P\_Web 183



Romain Denis – CID2B

ETML - Vennes

8 Semaines

Cédric Schaffter

Table des matières

Table des matières

[1 Spécifications 3](#_Toc187673788)

[1.1 Titre 3](#_Toc187673789)

[1.2 Description 3](#_Toc187673790)

[1.3 Matériel et logiciels à disposition 3](#_Toc187673791)

[1.4 Prérequis 3](#_Toc187673792)

[1.5 Cahier des charges 3](#_Toc187673793)

[1.5.1 Objectifs et portée du projet (objectifs SMART) 3](#_Toc187673794)

[1.5.2 Caractéristiques des utilisateurs et impacts 3](#_Toc187673795)

[1.5.3 Fonctionnalités requises (du point de vue de l’utilisateur) 3](#_Toc187673796)

[1.5.4 Contraintes 3](#_Toc187673797)

[1.5.5 Travail à réaliser par l'apprenti 4](#_Toc187673798)

[1.5.6 Si le temps le permet … 4](#_Toc187673799)

[1.5.7 Méthodes de validation des solutions 4](#_Toc187673800)

[1.6 Les points suivants seront évalués 4](#_Toc187673801)

[1.7 Validation et conditions de réussite 4](#_Toc187673802)

[2 Planification Initiale 4](#_Toc187673803)

[3 Analyse 4](#_Toc187673804)

[3.1 Opportunités 4](#_Toc187673805)

[3.2 Document d’analyse et conception 4](#_Toc187673806)

[3.3 Conception des tests 5](#_Toc187673807)

[3.4 Planification détaillée 5](#_Toc187673808)

[4 Réalisation 6](#_Toc187673809)

[4.1 Dossier de Réalisation 6](#_Toc187673810)

[6.1 Dockerisation L’ensemble des services web sera conteneurisé. 6](#_Toc187673811)

[6.2 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. 6.3 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 6](#_Toc187673812)

[6.4 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). 6](#_Toc187673813)

[6.5 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. 6](#_Toc187673814)

[6.6 Administration 6](#_Toc187673815)

[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. 6](#_Toc187673816)

[6.7 Protection contre les injections SQL 6](#_Toc187673817)

[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. 6](#_Toc187673818)

[6.8 Utilisation de bcrypt 6](#_Toc187673819)

[6.9 Versioning 6](#_Toc187673820)

[6.10 Documentation 7](#_Toc187673821)

[6.11 Utilisation de l’IA 7](#_Toc187673822)

[5 Tests 7](#_Toc187673823)

[5.1 Dossier des tests 7](#_Toc187673824)

[6 Conclusion 7](#_Toc187673825)

[6.1 Bilan des fonctionnalités demandées 7](#_Toc187673826)

[6.2 Bilan de la planification 7](#_Toc187673827)

[6.3 Bilan personnel 7](#_Toc187673828)

[7 Divers 7](#_Toc187673829)

[7.1 Journal de travail 7](#_Toc187673830)

[7.2 Bibliographie 7](#_Toc187673831)

[7.3 Webographie 8](#_Toc187673832)

[8 Annexes 8](#_Toc187673833)

# Spécifications

## Titre

P\_APP\_183 : Secured WebShop

## Description

A compléter,par une explication du contexte, de la situation, des raisons générales de la mise en route d’un tel projet. Le lecteur doit pouvoir comprendre les motivations du lancement du projet…

## Matériel et logiciels à disposition

Un ordinateur standard de la section informatique avec Docker Desktop

## Prérequis

A compléter par une description des compétences, des connaissances et de la formation minimum pour être à même de réaliser le 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

# 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

## 6.1 Dockerisation

*L’ensemble des services web sera conteneurisé.*

## 6.2 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.*

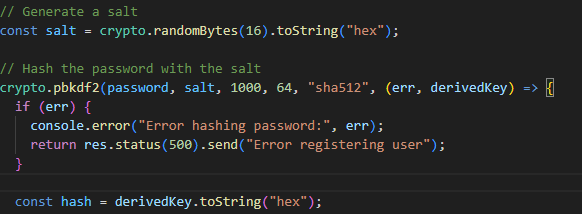
## 6.3 HTTPS

*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*

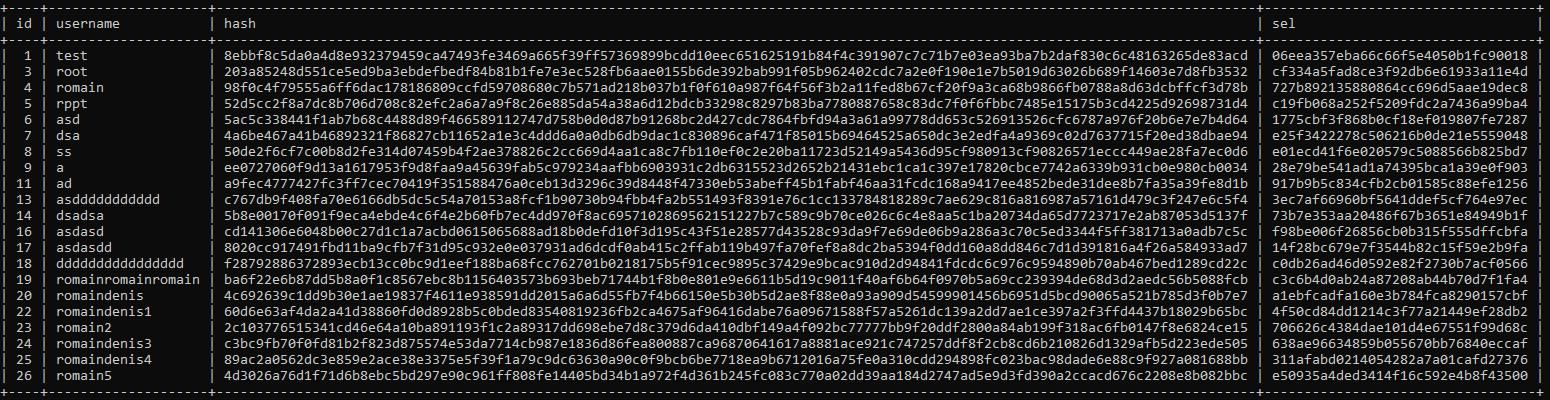
## 6.4 Authentification par mot de passe

*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).*

Le code hache et sale le mot de passe avant de le placer dans la base de données. Cela se fait dans la route POST pour /register, avec le code ci-dessous. The code uses



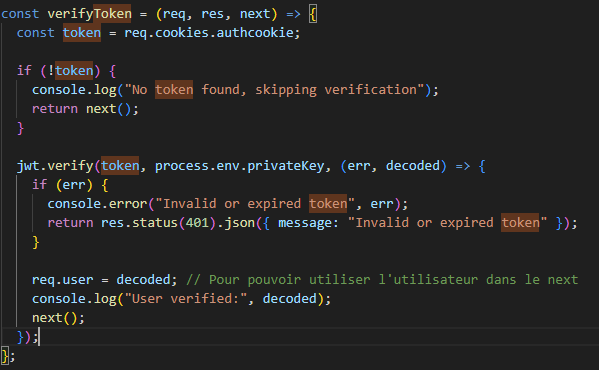
En conséquence, la base de données ressemble à ceci, avec le mot de passe haché et le sel à la fois avec l'utilisateur correspondant :

**

## 6.5 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.*

Le code vérifie automatiquement les JWT à l'aide du middleware verifyToken ci-dessous :



Ce code récupère le jeton JWT des cookies du site à l'aide de l'analyseur de cookies. S'il n'y a pas de jeton, la vérification est ignorée. Le programme qui utilise la fonction de la librairie jsonwebtoken, verify pour vérifier si le JWT est valide ou non. Si c'est le cas, l'utilisateur est autorisé à aller où il le souhaite.

## 6.6 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.*

## 6.7 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.*

Le code est protégé des injections SQL en utilisant des instructions préparées qui présentent une requête légèrement différente afin de représenter les entrées utilisateur et d'indiquer à la base de données que l'utilisateur ne peut pas quitter la requête et injecter du code malveillant.

Les entrées utilisateur sont représentées par les (?, ?, ?) et la ligne en dessous qui met les valeurs que l'utilisateur a saisies, pour éviter les injections SQL. Cela signifie également que nous n'avons pas besoin d'utiliser un ORM tel que sequelize pour ce projet

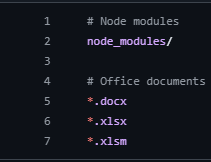
## 6.8 Utilisation de bcrypt

*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.*

## 6.9 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.*

Lien du repo GitHub : [romaindenis1/P\_APP](https://github.com/romaindenis1/P_APP)

Voici mon .gitignore, qui ignore les fichiers office et les binaires npm 

## 6.10 Documentation

• Journal de travail (1 ligne par quart d’heure de travail)

• Rapport, contenant :

Votre conceptualisation (schéma)

Des explications sur votre code o Une conclusion sur le travail fourni et sur l’attitude face au projet

## 6.11 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.

# 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

Il s’agit de reprendre point par point les fonctionnalités décrites dans les spécifications de départ et de définir si elles sont atteintes ou pas, et pourquoi.

Si ce n’est pas le cas, estimer en « % » ou en « temps supplémentaire » le travail qu’il reste à accomplir pour terminer le tout.

## Bilan de la planification

Distinguer et expliquer les tâches qui ont généré des retards ou de l'avance dans la gestion du projet. Indiquer les différence entre les planifications initiales et détaillées avec le journal de travail.

## Bilan personnel

Si c’était à refaire:

Qu’est-ce qu’il faudrait garder ? Les plus et les moins ?

Qu’est-ce qu’il faudrait gérer, réaliser ou traiter différemment ?

Qu’est que ce projet m’a appris ?

Suite à donner, améliorations souhaitables, …

Remerciements, signature, etc.

# 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.

## Bibliographie

Références des livres, revues et publications utilisés durant le projet.

## Webographie

Références des sites Internet consultés durant le projet.

# 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.