

Secure Coding Tips

API Abuse Coding Errors Can Lead To Vulnerabilities

This week's Secure Coding Tip is about how making API abuse 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]

An example of an API abuse type of vulnerability is calling a potentially dangerous function incorrectly, resulting in a vulnerability.[4] Another example is when a function is inherently dangerous and cannot be used safely (and thus should never be used).[5] API abuse 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-227: API Abuse**
- [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-676: Use of Potentially Dangerous Function**
- [5] MITRE Common Weakness Enumeration (CWE) **CWE-242: Use of Inherently Dangerous Function**

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:

3/22

[VA Working Group Registration Instructions](#)

[VA Application Registration Instructions](#)

Next Working Group Meeting:

3/7