



A large, spherical honeycomb structure is centered in a field of colorful flowers under a clear blue sky. Numerous bees are seen flying around and landing on the honeycomb. A white rectangular box with a semi-transparent hexagonal pattern is overlaid on the lower half of the honeycomb, containing the following text:

**Responsible Cybersécurité & Audit  
(Web & Base de données)**

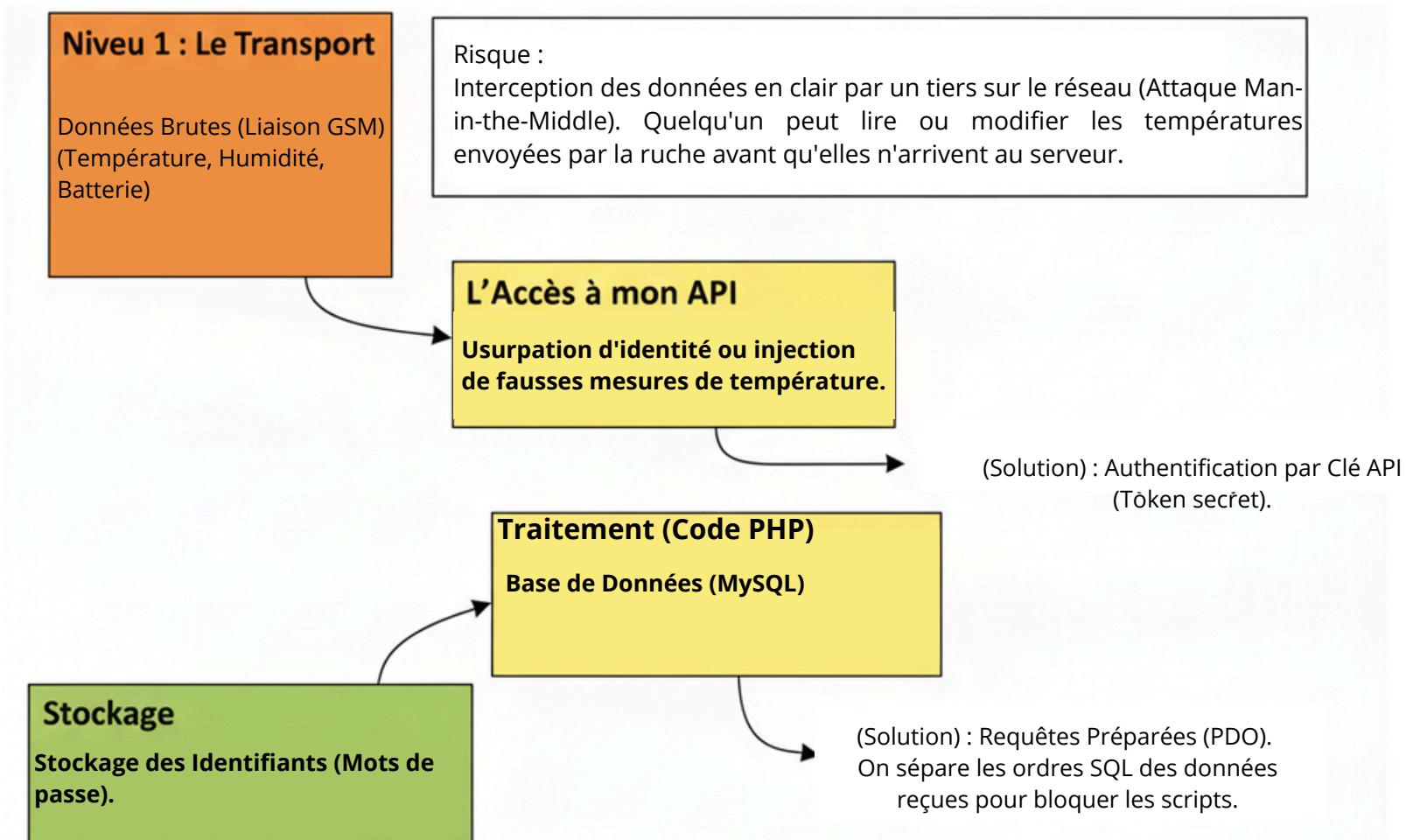
## Identification et liste des risques potentiels

Composant	Menace (Risque)	Description du scénario	Solution Technique (À mettre en place)
Base de Données (MySQL)	Injection SQL	Un pirate tape du code malveillant dans le champ "Login" (ex: ' OR 1=1 --) pour se connecter sans mot de passe ou effacer la table Mesure.	Requêtes Préparées (PDO) en PHP. Ne jamais insérer de variables directement dans le SQL.
Site Web (Accès Admin)	Brute Force	Un robot teste des milliers de mots de passe pour deviner celui de l'admin et accéder à la configuration des seuils.	Politique de Mots de Passe Forts (12 caractères, Maj, Min, Chiffres) + Limitation des tentatives (bloquer après 3 échecs).
Site Web (Affichage)	Faille XSS (Cross-Site Scripting)	Un pirate injecte un script Javascript dans le nom d'une ruche. Quand l'apiculteur se connecte, le script vole ses cookies.	Échappement des données : Utiliser htmlspecialchars() en PHP avant d'afficher n'importe quelle donnée venant de la base.
Base de Données (Stockage)	Vol de Mots de Passe	Si le serveur est piraté et que la base est volée, les mots de passe des utilisateurs sont lisibles en clair.	Hachage des mots de passe (Ne jamais stocker en clair). Utiliser password_hash() avec Argon2 ou Bcrypt.

## Analyse des risques sur la Transmission

Composant	Menace (Risque)	Description du scénario	Solution Technique (À mettre en place)
Liaison GSM -> Serveur	Attaque "Man-in-the-Middle" (Interception)	Comme vu sur ton diagramme de séquence, les données transitent par Internet. Quelqu'un sur le réseau intercepte la requête HTTP et lit les températures ou modifie les données.	HTTPS (Certificat SSL/TLS). Obliger la ruche à communiquer en HTTPS et non en HTTP simple. Les données seront chiffrées.
API (Ton script de réception)	Usurpation d'identité	Un petit malin envoie de fausses données de température à ton serveur sans avoir la ruche physique, juste en simulant la requête POST.	Token d'authentification (API Key). La ruche doit envoyer une clé secrète dans chaque message. Si la clé n'est pas bonne, le serveur rejette la mesure.
Alertes SMS	Sniffing GSM / Spoofing	Quelqu'un intercepte le SMS d'alerte (GSM non chiffré) ou envoie un faux SMS à l'apiculteur pour lui faire peur.	Validation croisée sur le site web. Conseiller à l'utilisateur de toujours vérifier l'alerte sur l'application sécurisée (HTTPS) avant d'agir.

# DIAGRAMME DES COUCHES DE PROTECTION



## Conclusion

**En conclusion, cet audit démontre que la sécurité de la Ruche Connectée ne peut pas se limiter à la protection physique du matériel. En tant que responsable du stockage et du serveur web, mon rôle est d'assurer la confidentialité et l'intégrité des données via une stratégie de "défense en profondeur".**

**La priorité immédiate sera de sécuriser le transport des données (chiffrement HTTPS/TLS pour les échanges GSM) et de durcir la base de données (utilisation stricte de requêtes préparées et hachage des mots de passe). Ces mesures techniques sont indispensables pour transformer ce prototype en une solution fiable et résiliente face aux menaces actuelles (injections SQL et interceptions).**