

gatherpress

github.com/GatherPress/gatherpress

Scanned 24 September 2026 at 10:05 · Report generated 29 October 2026 · PHP · 137 stars

OVERALL ASSESSMENT

High

Combined score 223 · 174 findings after filtering

Summary

This repository has a high vulnerability score of 221.0, which means there are several dangerous coding patterns that an attacker could easily exploit to steal secrets or run malicious code. The most serious issues involve using variable interpolation in GitHub Actions workflows and executing non-constant commands, which allows attackers to inject their own scripts into the build process. While some findings appear to be intentional malicious behavior, the majority of the remaining 174 issues are likely ordinary insecure coding practices rather than signs of a hidden attack. The code also contains many packages with loose version constraints that could potentially receive harmful updates from third parties. Overall, while there is no evidence of deliberate sabotage, the presence of these vulnerabilities makes it unsafe to use without applying security patches or fixing the identified patterns.

Written by a language model running locally on the scanning machine, from the findings in this report. The risk levels above and below were decided by the scoring model, not by this summary.

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

High (221)

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

MALICIOUS PATTERN

Low (2)

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	9	112	0	121
dep_checker	Vulnerable, unpinned or typosquatted dependencies	0	0	53	53

117 of 174 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	Using variable interpolation `\${{...}}` with `github` context data in a `run:` step could allow an attacker to inject their own code into the runner. This would allow them to steal secrets and code. `github` context data can have arbitrary user input and should be treated as untrusted. Instead, use	5	/.github/workflows/screenshot-generation.yml:183
HIGH	semgrep	Executing non-constant commands. This can lead to command injection.	4	/.github/scripts/check-pr-coverage.php:90
MEDIUM	semgrep	Access-Control-Allow-Origin response header is set to "*". This will disable CORS Same Origin Policy restrictions.	1	/.gatherpress-org/playground-preview/plugin-proxy.php:250
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	110	/.github/workflows/compress-images.yml:41

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	semgrep	Detection of insertAdjacentHTML from non-constant definition. This can inadvertently expose users to cross-site scripting (XSS) attacks if this comes from user-provided input. If you have to use insertAdjacentHTML, consider using a sanitization library such as DOMPurify to sanitize your HTML.	1	/src/blocks/rsvp-template/view.js:121
LOW	dep_checker	package.json has a 'postinstall' script that runs automatically on npm install — worth a manual look: patch-package	1	package.json
LOW	dep_checker	Loose version constraint: '@wordpress/commands^1.41.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@wordpress/url^4.41.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'patch-package^8.0.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@wordpress/blocks^15.14.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@wordpress/api-fetch^7.41.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'html-react-parser^5.2.17' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@wordpress/html-entities^4.41.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@wordpress/core-data^7.41.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@wordpress/data^10.41.0' — attacker could push malicious update	1	package.json

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: '@testing-library/react^16.3.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@testing-library/jest-dom^6.9.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@wordpress/scripts^35.0.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'jest-sonar-reporter^2.0.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'leaflet-gesture-handling^1.2.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'leaflet^1.9.4' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'lodash^4.18.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'moment-timezone^0.6.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'dotenv^17.3.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'moment^2.30.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'playwright^1.58.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'prettier^3.8.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'rimraf^6.1.3' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'stylelint-config-recommended-scss^17.0.1' — attacker could push malicious update	1	package.json

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: 'stylelint-scss^7.3.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'stylelint^17.15.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'uuid^14.0.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'webpack-remove-empty-scripts^1.1.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@wordpress/element^6.41.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@jest/globals^30.2.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@playwright/test^1.58.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@wordpress/a11y^4.42.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@wordpress/block-editor^15.14.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@wordpress/components^32.3.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@wordpress/compose^7.41.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@wordpress/date^5.41.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@wordpress/dom-ready^4.41.0' — attacker could push malicious update	1	package.json

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: '@wordpress/dom^4.41.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@wordpress/e2e-test-utils-playwright^1.41.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@wordpress/editor^14.41.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'clsx^2.1.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@wordpress/env^11.13.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@wordpress/hooks^4.41.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@wordpress/i18n^6.14.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@wordpress/icons^11.8.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@wordpress/interactivity-router^2.41.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@wordpress/interactivity^6.41.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@wordpress/plugins^7.41.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@wordpress/rich-text^7.41.0' — attacker could push malicious update	1	package.json

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: '@anthropic-ai/claude-code^2.1.163' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@wp-playground/cli^3.1.44' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'classnames^2.5.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'stylelint-config-standard^40.0.0' — 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 24 September 2026.