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 :
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 × prioritaire ×

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