SOFTWARE COMPOSITION ANALYSIS AND SUPPLY CHAIN SECURITY IN APACHE PROJECTS: AN EMPIRICAL STUDY

11/18/25

Xiangrui Ke,
David R. Cheriton School of Computer Science

UNIVERSITY OF WATERLOO

Motivation

- Modern software relies heavily on third-party components.
- These components may include known or unknown vulnerabilities.
- Attacks increasingly target the software supply chain (e.g., via dependencies).
- Developers often ignore or delay updates due to lack of awareness or perceived effort.

Research Gap

- Prior work focused on *detection capability* of SCA tools
- No causal studies on *effectiveness over time*

Research Gap

- Prior work focused on *detection capability* of SCA tools
- No causal studies on *effectiveness over time*

To what extent does the adoption of SCA tool impact software supply chain security?

Methodology: Cohort Study Design

Environment

- 298 Apache Java Maven projects on GitHub
- OWASP Dependency-Check (OWASP DC)
- 264-day follow-up period

Controlled for:

- Project age
- Number of dependencies
- Activity status

Methodology: Cohort Study Design

Content

Controlled for:

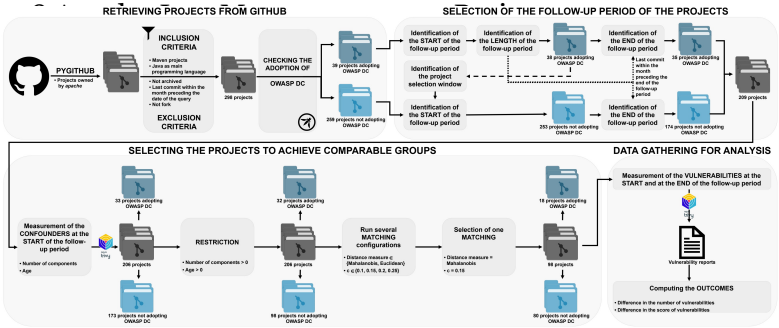


Fig. 1: Process describing the selection of projects.

Metrics & Analysis

Measured

- Change in vulnerability **count**
- Change in vulnerability **CVSS score**

Severity levels:

- Info, low, medium, high, critical

Used Generalized Linear Models (GLM)

RESULT

Severity	Info	Low	Medium	High	critical	Overall
Vulnerability After Using OWASP DC	↓	↑	↓	↓	↓↓	↓

- OWASP DC helps reduce serious vulnerabilities
- Statistically valid
- Developers may overlook **low-severity alert**

Pros & Cons

Strength

- Comprehensive methodology design
- Essential gap in software literature

Weakness

- Limited generalizability due to narrow language, ecosystem, and tool scope.
- Lack of validation in real-world development workflows.

Summary

Rating: 4/5

A methodologically rigorous and well-controlled empirical study

A timely empirical investigation into the real-world impact of SCA tools.

Despite modest effect sizes, the study provides meaningful insights for both academic research and industry practices on software supply chain security.

Future Work

Cross-language replication

Developer surveys or interviews:

Do OWASP DC alerts trigger actual remediation?

How AI tool can be integrated in SCA and further software develop workflows?

UNIVERSITY OF WATERLOO

Thank you !

TWO COLUMN CONTENT SLIDE LAYOUT

- Lorem ipsum dolor sit amet, consectetuer adipiscing elit
- Maecenas porttitor congue massa
- Fusce posuere, magna sed pulvinar ultricies, purus lectus malesuada libero, sit amet commodo magna eros quis urna
- Nunc viverra imperdiet enim.

- Lorem ipsum dolor sit amet, consectetuer adipiscing elit
- Maecenas porttitor congue massa
- Fusce posuere, magna sed pulvinar ultricies, purus lectus malesuada libero, sit amet commodo magna eros quis urna
- Nunc viverra imperdiet enim.

PAGE TITLE HERE

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Maecenas porttitor congue massa. Fusce posuere, magna sed pulvinar ultricies, purus lectus malesuada libero, sit amet commodo magna eros quis urna. Nunc viverra imperdiet enim. Fusce est. Vivamus a tellus.

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Proin pharetra nonummy pede. Mauris et orci. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Maecenas porttitor congue massa. Fusce posuere, magna sed pulvinar ultricies, purus lectus malesuada libero, sit amet commodo magna eros quis urna.

PAGE TITLE HERE

EXAMPLE.1

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus non sem semper, rhoncus quam nec.

EXAMPLE.2

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus non sem semper, rhoncus quam nec.

EXAMPLE.3

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus non sem semper, rhoncus quam nec.

UNIVERSITY OF WATERLOO

UNIVERSITY OF WATERLOO

YOU+WATERLOO

Our greatest impact happens together.

CONTEXT OR THEME

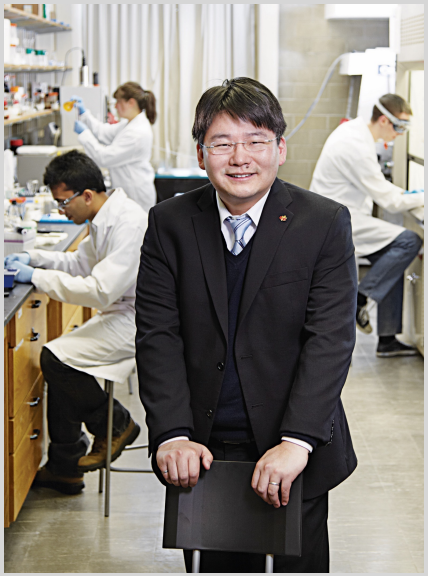
"Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus non sem semper, rhoncus quam nec, suscipit erat. In non scelerisque est. Cras eu sodales mauris."

NAME HERE

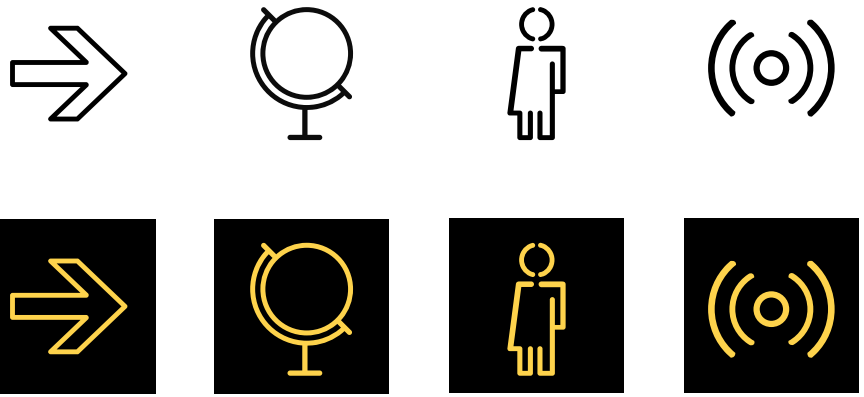
CONTEXT OR THEME

"Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus non sem semper, rhoncus quam nec, suscipit erat. In non scelerisque est. Cras eu sodales mauris."

NAME HERE

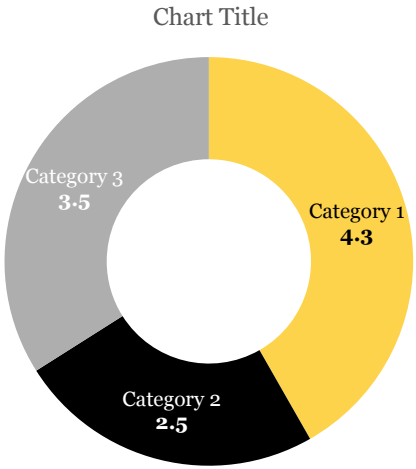


INFOGRAPHIC SYMBOLS / STYLE



UNIVERSITY OF WATERLOO

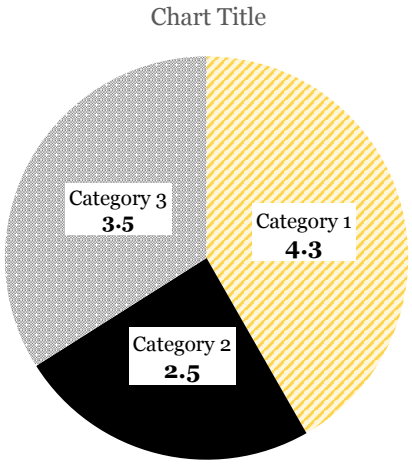
MASTER SLIDE CHART



- Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Maecenas porttitor congue massa.
- Fusce posuere, magna sed pulvinar ultricies, purus lectus malesuada libero, sit amet commodo.

UNIVERSITY OF WATERLOO

MASTER SLIDE CHART (accessible version)



- Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Maecenas porttitor congue massa.
- Fusce posuere, magna sed pulvinar ultricies, purus lectus malesuada libero, sit amet commodo.

UNIVERSITY OF WATERLOO

UNIVERSITY OF WATERLOO

UNIVERSITY OF WATERLOO

YOU+WATERLOO

Our greatest impact happens together.