**SDEV245 – Diss 2**

In 2019, Facebook found that millions of user passwords were accidentally saved as plain, readable text in their internal company logs. This meant employees could see these passwords if they had access, putting people’s accounts at risk.

This happened because passwords were not protected using hashing, so they were saved exactly as users entered them, making them easy for anyone with access to read. Additionally, programming mistakes or missing security checks allowed the systems to store passwords in logs.

To prevent incidents like storing passwords in plain text, it's important to always use secure hashing algorithms when protecting passwords. Adding a random ‘salt’ to each password makes them unique and more difficult to crack. Passwords should never be recorded in system logs, so it’s crucial to regularly check code and logs for any accidental exposures. Finally, sensitive data and logs should only be accessible to trusted individuals to maintain security.

**References**

23, R. M. (2019, March 21). *Facebook stored hundreds of millions of user passwords in plain text for years*. Krebs on Security. https://krebsonsecurity.com/2019/03/facebook-stored-hundreds-of-millions-of-user-passwords-in-plain-text-for-years/

Arias, D. (2025, January 17). *Add salt to hashing: A better way to store passwords*. Auth0. https://auth0.com/blog/adding-salt-to-hashing-a-better-way-to-store-passwords/

Authgear. (2025, September 9). *Comprehensive guide to cryptographic failures (OWASP top 10 A02)*. https://www.authgear.com/post/cryptographic-failures-owasp