**Summary Post – Unit 3**

Web applications and application programming interfaces (APIs) may not be properly configured to protect sensitive data, including personal identifiable information (PII) (OWASP, 2017, 2021). Thus, cyber-attacks may retrieve such information and use it to commit fraud or identity theft. Such sensitive data could be accessed by these unauthorised parties when encryption at rest or in transit, or permissions, are not appropriately set (OWASP, 2017, 2021).

These cryptographic failures (OWASP, 2021) are ranked second place (OWASP, 2021), beyond the third place achieved in 2017 (Mitre, 2017; OWASP, 2017). Authentication tokens, credentials (usernames and passwords), and online transactions are at times compromised and exposed to unauthorised parties (OWASP, 2021).

There may be SQL injection-related faults (OWASP, 2017, 2021) to retrieve sensitive details when in transit in clear text, which cyber-attackers may use for malicious purposes. Moreover, developer-related errors, such as not leveraging secure protocols, e.g., HTTPS, for logging in on web pages, using old encryption algorithms or storing passwords outside secret management tools, may also lead to cyber-attacks (Lazar *et al*., 2014).

A sequence diagram outlining the common causes and the key steps that may lead to cryptographic failures (Lazar *et al*., 2014; OWASP, 2021) is displayed in the attached **Fig. 1**, created via the tool Sequencediagram.org (Sequence Diagram tool, 2022), deemed appropriate to illustrate the key steps involved in ‘sensitive data exposure’ (OWASP, 2017).

Diagram

Description automatically generated

**Figure 1**. Sequence diagram of steps leading to cryptographic failures.

Such cryptographic failures can be prevented by leveraging (OWASP, 2017, 2021):

-   Robust and adaptive hashing algorithms with a delay factor to store credentials, such as Argon2 and PBKDF2.

-  Secure and up-to-date protocols to transfer sensitive information.

-  Authenticated encryption should be in place.

-  Random keys for masking credentials and storing them as byte arrays.

- Up-to-date hashing algorithms to store credentials, as one-way methods that cannot be decrypted.

**References**

Lazar, D., Chen, H., Wang, X. & Zeldovich, N. (2014) ‘Why does cryptographic software fail’.  *Proceedings of 5th Asia-Pacific Workshop on Systems*, 2014 Beijing, China. ACM, 7.

Mitre (2017) Weaknesses in OWASP Top Ten.

OWASP (2017) A3 Sensitive Data Exposure. Retrieved from [**https://cwe.mitre.org/data/definitions/1029.html**](https://cwe.mitre.org/data/definitions/1029.html).

OWASP (2021) A02 Cryptographic failures. Retrieved from [**https://owasp.org/Top10/A02\_2021-Cryptographic\_Failures/**](https://owasp.org/Top10/A02_2021-Cryptographic_Failures/).

[**Sequence Diagram**](https://sequencediagram.org/%20%20) tool (2022) Retrieved from sequencediagram.org.