ARCHITECTURE DECISION RECORD (ADR)

Decision Summary: CodeQL is established as a Software Factory Utility for Static Application Security Testing (SAST)

Approved by the VA Chief Architect (OIT/OCTO) on April 15, 2024

Context

Other Git-based configuration management tools that are TRM-approved have been evaluated, but it was determined by executive leadership that using GitHub.com and associated capabilities at the enterprise level was the best path forward for achieving standardization for configuration management and using scanning tools like CodeQL in a standardized way.

Decision

VA has made the strategic decision to adopt CodeQL as its standard Static Application Security Testing (SAST) tool for all GitHub.com repositories. It is also adopted as a Software Factory Utility for SAST. Development teams can pull a request against their repository's default branch, an automated check will occur to validate they are using CodeQL. If this check passes, the request will be marked as passed and can merge the code once all other checks have finished successfully.

AES has successfully completed the enablement of CodeQL enforcement for Code Scanning on GitHub.com repositories. Currently 98% of the repositories have the CodeQL Static Application Security Testing (SAST) tool enabled, while GitHub is doing manual configurations for the remaining 2% of the repositories.

This guidance requires Development teams to ensure repositories in which Critical vulnerabilities have been identified, are being remediated regardless of which tool identified the vulnerability. This process prevents code changes when a Critical vulnerability has been open for more than 30 days against the repository, and this policy will be enforced during the pull request process. It also uses Secure scanning enabled along with dependency analysis using a tool called Dependabot.

These features are already enabled on 100% of the GitHub.com repositories, and they are mandated for use along with Code Scanning done with CodeQL.

Rationale

CodeQL is a Static Application Security Testing (SAST) tool that is part of the native suite of tools available in GitHub Advanced Security. CodeQL analyzes application source code for vulnerabilities, making it susceptible to attack and helps developers understand how to remediate these vulnerabilities. CodeQL is deeply integrated in GitHub development processes and implements a system for providing continuous, real-time feedback to developers on vulnerabilities in their application source code.

The use of CodeQL for SAST arose from the detection of PII appearing as EI/CI + DOB in the testing code base repositories that have been utilized across the va.gov codebase for many years.

Tech Tuesday related to this topic:
https://dvagov.sharepoint.com/sites/oitdigitaltransformation/SitePages/TT32-Github-CodeQL.aspx

Impact(s)

All GitHub.com repositories (over 4000) have CodeQL enabled and will lead to much improved vulnerability identification and remediation. As CodeQL enforcement becomes officially mandated, we will coordinate with OIS to go from 30-day critical issues to zero days. This will be an enforcement of security code, code scanning for security vulnerabilities on GitHub repos. It could also be expanded to secret and PII scanning.

For questions or further clarification, contact the Enterprise Architecture team at ea@va.gov.

BASSAM KALDAWI

Digitally signed by BASSAM KALDAWI
Date: 2025.07.21 06:39:00 -07'00'

Sam Kaldawi
Chief Architect
Office of the Chief Technology Officer (OCTO)