Pourquoi certaines fonctions PHP sont désactivées par défaut

PHP · https://kyzoe.be/fr/docs/pourquoi-certaines-fonctions-php-sont-desactivees/

Chez **Kyzoe Hosting**, la sécurité, la stabilité et la fiabilité de notre environnement d'hébergement sont essentielles. Pour éviter les abus, les piratages et une charge serveur indésirable, un certain nombre de **fonctions PHP à risque sont désactivées par défaut** sur nos plateformes d'hébergement mutualisé et managé.

Cette mesure est conforme aux bonnes pratiques des environnements d'hébergement professionnels et répond aux exigences en matière de **security hardening**.

Quelles fonctions PHP sont désactivées ?

Les fonctions suivantes sont désactivées par défaut :

```
exec, system, passthru, shell_exec, dl, popen, show_source,
posix_kill, posix_mkfifo, posix_getpwuid, posix_setpgid,
posix_setsid, posix_setuid, posix_setgid, posix_seteuid,
posix_setegid, posix_uname,
pcntl_exec, expect_popen
```

Pourquoi ces fonctions sont-elles désactivées ?

1. Exécution de commandes serveur (risque de sécurité critique)

Des fonctions comme `exec`, `system`, `shell_exec`, `passthru`, `popen`, `pcntl_exec` et `expect_popen` permettent à PHP d'**exécuter directement des commandes système**.

➡ **Risque** :
Avec une extension ou un thème vulnérable, ou du code mal écrit, un attaquant peut :

- obtenir un accès shell

- installer des logiciels malveillants
- compromettre d’autres sites web sur le même serveur

---

2. Manipulation des processus système et des utilisateurs

Les fonctions `posix_*` donnent accès à des **fonctionnalités Unix de bas niveau**, comme :

- les droits des utilisateurs et des groupes
- la gestion des processus
- les informations système

➡ **Risque** :
Ces fonctions ne sont **pas nécessaires aux applications web standard** (comme WordPress, Joomla ou Laravel), mais peuvent être détournées pour une élévation de privilèges (privilege escalation).

---

3. Chargement dynamique d’extensions PHP (`dl()`)

La fonction `dl()` permet de charger des extensions PHP **pendant l’exécution**.

➡ **Risque** :

- Contournement de la configuration du serveur
- Comportement imprévisible et instabilité
- Exécution potentielle de code indésirable

---

4. Fuites d’informations via le code source

La fonction `show_source()` peut rendre visible le code source PHP.

➡ **Risque** :

- Exposition de clés API
- Divulgation de données de base de données ou de la logique interne

---

Mon site web a-t-il besoin de ces fonctions ?

Dans **99 % des cas : non**.

Les CMS et frameworks populaires fonctionnent **parfaitement sans ces fonctions** :

- WordPress
- WooCommerce
- Drupal
- Joomla
- Laravel
- Symfony

Si une application dépend malgré tout de telles fonctions, cela indique souvent :

- un logiciel obsolète
- du code sur mesure non sécurisé
- une application qui aurait davantage sa place sur un **VPS ou un serveur dédié**

Puis-je faire activer ces fonctions ?

Pour des raisons de sécurité, ces fonctions **ne peuvent pas être activées sur un hébergement mutualisé**.

Vous avez un cas d'usage légitime ?

- Contactez notre support
- Nous examinerons ensemble si une **solution VPS** ou une configuration de serveur personnalisée est indiquée

---

En résumé

✔ Sécurité renforcée
✔ Protection contre les piratages et les logiciels malveillants
✔ Meilleure stabilité du serveur
✔ Conforme aux normes d'hébergement professionnelles

En désactivant ces fonctions PHP, nous veillons à ce que **votre site web et les autres clients restent en sécurité**.