



SBOM Play



Anant Shrivastava
Cyfinoid Research

SBOM Play



- SBOM Exploration and intelligence extraction platform
- IN-Browser
- Fully client side


Creation Idea






- SBOM is just an inventory
- Using SBOM in non-infosec scenarios
- Showing is better then talking

One Field : As simple as it can get





 **SBOM Play**

Analysis License Vulnerabilities Quality Dependencies Authors  


 **SBOM Play**



Analyze Software Bill of Materials from GitHub organizations, users, and repositories to understand dependency patterns and usage. Supports direct GitHub URLs for easy analysis.

 **Privacy Assured:** All analysis happens in your browser. No data is sent to any server.

 **Analyze GitHub Organization or User**

Enter a GitHub organization, username, repository, or URL to analyze*

 **Start Analysis**

 **Remove Rate Limit by GitHub Authentication (Optional)** 

SBoM Play: Input



- A Github organization / user / repository
- Either in shortform user/repo or org/repo or username or org
- Or full github url <https://github.com/cyfinoid/sbomplay>
- P.S. We just need Dependency Graph enabled on repositories.

Under the Hood



1. INPUT

User provides a GitHub Org, User, or Repo URL.



2. FETCH

The browser queries the GitHub Dependency Graph API for SBOM data.



3. RESOLVE & AUGMENT

The in-browser engine resolves the full dependency tree by querying public registries (npm, PyPI, etc.) and vulnerability databases (OSV.dev).



4. ANALYZE & VISUALIZE

Results are processed and displayed across multiple interactive views.



5. STORE

All analysis data is stored locally in the browser's IndexedDB for persistence.

This entire process is managed by JavaScript running in the browser. Your sensitive data never leaves your machine.

Nested SBOM Creation



🔍 Analyze GitHub Organization or User

Enter a GitHub organization, username, repository, or URL to analyze*

sbomplay-demo

▶ Start Analysis

🔑 Remove Rate Limit by GitHub Authentication (Optional)

🔄 Analysis Progress

67%

Resolving rubygems dependencies (18/35 direct) → factory_bot_rails (17 remaining)

🕒 Started: 25/11/2025, 11:33:12

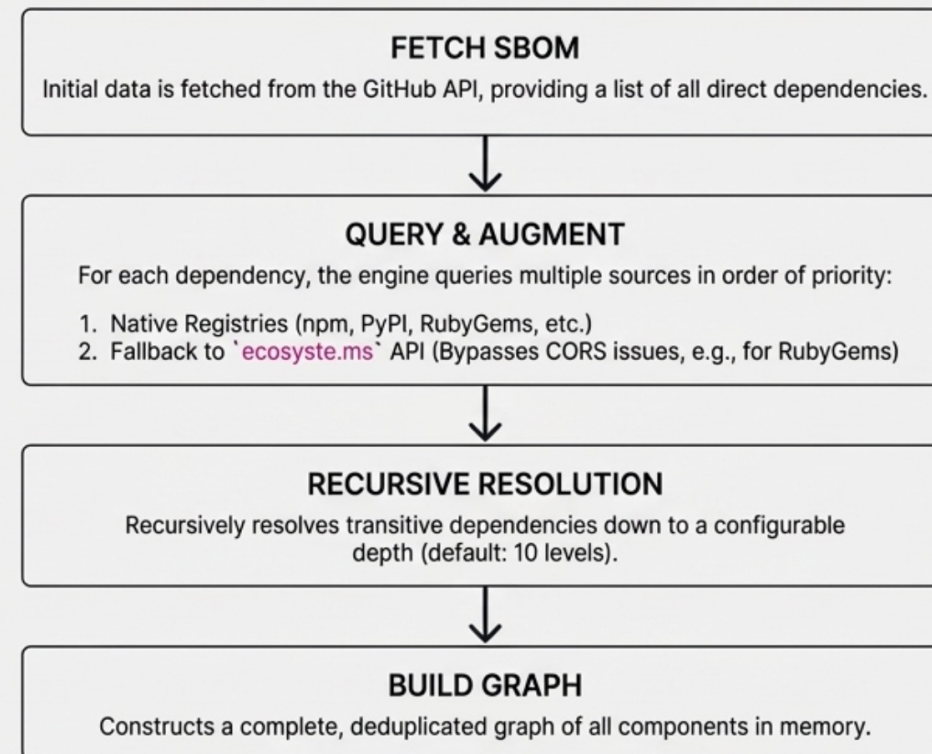
⌚ Elapsed: 19s

📦 Total packages processed: 18

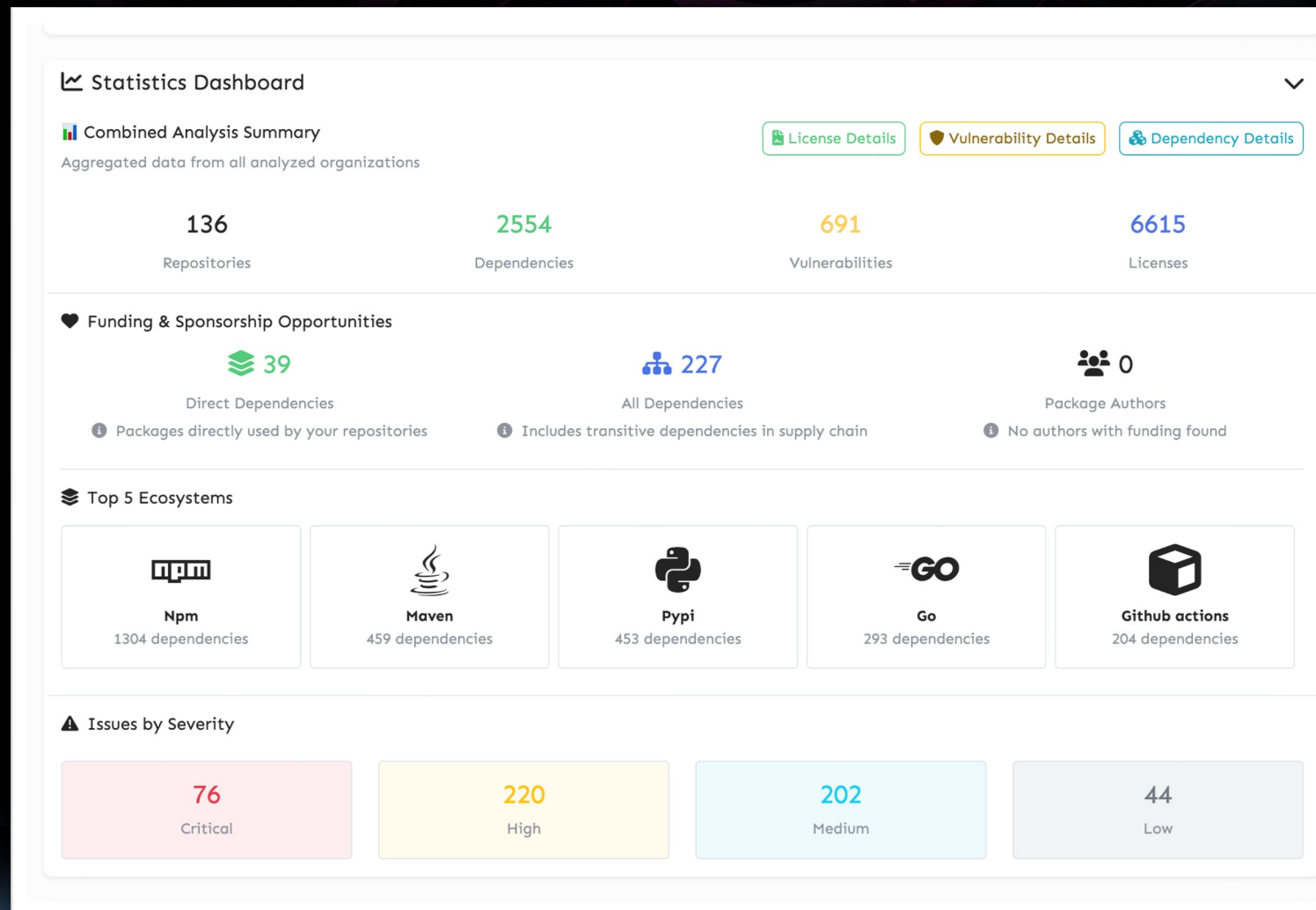
Rate Limit: 4928/5000 requests remaining

Reset Time: 11:53:40

Authenticated: Yes



Dashboard : 10K Feet view



Dependency View



Analysis

All Analyses (2272 deps) ▾

Search

Search package name...

Type

All ▾

Ecosystem

All ▾

Repository

All ▾

☐ Vulnerable

☐ Sponsorship

☐ Major Drift

☐ Minor Drift

☐ Unmaintained

2272

Total Dependencies

639

Direct

1633

Transitive

2272

Showing (filtered)

☰ Dependencies

Export CSV

Dependency ▾	Ecosystem ▾	Repos ▾	Vulns	License	Sponsor	Parent
webencodings@0.5.1 🕒 Stale (103m)	PyPI	4 repos	—	BSD	—	Direct
yaswfp@0.9.3 🕒 Stale (135m)	PyPI	4 repos	—	GPL-3.0	—	Direct
chardet@4.0.0 📈 Major: v5.2.0	PyPI	4 repos	—	LGPL	—	Direct

Vulnerability View



flask-appbuilder@4.3.10 ↑ Major: 5.0.2

6 vulnerabilities

MODERATE

MODERATE

MODERATE

CRITICAL

LOW

UNKNOWN

 Used in 4 repositories:

sbomplay-demo/license-conflict: flask-appbuilder@4.3.10

sbomplay-demo/python-deep-deps: flask-appbuilder@4.3.10

sbomplay-demo/seeking-sponsors: flask-appbuilder@4.3.10

sbomplay-demo/Dependency-trackers: flask-appbuilder@4.3.10

Repository View



Analysis

All Analyses (16 repos) ▾

Search

Search repository name...

Page Size

25 per page ▾

16

Total Repositories

16

With SBOM

8

With Vulnerabilities

16

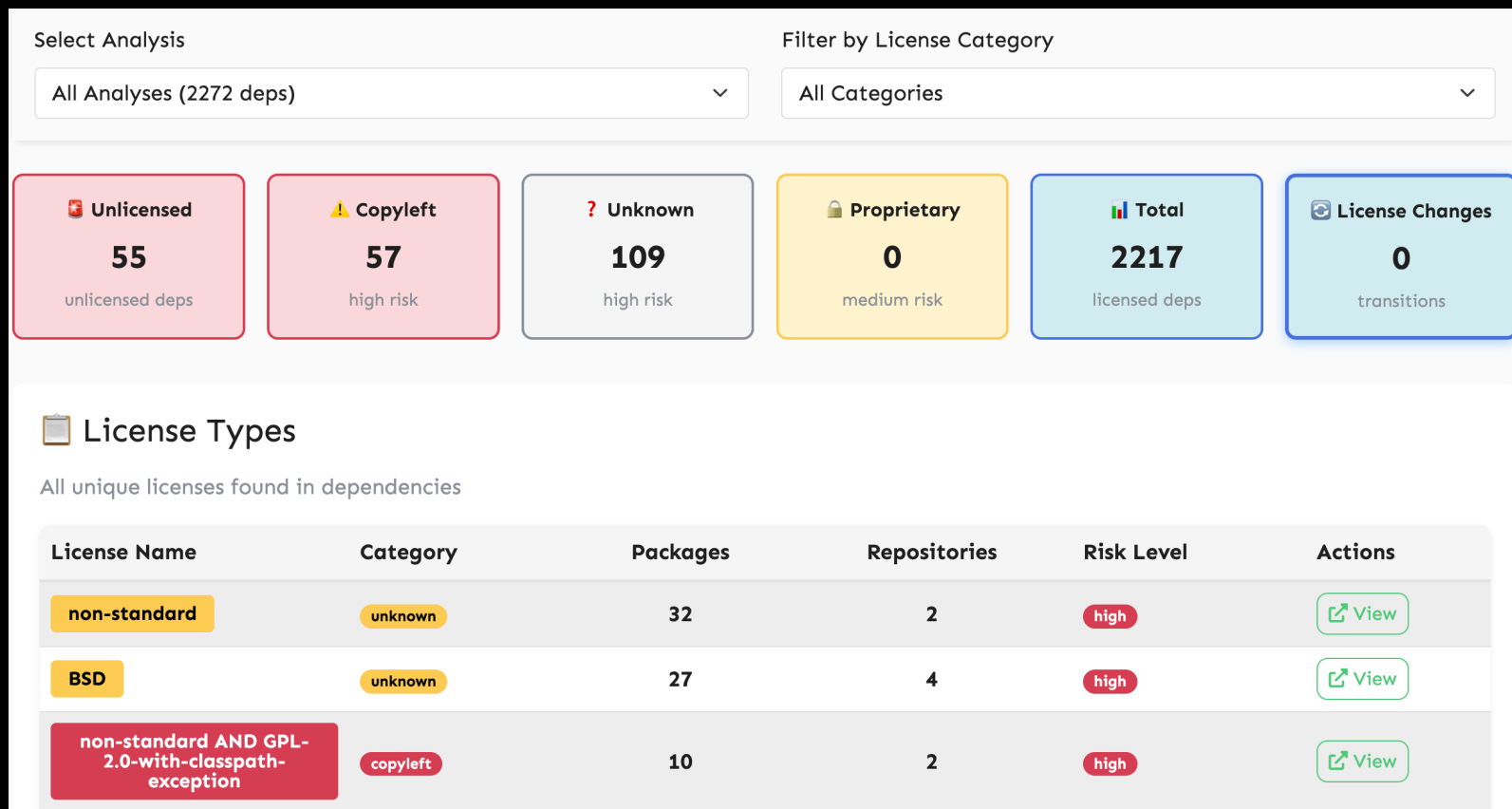
Showing (filtered)

☰ Repositories

Export CSV

Repository ▾	SBOM Grade ▾	Vulnerabilities ▾	Dependencies ▾	Authors ▾	Repository License ▾
sbomplay-demo/cargo-deep-deps	D (6.2)	—	12	89	—
sbomplay-demo/composer-deep-deps	D (6.3)	M:2 L:2	10	12	—
sbomplay-demo/Dependency-trackers	C (7.6)	H:129 M:100 L:32	809	971	GPL-3.0
sbomplay-demo/docker-deep-deps	D (6.9)	—	0	0	—

License Compliance



License Change



JUnit » 4.5

JUnit is a unit testing framework to write and run, organize, and execute automated tests, ensuring code quality and facilitate the development and running of test cases and test-driven development.

License	CPAL 1.0 CPL 1.0
Categories	Testing Frameworks & Tools
Tags	testing junit quality

[Home](#) » [junit](#) » [junit](#) » 4.12



JUnit » 4.12

JUnit is a unit testing framework to write and run, organize, and execute automated tests, ensuring code quality and facilitate the development and running of test cases and test-driven development.

License	EPL 1.0
Categories	Testing Frameworks & Tools
Tags	testing junit quality

Author Details



Select Analysis

Combined (All Scans) ▾

Filter by Ecosystem

All Ecosystems ▾

Filter by Location

All Locations ▾

☐ ❤️ Show only authors looking for sponsorship

☐ 🚫 Show only authors from sanctioned countries

⌵ Display Limit

📉 Top 25 Authors

☰ All Authors

☰ Authors by Contribution

Show Map

📘 Showing 25 of 329 human authors from 7 ecosystems (189 with multiple packages, 140 with single package across multiple repos)

Show All 329 Authors

#	Author	Ecosystem	Packages	Repository Usage	Location	Social	Sponsorship
1	Armin Ronacher	cargo	6	5 repos High Risk	Austria !		—
2	Hugo van Kemenade	pypi	23	4 repos Moderate Risk	Helsinki, Finland !		—
3	Jon Dufresne	pypi	18	4 repos Moderate Risk	Vancouver, BC, Canada !		—

Geographical View



VISUALIZING THE GLOBAL SUPPLY CHAIN



- **Geographic Distribution:** Visualize where your dependency authors are located, based on publicly available profile data.
- **Compliance & Risk:** Includes features to flag authors from sanctioned countries to aid in compliance checks.
- **Data Responsibility:** All location data is based on voluntary, public information and presented with clear disclaimers within the tool.

Version Sprawl



Top 5 Dependencies with Version Sprawl		
Package	Versions	Status
actions/checkout	11 versions	Version Sprawl
v2, v2.3.4, v3, v3.0.1, v3.1.0, v3.2.0, v3.3.0, v3.4.0, v3.5.0, v3.5.2, v3.6.0		
node-fetch	7 versions	Version Sprawl
lodash	4 versions	Version Sprawl
axios	2 versions	Version Sprawl
react	2 versions	Version Sprawl

Detects a single dependency being used with multiple different versions across your organization.

Shows the exact versions in use, highlighting fragmentation.

The Problem: Version sprawl increases the attack surface, creates compatibility issues, and makes patching inefficient.

The Solution: SBOM Play automatically surfaces the most fragmented dependencies, allowing engineering teams to prioritize standardization and reduce risk. Also highlights the most commonly used dependencies to focus efforts.

Beyond Vulnerabilities



- SBOM Play provides a unified "**Audit Findings**" view that consolidates risks from multiple sources:



- **GitHub Actions Security:** Insecure workflows, vulnerable actions.



- **SBOM Deficiencies:** Poor quality or incomplete SBOM files.



- **Package Health:** Stale, unmaintained, or deprecated packages.

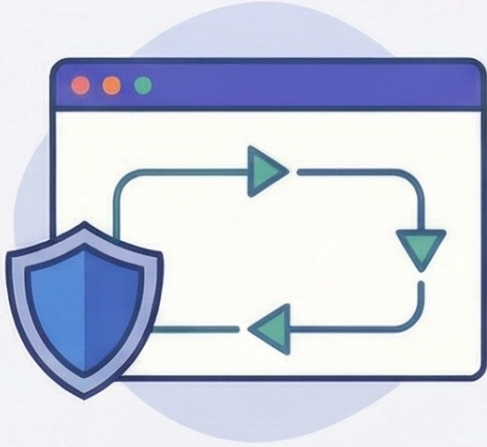


- **Version Drift:** Highlights when a dependency's latest version has drifted significantly from what's in use.



- **License Compatibility:** Automatically flagged license conflicts.

SBOM Play: SBOM Exploration and Intelligence Extraction Platform



Your SBOM Intelligence Hub - In Your Browser

Privacy-First by Design

All analysis happens locally in your browser; no data is ever sent to a server.



Simple Input, Powerful Insight

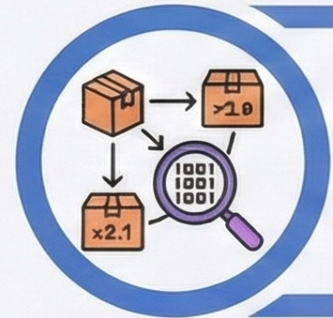
Just enter a GitHub organization, user, or repository URL to begin the analysis.



Multi-Ecosystem Support

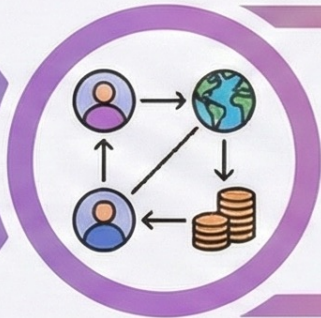
Tracks dependencies across npm, PyPI, Maven, Go, GitHub Actions, and more.

Go Beyond Vulnerability Scanning



Uncover Dependency Patterns

Identify commonly used packages and detect *version sprawl* across your projects.



Analyze Your Contributors

Identify third-party authors, visualize their locations, and discover funding opportunities.



Manage License Compliance

Assess license risks and automatically detect license changes between package versions.

Explore Your Supply Chain

Try It Now

<https://cyfinoid.github.io/sbomplay/>



A Product By **Cyfinoid Research**
cyfinoid.com

Thanks you for listening

- anant@cyfinoid.com
- [@anantshri](#)
- <https://cyfinoid.github.io/sbomplay/>
- <https://github.com/cyfinoid/sbomplay/>



Live URL



black hat[®]

EUROPE 2025

DECEMBER 8-11, 2025

EXCEL LONDON / UNITED KINGDOM