

VA Software Assurance

Office of Information Security

Secure Coding Tips

Tip: Not Auditing Issues Leaves Vulnerabilities Unaddressed

This week's Secure Coding Tip is about not auditing issues when performing scans using the HP Fortify Static Code Analyzer (SCA) software. Scanning source code to perform code review is an authorization requirement included in the Technical / Testing Requirements of the OCS Accreditation Requirements Guide / SOP [1], and enforced as part of the ATO issuance process.[2]

One of the top 10 issues[3] encountered by VA application developers using the HP Fortify SCA software is not auditing issues reported during a Fortify scan.[4] Auditing issues reported by Fortify is required by the VA Secure Code Review Standard Operating Procedures (SOP)[5] to ensure all Fortify scan results have been either mitigated or determined to be false positives.

There are several steps you can take to resolve the issue. [Read more...](#)

- [1] "Accreditation Requirements Guide / Standard Operating Procedures", Office of Cyber Security (OCS) Assessment and Authorization intranet site.
- [2] "Accreditation Requirements Expectation Memorandum" (Section 2.a.ii "Code Review"), VA Chief Information Security Officer (CISO) Stanley F. Lowe, March 19, 2014.
- [3] [VA Top 10 Fortify Scan Issues For 2015 \(Q2\)](#)
- [4] VA Top 10 Fortify Scan Issues For 2015 (Q2), [S7: Issues not audited](#)
- [5] [VA Secure Code Review SOP](#)

More Information

For more information about the VA Software Assurance Program Office, please visit our website [here](#).



Resources

[VA Software Assurance Support Site](#)

[VA Code Review Standard Operating Procedures](#)

[VA Code Review Process eLearning Module](#)

[VA-Licensed Fortify Request Instructions](#)

[VA Software Assurance Training Schedule](#)

[VA Software Assurance Frequently Asked Questions](#)

Next Class:

7/27