Bibliothèque de Scripts PHP Prêts à Copier

Cette page vous propose une collection de scripts PHP commentés pour réaliser les tâches courantes d'un site web : formulaire de contact, envoi d'email, upload d'image, gestion de session, etc. Chaque script est fourni avec des explications claires et des notes de sécurité essentielles. Copiez, adaptez et intégrez-les dans vos projets.

Les scripts fournis sont des exemples pédagogiques. Avant de les utiliser en production, testez-les dans un environnement de développement et adaptez-les à vos besoins. Assurez-vous de sécuriser vos formulaires (validation, protection CSRF) et de configurer correctement votre serveur (permissions, HTTPS).

Mode d'emploi

1. Créez un dossier sur votre serveur (par exemple /scripts) et placez-y les fichiers PHP.
2. Copiez le code de chaque script dans un fichier séparé avec l'extension .php.
3. Adaptez les variables de configuration (adresse email, chemins, etc.) à votre environnement.
4. Testez chaque script individuellement en l'appelant depuis votre navigateur.
5. Intégrez les scripts dans vos pages en utilisant include ou require.

Script 1 : Formulaire de contact sécurisé

Ce script gère un formulaire de contact avec validation des champs, protection contre les injections et envoi d'email. Il utilise filter_var pour valider l'email et htmlspecialchars pour échapper les données. Pensez à ajouter un jeton CSRF pour renforcer la sécurité.

Script 2 : Upload d'image avec vérification

Ce script permet d'uploader une image en vérifiant son type (MIME), sa taille et en générant un nom unique. Il limite les extensions autorisées et déplace le fichier dans un dossier sécurisé. N'oubliez pas de définir les permissions du dossier de destination.

Script 3 : Gestion de session utilisateur

Ce script illustre la création d'une session, la vérification de l'utilisateur connecté et la déconnexion. Il utilise session_start() et des variables de session pour stocker les informations. Pensez à régénérer l'ID de session après connexion pour éviter les attaques de fixation.

Modèle prêt à adapter

Envoyer Uploader Déconnexion '; } else { echo ' '; } ?>

Checklist

[ ] Valider toutes les entrées utilisateur avec filter_var ou htmlspecialchars.

[ ] Utiliser des requêtes préparées pour les accès à la base de données.

[ ] Limiter la taille et le type des fichiers uploadés.

[ ] Protéger les formulaires avec un jeton CSRF.

[ ] Utiliser session_regenerate_id() après la connexion.

[ ] Tester les scripts sur un serveur local avant la mise en production.

[ ] Configurer les permissions des fichiers et dossiers (755 pour les dossiers, 644 pour les fichiers).

[ ] Utiliser HTTPS pour chiffrer les données sensibles.

Questions fréquentes

Comment sécuriser un formulaire PHP contre les injections SQL ?

Utilisez des requêtes préparées avec PDO ou MySQLi. Par exemple : $stmt = $pdo->prepare('SELECT * FROM users WHERE email = ?'); $stmt->execute([$email]); Cela empêche l'injection SQL.

Pourquoi mon upload d'image ne fonctionne-t-il pas ?

Vérifiez que le dossier de destination existe et a les permissions d'écriture (par exemple 755). Vérifiez également que le formulaire a bien l'attribut enctype="multipart/form-data" et que la taille du fichier ne dépasse pas la limite définie dans php.ini.

Comment éviter le vol de session ?

Utilisez session_regenerate_id() après la connexion, définissez le paramètre httponly sur true pour les cookies de session, et utilisez HTTPS pour chiffrer les communications.