ID	Nature du risque	Description	Gravité	Probabilité	Criticité	Conséquences si avéré	Solution préventive	Solution corrective
R1	Technique	Vulnérabilités du code.	3	2	6	Vol de données Réputation	Mettre à jour régulièrement les solutions et les dépendances. Utiliser des pratiques fortes pour sécuriser l'application.	Il faut être en mesure de pouvoir corriger rapidement les failles de sécurité, et avoir un système de détection des intrusions.
R2	Technique	Attaques par injection	3	1	3	Vol de données Réputation	Prévoir des sécurités pour empêcher le problème.	Sauvegarde régulière de la base de données, et restauration de secours si besoin.
R3	Technique	Attaque par force brute	2	2	4	Vol de données Réputation	Imposer une politique de mots de passe forte, voire un système de double-authentification.	Bloquer un compte utilisateur qui aurait été usurpé suite à un vol de mot de passe par force brute.
R4	Technique	Attaque par déni de service (DdoS)	4	3	12	Utilisation perturbée Pertes financières Réputation	Utilisation d'outils de détection et de protection contre les DdoS, comme un pare-feu.	Suspendre certains services de l'application le temps de combler la faille de sécurité ou de trouver une solution de contournement.
R5	Humain	Accès non autorisé	1	2	2	Réputation Vol de données	Mettre en place des contrôles d'accès strictes pour protéger certains espaces sensibles.	N/D
R6	Humain	Perte de données	3	2	6	Réputation Juridique Pertes financières	Sauvegardes régulières des données afin de se protéger contre les pertes.	Restauration d'une sauvegarde de données utilisateurs.
R7	Humain	Ingénierie inverse	4	2	8	Réputation Pertes financières	Définir une licence et un copyright adapté à notre solution	Recours légaux.