Rapport malware et vulnérabilités serveur

Exemple de rapport malware et vulnérabilités serveur

Rapport généré: 24 nov. 2026, 10:10

> Les noms, noms de fichiers et arborescences de cet exemple public sont fictifs. Le code source, les données des requêtes, les notes du client et les identifiants ont été supprimés. Les avis ont été reformulés ; les nombres de signalements, les évaluations et les résultats de revue sont conservés.

Résultat actuel

Moyen

Signalements: 213 | À examiner : 137 | Probablement inoffensifs : 0 | Résolus, acceptés ou ignorés : 76

Le risque reflète les signalements à examiner. Ceux que l'IA juge probablement inoffensifs sont comptés séparément.

Gravité	Signalements initiaux	À examiner
Critique	0	0
Élevé	6	0
Moyen	8	4
Faible	191	125
À titre informatif	8	8

Résumé

Cette analyse réelle a relevé 213 éléments. Après revue, 137 restent à examiner : 4 de gravité moyenne, 125 faible et 8 informatifs. Les 76 autres ont été résolus, acceptés ou ignorés. Les versions PHP utilisées incluent le correctif PHP2Shell ; les anciennes versions inutilisées restent à nettoyer.

Les signalements sont des indices, pas des preuves, et une analyse ne voit que ce que ce compte peut lire. Aucune analyse ne peut prouver qu'un serveur n'a pas été compromis.

PHP2Shell

Corrigé là où il est utilisé

Le PHP utilisé par vos sites inclut le correctif. Un PHP plus ancien est installé, mais ce compte ne l'utilise pas : supprimez-le quand vous le pourrez.

PHP	Version	Statut	Corrigé dans	Utilisé
/opt/example-php/runtime-01/bin/php	8.2.35	Corrigé	8.2.35	Oui
/opt/example-php/runtime-02/bin/php	7.4.33	Non pris en charge	-	Non
/opt/example-php/runtime-03/bin/php	8.0.30	Non pris en charge	-	Non
/opt/example-php/runtime-04/bin/php	8.1.34	Non pris en charge	-	Non
/opt/example-php/runtime-05/bin/php	8.3.36	Corrigé	8.3.36	Non
/opt/example-php/runtime-06/bin/php	8.4.27	Corrigé	8.4.27	Non
/opt/example-php/runtime-07/bin/php	8.5.12	Corrigé	8.5.12	Non

PHP	Version	Statut	Corrigé dans	Utilisé
/opt/example-php/runtime-08/bin/php	7.4.33	Non pris en charge	-	Non
/opt/example-php/runtime-09/bin/php	8.0.30	Non pris en charge	-	Non
/opt/example-php/runtime-10/bin/php	8.1.34	Non pris en charge	-	Non
/opt/example-php/runtime-11/bin/php	8.2.35	Corrigé	8.2.35	Oui
/opt/example-php/runtime-12/bin/php	8.3.36	Corrigé	8.3.36	Non
/opt/example-php/runtime-13/bin/php	8.4.27	Corrigé	8.4.27	Non
/opt/example-php/runtime-14/bin/php	8.5.12	Corrigé	8.5.12	Non

Utilisé : ce que montrent les pools PHP-FPM, les processus en cours, la commande php et les tâches planifiées de ce compte. Un autre compte sur le même serveur peut encore utiliser un PHP marqué Non.

Vérifications

Vérifications	Statut
Serveur et système d’exploitation	Terminée
Panneau d’hébergement	Terminée
Versions de PHP	Terminée
Paquets PHP	Terminée
Correctifs PHP2Shell de la distribution	Terminée
Sites web et applications	Terminée
Réglages de débogage	Terminée
Tâches planifiées	Terminée
Fichiers de démarrage du shell	Terminée
Clés SSH	Terminée
Services utilisateur	Terminée
Programmes au démarrage	Terminée
Bibliothèques préchargées	Terminée
Dossiers temporaires	Terminée
Processus en cours	Terminée
Points d’accroche au démarrage de Python	Terminée
Inventaire des fichiers	Terminée
Motifs de code PHP	Terminée
Motifs de code Python	Terminée
Scripts au mauvais endroit	Terminée
Noms de fichiers déguisés	Terminée
PHP caché dans d’autres types de fichiers	Terminée

Vérifications	Statut
Code déguisé	Terminée
Fichiers de configuration du serveur	Terminée
Fichiers exposés	Terminée
Droits des fichiers	Terminée
Dates de fichiers modifiées	Terminée
Journaux d'accès web	Terminée
Journaux d'erreurs	Terminée
Évaluation PHP2Shell	Terminée
Réglage de suivi des téléversements PHP	Terminée

Signalements (213)

Fichier nommé comme une image ou un document mais exécuté comme PHP (3)

Ce que cela signifie: Le nom du fichier comporte deux extensions (par exemple photo.jpg.php) ou fait passer un fichier PHP pour un média. C'est un moyen courant de faire passer un script à travers les filtres de téléversement.

Comment corriger: Supprimez le fichier, sauf si vous savez exactement pourquoi il existe, puis vérifiez le formulaire de téléversement qui l'a accepté.

`/home/example-user/archive/sample-188.txt.php`

Élevé | Confiance moyenne | Résolu | Suspect (Avis de l'IA (à titre indicatif) #1)

`/home/example-user/archive/sample-189.txt.php`

Élevé | Confiance moyenne | Résolu | Suspect (Avis de l'IA (à titre indicatif) #1)

`/srv/example-app/packages/sample-190.txt.php`

Élevé | Confiance moyenne | Risque accepté | À examiner (Avis de l'IA (à titre indicatif) #2)

> #### Avis de l'IA (à titre indicatif) #1 - Suspect
>
> **Explication:** L'évaluation initiale de l'IA a relevé des caractéristiques suspectes à examiner. Elles ne prouvent pas à elles seules une compromission.
>
> **Comment vérifier:** Comparez le fichier à une version fiable de l'application et examinez son contexte avant toute modification.
>
> **Correction:** Supprimez le fichier, sauf si vous savez exactement pourquoi il existe, puis vérifiez le formulaire de téléversement qui l'a accepté.
>
> **Éviter que cela se reproduise:** Maintenez les logiciels pris en charge à jour et comparez les changements inattendus à une référence fiable.

> #### Avis de l'IA (à titre indicatif) #2 - À examiner
>
> **Explication:** L'évaluation initiale de l'IA n'a pas pu déterminer si cet élément était attendu. Examinez les preuves et le contexte de l'application.
>
> **Comment vérifier:** Comparez le fichier à une version fiable de l'application et examinez son contexte avant toute modification.
>
> **Correction:** Supprimez le fichier, sauf si vous savez exactement pourquoi il existe, puis vérifiez le formulaire de téléversement qui l'a accepté.
>
> **Éviter que cela se reproduise:** Maintenez les logiciels pris en charge à jour et comparez les changements inattendus à une référence fiable.

Code PHP dans un fichier qui n'est pas un fichier PHP (3)

Ce que cela signifie: Un fichier portant une autre extension (une image, un fichier texte ou une icône, par exemple) contient du code PHP. Avec un serveur mal configuré ou une inclusion, il peut être exécuté comme un script.

Comment corriger: Consultez le fichier en lecture seule. Supprimez-le s'il ne s'agit pas d'un fichier authentique, et cherchez le code qui l'inclut.

`/srv/example-app/public/media/sample-191.txt`

Élevé | Confiance moyenne | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

`/srv/example-app/public/media/sample-192.txt`

Élevé | Confiance moyenne | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

`/srv/example-app/public/media/sample-193.txt`

Élevé | Confiance moyenne | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

> ### Avis de l'IA (à titre indicatif) #1 - Probablement inoffensif
>
> **Explication:** L'évaluation initiale de l'IA jugeait cet élément probablement inoffensif dans le contexte de l'application. Cet avis ne prouve pas qu'un fichier est sûr.
>
> **Comment vérifier:** Comparez le fichier à une version fiable de l'application et examinez son contexte avant toute modification.
>
> **Correction:** Consultez le fichier en lecture seule. Supprimez-le s'il ne s'agit pas d'un fichier authentique, et cherchez le code qui l'inclut.
>
> **Éviter que cela se reproduise:** Maintenez les logiciels pris en charge à jour et comparez les changements inattendus à une référence fiable.

Sauvegarde ou archive dans le dossier web public (6)

Ce que cela signifie: Les sauvegardes, exports de base de données ou archives placés dans le dossier public peuvent souvent être téléchargés par quiconque devine leur nom.

Comment corriger: Déplacez les sauvegardes hors du dossier public et supprimez les copies dont vous n'avez plus besoin.

`/srv/example-app/public/sample-001.zip`

Moyen | Confiance moyenne | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

`/srv/example-app/public/sample-002.zip`

Moyen | Confiance moyenne | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

`/srv/example-app/public/media/sample-003.zip`

Moyen | Confiance moyenne | Ouvert | À examiner (Avis de l'IA (à titre indicatif) #2)

`/srv/example-app/public/media/sample-004.zip`

Moyen | Confiance moyenne | Ouvert | À examiner (Avis de l'IA (à titre indicatif) #2)

`/srv/example-app/public/media/sample-005.zip`

Moyen | Confiance moyenne | Ouvert | À examiner (Avis de l'IA (à titre indicatif) #2)

`/srv/example-app/public/media/sample-006.zip`

Moyen | Confiance moyenne | Ouvert | À examiner (Avis de l'IA (à titre indicatif) #2)

> ### Avis de l'IA (à titre indicatif) #1 - Probablement inoffensif
>
> **Explication:** L'évaluation initiale de l'IA jugeait cet élément probablement inoffensif dans le contexte de l'application. Cet avis ne prouve pas qu'un fichier est sûr.
>
> **Comment vérifier:** Comparez le fichier à une version fiable de l'application et examinez son contexte avant toute modification.
>
> **Correction:** Déplacez les sauvegardes hors du dossier public et supprimez les copies dont vous n'avez plus besoin.
>
> **Éviter que cela se reproduise:** Maintenez les logiciels pris en charge à jour et comparez les changements inattendus à une référence fiable.

> ### Avis de l’IA (à titre indicatif) #2 - À examiner
>
> **Explication:** L’évaluation initiale de l’IA n’a pas pu déterminer si cet élément était attendu. Examinez les preuves et le contexte de l’application.
>
> **Comment vérifier:** Comparez le fichier à une version fiable de l’application et examinez son contexte avant toute modification.
>
> **Correction:** Déplacez les sauvegardes hors du dossier public et supprimez les copies dont vous n’avez plus besoin.
>
> **Éviter que cela se reproduise:** Maintenez les logiciels pris en charge à jour et comparez les changements inattendus à une référence fiable.

Paquet de pages d’erreur pour développeurs installé (1)

Ce que cela signifie: Un paquet de pages d’erreur de développement (comme Laravel Ignition) est installé. D’anciennes versions présentaient des failles graves, et les pages de débogage divulguent des détails.

Comment corriger: N’installez que les dépendances de production (composer install --no-dev) ou mettez le paquet à jour, et laissez le mode débogage désactivé.

`/srv/example-app/packages/sample-007.php`

Moyen | Confiance moyenne | Ignoré | Probablement inoffensif (Avis de l’IA (à titre indicatif) #1)

> ### Avis de l’IA (à titre indicatif) #1 - Probablement inoffensif
>
> **Explication:** L’évaluation initiale de l’IA jugeait cet élément probablement inoffensif dans le contexte de l’application. Cet avis ne prouve pas qu’un fichier est sûr.
>
> **Comment vérifier:** Comparez le fichier à une version fiable de l’application et examinez son contexte avant toute modification.
>
> **Correction:** N’installez que les dépendances de production (composer install --no-dev) ou mettez le paquet à jour, et laissez le mode débogage désactivé.
>
> **Éviter que cela se reproduise:** Maintenez les logiciels pris en charge à jour et comparez les changements inattendus à une référence fiable.

Programme en cours d’exécution dont le fichier a été supprimé (1)

Ce que cela signifie: Un processus appartenant à ce compte s’exécute à partir d’un fichier qui n’existe plus. Les mises à jour logicielles peuvent en être la cause, mais les logiciels malveillants se suppriment aussi après leur lancement.

Comment corriger: Identifiez le processus avec ps et arrêtez-le si vous ne le reconnaissez pas.

`/srv/example-workers/sample-213.bin`

Moyen | Confiance faible | Ignoré | Probablement inoffensif (Avis de l’IA (à titre indicatif) #1)

> ### Avis de l’IA (à titre indicatif) #1 - Probablement inoffensif
>
> **Explication:** L’évaluation initiale de l’IA jugeait cet élément probablement inoffensif dans le contexte de l’application. Cet avis ne prouve pas qu’un fichier est sûr.
>
> **Comment vérifier:** Comparez le fichier à une version fiable de l’application et examinez son contexte avant toute modification.
>
> **Correction:** Identifiez le processus avec ps et arrêtez-le si vous ne le reconnaissez pas.
>
> **Éviter que cela se reproduise:** Maintenez les logiciels pris en charge à jour et comparez les changements inattendus à une référence fiable.

Les dates du fichier semblent modifiées (153)

Ce que cela signifie: L’heure de changement d’état du fichier (ctime) est bien plus récente que son heure de modification (mtime). Les attaquants reculent souvent les dates de modification pour qu’un fichier déposé se fonde parmi les plus anciens ; les restaurations et certains outils de déploiement peuvent aussi en être la cause.

Comment corriger: Vérifiez qui a modifié le fichier et quand. Si personne de votre côté ne l’a fait, examinez son contenu.

`/srv/example-app/packages/sample-008.php`

Faible | Confiance faible | Ouvert

`/srv/example-app/packages/sample-009.php`

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l’IA (à titre indicatif) #1)

/srv/example-app/packages/sample-010.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-011.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-012.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-013.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-014.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-015.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-016.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-017.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-018.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-019.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-020.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-021.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-022.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-023.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-024.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-025.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-026.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-027.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-028.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-029.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-030.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-031.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-032.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-033.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-034.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-035.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-036.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-037.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-038.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-039.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-040.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-041.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-042.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-043.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-044.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-045.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-046.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-047.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-048.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-049.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-050.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-051.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-052.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-053.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-054.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-055.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-056.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-057.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-058.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-059.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-060.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-061.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-062.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-063.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-064.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-065.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-066.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-067.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-068.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-069.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-070.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-071.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-072.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-073.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-074.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-075.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-076.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-077.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-078.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-079.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-080.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-081.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-082.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-083.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-084.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-085.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-086.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-087.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-088.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-089.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-090.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-091.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-092.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-093.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-094.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-095.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-096.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-097.php

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/srv/example-app/packages/sample-098.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-099.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-100.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-101.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-102.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-103.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-104.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-105.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-106.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-107.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-108.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-109.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-110.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-111.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-112.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-113.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-114.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-115.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-116.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-117.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-118.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-119.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-120.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-121.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-122.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-123.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-124.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-125.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-126.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-127.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-128.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-129.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-130.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-131.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-132.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-133.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-134.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-135.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-136.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-137.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-138.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-139.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-140.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-141.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-142.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-143.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-144.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-145.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-146.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-147.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-148.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-149.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-150.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-151.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-152.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-153.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-154.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-155.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-156.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-157.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-158.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-159.php

Faible | Confiance faible | Ouvert

/srv/example-app/packages/sample-160.php

Faible | Confiance faible | Ouvert

> ### Avis de l'IA (à titre indicatif) #1 - Probablement inoffensif
>
> **Explication:** L'évaluation initiale de l'IA jugeait cet élément probablement inoffensif dans le contexte de l'application. Cet avis ne prouve pas qu'un fichier est sûr.
>
> **Comment vérifier:** Comparez le fichier à une version fiable de l'application et examinez son contexte avant toute modification.
>
> **Correction:** Vérifiez qui a modifié le fichier et quand. Si personne de votre côté ne l'a fait, examinez son contenu.
>
> **Éviter que cela se reproduise:** Maintenez les logiciels pris en charge à jour et comparez les changements inattendus à une référence fiable.

Requêtes contenant des données qui ressemblent à une attaque (27)

Ce que cela signifie: Vos journaux d'accès contiennent des requêtes avec des charges d'attaque typiques. La plupart sont des sondages automatisés qui échouent ; elles sont listées pour le contexte.

Comment corriger: Aucune action n'est nécessaire, sauf si des requêtes correspondantes ont abouti. Maintenez vos logiciels à jour.

/var/log/example-app/sample-161.log

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/var/log/example-app/sample-162.log

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/var/log/example-app/sample-163.log

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/var/log/example-app/sample-164.log

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/var/log/example-app/sample-165.log

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/var/log/example-app/sample-166.log

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/var/log/example-app/sample-167.log

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/var/log/example-app/sample-168.log

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/var/log/example-app/sample-169.log

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/var/log/example-app/sample-170.log

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/var/log/example-app/sample-171.log

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/var/log/example-app/sample-172.log

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/var/log/example-app/sample-173.log

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/var/log/example-app/sample-174.log

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/var/log/example-app/sample-175.log

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/var/log/example-app/sample-176.log

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/var/log/example-app/sample-177.log

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/var/log/example-app/sample-178.log

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/var/log/example-app/sample-179.log

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/var/log/example-app/sample-180.log

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

/var/log/example-app/sample-181.log

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

`/var/log/example-app/sample-182.log`

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

`/var/log/example-app/sample-183.log`

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

`/var/log/example-app/sample-184.log`

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

`/var/log/example-app/sample-185.log`

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

`/var/log/example-app/sample-186.log`

Faible | Confiance faible | Ignoré | Probablement inoffensif (Avis de l'IA (à titre indicatif) #1)

`/var/log/example-app/sample-187.log`

Faible | Confiance faible | Ouvert

> ### Avis de l'IA (à titre indicatif) #1 - Probablement inoffensif
>
> **Explication:** L'évaluation initiale de l'IA jugeait cet élément probablement inoffensif dans le contexte de l'application. Cet avis ne prouve pas qu'un fichier est sûr.
>
> **Comment vérifier:** Comparez le fichier à une version fiable de l'application et examinez son contexte avant toute modification.
>
> **Correction:** Aucune action n'est nécessaire, sauf si des requêtes correspondantes ont abouti. Maintenez vos logiciels à jour.
>
> **Éviter que cela se reproduise:** Maintenez les logiciels pris en charge à jour et comparez les changements inattendus à une référence fiable.

Code fortement camouflé (4)

Ce que cela signifie: Le fichier contient de longues chaînes encodées, du texte construit caractère par caractère ou un camouflage similaire. Il peut s'agir de la protection anticopie d'une extension payante, ou d'un logiciel malveillant qui cache son but.

Comment corriger: Comparez le fichier avec la copie de l'éditeur. Les fichiers camouflés inconnus dans un dossier du site doivent être examinés par quelqu'un qui connaît l'application.

`/srv/example-app/packages/sample-194.php`

Faible | Confiance faible | Ouvert

`/srv/example-app/packages/sample-195.php`

Faible | Confiance faible | Ouvert

`/srv/example-app/packages/sample-196.php`

Faible | Confiance faible | Ouvert

`/srv/example-app/packages/sample-197.php`

Faible | Confiance faible | Ouvert

Ancien PHP installé, non utilisé par vos sites (6)

Ce que cela signifie: Ce PHP n'est plus pris en charge, est antérieur au correctif PHP2Shell ou son correctif n'a pas pu être confirmé, mais rien sur ce compte ne l'utilise : aucun pool PHP-FPM, aucun processus en cours, aucune commande php ni aucune tâche planifiée. Avec la configuration actuelle, il ne peut pas servir vos sites ; sa gravité est donc faible. Un autre compte sur le même serveur pourrait toutefois encore l'utiliser.

Comment corriger: Supprimez-le si rien n'en a besoin (votre hébergeur ou votre panneau de contrôle peut désinstaller une version de PHP), et ne basculez aucun site vers cette version.

/opt/example-php/sample-198.php

Faible | Confiance moyenne | Ouvert

/opt/example-php/sample-199.php

Faible | Confiance moyenne | Ouvert

/opt/example-php/sample-200.php

Faible | Confiance moyenne | Ouvert

/opt/example-php/sample-201.php

Faible | Confiance moyenne | Ouvert

/opt/example-php/sample-202.php

Faible | Confiance moyenne | Ouvert

/opt/example-php/sample-203.php

Faible | Confiance moyenne | Ouvert

Le suivi de progression des téléversements de PHP est activé (1)

Ce que cela signifie: session.upload_progress.enabled est activé. Les problèmes PHP2Shell concernent cette fonction ; la désactiver réduit donc l'exposition si vous ne l'utilisez pas.

Comment corriger: Définissez session.upload_progress.enabled = Off dans php.ini ou .user.ini si vos sites n'affichent pas la progression des téléversements.

/etc/example-php/sample-212.ini

Faible | Confiance moyenne | Ouvert

PHP inclut le correctif PHP2Shell (8)

Ce que cela signifie: Ce PHP est à la version corrigée ou au-delà, ou le paquet de son fournisseur confirme le correctif.

Comment corriger: Aucune action liée à PHP2Shell n'est nécessaire pour ce PHP.

/opt/example-php/sample-204.php

À titre informatif | Confiance élevée | Ouvert

/opt/example-php/sample-205.php

À titre informatif | Confiance élevée | Ouvert

/opt/example-php/sample-206.php

À titre informatif | Confiance élevée | Ouvert

/opt/example-php/sample-207.php

À titre informatif | Confiance élevée | Ouvert

/opt/example-php/sample-208.php

À titre informatif | Confiance élevée | Ouvert

/opt/example-php/sample-209.php

À titre informatif | Confiance élevée | Ouvert

/opt/example-php/sample-210.php

À titre informatif | Confiance élevée | Ouvert

/opt/example-php/sample-211.php

À titre informatif | Confiance élevée | Ouvert