

## Secure Coding Tips

### Tip: Not Scanning All Application Code May Leave Vulnerabilities Undetected

This week's Secure Coding Tip is about not including all of an application's source code files 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]

The current top issue[3] encountered by VA application developers using the HP Fortify SCA software is not scanning all source code files of an application.[4] If all source code files are not included in a scan, omitted files are not analyzed. All application source code files 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 2015 \(Q4\)](#)
- [4] VA Top 10 Fortify Scan Issues For 2015 (Q4), [S1: Code not scanned](#)
- [5] [VA Secure Code Review SOP](#)

## 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:

**11/17**

[VA Working Group Registration Instructions](#)

[VA Application Registration Instructions](#)

Next Working Group Meeting:

**11/9**