WebShop



Benjamin Blouin – Cid2A

Vennes

8 semaine

Gaël Sonney

gael.sonney@eduvaud.chTable des matières

[1 Spécifications 3](#_Toc192835201)

[1.1 Description 3](#_Toc192835202)

[2 Réalisation 3](#_Toc192835203)

[2.1 Https 3](#_Toc192835204)

[2.2 Route login 3](#_Toc192835205)

[2.3 Route getUser 4](#_Toc192835206)

[2.4 Les token JWT 4](#_Toc192835207)

[2.5 Les token JWT 4](#_Toc192835208)

[Conclusion 4](#_Toc192835209)

# Spécifications

## Description

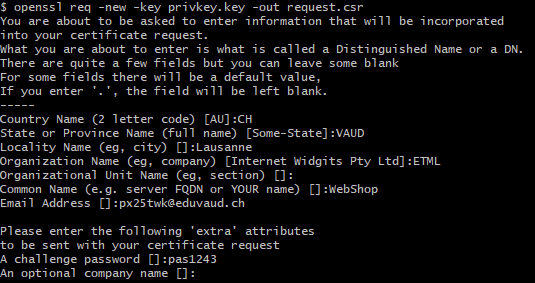
# Le projet consistait à créer un site web (boutique en ligne sécurisée) avec un login permettant aux utilisateurs et aux administrateurs de se connecter. Pour ce faire, nous avons utilisé des jetons JWT pour rester connectés, et nous avons également créé une base de données connectée au site web pour la gestion des utilisateurs. Sur la page d'administration, il y a une barre de recherche pour rechercher des utilisateurs dans une table.

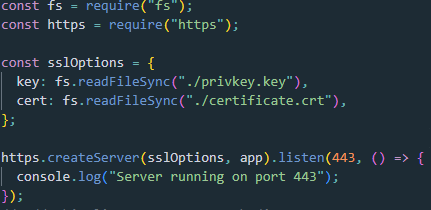
# Réalisation

## Https

Pour utiliser https, mon site utilise openSSL, qui génère un certificat et une clé privée. Cela se fait à l'aide de 3 commandes :

openssl genrsa -out server.key 6033  
openssl req -new -key server.key -out server.csr  
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt

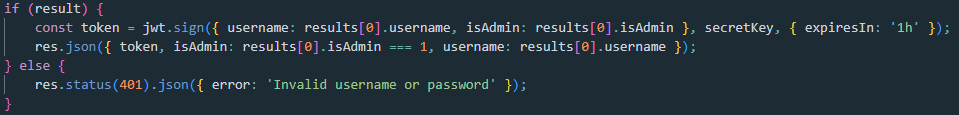


Remplacer le port par 443 et ajouter les fichiers privkey.key et certificate.crt.

## Route login

Pour se connecter au site, la requête passe par la route login, qui recherche un nom d'utilisateur comme celui-ci, ce qui, avec le [req.body.username] en dehors de la commande, le transforme en une chaîne de caractères et évite tout type d'ingection sql.

Une fois l'utilisateur trouvé, nous comparons le mot de passe saisi avec le mot de passe de la base de données, en utilisant bcrypt pour le hacher.

Enfin, si tout est juste, nous avons créé un jeton jwt avec le nom d'utilisateur et le bool isAdmin comme charge utile (pas le mot de passe, car un jeton jwt peut être décrypté).

## 2.3 Route getUser

La route get user permet de chercher la liste des utilisateurs pour l’afficher sur la page administration. Cela commence par chercher et vérifié le token jwt pour vérifier si c’est le bon utilisateur et après fait une recherche sur la base de donné en utilisant un like sur le nom d’utilisateur.





## 2.4 Les token JWT

Dans mon secure webshop les token jwt ne redirige pas l’utilisateur sur la page login si le token n’est pas/plus valide mais block le tableau et la barre de recherche sur la page admin qui le rends inutilisable.

# Conclusion

Secure Webshop m’a permis d’apprendre a utilisé des Framework reconnu comme « bycrpt », cela m’a aussi permis d’apprendre à construire des routes et de comment faire une authentification efficace. L’utilisation des token JWT m’a montré comment même les plus grand site fond pour protéger leurs routes. Ce module m’a forcé à chercher comment faire du SQL dans du java script qui m’a fait progresser.