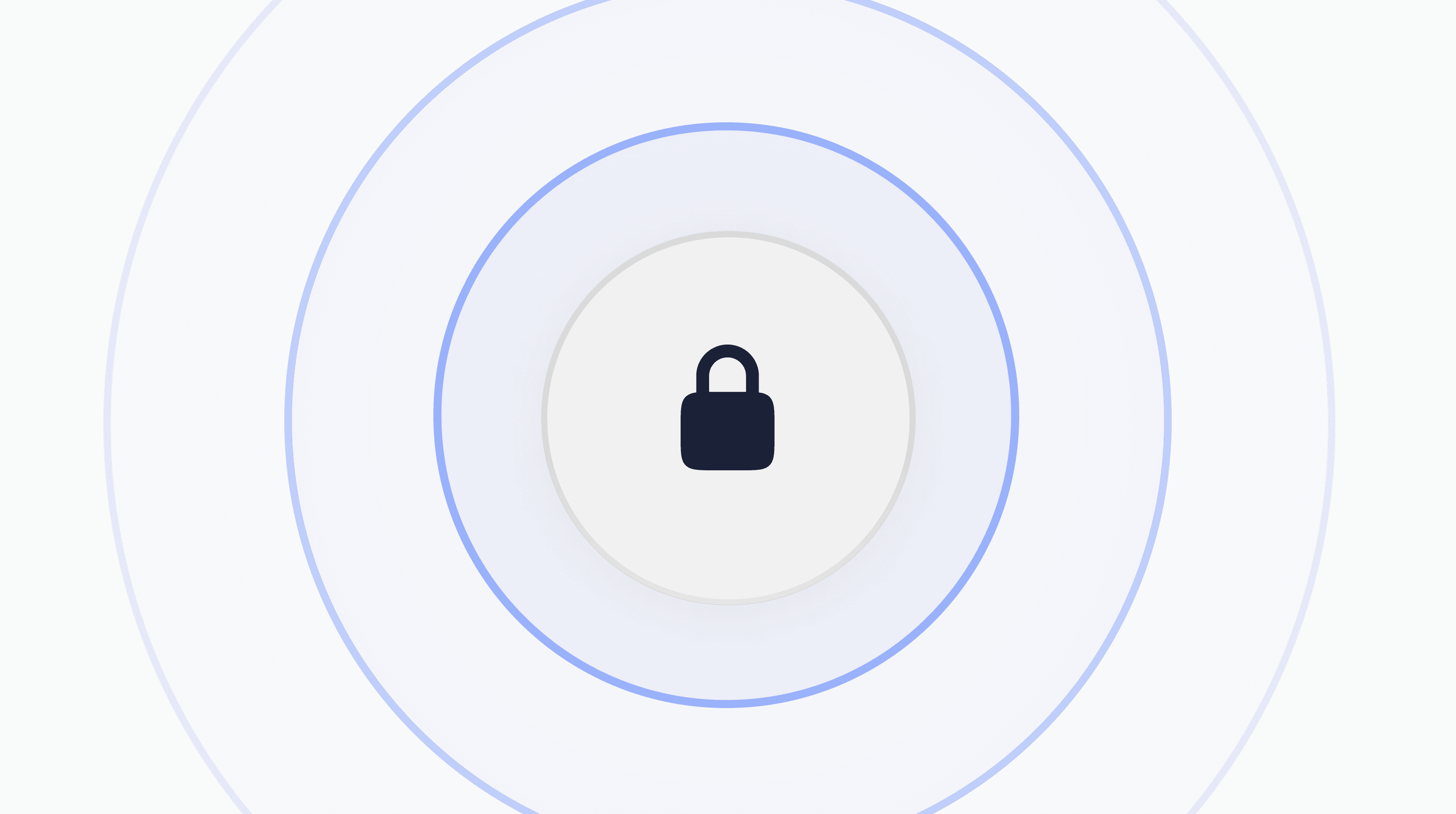
P\_APP\_183 : Secured WebShop



Yosef Nademo – CID2B

Vennes

24 périodes

Cédric SchaffterTable des matières

[1 Spécifications 3](#_Toc308526316)

[1.1 Titre 3](#_Toc308526317)

[1.2 Description 3](#_Toc308526318)

[1.3 Matériel et logiciels à disposition 3](#_Toc308526319)

[1.4 Prérequis 3](#_Toc308526320)

[1.5 Cahier des charges 3](#_Toc308526321)

[1.5.1 Objectifs et portée du projet (objectifs SMART) 3](#_Toc308526322)

[1.5.2 Caractéristiques des utilisateurs et impacts 3](#_Toc308526323)

[1.5.3 Fonctionnalités requises (du point de vue de l’utilisateur) 3](#_Toc308526324)

[1.5.4 Contraintes 3](#_Toc308526325)

[1.5.5 Travail à réaliser par l'apprenti 4](#_Toc308526326)

[1.5.6 Si le temps le permet … 4](#_Toc308526327)

[1.5.7 Méthodes de validation des solutions 4](#_Toc308526328)

[1.6 Les points suivants seront évalués 4](#_Toc308526329)

[1.7 Validation et conditions de réussite 4](#_Toc308526330)

[2 Planification Initiale 4](#_Toc308526331)

[3 Analyse 4](#_Toc308526332)

[3.1 Opportunités 4](#_Toc308526333)

[3.2 Document d’analyse et conception 4](#_Toc308526334)

[3.3 Conception des tests 5](#_Toc308526335)

[3.4 Planification détaillée 5](#_Toc308526336)

[4 Réalisation 5](#_Toc308526337)

[4.1 Dossier de Réalisation 5](#_Toc308526338)

[4.2 Modifications 5](#_Toc308526339)

[5 Tests 5](#_Toc308526340)

[5.1 Dossier des tests 5](#_Toc308526341)

[6 Conclusion 5](#_Toc308526342)

[6.1 Bilan des fonctionnalités demandées 5](#_Toc308526343)

[6.2 Bilan de la planification 5](#_Toc308526344)

[6.3 Bilan personnel 5](#_Toc308526345)

[7 Divers 6](#_Toc308526346)

[7.1 Journal de travail 6](#_Toc308526347)

[7.2 Bibliographie 6](#_Toc308526348)

[7.3 Webographie 6](#_Toc308526349)

[8 Annexes 6](#_Toc308526350)

# Spécifications

## Titre

Création d'un site e-commerce sécurisé avec gestion des utilisateurs et administration

## Description

Le projet consiste à créer une plateforme de commerce en ligne (webstore) sécurisée. Ce site offrira une authentification pour les utilisateurs (clients) et les administrateurs. La page d'authentification permettra aux utilisateurs de se connecter en toute sécurité via un mot de passe haché et salé. Un token JWT sera émis après une identification correcte de l'utilisateur, garantissant ainsi la sécurité des sessions. Le projet se concentrera sur l'authentification des utilisateurs, la gestion des rôles et l'administration du site, avec des protections contre les injections SQL et l'utilisation d'un certificat HTTPS pour assurer une connexion sécurisée. Ce projet vise à doter l'apprenant de compétences avancées en matière de sécurité web et de gestion des utilisateurs, tout en respectant les normes et les bonnes pratiques étudiées précédemment dans les modules.

## Matériel et logiciels à disposition

* **Matériel :** Un ordinateur standard de la section informatique avec accès à Docker Desktop pour la gestion des containers.
* **Logiciels :**
* Node.js pour le développement du backend.
* Docker pour la containerisation des services.
* IDE de développement.
* GitHub pour le versioning du code.

## Prérequis

* Connaissances de base en développement web, notamment en **HTML**, **CSS**, **JavaScript** et **Node.js**.
* Expérience avec les bases de données relationnelles (par exemple **MySQL**) et la gestion des utilisateurs.
* Connaissances en **sécurité web**, particulièrement concernant les mécanismes de hachage, de salage de mots de passe, et la gestion des tokens JWT.
* Compétences en **Docker** pour la mise en place d'un environnement de développement et de production containerisé.
* Compétence dans l'utilisation de **Git** et **GitHub** pour la gestion des versions du projet.

## Cahier des charges

### Caractéristiques des utilisateurs et impacts

es utilisateurs du site seront divisés en deux types principaux :

* **Clients** : Ils pourront se connecter via une page d’authentification et accéder à leur profil personnalisé.
* **Administrateurs** : Ils auront des privilèges supplémentaires pour rechercher des utilisateurs et accéder à des données sensibles.

**Impact sur la conception :**

* **Ergonomie** : La page de connexion et la page d'administration seront simplifiées et intuitives. Le design doit respecter les bonnes pratiques d'accessibilité.
* **Sécurité** : L'interface et les routes doivent être sécurisées par des mécanismes tels que l’authentification par mot de passe et le contrôle d'accès avec JWT. Les pages d'administration seront protégées contre les injections SQL.

### Fonctionnalités requises (du point de vue de l’utilisateur)

Le site comportera les fonctionnalités suivantes :

* **Page de connexion** : Permet à l’utilisateur de se connecter en utilisant son nom d’utilisateur et son mot de passe haché et salé.
* **Page d’administration** : Accessible uniquement aux administrateurs, elle permettra de rechercher des utilisateurs en fonction de leur nom et d’afficher les résultats.
* **Page de profil utilisateur(Page de détails )** : Affiche les informations de l'utilisateur connecté, récupérées via une route backend sécurisée.
* **Page d’acueill :** page general de conexion.

### Travail à réaliser par l'apprenti

L'apprenti devra :

* Concevoir l'architecture du site web et la mettre en œuvre en utilisant Node.js et MySQL.
* Implémenter l’authentification par mot de passe sécurisé avec hachage et salage, ainsi que l’émission et la vérification des tokens JWT.
* Développer la page d’administration avec une recherche par nom d'utilisateur.
* Assurer la protection contre les injections SQL.
* Utiliser Docker pour conteneuriser les services web et exécuter le projet de manière sécurisée en HTTPS.
* Rédiger un rapport détaillant la conceptualisation, les choix techniques, et les défis rencontrés.

### Si le temps le permet …

Si le temps permet, l’apprenti pourrait :

* Intégrer des fonctionnalités supplémentaires comme la gestion des rôles plus fine, avec des permissions pour chaque type d'utilisateur (client, administrateur, etc.).
* Ajouter une fonctionnalité de réinitialisation de mot de passe.

### Méthodes de validation des solutions

Les solutions seront validées de plusieurs façons :

* **Tests unitaires** : Les fonctions critiques, telles que l'authentification et la vérification des tokens JWT, seront couvertes par des tests unitaires.
* **Tests d'intégration** : La communication entre le frontend et le backend sera testée pour garantir la sécurité et l'intégrité des données.
* **Vérification de la sécurité** : Des tests seront effectués pour s'assurer que le site est protégé contre les injections SQL et d’autres attaques courantes.

# Planification Initiale

La planification initiale est en forme du fichier Exe est mis au disposition dans dossier documentation, et est accessible par ce liens : [m-planification-jnltrav-Yosef-Nademo.xlsm](https://eduvaud.sharepoint.com/:x:/r/sites/ETML_INF-GRP2D-24-25_Teams/Documents%20partages/P_183_SecureWebshop-CSR/Yosef%20Nademo/Documentation/m-planification-jnltrav-Yosef-Nademo.xlsm?d=w1eb6544e1adf41418347664f69f2253a&csf=1&web=1&e=XeHEY3)

# Analyse FONCTIONNELLE

## Conceptualisation (schéma)

## Explication de code

# Conclusion

## 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

Le journal de travail vous pouvez trouve dans ficher «GitHub\Secured-WebShop\Documentation\m-planification-jnltrav-Yosef-Nademo.xlsm »

Ou il est accessible par ce liens : [m-planification-jnltrav-Yosef-Nademo.xlsm](https://eduvaud.sharepoint.com/:x:/r/sites/ETML_INF-GRP2D-24-25_Teams/Documents%20partages/P_183_SecureWebshop-CSR/Yosef%20Nademo/Documentation/m-planification-jnltrav-Yosef-Nademo.xlsm?d=w1eb6544e1adf41418347664f69f2253a&csf=1&web=1&e=XeHEY3)

# Annexes

* <https://www.youtube.com/watch?v=AzA_LTDoFqY&t=30s&ab_channel=SamMeech-Ward>

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.