**Week 16.2**

**16.2.1 Auth using Cookies**

* Now the cookie is first set by the server and then in every subsequent request the cookie is sent by the browser.
* You can’t do localStorage in Next.js because the very first request that goes out when you enter the URL cannot access the localStorage item. In subsequent requests, we can send the auth header but not in the first request.
* Next.js server needs to have user specific data so it can do SSR and provide a pre-rendered page.
* When you log out, the cookie gets cleared.
* Browser automatically sets the set-cookie header when it comes back as a response header. It then automatically sents it in every subsequent request.
* CSRF – Cross Site Request Forgery. In CSRF attacks, cookies can be sent from any malicious website etc and the server accepts it. The thing is cookies get stored in the browser and if you go over on the malicious website then that website can send a request to our server and the cookie would be sent.
* SameSite solves this.
* You should never SameSite:none
* Lax is between none and strict. It only allows get request and top level navigation.
* Use jwt to encode cookies.