# Tracking Dependency Updates & Security: Do Bots Make a Difference?

Eimaan Saqib & Jaffer Iqbal

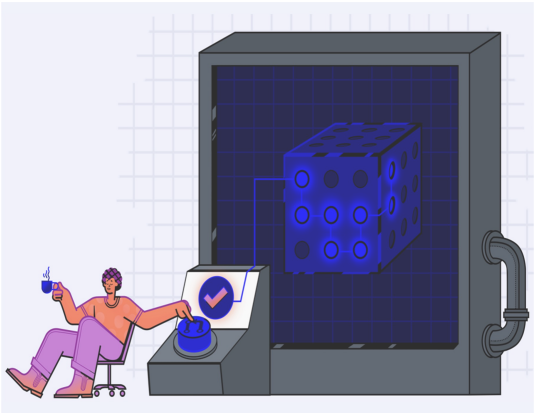
# Background

Risks in dependency management

- Security risks
- Technical debt
- Compliance issues

2021 Log4j vulnerability exposed millions of systems

74% open-source codebases contain at least one open-source vulnerability (2024 Synopsys report)



# Automated Dependency Management Tools

**Automatically open Pull Requests**

**Update dependencies on a collaborative platform like GitHub**

**Why?**

**Dependabot, RenovateBot, SnykBot, Depfu**


# Dataset & Tools

**Goblin Framework (represents libraries and releases)**

**Weaver to compute dependency freshness and vulnerability exposure windows**

**Python libraries for EDA and statistical analysis**

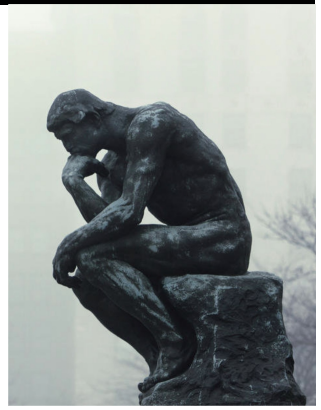
**GitHub API to get configuration files and CI/CD workflows**

# Research Questions

**RQ-1:** How often do projects update their dependencies, and what factors influence this frequency (e.g., project size, popularity, type)?

**RQ-2:** What is the average time taken to patch vulnerabilities in dependencies, and how does this vary across projects?

**RQ-3:** Does the adoption of dependency management bots correlate with reduced dependency update latency and vulnerability exposure windows?



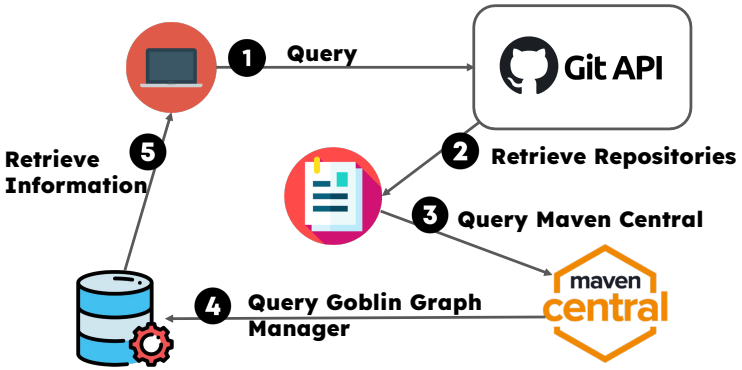
# Phase 1

Establish baseline trends (projects stratified by size, type, popularity, etc.)

Calculate dependency update frequency and vulnerability patching time

Statistical analysis for identifying correlations

# Phase 2




# Phase 3

# Threats to Validity

| | |
|---|---|
| 1: Repositories containing a .yml configuration file (like dependabot.yml) may not actively use the dependency management bot | Verify active bot usage by checking for pull requests authored by the bot, analyzing commit histories for dependency updates, checking config settings |
| 2: Selection bias could skew results | Use control groups of similar project size, popularity, and domain. |
| 3: Causal ambiguity in the findings | Perform longitudinal study to isolate tool impact. |