Authentication

From the moment you store valuable information like Personal Identifiable Information, sensitive or medical data, you must protect that data.

Authentication will identify the user and protect the access to data. It functions as a gatekeeper to access the user’s data.

A secure authentication mechanism must implement:

- A solid password policy
- Account information is securely stored by using the approved hashing algorithms using a user specific random value (salt)
- Login information must only be send using encrypted channels
- Anti-automation and brute force mitigations must protect your authentication against automated hacker attacks
- Ensure that forgotten or recover password mechanisms are according to OWASP recommendations.

In the OWASP Authentication Cheat sheet, you can find several recommendations about these topics.

When a user accesses authenticated pages, you need to keep track of his authentication. This is mostly done by a session.

To ensure a secure session, you must implement:

- The session identifier must be unique and have a good complexity
- The session identifier needs to be re-generated after authentication and re-authentication
- The session and all client stored data needs to be deleted after logout
- After a reasonable time of inactivity, the session needs to be automatically terminated