SBOM Sprint #1

Thomas Eby, Pranav Gonepalli, Evan Hellersund, Manel Leong,
Camron Rule, Skyler Walker, Duohan Xu, Rachel Zheng

College of William & Mary

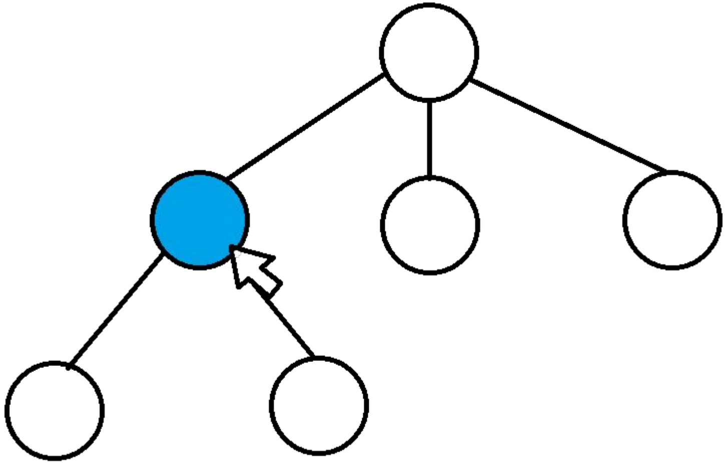
CSCI 435: Software Engineering
September 25, 2024

Sprint Goal

- Perform independent research to further understand:
  - What SBOMs are,
  - How developers use them in the real world,
  - What SBOM information would be useful in a visualization tool.
- Identify what capabilities our tool should support

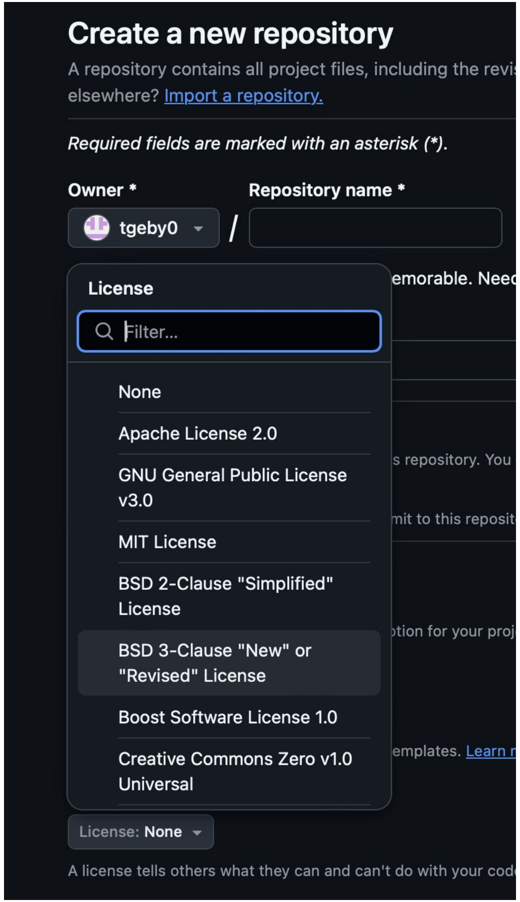
Capabilities

- Django website with interactive interface
  - HTML, CSS, JavaScript
- Tree-style traversal of SBOM
- Short 1-page PDF summary of important information
- Ability to specify the version and file type of SBOM before uploading it
  - Cyclone DX, SPDX, SWID tags for versions
  - Json and xml file types



Capabilities Continued

- Ability to filter SBOM data fields
- A way to query and display the restrictions placed on the project based on the licenses
    - Support for the software licenses available to associate with a GitHub repo
- A way to query a database for security vulnerabilities



Create a new repository

A repository contains all project files, including the revi

elsewhere? Import a repository.

Required fields are marked with an asterisk (*).

Owner * tgeby0 / Repository name *

emorable. Need

s repository. You

mit to this reposit

ption for your proj

emplates. Learn r

License: None

A license tells others what they can and can't do with your cod

License
Filter...
None
Apache License 2.0
GNU General Public License v3.0
MIT License
BSD 2-Clause "Simplified" License
BSD 3-Clause "New" or "Revised" License
Boost Software License 1.0
Creative Commons Zero v1.0 Universal

Tools and Dependencies

- Git, Visual Studio Code
- HTML, CSS, JavaScript, D3.js
- Django Rest Framework (DRF): To serve data as a JSON API.
- Django-MPTT or Django-Treebeard: For managing hierarchical models.

Next Sprint Backlog

- Issue tracker
- Artifacts - UML diagrams, etc.
    - Plan the layout of our visualization tree
- Research the requirements placed on the different software licenses
- Identify databases to use for identifying security vulnerabilities

Lessons

- Working asynchronously on shared documents resulted in slow response time.
  - We should try to meet in person or on Zoom at least once during a sprint to share what we have come up with.
- Meeting times couldn’t be made by all members of the team.
  - We should try and work out regular meeting times that can be made by all team members.

Contribution

Camron Rule: Created slideshow outline

Thomas Eby: Created capability proposal outline

All: Contributed to slideshow and capability proposals by contributing new ideas or affirming/challenging the ideas of others