

VA Software Assurance Secure Coding Tips

Time and State Coding Errors Can Lead To Vulnerabilities

This week's Secure Coding Tip is about how making time and state types of coding errors[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]

This type of vulnerability has to do with coding errors related to the improper management of time and state by multiple systems, processes, or threads. An example is session fixation: authenticating or establishing new user sessions without invalidating existing sessions.[4] Security feature coding errors such as these are errors that the HP Fortify Static Code Analyzer (SCA) can detect.

[Read more...](#)

[1] MITRE Common Weakness Enumeration (CWE) [CWE-361: Time and State](#)

[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-384: Session Fixation](#)

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 instructor-led class is on 8/2](#)
- [The next working group meeting is today](#)

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

