SE4030 – Secure Software Development

Semester 2, 2022

100 Marks

Instructions

- Assignment is a development-based group assignment.
- Students will need to create a team of 4 and the team leader will register the team using the link provided on Courseweb.
- You will have to develop a secure mobile/web app which meets the below given specifications.
- Marks will be allocated for given deliverables, and the marking scheme is given below.
- You will have to submit the implementation before the deadline. (Late submissions are not accepted; 50% marks will be decreased from overall marks for any delays).
- The deadline is 12/11/2022 12.00 Midnight.
- Deliverables
  - Web/mobile app and server
  - Report

Scenario

ABC Company is looking to create a custom web/mobile app to allow their staff to save messages or to upload files to a central server. The high-level functional requirements are given below.

- The proposed system is a client server system to be run over an unsecure network
- The client app will act as a simple interface which allows users to log in and provide messages or files
- The server app will act as a database/data repository which allows the messages or files to be stored
- The system should allow an administrator to create accounts for staff members – this can be hardcoded into system
- The staff can login to system using the username and password allocated to them
- The staff can be of two main roles
  - Workers – can only save messages
  - Managers – can save messages and upload files
- The system should be able to send the messages and files over an unsecure network (from client to server) with the below security requirements
  - Confidentiality
  - Integrity
  - Message authentication
  - The client should be able to identify the server before any files are sent

Tasks

1. Design the main process of the software you are developing and identify the threats that the software faces and the mitigations that can be used to secure it. You can use a tool such as Microsoft threat modeling tool to do this
2. Design and develop the web/mobile app and server ensuring that all functional and security requirements are met. You are expected to use industry standard tools, frameworks and communication protocols when doing this and follow a suitable SSDLC.
3. Test the developed software to ensure that both functional and security requirements are fulfilled.

Deliverables

1. The developed web/mobile app.
2. Report which includes the design documents, threat models and identified mitigations and testing plan and results.

Marking Scheme

Marking Criteria	Marks Allocated
Development (55)	
Functional requirements met	15
Security requirements met	
• User authentication	8
• Access control	8
• Integrity	8
• Confidentiality	8
• Message authentication	8
Report (25)	
Threat modeling	10
Suitable mitigations identified	5
Test plan	5
Test outcome	5
Viva	20