

Secure Coding Tips

Old Versions of Fortify Software May Leave Vulnerabilities Undetected

This week's Secure Coding Tip is about using old versions of Fortify software (as opposed to rulepacks) during scans when 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 using old versions of the software to perform a scan.[4] Scans that do not use the most recent version of Fortify may not include a complete set of results; for example build environment support may be more complete in newer versions. Other scan issues may also result.

There are several steps you can take to resolve the issue.

[Read more...](#)

- [1] "Accreditation Requirements Guide / Standard Operating Procedures", VA 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 \(Q4\)](#)

More Information

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



Resources

[Request VA-licensed code review tools, validations, and support here](#)

[Latest VA Software Assurance Program Office announcements can be found here](#)

[Learn more about VA code review processes here](#)

Next Class:

12/15

[VA Working Group Registration Instructions](#)

[VA Application Registration Instructions](#)

Next Working Group Meeting:

12/7