OFFICE OF INFORMATION SECURITY

PASS: This application has successfully completed the V&V Quality Code Review Validation Process.

Quality Code Review Validation Report

TAS API v01.00.65

Application-ID: 131EE542-0112-4831-8DC0-F8C0FAAB2145

Filename: VA SwA Quality Code Validation TAS API v01.00.65 2019-04-25 PASS.pdf

APRIL 25, 2019

U.S. Department of Veterans Affairs

Office of Information and Technology

Software Assurance Program Office

Table of Contents

1 Quality Code Review Validation Report Introduction

This document contains the results of the validation by the VA Software Assurance Program Office of a quality code review of TAS API performed by the developer.

This document contains the following additional sections:

Section 2. Quality Code Review Validation Results

This section summarizes the results of the validation of the developer quality code review.

Section 3. Quality Code Review Validation Process Details

This section describes how the validation of the developer quality code review was performed.

Section 4. Quality Code Review Validation Findings and Recommendations

This section provides residual quality code review validation findings that should have already been fixed prior to the validation. Recommendations are also provided.

Section 5. Quality Code Review Validation Report Conclusion

This section provides additional recommendations to build quality in during development.

1.1 Application Information

The version of TAS API for which static analysis tool scan results were provided was v01.00.65. The following was provided by the developer for review:

1. Completed V&V Quality Code Review Validation Request Form
2. TAS_API_01.00.65_fortify_scan.fpr - Fortify Static Code Analyzer (SCA) static analysis tool scan result file
3. TASAPI_01.00.65_src.zip - TAS API v01.00.65 source code
4. runFortifyScan.sh – Fortify scan script

2 Quality Code Review Validation Results

This document contains the results of a Verification and Validation (V&V) review, conducted by the VA Software Assurance Program Office, of developer-provided Fortify SCA static analysis tool scan result files, and of any provided custom scan tool custom rule files, as well as the TAS API v01.00.65 source code. Goals of performing quality code reviews at the VA include ensuring that unpredictable behavior caused by poor code quality is minimized. Goals of V&V quality code review validations include ensuring that quality code reviews performed by VA software developers have been done correctly and consistently.

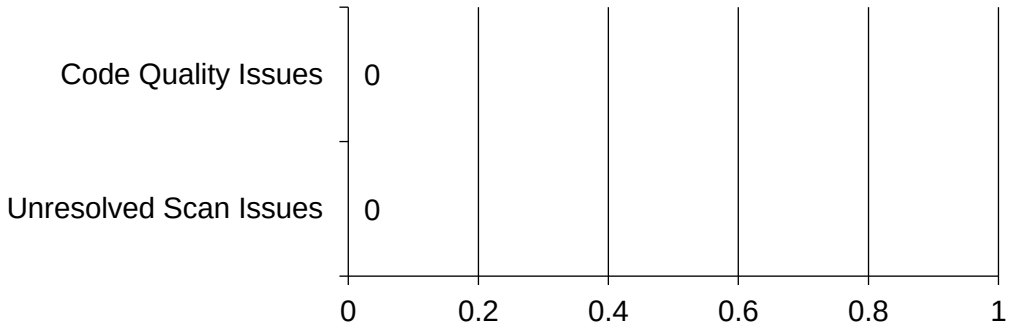
The V&V quality code review validation conducted by the VA Software Assurance Program Office covered provided materials to ensure that:

1. Application information in quality code review validation request packages is accurate and complete, and
2. Application scan results demonstrate that VA standards have been met, and
3. Application scan results demonstrate that mitigations must have been made for issues reported by the Fortify SCA static analysis tool, and
4. There are justifications provided for cases where Fortify SCA static analysis tool rules are disabled, or scan results are marked as false positives.

For more information about the validation process, see Section 3.

The V&V quality code review validation conducted by the VA Software Assurance Program Office identified a total of 0 residual code quality issues. There was a total of 0 unresolved scan issues.

Figure 1. Summary of Residual Vulnerabilities & Unresolved Scan Issues



For more information about residual code quality issues and unresolved scan issues that were identified during the quality code review validation, see Section 4.

3 Quality Code Review Validation Process Details

The **quality** code review validation was performed overall as follows:

Step 1. Perform initial planning

The first step that was performed was to perform initial planning. This included developing a strategy for performing the review and identifying considerations that should be taken into account during the review, such as any Fortify SCA static analysis tool custom rule files provided by the developer.

Step 2. Review source code

The next step is to perform the review. A combination of using Fortify SCA to review scan result files and manual analysis was used. The scan results were reviewed to ensure that best practices for performing quality code review have been followed, and that VA standards have been met, as noted in the previous section.

Step 3. Write report

The last step in the quality code review validation process is to write up the report, after working with the VA application developer to resolve any issues identified during review.

3.1 Validation Strategy

The quality code review validation was performed by reviewing Fortify SCA static analysis tool scan result files and any provided Fortify SCA static analysis tool custom rule files. The provided source code was reviewed as need to support analysis of the provided scan result and custom rule files. The quality code review validation included at a minimum the following checks:

Review developer-provided scan file for matching source code

This validation check consists of ensuring that the source code matches the uploaded static analysis tool scan result files. While during the comparison there may be some differences such as build files, source code files should not contain any differences.

Review developer-provided scan file for scanning issues

This validation check consists of reviewing static analysis tool scan result file for any anomalies in the scan. When running the scan there may have been issues reported by the static analysis tool that affected the quality or completeness of the scan that may have been overlooked.

Review developer-provided scan file for residual findings

This validation check consists of ensuring that there are no Code Quality findings in the uploaded static analysis tool scan result file (Fortify SCA “.fpr” extension

file) using Fortify Audit Workbench, after first configuring it to use any provided custom rule files.

Review developer-provided scan file for suppression of issues

This validation check consists of reviewing static analysis tool scan result files to ensure that issues reported by Fortify SCA have not been suppressed, as opposed to adding comments and developing custom rules as might be appropriate.

Review developer-provided custom rule files, if provided

This validation check consists of reviewing any provided static analysis tool custom rule files. Analysis includes examining custom rule files e.g. to ensure that there are no rules to disable built-in Fortify rules, unless those custom rules include documentation justifying their use.

Perform additional supporting analysis, as needed

This validation check consists of performing additional supporting analysis for items that may have been identified during the course of the validation for a particular application. For example, findings in the scan result files have been marked as N/A, checks would be performed to ensure there is some documented justification, and to verify the soundness of the justification. Alternately for example, analysis may be performed to determine the appropriateness of exclusions.

3.2 Tools Used for Validation

The VA Software Assurance Program Office uses the same static analysis tool (Fortify SCA) as VA application developers. The same static analysis tool is used in order to promote confidence in the outcome of the quality code review validation if the tool is in fact being used during development. Fortify SCA version 18.20 was used to review provided static analysis tool scan result and custom rule files. The Audit Workbench tool which is part of Fortify SCA was used to facilitate examining static analysis tool scan result files. Similarly, the Custom Rules Editor tool which is also part of Fortify SCA was used to facilitate examining custom rule files.

3.3 Categorization of Findings

The findings that resulted from performing the quality code review validation are grouped in Section 4 of this report.

Findings were reported as follows:

Code Quality Findings

All code quality findings must be fixed in order to successfully complete the quality code review validation process.

Findings that are unresolved scan issues

This finding categorization is reserved for issues having to do with how the scan was conducted, for example, source code not matching the uploaded static analysis tool scan result files.

Additional findings

This finding categorization is reserved for any additional concerns identified by the VA Software Assurance Program Office review that do not correspond to the categories above. For example, new issues may be identified during the course of the validation while reviewing supporting documentation.

4 Quality Code Review Validation Findings and Recommendations

4.1 Residual Code Quality Findings (0 Total)

Based on the information provided by the developer, it does not appear that code quality issues identified by Fortify SCA were left unmitigated.

4.2 Issues with How Scans Were Performed (0 Total)

4.2.1 Unresolved Scan Issues

Based on the information provided, it does not appear that there were unresolved issues when the scan of the source code was conducted.

4.2.2 Informational Scan Issues

Based on the information provided, it does not appear that there were informational issues when the scan of the source code was conducted.

4.3 Additional Findings (0 Total)

There were no additional findings that were identified during the course of the validation.

5 Quality Code Review Validation Report Conclusion

Implementing quality applications from the start is every VA application developer's responsibility. Poor code quality can impact an application's usability and also result in unpredictable behavior that could cause security issues. Quality issues generally manifest themselves as one of two types: **functional quality** that affects usage and **structural quality** that affects robustness and maintainability.

Fortify SCA should be used according to the VA Quality Code Review SOP to minimize structural quality flaws during application implementation. Fortify SCA supports a wide range of programming languages and build environments. The VA-licensed Fortify SCA can also be used as a standalone tool by VA developers, or integrated into for example Continuous Integration (CI) build environments.

The VA Software Assurance Program Office uses the same static analysis tool (Fortify SCA) as VA application developers during the quality code review validation process to ensure consistency and completeness of analysis.

Note that remediation estimates provided in this report are provided to assist with planning remediation work, if or as might be appropriate. Note that some bugs are harder to fix than others. Modifying a single line of code in a self-contained method for example is easier than modifying the result of a sequence of calls. Systems development program and project-specific considerations should also be taken into account when planning remediation work. Read more…

5.1 Resources that you may find helpful

The following resources may be helpful to readers of this report:

VA Software Assurance Support Site

This site provides VA Software Assurance Program Office resources to assist VA application developers with performing code reviews and design reviews during development and also during Assessment and Authorization (A&A) and continuous monitoring.

VA Quality Code Review Standard Operating Procedures (SOP)

This document establishes policies and procedures for performing quality code review (static analysis) of custom-developed applications at the VA.

Fortify product documentation

This documentation is included as part of Fortify software distribution. It includes system requirements documentation and user guides.