SAÉ 3.01 - DEVAPP
ANALYSE D’IMPACT

Groupe 2B11

Vue d’ensembles des traitements réalisés

Enregistrement de compte :

Description : Lorsque les utilisateurs soumettent le formulaire d'inscription, leur nom, prénom, adresse e-mail et mot de passe sont collectés.
Finalité : Ces informations sont ensuite utilisées pour créer un compte pour l'utilisateur sur le site e-commerce, permettant à l'utilisateur de passer des commandes, de suivre ses commandes et de bénéficier de certaines fonctionnalités personnalisées.
Enjeux : Si les informations collectées ne sont pas correctement protégées, il pourrait y avoir un risque de fuite de données ou d'utilisation frauduleuse des informations personnelles des utilisateurs.

Validation des informations d'inscription :

Description : Le code utilise des expressions régulières (regex) pour vérifier que les informations saisies par l'utilisateur (nom, prénom, adresse e-mail et mot de passe) sont valides.
Finalité : Cela permet de s'assurer que les informations saisies par les utilisateurs respectent un format valide et contiennent les caractéristiques de sécurité nécessaires pour garantir la sécurité de l'utilisateur.
Enjeux : Si des erreurs sont détectées lors de la validation des informations d'inscription, cela peut entraîner des erreurs dans la création du compte utilisateur et compromettre la sécurité de l'utilisateur.

Vérification de l'unicité de l'adresse e-mail :

Description : Le code vérifie si l'adresse e-mail saisie par l'utilisateur est déjà utilisée par un autre utilisateur en consultant la base de données.
Finalité : Empêcher les utilisateurs de créer plusieurs comptes avec la même adresse e-mail pour éviter des abus ou des fraudes.
Enjeux : Si cette vérification n'est pas effectuée, il pourrait y avoir des utilisateurs qui créent plusieurs comptes avec la même adresse e-mail, ce qui pourrait entraîner des problèmes de sécurité ou des abus.

Stockage des informations d'inscription :

Description : Si les informations d'inscription sont valides, les informations sont stockées dans la base de données pour créer un compte pour l'utilisateur.
Finalité : Stocke les informations d'inscription de l'utilisateur pour permettre l'accès à son compte et l'utilisation des fonctionnalités du site e-commerce.
Enjeux : Si les données stockées ne sont pas correctement protégées, il pourrait y avoir un risque de fuite de données ou d'utilisation frauduleuse des informations personnelles des utilisateurs.

Traitement des informations bancaires :

Description : Lors de la finalisation d'une commande, les informations bancaires de l'utilisateur (numéro de carte, date d'expiration, cryptogramme visuel) sont collectées et utilisées pour traiter le paiement.
Finalité : Permettre à l'utilisateur de payer pour ses achats en utilisant sa carte bancaire.
Enjeux : Si les informations bancaires ne sont pas correctement protégées, il pourrait y avoir un risque de fuite de données ou d'utilisation frauduleuse des informations bancaires de l'utilisateur.

Traitement des informations de livraison :

Description : Lors de la finalisation d'une commande, les informations de livraison de l'utilisateur (nom, adresse, code postal, ville, pays) sont collectées et utilisées pour organiser la livraison des articles commandés.
Finalité : Livrer les articles commandés à l'adresse de livraison spécifiée par l'utilisateur.
Enjeux : Si les informations de livraison ne sont pas correctement protégées, il pourrait y avoir un risque de fuite de données ou d'utilisation frauduleuse des informations de livraison de l'utilisateur. Il est également important de s'assurer que les informations de livraison sont correctes pour éviter les erreurs de livraison.

Description des processus, données et supports

Processus:

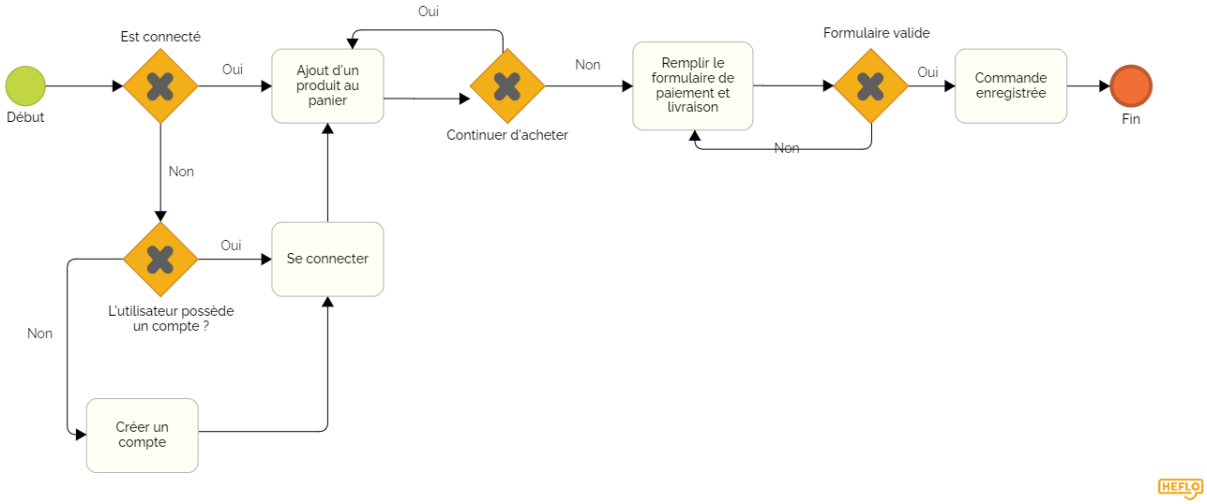
- Mise en place d'un système de commande et de livraison pour permettre aux clients de commander en ligne
- Utilisation de la digitalisation pour faire connaître les producteurs locaux et leur offrir une plus grande visibilité
- Mise en place d'un système de paiement en ligne pour faciliter les transactions

Données:

- Informations sur les produits (idproduit, idcategorie, nomproduit, prixproduit, fournisseurproduit, descriptionproduit, compositionproduit, quantitestock, promotion, prixpromo)
- Informations sur les clients (idclient, motpasseclient, nomclient, prenomclient, adresseclient, telephoneclient, mailclient)
- Informations sur les commandes (idcommande, idpaiement, idclient, datecommande, fraislivraison, adresselivraison, nomlivraison, codepostallivraison, villelivraison, telephonelivraison)

Supports:

- Site d'e-commerce développé à l'aide de sqldeveloper avec oracle pour gérer les commandes et les paiements en ligne



1. Le client accède au système en se connectant avec ses informations de compte ou en créant un nouveau compte.
2. Le système vérifie les informations de connexion et authentifie le client.
3. Le client utilise la barre de navigation ou la barre de recherche pour trouver les produits qu'il souhaite commander.
4. Le système affiche les produits correspondants à la recherche du client.
5. Le client sélectionne les produits qu'il souhaite commander en les ajoutant au panier.
6. Le système vérifie la disponibilité des produits sélectionnés dans la base de données.
7. Le client valide la commande et saisit les informations de livraison.
8. Le système vérifie la validité des informations de livraison.
9. Le système envoie à la page de traitement de commande pour le paiement et la livraison.
10. Le système enregistre la commande et les informations de livraison dans la base de données.
11. Le système envoie une confirmation de commande au client.

Dictionnaire des données

Table	Nom	Définition
Client	***idClient***	Identifiant du client
Client	nomClient	Nom du client
Client	prenomClient	Prénom du client
Client	adresseClient	Adresse du client
Client	TelephoneClient	Téléphone portable du client

Client	mailClient	Mail du client
Client	motPasseClient	Mot de passe client
Commande	***idCommande***	Identifiant de la commande
Commande	**idPanier**	Identifiant du panier
Commande	**idClient**	Identifiant du client
Commande	nomLivraison	Prénom à la livraison
Commande	adresseLivraison	Adresse de la livraison
Commande	codePostalLivraison	Code postal de livraison
Commande	VilleLivraison	Ville de la livraison
Commande	TelephoneLivraison	Téléphone à la livraison
Commande	dateCommande	date de la commande
Commande	FraisLiv (calcul)	frais de livraison

Récapitulatif des risques et conséquences en matière de cyber-sécurité

Risque	Principales menaces	Principaux impacts	Mesures pour réduire ce risque	Niveau de gravité
Accès illégitime à des données	Consultation /vol des données sur le serveur Usurpation d'un compte	Conséquences d'une communication d'informations potentiellement sensibles. Phishing Publicité ciblée	Limitation de l'accès a la base de donnée, chiffrement de mot de passe	**Importante**

Modification non désirée de données	Altération des données sur le serveur	Détérioration de la qualité du service	Sécurisation du site afin d'empêcher les faille XSS et les injections SQL	**Modérée**
Disparition de données	Suppression de données Détérioration de serveurs Dégradation physique d'un matériel	Nécessité de recréer un compte d'utilisation Perte de données Détérioration de la qualité du service	Sauvegardes régulières sur des disques durs en dehors du serveur	**Importante**

Mesures applicables et modalités de mise en place sur la protection des données

Mesure	modalités	Priorité
L'utilisateur a consenti au traitement de ses données à caractère personnel dans le but d'utiliser ses données pour la création de son compte sur le site web	Consentement recueilli à la création du compte client dans le formulaire	Important : Les données que nous recueillons permettent l'aboutissement des différentes commandes du client.
L'utilisateur a consenti au traitement de ses données à caractère personnel dans le but de répondre à son message	Consentement recueilli à l'envoie d'un message dans le formulaire	Modérée : Les données que nous recueillons lors de l'envoie d'un message de l'utilisateur permettent de l'identifier pour répondre au bon client
L'utilisateur a consenti au traitement de ses données à caractère personnel dans le but d'envoyer des nouvelles du site dans sa boîte mail	Consentement recueilli à l'inscription à l'inscription à la Newsletter	Faible : Les données que nous recueillons lors de l'inscription à la Newsletter permettent l'envoie de nouveautés sur la boîte mail du client
L'utilisateur a consenti au traitement de ses données à caractère personnel dans le but de pré-remplir les champs lors de sa prochaine connexion	Consentement recueilli à la connexion à un compte dans le formulaire	Modérée: Les données que nous recueillons lors de la connexion du client permettent la création d'un cookie de connexion qui pré-remplira les champs lors de la

		prochaine connexion.
L'utilisateur a consenti au traitement de ses données à caractère personnel dans le but d'utiliser ses données pour les commandes et les achats qu'il effectuera	Consentement recueilli lors de la validation de son consentement dans le formulaire	Importante : Les données que nous recueillons lors de la saisie des champs dans le formulaire permettent de finaliser la commande du client
L'utilisateur a consenti à l'archivage de ses données à caractère personnel	Consentement recueilli lors de la création d'un compte, à l'acceptation des conditions générales	Élevé : Les données à caractères personnels sont archivés jusqu'à demande de l'utilisateur L'archivage des données doit se faire avec le consentement de nos clients, alors si celui-ci souhaite qu'elles soient supprimées alors nous respecterons sa volonté.
L'utilisateur à consenti à ne pas divulguer ses données de connection	Consentement recueilli lors de l'inscription sur le site web par acceptation des conditions générales.	Importante : La connexion au compte de l'utilisateur doit être authentique. En effet, le client peut accéder et modifier ses données personnelles, il doit donc garder ses informations de connexion confidentielles..

Mesures applicables et leurs modalités de mise en place sur la sécurité des données

Mesure	modalités	Priorité
Chiffrement des données bancaire des clients	Les données bancaires sont chiffrées avant d'être insérer dans la base de données lorsque les clients passe commande	Importante : Il est important de devoir chiffrer les données stockées dans notre base de données car en cas de perte de ces données, elles seront bien plus difficilement traduisibles

		puis exploitables.
Chiffrement des données archiver des clients	Les données archiver des utilisés tels que les commandes finalisées sont chiffrés	Élevé :+ Les données à caractères personnels sont archivés jusqu'à demande de l'utilisateur L'archivage des données doit se faire avec le consentement de nos clients, alors si celui-ci souhaite qu'elles soient supprimées alors nous respecterons sa volonté.
Contrôle des accès logiques des clients	Vérification de la concordance entre le mot de passe et l'email lors de la connexion.	Importante : La connexion au compte de l'utilisateur doit être authentique. En effet, le client peut accéder et modifier ses données personnelles, il doit donc garder ses informations de connexion confidentielles..
Sécurisation du téléchargement des document sensibles (factures)	Les documents téléchargeables sensibles tels que les factures sont chiffrés avant d'être envoyés dans la boîte mail de l'utilisateur.	Élevé : Les factures de nos clients peuvent contenir des informations personnelles telles que l'adresse du client. Il est donc normal que nos clients ne souhaitent pas que ces informations soient divulguées facilement.
Sécurisation de l'espace Administrateur	Pour accéder à l'espace Administrateur, plusieurs mot de passe et code sont à saisir	Élevé : L'espace d'administration est un espace sensible dans lequel est présent les données des utilisateur et des produits

Issues à ajouter au dernier sprint

1. Ajouter une autorisation d'utiliser les cookie sur le site
2. Ajouter la double authentification sur le site (saisir 2 fois le mot de passe)
3. Sécuriser le téléchargement des données sensibles (factures, données personnel)

4. Ajouter la possibilité au client de réinitialiser son mot de passe
5. Ajouter la possibilité au client de demander la suppression de ses données à caractère personnel du site.
6. Sécuriser la base de données pour toutes les données sensible : haché les mot de passe, crypter les données bancaire
7. Sécuriser le site contre toute forme d'injection SQL et XSS