Semgrep

Semgrep SAST Scan Report for Repository: local_scan/secrets-testing

Report Generated at 2024-09-04 21:52

SAST Scan Summary

Vulnerability Severity	Vulnerability Count
Findings- SAST High Severity	0
Findings- SAST Medium Severity	1
Findings- SAST Low Severity	2

Findings Summary- High Severity

Finding Title	Finding Description & Remediation	severity	status	ref	location

Findings Summary- Medium Severity

Finding Title	Finding Description & Remediation	severity	status	ref	location
symmetric-hardcoded-key	A secret is hard-coded in the application. Secrets stored in source code, such as credentials, identifiers, and other types of sensitive data, can be leaked and used by internal or external malicious actors. Use environment variables to securely provide credentials and other secrets or retrieve them from a secure vault or Hardware Security Module (HSM).	medium	open	secrets	cry.js#L2

Findings Summary- Low Severity

Finding Title	Finding Description & Remediation	severity	status	ref	location
express-check-csurf-middleware-usage	A CSRF middleware was not detected in your express application. Ensure you are either using one such as `csurf` or `csrf` (see rule references) and/or you are properly doing CSRF validation in your routes with a token or cookies.	low	open	secrets	server.js#L2
unsafe-formatstring	Detected string concatenation with a non-literal variable in a util.format / console.log function. If an attacker injects a format specifier in the string, it will forge the log message. Try to use constant values for the format string.	low	open	secrets	server.js#L10