**Application Security Assignment & Case Study Specification**

**Introduction**

This is an **individual** assignment and case study.

This project aims to equip students with the skills and knowledge to protect software application code and data against cyber threats.

The project consists of the following parts.

* Part 1: Assignment Submission (20%) - Week 06
* Part 2: Assignment Presentation & Demonstrations (10%) - Week 07
* Part 3: Case Study Interim Submission (20%) - Week 12
* Part 4: Interim Presentation & Demonstrations (10%) - Week 13
* Part 5: Case Study Final Submission (20%) - Week 16
* Part 6: Final Presentation & Demonstrations (20%) - Week 17

**Part 1: Assignment Submission (20%)**

Problem Statement  
You are to develop a functional MVP (Minimum Viable Product) Web App (Backend Only – using NodeJS technologies ) to demonstrate your understanding of Authentication and Authorization in a Web App. The MVP web application is to be used as a Register/Login/Logout Endpoint for a company of your choice. (The front-end of the Web App will be developed later in the course.)  
You are free to choose any company. The selected company can be real or fictitious.

Your MVP Backend Endpoint should meet the following minimum requirements:

* Registering new users (An Admin role + 3 other different roles are required)
* Logging in of users
* Specific user-protected Endpoint (ie. Each user role will have at least ONE specific endpoint that only he has the authority to access. If such authority is absent, that particular endpoint will send back an error response. )

Refer to LMS for submission details

The deadline for Part 1 submission is on **Week 6, 30th May (Friday) 2025 at 2359HRS.**

**Part 2: Assignment Presentation & Demonstrations (10%)**

You are to do a 5-10 min presentation and demonstration of your MVP Backend Endpoint. You must be prepared to show and explain your codes when requested during the presentation. You are to use the Postman App or equivalent to demo the functionalities of your endpoint.

**Part 3: Case Study Interim Submission (20%)**

You are to develop a functional MVP Web App (Backend + Frontend). The MVP web application frontend will be used as a Register/Login/Logout Endpoint for the company of your choice. You are free to use any JS/CSS libraries if necessary.

Your MVP (Minimum Viable Product) Frontend Web App should meet the following minimum requirements:

* Registering new users (An Admin role + 3 other different roles are required)
* Logging in of user
* Logging out of user
* Specific user-protected Web page (ie. Each user role will have at least ONE Web page that only he has the authority to access. If such authority is absent, the user will be re-directed to the login page.)

Refer to LMS for submission details.

The deadline for Part 3 submission is on **Week 12, 11 July (Friday) 2025 at 2359HRS.**

**Part 4: Case Study Presentation & Demonstrations (10%)**

You are to do a 5-10 min presentation and demonstration of your MVP Web App. You must be prepared to show and explain your codes when requested during the presentation. You are to use the Frontend Web App to demo the functionalities of your entire WebApp.

**Part 5: Case Study Final Submission (20%)**

You are required to submit your **case study source codes (refer to LMS for additional instructions)**

Your Case Study will be assessed based on the following components:

* Complete the “Capture The Flag” by successfully exploring the top 10 security risks associated with APIs according to the OWASP API Security Project. (Refer to sign-up/login instructions in LMS) (5%)
* Implement up to 3 OWASP security measures to Part 4 web app. (15%)

Submit the entire project folder as a zipped file in LMS under the Assessment folder. Please ensure that you have a backup copy of your application in case there is a problem with the online submission. You are to also create a Youtube Demo Reel (<15min) with narration for the security measures implemented in your Web App. Please refer to LMS for additional instructions

The deadline for program codes final submission is on **Week 16, 8 August (Friday) 2025 at 2359HRS.**

**Part 6: Presentation and Demonstration (20%)**

You are to do a 10-15 min presentation and demonstration of your completed application and the OWASP slides. You must be prepared to show and explain your codes when requested during the presentation.

**Penalty for Late Submission**

late and <1 day: 10% deduction from absolute mark given for the assignment late >=1 and <2 days: 20% deduction from absolute mark

late >=2 days : No marks awarded

**Project - Grading Criteria**

The grading criteria for Part 1 Assignment will be based on the following:

|  |  |
| --- | --- |
| **Grades** | **Criteria** |
| **F** | * Program failed to compile or run successfully Clear evidence of plagiarism detected (*disciplinable offence*) |
| **D / D+** | * Backend Endpoint partially working * Program lack testing and robustness. Many (> 5) errors discovered during testing. |
| **C / C+** | * Backend Endpoint function as required * Some evidence of testing and robustness observed, some (3-5) errors discovered. |
| **B / B+** | * Backend Endpoint function as required * Evidence of testing and robustness observed, some (1-2) errors discovered. |
| **A / Z** | * Backend Endpoint function as required * Strong Evidence of testing and robustness observed |

The grading criteria for Part 3 Assignment will be based on the following:

|  |  |
| --- | --- |
| **Grades** | **Criteria** |
| **F** | * Program fails to compile or run successfully Clear evidence of plagiarism detected (*disciplinable offence*) |
| **D / D+** | * Front-End Web app partially working * Program lack testing and robustness. Many (> 5) errors discovered during testing. |
| **C / C+** | * Front-End Web app function as required * Some evidence of testing and robustness observed, some (3-5) errors discovered. |
| **B / B+** | * Front-End Web app function as required * Evidence of testing and robustness observed, some (1-2) errors discovered. |
| **A / Z** | * Front-End Web app function as required * Strong Evidence of testing and robustness observed * Authentication and Authorization works as specified |

The grading criteria for Part 5 Case Study Final Submission will be based on the following:

|  |  |
| --- | --- |
| **Grades** | **Criteria** |
| **F** | * Program failed to compile or run successfully Clear evidence of plagiarism detected (*disciplinable offence*) |
| **D / D+** | * Program lacks testing and robustness. Many (> 5) errors discovered during testing. * Poor integration of back-end and front-end * Minimal OWASP report was done and explanation was minimal |
| **C / C+** | * Some evidence of testing and robustness observed, some (3-5) errors discovered. * Moderate integration of back-end and front-end * Able to implement at least 1 OWASP measures to case study |
| **B / B+** | * Program is well tested and robust, very few (<3) errors discovered. * Integration of back-end and front-end for all functionalities * Able to implement at least 2 OWASP measures to case study * OWASP is well tested and robust, very few (<3) errors discovered. |
| **A / Z** | * Program is well tested and robust * Integration of back-end and front-end for all functionalities * Able to implement at least 3 OWASP measures to case study * Complexities of OWASP measures implementations * OWASP is well tested and robust |

The grading criteria for Part 2/4/6 : Presentation and Demonstration will be based on the following:

|  |  |
| --- | --- |
| **Grades** | **Criteria** |
| **F** | * Student was absent for project presentation and demonstration without a valid reason * Clear evidence of plagiarism detected (disciplinable offence) |
| **D / D+** | * Delivery is somewhat fluent and well-paced * Program failed to compile or run successfully during presentation * Unable to respond to most of the questions asked |
| **C / C+** | * Delivery is somewhat fluent and well-paced * Some (3 to 5) errors are discovered during presentation * Some questions are answered with difficulty and minimal elaboration is given |
| **B / B+** | * Delivery is mostly fluent and well-paced * Very few (<3) errors are discovered during presentation * Most questions are answered confidently with some elaboration |
| **A / Z** | * Delivery is very fluent and well-paced * No errors discovered during presentation * All questions are answered confidently with further elaboration * Evidence of clear understanding and explanation of advance features |