Une image contenant texte, Police, Graphique, capture d’écran

Description générée automatiquement

Luca Zacheo

luca.zacheo@heig-vd.ch

SLH – Lab02

Authentication

**Résumé**

The goal of this project is to manage the authentication of a simple website.

The authentication should be managed with JWT access and refresh tokens.

# Questions

* 1. **What is the purpose of a JWT access token?**

Les access tokens JWT servent à identifier et authentifier un utilisateur. Les access tokens peuvent être utilisés pour empêcher une personne non autorisée d’accéder à une ressource protégée.

**And what is the purpose of a JWT refresh token?**

refresh tokens sont utilisés pour générer un nouvel access token.

En général, si l‘access token a une date d'expiration, une fois qu'il expire, l'utilisateur devrait se réauthentifier pour en obtenir un nouveau.

Avec le jeton de rafraîchissement, cette étape peut être contournée, et en faisant une demande à l'API, obtenir un nouveau jeton d'accès qui permet à l'utilisateur de continuer à accéder aux ressources de l'application.

Haut du formulaire

**Why do we have both?**

Un sert à définir si une personne est légitime à accéder à certaines données et un autre sert à renouveler cette légitimité dans le cas où elle viendrait à expirer à un moment où l’utilisateur a toujours besoin de cet accès.

* 1. **Where are the access tokens stored?**

Ils sont stockés dans les cookies et envoyés au client.

**Where are the refresh tokens stored?**

Ils sont stockés côtés serveur sur de stockage persistant. (DB par exemple)

* 1. **Is it a good idea to store them there?**

Conserver les tokens côté client est une méthode fréquemment utilisée et elle peut être sûre lorsqu'elle est correctement mise en œuvre. Mon code utilise les paramètres « HTTP-only » et « Secure » pour les cookies, dans le but d'empêcher leur accès par des scripts exécutés côté client, ce qui diminue les potentiels risques liés aux attaques XSS.

**Is there a better solution?**

Actuellement, l'équilibre entre efficacité et sécurité est bien maintenu par la méthode que j'utilise.

Toutefois, on pourrait renforcer la sécurité, en déplaçant le stockage des tokens du côté serveur. Cette approche impliquerait de limiter la communication avec le client aux seuls identifiants de session, réduisant ainsi les risques associés au vol de jetons. Il est à noter, cependant, que cette méthode pourrait augmenter la charge et la complexité du serveur, contrairement à l'utilisation actuelle des caractéristiques « HTTP-only » et « Secure » pour les cookies, qui offre déjà un niveau de sécurité suffisant.**Haut du formulaire**