two buttons: 'Cancel changes' and 'Commit changes...'. Below the file name, there are tabs for 'Edit' and 'Preview', and settings for 'Spaces' (set to 2) and 'No wrap'. The editor area contains a single line of text: '1 Enter file contents here'. A mouse cursor is visible at the bottom right of the editor area.



Custom Secret Patterns

The screenshot shows the GitHub 'Code security & analysis / New custom pattern' page. A red box highlights the 'Generate with AI' button in the top right corner. The page contains several form fields and sections:

- Pattern name ***: A text input field containing the Japanese text '社内用シークレットURL'. Below the field is a warning: 'This cannot be edited after saving.'
- Secret format (specified as a regular expression) ***: A text input field containing the regular expression 'https://secure-[0-9]{10}\.secret-domain\.example\.com'. Below the field is a description: 'The pattern for the secret, specified as a regular expression. [Learn more about defining custom patterns.](#)'
- More options**: A section with a chevron icon and the text '> More options'.
- Test string * - 2 matches**: A section showing a list of test strings with two highlighted matches: 'https://secure-1035142300.secret-domain.example.com' and 'https://secure-1035142399.secret-domain.example.com'. Other strings shown are 'https://insecure-xxx.domain.example.com' and 'https://example.com'.

Custom Secret Patterns

Issues 3 Pull requests 9 Actions Projects

Code security & analysis

Pattern name *

社内用シークレットURL

This cannot be edited after saving.

Secret format (specified as a regular expression)

https://secure-[0-9]{10}\.secret-domain.example.com

The pattern for the secret, specified as a regular expression.

> More options

Test string * - 2 matches

```
https://secure-1035142300.secret-domain.example.com
https://insecure-xxx.domain.example.com
https://secure-1035142399.secret-domain.example.com
https://example.com
```

Generate regular expression [Give feedback](#)

I want a regular expression that *

https://secure + 整数10桁 + secret-domain.example.comのようなパターン

Examples of what I am looking for

```
https://secure-1035142300.secret-domain.example.com
https://secure-1035142399.secret-domain.example.com
```

This AI-powered feature may produce inaccurate results. Double-check the expressions generated and make any necessary adjustments.

Generate suggestions

Results

> https://secure-[0-9]{10}\.secret-dom... [Use result](#)

Copilot Secret Scanning

The screenshot shows a GitHub Secret Scanning alert for a password. The alert is titled "Password" and indicates it was detected 20 days ago. The secret value is "DeliberatelyInsecure1234". The detection is attributed to "Copilot Secret Scanning". The secret was found in the file "src/main/java/com/example/demo/Utility.java". The code snippet shows two lines where the password is assigned to static final variables: "PASSWORD_SALT_SIMPLE" and "PASSWORD_SALT_ADMIN".

Password

Open GitHub detected a secret 20 days ago

Possibly active secret

DeliberatelyInsecure1234

Detected by [Copilot Secret Scanning](#)

Detected in 1 location

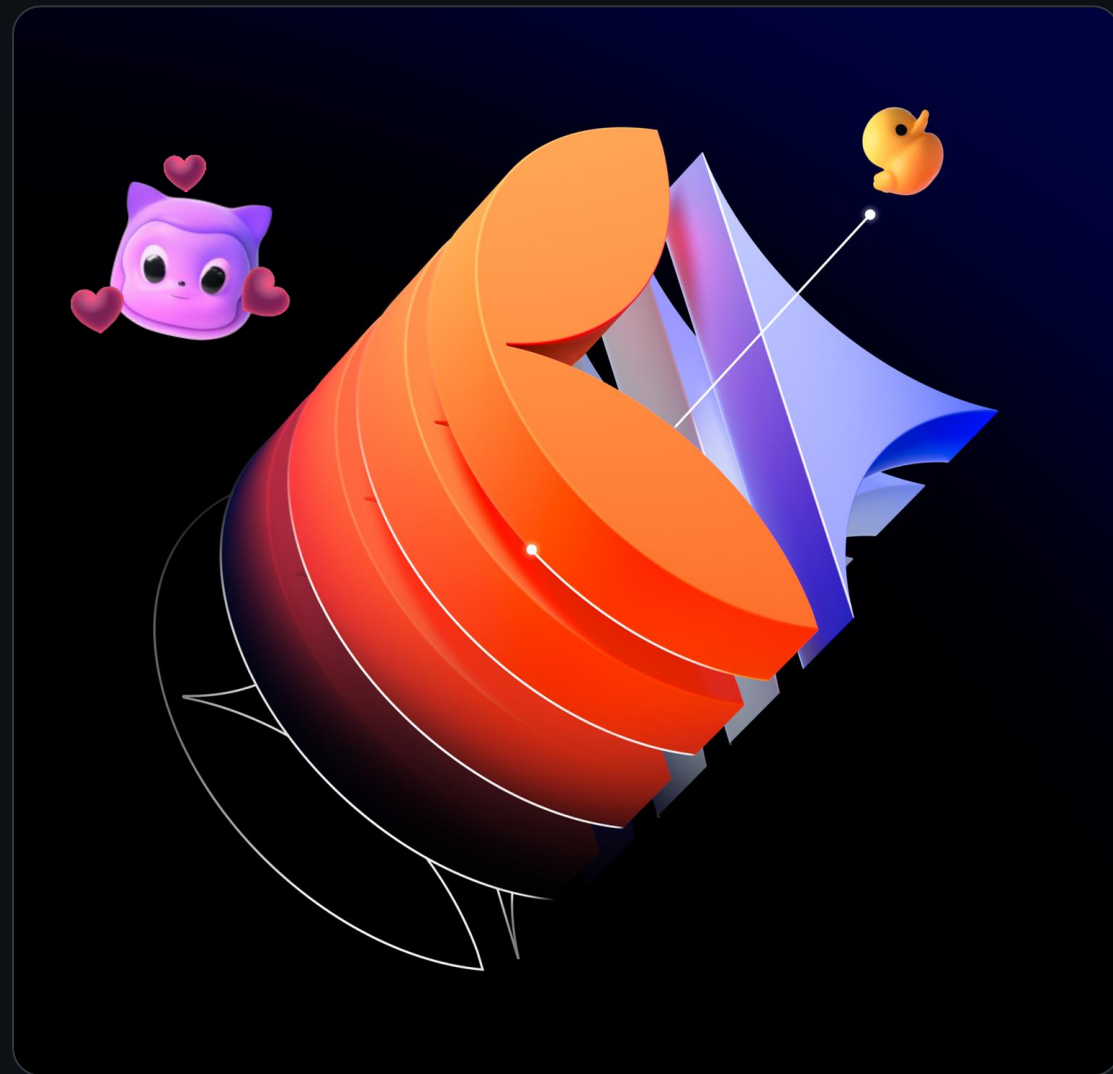
```
src/main/java/com/example/demo/Utility.java
```

```
1 package com.example.demo;
2
3 class Utility {
4     public static final String PASSWORD_SALT_SIMPLE = "DeliberatelyInsecure1234";
5     public static final String PASSWORD_SALT_ADMIN = "DeliberatelyInsecure1235";
```

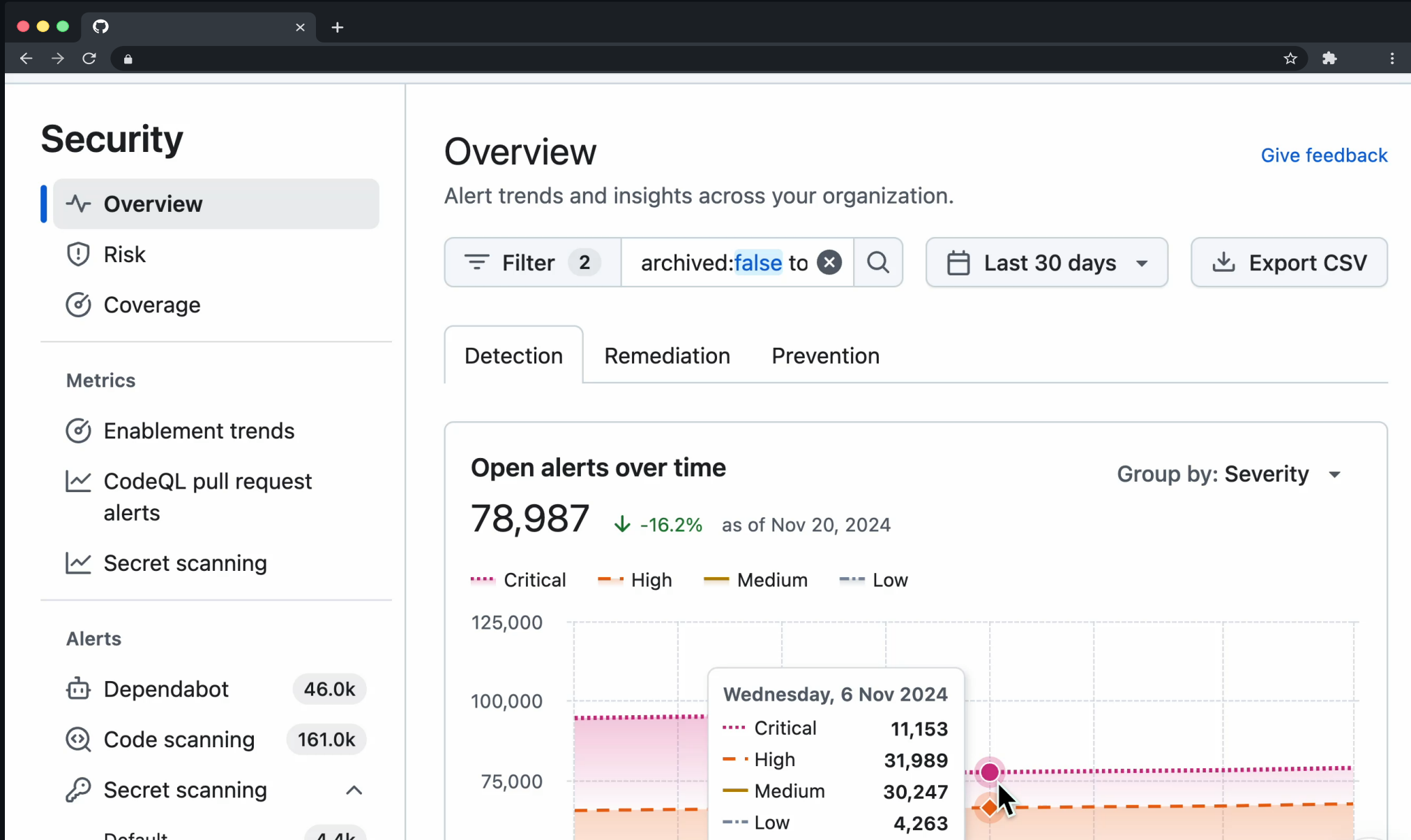
Security Overview

セキュリティ機能のアラートを
ダッシュボードで集約

- 効率的な情報収集
- 重要度判断のための可視化



Security Overview (Summary)



Security Overview (Risk)

Navigation: Overview, Repositories, Discussions, Projects, Packages, Teams, People, **Security**, Insights

Security

- Overview
- Risk**
- Coverage

Metrics

- Enablement trends
- CodeQL pull request alerts
- Secret scanning

Alerts

- Dependabot: 1.4k
- Code scanning: 3.3k
- Secret scanning: 85 (Default), 22 (Experimental)

Security risk

Open alert counts across your organization. [Give feedback](#)

Search: archived:false Teams Export CSV

Dependabot

19% of repositories affected

Repositories: 55 affected, 221 unaffected

Open alerts: 133 critical, 478 moderate, 629 high, 147 low

Code scanning

19% of repositories affected

Repositories: 54 affected, 222 unaffected

Open alerts: 37 critical, 183 medium, 2,849 informational, 185 high, 6 low

Secret scanning

7% of repositories affected

Repositories: 20 affected, 256 unaffected

Open alerts: 85 alerts

276 Active 6 Archived Sort by: Recently updated

Repository	Internal	Dependabot	Code scanning	Secret scanning
bookstore-demo-typescript	Internal	1	3	8
...



Security Overview (CodeQL Alerts)

The screenshot shows the GitHub Security Overview page for CodeQL Alerts. The left sidebar contains navigation links for Overview, Risk, Coverage, Metrics, Enablement trends, CodeQL pull request alerts (selected), and Secret scanning. Below these are alert counts for Dependabot (46.0k), Code scanning (161.0k), Secret scanning (4.4k), and a Default category. The main content area is titled 'CodeQL pull request alerts' and includes a 'Give feedback' link. A description states: 'A report of vulnerabilities prevented by CodeQL, caught in pull requests that have been merged to the default branch'. Below this is a filter bar with 'Filter 1' and 'archived:false', a search icon, a date range of 'Last 90 days', and an 'Export CSV' button. Three summary cards are displayed: 'Alerts found' (10), 'Copilot Autofix suggestions' (9), and 'Alerts fixed' (1). A fourth card for 'Alerts in pull requests' is partially visible at the bottom.

Security

- Overview
- Risk
- Coverage

Metrics

- Enablement trends
- CodeQL pull request alerts**
- Secret scanning

Alerts


- Dependabot 46.0k
- Code scanning 161.0k
- Secret scanning 4.4k
- Default 4.4k

CodeQL pull request alerts [Give feedback](#)

A report of vulnerabilities prevented by CodeQL, caught in pull requests that have been merged to the default branch


Filter 1 archived:false Last 90 days

Alerts found

 10


Total CodeQL alerts created in pull requests merged to the default branch

Copilot Autofix suggestions

 9

90% of pull request alerts have an autofix suggestion

Alerts fixed

 1

10% of alerts detected in pull requests were fixed

Alerts in pull requests



Security Campaigns

Security

- Overview
- Risk
- Coverage

Metrics

- Enablement trends
- CodeQL pull request alerts
- Secret scanning

Alerts

- Dependabot 46.2k
- Code scanning 161.8k
- Secret scanning ^
 - Default 4.4k
 - Experimental 2.4k

Requests

- Push protection bypass

Campaigns +

- Cross-site scripting (CWE-79) 994

Cross-site scripting (CWE-79) managed by heyamie

[Preview](#) [Give feedback](#) ⋮

Remediating Cross-Site Scripting (XSS) vulnerabilities prevents data theft, session hijacking, and unauthorized actions, ensuring regulatory compliance, maintaining application integrity, and enhancing user trust.

Campaign progress

0% (1 alert) 994 alerts left

● 1 closed ● 10 in progress

Campaign started 34 days ago

Status

36 days left

Due date is Tue, Dec 31

Copilot Autofix

995 supported alerts

Copilot Autofix will try to suggest fixes for the supported alerts. Read more about [Copilot Autofix](#).

Filter 1 is:open ✕ 🔍

Open 994
Closed 1
Group by: Repository ▾

>	Abeck_GHAS2	17% closed (6 alerts)
>	AccessGroup-GHAS-demo	0% closed (89 alerts)
>	activemq	0% closed (21 alerts)
>	adrienpessu-juice-shop	0% closed (3 alerts)
>	Azure-WebApp-Container-Deploy	0% closed (10 alerts)



Found Means Fixed



脆弱性、
お前はすでに
修正されている...



Thank you!

