

Groupe G2A-9

Thomas Demeyere 🤖

Anton Xu 🤖

Louis Yvelin 🍪

Oryann Prochaska 🚀

Analyse d'impact

SOMMAIRE

1. Vue d'ensemble	3
1.1 Présentation du (des) traitement(s) considéré(s)	3
2. Données, processus et supports	4
2.1 Description des données, destinataires et durées de conservation	4
3. Récapitulatif des risques et solutions apportées	4
4. Liste des issues prioritaires	5
5. Processus BPMD de la connexion/inscription	6

1. Vue d'ensemble

1.1 Présentation du (des) traitement(s) considéré(s)

Description du traitement	Commerce de la rue collecte des informations sur ses clients afin de pouvoir exercer leur activité de commerce en ligne et satisfaire au mieux le client.
Finalité du traitement	<ul style="list-style-type: none">• Acheter des produits en ligne• Recevoir les produits chez lui• Enregistrer ses informations pour passer commande plus vite la prochaine fois
Enjeux du traitement	Création d'un service de vente en ligne avec pour thème le commerce de composant informatique.
Responsable du traitement	<i>Commerce de la Rue</i>
Sous-traitant(s)	Oracle outil de gestion de base de données situé aux États-Unis

2. Données, processus et supports

2.1 Description des données, destinataires et durées de conservation

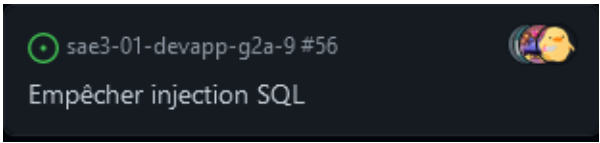
Données	Destinataires	Durée de conservation
Fournies par l'utilisateur : Adresse électronique, numéro de téléphone, Cartes bancaires	Commerce de la rue et fournisseurs	Jusqu'à la demande de suppression par l'utilisateur.
Données relevées : Température, humidité, taux de CO2	Salariés de l'entrepôt de l'entreprise <i>Commerce de la rue</i>	3 mois de conservations en archives
Factures liées aux commandes	Commerce de la rue	10 ans


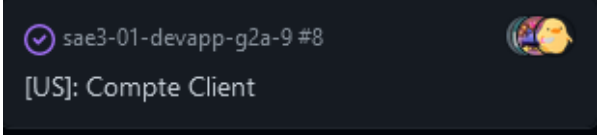
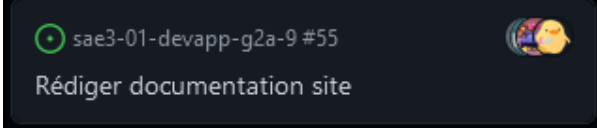
3. Récapitulatif des risques et solutions apportées

Risque	Principales menaces	Principaux impacts	Mesures pour réduire ce risque	Niveau de gravité
Accès direct à la base de données	Logs en clair dans le code	Modification / suppressions/ diffusions de données personnelles et/ou sensibles (informations bancaires)	Logs de la base de données dans un fichier séparé du code principal.	Très élevé
Injectons SQL	Formulaires	Modification /	Fonctions PHP	Très élevé

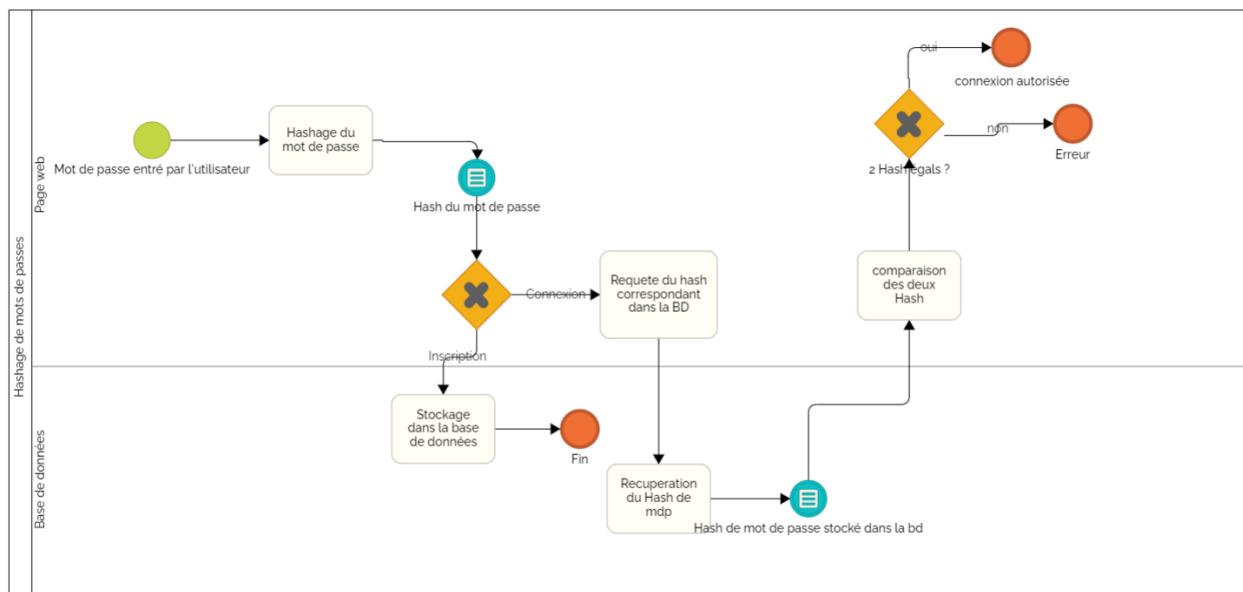
	HTML sur le site web	suppressions/ diffusions de données personnelles et/ou sensibles (informations bancaires)	permettant d'éviter les injonctions	
Vols de mots de passe	Mots de passes en clair dans la Base de données	Vols de données personnel des utilisateurs	Hachage des mots de passe	Élevé
Perte de l'accès à son compte	Oubli de mot de passe	Impossibilité de consulter/modifier ses données personnelles	Formulaire de réinitialisation du mot de passe	Modéré

4. Liste des issues prioritaires

	<p>Ce procédé empêche l'utilisateur de faire une requête à la base de données qui pourrait compromettre des informations sensibles</p>
---	---

	<p>L'utilisateur peut à tout moment changer son mot de passe depuis son compte client s'il a des doutes sur la vulnérabilité de ce dernier.</p>
	<p>Permet à l'utilisateur d'enregistrer sans crainte ses informations pour la prochaine fois, même si quelqu'un d'autre utilise le site sur son ordinateur, il y a besoin d'une connexion.</p>
	<p>La documentation que nous allons fournir à l'entreprise <i>Commerce de la rue</i> aura pour but de les guider et d'apporter des précisions sur les mesures de sécurité prises par nos développeurs dans l'optique qu'ils fassent un jour reprendre le site par d'autres développeurs.</p>

5. Processus BPMN de la connexion/inscription



Ce processus correspond à la gestion du mot de passe lors de la connexion ou à l'inscription d'un utilisateur sur notre site. On peut y voir les 2 acteurs ; la page web en haut et la base de données en bas et comment ils interagissent entre eux. Lorsque l'utilisateur entre un mot de passe sur le site internet, ce dernier est hashé pour qu'il ne soit pas stocké en clair dans la base de données. Si l'utilisateur crée son compte, on envoie le hash directement dans la base de données afin de le stocker. Dans le cas où l'utilisateur souhaite se connecter à son compte, une requête est envoyée à la base de données en vue de récupérer le hash de mot de passe associé à ce compte. Le hash est alors renvoyé vers le site afin de le comparer au hash du mot de passe entré par l'utilisateur. Si les deux hash sont égaux, la connexion est validée et l'utilisateur peut accéder à son compte. Dans le cas inverse, la connexion lui est refusée.