2025/2026	AP – Itération 2
BTS SIO	Auteur : Taillé Jade & Delaunay-Guitton Benjamin & Portolleau Anaïs
2SLAM	Date de rédaction : 29/09/2025

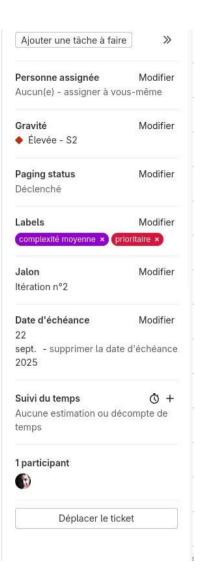
Projet site web R3st0.fr - Itération n°2 - résolution de tickets

Ticket n°10 - faille de sécurité sur la page d'authentification Modifier Ouvert I Incident créé Il v a 3 minutes par Bourgeois Résumé Chronologie On m'a signalé qu'une attaque par injection SQL est possible sur la page de connexion. Scénario: l'utilisateur saisit la chaîne de caractères suivante dans le champ de saisie de l'email; zzz' OR 1 = 1: DELETE FROM photo WHERE '1' et une valeur quelconque dans le mot de passe. L'application refuse l'authentification en affichant le message d'erreur suivant : Liste des erreurs execute queries while there are pending result sets. Consider unsetting the previous PDOStatement or calling PDOStatement::closeCursor() Mais, ensuite, on peut constater que l'attaque a réussi, car les photos des restaurants ne sont plus affichées sur la page d'accueil (ni ailleurs) : les données de la table photo ont été supprimées! Avant: Top 4 des meilleurs restaurants

Après:



On souhaite donc rendre impossibles les attaques par injection SQL sur ce formulaire.



2025/2026	AP – Itération 2
BTS SIO	Auteur : Taillé Jade & Delaunay-Guitton Benjamin & Portolleau Anaïs
2SLAM	Date de rédaction : 29/09/2025

Projet site web R3st0.fr - Itération n°2 - résolution de tickets

Pour empêcher une injection il faut changer le code dans le fichier "connexion.php" lignes 35 à 39 :

```
$mdpU=$ POST["mdpU"];
  35
  36
            $pdo = new PDO('mvsgl:host=localhost;dbname=root', $mailU, $mdpU);
            $stmt = $pdo->prepare('SELECT * FROM utilisateur WHERE mailU = :mailU');
  37
            $stmt->bindParam(':mailU', $mailU);
  38
            $stmt->execute();
  40
  41
            // on tente l'authentification
  42
            //login($mailU,$mdpU);
Aiout du code :
```

\$pdo = new PDO('mysql:host=localhost;dbname=root', \$mailU, \$mdpU); \$stmt = \$pdo->prepare('SELECT * FROM utilisateur WHERE mailU = :mailU'); \$stmt->bindParam(':mailU', \$mailU); \$stmt->execute();

2025/2026	AP – Itération 2
BTS SIO	Auteur : Taillé Jade & Delaunay-Guitton Benjamin & Portolleau Anaïs
2SLAM	Date de rédaction : 29/09/2025



Après avoir entré une injection sql:



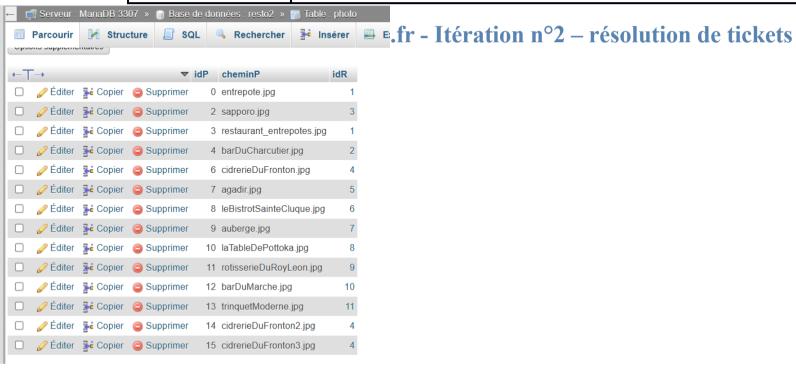
2025/2026	AP – Itération 2
BTS SIO	Auteur : Taillé Jade & Delaunay-Guitton Benjamin & Portolleau Anaïs
2SLAM	Date de rédaction : 29/09/2025



Nous pouvons voir que les photos n'ont pas été supprimer, elles sont toujours présente.

On vérifie sur la bdd distante :

2025/2026	AP – Itération 2
BTS SIO	Auteur : Taillé Jade & Delaunay-Guitton Benjamin & Portolleau Anaïs
2SLAM	Date de rédaction : 29/09/2025



Les photos sont toujours là donc c'est bon