

Announcing VA Top 10 Fortify Scan Issues For 2015 (Q1)

The purpose of this announcement is to communicate an update to the top ten list of the most common issues encountered at the VA when scanning source code using the HP Fortify Static Code Analyzer (SCA) tool, according to the [VA Secure Code Review Standard Operating Procedures \(SOP\)](#).

This list does not contain any vulnerability information. This list can be used to learn from the mistakes of others. And, to help System Owners, Project Managers, Information Security Officers (ISOs), and all system / project / contractor staff with furthering awareness of the risk that software creates in the agency.

The [VA Top 10 Fortify Scan Issues For 2015 \(Q1\)](#) are:

- **S1:** Errors during scan
- **S2:** Code not scanned
- **S3:** Old version of Fortify used during scan
- **S4:** Old version of rulepacks used during scan
- **S5:** Issues not audited
- **S6:** Scanned source differs from provided source
- **S7:** Hidden and suppressed Issues
- **S8:** Default rulepacks were not used during scan
- **S9:** Removed Findings
- **S10:** Cannot determine what source code provided corresponds to source code scanned

This list is the result of actual code review validations performed according to the [VA Secure Code Review SOP](#) by the VA Software Assurance Program Office.