

Secure Coding Tips

HP Fortify Custom Rules Development Standard Operating Procedures

This week's Secure Coding Tip is about the development of custom rules for use with HP Fortify Static Code Analyzer (SCA) software. Scanning source code to perform code review[1] is an authorization requirement included in the Technical / Testing Requirements of the OCS Accreditation Requirements Guide / SOP [2] , and enforced as part of the ATO issuance process.[3]

It is possible to extend the functionality of Fortify and the Secure Coding Rulepacks by writing custom rules. However, VA Secure Code Review SOP for doing so requires that they are well documented and independently verifiable by the VA Software Assurance Program Office when secure code review validations are performed.

[Read more...](#)

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

[2] "Accreditation Requirements Guide / Standard Operating Procedures", VA OCS Assessment and Authorization intranet site.

[3] "Accreditation Requirements Expectation Memorandum" (Section 2.a.ii "Code Review"), VA Chief Information Security Officer (CISO) Stanley F. Lowe, March 19, 2014.

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:

2/23

[VA Working Group Registration Instructions](#)

[VA Application Registration Instructions](#)

Next Working Group Meeting:

3/7