Initial Post: Discussion 1

I have selected Cryptographic Failures, holding the position of number two in the OWASP Top 10 identified weakness (OWASP, 2021). The flowchart of processes and decisions is presented in Figure 1.

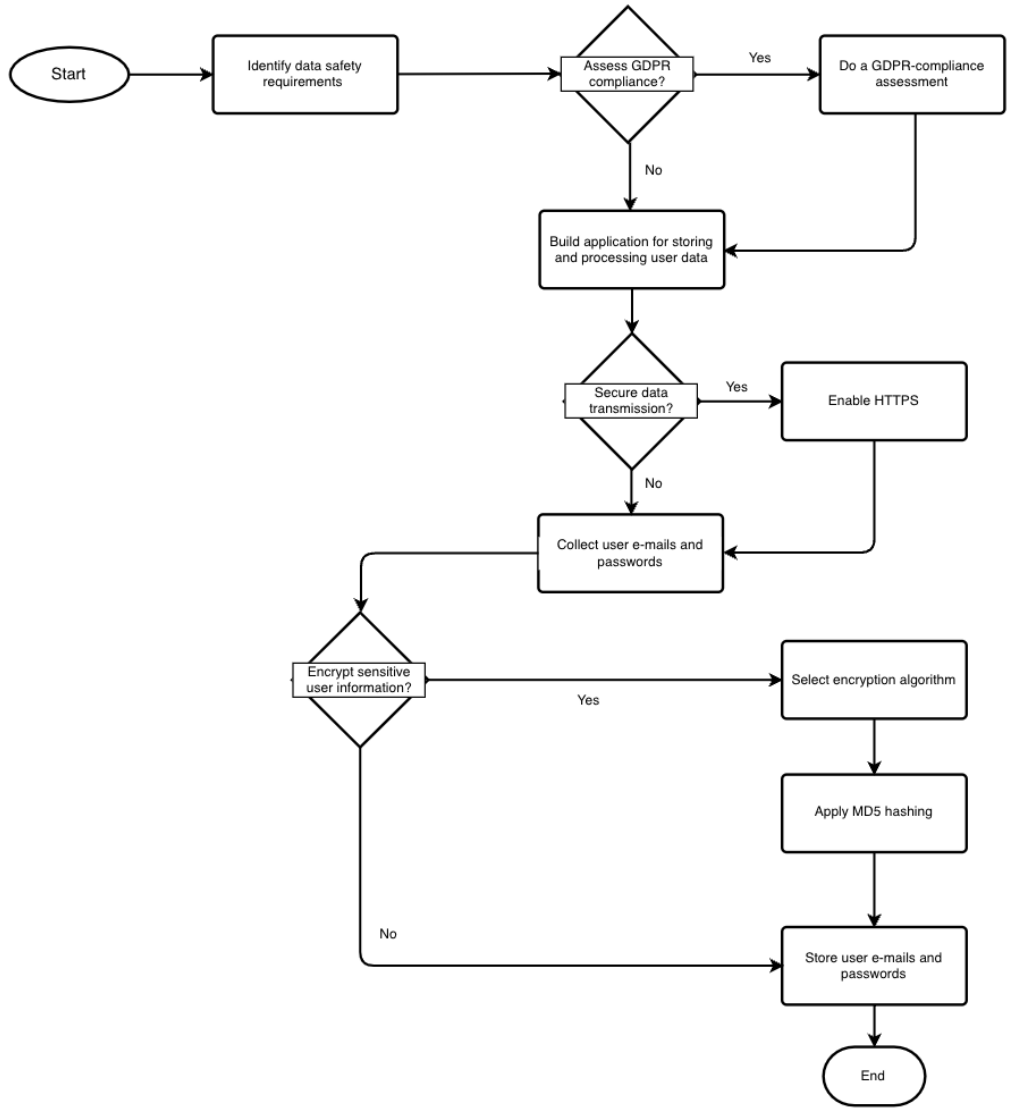

Figure 1. Flowchart of introducing a subset of cryptographic failures.

Following the phase of SDLC, the first stage, Planning stage, considers the project requirements. Here, insufficient assessment of what data needs to be encrypted and secured, and the strength at which it needs to be secured, can lead to weak software security designs. Additionally, depending on where the data is processed, additional

GDPR compliance measures may apply, including the requirement of sufficient systems and data securement (Allen, 2023). An incomplete assessment or failing to assess GDPR compliance of designed systems can lead to heavy fines and reputation loss.

When designing the application, there are critical decisions pertaining to security. Firstly, when transmitting data, a secure internet protocol such as HTTPS must be implemented to transmit sensitive data. Failure to do so can result in interception by malicious actors. Following this, any data stored must be encrypted and a sufficiently secure encryption algorithm must be selected. For example, MD5 hashing algorithm, although fast, is vulnerable to brute-force and collision attacks (Stec, 2024). SHA256 however currently has no known vulnerabilities.

In conclusion, cryptographic failures can occur at all stages of software design and development, with most critical decisions pertaining to encrypting data when processing, storing and retrieving. When designing software, a thorough assessment should be done to ensure the application is fully secure and compliant with the relevant security standards (GDPR, and also PCI-DSS, for example).

References:

Allen, C. (2023) Encryption For GDPR Compliance. *Cryptomathic*. Available from: https://www.cryptomathic.com/blog/encryption-for-gdpr-compliance [Accessed 27 October 2024]

OWASP (2021) OWASP Top 10. *OWASP*. Available from: https://owasp.org/www-project-top-ten/ [Accessed 25 October 2024]

Stec, A. (2024) MD5 vs. SHA Algorithms. *Baeldung*. Available from: https://www.baeldung.com/cs/md5-vs-sha-algorithms [Accessed 27 October 2024]