Access Control

Access control determines what functionality and which data a user can see or edit. You must create a clear overview of which functionalities are accessible by which roles and which users.

The access control mechanism must implement:

- The mechanism must be implemented centrally
- Different users must not be able to access another user his information
- A user must not be able to get more privileges that his roles allow.
- Protection against tampering
- They need to be implemented at the client as the server side

If the application has a higher security risk, step-up authentication needs to be implemented to access high value/risk transactions.

OWASP has an access control cheat sheet where you can find more information about the different types of access control and how to safely implement them.