Insecure Cryptographic Storage

- **Attackers typically don't break the crypto. They break something else, such as find keys, get cleartext copies of data**, or access data via channels that automatically decrypt.
- **The most common flaw in this area is simply not encrypting data that deserves encryption.**
- **Use of weak or unsalted hashes to protect passwords** is also common.
- External attackers have difficulty detecting such flaws due to limited access.
- **Failure frequently compromises all data that should have**
- **been encrypted. Typically this information includes sensitive data such as health records, credentials, personal data, credit cards, etc.**

The first thing you **have to determine is which data is sensitive enough to require encryption**. For example, **passwords, credit cards, health records, and personal information should be encrypted**. For all such data, ensure:

1. It is **encrypted everywhere it is stored long term, particularly in backups of this data**.
2. **Only authorized users can access decrypted copies** of the data (i.e., access control – See A4 and A8).
3. A **strong standard encryption algorithm** is used.

4. A strong key is generated, protected from unauthorized access, and key change is planned for.

The full perils of unsafe cryptography are well beyond the scope of this Top 10. That said, for all sensitive data deserving encryption, do all of the following, at a minimum:

1. Considering the threats you plan to protect this data from (e.g., insider attack, external user), make sure you encrypt all such data at rest in a manner that defends against these threats.
2. Ensure **offsite backups are encrypted, but the keys are managed and backed up separately.**
3. Ensure **appropriate strong standard algorithms** and strong keys are used, and key management is in place.
4. Ensure passwords **are hashed with a strong standard algorithm and an appropriate salt** is used.
5. Ensure **all keys and passwords are protected from unauthorized access.**