FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Review report of a final thesis

Reviewer:	Ing. Simona Fornůsek, Ph.D.
Student:	Oliver Šmakal
Thesis title:	Automated Vulnerability Scanning of Web Applications
Branch / specialization:	Computer Security and Information technology
Created on:	5 February 2023

Evaluation criteria

1. Fulfillment of the assignment

▸ [1] **assignment fulfilled**
[2] assignment fulfilled with minor objections
[3] assignment fulfilled with major objections
[4] assignment not fulfilled

All the points of the assignments are fulfilled, thesis is well structured, and follows the assignment.

2. Main written part 89/100 (B)

The thesis is well structured and easy to follow. I only have a remark to Chapter 1 describing the nature of SQL and XSS attacks - as this should be one of core parts of the thesis, I would expect more details, including examples, and implementation detail of the attack. However, it is no doubt student have studied and understood all the types of the attacks, which is also proved by the list of bibliography used, which is considerably rich for the bachelor thesis.

3. Non-written part, attachments 90/100 (A)

Since the implementation is in form of ZAP plugin, it is very well usable practically, as the ZAP is commonly used web app tool nowadays. The technology used is therefore well suitable and adequate.

4. Evaluation of results, publication outputs and awards 90/100 (A)

The implemented plugin might be used in practical web applications scanning scenarios.

The overall evaluation

90 /100 (A)

The thesis is very well made. It's easy to follow, informationally rich, student processed a significant amount of bibliography. The implemented plugin is practically usable. Therefore, I recommend thesis for defense and propose the grade A.

Questions for the defense

Why you have chosen XSS detection?
How your implementation decisions would differ, if you have chosen SQL detection, if at all?

Instructions

Fulfillment of the assignment

Assess whether the submitted FT defines the objectives sufficiently and in line with the assignment; whether the objectives are formulated correctly and fulfilled sufficiently. In the comment, specify the points of the assignment that have not been met, assess the severity, impact, and, if appropriate, also the cause of the deficiencies. If the assignment differs substantially from the standards for the FT or if the student has developed the FT beyond the assignment, describe the way it got reflected on the quality of the assignment's fulfilment and the way it affected your final evaluation.

Main written part

Evaluate whether the extent of the FT is adequate to its content and scope: are all the parts of the FT contentful and necessary? Next, consider whether the submitted FT is actually correct – are there factual errors or inaccuracies?

Evaluate the logical structure of the FT, the thematic flow between chapters and whether the text is comprehensible to the reader. Assess whether the formal notations in the FT are used correctly. Assess the typographic and language aspects of the FT, follow the Dean's Directive No. 52/2021, Art. 3.

Evaluate whether the relevant sources are properly used, quoted and cited. Verify that all quotes are properly distinguished from the results achieved in the FT, thus, that the citation ethics has not been violated and that the citations are complete and in accordance with citation practices and standards. Finally, evaluate whether the software and other copyrighted works have been used in accordance with their license terms.

Non-written part, attachments

Depending on the nature of the FT, comment on the non-written part of the thesis. For example: SW work – the overall quality of the program. Is the technology used (from the development to deployment) suitable and adequate? HW – functional sample. Evaluate the technology and tools used. Research and experimental work – repeatability of the experiment.

Evaluation of results, publication outputs and awards

Depending on the nature of the thesis, estimate whether the thesis results could be deployed in practice; alternatively, evaluate whether the results of the FT extend the already published/known results or whether they bring in completely new findings.

The overall evaluation

Summarize which of the aspects of the FT affected your grading process the most. The overall grade does not need to be an arithmetic mean (or other value) calculated from the evaluation in the previous criteria. Generally, a well-fulfilled assignment is assessed by grade A.