Brayden Levinson
12/4/25

SBOOM Report

1. SBOM Generation Results

Syft generated an SBOM in SPDX format with 108 components, and Trivy generated an SBOM in CDX format. Syft reported a few more components than Trivy, whose issue was how each tool identifies or categorizes components. But both tools successfully created files in the deliverable folder.

2. Top 5 Vulnerabilities

CVE / GHSA ID	Severity	Component	Version	Comment	Column 1
GHSA-5rjg-fvgr-3xxf	High	setuptools	72.1.0	Update to 78.1.1	
GHSA-2qfp-q593-8484	High	brotli	1.1.0	Update to 1.2.0	
GHSA-768j-98cg-p3fv	Medium	fonttools	4.57.0	Update to 4.60.2	
GHSA-9hjg-9r4m-mvj7	Medium	requests	2.32.3	Update to 2.32.4	
GHSA-pq67-6m6q-mj2v	Medium	urllib3	2.2.2	Update to 2.5.0	

3. Vulnerability Summary

Setuptools GHSA-5rjig-fvgr-3xxf: the vulnerability in version 72.1.0 would allow a bad actor to save malicious files to locations on the computer they should not have access to, rather than the intended directory.

4. Reflection

During this assignment, I learned how valuable Sboom tools like Syft, Trivy, and Grype are for providing complete transparency into software projects, which can be very helpful for identifying potential vulnerabilities. The longest part of the assignment was my codespace trying to launch; it took forever for some reason.