Malware- und Server-Schwachstellenbericht

Beispielbericht für Malware und Server-Schwachstellen

Bericht erstellt: 24 Nov 2026, 14:10

> Namen, Dateinamen und Verzeichnisstrukturen in diesem öffentlichen Beispiel sind erfunden. Quellcode, Anfragedaten, Kundennotizen und Kennungen wurden entfernt. Hinweise wurden neu formuliert; Anzahl, Bewertungen und Prüfentscheidungen bleiben erhalten.

Aktuelles Ergebnis

Mittel

Funde: 213 | Zu prüfen: 137 | Wahrscheinlich harmlos: 0 | Behoben, akzeptiert oder ignoriert: 76

Das Risiko berücksichtigt noch zu prüfende Funde. Von der KI als wahrscheinlich harmlos bewertete Funde werden separat gezählt.

Schweregrad	Ursprüngliche Befunde	Zu prüfen
Kritisch	0	0
Hoch	6	0
Mittel	8	4
Niedrig	191	125
Informativ	8	8

Zusammenfassung

Dieser echte Scan ergab 213 Funde. Nach der Prüfung benötigen 137 weiterhin Aufmerksamkeit: 4 mittlere, 125 niedrige und 8 informative Funde. Die übrigen 76 wurden behoben, akzeptiert oder ignoriert. Die verwendeten PHP-Versionen enthalten den PHP2Shell-Fix; ungenutzte ältere Versionen sollten noch bereinigt werden.

Funde sind Anzeichen, keine Beweise, und ein Scan sieht nur, was dieses Konto lesen kann. Kein Scan kann beweisen, dass ein Server nicht kompromittiert wurde.

PHP2Shell

Behoben, wo es genutzt wird

Das PHP, das Ihre Websites nutzen, enthält die Korrektur. Älteres PHP ist zwar installiert, wird von diesem Konto aber nicht genutzt: Entfernen Sie es bei Gelegenheit.

PHP	Version	Status	Behoben in	Genutzt
/opt/example-php/runtime-01/bin/php	8.2.35	Behoben	8.2.35	Ja
/opt/example-php/runtime-02/bin/php	7.4.33	Nicht mehr unterstützt	-	Nein
/opt/example-php/runtime-03/bin/php	8.0.30	Nicht mehr unterstützt	-	Nein
/opt/example-php/runtime-04/bin/php	8.1.34	Nicht mehr unterstützt	-	Nein
/opt/example-php/runtime-05/bin/php	8.3.36	Behoben	8.3.36	Nein
/opt/example-php/runtime-06/bin/php	8.4.27	Behoben	8.4.27	Nein
/opt/example-php/runtime-07/bin/php	8.5.12	Behoben	8.5.12	Nein

PHP	Version	Status	Behoben in	Genutzt
/opt/example-php/runtime-08/bin/php	7.4.33	Nicht mehr unterstützt	-	Nein
/opt/example-php/runtime-09/bin/php	8.0.30	Nicht mehr unterstützt	-	Nein
/opt/example-php/runtime-10/bin/php	8.1.34	Nicht mehr unterstützt	-	Nein
/opt/example-php/runtime-11/bin/php	8.2.35	Behoben	8.2.35	Ja
/opt/example-php/runtime-12/bin/php	8.3.36	Behoben	8.3.36	Nein
/opt/example-php/runtime-13/bin/php	8.4.27	Behoben	8.4.27	Nein
/opt/example-php/runtime-14/bin/php	8.5.12	Behoben	8.5.12	Nein

Genutzt: was die PHP-FPM-Pools, die laufenden Prozesse, der php-Befehl und die geplanten Aufgaben dieses Kontos zeigen. Ein anderes Konto auf demselben Server kann ein mit Nein markiertes PHP trotzdem nutzen.

Prüfungen

Prüfungen	Status
Server und Betriebssystem	Abgeschlossen
Hosting-Panel	Abgeschlossen
PHP-Versionen	Abgeschlossen
PHP-Pakete	Abgeschlossen
PHP2Shell-Korrekturen der Distribution	Abgeschlossen
Websites und Anwendungen	Abgeschlossen
Debug-Einstellungen	Abgeschlossen
Geplante Aufgaben	Abgeschlossen
Shell-Startdateien	Abgeschlossen
SSH-Schlüssel	Abgeschlossen
Benutzerdienste	Abgeschlossen
Autostart-Einträge	Abgeschlossen
Vorgeladene Bibliotheken	Abgeschlossen
Temporäre Ordner	Abgeschlossen
Laufende Prozesse	Abgeschlossen
Python-Start-Hooks	Abgeschlossen
Dateibestand	Abgeschlossen
PHP-Codemuster	Abgeschlossen
Python-Codemuster	Abgeschlossen
Skripte am falschen Ort	Abgeschlossen
Getarnte Dateinamen	Abgeschlossen
In anderen Dateitypen verstecktes PHP	Abgeschlossen

Prüfungen	Status
Getarnter Code	Abgeschlossen
Server-Konfigurationsdateien	Abgeschlossen
Offen zugängliche Dateien	Abgeschlossen
Dateiberechtigungen	Abgeschlossen
Veränderte Dateidaten	Abgeschlossen
Web-Zugriffsprotokolle	Abgeschlossen
Fehlerprotokolle	Abgeschlossen
PHP2Shell-Bewertung	Abgeschlossen
PHP-Einstellung für den Upload-Fortschritt	Abgeschlossen

Funde (213)

Datei, die wie ein Bild oder Dokument heißt, aber als PHP ausgeführt wird (3)

Was das bedeutet: Der Dateiname hat zwei Endungen (zum Beispiel photo.jpg.php) oder tarnt eine PHP-Datei als Mediendatei. Auf diese Weise wird häufig ein Skript an Upload-Filtern vorbeigeschleust.

So beheben Sie es: Entfernen Sie die Datei, sofern Sie nicht genau wissen, warum sie existiert, und prüfen Sie dann das Upload-Formular, das sie angenommen hat.

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

Hoch | Mittlere Zuverlässigkeit | Erledigt | Verdächtig (KI-Einschätzung (unverbindlich) #1)

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

Hoch | Mittlere Zuverlässigkeit | Erledigt | Verdächtig (KI-Einschätzung (unverbindlich) #1)

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

Hoch | Mittlere Zuverlässigkeit | Akzeptiertes Risiko | Muss untersucht werden (KI-Einschätzung (unverbindlich) #2)

> #### KI-Einschätzung (unverbindlich) #1 - Verdächtig
>
> **Erklärung:** Die ursprüngliche KI-Bewertung fand verdächtige Merkmale, die geprüft werden sollten. Sie allein belegen keine Kompromittierung.
>
> **So überprüfen Sie es:** Vergleichen Sie die Datei mit einer vertrauenswürdigen Anwendungsversion und prüfen Sie den Kontext, bevor Sie etwas ändern.
>
> **Behebung:** Entfernen Sie die Datei, sofern Sie nicht genau wissen, warum sie existiert, und prüfen Sie dann das Upload-Formular, das sie angenommen hat.
>
> **Wiederholung verhindern:** Halten Sie unterstützte Software aktuell und vergleichen Sie unerwartete Änderungen mit einem vertrauenswürdigen Ausgangsstand.

> #### KI-Einschätzung (unverbindlich) #2 - Muss untersucht werden
>
> **Erklärung:** Die ursprüngliche KI-Bewertung konnte nicht feststellen, ob dies erwartet war. Prüfen Sie die Belege und den Anwendungskontext.
>
> **So überprüfen Sie es:** Vergleichen Sie die Datei mit einer vertrauenswürdigen Anwendungsversion und prüfen Sie den Kontext, bevor Sie etwas ändern.
>
> **Behebung:** Entfernen Sie die Datei, sofern Sie nicht genau wissen, warum sie existiert, und prüfen Sie dann das Upload-Formular, das sie angenommen hat.
>
> **Wiederholung verhindern:** Halten Sie unterstützte Software aktuell und vergleichen Sie unerwartete Änderungen mit einem vertrauenswürdigen Ausgangsstand.

PHP-Code in einer Datei, die keine PHP-Datei ist (3)

Was das bedeutet: Eine Datei mit einer anderen Endung (zum Beispiel eine Bild-, Text- oder Icon-Datei) enthält PHP-Code. Bei einem falsch konfigurierten Server oder über eine Einbindung kann sie als Skript ausgeführt werden.

So beheben Sie es: Sehen Sie sich die Datei nur lesend an. Entfernen Sie sie, wenn es keine echte Datei dieses Typs ist, und suchen Sie nach Code, der sie einbindet.

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

Hoch | Mittlere Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Hoch | Mittlere Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Hoch | Mittlere Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

> ### KI-Einschätzung (unverbindlich) #1 - Wahrscheinlich harmlos
>
> **Erklärung:** Die ursprüngliche KI-Bewertung hielt diesen Fund im Anwendungskontext für wahrscheinlich harmlos. Diese Einschätzung beweist nicht, dass eine Datei sicher ist.
>
> **So überprüfen Sie es:** Vergleichen Sie die Datei mit einer vertrauenswürdigen Anwendungsversion und prüfen Sie den Kontext, bevor Sie etwas ändern.
>
> **Behebung:** Sehen Sie sich die Datei nur lesend an. Entfernen Sie sie, wenn es keine echte Datei dieses Typs ist, und suchen Sie nach Code, der sie einbindet.
>
> **Wiederholung verhindern:** Halten Sie unterstützte Software aktuell und vergleichen Sie unerwartete Änderungen mit einem vertrauenswürdigen Ausgangsstand.

Backup oder Archiv im öffentlichen Web-Ordner (6)

Was das bedeutet: Backups, Datenbank-Dumps oder Archive im öffentlichen Ordner können oft von jedem heruntergeladen werden, der den Namen errät.

So beheben Sie es: Verschieben Sie Backups aus dem öffentlichen Ordner und löschen Sie Kopien, die Sie nicht mehr benötigen.

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

Mittel | Mittlere Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Mittel | Mittlere Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Mittel | Mittlere Zuverlässigkeit | Offen | Muss untersucht werden (KI-Einschätzung (unverbindlich) #2)

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

Mittel | Mittlere Zuverlässigkeit | Offen | Muss untersucht werden (KI-Einschätzung (unverbindlich) #2)

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

Mittel | Mittlere Zuverlässigkeit | Offen | Muss untersucht werden (KI-Einschätzung (unverbindlich) #2)

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

Mittel | Mittlere Zuverlässigkeit | Offen | Muss untersucht werden (KI-Einschätzung (unverbindlich) #2)

> ### KI-Einschätzung (unverbindlich) #1 - Wahrscheinlich harmlos
>
> **Erklärung:** Die ursprüngliche KI-Bewertung hielt diesen Fund im Anwendungskontext für wahrscheinlich harmlos. Diese Einschätzung beweist nicht, dass eine Datei sicher ist.
>
> **So überprüfen Sie es:** Vergleichen Sie die Datei mit einer vertrauenswürdigen Anwendungsversion und prüfen Sie den Kontext, bevor Sie etwas ändern.
>
> **Behebung:** Verschieben Sie Backups aus dem öffentlichen Ordner und löschen Sie Kopien, die Sie nicht mehr benötigen.
>
> **Wiederholung verhindern:** Halten Sie unterstützte Software aktuell und vergleichen Sie unerwartete Änderungen mit einem vertrauenswürdigen Ausgangsstand.

> ### KI-Einschätzung (unverbindlich) #2 - Muss untersucht werden
>
> **Erklärung:** Die ursprüngliche KI-Bewertung konnte nicht feststellen, ob dies erwartet war. Prüfen Sie die Belege und den Anwendungskontext.
>
> **So überprüfen Sie es:** Vergleichen Sie die Datei mit einer vertrauenswürdigen Anwendungsversion und prüfen Sie den Kontext, bevor Sie etwas ändern.
>
> **Behebung:** Verschieben Sie Backups aus dem öffentlichen Ordner und löschen Sie Kopien, die Sie nicht mehr benötigen.
>
> **Wiederholung verhindern:** Halten Sie unterstützte Software aktuell und vergleichen Sie unerwartete Änderungen mit einem vertrauenswürdigen Ausgangsstand.

Entwickler-Fehlerseitenpaket installiert (1)

Was das bedeutet: Ein Fehlerseitenpaket für die Entwicklung (etwa Laravel Ignition) ist installiert. Ältere Versionen hatten schwere Sicherheitslücken, und Debug-Seiten geben Details preis.

So beheben Sie es: Installieren Sie nur Produktionsabhängigkeiten (composer install --no-dev) oder aktualisieren Sie das Paket, und lassen Sie den Debug-Modus ausgeschaltet.

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

Mittel | Mittlere Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

> ### KI-Einschätzung (unverbindlich) #1 - Wahrscheinlich harmlos
>
> **Erklärung:** Die ursprüngliche KI-Bewertung hielt diesen Fund im Anwendungskontext für wahrscheinlich harmlos. Diese Einschätzung beweist nicht, dass eine Datei sicher ist.
>
> **So überprüfen Sie es:** Vergleichen Sie die Datei mit einer vertrauenswürdigen Anwendungsversion und prüfen Sie den Kontext, bevor Sie etwas ändern.
>
> **Behebung:** Installieren Sie nur Produktionsabhängigkeiten (composer install --no-dev) oder aktualisieren Sie das Paket, und lassen Sie den Debug-Modus ausgeschaltet.
>
> **Wiederholung verhindern:** Halten Sie unterstützte Software aktuell und vergleichen Sie unerwartete Änderungen mit einem vertrauenswürdigen Ausgangsstand.

Laufendes Programm, dessen Datei gelöscht wurde (1)

Was das bedeutet: Ein Prozess dieses Kontos läuft aus einer Datei, die nicht mehr existiert. Software-Updates können das verursachen, aber Schadsoftware löscht sich auch nach dem Start selbst.

So beheben Sie es: Identifizieren Sie den Prozess mit ps und beenden Sie ihn, wenn Sie ihn nicht kennen.

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

Mittel | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

> ### KI-Einschätzung (unverbindlich) #1 - Wahrscheinlich harmlos
>
> **Erklärung:** Die ursprüngliche KI-Bewertung hielt diesen Fund im Anwendungskontext für wahrscheinlich harmlos. Diese Einschätzung beweist nicht, dass eine Datei sicher ist.
>
> **So überprüfen Sie es:** Vergleichen Sie die Datei mit einer vertrauenswürdigen Anwendungsversion und prüfen Sie den Kontext, bevor Sie etwas ändern.
>
> **Behebung:** Identifizieren Sie den Prozess mit ps und beenden Sie ihn, wenn Sie ihn nicht kennen.
>
> **Wiederholung verhindern:** Halten Sie unterstützte Software aktuell und vergleichen Sie unerwartete Änderungen mit einem vertrauenswürdigen Ausgangsstand.

Die Zeitstempel der Datei wirken verändert (153)

Was das bedeutet: Die Statusänderungszeit der Datei (ctime) ist deutlich neuer als ihre Änderungszeit (mtime). Angreifer stellen Änderungsdaten oft zurück, damit eine abgelegte Datei zwischen älteren Dateien nicht auffällt; auch Wiederherstellungen und manche Deployment-Werkzeuge können das verursachen.

So beheben Sie es: Prüfen Sie, wer die Datei wann geändert hat. Wenn niemand auf Ihrer Seite das war, prüfen Sie den Inhalt der Datei.

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

> ### KI-Einschätzung (unverbindlich) #1 - Wahrscheinlich harmlos
>
> **Erklärung:** Die ursprüngliche KI-Bewertung hielt diesen Fund im Anwendungskontext für wahrscheinlich harmlos. Diese Einschätzung beweist nicht, dass eine Datei sicher ist.
>
> **So überprüfen Sie es:** Vergleichen Sie die Datei mit einer vertrauenswürdigen Anwendungsversion und prüfen Sie den Kontext, bevor Sie etwas ändern.
>
> **Behebung:** Prüfen Sie, wer die Datei wann geändert hat. Wenn niemand auf Ihrer Seite das war, prüfen Sie den Inhalt der Datei.
>
> **Wiederholung verhindern:** Halten Sie unterstützte Software aktuell und vergleichen Sie unerwartete Änderungen mit einem vertrauenswürdigen Ausgangsstand.

Anfragen mit angriffsähnlichen Daten (27)

Was das bedeutet: Ihre Zugriffsprotokolle enthalten Anfragen mit typischen Angriffsdaten. Die meisten sind automatisierte Versuche, die scheitern; sie werden zur Einordnung aufgeführt.

So beheben Sie es: Es ist nichts zu tun, sofern keine passenden Anfragen erfolgreich waren. Halten Sie Ihre Software aktuell.

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Ignoriert | Wahrscheinlich harmlos (KI-Einschätzung (unverbindlich) #1)

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

Niedrig | Geringe Zuverlässigkeit | Offen

> ### KI-Einschätzung (unverbindlich) #1 - Wahrscheinlich harmlos
>
> **Erklärung:** Die ursprüngliche KI-Bewertung hielt diesen Fund im Anwendungskontext für wahrscheinlich harmlos. Diese Einschätzung beweist nicht, dass eine Datei sicher ist.
>
> **So überprüfen Sie es:** Vergleichen Sie die Datei mit einer vertrauenswürdigen Anwendungsversion und prüfen Sie den Kontext, bevor Sie etwas ändern.
>
> **Behebung:** Es ist nichts zu tun, sofern keine passenden Anfragen erfolgreich waren. Halten Sie Ihre Software aktuell.
>
> **Wiederholung verhindern:** Halten Sie unterstützte Software aktuell und vergleichen Sie unerwartete Änderungen mit einem vertrauenswürdigen Ausgangsstand.

Stark verschleierter Code (4)

Was das bedeutet: Die Datei enthält lange kodierte Zeichenketten, Zeichen für Zeichen zusammengesetzten Text oder eine ähnliche Verschleierung. Das kann der Kopierschutz eines kostenpflichtigen Plugins sein oder Schadsoftware, die ihren Zweck verbirgt.

So beheben Sie es: Vergleichen Sie die Datei mit der Kopie des Herstellers. Unbekannte verschleierte Dateien in einem Website-Ordner sollte jemand prüfen, der die Anwendung kennt.

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

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

Niedrig | Geringe Zuverlässigkeit | Offen

Älteres PHP installiert, von Ihren Websites nicht genutzt (6)

Was das bedeutet: Dieses PHP wird nicht mehr unterstützt, ist älter als die PHP2Shell-Korrektur oder seine Korrektur konnte nicht bestätigt werden, aber nichts in diesem Konto nutzt es: kein PHP-FPM-Pool, kein laufender Prozess, kein php-Befehl und keine geplante Aufgabe. Bei der aktuellen Konfiguration kann es Ihre Websites nicht ausliefern, daher erhält es den Schweregrad Niedrig. Ein anderes Konto auf demselben Server könnte es trotzdem noch nutzen.

So beheben Sie es: Entfernen Sie es, wenn es nicht gebraucht wird (Ihr Hosting-Anbieter oder Ihr Control Panel kann eine PHP-Version deinstallieren), und stellen Sie keine Website darauf um.

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

Niedrig | Mittlere Zuverlässigkeit | Offen

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

Niedrig | Mittlere Zuverlässigkeit | Offen

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

Niedrig | Mittlere Zuverlässigkeit | Offen

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

Niedrig | Mittlere Zuverlässigkeit | Offen

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

Niedrig | Mittlere Zuverlässigkeit | Offen

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

Niedrig | Mittlere Zuverlässigkeit | Offen

Die Upload-Fortschrittsverfolgung von PHP ist eingeschaltet (1)

Was das bedeutet: session.upload_progress.enabled ist eingeschaltet. Die PHP2Shell-Probleme betreffen diese Funktion; wenn Sie sie nicht nutzen, verringert das Ausschalten die Angriffsfläche.

So beheben Sie es: Setzen Sie session.upload_progress.enabled = Off in php.ini oder .user.ini, wenn Ihre Websites keinen Upload-Fortschritt anzeigen.

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

Niedrig | Mittlere Zuverlässigkeit | Offen

PHP enthält die PHP2Shell-Korrektur (8)

Was das bedeutet: Dieses PHP hat die korrigierte Version oder eine neuere, oder das Paket des Anbieters bestätigt die Korrektur.

So beheben Sie es: Für dieses PHP ist in Bezug auf PHP2Shell nichts zu tun.

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

Informativ | Hohe Zuverlässigkeit | Offen

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

Informativ | Hohe Zuverlässigkeit | Offen

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

Informativ | Hohe Zuverlässigkeit | Offen

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

Informativ | Hohe Zuverlässigkeit | Offen

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

Informativ | Hohe Zuverlässigkeit | Offen

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

Informativ | Hohe Zuverlässigkeit | Offen

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

Informativ | Hohe Zuverlässigkeit | Offen

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

Informativ | Hohe Zuverlässigkeit | Offen