ČVUT
ČESKÉ VYSOKÉ
UČENÍ TECHNICKÉ
V PRAZE

SUPERVISOR‘S OPINION OF FINAL THESIS

I. IDENTIFICATION DATA

Thesis name:	Analysis of tools for static security testing of applications
Author's name:	Leonid Golovyrin
Type of thesis :	bachelor
Faculty/Institute:	Faculty of Electrical Engineering (FEE)
Department:	Department of Computer Science
Thesis supervisor:	Ing. Josef Kokeš, Ph.D.
Supervisor's department:	Faculty of Information Technology, Department of Information Security

II. EVALUATION OF INDIVIDUAL CRITERIA

Assignment **ordinarily challenging**

Evaluation of thesis difficulty of assignment.

I consider the assignment to be of about average complexity. The actual execution of the assignment can be made more or less complex, depending on the student's intentions.

Satisfaction of assignment **fulfilled**

Assess that handed thesis meets assignment. Present points of assignment that fell short or were extended. Try to assess importance, impact or cause of each shortcoming.

The assignment was fulfilled.

Activity and independence when creating final thesis **D - satisfactory.**

Assess that student had positive approach, time limits were met, conception was regularly consulted and was well prepared for consultations. Assess student's ability to work independently.

The student opted for an almost completely independent work, the consultations were few and far between. I don't consider that a problem, especially in our field where many people prefer to work in this fashion, as long as the student accepts responsibility for the results.

Technical level **B - very good.**

Assess level of thesis specialty, use of knowledge gained by study and by expert literature, use of sources and data gained by experience.

While the early parts of the thesis (esp. chapter 2) seem rather shallow, I am quite happy with the later parts (esp. chapters 5 and 6). It may not be obvious at a first glance, but there is a lot of specialized work hidden behind the scenes, e.g. the evaluation of SAST tools results in chapter 6.1 or the preparation of scenarios for evaluation in chapter 6.2. Even chapter 2, which I find the least comprehensive, makes sense – a thesis has time and space constraints and I can accept that the student had to sacrifice some details to fit.

Formal and language level, scope of thesis **A - excellent.**

Assess correctness of usage of formal notation. Assess typographical and language arrangement of thesis.

The technical aspects of the thesis text are very nearly perfect. I did notice a few places where the language could be improved, but that's true for any work and overall, I think the ratio or “correct” vs. “incorrect” is much better in this thesis than in most other theses.

Selection of sources, citation correctness **B - very good.**

Present your opinion to student's activity when obtaining and using study materials for thesis creation. Characterize selection of sources. Assess that student used all relevant sources. Verify that all used elements are correctly distinguished from own results and thoughts. Assess that citation ethics has not been breached and that all bibliographic citations are *complete and in accordance with citation convention and standards.*

I consider the student’s selection of sources a reasonable one. The identification of external sources is correct in the text of the thesis. It is much less clear in the code, even after checking the commit history I am not quite sure if the plugin examples are the student’s own work or not.

Additional commentary and evaluation

Present your opinion to achieved primary goals of thesis, e.g. level of theoretical results, level and functionality of technical or software conception, publication performance, experimental dexterity etc.

Overall, I am quite happy with the thesis as a whole. It’s not a typical software-engineering thesis, but I do think that the subject matter is an important one and I am glad the student performed quite an extensive research and testing towards the possibility of applying SAST as a part of the CI/CD pipeline of a project. Especially the experiment conducted with real-world developers is very useful.

A few minor aspects to consider for future improvement:

1) The documentation on how to integrate the created template with an existing codebase needs to be more comprehensive. Appendix B is way too short and incomplete. In particular, the user needs to study the sources to discover that they are supposed to save their source code into the “corpus” directory.

2) When pushing changes to the project to a repository, I would recommend rebasing to keep logical units together rather than as a sequence of commits (e.g. bff5db3 to c38fd20 would be better combined into one commit) and to add reasons to the commit messages (e.g. what’s wrong with the original code that commit af3c634 needs to fix).

III. OVERALL EVALUATION, QUESTIONS FOR DEFENSE, CLASSIFICATION SUGGESTION

Summarize thesis aspects that swayed your final evaluation.

I evaluate handed thesis with classification grade **B - very good.**

Date: 10.6.2023 Signature: