Cairo University - Faculty of Computer and Artificial Intelligence
SCS359 - Software Security

Assignment #1

Task 1: Utilize the DES algorithm for file encryption and decryption

- Implement a DES algorithm sourced from any online platforms or use your own implementation
- Employ your DES algorithm to encrypt the provided file and save the ciphertext in a separate file
- Ensure the ciphertext file can be uploaded to the DES decryption function to recover the original file

Task 2: Implement RSA from Scratch

Create a CPP program to implement the **RSA algorithm** for encryption and decryption. The program should include functions for the following:

- Generating keys
- Encrypting messages
- Decrypting ciphertext

Task 3: Secure Application Development with Penetration Testing

1. Application Description:
   Select an application that requires multiple pages and access control (you can either choose a previously developed app or implement a new one)
2. Security Requirements:
   a. Implement access control mechanisms (e.g., user roles, permissions) in your application.
   b. Ensure sensitive data is properly encrypted.
   c. The application should follow secure coding practices (e.g., input validation, output encoding, secure authentication).
3. Penetration Testing:
   a. Perform penetration testing on your application to identify security vulnerabilities.
   b. Document the testing methodology, tools used, and findings.
   c. Provide recommendations for mitigating the identified vulnerabilities.
4. Report:
   Write a detailed report that includes:
   a. Description of the application and its functionalities.
   b. Security measures implemented (access control, encryption, etc.).
   c. Penetration testing methodology and findings.
   d. Recommendations for improving the application's security.

Submission Guidelines:

- You should work in teams of 5 (minimum 4)
- Team members must all be from the same lab (or have the same TA)
- Cheating is NOT tolerated by any means

Deliverables:

- ONLY the team leader should submit a Zip file under the name:
  <G#_TeamLeaderName_TeamLeaderID>
- The zip file should include
  - A text file with the teams' names and IDs
  - A CPP program for the DES implementation
  - The CPP program for the RSA implementation
  - Source code of the app along with the penetration testing report

Deadline:

- Date: Saturday, 20th of April, 2024
- Time: 11:59 PM