P\_APP Site E-commerce



Samuel Sallaku – CID2B

Section Informatique

24p

C. Schaffter

Table des matières

[1 Spécifications Erreur ! Signet non défini.](#_Toc192844246)

[1.1 Titre **Erreur ! Signet non défini.**](#_Toc192844247)

[1.2 Description **Erreur ! Signet non défini.**](#_Toc192844248)

[1.3 Matériel et logiciels à disposition **Erreur ! Signet non défini.**](#_Toc192844249)

[1.4 Prérequis **Erreur ! Signet non défini.**](#_Toc192844250)

[2 Planification Initiale 5](#_Toc192844251)

[3 Réalisation 5](#_Toc192844252)

[3.1 Schéma 5](#_Toc192844253)

[3.2 Explication du code 6](#_Toc192844254)

[4 Tests 7](#_Toc192844255)

[4.1 Dossier des tests 7](#_Toc192844256)

[5 Conclusion 7](#_Toc192844257)

[5.1 Bilan des fonctionnalités demandées 7](#_Toc192844258)

[5.2 Bilan personnel 7](#_Toc192844259)

[6 Divers 7](#_Toc192844260)

[6.1 Utilisation d’IA 7](#_Toc192844261)

# Spécifications

## Titre

P\_App-Webstore

## Description

Développer un site e-commerce avec une authentification sécurisée (hashage personnalisé et JWT), incluant une page de login, une interface admin et une page utilisateur.

## Matériel et logiciels à disposition

Un ordinateur standard de la section informatique avec Docker Desktop

## Prérequis

I183-SécuritéApplication-CSR

## 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

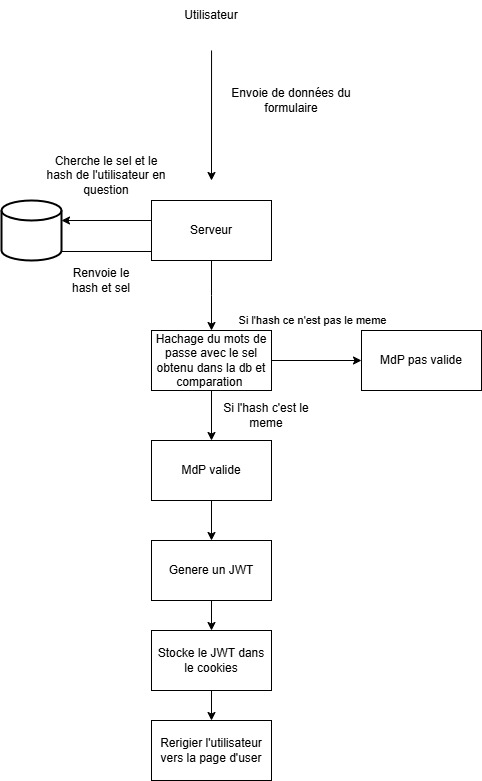
# Planification Initiale

Voir la planification dans le Journal de travail. J’ai commencé par planifier les 3 premières semaines et au fil du temps j’ai rempli le reste, tout en remplissant chaque séquence le journal de travail.

# Réalisation

## Schéma

Pas eu le temps de faire un schéma, mais j’ai repris celui d’un de mes camarades qui correspond à ce que j’ai. (Gonzalo)



## Explication du code

**App/controllers :** La plupart de l’implémentation des routes se trouve dans le contrôleur. Elles sont ensuite appelées dans le app.mjs et utilisées là, avec les vérifications d’authentification. Il y a des routes qui se trouvent dans « UserRoutes.mjs », où j’ai fait les routes qui vont afficher le profil d’un utilisateur.

**Nb pages :**  Il existe plusieurs pages, dont

* Homepage
* Login
* Register
* Admin
* Users
* Logout(pas vraiment une page)

**App/public/css** : Ce sont les feuilles de style utilisées pour donner un style au site web.

**App/auth :** Ceci contient le fichier pour la clé privée utilisée lors de l’hashage du mot de passe. Il contient aussi les méthodes qui vont vérifier les jetons JWT afin de laisser l’accès aux routes protégées (auth.js).

**App/models :** ceci est le fichier qui va établir la connexion avec la DB, ainsi que créer une connexion afin de pouvoir faire des requêtes.

**App/routes :** Contient le fichier userRoutes.js, qui permet le routage vers le profil d’un utilisateur

**Server.js**: Contient des middlewares qui vont créer certaines URL et protéger les routes

**De manière générale :** Les importations sont toutes faites en haut de chaque fichier, afin de savoir ce qu’on importe et ne pas se perdre dans le code.

# Tests

## Dossier des tests

Les tests effectués ont été minimales, j’ai seulement testé si les routes marchaient, si les mots de passe étaient bien hashés ainsi que le salt, puis si la connexion d’utilisateur fonctionne.

Et encore, les routes protégées donc la page /admin est seule accessible par un utilisateur avec le rôle admin.

# Conclusion

## Bilan des fonctionnalités demandées

Il n’était pas compliqué d’implémenter ce qui a été demandé car la théorie et ce qu’il fallait faire avaient un bon lien et on comprenait.

Pour ce rapport, je n’ai pas pu le terminer à 100% car avec tous les modules au même temps, nous avions beaucoup de travail à réaliser surtout la dernière semaine. Donc si c’était à refaire, je commencerais depuis le début avec le rapport et je le remplirais au fur et à mesure.

## Bilan personnel

J’ai trouvé ce projet assez intéressant et utile pour ma formation car, il est très important de sécuriser une app ou un site web lors du développement. J’ai trouvé utile et cela va me servir pour ma formation ainsi que mon futur. L’espace et l’ambiance où j’ai travaillé a été favorable pour moi et sans doute pour tout le monde. J’ai aussi pu aider certains camarades qui étaient bloqués ce qui m’a permis d’améliorer mes compétences

# Divers

## Utilisation d’IA

J’ai utilisé l’IA quelques fois afin de me renseigner sur certains sujets, comme les jetons JWT. J’ai manqué la séance où les jetons ont été faits en classe et donc je me suis renseigné sur ChatGPT sans copier de code, ce qui m’a permis de mieux comprendre comment les utiliser, comme le payload.