

grab

github.com/Skidotus/grab

Scanned 29 October 2026 at 09:49 · Report generated 29 October 2026 · PHP · 1 stars

OVERALL ASSESSMENT

Medium

Combined score 75 · 24 findings after filtering

Summary

22 findings likely need attention, 2 look like noise. Most notable: User data flows into this manually-constructed SQL string. User data can be safely inse... (56% 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 (75)

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

MALICIOUS PATTERN

Safe (0)

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	4	18	0	22
dep_checker	Vulnerable, unpinned or typosquatted dependencies	0	0	2	2

22 of 24 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	User data flows into this manually-constructed SQL string. User data can be safely inserted into SQL strings using prepared statements or an object-relational mapper (ORM). Manually-constructed SQL strings is a possible indicator of SQL injection, which could let an attacker steal or manipulate data	4	/ accept.php :45
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	18	/ accept.php :88
LOW	dep_checker	Loose version constraint: '@tailwindcss/cli^4.1.15' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'tailwindcss^4.1.17' — 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.