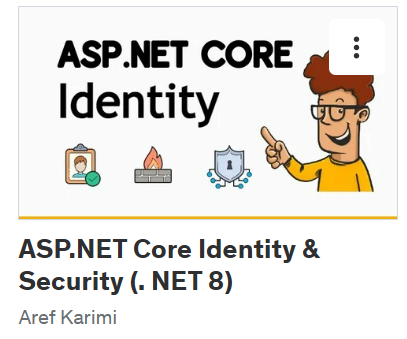
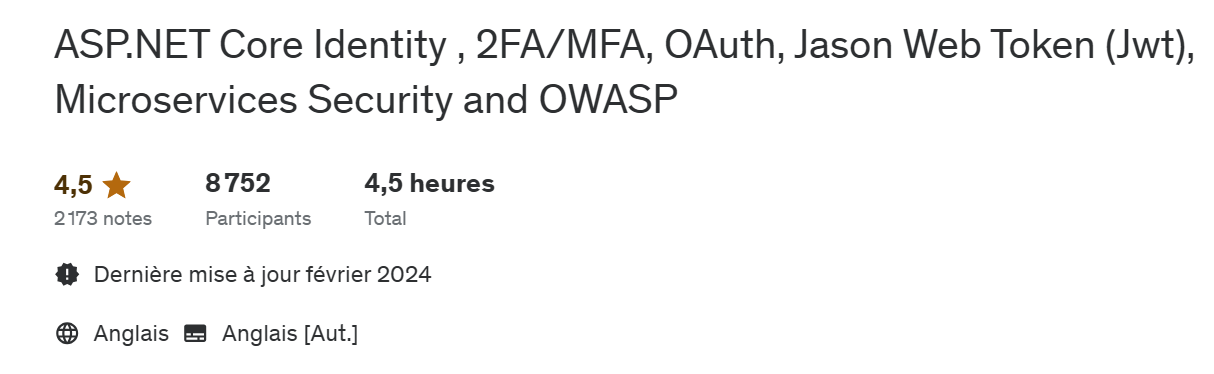
# ASPNET Core Identity & Security

<https://mern.udemy.com/course/aspnet-core-2-security-and-identity-management-with-c/learn/lecture/9908504#overview>





# Identity, Rôle and Claim





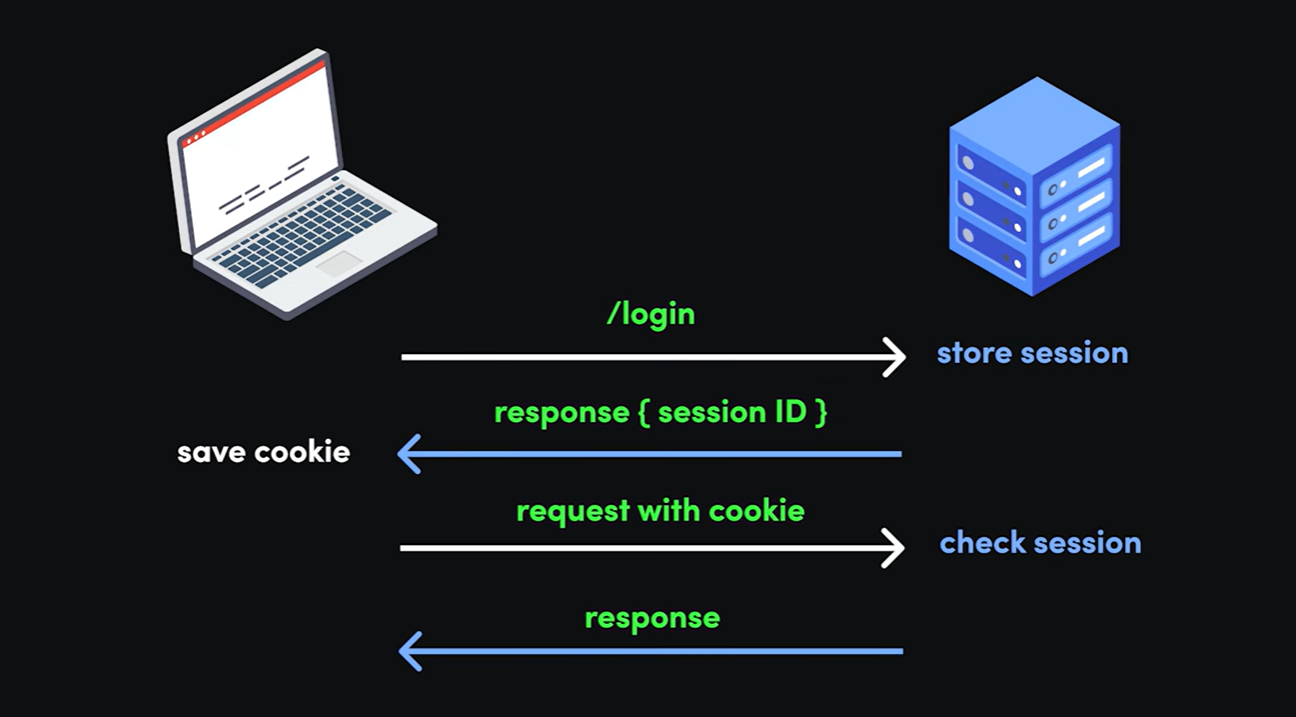


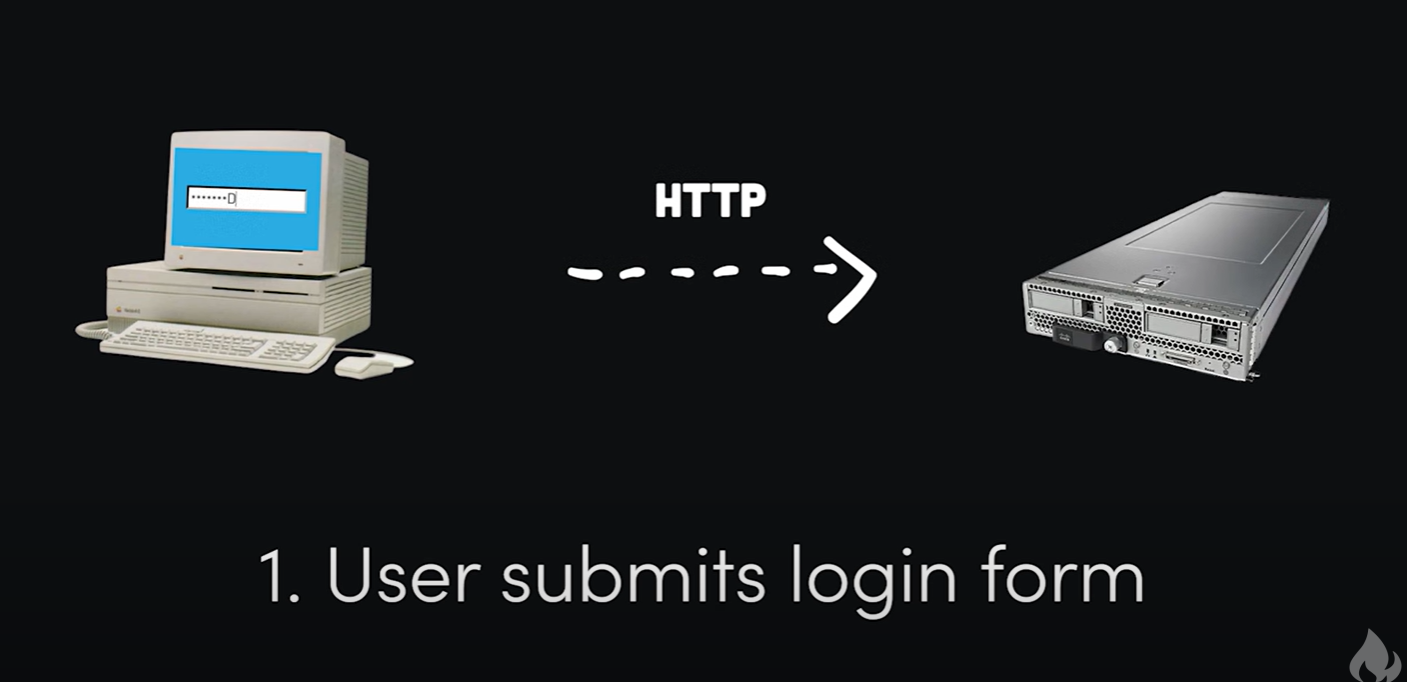
<https://www.youtube.com/watch?v=UBUNrFtufWo>

**Token Auth (JWT)** : Open Authentication : Users and claims are managed by OAuth Provider (ie, Google, FaceBook…), good for mobile apps, javascript…

**Session Cookie Auth**: Users, Roles and Claims are stored in and managed by the application, good for server to server auth

Le session est gardé en mémoire sur le serveur ou dans une BD (SQL, AWS Cognito, 3rd Party Auth Provider, e.g.AuthO <https://auth0.com/>



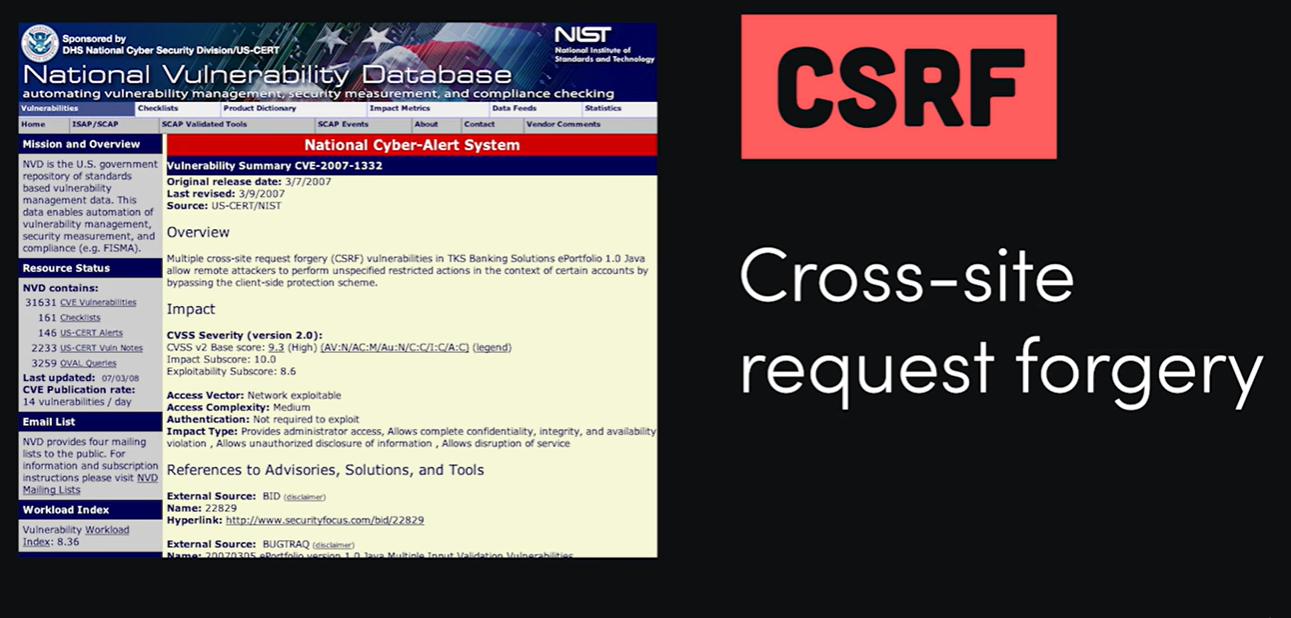
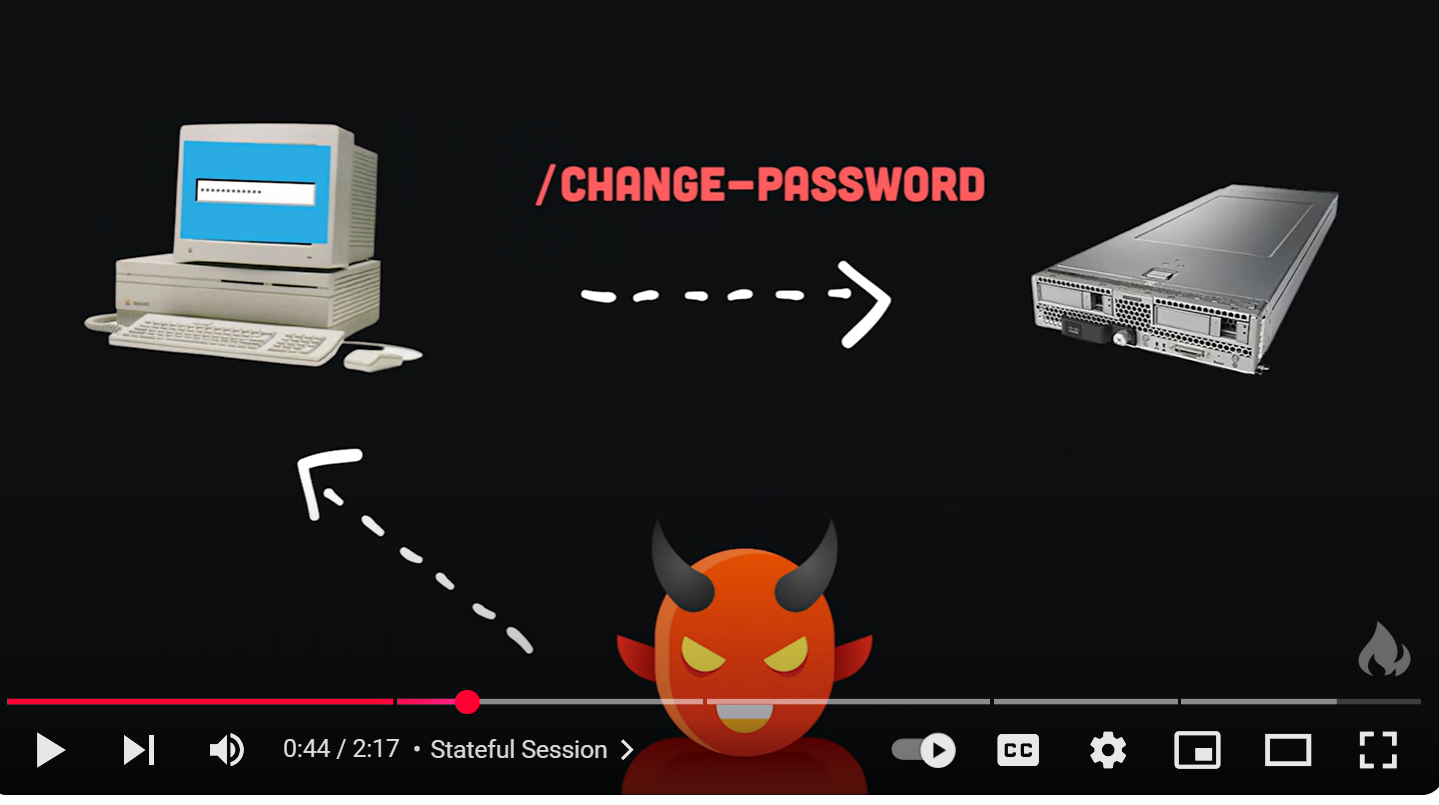








L’inconvenant du Session Cookie:

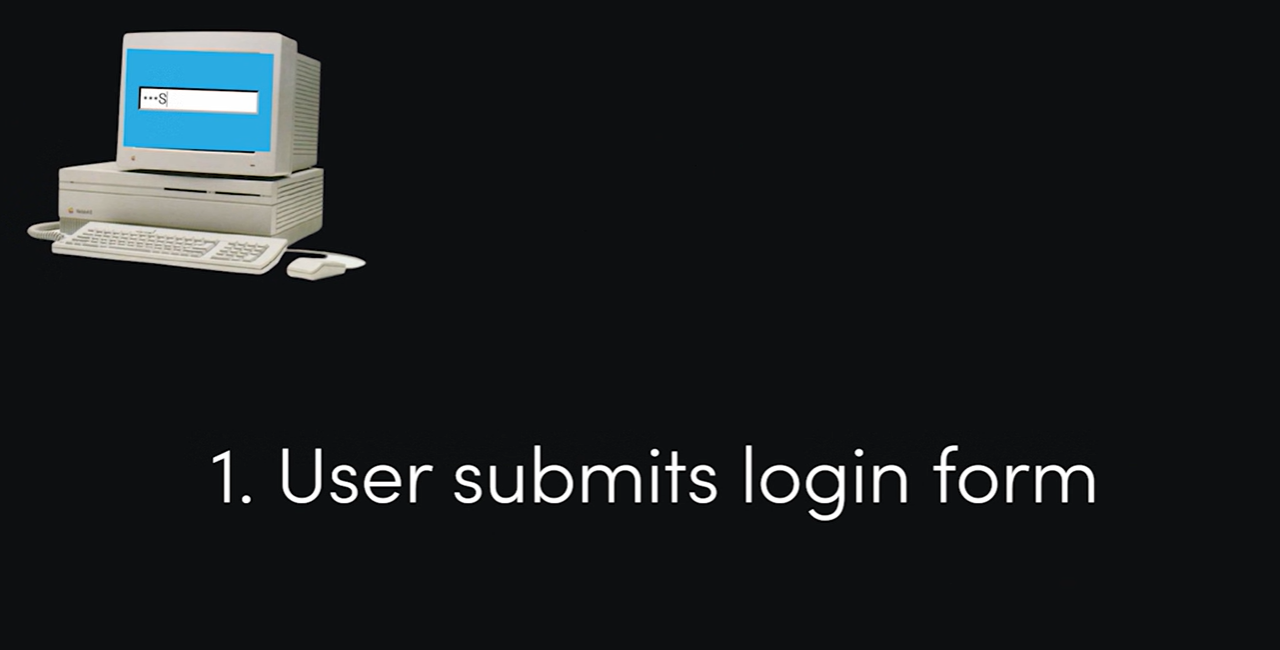


Brings bottle neck!!!



Plus populaire aujourd’hui :















Mais le token pourrait être intercepte par un hacker







# ASP.NET Identity

* IdentityUser
* IdentityRole
* IdentityUserRole
* IdentityUserClaim

Github : <https://github.com/aussiearef/asp-net-identity-v2?tab=readme-ov-file>