



SBOMPlay

 **black hat**[®]
ARSENAL

APRIL 23-24, 2026

MARINA BAY SANDS / SINGAPORE

Anant Shrivastava
Cyfinoid Research



Cyfinoid



SBOM Play

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

The screenshot shows the SBOM Play web application interface. At the top, there is a navigation bar with the following links: Home, License, Vulns, Audit, Findings, Deps, Repos, Authors, Settings, and About. The main heading is "SBOM Play" with a sub-heading "Analyze Software Bill of Materials from GitHub organizations, users, and repositories to understand dependency patterns and usage. Supports direct GitHub URLs for easy analysis." Below this, there are several social media and sponsorship buttons: "Presented @ BlackHat EU 2025 Arsenal", "Launched @ PeerList", "Sponsor", and "Buy Me A Coffee". A privacy notice states: "Privacy Assured: All analysis happens in your browser. No data is sent to any server." The main input area features a "GitHub" icon and an "Upload SBOM" button. Below this is a text input field with the placeholder "Enter a GitHub organization, username, repository, or URL to analyze" and an example "e.g., microsoft, torvalds, microsoft/vscode, or https://github.com/cyfinoid/sbomplay". A "Start Analysis" button is positioned to the right of the input field. At the bottom, there is a checkbox labeled "Remove Rate Limit by GitHub Authentication (Optional)".

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



SBOM is just an inventory

Beyond the Code / SBOM
Supply Chain Security

2023

- Initial Idea
- Bsides London presentation


SBoM
The Fad, The Future, and In-Between
Anant Shrivastava

2024

- Bsides Bangalore
- c0c0n
- SBOMPlay python


**We got the Shiny SBoM;
what next?**
Anant Shrivastava

2025

- SBOMPlay created



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



SBOM Beyond Infosec

- SBOMPlay showcases different ways to use sbom
- Using SBOM in non-infosec scenarios
- Showing is better than talking



Input

- Github*
 - A Github organization / user / repository
 - Either in shortform user/repo or org/repo or username or org
 - full github url <https://github.com/cyfinoid/sbomplay>
- Upload SBOM
 - spdx or cyclonedx json format supported

**Github repos need to have dependency graph enabled*



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.

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



Privacy Preservation as a core principle

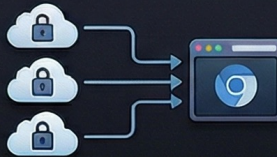
Browser-Native Privacy

100% Client-Side Processing



All analysis and dependency resolution happens in your local JavaScript runtime, not a server.

Direct Server Fetching



Data is fetched directly from registries to your browser; no third party holds a copy.

Zero Server-Side Footprint



There is nothing stored at the tool's end, leaving no server-side data to protect.

SBOM Play:

Privacy-Preserving Supply Chain Intelligence

A browser-native analysis tool enriching SBOM data with vulnerability and license insights, eliminating intellectual property uploads by processing all data locally.

Local Data Sovereignty

Persistent IndexedDB Storage



Analysis results are saved in your browser's local database, granting you full data control.

Ephemeral Token Handling



GitHub tokens are used only for rate limits and are never persisted or transmitted.

Traditional SaaS vs. SBOM Play

	Traditional SaaS Tools	SBOM Play
Data Location	Centralized Server/Cloud	Local Browser (IndexedDB)
IP Disclosure	Required (Uploads)	None (Local Processing)
Attack Surface	Vendor Database	User's Machine Only

Universal Portability

Standalone HTML Execution



Download the zip, unzip, and double-click index.html to run the full application.

Air-Gap Compatible



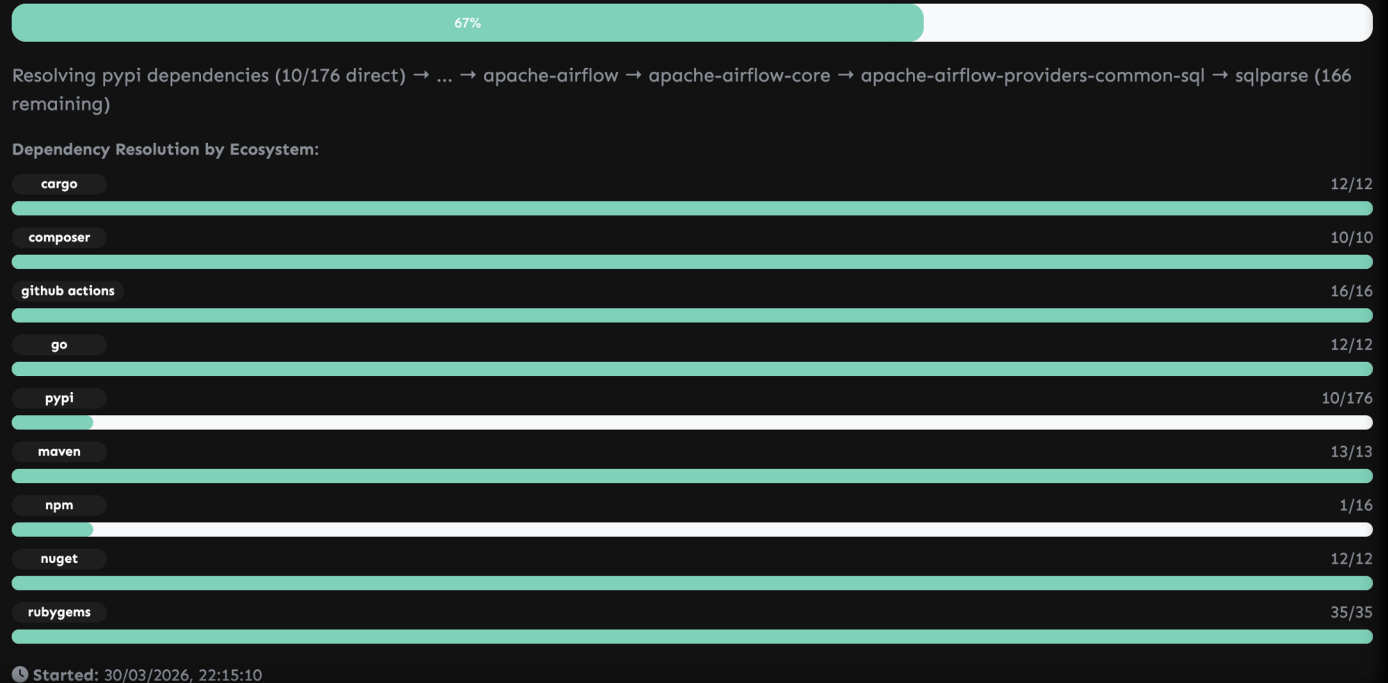
Supports network-isolated environments by allowing local hoisting of all CDN assets.



SBOM Data extraction

- Cascading SBoM resolutions
- 10 levels deep (configurable)
- Live parallel query to the registeries

Analysis Progress





Dashboard

Statistics Dashboard

Combined Analysis Summary

Aggregated data from all analyzed organizations

[License Details](#)[Vulnerability Details](#)[Dependency Details](#)

2

Repositories

1271

Dependencies

499

Vulnerabilities

1271

Licenses

Funding & Sponsorship Opportunities

12

Direct Dependencies

i Packages directly used by your repositories

12

All Dependencies

i Includes transitive dependencies in supply chain

13

Package Authors

i Maintainers accepting personal sponsorships

Top 5 Ecosystems



Npm

840 dependencies



Pypi

399 dependencies



Rubygems

17 dependencies



Maven

11 dependencies



Github actions

4 dependencies

Issues by Severity

33

Critical

131

High

114

Medium

35

Low

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



Dependency View

Analysis: All Analyses (1271 deps) | Search: Search package name... | Type: All | Ecosystem: All | Repository: All

Vulnerable | Sponsorship | Major Drift | Minor Drift | Unmaintained | End-of-Life

1271 Total Dependencies | 345 Direct | 926 Transitive | 1271 Showing (filtered)

☰ Dependencies 📄 Export CSV

Dependency	Ecosystem	Repos	Vulns	License	Sponsor	Parent
abbrev@1.1.1	npm	1 repo	—	ISC	—	Unknown
accepts@1.3.7	npm	1 repo	—	MIT	—	Unknown
acorn@7.3.1	npm	1 repo	—	MIT	—	Unknown



Vulnerability View

`org.apache.tomcat.embed:tomcat-embed-core@10.1.16`

20 vulnerabilities



🔗 Used in 2 repositories:

[View Details](#)

sbomplay-demo/maven-deep-deps: `org.springframework.boot:spring-boot-starter-web@3.2.0` → `org.springframework.boot:spring-boot-starter-tomcat@3.2.0` → `org.apache.tomcat.embed:tomcat-embed-core@10.1.16`

sbomplay-demo/Dependency-trackers: `org.springframework.boot:spring-boot-starter-web@3.2.0` → `org.springframework.boot:spring-boot-starter-tomcat@3.2.0` → `org.apache.tomcat.embed:tomcat-embed-core@10.1.16`



Repository View

Analysis

All Analyses (17 repos)

Search

Search repository name...

Page Size

25 per page

17

Total Repositories

17

With SBOM

8

With Vulnerabilities

17

Showing (filtered)

☰ Repositories

📄 Export CSV

Repository	SBOM Grade	Vulnerabilities	Dependencies	Authors	Repository License
sbomplay-demo/cargo-deep-deps	D (5.2)	—	12	88	—
sbomplay-demo/composer-deep-deps	D (5.2)	H:1 M:2 L:2	10	12	—
sbomplay-demo/Dependency-trackers	D (6.5)	H:158 M:125 L:59	808	968	GPL-3.0
sbomplay-demo/docker-deep-deps	D (5.3)	—	0	0	—
sbomplay-demo/github-actions-basic	D (5.1)	—	4	1	—
sbomplay-demo/github-actions-nested	D (5.1)	—	10	5	—
sbomplay-demo/go-deep-deps	D (6.7)	—	12	6	—

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



License Compliance

Select Analysis: All Analyses (1271 deps) | Filter by License Category: All Categories

Unlicensed 38 unlicensed deps	Copyleft 0 high risk	Unknown 27 high risk	Proprietary 0 medium risk	Total 1233 licensed deps	License Changes 2 transitions
--	-----------------------------------	-----------------------------------	--	---------------------------------------	--

License Types

All unique licenses found in dependencies

License Name	Category	Packages	Repositories	Risk Level	Actions
GPL-3.0	copyleft	98	1	high	View
BSD	unknown	7	1	high	View
GPL-3.0-or-later	copyleft	5	1	high	View

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



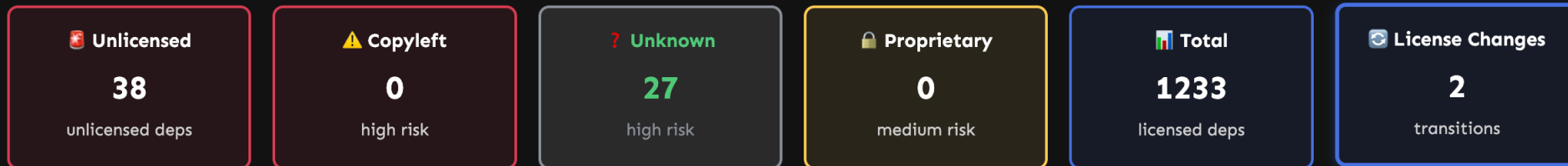
License Changes

Select Analysis

All Analyses (1271 deps)

Filter by License Category

All Categories



License Changes Detected

All license changes across all dependencies (not just high-risk)

Dependency	Version 1 @ License 1	Version 2 @ License 2	Repositories
wordwrap	0.0.2 MIT/X11	0.0.3 MIT	1
es6-symbol	3.1.1 MIT	3.1.3 ISC	1



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 333 human authors from 7 ecosystems (191 with multiple packages, 142 with single package across multiple repos)

Show All 333 Authors

#	Author	Ecosystem	Packages	Repository Usage	Location	Social	Sponsorship
1	Armin Ronacher	cargo	7	5 repos High Risk	Austria		—
2	Hugo van Kemenade	pypi	24	4 repos Moderate Risk	Helsinki, Finland		—
3	Jon Dufresne	pypi	18	4 repos Moderate Risk	Vancouver, BC, Canada		—
4	Thomas Kriechbaumer	pypi	10	4 repos Moderate Risk	London, England		—



Geographical Distribution

Author Locations Map

Hide Map

⚠ Location Data Disclaimer: Author locations shown on this map are based on voluntarily provided information from authors themselves (typically from their GitHub profiles, package registry profiles, or other public sources). This information may be incomplete, outdated, or inaccurate. Locations are geocoded automatically and may not reflect the actual current location of authors.



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



Common Dependencies

★ Top 5 Most Commonly Used Dependencies ✓

backcall@0.2.0

Used in 4 repositories

[View](#)

chardet@4.0.0

Used in 4 repositories

[View](#)

brotli@1.0.9

Used in 4 repositories

[View](#)

pysocks@1.7.1

Used in 4 repositories

[View](#)

urwid@2.1.2

Used in 4 repositories

[View](#)



Version Sprawl

🔗 Top 5 Dependencies with Version Sprawl

org.slf4j:slf4j-api 7 versions Version Sprawl

Versions: 1.7.25, 1.7.32, 1.7.36, 2.0.0-alpha1, 2.0.2 ... and 2 more

View

protobuf 6 versions Version Sprawl

Versions: 3.18.3, 3.19.6, 4.21.12, 4.25.9, 6.33.6 ... and 1 more

View

flask 6 versions Version Sprawl

Versions: 1.1.2, 2.0.3, 2.2.5, 2.3.3, 3.1.3 ... and 1 more

View

importlib-metadata 5 versions Version Sprawl

Versions: 1.6.0, 2.0.0, 8.7.1, 9.0.0, unknown

View

commander 5 versions Version Sprawl

Versions: 11.1.0, 2.20.3, 4.1.1, 7.2.0, 8.3.0

View



SBoM Audit and Compliance Findings

Select Analysis
All Analyses (1271 deps)

Filter by Severity
All Severities

Filter by Section
All Sections

Filter by Repository
All Repositories

SBOM Audit

2/2

Repositories with SBOM

0

CISA 2025

1

Fresh SBOMs

64%

Avg Completeness

Grade Distribution

D: 2

CISA 2025: 0/2 (0%)
US Federal SBOM requirements

BSI TR-03183: 0/2 (0%)
German/EU technical guideline

CERT-In: 0/2 (0%)
Indian CERT guidelines

Repository SBOM Quality

Source	Repository	Format	Grade	Score	CISA	BSI	CERT	Freshness	Complete	Details
	upload/deconfuse		D	6.3/10					65%	8
	anantshri-clones/Dependency-trackers		D	6.5/10					63%	12

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



EoX and Dependency Confusion Detection

Select Analysis: All Analyses (3469 deps) | Filter by Severity: All Severities | Filter by Finding Type: All Types | Filter by Repository: All Repositories

Security Findings Summary

555 Total Findings	468 High	87 Medium	0 Warning
90 GitHub Actions	2 Dependency Confusion	463 EOX (End-of-Life/Support)	0 Dead Source Repos

- HIGH** EOX (End-of-Life/Support) **Highly Likely EOL (Abandoned)** 376 findings
- HIGH** GitHub Actions **Unpinned Action Reference** 80 findings
- HIGH** GitHub Actions **Mutable Tag Reference** 10 findings
- HIGH** Dependency Confusion **HIGH-CONFIDENCE Dependency Confusion (Namespace Missing)** 1 finding
- HIGH** Dependency Confusion **Potential Dependency Confusion** 1 finding
- MEDIUM** EOX (End-of-Life/Support) **Probable EOL** 87 findings

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



SBOMPlay : SBOM Exploration and intelligence extraction

Client-side web application for analyzing Software Bill of Materials (SBOM) data from GitHub. It empowers security professionals to identify vulnerabilities, assess license compliance, and detect supply chain risks—all processed locally within the browser.

Deep Supply Chain Intelligence

Automated Vulnerability Scanning



Integrated OSV.day scanning identifies CVEs across dependencies with severity-based filtering.

Advanced License Compliance



Categorizes 100+ licenses by risk level and detects complex dual-license conflicts.

Privacy-First Architecture

100% Client-Side Processing



Your SBOM data never leaves your machine; all analysis happens in-browser.

IndexedDB Persistent Storage



Efficiently stores gigabytes of local analysis data without requiring a back-end server.

Author & Funding Detection



Tracks author geolocation, deduplicates contributors, and identifies open-source sponsorship opportunities.

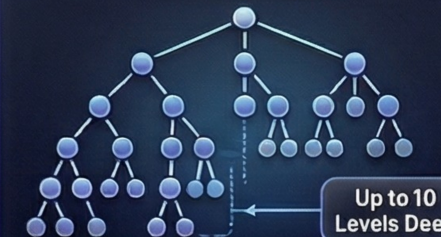




APRIL 23-24, 2026
MARINA BAY SANDS / SINGAPORE



Deep Dependency Resolution



Resolves transitive dependency trees up to 10 levels deep across multiple ecosystems.



Thanks

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

