



Request Fortify software, training, and support [HERE](#)

VA Software Assurance Secure Coding Tip

Input Validation Coding Errors Can Lead To Vulnerabilities

This week's Secure Coding Tip is about how making input validation coding errors can introduce vulnerabilities in 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 [1], and enforced as part of the ATO issuance process.[2]



Not assuming that all input is malicious, and for example not strictly validating inputs, can result in an application receiving unintended input, which may result in altered control flow, arbitrary control of a resource, or arbitrary code execution.[3] Input validation coding errors such as SQL Injection[4] are errors that the HP Fortify Static Code Analyzer (SCA) can detect.

[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] MITRE Common Weakness Enumeration (CWE) [CWE-20: Improper Input Validation](#)

[4] MITRE Common Weakness Enumeration (CWE) [CWE-89: SQL Injection](#)

Resources

- [VA Software Assurance Support Site](#)
- [Request VA-licensed code review tools, validations, and support](#)
- [Latest VA Software Assurance Program Office announcements](#)
- [Check if your application has been registered \(internal link\)](#)

Reminders

- [The next working group meeting is on 1/10](#)

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

VA



**U.S. Department
of Veterans Affairs**

**Office of Information
and Technology**

*Software Assurance
Program Office*