

Poc-Monitor_v1.0.1

github.com/adminlove520/Poc-Monitor_v1.0.1

Scanned 29 July 2026 at 15:18 · Report generated 29 October 2026 · Go · 237 stars

This repository is no longer available on GitHub. It was deleted or made private after this scan, so these findings cannot be re-verified. Read them as a record of what the repository contained on 29 July 2026.

OVERALL ASSESSMENT

Low

Combined score 20 · 2 findings after filtering

Summary

The repository has been checked and found to have a very low overall risk score of 20.0, which means the code itself is safe from malicious intent and does not contain hidden traps or dangerous patterns. The only thing that was flagged is a Facebook OAuth detection issue, which appears twice in the code and is highly likely to be a mistake rather than a real security problem. This finding is considered ordinary insecure coding because it involves using an API incorrectly instead of being intentionally harmful, so it does not need to be fixed immediately. You can safely use this project for your work without worrying about malicious behavior or critical vulnerabilities.

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

Low (20)

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	2	0	0	2

2 of 2 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	Facebook OAuth detected	2	/dateLog/2023-01-10.json:1

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 July 2026.