** Task group: Access control **

Context

AAAA: Authentication, Authorization, Accounting and Auditing for the application. This task is about developing the authorisation and authentication components of the application. You may use the features of the APS.NET Core framework. The components need to comply with the ASVS level 2 requirements. You need to implement the following functionalities for account management:

- registration of a new user page
- login page
- change password page
- lost password page

Deliverables

- Show your account management application in the Test and Acceptance environment, with
  - proper password handling
  - proper session handling
  - 2 factor authentiation
  - proper error handling
  - proper logging
  - proper RBAC
- Show updated design documents
- Show an updated ASVS excel sheet with the controls that you applied to your account management pages

Task

Design, build and test an account management application.

Approach

As a software engineer you must be able to interiorize new technologies. Explore the AAAA options of the ASP.NET framework and implement them in your account management application.

Subtask: Authentication

1. Design, develop and test a *new user registration* web page
2. Design, develop and test a *login* web page
3. Store passwords in the database in secure fashion (e.g. scrypt, bcrypt)
4. Use proper password strength controls
5. Use secure session IDs

6. Design and develop and test change password page
7. Design and develop and test lost/forgotten password pages
8. Use a CAPTCHA.
9. Add 2-factor authentication (FIDO2 or TIQR or FreeOTP or Google Authenticator)

Subtask: Authorization

1. Design roles and permissions (CRUDA of accounts) with an access control matrix
   - 'normal' users may only change their password attribute and read their profile.
   - 'Moderator' role may update (i.e. reset) password and 2-factor registration information of 'normal' users
   - 'Administrator' role may create, read, update, delete and archive accounts and change high scores.
   - Add your designed access control matrix to the design document
2. Setup access control according to access control matrix
   - Setup account profiles with appropriate attributes: username, id, password, email, roles, TOTP shared secret key
   - Show your account and role database tables.
3. Design and implement web pages for the account management web application using the database tables

Subtask: Accounting and Auditing

1. Use well designed error messages
2. Use appropriate logging messages for accounting and auditing

Done