ENPM 809W – Introduction Secure Software Engineering Final Exam

Final Exam

Now that you have fully covered all the security topics, implemented a project and performed a code review of your colleague's code bases, for the final exam you will apply all the skills, knowledge and practical experience to performing one final code review of a real-world software system.

The **project** you will be reviewing will be: **Sonarr**

URL: https://github.com/Sonarr/Sonarr/tree/develop

Git URL: https://github.com/Sonarr/Sonarr.git

Branch for review: **develop** branch

Important Deliverable and Due Date:

Deliverable	**Due Date and Time**
Final Exam Code Review Spreadsheet	*December 15, 2021 by 11:59 PM (No exceptions!)*

Grading Criteria

	Grading Criteria
Final Exam	20% of your course grade. Depends on: • The quality of findings and description from the code review. • The quality of proposed fixes based on the findings. • Timely submission. • What your colleagues in the class find (out of all the valid findings, if one of your colleagues find more, you will be expected to also find all of the same findings).

Final Exam: Code Review

For the final exam, you are assigned the application stated at the top of this document with the given Git branch and you will perform a Secure Code Review for only that branch.

An Excel spreadsheet has been provided as a template for you to fill out, where you will record any findings and related details you come across as you perform the secure code review for the application that pertain to the categories given below.

- Categories to use for the code review:
    - Input Handling
    - Cryptography
    - Authentication

- Authorization
- Session Management
- Error Handling
- Logging
- Debug

Secure Code Review

Now you will perform a secure code review based on your own manual code review and analysis as well as any code analysis tools you choose to use to find issues related to the security categories listed above. An Excel based spreadsheet template for the final exam is also provided. You are ***required*** to fill out the ***given spreadsheet*** and the two sections: Code Review Information and Code Review Findings.

The Findings section of the spreadsheet has the following columns:

- **CWE-ID** = This should ONLY include the CWE-ID. For example: CWE-20.
- **Security Category** = This should ONLY include the Category from the list given above.
- **Filename** = A single filename or multiple filenames separated by semicolon or N/A. For example: Test.cs; Main.cs. The CWE-ID must be directly applicable in all the findings in the files specified.
- **Line number: Position** = A range or list of line number: position values separated by comma or dashes or N/A reported per file. This is then repeated for any additional files specified separated by semicolon. For example:
  - Filename = Test.cs; Main.cs
  - Line Number: Position = 9:3,11-13; 21.
- **Description** = This field should be very detailed on what security issue is found and why it is a real issue (for example, if an attack cannot take advantage of the weakness, it should not be included as a finding). This should include the consequence of a weakness or what could happen attack-wise to the software system.
- **Technical Impact** = Each weakness CWE has a potential technical impact associated with it. What is the technical impact for the weakness you have chosen specifically with regards to the application you are reviewing? If there are multiple, choose the one that is most detrimental to the application.
- **Criticality** = Critical, High, Medium, Low, Info. You should choose this based on the potential technical impact an attack (that you identified in the Description and Technical Impact above) can have on the application.
- **Potential Mitigation** = This field should include how a potential fix could be implemented to avoid the weakness identified. This should be as specific as possible. For example, if input validation or filtering needs to be performed using regular expressions (regex), then the exact regex need not be specified.
- **Comments** = Your comments on the finding to the developer of the project.

Remember the following guidelines:

- If you have the same finding multiple times, you must report three of those as separate findings, and any additional instances as a single additional finding (fourth finding) with a list of filenames and line numbers as given above.
- You must choose the correct specific weakness and applicable location. While some findings may not have a specific location, N/A may be used.
- While the same exact location may contain many weaknesses, each of those must be listed as a separate finding if each of those weaknesses are able to be exercised as an attack.
- For a weakness occurring on a range of lines, use the – to specify a range of line numbers. For a weakness occurring in multiple different lines, use the comma (,) to specify all applicable line numbers within the given file. In general, each row should really only contain one filename.
- For the same finding across multiple files, just create a new row for each filename that contains the finding and repeat it, modifying any details as necessary to reflect the correct details.
- Do not just use descriptions from the CWE website.

Submission Criteria

Please upload an Excel spreadsheet file ending in the xlsx extension. Please fill out the Review Information section for the cells specified as 'FILL THIS'. Also put all your findings in the Findings section.

Important: Please name the Excel spreadsheet as FinalExam_<UMD Email ID>.xlsx. For example, 'FinalExam_gkini.xlsx'. Make sure your submission is updated to include the following:

- Your Name (Example: Gananand Kini)
- Your UMD email id (Example: gkini@umd.edu)
- The content for the report excel document as outlined above.