

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

Bourgeois / SiteResto2025 / Tickets / #5

Ticket n°5 - amélioration du chiffrement des mots de passe

Modifier :

Ouvert Incident créé Il y a 7 minutes par Bourgeois[Résumé](#) [Chronologie](#)

Par souci de renforcer la sécurité de l'application, les maîtres d'œuvre souhaitent faire évoluer le traitement des mots de passe des utilisateurs (authentification, nouvelle inscription) pour respecter les préconisations de PHP en la matière. Actuellement, le chiffrement des mots de passe utilise la fonction crypt() avec un sel simpliste (= "sel"). PHP conseille l'usage du couple de fonctions password_hash / password_verify avec l'algorithme de hachage par défaut BCrypt.

Références :

- password_hash <https://www.php.net/manual/fr/function.password-hash.php>
- crypt <https://www.php.net/manual/fr/function.crypt.php>

Avantages de l'utilisation de password_hash : • meilleur algorithme de hachage par défaut (BCRYPT) • évolutive (adaptation automatique aux améliorations des algorithmes) • salage efficace • compatibilité avec crypt, donc les anciens mots de passe resteront utilisables, même s'il sera préférable de les modifier pour générer une meilleure empreinte.

Lexique fonction de hachage : calcule une empreinte numérique non réversible. salage : renforce la sécurité du hachage en y ajoutant une donnée supplémentaire (le sel) afin d'empêcher que deux informations identiques conduisent à la même empreinte => protège des attaques par force brute et par table arc-en-ciel. coût : rend l'algorithme arbitrairement lent et contribue à dissuader les attaques par table arc-en-ciel et par force brute. table arc-en-ciel : table comportant un grand nombre d'empreintes connues, permettant de retrouver un mot de passe à partir de son empreinte.

Modification effectuée à l'instant par Bourgeois



Créer une requête de fusion

Éléments enfants 0

Ajouter

Aucun élément enfant n'est actuellement assigné. Utilisez des éléments enfants pour diviser ce ticket en parties plus petites.

Incidents ou tickets liés 0

Ajouter

Références :

- password_hash <https://www.php.net/manual/fr/function.password-hash.php>
- crypt <https://www.php.net/manual/fr/function.crypt.php>

Ajouter une tâche à faire >>

Personne assignée Modifier
Aucun(e) - assigner à vous-même**Gravité** Modifier
Élevée - S2**Paging status** Modifier
Déclenché**Labels** Modifier
complexe x prioritaire x**Jalon** Modifier
Itération n°2**Date d'échéance** Modifier
29 sept. - supprimer la date d'échéance 2025**Suivi du temps** +
Aucune estimation ou décompte de temps

1 participant



Déplacer le ticket