P\_APP\_183-Secured-WebShop

Une image contenant personne, ordinateur, Appareil électronique, ordinateur portable

Le contenu généré par l’IA peut être incorrect.

<https://www.cyberuniversity.com/post/quest-ce-que-lauthentification-et-pourquoi-cest-crucial-en-matiere-de-securite-informatique>

Mathieu Bamert – CID 2B

Lausanne Venne

24p

Cédric Schaffter

Table des matières

[1 Spécifications 3](#_Toc192846289)

[1.1 Titre 3](#_Toc192846290)

[1.2 Description 3](#_Toc192846291)

[1.3 Matériel et logiciels à disposition 3](#_Toc192846292)

[1.4 Prérequis 3](#_Toc192846293)

[1.5 Cahier des charges 3](#_Toc192846294)

[1.5.1 Dockerisation 3](#_Toc192846295)

[1.5.2 Profil du client 3](#_Toc192846296)

[1.5.3 HTTPS 3](#_Toc192846297)

[1.5.4 Authentification par mot de passe 3](#_Toc192846298)

[1.5.5 Vérification du token JWT 3](#_Toc192846299)

[1.5.6 Administration 4](#_Toc192846300)

[1.5.7 Protection contre les injections SQL 4](#_Toc192846301)

[1.5.8 Utilisation de bcrypt 4](#_Toc192846302)

[1.5.9 Versioning 4](#_Toc192846303)

[1.5.10 Documentation 4](#_Toc192846304)

[1.5.11 Utilisation de l’IA 4](#_Toc192846305)

[1.6 Les points suivants seront évalués 4](#_Toc192846306)

[1.7 Validation et conditions de réussite 4](#_Toc192846307)

[2 Planification Initiale 5](#_Toc192846308)

[3 Analyse 5](#_Toc192846309)

[3.1 Explication du code 5](#_Toc192846310)

[5](#_Toc192846311)

[4 Réalisation 8](#_Toc192846312)

[4.1 Conception de Schéma 8](#_Toc192846313)

[5 Tests 9](#_Toc192846314)

[5.1 Dossier des tests 9](#_Toc192846315)

[6 Conclusion 9](#_Toc192846316)

[6.1 Bilan personnel 9](#_Toc192846317)

[7 Divers 9](#_Toc192846318)

[7.1 Webographie 9](#_Toc192846319)

# Spécifications

## Titre

Création d’un site d’e-commerce sécurisé

## Description

On doit créer un site d’e-commerce sécurisé. On se concentre principalement sur la page d’authentification. Les mots de passe sera protégé par un hashage, salage et un JWT.

## Matériel et logiciels à disposition

Un ordinateur standard de la section informatique avec Docker Desktop

## Prérequis

On doit avoir suivi le module 183.

## Cahier des charges

### Dockerisation

L’ensemble des services web sera conteneurisé.

### Profil du client

Le client peut accéder à son propre profil depuis la page de bienvenue. Seul son profil lui sera rendu visible et les routes du backend seront protégées.

### HTTPS

Il doit être possible d’accéder à votre site de e-commerce de manière sécurisée (https://localhost). Le port utilisé sera le 443. Le certificat sera auto-signé par OpenSSL.

### Authentification par mot de passe

L’utilisateur devra s’authentifier par la page https://localhost/login Le mot de passe sera haché et salé avant d’être stocké dans la base de données (table t\_users).

### Vérification du token JWT

Le token devra être vérifié lorsque l’utilisateur vous l’envoie et la signature du jeton devra aussi être utilisée pour vérifier que le token n’a pas été modifié.

### Administration

Une page d’administration devra avoir un champ de recherche (Nom du visiteur) et permettre d’afficher tous les utilisateurs ayant tout ou partie de ce nom.

### Protection contre les injections SQL

Votre page d’administration devra être protégée contre les injections SQL. Sans utiliser sequelize ou tout autre ORM, votre site devra être robuste face aux injections. L’utilisation de sequelize (ou autre ORM) sera autorisée dans l’approfondissement du projet.

### Utilisation de bcrypt

Une fois l’authentification faite avec votre propre mécanisme (mot de passe en base de données, salé et haché). Vous modifierez votre code pour utiliser bcrypt. Votre code doit prévoir une condition pour utiliser soit bcrypt soit votre propre implémentation.

### Versioning

Votre code sera versionné sur Github et un .gitignore empêchera de versionner les binaires npm (dossiers node\_modules, documents word/excel). Votre dépôt sera partagé avec votre chef de projet dès le début du projet.

### Documentation

* Journal de travail (1 ligne par quart d’heure de travail)
* Rapport, contenant :
  + Votre conceptualisation (schéma)
  + Des explications sur votre code
  + Une conclusion sur le travail fourni et sur l’attitude face au projet

### Utilisation de l’IA

Une utilisation injustifiée de l’IA ou une absence de maîtrise du code, induira un non-acquis dans les compétences techniques du projet.

## Les points suivants seront évalués

* Le rapport
* Les planifications (initiale et détaillée)
* Le journal de travail
* Le code et les commentaires
* Les documentations de mise en œuvre et d’utilisation

## Validation et conditions de réussite

* Compréhension du travail
* Possibilité de transmettre le travail à une personne extérieure pour le terminer, le corriger ou le compléter
* Etat de fonctionnement du produit livré

# Planification Initiale

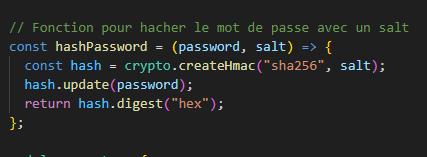
Ma planification n’était pas très bien, je n’ai pas bien expliqué mes taches que j’allais faire la semaine d’après.

# Analyse

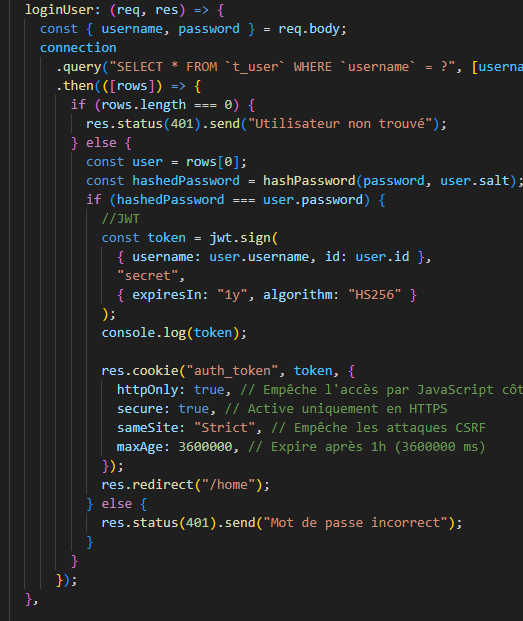
## Explication du code

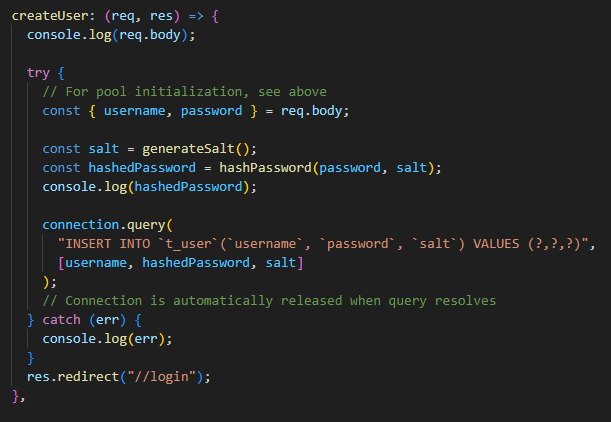
# 

Cette fonction va permettre de vérifier si le token est valable ou pas. Et après no va nous rediriger sur la route /home si le token est valide. Sinon on nous redirige à nouveau sur la route /login.



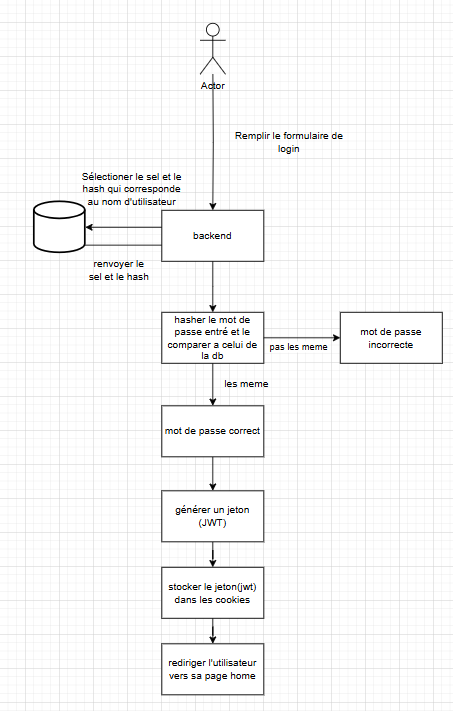
Cette fonction sert a haché mon mot de passe et le salt. Avec la manière sha-256.





# Réalisation

## Conception de Schéma



J’ai fait un schéma, comment marche le login. L’utilisateur rempli le formulaire de login. On compare les hash, si le hash est le même le mot de passe est correct s’il est différent le mot de passe est faux. Après on va générer le jeton (JWT) et on le stocke dans les cookies

# Tests

## Dossier des tests

Mon plus gros problème que j’ai eu était dans mon code, ça ne marchait pas car je n’avais pas importé une librairie. Ça m’a pris presque 2 semaines à le faire. Et là j’ai un problème dans mes routes, la page home ne s’affiche pas.

# Conclusion

## Bilan personnel

Je trouvais ce projet très intéressant car j’ai découvert comment fonctionnais l’authentification dans un site Web et que notre mot de passe n’est pas noté en brut dans une base de données. Cependant il y avait beaucoup trop de point dans le cahier des charges. Si je devais refaire ce projet, j’essayerais de passée plus de temps à faire mon rapport.

# Divers

## Webographie

J’ai utilisé l’IA pour régler un problème de redirection. Mais ça ne m’a pas plus aider.

<https://www.w3schools.com/TAGS/att_input_type_email.asp>

<https://stackoverflow.com/questions/18629327/adding-css-file-to-ejs>

<https://www.geeksforgeeks.org/how-to-connect-to-a-mysql-database-using-the-mysql2-package-in-node-js/>

<https://github.com/mysqljs/mysql?tab=readme-ov-file#introduction>

<https://www.npmjs.com/package/body-parser>

<https://sidorares.github.io/node-mysql2/docs#first-query>

<https://stackoverflow.com/questions/11625519/how-to-access-the-request-body-when-posting-using-node-js-and-express>

<https://stackoverflow.com/questions/62455716/typeerror-cannot-destructure-property-userid-of-req-body-as-it-is-undefined>

<https://laconsole.dev/blog/hacher-mot-de-passe-js-bcrypt#utiliser-bcrypt-pour-hacher-un-mot-de-passe>

[Implémentation de Bcrypt pour le hachage des mots de passe dans Node.j – peerdh.com](https://peerdh.com/fr/blogs/programming-insights/implementing-bcrypt-for-password-hashing-in-node-js)

<https://dev.to/franciscomendes10866/using-cookies-with-jwt-in-node-js-8fn>

[authentification - Recherche](https://www.bing.com/images/search?view=detailV2&ccid=tw4HmwD6&id=6EEA72A4136BE55FBBA3EDA5D7133D667B2FD1F3&thid=OIP.tw4HmwD6M2_WMa_UwfeF4wHaDh&mediaurl=https%3a%2f%2fuploads-ssl.webflow.com%2f601057763f823a0bf65a8071%2f61dec7c565cc1be23d0d35af_Authentification+article.png&cdnurl=https%3a%2f%2fth.bing.com%2fth%2fid%2fR.b70e079b00fa336fd631afd4c1f785e3%3frik%3d89Eve2Y9E9el7Q%26pid%3dImgRaw%26r%3d0&exph=918&expw=1927&q=authentification+&simid=608014211621138924&FORM=IRPRST&ck=429B359EA31E3D88859D528AC93FA5BB&selectedIndex=1&itb=0&mode=overlay)