Projet P\_Sec  
Site d’e-commerce sécurisé (webstore)

De Pina Correia Ryan – Grp2C

ETML

01.02.2024

Gaël Sonney

Table des matières

[1 Spécifications 3](#_Toc189289868)

[1.1 Titre 3](#_Toc189289869)

[1.2 Description 3](#_Toc189289870)

[1.3 Matériel et logiciels à disposition 3](#_Toc189289871)

[1.4 Prérequis 3](#_Toc189289872)

[1.5 Cahier des charges 3](#_Toc189289873)

[1.5.1 Objectifs et portée du projet (objectifs SMART) 3](#_Toc189289874)

[1.5.2 Caractéristiques des utilisateurs et impacts 3](#_Toc189289875)

[1.5.3 Fonctionnalités requises (du point de vue de l’utilisateur) 3](#_Toc189289876)

[1.5.4 Contraintes 3](#_Toc189289877)

[1.5.5 Travail à réaliser par l'apprenti 4](#_Toc189289878)

[1.5.6 Si le temps le permet … 4](#_Toc189289879)

[1.5.7 Méthodes de validation des solutions 4](#_Toc189289880)

[1.6 Les points suivants seront évalués 4](#_Toc189289881)

[1.7 Validation et conditions de réussite 4](#_Toc189289882)

[2 Planification Initiale 4](#_Toc189289883)

[3 Analyse 4](#_Toc189289884)

[3.1 Opportunités 4](#_Toc189289885)

[3.2 Document d’analyse et conception 4](#_Toc189289886)

[3.3 Conception des tests 5](#_Toc189289887)

[3.4 Planification détaillée 5](#_Toc189289888)

[4 Réalisation 5](#_Toc189289889)

[4.1 Dossier de Réalisation 5](#_Toc189289890)

[4.2 Modifications 5](#_Toc189289891)

[5 Tests 5](#_Toc189289892)

[5.1 Dossier des tests 5](#_Toc189289893)

[6 Conclusion 5](#_Toc189289894)

[6.1 Bilan des fonctionnalités demandées 5](#_Toc189289895)

[6.2 Bilan de la planification 5](#_Toc189289896)

[6.3 Bilan personnel 5](#_Toc189289897)

[7 Divers 6](#_Toc189289898)

[7.1 Journal de travail 6](#_Toc189289899)

[7.2 Bibliographie 6](#_Toc189289900)

[7.3 Webographie 6](#_Toc189289901)

[8 Annexes 6](#_Toc189289902)

# Spécifications

## Titre

Un site d’e-commerce très simple pour des fonctionnalités simple

## Description

Ce projet vise à concevoir et développer un site d’e-commerce sécurisé en Node.js. L'objectif principal est de mettre en place un système d’authentification sécurisé pour les clients et les administrateurs du site, avec un accent sur la protection des données.

## Matériel et logiciels à disposition

• Un ordinateur équipé de Docker Desktop pour la conteneurisation.

## Cahier des charges

### Authentification et sécurité

• Mise en place d’un système d’authentification basé sur JWT.

• Protection des mots de passe avec un mécanisme personnalisé puis bcrypt.

• Utilisation de certificats HTTPS auto-signés via OpenSSL.

### Administration

• Création d’une page d’administration réservée aux administrateurs.

• Recherche et gestion des utilisateurs.

### Protection des données

• Sécurisation contre les injections SQL en limitant l’accès aux bases de données.

• Restriction de l’accès aux profils utilisateurs.

### Documentation

• Versioning du code sur GitHub avec un fichier. gitignore.

• Rapport détaillant la conceptualisation et l’implémentation.

### Technologies utilisées

• Node.js et Express pour le backend.

• SQLite pour la gestion de la base de données.

• JSON Web Token (JWT) pour l’authentification sécurisée.

• OpenSSL pour la gestion des certificats HTTPS.

• bcrypt pour le hachage des mots de passe.

• Docker pour la conteneurisation des services.

## 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

# Analyse

## Opportunités

Ce paragraphe énumère la liste des difficultés potentielles de tout ordre :

Liste des compétences à acquérir ou approfondir

Liste du matériel à exploiter

Recherche d’informations particulières

Gestion du travail en équipe & collaboration

Ainsi que les solutions possibles

Si les spécifications de départ ne laissent pas de doutes sur la manière de réaliser un projet, ce chapitre ne fera que renvoyer le lecteur aux spécifications.

## Document d’analyse et conception

Ce paragraphe décrit le fonctionnement de manière détaillée.

Autant que possible de manière graphique, imagée, tableaux, etc.

Tous les cas particuliers devraient y être spécifiés…

Il s’agit d’y présenter les fonctionnalités à développer :

Découpage en étapes, en modules, en fonctionnalités, etc.

Formulaires, interfaces graphiques, pages web, etc.

Schémas de navigation, schémas événementiels, structogramme, pseudocode, etc.

Si le projet inclut une base de données :

Dictionnaire des données

Modèle conceptuel des données, modèles logique des données.

## Conception des tests

Ce paragraphe permet de spécifier la stratégie de test qui sera menée au point 5.1

Qui, quand, avec quelles données, dans quel ordre, etc.

## Planification détaillée

A ce stade, après l’analyse complète du projet, un planning détaillé et complet (avec tâches, sous-tâches, dépendances, durée, …) peut être finalisé.

Le planning détaillé doit s’inscrire dans le planning initial. Il faut que l’on puisse situer cette planification détaillée par rapport à la planification initiale.

# Réalisation

## Dossier de Réalisation

### Page d’inscription (Signup)

### Page de connexion(Login)

### Page d’Administration (Admin)

### Page de profile (Profile)

## Modifications

Historique des modifications demandées (ou nécessaires) aux spécifications détaillées.

Date, raison, description, etc.

# Tests

## Dossier des tests

On dresse le bilan des tests effectués (qui, quand, avec quelles données…) sous forme de procédure. Lorsque cela est possible, fournir un tableau des tests effectués avec les résultats obtenus et les actions à entreprendre en conséquence (et une estimation de leur durée).

Si des tests prévus dans la stratégie n'ont pas pu être effectués :

raison, décisions, etc.

Liste des bugs répertoriés avec la date de découverte et leur état:

Corrigé, date de correction, corrigé par, etc.

# Conclusion

## Bilan des fonctionnalités demandées

Le site de e-commerce présente plusieurs fonctionnalités clés côté client, visant à offrir une expérience utilisateur fluide, sécurisée et personnalisée. L'utilisateur a accès à son profil via une interface dédiée, accessible uniquement après connexion, garantissant que ses informations personnelles (nom, adresse, préférences) restent privées et sécurisées. L'authentification se fait par une page de connexion sécurisée via HTTPS, où le mot de passe est haché et salé pour être vérifié en toute sécurité. Un token JWT est généré après la connexion pour maintenir l'utilisateur authentifié lors de ses interactions avec le site, assurant ainsi la sécurité des sessions. L'interface d'administration permet aux administrateurs de rechercher et de gérer les utilisateurs, tout en garantissant la protection contre les injections SQL. Enfin, le mot de passe utilisateur est haché à l'aide de bcrypt avant d'être stocké dans la base de données, offrant ainsi une couche supplémentaire de sécurité. Ce système garantit une expérience utilisateur simple, intuitive et conforme aux meilleures pratiques de sécurité web.

## Bilan de la planification

Pour un projet de cette envergure nous avions très largement le temps si nous avions les compétences nécessaires pour le faire dès le départ.

## Bilan personnel

Il manque dans ce projet, une partie théorie car finalement nous ne savions pas comment commencer et avancer le projet dans sa globalité. Sans les outils comme les IA, les vidéos YouTube durant le projet nous n’aurions pas vraiment le temps de finir le projet à temps.

# Divers

## Journal de travail

Date, activité (description qui permet de reproduire le cheminement du projet), durée, liens et références sur des documents externes. Lorsqu’une activité de recherches a été entreprise, il convient d’énumérer ce qui a été trouvé, avec les références.

## Webographie

JWT : [jsonwebtoken - npm](https://www.npmjs.com/package/jsonwebtoken)

Chat GPT : [ChatGPT](https://chatgpt.com/) (Prompt : (tu arrives à me faire chaque chapitre pour un rapport mais côté client donc frontend ce qu’il voit des fonctionnalités etc.))

# Annexes

Listing du code source (partiel ou, plus rarement complet)

Guide(s) d’utilisation et/ou guide de l’administrateur

Etat ou « dump » de la configuration des équipements (routeur, switch, robot, etc.).

Extraits de catalogue, documentation de fabricant, etc.