

Ticket n°10

Titre du ticket : faille de sécurité sur la page d'authentification

Type du ticket : incident (évolution/incident)	Niveau de gravité : <input type="checkbox"/> Bloquant <input checked="" type="checkbox"/> Majeur <input type="checkbox"/> Mineur
Émetteur : Nicolas BOURGEOIS (nom de l'émetteur)	Date signalement : 21/09/2024 (jj/mm/aaaa)
Assignation : Stefen (nom du membre de l'équipe en charge du ticket)	Date de résolution souhaitée : 14/10/2024 (jj/mm/aaaa)

Application concernée : R3st0.fr

Version : 1.0 initiale – septembre 2024

Description du problème (avec éventuelles captures d'écran, messages d'erreurs) :

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 :


Top 4 des meilleurs restaurants




L'entresolée
2 rue Maurice Ravel
33000 Bordeaux



Cidrerie du fronton
Place du Fronton
64210 Arbonne



le bar du charcutier
30 rue Parlement Sainte-Catherine
33000 Bordeaux



la petite auberge
15 rue des cordeliers
64100 Bayonne

Top 4 des meilleurs restaurants

L'entresolée

2 rue Maurice Ravel
33000 Bordeaux

Cidrerie du fronton

Place du Fronton
64210 Arbonne

le bar du charcutier

30 rue Parlement Sainte-Catherine
33000 Bordeaux

la petite auberge

15 rue des cordeliers
64100 Bayonne

*Classement basé sur les critiques de nos utilisateurs

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

Solution (diagnostic, localisation, modification, test) :

La méthode qui permet l'authentification est défini dans le fichier authentication.inc.php. Elle utilise la fonction getOneByEmail() pour savoir si l'utilisateur est connu de la BDD ; c'est cette fonction qui nous intéresse.

Pour empêcher les injections SQL, il faut utiliser des requêtes préparées pour séparer le requête SQL et les données utilisateur.

```
public static function getOneByEmail(string $mailU): ?Utilisateur {
    $leUser = null;
    try {
        $requete = "SELECT * FROM utilisateur WHERE mailU = :mailU";
        $stmt = Bdd::getConnection()->prepare($requete);
        $stmt->bindParam(':mailU', $mailU, PDO::PARAM_STR);
        $stmt->execute();

        // Si au moins un (et un seul) utilisateur (car login est unique), c'est que le mail existe dans la BDD
        if ($stmt->rowCount() > 0) {
            $enreg = $stmt->fetch(PDO::FETCH_ASSOC);
            $idU = $enreg['idU'];
            $lesRestosAimes = RestoDAO::getAimesByIdU($idU);

            $leUser = new Utilisateur($idU, $enreg['mailU'], $enreg['mdpU'], $enreg['pseudoU']);

            $leUser ->setLesRestosAimes($lesRestosAimes);
        }
    } catch (PDOException $e) {
        throw new Exception("Erreur dans la méthode " . get_called_class() . "::getOneByEmail : <br/>" . $e->getMessage());
    }
    return $leUser ;
}
```

Un nouveau message d’erreur apparaît stipulant cette fois une erreur lors de la connexion.

Liste des erreurs

- Connexion : erreur de login ou de mot de passe

Connexion

[Inscription](#)

Et les images sont toujours présentes.

