UNIVERSITÉ DE LORRAINE | IUT Metz

SAÉ 4.01
Livrable 2 – Semaine 1

BONDON Loric

BROCHOT Joshua

BRODIER Baptiste

ROTH Sevan

Année 2024/2025

I. Code de l'application

Le code de l'application se situe sur :

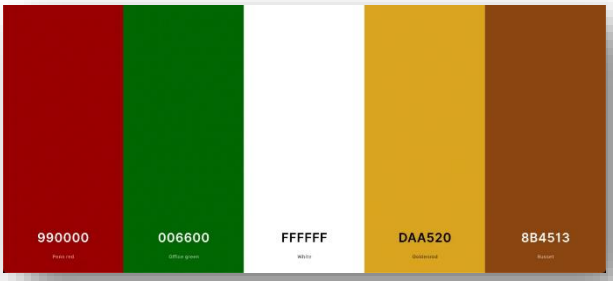
GitHub via ce lien (branche version1) :
https://github.com/LoricBndn/SAE4.01

DevWeb via ce lien :
https://devweb.iutmetz.univ-lorraine.fr/~bondon3u/2A/SAE4.01/Application/V1/client/accueil.html

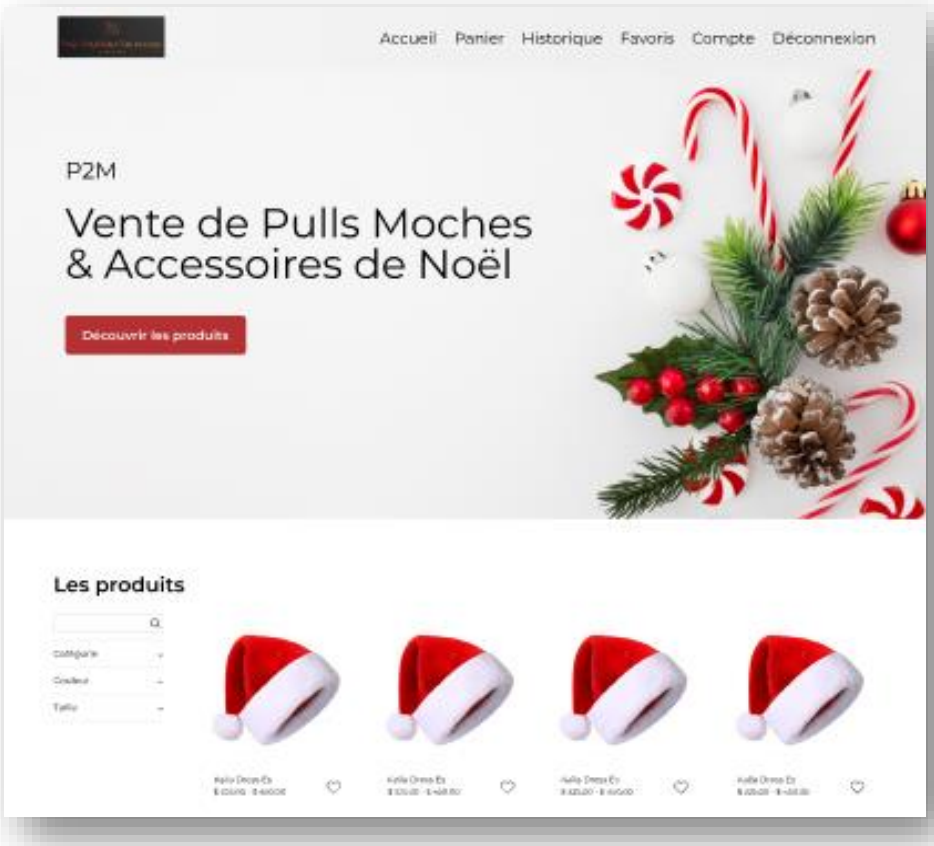
II. Documents

A. Maquettes

1. Palettes de couleurs



2. 1ère version maquette site



B. RGPD, obligations légales, sécurité, etc

Recherches effectuées :

1. Mentions légales obligatoires

Tout site e-commerce doit afficher des mentions légales claires et accessibles, incluant :

- **Identité de l'éditeur** : nom ou raison sociale, adresse du siège social, numéro de téléphone, numéro d'inscription au RCS ou au répertoire des métiers.
- **Directeur de la publication** : nom du responsable éditorial.
- **Hébergeur du site** : nom, dénomination ou raison sociale, adresse et téléphone.
- **Traitement des données personnelles** : informations sur la collecte et le traitement des données des utilisateurs.

Ces informations doivent être facilement accessibles depuis toutes les pages du site, souvent via un lien en pied de page intitulé "Mentions légales".

---

2. Gestion des cookies et respect du RGPD

L'utilisation de cookies requiert le consentement préalable de l'utilisateur, sauf pour ceux strictement nécessaires au fonctionnement du site. Il faut :

- **Informer clairement les utilisateurs** de la finalité des cookies utilisés.
- **Obtenir leur consentement explicite** avant de les déposer, notamment pour les cookies liés à la publicité ciblée ou aux réseaux sociaux.
- **Offrir la possibilité de les refuser** ou de les paramétrer.

Le non-respect de ces obligations peut entraîner des sanctions de la CNIL.

---

3. Sécurité des cookies et des sessions

Stocker des informations sensibles, comme un id_user, dans des cookies non sécurisés expose le site à des risques tels que l'usurpation de compte. Pour renforcer la sécurité :

- **Évitez de stocker des données sensibles en clair dans les cookies**. Privilégiez l'utilisation de tokens sécurisés.
- **Définissez une durée de vie limitée pour les cookies** et utilisez l'attribut HttpOnly pour empêcher leur accès via JavaScript.
- **Implémentez des sessions sécurisées** côté serveur pour gérer l'authentification des utilisateurs.

4. Bonnes pratiques avec JWT (JSON Web Tokens)

Si vous envisagez d'utiliser des JWT pour l'authentification :

- **Ne stockez pas de données sensibles dans le payload du JWT**, car il est encodé en Base64 et facilement décodable.
- **Utilisez une clé secrète robuste** pour signer les tokens et assurez-vous qu'elle est bien protégée.
- **Définissez une expiration courte des tokens** et mettez en place un mécanisme de renouvellement sécurisé.
- **Stockez les tokens de manière sécurisée** côté client, en évitant le stockage dans le localStorage qui est accessible via JavaScript.

---

5. Fonctionnalité de résiliation en ligne

Depuis le 1er juin 2023, si vous proposez des contrats d'abonnement en ligne, vous devez mettre à disposition une fonctionnalité permettant aux consommateurs de résilier leur contrat par voie électronique. Cette fonctionnalité doit être :

- **Gratuite et facilement accessible** depuis votre site ou application mobile.
- **Présentée sous la mention "résilier votre contrat"** ou une formule équivalente claire.
- **Accompagnée d'informations** sur les conditions de résiliation (délais, frais éventuels, etc.).

Le non-respect de cette obligation peut entraîner une amende de 15 000 € pour une personne physique et 75 000 € pour une personne morale. (entreprendre.service-public.fr)

C. Base de données

1. Schéma relationnel

USER (*id_user*, #id_perm, nom, prénom, email, date_naiss, mdp)

PERMISSION (*id_perm*, nom_perm)

CATEGORIE (*id_categorie*, nom)

PRODUIT (*id_produit*, #id_categorie, SKU, nom, description, photo)

DETAIL_PRODUIT (*reference*, #id_produit, taille, couleur, prix, stock)

FAVORI (*id_user, reference*)

PANIER (*id_panier*, #id_user, #*reference*, quantite)

COMMANDE (*id_commande*, #id_user, date_commande, total, statut)

DETAIL_COMMANDE (*id_detail*, #id_commande, #*reference*, quantite, prix_unitaire)

PAIEMENT (*id_paiement*, #id_commande, methode, statut, transaction_id)

FRAIS_PORT (*id_categorie, seuil_quantite, frais*)

SOLDE (*id_solde*, #*reference*, reduction, date_debut, date_fin)

---

2. Améliorations apportées

- Suppression des redondances : les tailles et couleurs sont gérées via DETAIL_PRODUIT.
- Meilleure gestion du stock : suivi précis via DETAIL_PRODUIT et DETAIL_COMMANDE.
- Préparation aux futures promotions : table SOLDE pour anticiper les soldes.
- Gestion dynamique des frais de port en fonction des catégories et quantités commandées.
- Enregistre les paiements pour les simulations via un « Paypal sandbox account »

III. Planning

Le planning de la semaine à venir est disponible sur :

Jira via ce lien :
https://sae401-2425.atlassian.net/jira/software/projects/SMS/list?atlOrigin=eyJpIjoiNDIyNDA0ZDc5MjFlNDA5ZGIzODEyMDFkMDcyYjFiYjIiLCJwIjoiaiJ9

Github (en version pdf) via ce lien :
https://github.com/LoricBndn/SAE4.01

IV. Bilan

A. Bilan de la semaine *(03 – 07 mars) par rapport au planning prévu*

Objectif initial : Sécuriser l'application et assurer la conformité légale

1. Analyse

Tâche prévue	Avancement	Observation
Sécurité & conformité légale	☑ Partiellement réalisé	
→ Corriger la gestion des cookies	✗ Non fait	Toujours en attente, id_user est toujours stocké en clair.
→ Restreindre l'accès aux fichiers sensibles	☑ Fait (Loric)	Pages inutiles et dangereuses supprimées.
→ Ajouter un bandeau RGPD et mentions légales	☑ Partiellement réalisé (Loric)	Recherche effectuée, mais implémentation non finalisée.
→ Vérifier les permissions d'accès aux fichiers	✗ Non fait	Aucun retour sur les vérifications des permissions serveurs.
Fonctionnalités essentielles manquantes	☑ Partiellement réalisé	
→ Implémenter le tunnel de commande	✗ Non fait	Pas encore abordé.
→ Gérer les frais de port	☑ Planifié (Joshua)	Ajout de la table FRAIS_PORT dans la base de données.
→ Implémenter le paiement PayPal	☑ Préparation en base (Joshua)	Table PAIEMENT ajoutée, mais intégration PayPal non commencée.
Correction des bugs et ergonomie	☑ Partiellement réalisé	
→ Correction de l'affichage des erreurs de formulaire	☑ Fait (Baptiste)	Correction de l'affichage des messages d'erreurs.
→ Modification du comportement du champ mot de passe	☑ Fait (Baptiste)	
Améliorations UX/UI et design	☑ Partiellement réalisé	
→ Refonte du design	☑ En cours (Sevan)	Maquette du site réalisées avec palette de couleurs.
→ Amélioration de l'affichage des produits	✗ Non fait	Aucune correction des tailles d'images et du design produit.
Améliorations base de données et architecture	☑ Bien avancé	

→ Optimisation du schéma relationnel	✅ Fait (Joshua)	Réorganisation des relations pour une meilleure gestion des tailles, couleurs et stocks.
→ Suppression des redondances	✅ Fait (Joshua)	Déplacements des tailles et couleurs dans DETAIL_PRODUIT.
→ Ajout d'un suivi des soldes	✅ Fait (Joshua)	Création de la table SOLDE.

2. Evaluation globale de la semaine

Points positifs :

- Sécurisation du site en cours : Suppression des pages dangereuses et recherches RGPD avancées.
- Correction de bugs d'ergonomie : Amélioration de l'affichage des erreurs et des champs de connexion.
- Améliorations significatives de la base de données : Nouvelle structure plus efficace, anticipation des soldes et gestion avancée du stock.
- Premiers travaux de design : Maquettes et choix de la palette de couleurs pour le redesign.

Points à améliorer :

- Gestion des cookies toujours vulnérable (doit être corrigée en priorité).
- Implémentation des permissions d'accès aux fichiers serveurs en attente.
- Tunnel de commande et intégration PayPal non commencés.
- Amélioration visuelle des fiches produits et gestion des images encore à faire.

3. Objectifs pour la semaine prochaine (08 – 14 mars)

Priorité absolue : Corriger la gestion des cookies et sécuriser les sessions.

- Finaliser le bandeau RGPD et la page des mentions légales.
- Commencer l'implémentation du tunnel de commande.
- Lancer l'intégration PayPal (API et simulation avec PayPal Sandbox).
- Continuer l'amélioration de l'UI avec un design plus professionnel.

Globalement, les bases sont bien posées, mais la partie sécurité doit être renforcée et le tunnel de commande doit être lancé dès la semaine prochaine.