



DEPENDENCY-TRACK COMMUNITY MEETING

OCTOBER
2024

THE DEPENDENCY-TRACK TEAM

www.owasp.org

Dependency-Track Community Meeting - October 2024

Organizational

- Community Meetings are recorded and [uploaded to YouTube](#)
- Slides will be published in the [DependencyTrack/community](#) repository
- Please use the Zoom chat to ask questions during the presentation
- There will be an open Q&A section towards the end

AGENDA

Hot off the Press: v4.12.0

01

Demo: v4.12.0

02

Looking ahead: v4.13.0

03



04

Q&A

05



HOT OFF THE PRESS: v4.12.0



HOT OFF THE PRESS: v4.12.0



- 29 contributors **across main and frontend repo*
- 20 *new* contributors **across main and frontend repo*
- >50 enhancements
- >20 fixes **excluding 4.11.x backports*



<https://docs.dependencytrack.org/changelog/#v4-12-0>

HOT OFF THE PRESS: v4.12.0

Highlights

- 🏷️ Breadth of tag-related features (incl. tag management)
- ⚖️ Global Policy Violation Audit View **DEMO**
- 🔒 Authorization for badges **DEMO**
- ✨ Tech stack modernization
- ⚠️ Multiple deprecations *(please check upgrade notes!)*

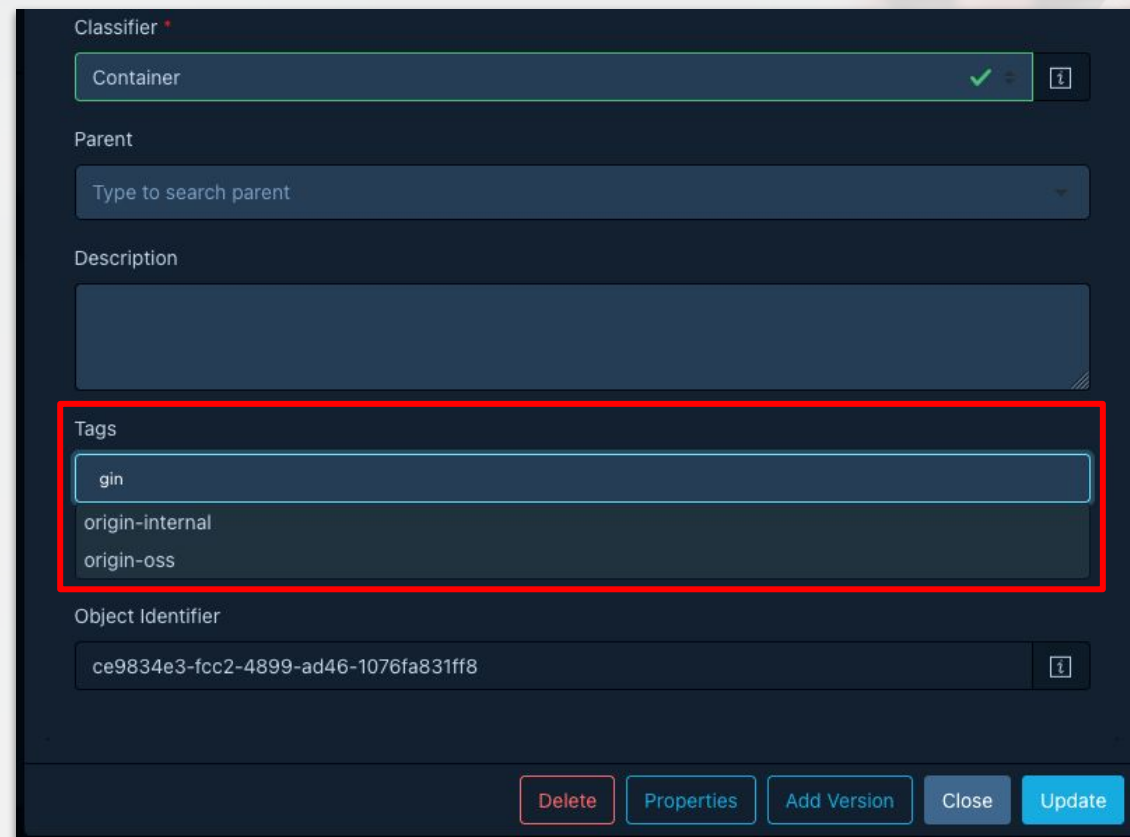
dependencies 0 3 25 0 3



<https://docs.dependencytrack.org/changelog/#v4-12-0>

HOT OFF THE PRESS: v4.12.0

Autocomplete for Tag Inputs



The screenshot displays a dark-themed form for creating or editing an object. The form includes several fields: 'Classifier' (set to 'Container'), 'Parent' (with a search prompt), 'Description' (a large text area), 'Tags' (a list of tags with 'gin' selected), and 'Object Identifier' (set to 'ce9834e3-fcc2-4899-ad46-1076fa831ff8'). The 'Tags' section is highlighted with a red border, showing a list of suggestions: 'gin', 'origin-internal', and 'origin-oss'. At the bottom, there are buttons for 'Delete', 'Properties', 'Add Version', 'Close', and 'Update'.

Classifier *

Container

Parent

Type to search parent

Description

Tags

gin

origin-internal

origin-oss

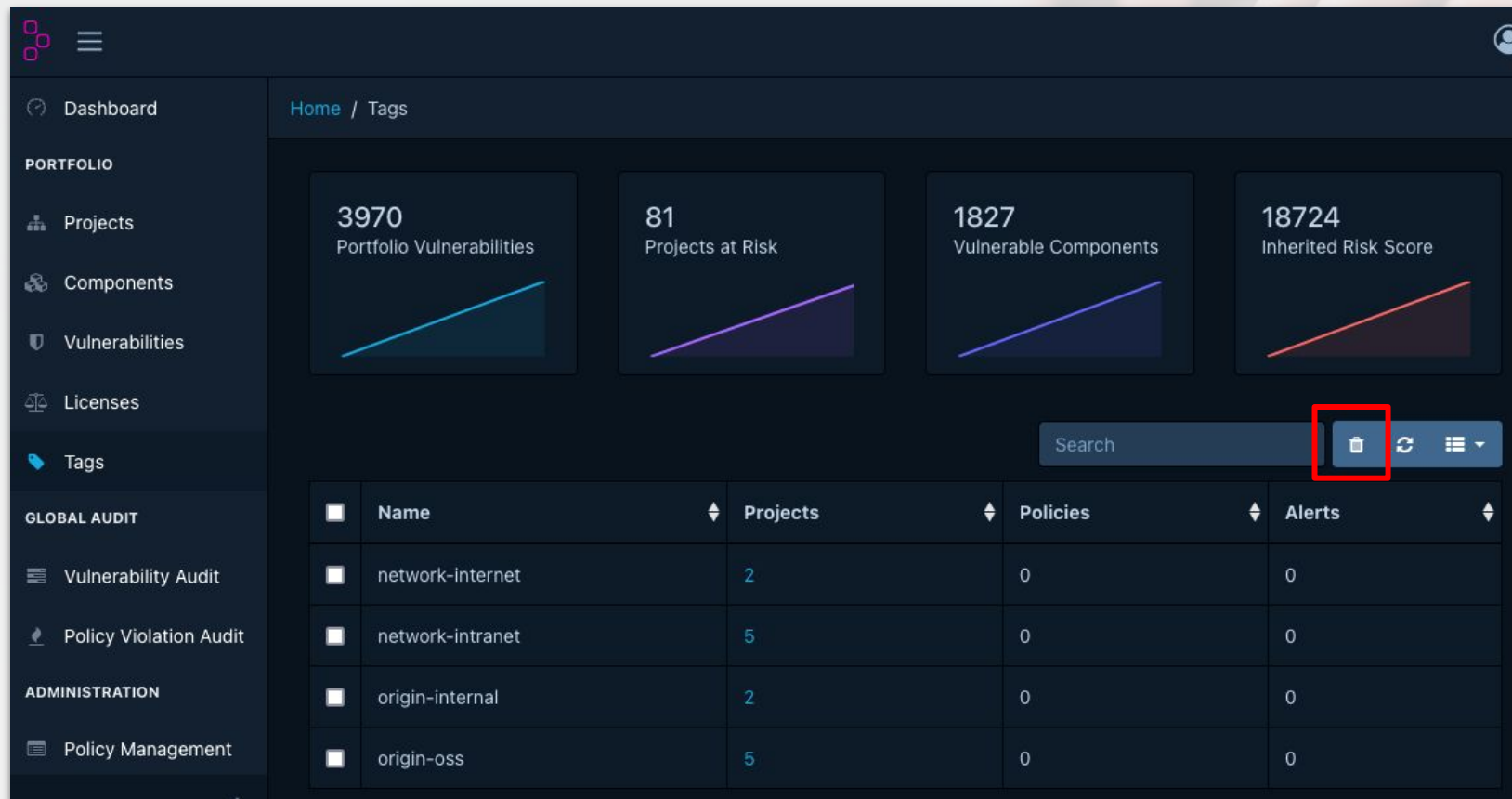
Object Identifier

ce9834e3-fcc2-4899-ad46-1076fa831ff8

Delete Properties Add Version Close Update

HOT OFF THE PRESS: v4.12.0




Tag Management



HOT OFF THE PRESS: v4.12.0

Tag Management

Projects tagged with network-intranet

<input type="checkbox"/>	Name	Version
<input type="checkbox"/>	apache/airflow:2.0.0	d4f54e56-350d-4d0c-b182-5354bd68a044
<input type="checkbox"/>	apache/airflow:2.5.3	ea547eff-912e-438c-8474-a4eae53e92
<input type="checkbox"/>	apache/airflow:2.9.1	6c5298db-48b8-40d2-a093-55cd604a2e3d
<input type="checkbox"/>	apache/flink:1.17	f369e597-cb73-4641-9eb2-4c8ccb94c32c
<input type="checkbox"/>	apache/kafka:3.7.0	c829ab91-ee5a-473a-8cea-b2f751bb9b4c

Showing 1 to 5 of 5 rows

Cancel

HOT OFF THE PRESS: v4.12.0

Selective BOM Validation with Tags

The screenshot displays the configuration interface for OWASP Dependency-Track. On the left is a sidebar menu with the following items: Configuration (expanded), General, BOM Formats (highlighted in blue), Email, Welcome Message, Internal Components, Task scheduler, Search, Analyzers, Vulnerability Sources, Repositories, and Notifications. The main content area is titled 'General' and contains the following sections:

- General**: A description stating 'Enables support for processing BOMs of various formats. Only BOM formats which are enabled will be processed.'
- BOM Formats**: A toggle switch for 'Enable CycloneDX' which is currently turned on.
- BOM Validation**: A section highlighted with a red border, containing 'Validation Mode' options:
 - Enabled (radio button)
 - Disabled (radio button)
 - Enabled for tags (radio button) with an 'Add Tag' button
 - Disabled for tags (radio button, selected) with a 'no-validation X' button and an 'Add Tag' button
- Update**: A button at the bottom of the configuration panel.

HOT OFF THE PRESS: v4.12.0

Limiting Alerts to Tags

+ Create Alert

Search

↺

☰

Name	Publisher	Scope	Notification level	Enabled
Demo	Slack	PORTFOLIO	INFORMATIONAL	☑

Name *

Demo

✓

☑

 Enabled

☑

 Log successful publish

Publisher

Slack

Publisher class

org.dependencytrack.notification.publisher.SlackPublisher

Notification level

Informational

Destination *

https://example.com

✓

Limit to projects

+

Limit to tags

origin-internal X Add Tag

Scope

PORTFOLIO

Group

☑ NEW_VULNERABILITY

☐ NEW_VULNERABLE_DEPENDENCY

☐ PROJECT_AUDIT_CHANGE

☐ BOM_CONSUMED

☐ BOM_PROCESSED

☐ BOM_PROCESSING_FAILED

☐ BOM_VALIDATION_FAILED

☐ VEX_CONSUMED

☐ VEX_PROCESSED

☐ POLICY_VIOLATION

☐ PROJECT_CREATED

Perform Test

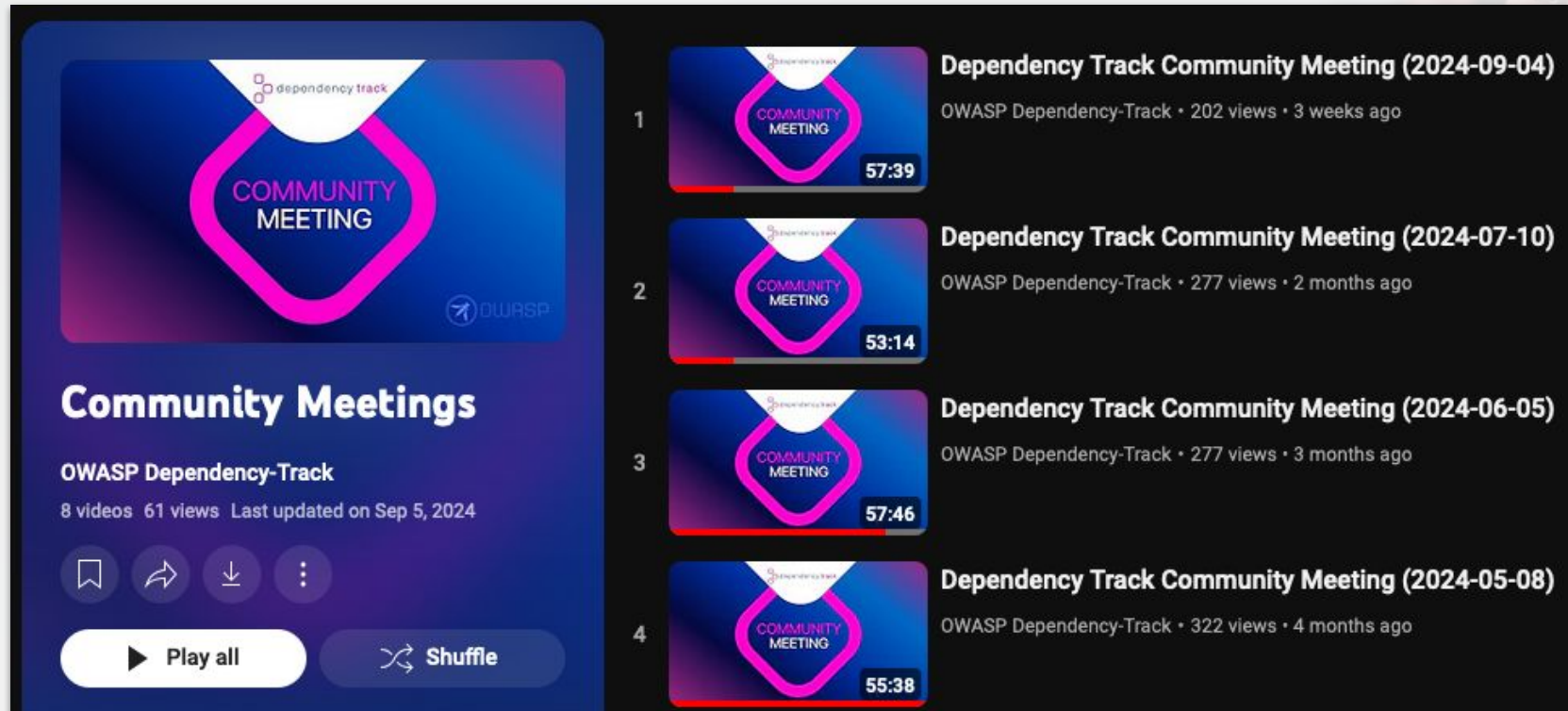
⬆ Limit To

Delete Alert

Submit

HOT OFF THE PRESS: v4.12.0

Full Demos in Previous Meetings



The image shows a YouTube playlist titled "Community Meetings" for the "OWASP Dependency-Track" channel. The playlist contains 8 videos with 61 views, last updated on Sep 5, 2024. The interface includes a "Play all" button and a "Shuffle" button. The video thumbnails feature a pink and blue design with the text "COMMUNITY MEETING" and the OWASP logo. The video titles and details are listed on the right side of the playlist.

Video Title	Views	Time Ago
Dependency Track Community Meeting (2024-09-04)	202 views	3 weeks ago
Dependency Track Community Meeting (2024-07-10)	277 views	2 months ago
Dependency Track Community Meeting (2024-06-05)	277 views	3 months ago
Dependency Track Community Meeting (2024-05-08)	322 views	4 months ago



https://www.youtube.com/playlist?list=PLQhgERhSEs97X4LRC_wc4Z3Sr9soAayJR



DEMO: v4.12.0





LOOKING AHEAD: v4.13.0



LOOKING AHEAD: v4.13.0

Project Collections

Home / Projects / test

Metrics of collection project are calculated by aggregating numbers of all direct children.

test

View Details >

Overview

Collection Projects

+ Create Project

Show inactive projects

Show flat project view

Search

Project Name	Tags	Version	Classifier	Last BOM Import	BOM Format	Risk Score	Active	Policy Violations	Vulnerabilities
asdasd			Container	29 Nov 2023 at 00:44:23	CycloneDX 1.4	304	✓	0	5 19 48 5
t2			Application	29 Nov 2023 at 00:44:14	CycloneDX 1.4	119	✓	0	3 4 23
t3			Application	-	-	119	✓	0	3 4 23
t4			Application	-	-	150	✓	0	4 7 25

Showing 1 to 4 of 4 rows

<https://github.com/DependencyTrack/dependency-track/pull/3258>

LOOKING AHEAD: v4.13.0

Scheduled Summary Notifications

[Dependency-Track] 7 new Vulnerability(s) in 2 component(s) in Scheduled Rule "Test Scheduled"

7 new Vulnerability(s) in 2 component(s) in Scheduled Rule "Test Scheduled"

Find below a summary of new vulnerabilities since 2024-07-07T16:14:27.909 in Scheduled Notification Rule "Test Scheduled".

Overview

Projects included in this rule	1
Total new vulnerabilities	7
New vulnerabilities (HIGH)	7
Components affected by new vulnerabilities	2
Suppressed new vulnerabilities (not included above)	0

Summary per project in this rule

Project Name	Version	New Vulnerabilities	All Vulnerabilities	Suppressed New Vulnerabilities
Testproject	dev	HIGH: 7	HIGH: 7	

New vulnerabilities per project

Project "Testproject" [Version: dev]

Component	Version	Group	Vulnerability	Severity	Analyzer	Attributed On	Analysis	Suppressed
guzzle	6.5.5	guzzlehttp	CVE-2022-29248	HIGH	OSSINDEX_ANALYZER	2024-07-07T16:05:22Z		No
guzzle	6.5.5	guzzlehttp	CVE-2022-31042	HIGH	OSSINDEX_ANALYZER	2024-07-07T16:05:22Z		No
guzzle	6.5.5	guzzlehttp	CVE-2022-31043	HIGH	OSSINDEX_ANALYZER	2024-07-07T16:05:22Z		No
guzzle	6.5.5	guzzlehttp	CVE-2022-31090	HIGH	OSSINDEX_ANALYZER	2024-07-07T16:05:22Z		No
guzzle	6.5.5	guzzlehttp	CVE-2022-31091	HIGH	OSSINDEX_ANALYZER	2024-07-07T16:05:22Z		No
psr7	1.8.3	guzzlehttp	CVE-2022-24775	HIGH	OSSINDEX_ANALYZER	2024-07-07T16:05:22Z		No
psr7	1.8.3	guzzlehttp	CVE-2023-29197	HIGH	OSSINDEX_ANALYZER	2024-07-07T16:05:22Z		No

Executed: 2024-07-07T18:05:37.037979100

<https://github.com/DependencyTrack/dependency-track/pull/3925>

LOOKING AHEAD: v4.13.0

Better Configuration Docs

The screenshot displays the 'API Server' configuration page in the OWASP Hyades documentation. On the left, a sidebar lists the navigation structure: 'Reference' (selected), 'Configuration', 'Overview', 'API Server', 'CORS', and 'Database'. The 'CORS' section is expanded, showing a list of configuration properties. The main content area is titled 'API Server' and 'CORS'. It details the 'alpine.cors.allow.credentials' property, which controls the 'Access-Control-Allow-Credentials' response header. A table lists its configuration details: Required (false), Type (boolean), Default (true), and ENV (ALPINE_CORS_ALLOW_CREDENTIALS). Below this, the 'alpine.cors.allow.headers' property is introduced, controlling the 'Access-Control-Allow-Headers' response header, with its own configuration table: Required (false) and Type (string).

Reference
Configuration
Overview
API Server
CORS
Database

alpine.cors.allow.credentials
alpine.cors.allow.headers
alpine.cors.allow.methods
alpine.cors.allow.origin
alpine.cors.enabled
alpine.cors.expose.head...
alpine.cors.max.age
alpine.database.password
alpine.database.passwor...
alpine.database.pool.ena...
alpine.database.pool.idle...
alpine.database.pool.ma...
alpine.database.pool.ma...
alpine.database.pool.min...
alpine.database.url
alpine.database.username
database.migration.pass...
database.migration.url
database.migration.user...
database.run.migrations

API Server

CORS

alpine.cors.allow.credentials

Controls the content of the `Access-Control-Allow-Credentials` response header.
Has no effect when `alpine.cors.enabled` is `false`.

Required	false
Type	boolean
Default	true
ENV	ALPINE_CORS_ALLOW_CREDENTIALS

alpine.cors.allow.headers

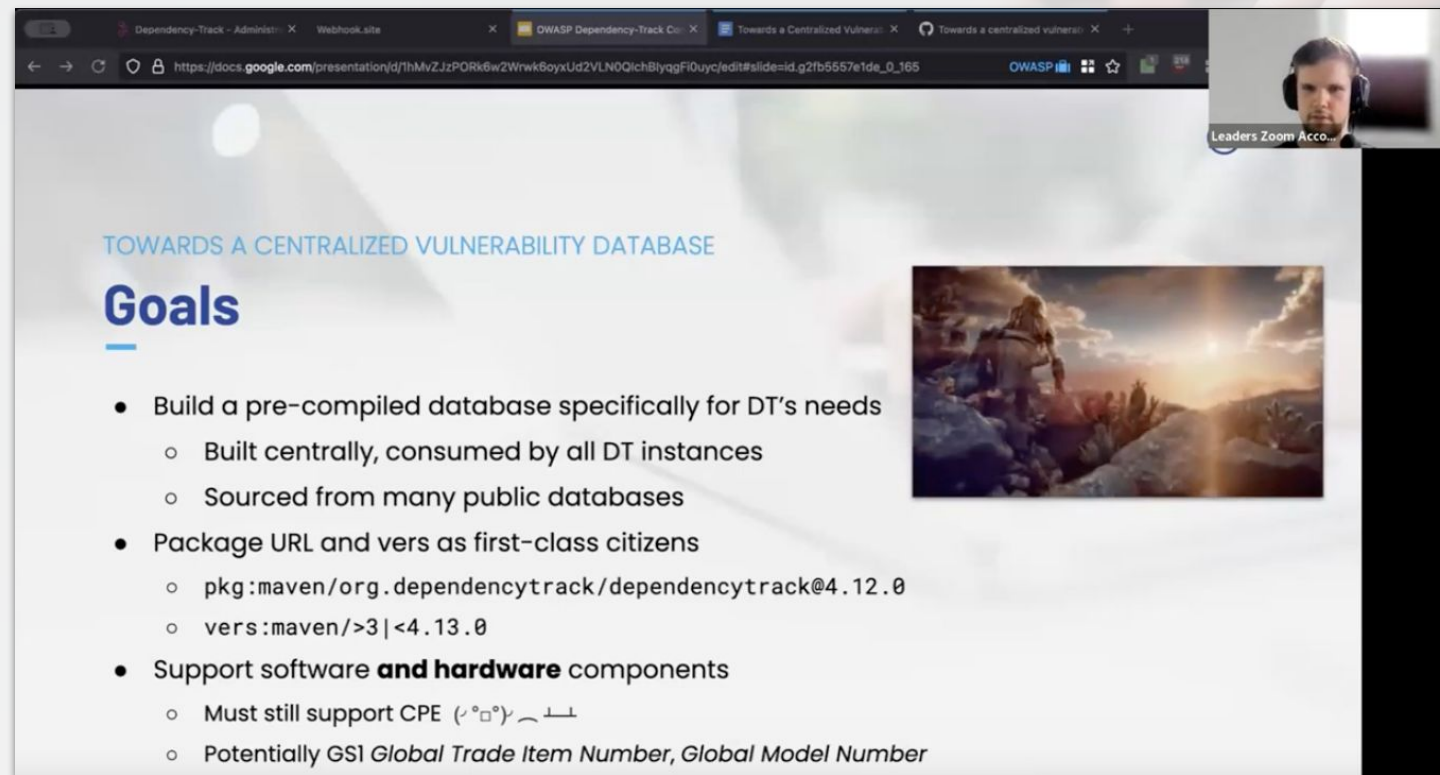
Controls the content of the `Access-Control-Allow-Headers` response header.
Has no effect when `alpine.cors.enabled` is `false`.

Required	false
Type	string

<https://dependencytrack.github.io/hyades/0.6.0-SNAPSHOT/reference/configuration/api-server/>

LOOKING AHEAD: v4.13.0

Improved Vulnerability DB (???)



The screenshot shows a presentation slide titled "TOWARDS A CENTRALIZED VULNERABILITY DATABASE" with the subtitle "Goals". The slide is displayed in a browser window with several tabs open, including "Dependency-Track - Administ...", "Webhook site", "OWASP Dependency-Track Co...", "Towards a Centralized Vulner...", and "Towards a centralized vulner...". The URL in the address bar is "https://docs.google.com/presentation/d/1hMvZJzPORK6w2Wrnk6oyxUd2VLN0Qich8IyqgFI0uyc/edit#slide=id.g2fb5557e1de_0_165". A video thumbnail on the right side of the slide shows a person in a desert landscape. A small video feed of a person is visible in the top right corner of the browser window.

TOWARDS A CENTRALIZED VULNERABILITY DATABASE

Goals

- Build a pre-compiled database specifically for DT's needs
 - Built centrally, consumed by all DT instances
 - Sourced from many public databases
- Package URL and vers as first-class citizens
 - `pkg:maven/org.dependencytrack/dependencytrack@4.12.0`
 - `vers:maven/>3|<4.13.0`
- Support software **and hardware** components
 - Must still support CPE (°□°) ˘ ˘ ˘
 - Potentially GSI *Global Trade Item Number, Global Model Number*

<https://www.youtube.com/watch?v=hzelt7jv6dE&t=1188s>



Looking for contributions

Hacktoberfest

- October open source contributor challenge hosted by DigitalOcean
- Goal: Submit four high-quality pull/merge requests between October 1 and October 31
- Unlock digital badges with each pull request, up to 4 to complete the challenge
- Learn more and register at: <https://hacktoberfest.com/>



QUESTIONS & ANSWERS

