

# Faculty of engineering, Environment and Computing



## Module: 6005-CEM Security

### Assignment Brief

<b>Module Title:</b> Security	<b>Group / Individual</b> Individual	<b>Cohort</b> Sept	<b>Module Code</b> 6005-CEM
<b>Coursework Title</b> CW2: Secure Development			<b>Handout Date</b> 1st Week
<b>Lecturer</b> Dan Goldsmith			<b>Due Date and Time</b>
<b>Estimated Time (hrs)</b> 20 Hours	<b>Coursework Type</b> Report		<b>Credits of Assessment</b> 10
<b>Submission Arrangements</b> Via: Learning Platform  Marks release expected: None  Feedback Method: Feedback Via LMS  Word limit: 1000			

## Module Learning Outcomes Assessed

- 1. Critically evaluate a range of encryption and authentication methods for a given set of requirements.
- 2. Utilise systematic knowledge to create secure environments at the host or network level.
- 3. Develop and evaluate software that addresses the most common and most severe security concerns.

# Task and Mark Distribution

In this coursework you are required to design a simple web application. And write a short report on the design choices made with regard to security implications.

The coursework has two components:

1. Design a simple web application, based on the requirements below.
2. A Report on the website design. This should discuss and justify any design decisions made with regard to security.

## Website Requirements

The website you need to develop is a simple messaging board, that supports stack overflow style questions, and responses.

The Website has the following requirements:

- User Account Creation
  - It should be possible to create a new user account on the system
- User Login:
  - Users Should be able to authenticate with the server
- Forum Style Messaging.
  - Users should be able to ask "Questions" for other users to answer
  - Users should be able to view questions on the system
  - Users should be able to respond to questions on the system
- Admin Account:
  - Admin account: Should provide an overview of activity on the site
- Very Simple Web API:
  - GET: A List of all Threads
  - GET: An Individual Message Thread
  - POST: New Message

## Report Requirements

The report should be written in a style suitable for a technical audience. The report should provide details of the **design** of the system, and the security based decisions behind it. You are expected to justify your design choices by referring to the relevant literature

- You **do not** need to justify decisions based on infrastructure, or formatting (unless this has an impact on security)

A suggested report structure is as follows:

- Introduction
  - Scope of the report, design overview
- Design:
  - Discussion of potential security issues for each element of the design
- Implementation details:
  - Description of how you address potential security issues
- Summary:
  - Summary section, highlighting the issues resolved, and the key findings of the report.

There is also an element for Background Research. While I am not expecting a full literature review, you should **support** your design decisions using the relevant literature.

## Important Note:

You are marked on the functionality of the system, rather than its look and feel. The site should be usable via a web browser. Simple formatting using CSS (or something like Twitter Bootstrap) is more than sufficient. Other than that the choice of infrastructure is up to you.

Additionally, in the report, you do not need to justify and non-security design decisions. For example, there is no need to justify the choice of database (sqlite, MySQL, mongo) **UNLESS** there is a specific feature of the database that has a security implication.

## Marking.

- Report (1000%): Justification for the design choices.

## Marking Scheme

Report:

<b>Component</b>	<b>Marks (of 100)</b>
Introduction and Conclusions	10
Systems Design	30
Discussion of Implementation	30
Report Conclusions	10
Background Research	10
Report Structure	10

## Submission Instructions

Please submit:

- Your final report in **PDF Format** by the submission date.

# Notes:

1. You are expected to use the [Coventry University APA](#) style for referencing. For support and advice on this, students can contact [Centre for Academic Writing \(CAW\)](#).
2. Please notify your registry course support team and module leader for disability support.
3. Any student requiring an extension or deferral should follow the [university process as outlined here](#).
4. The University cannot take responsibility for any coursework lost or corrupted on disks, laptops or personal computer. Students should therefore regularly back-up any work and are advised to save it on the University system.
5. If there are technical or performance issues that prevent students submitting coursework through the online coursework submission system on the day of a coursework deadline, an appropriate extension to the coursework submission deadline will be agreed. This extension will normally be 24 hours or the next working day if the deadline falls on a Friday or over the weekend period. This will be communicated via your Module Leader.
6. You are encouraged to check the originality of your work by using the draft Turnitin links on Aulana.
7. Collusion between students (where sections of your work are similar to the work submitted by other students in this or previous module cohorts) is taken extremely seriously and will be reported to the academic conduct panel. This applies to both courseworks and exam answers.
8. A marked difference between your writing style, knowledge and skill level demonstrated in class discussion, any test conditions and that demonstrated in a coursework assignment may result in you having to undertake a Viva Voce in order to prove the coursework assignment is entirely your own work.
9. If you make use of the services of a proof reader in your work you must keep your original version and make it available as a demonstration of your written efforts.
10. You must not submit work for assessment that you have already submitted (partially or in full), either for your current course or for another qualification of this university, unless this is specifically provided for in your assignment brief or specific course or module information. Where earlier work by you is citable, ie. it has already been published/submitted, you must reference it clearly. **Identical pieces of work submitted concurrently will also be considered to be self-plagiarism.**