INTI International College Penang **School of Computing**

3+0 Bachelor of Science (Hons) in Computer Science, in collaboration with Coventry University, UK

3+0 Bachelor of Science (Hons) in Computing, in collaboration with Coventry University, UK

Module Title	**Security**
Module Code	**INT6005CEM**
Semester	**August 2023**
Coursework Title	**Secure Application Development**
Handout Date	**5th October 2023**
Lecturer	**R.K. Krishnamoorthy**
Due Date	**23rd November 2023**
Coursework Type	**Group Project and Report**
% of Module Mark	**50%**
Word Limit	**1500 - 2000 words**

Coursework Learning Outcomes:

1. Develop and evaluate software that addresses the most common and most severe security concerns (CLO3).
2. Critically evaluate the security of an IT ecosystem (CLO4).

Assignment Descriptions:

You are required to design and develop a simple application and to write a report on the design and development choices made with the security implications. The coursework has **TWO** main components:

1. Design and develop the infrastructure for a simple application based on the requirements below.

2. A report on security considerations in the application development. The report should focus on security based design and development of a secured application which includes methods, functions, techniques implemented and its relevant justifications. For example you should be focusing on type of information and how information such as passwords are stored securely in database. Discussion on database table structure and justification on type of database is not necessarily required unless there is a specific feature of database that has security implications. The application is expected to be fully functional with security features at specific level.

You may use the project which you have developed previously in this program and enhance it with security features where it is deemed important and meeting the requirement stated in the next section.

Application Requirements:

1. Level of Access
    a. The developed application should be able to support multiple users' interactions at various level – for example, an e-commerce application or student-staff social media page.
    b. Multiple users should be able to access with user registration, secured login authentication and users' authorization with Role-based Access Control (RBAC) or Attribute-based Access Control (ABAC) – whichever applicable.
2. Input Validation, Output Encoding and Error Handling
    a. The application should validate and sanitize all user input to prevent common vulnerabilities such as SQL injections.
    b. Use proper output encoding functions based on output context.
    c. Implement proper error handling to avoid exposing sensitive information. Provide user-friendly error messages without revealing detailed system or application information.
3. Administration
    a. The admin should be able to add and remove users on the system.
    b. The admin should be able to change access levels of users.
    c. The admin should be able to view, modify, update and remove any content.
4. Secure Communication
    a. Use appropriate techniques to encrypt all communication between the application and user to protect against security threats.
    b. Suggest or implement proper certificate validation and configuration to establish a secure and trusted connection.
5. Data Protection and User Education
    a. Provide privacy regulations and best practices for handling and storing user data depending on applications domains.
    b. Educate users about best practices for secure usage of application.
6. Logging and Analytics (Advanced Features)
    a. The application should be able to gather logging and analytics information to track on users' interaction within a system.
    b. The logging and analytics information will be presented in dashboard and viewed based on RBAC/ABAC. The information presented in dashboard must reflect the nature and importance of details to specific users

Report Structure:

A structure for the report would be as follow:

- INTI – Coventry Cover Sheet:
- Table of Content (TOC)
- 1.0: Introduction and System Overview
- 2.0: Design
  - i. Discussion on potential security issues for each element of design.
  - ii. Recommendations for dealing with potential security issues
- 3.0: Implementation
  - i. Discussion on how the implementation addresses the potential security issues in section 2.0
  - ii. Highlight techniques and methods used to address them and its security implications
- 4.0: Discussion
  - i. Key findings and highlight the issue resolved
  - ii. Discuss on how security issues can be enhance as part of continuous improvement and maintenance.
- 5.0: Summary
  - i. Conclusion
  - ii. Learning Outcome achieved.
- 6.0: References
- 7.0: Appendix (if any)

It is expected that students to use of supporting literature and relevant citations to support your finding. Submit your final report before or on the deadline in PDF format, via Canvas submission link. Student are expected to use the **Harvard Referencing** style for referencing.

Marking Scheme:

Report Components	**Marks (max)**
Introduction and System Overview	**5**
System Design	**15**
Security Implementation (Individual)	**15**
Discussion, Improvement and Summary	**10**
Background Research and Quality of Report	**10**
Report Format, Citation and Referencing	**5**
Total	**60**

Development Components & Viva	**Marks (max)**
Overall Functionality of System	**10**
Security Issues Addressed (Individual)	**10**
Security Solutions Implemented (Individual)	**20**
Total	**40**

Marking Matrix:

Report Components

Criteria	**Excellent** (>= 8 to10)	**Good** (>= 6 and < 8)	**Average** (>= 4 and < 6)	**Poor** (0 to <4)
Introduction and System Overview (5%)	Provides a clear and concise introduction to the system and demonstrates a deep understanding of the context and background related to the system. Provides an overview of the system architecture, components and major functionalities with relevant references and citations to support the presented information.	Offers a well-written introduction and overview of the system and demonstrates an adequate understanding of the context and background related to the system Provides a basic overview of the system architecture, components and major functionalities with some references and citations to support the presented information.	Provides a basic introduction and overview of the system and demonstrates a limited understanding of the context and background related to the system. Provides a basic descriptions of the system architecture, components and major functionalities but lack of details. Lack sufficient references and citations to support the presented information.	Provides an inadequate or unclear introduction and overview of the system and demonstrates a lack of understanding of the context and background related to the system. Provides an incomplete or inaccurate description of system architecture with lack of references and citations to support the presented information.
System Design (15%)	Demonstrates a comprehensive understanding of application security principles and best practices. Applies appropriate security measures throughout the system design, considering	Demonstrates a solid understanding of application security principles and best practices. Applies appropriate security measures in the system design, considering authentication, authorization, data	Demonstrates basic understanding of application security principles and best practices. Implements basic security control for authentication, authorization, data encryption, input validation and secure	Demonstrates a weak or inadequate understanding of application security principles and best practices. Fails to implement essential security controls for authentication, authorization, data encryption, and input

	authentication, authorization, data encryption, input validation and secure communication. Provides a detailed and well-justified rationale for the chosen security design decision.	encryption, input validation and secure communication. Provides a rationale for the chosen security design decisions, although it may lack some depth or details.	communication. Provides a basic rationale for the chosen security design decisions, but lacks some depth or details.	validation and secure communication. Provides inadequate or no rationale for the chosen security design decisions.
Security Implementation (15%)	Implements industry standard security controls and applies secure coding practices and frameworks consistently and effectively. Provides clear and well documented code with proper comments and annotations for security related functionalities and highlighting key security features and their implications.	Incorporates standard security controls and applies secure coding practices and frameworks consistently. Provides a well-structured and readable code with some comments and annotations for security related functionalities and covered important security features and their implications.	Includes essential security controls and applies some coding practices and frameworks. Provides readable code with limited comments and annotations for security related functionalities and focusing on major security features.	Lacks of essential security controls and fail to apply secure coding practices and frameworks effectively. Provides poorly structured or unreadable code with minimal or no comments and annotations for security related functionalities and omitting important security aspects.
Discussion and Improvement (10%)	Provides a comprehensive and insightful discussion of the design and development choices made, with strong focus on the security implications. Shows an awareness of emerging	Provides a solid discussion of the design and development choices made, with some consideration on the security implications. Shows some awareness of emerging security	Provides a basic discussion of the design and development choices made, with limited consideration on the security implications. Shows limited awareness of emerging security	Provides a weak or inadequate discussion of the design and development choices made, with little consideration on the security implications. Shows little or no

	security trends or future considerations in application development with detailed and well justified plan for implementing the suggested improvements.	trends or future considerations in application development with plans for implementing the suggested improvements.	trends or future considerations in application development with basic plan for implementing the suggested improvements, but lacks some necessary details.	awareness of emerging security trends or future considerations in application development. Lack a clear plan for implementing the suggested improvements or provide no plans at all.
Background Research and Quality of Report (10%)	Demonstrates exceptional quality in term of research, organization, structure and writing style. Displays originality, excellent use of research and creativity in approach, analysis or presentation of information. Shows a high level attention to details, accuracy and precision in the report.	Demonstrates good quality in term of research organization, structure and writing style. Displays some originality or unique perspectives in the approach, analysis or presentation of information. Shows attention to details, accuracy and precision in the report.	Demonstrates acceptable level of quality in term of research, organization, structure and writing style. Displays limited originality or unique perspectives in the approach, analysis or presentation of information. Shows some attention to details, accuracy and precision in the report but with some inconsistencies.	Demonstrates poor quality in term of research, organization, structure and writing style. Lack of originality or unique perspectives in the approach, analysis or presentation of information. Show significant issues with attention to detail, accuracy and precision in the report.
Report Format, Citation and Referencing ***(5%)***	Presents a visually appealing and professional looking report with appropriate formatting and visuals. Incudes thorough citations and references, following the appropriate citation style.	Presents a visually clear and well formatted report with appropriate formatting and visuals. Incudes proper citations and references, following the appropriate citation style.	Presents report with adequate formatting and visuals, but room for improvement. Incudes citations and references, but with minor errors or inconsistencies in the format	Presents a poorly formatted report and ineffective visuals. Lacks of proper citations and references and contains significant errors in the citation style.

Marking Matrix

Development Components

Criteria	**Excellent** (>= 8 to10)	**Good** (>= 6 and < 8)	**Average** (>= 4 and < 6)	**Poor** (0 to <4)
Overall Functionality of System **(10%)**	The application demonstrates exceptional functionality, meeting all specific requirements and objectives with no errors or issues. The system exhibit excellent stability, error handling and quality assurance measures have been employed resulting in high quality and robust applications.	The application demonstrates good functionality, meeting most of the specific requirements and objectives with minor issues and limitations. The system exhibit good stability, error handling and quality assurance measures have been employed resulting in a reasonably reliable and functional applications.	The application demonstrates basic functionality, but may fall short in meeting some of the specific requirements and objectives and may have noticeable issues and limitations. The system exhibit average stability, error handling to some extend and some quality assurance measures have been employed, but the application may have some notable bugs or inconsistencies.	The application demonstrates poor functionality, failing to meet several of the specified requirements and objectives and may have significant issues and limitations. The system exhibit poor stability, error handling are poorly implemented and no quality assurance measures have been employed, resulting in an unreliable and dysfunctional application.
Security Issues Addressed **(10%)**	Identifies and addresses a comprehensive range of security issues and proactively addresses emerging security concerns and incorporates industry best	Identifies and addresses a significant number of security issues and considers some emerging security concerns and incorporates industry best practices relevant to the	Identifies and addresses a limited number of security issues and lacks of considerations of emerging security concerns and industry best practices relevant to	Fails to identify and address security issues and ignores emerging security concerns and industry best practices relevant to the application. Demonstrates a lack of

	practices relevant to the application. Demonstrates a high level of attention to details and accuracy in addressing security issues.	application. Demonstrates a good level of attention to details and accuracy in addressing security issues.	the application. Demonstrates an average level of attention to details and accuracy in addressing security issues.	attention to details and accuracy in addressing security issues.
Security Solutions Implemented (20%)	Implements robust security measures to mitigate identified risks. Applies multiple layers of security control and utilizes advanced security technologies and frameworks. Integrates secure coding practices in the development process. Conducts rigorous testing and validation of the implemented security solutions.	Implements solid range of effective security measures. Applies essential security control and utilizes standard security technologies and frameworks. Applies secure coding practices in the development process. Conducts adequate testing and validation of the implemented security solutions.	Implements basic security solutions. Applies some essential security control and utilizes basic security technologies and frameworks. Applies some secure coding practices in the development process. Conducts limited testing and validation of the implemented security solutions.	Implements weak or inadequate security solutions. Fails to apply security control and lacks of utilization basic security technologies and frameworks. Fail to apply some secure coding practices in the development process. Conducts minimal or no testing and validation of the implemented security solutions.