

2025/2026	AP – Itération 2
BTS SIO 2SLAM	Auteur : Taillé Jade & Delaunay-Guitton Benjamin & Portolleau Anaïs 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 Incident créé Il y 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' = '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

- connexion : Erreur dans la méthode modele\dao\RestoDAO::getAimesByIdU : <br/>SQLSTATE[HY000]: General error: 2014 Cannot 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 :



Après :



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

Ajouter une tâche à faire



Personne assignée

Modifier

Aucun(e) - assigner à vous-même

Gravité

Modifier

Élevée - S2

Paging status

Modifier

Déclenché

Labels

Modifier

complexité moyenne x

prioritaire x

Jalon

Modifier

Itération n°2

Date d'échéance

Modifier

22

sept. - supprimer la date d'échéance 2025

Suivi du temps



Aucune estimation ou décompte de temps

1 participant



Déplacer le ticket

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

```

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

```

Ajout 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 2SLAM	Auteur : Taillé Jade & Delaunay-Guitton Benjamin & Portolleau Anaïs
	Date de rédaction : 29/09/2025

http://localhost/PhpProjectSiteRestolInitial/?action=connexion

Accueil Recherche 

## Connexion

zzz' OR 1 = 1 ; DELETE FROM photo WHERE '1' = '1'

....|

Envoyer

[Inscription](#)



---

Utilisateur de test :  
login : test@bts.sio  
mot de passe : sio

## Connexion n°2 – résolution de tickets

Après avoir entré une injection sql :

http://localhost/PhpProjectSiteRestolInitial/?action=connexion 110 %

Accueil Recherche  CGU 

## Liste des erreurs

- connexion : Erreur dans la méthode modele\dao\RestoDAO::getAimesByIdU :   
SQLSTATE[HY000]: General error: 2014 Cannot execute queries while there are pending result sets. Consider unsetting the previous PDOStatement or calling PDOStatement::closeCursor()

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

Accueil
Recherche
CGU
Cont

# *Decouvrez les meilleurs restaurants avec resto.fr*

## Top 4 des meilleurs restaurants

[Cidre du fronton](#)  
Place du Fronton  
64210 Arbonne

[la petite auberge](#)  
15 rue des cordeliers  
64100 Bayonne

[Le Bistrot Sainte Cluque](#)  
9 Rue Hugues  
64100 Bayonne

[La Rotisserie du Roy Léon](#)  
8 rue de coursic  
64100 Bayonne

Classement basé sur les critiques de nos utilisateurs.

Mise à jour effectuée par l'équipe n°P1\_G3

## 2 – résolution de tickets

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 2SLAM	Auteur : Taillé Jade & Delaunay-Guitton Benjamin & Portolleau Anaïs
	Date de rédaction : 29/09/2025

← Serveur : MariaDB:3307 » Base de données : resto2 » Table : photo

Parcourir Structure SQL Rechercher Insérer Exporter

Options supplémentaires

				idP	cheminP	idR
<input type="checkbox"/>	Éditer	Copier	Supprimer	0	entrepote.jpg	1
<input type="checkbox"/>	Éditer	Copier	Supprimer	2	sapporo.jpg	3
<input type="checkbox"/>	Éditer	Copier	Supprimer	3	restaurant_entrepotes.jpg	1
<input type="checkbox"/>	Éditer	Copier	Supprimer	4	barDuCharcutier.jpg	2
<input type="checkbox"/>	Éditer	Copier	Supprimer	6	cidrerieDuFronton.jpg	4
<input type="checkbox"/>	Éditer	Copier	Supprimer	7	agadir.jpg	5
<input type="checkbox"/>	Éditer	Copier	Supprimer	8	leBistrotSainteCluque.jpg	6
<input type="checkbox"/>	Éditer	Copier	Supprimer	9	auberge.jpg	7
<input type="checkbox"/>	Éditer	Copier	Supprimer	10	laTableDePottoka.jpg	8
<input type="checkbox"/>	Éditer	Copier	Supprimer	11	rotisserieDuRoyLeon.jpg	9
<input type="checkbox"/>	Éditer	Copier	Supprimer	12	barDuMarche.jpg	10
<input type="checkbox"/>	Éditer	Copier	Supprimer	13	trinquetModerne.jpg	11
<input type="checkbox"/>	Éditer	Copier	Supprimer	14	cidrerieDuFronton2.jpg	4
<input type="checkbox"/>	Éditer	Copier	Supprimer	15	cidrerieDuFronton3.jpg	4

## .fr - Itération n°2 – résolution de tickets

Les photos sont toujours là donc c'est bon