FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Review report of a final thesis

Reviewer:	Ing. Michal Polák
Student:	Konstantin Shadakh
Thesis title:	Security Analysis of Data Stewardship Wizard Project
Branch / specialization:	Computer Security and Information technology
Created on:	9 February 2024

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

The thesis contains most of the analysis requested in the assignment within sufficient depth. However some parts such as dependency checks or static code analysis are not described enough in my opinion. On the other hand the amount of work submitted in the thesis is still substantial especially for bachelor's thesis and no particular part is missing. As such I believe that the student fulfilled the assignment.

2. Main written part

90 / 100 (A)

From the formal side the thesis is very well written. It doesn't suffer from grammatical errors and other then few listings split on multiple pages is formatted properly. However the thesis begins with substantial amount of almost poetic language such as "sanctity of research data" or "born out of genuine concern" which I found almost disturbing to the reader. However this lasts only for a few pages. Regarding the contents I think that some parts like a static code analysis or technology recommendations could be described more, because from the thesis itself the depth of analysis is unclear. From the technical point of view, there is a misconception between DoS and DDoS in section 6.2.5, however student managed to successfully find DoS vulnerability in the next section. Also some of the critique of the DSW like in the section 6.2.8 is easily remediated by using TLS, which the thesis does not mention. Outside of these minor objections, I think the technical part of the thesis is more then sufficient.

3. Non-written part, attachments 80 /100 (B)

I would like to praise author for including the audited version of DSW. However I believe that including scripts that would allow reader to easily replicate each attack described or at least full logs of these attacks is also necessary.

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

The student managed to identify real vulnerabilities, even high priority ones. As a result, practical impact of this thesis is undeniable.

The overall evaluation 92 /100 (A)

The submitted thesis is very well written and with real world impact. Other than some minor errors and parts that would deserve a bit more attention, I believe the scope of the work exceeds the expectations for a bachelor's thesis. The assignment was fulfilled. It is pity that automated scripts to replicate the tests or logs providing with the full scale results of each test are missing. However I still believe that this work should be evaluated with the highest grade.

Questions for the defense

1) Why do you think that the regular internal audit of DSW did not manage to find vulnerabilities discovered in your thesis?
2) You have found server side template injection vulnerability and marked it as medium severity while bruteforce attacks are marked as high. Is the arbitrary code injection less severe? Why?
3) In section 5.2 you point out the unfortunate use of AES cipher in counter mode without proper initial vector. What could be the practical impact of such vulnerability?

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.