Malware & server vulnerability report

Malware & server vulnerability example report

Report generated: 25 Nov 2026, 13:11

> Names, filenames and directory layouts in this public example are fictional. Source code, request data, customer notes and identifiers have been removed. Advisory wording has been rewritten; the finding counts, assessments and review outcomes are preserved.

Current outcome

Medium

Findings: 213 | Need attention: 137 | Likely harmless: 0 | Resolved, accepted or ignored: 76

Risk reflects findings needing attention. AI assessments of likely harmless findings are counted separately.

Severity	Original findings	Needing attention
Critical	0	0
High	6	0
Medium	8	4
Low	191	125
Informational	8	8

Summary

This real scan found 213 items. After review, 137 still need attention: 4 medium, 125 low and 8 informational findings. The other 76 were resolved, accepted or ignored. The PHP runtimes in use include the PHP2Shell fix; unused older versions still need housekeeping.

Findings are indicators, not proof, and a scan only sees what this account can read. No scan can prove a server has not been compromised.

PHP2Shell

Fixed where it is used

The PHP your websites use includes the fix. Older PHP is installed but not used by this account: remove it when you can.

PHP	Version	Status	Fixed in	In use
/opt/example-php/runtime-01/bin/php	8.2.35	Fixed	8.2.35	Yes
/opt/example-php/runtime-02/bin/php	7.4.33	Unsupported	-	No
/opt/example-php/runtime-03/bin/php	8.0.30	Unsupported	-	No
/opt/example-php/runtime-04/bin/php	8.1.34	Unsupported	-	No
/opt/example-php/runtime-05/bin/php	8.3.36	Fixed	8.3.36	No
/opt/example-php/runtime-06/bin/php	8.4.27	Fixed	8.4.27	No
/opt/example-php/runtime-07/bin/php	8.5.12	Fixed	8.5.12	No

PHP	Version	Status	Fixed in	In use
/opt/example-php/runtime-08/bin/php	7.4.33	Unsupported	-	No
/opt/example-php/runtime-09/bin/php	8.0.30	Unsupported	-	No
/opt/example-php/runtime-10/bin/php	8.1.34	Unsupported	-	No
/opt/example-php/runtime-11/bin/php	8.2.35	Fixed	8.2.35	Yes
/opt/example-php/runtime-12/bin/php	8.3.36	Fixed	8.3.36	No
/opt/example-php/runtime-13/bin/php	8.4.27	Fixed	8.4.27	No
/opt/example-php/runtime-14/bin/php	8.5.12	Fixed	8.5.12	No

In use: what this account's PHP-FPM pools, running processes, php command and scheduled tasks show. Another account on the same server may still use a PHP marked No.

Checks

Checks	Status
Server and operating system	Completed
Hosting panel	Completed
PHP versions	Completed
PHP packages	Completed
Distribution fixes for PHP2Shell	Completed
Websites and applications	Completed
Debug settings	Completed
Scheduled tasks	Completed
Shell start-up files	Completed
SSH keys	Completed
User services	Completed
Autostart entries	Completed
Preloaded libraries	Completed
Temporary folders	Completed
Running processes	Completed
Python start-up hooks	Completed
File inventory	Completed
PHP code patterns	Completed
Python code patterns	Completed
Scripts in the wrong place	Completed
Disguised file names	Completed
PHP hidden in other file types	Completed
Disguised code	Completed

Checks	Status
Server configuration files	Completed
Exposed files	Completed
File permissions	Completed
Altered file dates	Completed
Web access logs	Completed
Error logs	Completed
PHP2Shell assessment	Completed
PHP upload-progress setting	Completed

Findings (213)

File named like an image or document but runs as PHP (3)

What this means: The file name has two extensions (for example photo.jpg.php) or disguises a PHP file as media. This is a common way to slip a script past upload filters.

How to fix it: Remove the file unless you know exactly why it exists, then check the upload form that accepted it.

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

High | Medium confidence | Resolved | Suspicious (AI view (advisory) #1)

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

High | Medium confidence | Resolved | Suspicious (AI view (advisory) #1)

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

High | Medium confidence | Accepted risk | Needs investigation (AI view (advisory) #2)

> #### AI view (advisory) #1 - Suspicious
>
> **Explanation:** The original AI assessment found suspicious characteristics that warranted investigation. They do not by themselves establish compromise.
>
> **How to verify:** Check the file against the application's trusted release and review its context before changing anything.
>
> **Fix:** Remove the file unless you know exactly why it exists, then check the upload form that accepted it.
>
> **Prevent it happening again:** Keep supported software up to date and review unexpected changes against a trusted baseline.

> #### AI view (advisory) #2 - Needs investigation
>
> **Explanation:** The original AI assessment could not establish whether this was expected. Review the evidence and application context.
>
> **How to verify:** Check the file against the application's trusted release and review its context before changing anything.
>
> **Fix:** Remove the file unless you know exactly why it exists, then check the upload form that accepted it.
>
> **Prevent it happening again:** Keep supported software up to date and review unexpected changes against a trusted baseline.

PHP code inside a file that is not PHP (3)

What this means: A file with another extension (an image, text or icon file, for example) contains PHP code. With a misconfigured server or an include, it can be run as a script.

How to fix it: Look at the file read-only. Remove it if it is not a genuine file, and look for code that includes it.

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

High | Medium confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

High | Medium confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

High | Medium confidence | Ignored | Likely harmless (AI view (advisory) #1)

> ### AI view (advisory) #1 - Likely harmless
>
> **Explanation:** The original AI assessment considered this likely harmless in its application context. This is an advisory assessment, not proof that a file is safe.
>
> **How to verify:** Check the file against the application's trusted release and review its context before changing anything.
>
> **Fix:** Look at the file read-only. Remove it if it is not a genuine file, and look for code that includes it.
>
> **Prevent it happening again:** Keep supported software up to date and review unexpected changes against a trusted baseline.

Backup or archive in the public web folder (6)

What this means: Backups, database dumps or archives inside the public folder can often be downloaded by anyone who guesses the name.

How to fix it: Move backups outside the public folder and delete copies you no longer need.

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

Medium | Medium confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Medium | Medium confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Medium | Medium confidence | Open | Needs investigation (AI view (advisory) #2)

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

Medium | Medium confidence | Open | Needs investigation (AI view (advisory) #2)

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

Medium | Medium confidence | Open | Needs investigation (AI view (advisory) #2)

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

Medium | Medium confidence | Open | Needs investigation (AI view (advisory) #2)

> ### AI view (advisory) #1 - Likely harmless
>
> **Explanation:** The original AI assessment considered this likely harmless in its application context. This is an advisory assessment, not proof that a file is safe.
>
> **How to verify:** Check the file against the application's trusted release and review its context before changing anything.
>
> **Fix:** Move backups outside the public folder and delete copies you no longer need.
>
> **Prevent it happening again:** Keep supported software up to date and review unexpected changes against a trusted baseline.

> ### AI view (advisory) #2 - Needs investigation
>
> **Explanation:** The original AI assessment could not establish whether this was expected. Review the evidence and application context.

> **How to verify:** Check the file against the application's trusted release and review its context before changing anything.
>
> **Fix:** Move backups outside the public folder and delete copies you no longer need.
>
> **Prevent it happening again:** Keep supported software up to date and review unexpected changes against a trusted baseline.

Developer error-page package installed (1)

What this means: A development error-page package (such as Laravel Ignition) is installed. Older versions had serious flaws, and debug pages leak details.

How to fix it: Install production dependencies only (composer install --no-dev) or update the package, and keep debug mode off.

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

Medium | Medium confidence | Ignored | Likely harmless (AI view (advisory) #1)

> ### AI view (advisory) #1 - Likely harmless
>
> **Explanation:** The original AI assessment considered this likely harmless in its application context. This is an advisory assessment, not proof that a file is safe.
>
> **How to verify:** Check the file against the application's trusted release and review its context before changing anything.
>
> **Fix:** Install production dependencies only (composer install --no-dev) or update the package, and keep debug mode off.
>
> **Prevent it happening again:** Keep supported software up to date and review unexpected changes against a trusted baseline.

Running program whose file was deleted (1)

What this means: A process owned by this account is running from a file that no longer exists. Software updates can cause this, but malware also deletes itself after starting.

How to fix it: Identify the process with ps and stop it if you do not recognise it.

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

Medium | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

> ### AI view (advisory) #1 - Likely harmless
>
> **Explanation:** The original AI assessment considered this likely harmless in its application context. This is an advisory assessment, not proof that a file is safe.
>
> **How to verify:** Check the file against the application's trusted release and review its context before changing anything.
>
> **Fix:** Identify the process with ps and stop it if you do not recognise it.
>
> **Prevent it happening again:** Keep supported software up to date and review unexpected changes against a trusted baseline.

File dates look altered (153)

What this means: The file's change time is much newer than its modification time. Attackers often wind modification dates back so a planted file blends in with older ones; restores and some deployment tools can cause it too.

How to fix it: Check who changed the file and when. If nobody on your side did, review the file's contents.

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

Low | Low confidence | Open

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Open

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Open

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Open

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Open

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Open

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Open

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

> ### AI view (advisory) #1 - Likely harmless
>
> **Explanation:** The original AI assessment considered this likely harmless in its application context. This is an advisory assessment, not proof that a file is safe.
>
> **How to verify:** Check the file against the application's trusted release and review its context before changing anything.
>
> **Fix:** Check who changed the file and when. If nobody on your side did, review the file's contents.
>
> **Prevent it happening again:** Keep supported software up to date and review unexpected changes against a trusted baseline.

Requests carrying attack-like data (27)

What this means: Your access logs contain requests with typical attack payloads. Most are automated probes that fail; they are listed for context.

How to fix it: No action is needed unless matching requests succeeded. Keep your software up to date.

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Ignored | Likely harmless (AI view (advisory) #1)

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

Low | Low confidence | Open

> ### AI view (advisory) #1 - Likely harmless
>
> **Explanation:** The original AI assessment considered this likely harmless in its application context. This is an advisory assessment, not proof that a file is safe.
>
> **How to verify:** Check the file against the application's trusted release and review its context before changing anything.
>
> **Fix:** No action is needed unless matching requests succeeded. Keep your software up to date.
>
> **Prevent it happening again:** Keep supported software up to date and review unexpected changes against a trusted baseline.

Heavily disguised code (4)

What this means: The file contains long encoded strings, text built one character at a time, or similar disguise. It can be a paid plugin's copy protection, or malware hiding its purpose.

How to fix it: Compare the file with the vendor's copy. Unknown disguised files in a site folder should be reviewed by someone who knows the application.

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

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

Low | Low confidence | Open

Older PHP installed, not used by your websites (6)

What this means: This PHP is unsupported, older than the PHP2Shell fix, or its fix could not be confirmed, but nothing on this account uses it: no PHP-FPM pool, running process, php command or scheduled task. It cannot serve your websites as they are set up now, so it counts as low. Another account on the same server could still use it.

How to fix it: Remove it if nothing needs it (your host or control panel can uninstall a PHP version), and do not switch a website to it.

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

Low | Medium confidence | Open

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

Low | Medium confidence | Open

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

Low | Medium confidence | Open

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

Low | Medium confidence | Open

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

Low | Medium confidence | Open

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

Low | Medium confidence | Open

PHP upload-progress tracking is on (1)

What this means: session.upload_progress.enabled is on. The PHP2Shell issues involve this feature, so turning it off reduces exposure if you do not use it.

How to fix it: Set session.upload_progress.enabled = Off in php.ini or .user.ini if your sites do not show upload progress.

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

Low | Medium confidence | Open

PHP includes the PHP2Shell fix (8)

What this means: This PHP is at or above the fixed release, or its vendor package confirms the fix.

How to fix it: No PHP2Shell action is needed for this PHP.

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

Informational | High confidence | Open

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

Informational | High confidence | Open

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

Informational | High confidence | Open

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

Informational | High confidence | Open

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

Informational | High confidence | Open

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

Informational | High confidence | Open

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

Informational | High confidence | Open

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

Informational | High confidence | Open