Graphical user interface, text, application

Description automatically generatedGraphical user interface, text, application, email

Description automatically generated

Diagram

Description automatically generated

Web applications and application programming interfaces (APIs) in finance and healthcare 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, or they may compromise its integrity. Such sensitive data are often accessed by these unauthorised parties when absent or inadequate data protection mechanisms occur, e.g., encryption at rest or in transit, or permissions not appropriately set (OWASP, 2017, 2021).

Until the OWASP’s ranking in 2017 (Mitre, 2017), these cryptographic failures (OWASP, 2021), were named ‘sensitive data exposure’, were ranked third (OWASP, 2017), but recently rose to the second place (OWASP, 2021). Besides PII, applications’ authentication tokens, credentials (usernames and passwords), and online transactions are at times compromised and exposed to unauthorised parties (OWASP, 2021).

For example, whilst cards’ details may be encrypted automatically at rest, when such information is in transit, there may be SQL injection-related faults (OWASP, 2017, 2021), which my colleague Andrea discussed, to retrieve such cards’ details in clear text, which cyber-attackers may use for malicious purposes.

A flowchart of the key steps that may lead to cryptographic failures is displayed in **Fig. 1**, created via the tool Sequencediagram.org (Sequence Diagram tool, 2022), deemed appropriate to illustrate the key steps involved in ‘sensitive data exposure’.

Diagram

Description automatically generated

**Figure 1**. A flowchart of the key steps leading to cryptographic failures, created via the tool Sequencediagram.org (Sequence Diagram tool, 2022).

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

* Robust and adaptive hashing algorithms with a delay factor to store credentials, such as Argon2 and PBKDF2.
* Avoiding old protocols, e.g., file transfer protocol (FTP) and simple mail transfer protocol (SMTP), to transfer sensitive information.
* Rather than solely using encryption, authenticated encryption should be in place.
* Random keys should be generated for masking credentials, such as passwords, and stored as byte arrays.

**References**

Mitre (2017) Weaknesses in OWASP Top Ten.

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

OWASP (2021) A02 Cryptographic failures. Retrieved from <https://owasp.org/Top10/A02_2021-Cryptographic_Failures/>.

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