

PHP – Semaine 3/6 – Séance d'exercices 2/3

Exercice n°22 – Insertion de données en provenance d'un formulaire

Ajoutez dans la page concernant les livres du site des bonnes nouvelles un formulaire HTML qui permette d'ajouter un enregistrement dans la table des livres.

Les Livres

Bienvenue sur la page des livres.

Titre	Auteur
L'instant présent	Main Tenant
Terre: ma Nature	V. du Ciel
Manger jeune, sain et bio	KidsinCuisine
Vivre chaque instant	A. Bonsplans
Le secret du bonheur: aimer	Jolie Joanne
Le grand livre des bonnes nouvelles	M. Youpie Lavie

Titre du livre :

Auteur :

Excellente journée qu'aujourd'hui le 9/02/2019 :: 21.002ms pour exécuter le script PHP :: jeanluc.collinet@vinci.be

Les données du formulaire sont à transmettre au script PHP par la méthode POST.

L'action qui permet de traiter le formulaire est `index.php?action=livres` .

Soyez vigilants : quand vous permettez à un utilisateur d'entrer des données dans un formulaire, celui-ci pourrait taper un script et « attaquer » votre site Web. Par exemple, entrez comme titre du livre `<script>alert('bonjour, je suis un hacker')</script>` et observez le résultat.



Cette page ne fonctionne pas

Chrome a détecté un code inhabituel sur cette page et a bloqué cette dernière pour protéger vos informations personnelles (mots de passe, numéros de téléphone et de cartes de paiement).

Essayez de [consulter la page d'accueil du site](#).

ERR_BLOCKED_BY_XSS_AUDITOR

Cette opération s'appelle une faille XSS, lisez l'article suivant à ce sujet :

http://fr.wikipedia.org/wiki/Cross-site_scripting

De quel type de faille s'agit-il ici, réfléchi ou stocké ?

Pour se prémunir contre cette faille XSS, il suffit d'utiliser la fonction `htmlspecialchars` sur chaque élément du tableau à afficher.
Corrigez votre modèle et votre vue pour éviter les failles XSS dans le futur, et testez-le.

Les Livres	
Bienvenue sur la page des livres.	
Titre	Auteur
<script>alert('bonjour, je suis un hacker')</script>	HaCkEr
L'instant présent	Main Tenant

Dans le code source HTML produit, grâce à la fonction `htmlspecialchars`, `<` est remplacé par `<` et `>` est remplacé par `>`. Ainsi le JavaScript ne s'exécute pas.

```
<tr>
<td><span class="html">&lt;script&gt;alert('bonjour, je suis un hacker')&lt;/script&gt;</span></td>
<td>HaCkEr</td>
```

Enfin, pour terminer cet exercice, affichez une notification adéquate à l'utilisateur selon tous les cas possibles :

- Veuillez entrer un titre et un auteur
- Veuillez entrer un titre
- Veuillez entrer un auteur
- Ajout bien fait

Les Livres	
Bienvenue sur la page des livres.	
Ajout bien fait	
Titre	Auteur
La maîtrise de PHP	Éléphant man
L'instant présent	Main Tenant

Exercice n°23 – Outil formulaire de recherche dans la table des livres

Améliorez la page traitant les livres en créant un outil de recherche : un formulaire HTML avec une zone de texte et un bouton.

En entrant un mot clé, affichez la liste des livres dont le mot clé est présent dans le titre du livre. Cette recherche est réalisée grâce à la clause LIKE en SQL.

Si l'utilisateur n'entre rien comme mot clé, la liste de tous les livres s'affiche.

Les Livres

Bienvenue sur la page des livres.

Rechercher :

Titre	Auteur
Le secret du bonheur: aimer	Jolie Joanne
Le grand livre des bonnes nouvelles	M. Youpie Lavie

Remarque : vérifiez que votre solution fonctionne avec des quotes « ' » et aussi les lettres accentuées, minuscules et majuscules, et, cerise sur le gâteau, même avec un « % » dans le titre d'un livre.

Enfin, veillez à retenir le mot clé que l'utilisateur entre dans la zone de texte, et à sécuriser la faille XSS pour le réaffichage de ce mot clé de recherche.