

VA Software Assurance

Office of Information Security

Secure Coding Tips

Tip: Poor Code Quality Can Lead To Vulnerabilities

This week's Secure Coding Tip is about how poor code quality[1] can introduce vulnerabilities into VA applications. Scanning source code to perform code review 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]

Poor code quality can lead to unpredictable behavior. For an attacker it provides an opportunity to stress the system in unexpected ways. An example is not releasing or incorrectly releasing a resource before it is made available for re-use.[4] Code quality errors with potential security implications are errors that the HP Fortify Static Code Analyzer (SCA) can detect.

[Read more...](#)

- [1] MITRE Common Weakness Enumeration (CWE) **CWE-398: Indicator of Poor Code Quality**
- [2] "Accreditation Requirements Guide / Standard Operating Procedures", Office of Cyber Security (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.
- [4] MITRE Common Weakness Enumeration (CWE) **CWE-404: Improper Resource Shutdown or Release**

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-Licensed Fortify Request Instructions](#)

[VA Software Assurance Frequently Asked Questions](#)

Training

[VA Code Review Process](#)

[VA Fortify End User Course](#)

[VA Secure Coding Course](#)