OWASP Dependency Track

Table of Contents

[1 Overview 2](#_Toc278972948)

[1.1 What is OWASP Dependency Track? 3](#_Toc1567514315)

[1.2 Why is OWASP Dependency Track so valuable? 3](#_Toc513203527)

[2 References 4](#_Toc1804753420)

# Overview

Imagine your software development project as a bustling city, constantly under construction. Components and materials flow in from various suppliers, each playing a vital role in the final structure. But what if some of these materials were unknowingly flawed or compromised? This is where OWASP Dependency Track comes in, acting as your city's guardian angel, ensuring the integrity and security of your entire software supply chain.

## What is OWASP Dependency Track?

It's an open-source intelligence platform that goes beyond traditional software composition analysis (SCA) tools. Think of it as a comprehensive security scanner that goes beyond just identifying individual component vulnerabilities. Dependency Track delves deeper, providing:

* Full-stack component inventory: Tracks all components across your entire software portfolio, from libraries and frameworks to applications, containers, operating systems, and even firmware. This holistic view ensures no stone is left unturned.
* Accurate vulnerability detection: Leverages various sources to identify known vulnerabilities in your components, including the National Vulnerability Database (NVD), OSS Index, GitHub, Snyk, OSV, and VulnDB. You get a complete picture of potential security risks.
* Policy evaluation: Measures and enforces security, operational, and license compliance for individual projects or your entire portfolio. This ensures your components not only function as needed but also adhere to your set standards.
* Impact analysis: Rapidly pinpoints projects affected by identified vulnerabilities, enabling you to prioritize and focus your remediation efforts where they matter most. You don't waste time chasing false alarms.
* Integration and automation: Works seamlessly with existing development workflows and CI/CD pipelines, making security an intrinsic part of your development process, not a separate burden.

## Why is OWASP Dependency Track so valuable?

* Proactive and comprehensive: It moves beyond just identifying vulnerabilities; it provides actionable insights and helps you manage risk throughout your software supply chain.
* Customizable and adaptable: You can tailor Dependency Track to your specific needs and integrate it with other security tools for a unified view.
* Open-source and community-driven: You access continuous updates and improvements from a vibrant community of developers and security experts.

# References

1. <https://dependencytrack.org/>
2. <https://www.youtube.com/watch?v=n-oSe53_x_U>