**School of Computing (SoC)**

**ESDE - Enterprise Systems Development - Secure Coding**

**2020/2021 Semester 2**

**Assignment (Part 1 - Secure Coding)**

**Instructions and Guidelines:**

1. This is a group assignment (2 per group by default) to be handed in by **3rd January 2021, 12 pm**. The assignment part 2 will be released immediately after the deadline.
2. The assignment part 1 *together with* assignment part 2 contributes towards 30% weightage of your overall module result.

Assignment part 1

|  |  |
| --- | --- |
| Report for assignment part 1 | 80% |
| Presentation for assignment part 1 | 20% |

1. Students are required to submit a softcopy of their work via the course website in BlackBoard.

|  |
| --- |
| Report |
| Zip file which contains your own NodeJs version of the project which addresses the vulnerabilities. The project must include the **node\_modules** files because the respective markers **will not** be doing any **npm install** to install the packages. |

1. The interview will be conducted the week: **4th Jan 2020 to 8th Jan 2020** during lesson.Students are expected to explain their work.

5. **No marks will be awarded**, if the work is copied or you have allowed others to copy your work. Warning: Plagiarism means passing off as one's own the ideas, works, writings, etc., which belong to another person. In accordance with this definition, you are committing plagiarism if you copy the work of another person and turning it in as your own, even if you would have the permission of that person. Plagiarism is a serious offence and disciplinary action will be taken against you. If you are guilty of plagiarism, you may fail all modules in the semester, or even be liable for expulsion.

6. Absent for presentation without valid LOA during the two lesson slots timetabled during that period will have 50% of overall assignment part 1 marks deducted.

7. 50% of the marks will be deducted for assignments that are received within ONE (1) **calendar day** *after* the submission deadline. No marks will be given thereafter. Exceptions to this policy will be given to students with valid LOA on medical or compassionate grounds. Students in such cases will need to inform the lecturer as soon as reasonably possible. Students are not to assume on their own that their deadline has been extended.

**1. Objectives**

Background information

An organization is hosting a global design competition. Participants can register as user in a hosted system, Bee Design Award Competition system to submit the design files. The system has two user roles. The roles are admin and user. The competition committee wants the IT department to make the existing system more secure. Incidents such as information theft and sabotage has severe impact. You are a member in a team which will **code-review** the system's code and **perform vulnerability tests** to give the competition committee an assurance on the preventive measures. Key challenge: The organization boss is **not IT literate** at all. Yet, he still wants to read the report and feel the assurance.

The goal of this assignment is for you to apply your ➀code review-analyzing and ➁web penetration skills for secure coding on a web project. A web project with source codes is provided for you to analyze. You can deploy and test the web application and review the source codes and find out the security vulnerabilities of the program. In the report, identify the web pages and the code which constitute a security vulnerability. Suggest fixes for the flaws, providing code snippets as necessary inside the report.

Your report must indicate:

➀ Step-by-step on *how* the flaw can be exploited

➁ Where the flaw is found (web page name and code)

➂ Suggestion(s) on how the flaw can be resolved.

➃ Evidences (pictures and code snippet) on the results *after* the flaw has been addressed.

For the presentation, you are to demonstrate how the vulnerability **(your assigned category**) can exploited by a malicious hacker through running the web app on your laptop. A realistic demo showcasing the impact severity on the exploit will garner higher marks. For this part, you have to demo and show the particular vulnerability is fixed in the actual project by running the web app and executing the supposed attack.

Your report must address **1 vulnerability for each category** listed below

*Reference: https://www.owasp.org/index.php/Top\_10-2017\_Top\_10*

1) Injection (SQL Injection)

2) Broken Authentication

3) Sensitive Data Exposure

4) Broken Access Control

5) XSS

6) Insufficient Logging & Monitoring (Requires own research)

7) Others

Your report should have a **brief introduction** on how you can improve the **entire** project on two areas: (a) Poor error handling which is usually caused by nested callbacks (b) Inconsistent JSON response data structure due to a system done by more than two developers and each uses their own style. You are required to modify the project to showcase how your code structure can prevent future vulnerabilities when developers need to *add* new functionalities or new API methods for the backend project.

When evaluating the **security of the website**, please address all of the following elements:

* Type of flaw detected
* How it can be exploited specifically (demo with screenshots)
* Identify the code snippet which caused the vulnerability (if applicable)
* Recommendation
* Code snippets to solve the vulnerability (Prepare your own project to showcase the improved version)
* Tools and methods you employed to test the web system.

Your grade for this assignment will be based on the **thoroughness and clarity** of your discussion of ALL of the elements above.

A sample penetration testing report format can be found at: <http://www.cstl.com/CST/Penetration-Test/CST-Web-Application-Testing-Report.pdf>

Section 4 on detailed findings is an example of how your report might focus on and should cover for secure coding.

Pdf containing an example of how you can write the detailed finding can also be found in the same assignment folder.

Reminder: Know your target audience. Do not *blindly* reuse the examples. The business owner has no IT background. The business owner need to fork out a budget to fix the web application. Therefore, the business owner will definitely read the report thoroughly (many times) to feel the severity and consult IT professional friends.

**2.** Code Review

Fix the node project to address the one of the following issues to prevent future vulnerabilities:

(a) Developers do not have **standardized way** to returning JSON data. How to apply a standardized technique so that future vulnerabilities can be reduced when new functionalities are added into the system.

(b) Very bad error handling techniques is seen inside the project. As a result, attackers who uses automated tools will "hang" the hosted project for many days.

(Hint: the REST API code which handlers the pagination feature has more stable error handling because **async** and **await** technique was applied to replace the callbacks. Unfortunately, it is still partial solution. A good video reference can be found at <https://youtu.be/V_Kr9OSfDeU> )

**3. Interview/Presentation (20 marks)**

In this session, please address the following elements:

* Demo of how a malicious user can exploit your system for the category(topic) you are assigned
* How the exploit can be addressed

Please note this should include a live demo using the application, before and after the code fix is employed in the code.

**- End -**