

php-debugbar

github.com/php-debugbar/php-debugbar

Scanned 29 October 2026 at 09:49 · Report generated 29 October 2026 · PHP · 4,381 stars

OVERALL ASSESSMENT

Medium

Combined score 66 · 45 findings after filtering

Summary

33 findings likely need attention, 11 look like noise. Most notable: This Node.js version file pins a runtime that is affected by CVE-2026-111497 (Brotli de... (95% confidence).

Generated from finding counts. A plain-English summary was not available for this scan.

Risk, by type

MalDet scores two different questions separately, because they call for different responses: code can be badly written without being hostile, and hostile code is not always badly written.

VULNERABILITY

Medium (63)

Insecure coding an attacker could exploit. Usually mistakes, and usually fixable in place.

MALICIOUS PATTERN

Low (3)

Signs the code may be trying to do harm: hidden payloads, credential access, persistence, exfiltration.

What each detector found

DETECTOR	LOOKS FOR	HIGH	MEDIUM	LOW	TOTAL
semgrep	Insecure coding patterns across many languages	1	34	0	35
dep_checker	Vulnerable, unpinned or typosquatted dependencies	0	0	9	9
guarddog	Malicious package and install-time behaviour	0	1	0	1

33 of 45 findings were rated more likely genuine than noise by the classifier.

Evidence

Identical findings are grouped, so a single rule firing many times takes one row. Ordered worst first. “Seen” is how many times that finding occurred.

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
HIGH	semgrep	This Node.js version file pins a runtime that is affected by CVE-2026-111497 (Brotli decoder out-of-bounds write, remote code execution) or a floating alias whose patch level cannot be verified. Pin to a fixed release 22.23.4, 24.22.1, 26.12.1 or later on the same line. Node.js 20 and older, 23 and	1	/.nvmrc:1
MEDIUM	semgrep	Found direct access to a PHP variable without HTML escaping inside an inline PHP statement setting data from `\$_REQUEST[...]`. When untrusted input can be used to tamper with a web page rendering, it can lead to a Cross-site scripting (XSS) vulnerability. XSS vulnerabilities occur when untrusted input	2	/demo/bootstrap.php:151
MEDIUM	guarddog	Detects unicode homoglyphs and uncommon characters used for obfuscation [threat-runtime-obfuscation-unicode]	1	/resources/widgets.js:872
MEDIUM	semgrep	Access-Control-Allow-Origin response header is set to "*". This will disable CORS Same Origin Policy restrictions.	1	/demo/ajax_corshp:4
MEDIUM	semgrep	GitHub Actions step uses a mutable tag or branch reference. Tags and branch names can be silently repointed by the action owner, enabling supply-chain attacks — as seen in the trivy-action and kics-github-action compromises. Pin the reference to a full 40-character commit SHA instead, e.g. `uses: ac	28	/.github/workflows/screenshots.yml:26
MEDIUM	semgrep	Possibility of prototype polluting function detected. By adding or modifying attributes of an object prototype, it is possible to create attributes that exist on every object, or replace critical attributes with malicious ones. This can be problematic if the software depends on existence or non-existence	1	/resources/debugbar.js:31
MEDIUM	semgrep	Using user input when deleting files with `unlink()` is potentially dangerous. A malicious actor could use this to modify or access files they have no right to.	2	/src/Storage/FileStorage.php:163

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: '@antfu/eslint-config^6.7.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@eslint/js^9.39.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@sqltools/formatter^1.2.5' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@tabler/icons^3.36.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'esbuild^0.27.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'eslint-plugin-jquery^1.5.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'eslint^9.39.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'globals^16.5.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'highlight.js^11.11.1' — attacker could push malicious update	1	package.json

How to read this report

- **This is a static scan.** The code was read, never executed. Behaviour that only appears at runtime is outside what any of these detectors can see.
- **Findings are not all equally real.** A classifier rates each finding on how likely it is to be genuine rather than noise, and that rating weights the scores. Measured against a hand-reviewed sample it reached precision 0.52 and recall 0.62 — useful for ranking, not a verdict on any single finding.
- **A high score is not proof of malice.** Security tools, penetration-testing frameworks and malware research repositories contain the same patterns as real malware by design. The two risk types above exist to keep that distinction visible.
- **Absence of findings is not proof of safety.** A detector that is not installed, or a language none of them parse, produces silence rather than a warning.
- **This scan is a snapshot.** The repository may have changed since 29 October 2026.