Livrable 1 : Analyse des Menaces (Modèle STRIDE)

Projet : BricoSûr

Date : 7 Janvier 2026

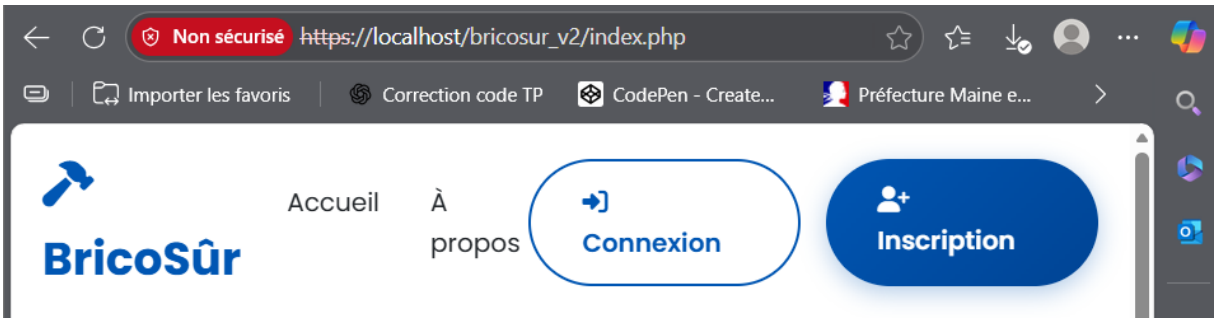
Auteur : DAYAWA Germain Mike

Objectif : Identifier les menaces potentielles et documenter les mesures d'atténuation techniques mises en œuvre pour garantir la sécurité des utilisateurs et des données.

---

1. Introduction technique

BricoSûr repose sur une architecture PHP/MySQL sécurisée. Les données sont hébergées sur une base de données isolée via le **port 3307** et toutes les communications sont protégées par un chiffrement **SSL/TLS (HTTPS)**. La gestion des accès repose sur un modèle **RBAC** (Contrôle d'accès basé sur les rôles) distinguant les Clients, les Prestataires et l'Administrateur.



---

2. Matrice d'Analyse STRIDE

Catégorie	Menace Identifiée	Mesure d'Atténuation (Contre-mesure)
Spoofing	Usurpation d'identité d'un client ou d'un artisan.	Authentification forte, sessions avec drapeaux **HttpOnly/Secure** et affichage du statut **MFA**.
Tampering	Modification des prix des services ou injection de scripts (XSS).	Requêtes préparées **PDO** et neutralisation des sorties via **htmlspecialchars()**.
Repudiation	Un utilisateur nie avoir effectué une action critique (ex: suppression).	Journalisation systématique dans la table activity_logs (IP + Horodatage).

Catégorie	Menace Identifiée	Mesure d'Atténuation (Contre-mesure)
Information Disclosure	Accès non autorisé aux messages privés ou données personnelles.	Chiffrement **SSL** et vérification de l'ID utilisateur en session (prévention IDOR).
Denial of Service	Surcharge de la base de données par des requêtes malveillantes.	Isolation sur le port 3307 et optimisation des requêtes SQL pour la performance.
Elevation of Privilege	Un client accédant aux outils de modération de l'Administrateur.	Vérification stricte du rôle en session à chaque chargement de page sensible (**RBAC**).

---

3. Analyse détaillée des défenses

A. Intégrité et Protection des Entrées (Tampering)

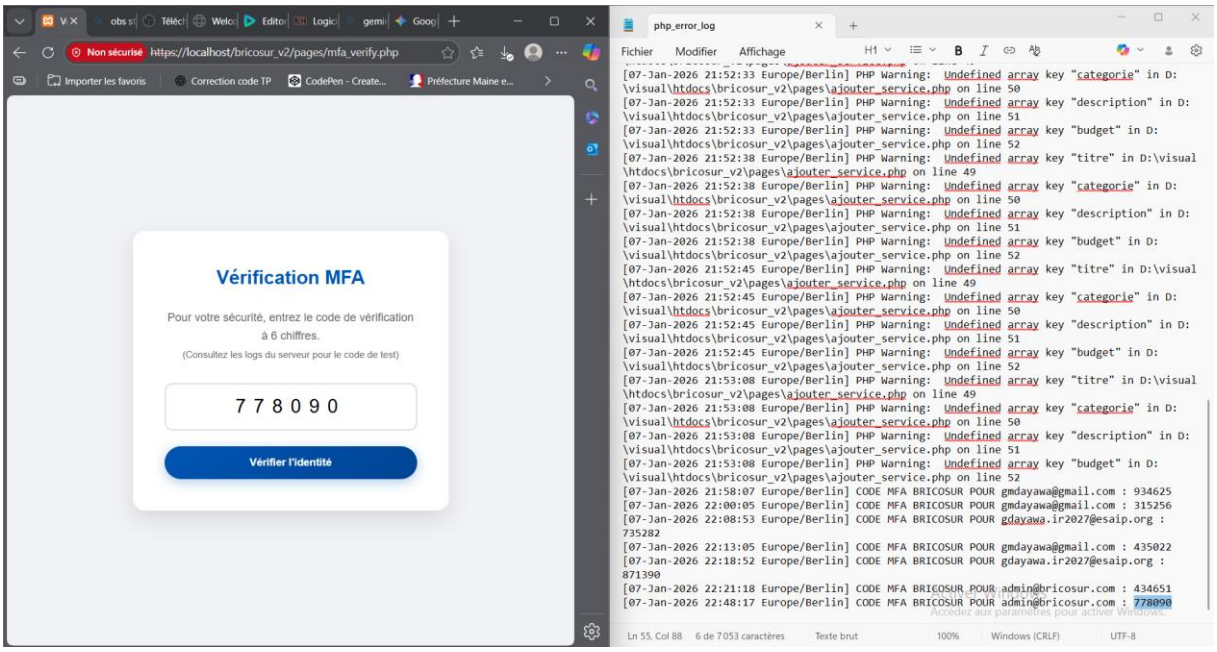
Pour lutter contre l'altération des données, aucune variable utilisateur n'est concaténée directement dans le SQL.

- **Technique :** Utilisation de PDO::prepare() pour toutes les opérations CRUD.
- **Résultat :** Immunité contre les injections SQL classiques.

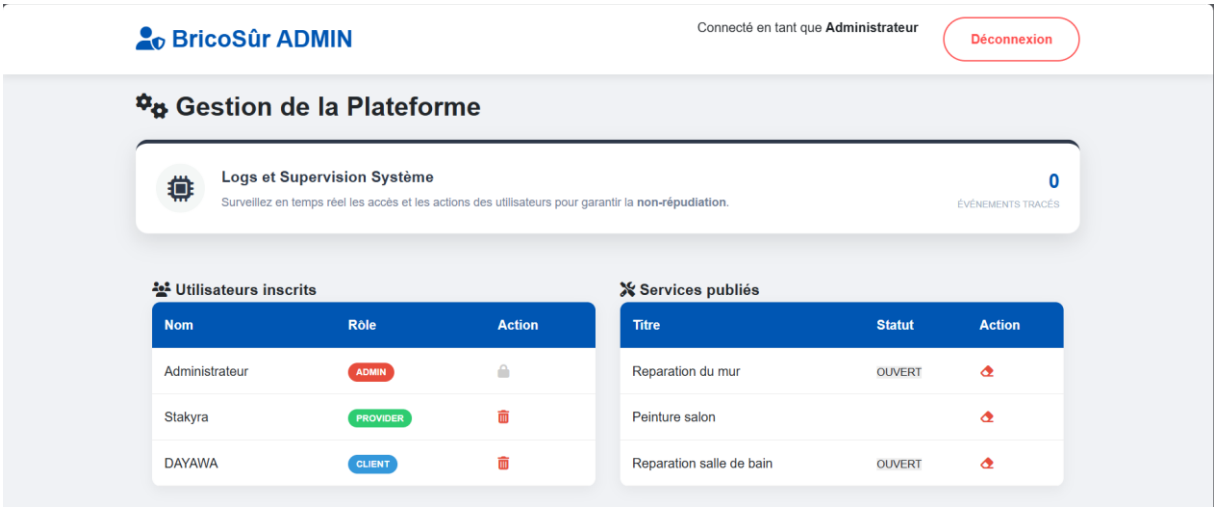
B. Traçabilité et Non-Répudiation (Repudiation)

Chaque action effectuée sur la plateforme (connexion, publication, suppression) génère une entrée dans la console de supervision admin.

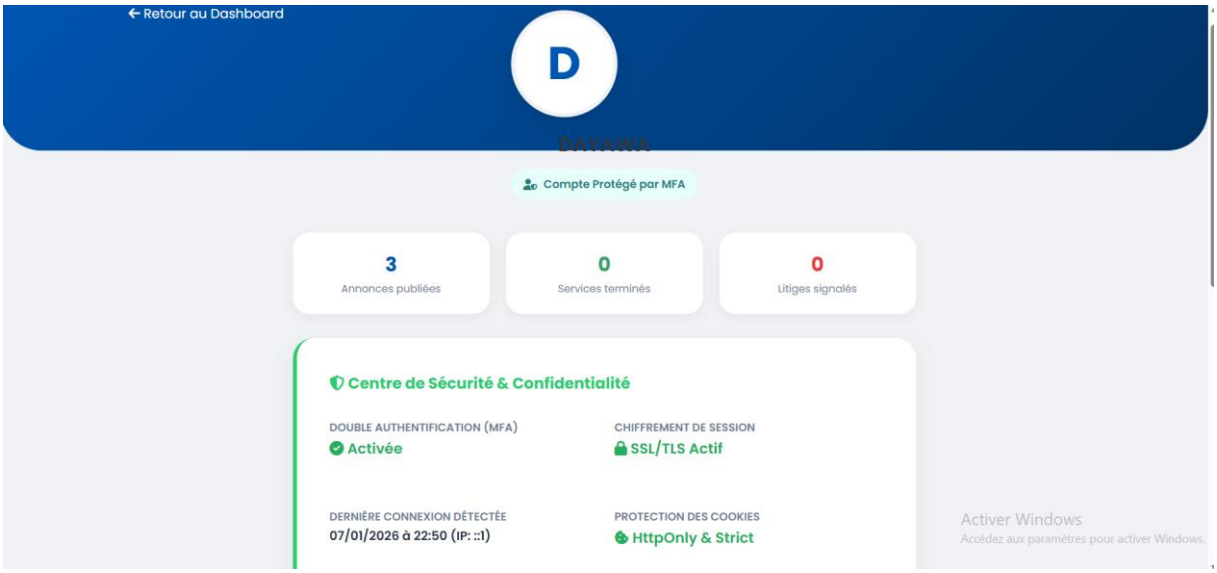
- **Technique :** Capture automatique de $_SERVER['REMOTE_ADDR'] lors des actions sensibles.
- **Résultat :** Preuve d'audit irréfutable en cas d'incident.



Verification MFA.



Page admin



Profil utilisateur securise