

Website Scanner > Scans > Free Website Scanner Report (Light)

Website Scanner (Light)

Target
https://warthunder.com/en

[Download report](#)

Scan finished
Your scan for https://warthunder.com/en has finished successfully.

+ New scan | Rescan | Report incorrect result

[Summary](#) [Findings](#) [Performed Tests](#) [Scan Parameters](#)

Summary

Overall risk level

0 Critical	1 High	2 Medium	5 Low	31 Info
------------	--------	----------	-------	---------

Start time: Oct 31, 2025 - 13:42 | Finish time: Oct 31, 2025 - 13:43 | Scan duration: 50 seconds | Tests performed: 39/39

Evidence

CVE	CVSS	EPSS Score	EPSS Percentile	Summary
CVE-2024-8932	9.8	0.00637	0.69674	In PHP versions 8.1.* before 8.1.31, 8.2.* before 8.2.26, 8.3.* before 8.3.14, uncontrolled long string inputs to ldap_escape() function on 32-bit systems can cause an integer overflow, resulting in an out-of-bounds write.
CVE-2024-11236	9.8	0.0114	0.7773	In PHP versions 8.1.* before 8.1.31, 8.2.* before 8.2.26, 8.3.* before 8.3.14, uncontrolled long string inputs to ldap_escape() function on 32-bit systems can cause an integer overflow, resulting in an out-of-bounds write.
CVE-2024-8926	8.1	0.0444	0.88524	In PHP versions 8.1.* before 8.1.30, 8.2.* before 8.2.24, 8.3.* before 8.3.12, when using a certain non-standard configurations of Windows codepages, the fixes for CVE-2024-4577 https://github.com/advisories/GHSA-vxpp-6299-mwx3 may still be bypassed and the same command injection related to Windows "Best Fit" codepage behavior can be achieved. This may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.
CVE-2024-8927	7.5	0.00121	0.31991	In PHP versions 8.1.* before 8.1.30, 8.2.* before 8.2.24, 8.3.* before 8.3.12, HTTP_REDIRECT_STATUS variable is used to check whether or not CGI binary is being run by the HTTP server. However, in certain scenarios, the content of this variable can be controlled by the request submitter via HTTP headers, which can lead to cgi.force_redirect option not being correctly applied. In certain configurations this may lead to arbitrary file inclusion in PHP.
CVE-2025-1861	6.3	0.0016	0.375	In PHP from 8.1.* before 8.1.32, from 8.2.* before 8.2.28, from 8.3.* before 8.3.19, from 8.4.* before 8.4.5, when parsing HTTP redirect in the response to an HTTP request, there is currently limit on the location value size caused by limited size of the location buffer to 1024. However as per RFC910, the limit is recommended to be 8000. This may lead to incorrect URL truncation and redirecting to a wrong location.

+ Details

0/2 daily free scans available | Ctrl + I | ^

Recommended steps to help address [CVE-2025-1861](#).

Upgrade the PH. An effective solution is to upgrade to a patched version of PHP. Some versions you'd consider are: PHP 8.1.32, PHP 8.2.28, PHP 8.3.19, and PHP 8.4.5. Another step you could add is to implement an alternative HTTP client mechanism, if possible, using an alternative HTTP client that correctly implements RFC-9110, for example, the cURL extension is a good option.