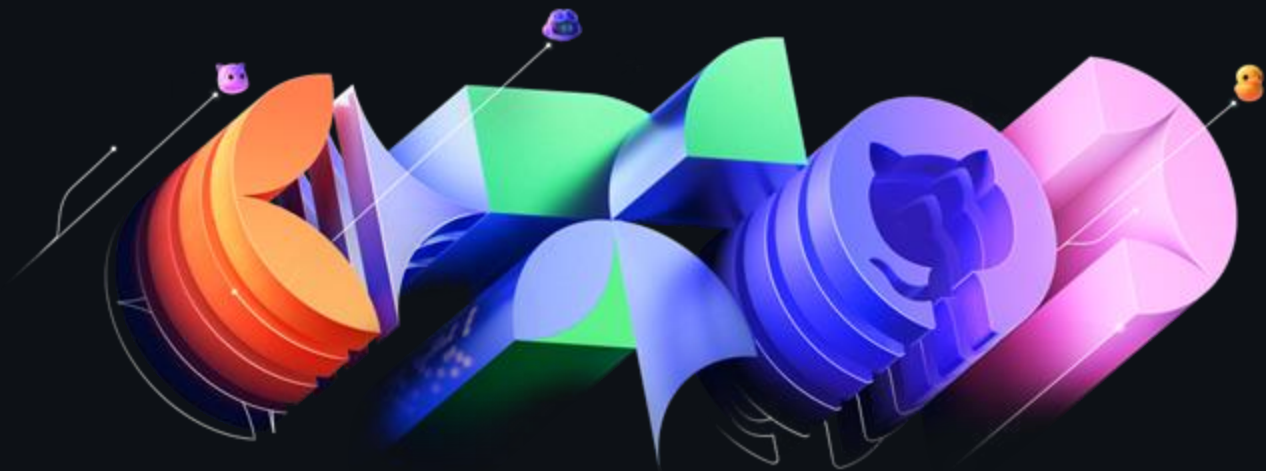


UNIVERSE'24 RECAP



脆弱性、お前はすでに修正されている...
AIでコードをセキュアに 🛡️



Kenta Nakase / @parroty
Senior Solutions Engineer, GitHub

Octoverse 2024 Report

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



The screenshot shows a web 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.



At the bottom of the page, there is a GitHub logo followed by the text "Octoverse 2024". The background of the page features an abstract graphic with glowing lines and dots in blue, green, and orange.

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

The state of generative AI in 2024

Injectionの脆弱性がトップ

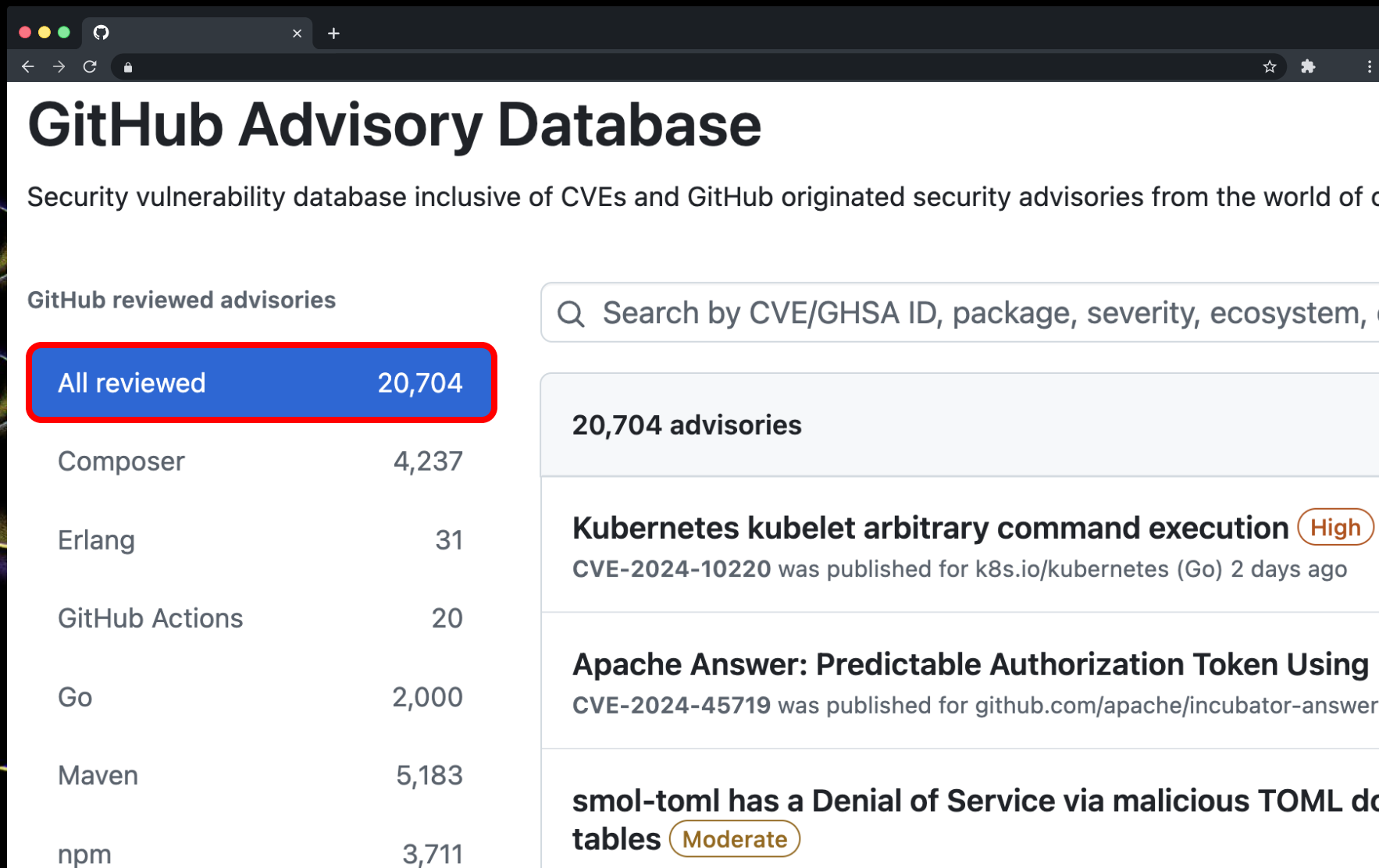
The state of security and automation in 2024

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>)



The screenshot shows the GitHub Advisory Database interface. At the top, the title "GitHub Advisory Database" is displayed in a large, bold font. Below the title, a subtitle reads "Security vulnerability database inclusive of CVEs and GitHub originated security advisories from the world of open source".

Under the heading "GitHub reviewed advisories", there is a search bar with the placeholder text "Search by CVE/GHSA ID, package, severity, ecosystem, or ecosystem". Below the search bar, a list of advisory categories is shown, with "All reviewed" highlighted in a blue box and containing 20,704 advisories. Other categories include Composer (4,237), Erlang (31), GitHub Actions (20), Go (2,000), Maven (5,183), and npm (3,711).

On the right side of the page, a list of specific advisories is displayed. The first entry is "Kubernetes kubelet arbitrary command execution" with a "High" severity rating. The second entry is "Apache Answer: Predictable Authorization Token Using Usernames" with a "Moderate" severity rating. The third entry is "smol-toml has a Denial of Service via malicious TOML documents" with a "Moderate" severity rating.

Category	Count
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 Usernames** (Moderate)
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 documents** (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
脆弱性がバックログに
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 web interface with the 'Security' tab selected. The alert is for a 'Regular Expression Denial of Service' in the 'semver' package. A pull request is suggested to bump the version from 5.7.1 to 5.7.2. The severity is 'High' with a score of 7.5/10. A table lists affected versions (< 5.7.2) and the patched version (5.7.2). A CVSS v3 base metrics table is also present on the right.

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 the GitHub web interface for a repository's dependency graph. The top navigation bar includes links for Code, Issues (3), Pull requests (9), Actions, Projects, Wiki, and Security (14). The left sidebar contains various repository metrics like Pulse, Contributors, and Traffic. The main content area is titled "Dependency graph" and has tabs for "Dependencies" and "Dependabot". A search bar contains the text "express". Below the search bar, a summary shows "7 Total" dependencies. The first dependency listed is "@types/express" with version "4.17.21", which is underlined in red. Below it is "express" with version "4.19.2", and at the bottom is "express-openid-connect" with version "2.7.2". A red underline is also present under the "Export SBOM" button in the top right of the graph area.

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](#)

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 interface. At the top, the navigation bar includes 'Code', 'Issues 3', 'Pull requests 9', 'Actions', 'Projects', 'Wiki', and 'Security 14'. The pull request title is 'Bump the npm_and_yarn group with 4 updates #291'. Below the title, it says 'dependabot wants to merge 1 commit into main from dependabot/npm_and_yarn/npm_and_yarn-bef8bfe7f'. A green 'Open' button is visible. The pull request details show 'Conversation 1', 'Commits 1', 'Checks 6', and 'Files changed 2'. A comment from 'dependabot bot' is highlighted with a red box, stating: 'Bumps the npm_and_yarn group with 4 updates: [express](#), [body-parser](#), [path-to-regexp](#) and [serve-static](#).' Below the comment, it lists 'Updates express from 4.19.2 to 4.20.0' and provides links for 'Release notes', 'Changelog', and '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...". A green "Open" label is on the left. The main content area is titled "All checks have passed" with a green checkmark icon and "8 successful checks". A "Hide all checks" link is on the right. Below this is a list of checks, each with a green checkmark, a GitHub logo, a title, a status, and a "Details" link. The "Dependency Review / dependency-review (pull_request)" check is highlighted with a red underline. At the bottom of the checks list, there is a green checkmark and the text "This branch has no conflicts with the base branch" and "Merging can be performed automatically.". At the very bottom, there is a green button that says "Merge pull request". On the right side of the page, there are sections for "Labels", "Projects", "Milestone", "Development", and "Notifications". The "Labels" section says "None yet". The "Projects" section says "None yet". The "Milestone" section says "No milestone". The "Development" section says "Successfully merging this pull request may close these issues." and "None yet". The "Notifications" section has a button that says "Unsubscribe" and the text "You're receiving notifications because you are subscribed to this pull request".

Open 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 subscribed to this pull request.

Dependabot Rules (Custom Auto Triage Rule)

The screenshot shows the GitHub interface for creating a new Dependabot rule. The left sidebar contains navigation options: General, Access (Collaborators and teams, Team and member roles), Code and automation (Branches, Tags, Rules, Actions, Webhooks, Copilot, Environments, Codespaces, Pages, Custom properties), and Alerts (Alerts, Alerts by severity, Alerts by ecosystem, Alerts by scope, Alerts by repository type, Alerts by repository type and ecosystem, Alerts by repository type and scope, Alerts by repository type and ecosystem and scope). The main content area is titled 'Code security / Dependabot rules / New rule' and includes the following fields:

- Rule name:** 優先度の低いアラートを除外
- State:** Enabled
- Target alerts:** severity:low scope:development ecosystem:npm
- Rules:** Dismiss alerts (checked), Until patch is available

Copilot Autofix for Dependabot

The screenshot shows a GitHub pull request interface. At the top, navigation tabs include Code, Issues, Pull requests (1), Actions, Projects, Wiki, Security (7), and Insights. The pull request title is "Bump lodash and @types/lodash #23". Below the title, it states "dependabot wants to merge 1 commit into main from dependabot/npm_and_yarn/multi-a2dacc6af4". A comment from the dependabot bot is visible, explaining the update of dependencies and providing links to release notes, commits, and maintainer changes. On the right side, there are sections for Reviewers (landongrindheim) and Assignees (No one—assign yourself).

Bump lodash and @types/lodash #23

Edit <> Code

Open dependabot wants to merge 1 commit into main from dependabot/npm_and_yarn/multi-a2dacc6af4

Conversation 1 Commits 1 Checks 2 Files changed 2 +11 -12

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 'parrot-demo / bookstore-demo-javascript'. The 'Security' tab is active, showing 18 alerts. A specific alert is displayed for 'Reflected cross-site scripting', which is 'Open' in the 'main' branch on July 2. The alert has a 'High' severity and is affecting the 'main' branch. The code snippet shows a JavaScript function that echoes a user-provided message, with the string interpolation part highlighted in yellow. A description below the code states: 'Cross-site scripting vulnerability due to a user-provided value'. The interface includes navigation links for Code, Issues (1), Pull requests (7), Actions, Projects, Wiki, and Security (18). A 'Dismiss alert' dropdown and a 'Create issue' button are visible. A 'Generate fix' button is also present, along with a link to 'Copilot Autofix for CodeQL'. The 'Affected branches' section shows 'main' with a warning icon. The 'Security campaigns' section indicates that no campaign is currently tracking this alert.

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)

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

...	<code>@@ -2,2 +2,3 @@</code>	
2	<code>import { listBooks } from './query-handler'</code>	2 <code>import { listBooks } from './query-handler'</code>
		3 <code>import escapeHtml = require('escape-html')</code>
3		4
...	<code>@@ -26,3 +27,3 @@</code>	
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 interface with a code scanning alert for "Reflected cross-site scripting". The alert is marked as "Open" and was detected in the "main" branch yesterday. A Copilot Autofix (AI) was generated less than a minute ago. The fix involves sanitizing user input by using the "escape-html" library to escape user-provided content in the response, specifically in the "src/index.js" file. A Copilot chat window is open on the right, showing a user request in Japanese: "このアラートの概要を日本語で解説して" (Explain the summary of this alert in Japanese). Copilot's response explains that the alert is about Reflected Cross-Site Scripting (Reflected Cross-Site Scripting) and provides a summary and recommended countermeasures in Japanese.

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 it is rendered in the HTML response. The best way to do this is by using a library that provides HTML escaping to ensure that any potentially malicious scripts in the user input are escaped and rendered as plain text.

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

`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, there's a navigation bar with tabs for Code, Issues, Pull requests (5), Actions, Projects, Wiki, Security (13), and Insights. The main title is 'Update application.js #6' with 'Edit' and '<> Code' buttons. Below the title, it says '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.' Below the comment, it lists the commits: 'rvermeulen added 2 commits 2 months ago', 'Update application.js' (Verified, 436d2a2), and 'Update .eslintrc.yml' (Verified, c087527). The right sidebar contains sections for Reviewers (No reviews, Convert to draft), Assignees (No one—assign yourself), and Labels (None yet).

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

parrot-demo / bookstore-demo-javascript

Code Issues 2 Pull requests 7 Actions Projects Wiki Security 18

bookstore-demo-javascript / config.yaml in main

Cancel changes Commit changes...

Edit Preview Spaces 2 No wrap

1 Enter file contents here



Custom Secret Patterns

The screenshot shows the 'Code security & analysis / New custom pattern' page in a browser. The page has a sidebar on the left with various navigation options. The main content area contains the following sections:

- Code security & analysis / New custom pattern**: The page title, with a 'Generate with AI' button highlighted by a red box.
- Pattern name ***: A text input field containing the Japanese text '社外用シークレット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 dropdown menu icon.
- Test string * - 2 matches**: A list of test strings with two highlighted matches:
 - `https://secure-1035142300.secret-domain.example.com` (highlighted)
 - `https://insecuret-xxx.domain.example.com`
 - `https://secure-1035142399.secret-domain.example.com` (highlighted)
 - `https://example.com`

Custom Secret Patterns

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**

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

Copilot Secret Scanning

The screenshot shows a GitHub Copilot Secret Scanning interface. At the top, a browser window displays the title "Password" and a notification: "Open GitHub detected a secret 20 days ago". Below this, a red heading reads "Possibly active secret". A light gray box contains the secret value "DeliberatelyInsecure1234" with a copy icon to its right. Underneath, it says "Detected by [Copilot Secret Scanning](#)". A red underline is drawn under the detection text. The section "Detected in 1 location" follows, showing a file path "src/main/java/com/example/demo/Utility.java" with a dropdown arrow and a copy icon. The code snippet below shows the secret value assigned to a variable in a Java file:

```
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";
```

On the right side of the interface, there are sections for "Secrets", "Tags" (with a "Multi-repo" tag), and "Related" items, each with a lock icon. A "Note: thi" is partially visible at the bottom right.

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)

The screenshot shows a web browser window displaying a security dashboard. The main content area is titled "Overview" and shows "Alert trends and insights across your organization." It includes a filter bar with "Filter 2" and "archived:false" selected, a search icon, a date range of "Last 30 days", and an "Export CSV" button. Below the filter bar are tabs for "Detection", "Remediation", and "Prevention". The primary chart is "Open alerts over time", which is a stacked area chart showing the number of open alerts from September to November 2024. The total number of open alerts is 78,987, with a 16.2% decrease as of November 20, 2024. The chart is grouped by severity: Critical (pink), High (orange), Medium (yellow), and Low (blue). A tooltip for Wednesday, 6 Nov 2024, shows the following counts: Critical (11,153), High (31,989), Medium (30,247), and Low (4,263). The left sidebar contains navigation options for "Overview", "Risk", and "Coverage", along with a "Metrics" section listing "Enablement trends", "CodeQL pull request alerts", and "Secret scanning". At the bottom of the sidebar, an "Alerts" section lists "Dependabot" (46.0k), "Code scanning" (161.0k), "Secret scanning" (4.4k), and "Default" (4.4k).

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

Overview

Alert trends and insights across your organization. [Give feedback](#)

Filter 2 archived:false to [X] [Q] Last 30 days [v] Export CSV [d]

Detection Remediation Prevention

Open alerts over time

Group by: Severity [v]

78,987 ↓ -16.2% as of Nov 20, 2024

Legend: Critical (pink), High (orange), Medium (yellow), Low (blue)

Severity	Count
Critical	11,153
High	31,989
Medium	30,247
Low	4,263



Security Overview (Risk)

Security

- Overview
- Risk**
- Coverage

Metrics

- Enablement trends
- CodeQL pull request alerts
- Secret scanning

Alerts

- Dependabot 1.4k
- Code scanning 3.3k
- Secret scanning ^
- Default 85
- Experimental 22

Security risk

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

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	Status	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 [X] [Q] Last 90 days [v] Export CSV [d]

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

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

Repository	Closed Alerts	Total Alerts
> Abeck_GHAS2	17% closed (6 alerts)	35
> AccessGroup-GHAS-demo	0% closed (89 alerts)	89
> activemq	0% closed (21 alerts)	21
> adrienpessu-juice-shop	0% closed (3 alerts)	3
> Azure-WebApp-Container-Deploy	0% closed (10 alerts)	10



Found Means Fixed



脆弱性、
お前はすでに
修正されている...



Thank you!

