Assignment Task

Overview (Secure Design and Developmen)

This assignment requires you to design and develop **strictly** with the aid of a Large language Model (LLM), a functional secure system. The assignment consists of the following parts:

- A functional prototype of a secure online system. You have to submit the complete source code and video report showcasing prototype.
- An individual report of 2000 words that describes the design consideration, development and testing of the developed prototype.
- Any test/login credentials to the prototype should be included in the files.

The weighting is 100% including all elements. Practical work, written and video reports will be assessed against the same grading rubric table.

Practical Part Brief

Creative SkillZ LLC hired you as external consultants to help creating their newly proposed "PixelForge Nexus" system.

Your task is to implement a secure online system, tentatively named "PixelForge Nexus," using any language/system of your choice with the aid of an LLM (ChatGPT or Google Gemini). The prototype should contain the following functionality:

Core Functionality

1. **Project Management:**
    a. **Add/Remove Projects:** Admins can add new game projects (with name, description, and an initial deadline). Admins can also mark projects as "Completed"
    b. **View Projects:** All users can view a list of active projects.
2. **Team Assignment:**
    a. **Assign Team Members:** Project Leads can assign developers to their specific projects.
    b. **View Assigned Projects:** Developers can see a list of projects they are currently assigned to.
3. **Basic Asset & Resource Management:**
    a. **Upload Project Documents:** Admins and Project Leads can upload general project documents (e.g., design docs, meeting notes) associated with a project. *We'll skip version control for assets to simplify, but you can do it for 80%+.*
    b. **View Documents:** All users assigned to a project can view its uploaded documents.

Privilege Separation

- **Admin:** Can add/remove projects, manage all user accounts (create, edit roles), and upload documents for any project.
- **Project Lead:** Can assign developers to their projects and upload documents for their projects.
- **Developer:** Can view projects they are assigned to and access associated project documents.

Login Security

- **Robust Login System:** Essential for secure password hashing and storage (e.g., using bcrypt).
- **MFA Implementation: (**Optional but highly recommended): Adding Multi-Factor Authentication would significantly boost security.

Proposed Pages

- **Sign In/Register:**
    - Allows existing team members to log in.
    - Admin-only functionality to register new team members (no self-registration for simplification).
- **User Dashboard (Single Dashboard for All Roles):**
    - Developers: See a list of their assigned projects with links to documents.
    - Project Leads: See projects they lead, with options to assign team members and upload documents.
    - Admins: Access to add/mark projects as complete, and manage user accounts (add/edit roles).
- **Account Settings:**
    - Users can update their password.
    - MFA setup (if implemented).
- **Project Details Page:**
    - Displays project name, description, deadline, assigned team members, and uploaded documents.

Evidence for Practical Part / Overview of the marking rubric

1. System Design (35%):
    a. Produce a design for the system to be implemented and explain what design and security principles have been considered and why.
    b. Describe how the chosen principles or features enhance the functioning and security of that system in this stage of the development life-cycle.
2. Security testing and analysis (35%):
    a. Critically evaluate the application of security techniques and propose the possible solutions for the issues discovered.
    b. Propose solutions for the issues discovered during the testing and analysis process showing how they can mitigate the detected problems.
3. System Development (20%):
    a. Develop and demonstrate functional prototype that complies with the design provided above, including legal and ethical context of the development.
    b. Demonstrate the proper functioning and security mechanisms of the developed system in accordance with the existing secure development standards and methodologies.
4. Formal Methods (10%):
    a. Application of formal methods, to produce the behavioural model of the system that will be based on the design or development stage of the system life-cycle.
    b. Verify the correctness of the system with respect to its specification using the appropriate verification techniques and tools.

Submission Instructions

Submission

Deadline is **28/07/2025** Note that you should submit your own work.

For your submission, you will create and submit a written report (.docx file) that contains 2 links at the top:

- 1 link will be to your **prototype** complete source code in a drive folder.
- 1 link will be to your **video report.**
- The rest of the document will be the **Individual Report Brief**.

You will upload this .**docx file**

The complete source code and related documentation MUST be supplied. The source code should be appropriately and correctly commented. You should also identify any assumptions that you have made.

Your work will be marked using the grading rubric.

About Video Report

You will also record a video report (a singular video, totalling **8 minutes or less**) which shows:

- A fly-through of the output of the coursework, highlighting the significant aspects of the work (see the marking rubric below for the aspects that should be covered).
- You are required to use voice-overs and/or text overlays to explain what is happening in the video.

The video should be uploaded to GDrive and you should copy a link to the video which allows people to View the video.

The following issues, in relation to the prototype developed in the practical element of the assignment, must be included in system documentation:

a) Explanation of the methods and techniques followed in the practical task for the development of the system
b) Discussion of all the stages of the development life-cycle (e.g., specification, design, development, etc

Submission Guidelines:

1. Upload all deliverables into a single Google Drive folder.

2. Do not zip the files.

3. Make sure the folder link is set to: ”Anyone with the link can view.”

Assessment Marking Criteria

	System Design Weighting**: 35%** **(also Demonstrated in Video)**	**Security Testing and Analysis** Weighting: **35%** **(also Demonstrated in Video)**	**System Development** Weighting: **20%**	**Formal Methods** Weighting: **10%**
80 to 100%	Marks above 80 will be awarded for going above and beyond the requirements for a distinction and demonstrate and innovative approach and insight. A system design of professional standards, which is optimized for the given scenario. The system design demonstrates a deep understanding of secure design principles. The system design includes a comprehensive threat model that identifies and prioritizes potential security risks. The system design includes, clear access control mechanisms, comprehensive data encryption strategies. Detailed documentation illustrates how security principles are applied throughout the system design	Marks above 80 will be awarded for going above and beyond the requirements for a distinction and demonstrate and innovative approach and insight. Professional standard security analysis and testing followed by security measures that significantly improve the overall system security and functioning. The entire security process is comprehensively documented. The report includes comprehensive test cases and results, including code scanning reports	Marks above 80 will be awarded for going above and beyond the requirements for a distinction and demonstrate and innovative approach and insight. System development is professionally executed, fully complying with all the respective methods and standards. The codebase displays exceptional code quality and adherence to secure coding practices. The documentation of the process is thorough, including detailed explanations of secure coding practices.	Marks above 80 will be awarded for going above and beyond the requirements for a distinction and demonstrate and innovative approach and insight. Formal modelling and verification processes are professionally applied to the system covering and examining all the potential issues. The report demonstrates a deep understanding of formal methods, with minimal errors in their application. The process is fully documented.
70 to 79%	Detailed system design fully based on the secure design	An extensive security analysis and testing has been conducted	System development fully complies with the secure	Formal modelling and verification processes fully examine the

	methodologies and standards. Thorough and well-justified documentation. The system design is well structured and display a clear understanding of security principles and a fully detailed threat model. Most security controls are appropriately integrated into the design, with effective strategies for reducing threat.	providing mitigation techniques for the identified security issues. The testing process covers key aspects of security. Test cases and results provide a detailed overview of the security testing process. Thorough and well-justified Documentation	development methods and standards. The codebase demonstrates a high degree of adherence to secure coding practices, with minimal security vulnerabilities. Thorough and well-justified documentation.	functioning and security issues of the system Formal methods are effectively used to analyse and address security concerns, with minimal errors. The formal analysis is very well justified in the report.
60 to 69%	System design incorporates an extensive range of principles which are very well discussed in the report. The system design shows awareness of security concerns but may lack detail in threat modelling. Most security controls are present but need further clarification.	A medium range of security analysis and testing techniques have been used providing effective solution for the detected problems. Process is very well described in the report.	System development fully complies with the proposed design, but partially with the secure development methods and standards. Process is very well described in the report.	Formal modelling and verification processes extensively examine a wide range of functioning and security issues. The formal analysis is very well described in the report
50 to 59%	System design incorporates the principles required for the proper functioning and security of the system but required more details. Adequate discussion in the report.	A small range of security analysis and testing techniques have been used providing the respective solutions. Test cases and results are provided but may lack completeness. Adequate discussion in the report	System development considers basic functioning and limited security of the system with good explanation of the development stage. The system development phase has basic security measures in place, but there are notable areas where secure coding practices could be improved.	Behavioural model presents the basic functioning of the system incorporating security aspects as well. Verification examines the basic security issues. Adequate discussion in the report.

40 to 49%	System design meets the basic requirements with lack of details. Short discussion in the report. Security controls are present, but it is generic or incomplete.	Very limited security analysis and testing of the system with very few solutions provided. Test cases and results are limited in scope. Short discussion in the report.	System development complies with the requirement of a basic design. Short discussion in the report.	A very basic attempt of modelling the behaviour of the system and then verify it. Short discussion in the report.
Fail 30, 35%	No system design built or incomplete design provided. which is severely deficient in security aspects	There is no evidence of security testing or analysis provided or very poor system security and testing carried out with no recommended solutions.	No system developed or incomplete implementation of the system. No attention to system security	No or very poor application of formal methods to the system analysis.
Fail 0 to 29%	The system design is entirely devoid of security considerations and outcome not met or no system design built	No attempt or no system security testing carried .	Outcome not met or no system developed	No attempt or no application of formal methods to the system analysis.