Secure Software Engineering Individual Assignment 3

Course Name: Secure Software Engineering
Course Code: COMP SCI 4412/7412
Assessment Component: Assignment 3 (15%) - Individual Assessment
Release Date: 20/09/2023
Due Date: 18/10/2023 by 11:55pm
Submission: MyUni

Part 1 (7 points)

1. Study about strings vulnerabilities, *i.e.*, **Buffer Overflow** and **Arc Injection**, on Common Weakness Enumeration and related websites;

2. Identify 3 security threats in open-source GitHub repositories. Each type of vulnerability must have at least one source code file. The projects must satisfy the following conditions:

   - The programming languages must be either C or C++
   - The repository has more 100 stars and 10 contributors on GitHub

3. Include the following artifacts about each file you have found in the report:

   - Link to the file
   - Link to the commit that fixes the vulnerable file
   - Name of the file
   - The programming language used in the file
   - Name of the repository
   - Number of repository stars
   - Number of contributors in the repositories
   - Type of vulnerability (CWE)

4. Pinpoint the code lines within the source code files you have identified that contain the vulnerabilities you found.

5. Also enter the information you have found in tasks 3 and 4 into the link for Assignment 3 Part 1 on MyUni along with your name and student ID to avoid duplicate submission.

6. Explain how the vulnerable lines correlate to the definition or causes of the vulnerability you have studied

7. Show how to fix the vulnerability and explain in details. It is not mandatory that the fix has to be executable, but the explanation must be reasonable. If there is already a fix available, explain how this fix complies with the standard mitigation techniques for the vulnerability.

8. Write your findings in the report.

9. Please visit the link for Assignment 3 Part 1 on MyUni to input your identified vulnerable source code files *as soon as possible* after you find them. You can do the analyses and put your findings in the report later (but still before the deadline). The student who submits earlier will claim the authorship of the source code file and the later ones must choose a different file to work on. In case you accidentally select the same source code file, there will be a red flag to notify you.

Part 2 (8 points)

1. Based on the threat modeling case study in the Working Session 3, select one software system of your choice
    - Identify and draw a use case diagram, with at least 5 misuse cases included
    - Write down the description of the (mis)use cases
    - Draw a data flow diagram with at least 5 external entities and 5 processes using Lucidchart
2. Identify three security threats in the data flow diagram
3. Perform the following tasks
    - Briefly describe the software system you have chosen
    - Explain each security threat in details
    - Include a use case diagram containing the misuse cases related to your identified threats (You should highlight such misuse cases.)
    - Include a data flow diagram containing your identified threats (You should specify the entities, processes and data stores involved. It is ok if some elements are missing.)
    - Assess the risk of each security threat using the threat library of EMC and/or Common Vulnerability Scoring System (You should mention which assessment framework you are using)
    - Describe how you can potentially fix each security threat
4. Write your findings in the report

The report of this activity should be in A4-size page with Times New Roman or similar font size 12. The first page of the report should include your full name and student ID.

Tips about how I would go about doing this activity:

Part 1

I will first study about the vulnerabilities mentioned in the task on Common Weakness Enumeration website. Google is also always worth a try if I want to explore more. Then, I will try to use the name of the vulnerability and search it on GitHub. After I find the repositories, I will filter them using the above criteria. Then, I will focus on the vulnerable files and analyze them line-by-line or use existing tool. If there is already a fix for that vulnerability, I will include it in my report. Otherwise, I will try to see how I can fix it using the mitigation techniques I have learned for the vulnerability. I will explain how my findings match with the materials I have learned for that vulnerability. Most importantly, I will try to input my identified source code files the link for Assignment 3 Part 1 on MyUni as soon as I find them to avoid duplication and having to search again.

Part2

I will choose a system and draw a use case diagram. Then, I will try to identify as many security threats as possible in the data flow diagram. After that, I will try to relate the security threats to the misuse cases in the use case diagram. I will also see how I can use the threat library of EMC with CVSS (in the slides of seminar session 5 and reading material) to assess the risk of each security threat. Then, I will think about how I can mitigate these security risks as a developer. I can utilize the materials in seminar sessions, vulnerability demos as well as the experience I have gained from assignment 1 and assignment 2 to figure out the solutions. Finally, I will put all of the results along with relevant diagrams in the report.

Please note that answer without explanation would not receive any point.

How to Submit: The assignment will be submitted via Canvas as there is an upload facility created for this assignment on Canvas.

This assignment is designed to help you to achieve the learning outcomes #3 and #4 in the course outline.