What is a Cookie?

- We got an User, interact with frontend, frontend send a request to the server, and that request requires us to store somekind of data in the browser (login), so that when the user reload the page we still have that information that the user login, to do this we send back the cookie from the server which is basically store the user autenthication back to the client-side.
- With cookies we can store data in the browser which are customized to that user and does not effect that browser and can be send with request.

Cookie disadvantage

- Since the cookie is now store in the browser with the authentication, user can easily access that cookie and modify the value through the application tab. Because of this reason sensitive data such as login information should not be store in the browser.

What is a Session

+ A session is basically similar to a cookie but instead of storing it in the frontend it session is store in the server-side, at a memmory but eventually we will move to the data base. A client needs to tell the sever to which session he belongs

+ The server will first verify the credentials, if match with the DB, it will generate the Session and send the Session ID back to the browser which is the client side and the Session ID will be store inside of the cookie.

+ Expression session is a server-side framework used to create and manage a session middleware.

Session disadvantages

- As the session state data is stored in the server memeory, it is not good if you are dealing with large amount of data.

What is JWT

+ JSON WebToken, is an open standard that defines a compact and self-contained way for securly transmitting information between parties as a JSON object.

+ JWT contain a header, payload and signature

----------=

What is CSRF

+ Stands for Cross-Site Request Forgery, special kind of attack pattern where people can abuse your session and trick user of your application to execute malicious code.

+ A link via email, that take user to a fake site that looks like our own side, where that fake side will have request that send money to different person using the same validated token in the session. To prevent this we can ensure that people can only use your session when they are working with your views rendered by your application.

Token-based Login

- To ensure this we can use token-based login. Token authentication appoarch is stateless. A token a string value and we can embedeed this into our page, for every request that change the user state (like anything like ordering or does something sensitive) on the server the csurf package will check if the incoming request does have that token. Token is random hash value().

Cookie-based login vulnerable to cross-site request forgery

+ You need to store the session data in a database or keep it in memeory on the server

+ Cookies will be added to the request automatically,

----------=

What is SSO

+ Single sign- on authentication scheme that allows a user to log in with a single ID and password to any of the servral related yet indipendent, software system.

HTTP is stateless

+ a stateless protocol does not require the http server to retain information or status about each user for the duration of multiple requests.

What is OAUTH 2.0

+ an authorization protocol and not authentication protocol. As such it is designed primarily as means of granting access to a set of resouces