Opslaan JWT-token en UserID in front-end

Localstorage

Geen goed idee om hem in local storage op te slaan, sinds de token dan gehackt kan worden via een xss (cross site scripting) aanval. Localstorage is goed te gebruiken, maar als het gaat om gevoelige informatie zoals een JWT-Token of een UserID is dit niet aan te raden.

Cookie

Het gebruik van een cookie is in dit project een uitstekende oplossing om gevoelige data op te slaan. Door het gebruik van een cookie is het alleen mogelijk voor de server om de data uit te lezen. Niemand aan de client side kan de contents van de cookie inzien. Dit is daarom ook ideaal geschikt voor het opslaan van gevoelige data. In dit project zal dan ook gebruik gemaakt gaan worden van cookies in de frontend.

In deze cookie wordt alleen de JWT Token opgeslagen. Alle benodigde informatie die nodig is voor de server, zoals de token en de user UUID wordt daarin opgeslagen. De token wordt gedecode telkens dat deze informatie nodig is.