I5020 Computer Security

Coding 2: Secure password storage

This assessment evaluates the following competencies:

- *CS001 – Understand the CIA triad and use it to explain the key objectives of computer security*
- *CS003 – Identify weaknesses in a computer system or infrastructure and propose solutions*
- *CS103 – Write a program that encrypts data with the suitable libraries*
- *CS204 – Discuss about general design principles for protection mechanisms*
- *CS202 – Discuss about the differences and importance of authentication and access control*
- *CS203 – Identify security risks related to operating systems, network, database, cloud and IoT and propose solutions to decrease them*
- *CS303 – Apply code design principles in developed software*
- *CS403 – Discuss about the risks that a company assets are exposed to and propose solutions to decrease them*
- *CS005 – Identify residual risks that come from a countermeasure*
- *CS106 – Identify the suitable cryptographic tool for a given security issue*
- *CS205 – Write an application that stores passwords securely*
- *CS304 – Program, configure and launch a secured HTTPS server*

For this assessment, you have to write a small website that allows used to create an account and then to connect to their account. Passwords of the users must be stored securely in the database, that is, in hashed form.

Pay attention to the following elements:

- The design and content of the website served is not important.
- Use the suitable hash/encryption cryptographic tool to store the passwords.

Prepare yourself for the following manipulations/questions:

- Explain the role of hashing/encrypting passwords in a database regarding the CIA triad.
- Why is is so important to not store passwords in clear in a database?
- For such a system, is it necessary to have an HTTPS server?
- Think about the residual risks of hashing/encrypting all the passwords in the database.