POSTER: ‘False negative - that one is going to kill you’: Understanding Industry Perspectives of Static Analysis based Security Testing

Amit Seal Ami*, Kevin Moran†, Denys Poshyvanyk*, and Adwait Nadkarni*

*William & Mary, Williamsburg, VA, USA; aami@, denys@cs., nadkarni@cs.wm.edu
†University of Central Florida, Orlando, FL, USA; kpmoran@ucf.edu

Title: ‘False negative - that one is going to kill you’: Understanding Industry Perspectives of Static Analysis based Security Testing

Authors: Amit Seal Ami, Kevin Moran, Denys Poshyvanyk, Adwait Nadkarni

Venue: 2024 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2024

DOI: 10.1109/SP54263.2024.00019


Abstract: The demand for automated security analysis techniques, such as static analysis based security testing (SAST) tools continues to increase. To develop SASTs that are effectively leveraged by developers for finding vulnerabilities, researchers and tool designers must understand how developers perceive, select, and use SASTs, what they expect from the tools, whether they know of the limitations of the tools, and how they address those limitations. This paper describes a qualitative study that explores the assumptions, expectations, beliefs, and challenges experienced by developers who use SASTs. We perform in-depth, semi-structured interviews with 20 practitioners who possess a diverse range of software development expertise, as well as a variety of unique security, product, and organizational backgrounds. We identify 17 key findings that shed light on developer perceptions and desires related to SASTs, and also expose gaps in the status quo - challenging long-held beliefs in SAST design priorities. Finally, we provide concrete future directions for researchers and practitioners rooted in an analysis of our findings.

Understanding Industry Perspectives of Static Analysis-based Security Testing

Amit Seal Ami1, Kevin Moran4, Denys Poshvyanky4 and Adwait Nadkarni5
1William & Mary, 4University of Central Florida

1ami@, denys@cs, nadkarni@cs.edu, kpomaran@ucf.edu
https://amisebamis.com

Introduction
• Increasing Reliance on program analysis for security, e.g., SASTs
• SASTs suffer from design and implementation flaws
• We have a Limited Understanding of the Perceptions, Expectations, and Beliefs regarding SASTs

Research Questions
• How are SASTs chosen at organizations with different business and security needs?
• What do practitioners know and believe about the limitations of SASTs?
• How do practitioners navigate, address, or work around flaws of SASTs?

Findings
Selecting SASTs

F04 - Participants generally avoid selecting SASTs due to design and implementation flaws, such as uncontrolled variables, client-side vulnerabilities, and cost. Practitioners believe a flawed SAST won't impact them because they can work around flaws of SASTs.

Reducing False Negatives vs False Positives

F15 - Practitioners generally are more tolerant of false positives than the 20% upper bound proposed in literature. They believe that some findings are not real vulnerabilities and can be dismissed.

Effective False Positives and SAST

F12 - Practitioners are generally against letting developers define “effective” false positives, or letting them decide when to run SASTs. They want SASTs to be reliable and accurate.

Addressing/Reporting flaws to SASTs

F15 - Participants may hesitate to report flaws/false negatives for several reasons, e.g., prior negative experiences with SASTs, including interaction on reported flaws; issues internal to the organization, such as the need to maintain product consistency without an explicit NDA; red tape, and the lack of incentive to perform the additional effort.

Exploiting Flaws and Evasive Developers

F13 - The risk of evasive developers is real. That is, while some practitioners consider the scenario of “evasive developers” as adequately predicted by existing code-reviewer, this optimism is not universal. Others have prior experience of evasive developers in their teams, or have advised SASTs themselves.

Methodology

Survey: Participants completed a semi-structured interview to gather data about their practices, perceptions, and beliefs regarding SASTs.

Interview: Participants were asked about their experiences and beliefs regarding SASTs.

Purpose

Learn about
• Participant, project, and organization
• Security and Organization
• Organizational Context of SASTs
• Limitations and Expectations about SAST
• Impact of Unsound SAST
• Challenges and Improvements relating to the SAST

Participents

• Developers - Spread across Asia, Europe, the United Kingdom, and North America
• Developers - Working in Local or International Projects
• Developers - Different Business and Security Needs
• Developers - Different Industry Contexts
• Developers - Working in Local or International Projects
• Developers - Diverse Security contexts, etc., compliance

Takeaways

Pioneers tend to rely on ad-hoc/subjective criteria. A solid preference for security is universally expressed. BUT, that is not reflected in the selection process of SASTs.

Unreasonable Optimism and Trust
in Reputation of SASTs dissuade pioneers from evaluating SASTs.

Benchmarks are insufficient
Developers interested in evaluating SASTs lack the means.

Developers want (a) ease of use and (b) SASTs to detect vulnerabilities.

Paradoxical Takeaway - Industry is not Ready for Flaws of SASTs

1. Practitioners use SASTs to cover blind spots, subjective bias, and knowledge gaps in manual analysis, i.e., detect vulnerabilities they are unaware of.
2. Practitioners believe a flawed SAST won’t impact them because they can find the remaining vulnerabilities using manual analysis.

References