THESIS REVIEWER'S REPORT

I. IDENTIFICATION DATA

Thesis title:	**Analýza nástrojů pro statické testování bezpečnosti aplikací**
Author's name:	**Leonid Golovyrin**
Type of thesis :	bachelor
Faculty/Institute:	Faculty of Electrical Engineering (FEE)
Department:	Department of Computer Science
Thesis reviewer:	Ing. Karel Frajták, PhD
Reviewer's department:	System Testing IntelLigent Lab

II. EVALUATION OF INDIVIDUAL CRITERIA

Assignment	**ordinarily challenging**
The assignment is not very challenging. The goal of the thesis was to analyze the tools for security testing and to implement a practical project demonstrating selected tools.	

Fulfilment of assignment	**fulfilled with major objections**
The primary goals were achieved. The research part is quite extensive and well written, though it covers only 4 selected tools. The implementation part is minimalistic. I do not understand why the experiment was conducted the way it is described in the thesis or why it was conducted at all. I understand usability may be a key concern when using a tool, but in security testing other there is an aspect that is more important – coverage.	

Methodology	**Choose an item.**
The author's approach to the problem is correct.	

Technical level	**E - sufficient.**
The research part demonstrates some scientific approach when comparing various SAST tools, the technical part is very limited consisting of just few CI scripts.	

Formal and language level, scope of thesis	**B - very good.**
The thesis is well written and organized. The language is understandable. The level of English is quite high. Author could have provided examples of the code of the rules for individual tools, while this plays significant role in the experiment, the reader is kept in the dark.	

Selection of sources, citation correctness	**A - excellent.**
Sources are correctly cited. Bibliographic citations meet the standards.	

Additional commentary and evaluation (optional)
The link to questionnaires and results on page 46 does not work. The task given to participants of the experiment is in my opinion incorrect and does not demonstrate the exploit and the code to prevent it. The author chose `deluge' as project to demonstrate the proposed solution, the project is said to have a history of security issues (3 in total), while there is an OWASP benchmark project designed to evaluate the accuracy, coverage, and speed of automated software vulnerability detection tools and thus containing many security issues.

III. OVERALL EVALUATION, QUESTIONS FOR THE PRESENTATION AND DEFENSE OF THE THESIS, SUGGESTED GRADE

Questions for student:

1. Why was the usability experiment carried this way?
2. Why the OWASP benchmark project was not chosen for the evaluation?
3. Can you fix the example code that was given to the participants of the experiment?

The grade that I award for the thesis is **C - good.**

Date: **29.5.2023** Signature: