

# VA Software Assurance Secure Coding Tips

## Not Knowing What Code Was Actually Scanned May Leave Vulnerabilities Undetected

This week's Secure Coding Tip is about not knowing (or losing track of) which application source code files (or even which application's) were scanned when auditing HPE Security Fortify Static Code Analyzer (SCA) scans. 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 issues[3] encountered by VA application developers using the HPE Security Fortify SCA software is not knowing (or losing track of) what (or which application's) source code files were scanned.[4] If source code files are not included in a scan, omitted files are not analyzed. All source code files belonging to an application must be scanned according to the VA Secure Code Review Standard Operating Procedures (SOP)[5] to ensure the most accurate set of results.

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 2016 \(Q2\)](#)

[4] [VA Top 10 Fortify Scan Issues For 2016 \(Q2\), S8: Cannot determine what source code provided corresponds to source code scanned](#)

[5] [VA Secure Code Review SOP](#)

### Resources

- [VA Software Assurance Support Site](#)
- [Request VA-licensed code review tools, validations, and support](#)
- [Latest VA Software Assurance Program Office announcements](#)
- [Learn more about VA code review processes](#)
- [VA Working Group Registration Instructions](#)

- [VA Application Registration Instructions](#)

## **Reminders**

- [The next working group meeting is 9/12](#)

You have received this message because you are subscribed to VA Software Assurance Secure Coding Tips. To unsubscribe to these announcements or to subscribe, email: [OISSwASupportGroup@va.gov](mailto:OISSwASupportGroup@va.gov)

