



Supervisor's statement of a final thesis

Supervisor: Ing. David Knap
Student: Jan Sedláček
Thesis title: Design of Commercial Bug Bounty Program
Branch / specialization: Computer Security
Created on: 21 May 2021

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 assignment was fulfilled without any objections.

2. Main written part

85 /100 (B)

All parts of the thesis are useful for the goal, there are no unnecessary parts. While list of references makes use of fewer traditional media than usual, it is in this case well acceptable, as bug bounty is a relatively new field and there is still a lack of serious publications; despite that, all statements and quotes are still well referenced and supported by relevant sources. From the language perspective it is clear that the author is not a native English speaker, especially by extensive use of Czech idioms that don't share the exact same meaning or sense in English; and even while there are little to no typos in general, the thesis could use more delicate review in terms of capitalization consistency and overall form. On the other hand, the content itself is surely professional and aggregates a lot of useful information about this field of cybersecurity that is not easily available elsewhere. I especially appreciate the comparison with other cybersecurity testing fields, as it helps to better outline advantages and limits of bug bounty, and its connection to other means of testing.

3. Non-written part, attachments

85 /100 (B)

The later parts of the thesis assess pros and cons of current major bug bounty platforms, try to identify weak points present and offer solution. Some of the projects are here criticized for low amount of participating companies, but this topic is unfortunately not later discussed when designing yet another platform that could split the market even

further. Nonetheless author presents some innovative ideas, especially a new scoring system for hackers that would take into consideration not just achieved education and certifications, but also the practical work on bugfinding itself. This can allow also participation of talented hackers that don't have social background for traditional certificates worth thousands of dollars, and relieve the pressure on cybersecurity experts in the beginning of their career.

4. Evaluation of results, publication outputs and awards 85 /100 (B)

The requirements and user stories laid out in the final part of the thesis can be used as a starting point for a small start-up or for a new service for established security company and serve as a good base for further detailed documentation.

5. Activity of the student

- ▶ [1] **excellent activity**
- [2] very good activity
- [3] average activity
- [4] weaker, but still sufficient activity
- [5] insufficient activity

The author was working on thesis throughout the semester and delivered results well ahead of time.

6. Self-reliance of the student

- ▶ [1] **excellent self-reliance**
- [2] very good self-reliance
- [3] average self-reliance
- [4] weaker, but still sufficient self-reliance
- [5] insufficient self-reliance

The author was working mostly on his own and did not require any major steering at any point.

The overall evaluation 85 /100 (B)

Comparative thesis topics are often the easier ones, but this one is focusing on unexplored area where not many authors have yet published. It captures a snapshot of a new cybersecurity field that is still emerging and attempts to help to define and shape it. The form is a little bit lagging behind the content, but overall the thesis is beneficial to the field, as author attempts to bring new ideas to bug bounty expansion and suggests how to open it not just to already established experts, but also to amateur enthusiasts.

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. 26/2017, 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.

Activity of the student

From your experience with the course of the work on the thesis and its outcome, review the student's activity while working on the thesis, his/her punctuality when meeting the deadlines and whether he/she consulted you as he/she went along and also, whether he/she was well prepared for these consultations.

Self-reliance of the student

From your experience with the course of the work on the thesis and its outcome, assess the student's ability to develop independent creative work.

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.