DAVINCI
RECHENZENTRUM

KOSTENLOSES PRÜFWERKZEUG · VERSION 1.1

Spurensuche nach einem Vorfall

Anleitung zur Prüfung eines Linux- oder Windows-Servers auf die Spuren, die nach einem erfolgreichen Angriff auf PHP zurückbleiben.

Verändert nichts

Keine Datei wird gelöscht, verschoben oder repariert. Nur Lesezugriffe.

Sendet nichts

Keine Netzwerkverbindung, kein Rückkanal. Der Bericht bleibt auf Ihrem Server.

Verspricht nichts

Ein leerer Befund ist kein Freispruch. Die Grenzen stehen in jedem Bericht.

DAVINCI Rechenzentrum GmbH · Mannheim · davinci-rechenzentrum.de/php-spurensuche
Stand 22. Oktober 2026 · Frei verwendbar, auch gewerblich · Ohne Gewähr

1 Worum es geht

Der Patch ist eingespielt, die Seite läuft wieder. Offen bleibt die Frage, die sich von außen nicht beantworten lässt: War vorher schon jemand da?

Dieses Werkzeug sucht auf Ihrem Server nach den Spuren, die ein erfolgreicher Angriff üblicherweise hinterlässt. Es ist ein einzelnes PHP-Skript — kein Installationsprogramm, keine ausführbare Datei. Das hat einen Grund: Wir bitten Sie, auf einem möglicherweise betroffenen System etwas mit hohen Rechten zu starten. Also bekommen Sie etwas, das Sie vorher lesen können.

> **Es räumt bewusst nicht auf.** Nach einem Vorfall entscheidet eine einzige Frage über alles Weitere: seit wann? Erst die Antwort darauf sagt Ihnen, welche Datensicherung noch sauber ist — und sie steckt in den Zeitstempeln der gefundenen Dateien und in den Protokollen. Wer zuerst löscht, vernichtet genau das.

Voraussetzungen

Betriebssystem	Linux oder Windows Server
PHP	Version 7.4 oder neuer, auf der Kommandozeile erreichbar
Rechte	Administrator beziehungsweise root — ohne sie bleiben Aufgabenplanung, Autostarts und Protokolle unlesbar
Dauer	Zehn Sekunden bis drei Minuten, je nach Größe der Installation

2 Was geprüft wird

Zwölf Bereiche. Jeder Befund erscheint im Bericht mit Fundort, Zeitstempel und einer Einordnung, was er bedeutet.

BEREICH	GEPRÜFT WIRD
PHP-Fassung	Vergleicht die laufende Unterversion mit der, in der PHP2Shell geschlossen ist: 8.5.12, 8.4.27, 8.3.36, 8.2.35. Bei Linux-Rückportierungen (Debian, Ubuntu, Alma, RHEL) wird zusätzlich der Paketstand abgefragt — dort bleibt die Nummer trotz Korrektur alt.
Seit dem Stichtag geändert	Alle ausführbaren Dateien, die seit dem 17.10.2026 angefasst wurden, mit Zeitstempel. Der wertvollste Einzelbefund: Was nicht zu einer Veröffentlichung oder einem Update gehört, ist erklärungsbedürftig.
wp-content/mu-plugins	Dateien dort werden bei jedem Aufruf geladen, ohne in der Pluginliste zu erscheinen oder aktiviert zu sein.
Abstürze des PHP-Arbeiters	Speicherfehler (SIGSEGV, Signal 11) im PHP-FPM- und Systemprotokoll — ein beschriebenes Anzeichen, wenn sie sich häufen.
Verbindungen nach außen	Bestehende Verbindungen auf ungewöhnlichen Anschlüssen. Eine Gegenverbindung lauscht nicht, sie meldet sich — und fällt in Anschlusslisten deshalb nicht auf.
PHP-Einstellungen	auto_prepend_file und auto_append_file laden bei jedem Aufruf eine Datei mit, ohne dass im Webverzeichnis etwas auffällt. Dazu allow_url_include und leeres disable_functions.
Code im Webverzeichnis	Sucht die Kombination aus einer Ausführungsfunktion und einer Benutzereingabe im selben Ausdruck — das Kennzeichen jeder Webshell.
PHP an Datenorten	Eine PHP-Datei in wp-content/uploads, typo3temp oder var/cache gehört dort nicht hin. Einer der verlässlichsten Hinweise überhaupt.
Doppelte Endungen	bild.jpg.php und shell.php.jpg dienen dazu, Upload-Prüfungen zu umgehen.
.htaccess / .user.ini	Einträge, die harmlose Endungen ausführbar machen oder bei jedem Aufruf fremden Code laden.
Geplante Aufgaben	Linux: crontab, /etc/cron.d, systemd-Dienste, rc.local, ld.so.preload. Windows: Aufgabenplanung und Autostart-Schlüssel der Registry.
Zugänge	Hinterlegte SSH-Schlüssel, Konten mit Anmeldemöglichkeit, unter Windows die Mitglieder der Administratorgruppe.
Lauschende Dienste	Anschlüsse jenseits der erwarteten, auf denen etwas auf Verbindungen wartet.

BEREICH	GEPRÜFT WIRD
Zugriffsprotokolle	Erfolgreiche Aufrufe typischer Hintertür-Namen und POST-Anfragen an Bilddateien. Abgewehrte Versuche werden getrennt gezählt, Serverfehler (5xx) nach Multipart-Anfragen gesondert gemeldet. Rotierte und gepackte Protokolle werden mitgelesen.
Zeitstempel	Änderungszeiten, die in der Zukunft liegen — ein Zeichen für nachträglich gesetzte Stempel.
Rückreichweite	Wie weit Ihre Protokolle zurückgehen. Unter 30 Tagen wird die Aufarbeitung eines Vorfalls schwierig.

3 Schritt für Schritt

Sie brauchen keine Programmierkenntnisse, nur Zugang zum Server.

1 Prüfen, ob PHP auf der Kommandozeile läuft

Es muss eine Versionsnummer erscheinen, etwa `PHP 8.2.35 (cli)`. Kommt stattdessen eine Fehlermeldung, suchen Sie die Datei — unter Windows liegt sie häufig unter `C:\php\php.exe` und muss dann überall mit vollem Pfad angegeben werden.

```
php -v
```

2 Die Datei ablegen — aber nicht ins Webverzeichnis

Das Skript weigert sich zwar, über einen Browser zu starten. Trotzdem gehört eine solche Datei nicht dorthin, wo das Internet sie erreicht.

```
Linux     /root/davinci-spurensuche.php
Windows   C:\Temp\davinci-spurensuche.php
```

3 Starten und den Bericht mitschreiben lassen

Den Pfad hinter `--pfad` durch Ihr Webverzeichnis ersetzen. Kennen Sie es nicht, lassen Sie den Teil weg — dann wird an den üblichen Stellen gesucht.

```
Linux
sudo php /root/davinci-spurensuche.php \
     --pfad /var/www/html \
     --bericht /root/bericht.txt

Windows (Eingabeaufforderung als Administrator)
C:\php\php.exe C:\Temp\davinci-spurensuche.php ^
     --pfad C:\inetpub\wwwroot\ihre-seite.de ^
     --bericht C:\Temp\bericht.txt
```

4 Den Bericht öffnen

Die Datei `bericht.txt` lässt sich mit jedem Texteditor lesen. Zusätzlich gibt es `--json` für die maschinelle Weiterverarbeitung.

4 Das Ergebnis lesen

Drei Stufen, von oben nach unten sortiert. Die oberste wird sparsam vergeben.

[!]

Sollte so nicht sein

Hier fällt uns keine harmlose Erklärung ein. Gehört heute angesehen, nicht nächste Woche.

[?]

Bitte ansehen

Kann harmlos sein und ist es meistens. Baukästen erzeugen solche Muster regelmäßig.

[i]

Information

Kein Verdacht. Steht da, damit Sie den Zustand kennen.

Am Ende jedes Berichts steht ein Abschnitt **Nicht geprüft**. Er listet auf, woran das Werkzeug nicht herankam. Diese Punkte sind weder in Ordnung noch auffällig — sie sind offen. Bitte nicht überspringen.

Wenn Sie einen roten Befund haben: löschen Sie nichts.

Das ist der häufigste und teuerste Fehler. Eine entfernte Hintertür bei offener Lücke ist am nächsten Tag wieder da — dann allerdings ohne die Spur, an der sich der Zeitraum hätte ablesen lassen.

Die richtige Reihenfolge: **1.** Bericht sichern. **2.** Zugriffsprotokolle wegkopieren, bevor sie rotieren. **3.** Eine Sicherung des aktuellen Zustands anlegen, auch des befallenen — man braucht sie später. **4.** Erst danach entscheiden, was entfernt wird.

5 Grenzen und häufige Fragen

Darüber schreiben wir lieber zu viel als zu wenig.

Kein Freispruch	Geprüft wird auf die gängigsten Varianten solcher Angriffe. Wer sich Mühe gibt, hinterlässt keine davon.
Läuft im System	Das Skript läuft auf dem Server, den es prüfen soll. Wer dort genug Rechte hat, um sich einzunisten, hat auch genug, um ein Werkzeug zu täuschen. Belastbar ist nur eine Prüfung von außen oder an einem abgezogenen Abbild.
Ohne Datenbank	Neu angelegte Redakteurskonten, manipulierte Inhalte und Einträge in Erweiterungstabellen bleiben unsichtbar.
Kein Freispruch bei Datenabfluss	Bei dieser Art von Fehler kann Arbeitsspeicher eines PHP-Prozesses nach außen gelangen, ohne dass Code ausgeführt oder eine Datei verändert wird. Dafür gibt es auf dem System keine Spur, die dieses Werkzeug finden könnte.
Versionsliste altert	Die hinterlegten Fassungen tragen ein Datum. Ist es älter als 90 Tage, sagt der Bericht das — über Lücken, die danach bekannt wurden, kann er nichts wissen.
Ohne Gewähr	Frei verwendbar, auch gewerblich. Eine Haftung für Vollständigkeit oder Richtigkeit der Befunde übernehmen wir nicht.

Änderungen in dieser Fassung

Version 1.1 · 22. Oktober 2026. Versionsliste auf den Stand vom 21.10.2026 (8.5.12, 8.4.27, 8.3.36, 8.2.35). Rückportierungen bei Debian, Ubuntu, Alma und RHEL werden erkannt. IIS-Standardprotokolle sowie rotierte und gepackte Protokolle werden ausgewertet, Serverfehler nach Multipart-Anfragen gesondert gemeldet. Neu hinzugekommen sind die Liste der seit dem Stichtag geänderten Dateien, `mu-plugins`, Abstürze des PHP-Arbeiters und Verbindungen nach außen. Läuft ab PHP 7.4. Wer noch Version 1.0 einsetzt, sollte auf 1.1 wechseln.

Kann das Werkzeug meinen Server beschädigen?

Nein. Es öffnet Dateien ausschließlich zum Lesen. Die einzige Datei, die es schreibt, ist der Bericht — und nur, wenn Sie ihn mit `--bericht` anfordern.

Werden Daten an DAVINCI übertragen?

Nein. Im Quelltext steht keine einzige Netzwerkfunktion. Sie dürfen das vor dem Start nachsehen; genau dafür geben wir den Quelltext lesbar heraus.

Warum bekomme ich gelbe Treffer, obwohl nichts passiert ist?

Weil WordPress, TYPO3 und ihre Erweiterungen Techniken verwenden, die auch in Schadcode vorkommen. Genau deshalb sind diese Treffer gelb und nicht rot.

Es meldet abgewehrte Zugriffsversuche. Bin ich angegriffen worden?

Versucht ja, erfolgreich nein. Jeder öffentlich erreichbare Server wird rund um die Uhr abgesucht. Abgewehrt heißt: Es gab nichts zu finden.

Läuft es auch bei geteiltem Webspace?

Nur eingeschränkt — dort fehlt meist der Kommandozeilenzugang. Viele Anbieter richten SSH auf Anfrage ein.

Reicht das als Nachweis für Versicherung oder Aufsicht?

Nein. Der Bericht ist ein Ausgangspunkt, keine forensische Untersuchung. Dafür braucht es eine Prüfung an einem gesicherten Abbild.

Prüfsumme der Programmdatei (SHA-256)

Damit lässt sich feststellen, ob eine weitergereichte Datei noch die Originalfassung ist. Hier steht bewusst nur die Prüfsumme von `davinci-spurensuche.php`: Die des ZIP-Pakets kann nicht in der PDF stehen, weil die PDF selbst darin liegt. Sie finden sie auf davinci-rechenzentrum.de/php-spurensuche.

```
davinci-spurensuche.php  c0ada23fbc347bd9f4758129ead362c0d2168e6caa3ade7b312478b7f190332c
```

Einen roten Befund im Bericht?

Schicken Sie uns den Bericht. Wir sehen ihn uns an und sagen Ihnen, was er bedeutet — auch dann, wenn die Antwort lautet, dass nichts passiert ist.

post@davinci-rechenzentrum.de · +49 621 877 55 990
davinci-rechenzentrum.de/php-spurensuche