To do: Make a submission

Due: Monday, 2 December 2024, 11:55 PM

In this unit, the focus is on the first objective/deliverable, the design document. This assignment has two component parts, the team submission and your individual peer assessment. All components must be submitted by end of unit 6. This accounts for 20% of your final module mark.

Only one submission is required from each team. Nominate one member of your team to submit on the team's behalf. The word count is 1,000 words.

Full Brief

For this assessment, you are advised to position yourself and your team as software system designers that will ultimately respond to a legitimate system user and a hacker.

You are required to firstly develop a secure application, for either one of a school (Falana et al., 2021), online retailer (D'Adamo et al., 2021), or the international space station (Pipikaite et al., 2022). The system's capabilities should be tailored to the specific needs of the chosen domain.

Application requirements:

The agreed criteria for successful development are:

- The application should be developed using the Python programming language.
- The data repository should be created in Python. You are required to use at least three different structures to store the data within the data repository.
- The application should be accessed via a terminal, using a Command Line Interface as the User Interface.
- All functionality of the system should adhere to GDPR (anon, n.d.a).
- The system should be designed so that a design pattern may be applied.
- Mechanisms should be deployed to minimise the attack surface of the solution. At a minimum, the application should include authentication, authorisation, data encryption and event monitoring. Capabilities should also be enabled to protect against the hacker attacks (details below).
- The system should support ability to turn secure capability on and off.
- Object-oriented programming practices should be used.
- Write unit tests to examine the effectiveness and completeness of your programme. These should be integrated as part of a testing suite, additionally including system, integration, and user acceptance.
- At least one API should be used to support system functionality.

Legitimate User Requirements:

- A user should have ability to perform CRUD functions (anon, n.d.b).
- A user should be able to create a secure account.

Hacker Requirements:

- A hacker should have the ability to carry out a brute force attack on the local network system.
- A hacker should be able to carry out a Denial of Service attack on the local network system.
- A hacker should be able to carry out an API injection attack (Sani et al., 2022).

The overall goal of the system is to be able to turn security on from the command line user interface and prove that the system is secure against brute force, Denial of Service, and API injection attacks. The system should therefore also be able to be run with security turned off.

Part 1: The Design Proposal Document

Your team is expected to create a system design, describing how you will meet the requirements, and prepare this as a design document. In your document, you should detail the system requirements and assumptions influencing the design. You should identify the security challenges that the system has been designed to protect against. You should produce a minimum of two different UML designs which illustrate different views of the system, one of which should be a misuse case diagram (Pauli & Xu, 2005). You should also state the tools and libraries which you will use in your solution. You should describe how you are applying a solo developer (Pagotto et al., 2016) (Moyo & Mnkandla, 2020) approach to manage the project. Note that the associated grading criteria are highlighted in the requirements below, to be reviewed alongside the criteria grid (Module Resources).

The design document will be assessed according to:

- Knowledge and understanding of the topic/issues under consideration (25%).
  - Evidence of awareness of the security-related challenges of the domain.
  - Evidence of awareness of the software features that can be used to enable a secure solution.
  - Accurate and effective use of UML.
  - Application of project management as a solo developer.
- Presentation and communication skills (30%).
  - Depth of solution design communicated.
- Criticality (25%)
  - Awareness of the competing decisions that may support the system design with variable cost-benefits.
- Structure and presentation (10%).
  - Document design.
  - Document content.
- Use of relevant sources (10%).
  - Reference to academic literature throughout the document.

Please note that appendices should not be used to extend the core report as reports should stand alone, complete and concise, without the appendices. They should really only be used if required, and only for supplementary and/ or supporting information. One key part of the exercises in this module is the need to be to be able to express ideas succinctly, concisely and with necessary brevity.

Submission Checklist:

- Bulleted list of system requirements and assumptions, design decisions and approaches you will use based on background information and additional academic research (ensure you include any references you have used).
- Bulleted list of security risks/ vulnerabilities you have identified, including reference to frameworks used (e.g. STRIDE, OWASP) with potential mitigations and references.
- UML design(s) of solution (e.g. class, sequence, activity).
- Bulleted list of tools (including development and test tools), libraries and models you will use.
- Remember to use a spell checker and proofread your work before submission.
- You should get your design outline reviewed and approved by your tutor **BEFORE** you submit the final version in this Unit.You are invited to arrange a meeting between your team and the tutor to get feedback.

Learning Outcomes

- Identify and manage security risks as part of a software development project.
- Critically analyse development problems and determine appropriate methodologies, tools and techniques (including program design and development) to solve them.
- Systematically develop and implement the skills required to be effective member of a development team in a virtual professional environment, adopting real-life perspectives on team roles and organisation.

Turnitin Originality Check

Before submitting your assignment, it is important to check the originality of your work by submitting your assignment to **Turnitin**.

By submitting your assignment to this tool you will receive an originality report which can be used to check that you have not included other authors work without correct citation. It is important to note that submitting your work to the Turnitin Originality Check tool does not count as a submission of your final work. You must still submit your assignment below.

Academic Integrity and Plagiarism

We take academic integrity very seriously. Academic integrity means acting with fairness and honesty, giving credit to others where you are referring to their ideas or research and respecting the work of others. Plagiarism is defined as: 'Using or copying the work of others (whether written, printed or in any other form) without proper acknowledgement'. Before you finalise your assignment take time to check that all your statements are backed up with supporting evidence, that all sources you use - whether referring to their ideas, quoting directly or paraphrasing - are correctly referenced in the text. Correct use of referencing acknowledges the academic whose work has informed yours, enables the reader to find the sources you have used and demonstrates your ability to find and analyse relevant information.

Failure to properly acknowledge the work of others is an academic offence and may result in your work incurring a penalty or, in the most serious cases, you being removed from the course for academic dishonesty.

If you are unsure about referencing or plagiarism there are useful resources available in the Study Skills Hub which is accessible from the menu on the left hand side. If you are still experiencing difficulties with academic integrity then you can **contact the Study Skills Team** for individualised support.

Please note, a word count penalty applies to this assessment.

If your assessment exceeds the word count limit or range by more than 10% then your awarded grade will be reduced by 10% grade points. For more information please see your **student handbook**.

Not meeting the word count

There is no grade reduction applied if your assignment does not meet the word count range or limit, but to maximise your opportunity to achieve the highest grade possible, you should aim to meet the word count or range as closely as possible.

Submission Instructions

- Submit your saved document below before the end of Unit 6.
- After the deadline, the submission page will be locked.

Add submission

Submission status

Group	Group 2
Attempt number	This is attempt 1.
Submission status	Nothing has been submitted for this assignment
Grading status	Not graded
Time remaining	37 days 14 hours remaining
Last modified	-
Submission comments	Comments (0)