

# Fortify Scan Issue: Audit was not performed within Fortify

 This page has been made public for vendors

## Question

What does the Fortify scan issue "Audit was not performed within Fortify" mean, how can I detect it, and how can I fix it?

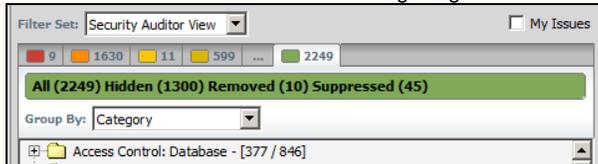
## Answer

This scan issue indicates that the issues reported by Fortify have not been audited in Fortify by the developers. However, the audits were provided in a format outside Fortify (e.g., in a text document or spreadsheet). The **VA Secure Code Review SOP** requires that the developers audit all the issues within Fortify.

## How to detect

Open the FPR file in either Audit Workbench or the IDE where you generate the FPR.

- First ensure that Audit Workbench is displaying all the issues reported by the scan. Look for the "Filter Set" drop down box in the upper left hand corner of Audit Workbench as shown in the following image:



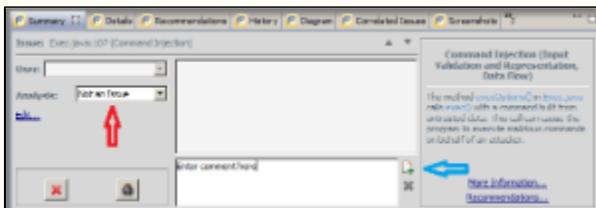
The Filter Set should be set to "Security Auditor View." Other values only display a subset of the reported issues.

- Next, look at each issue displayed in that issues panel. After each issue, it displays the number of audited instances of the issue against the total number of reported instances - [ <audited instances> / <total instances> ]. For each issue, the number of audited instances should match the total number of instances.
- If audit comments were supplied in an alternative format, then this issue is a concern.

Note that it is acceptable to provide additional details for some complex issues in an external document (such as a design document), but the audit comments in Fortify must reference the external document.

## How to resolve

This issue should be resolved by auditing all issues within Fortify. This is done by selecting an issue, then going to the audit pane and filling in the appropriate information. Each issue should be marked as to whether it is a false positive or not (false positives are marked by using the Analysis tag of "Not an Issue") and including comments supporting that tag. If it is marked as a false positive, provide a detailed explanation of why it is a false positive or the mitigations in place to fix the issue. The more details (such as file name and line numbers where input is validated) the easier it is for the reviewers to validate the mitigation.



Note that if the same comment applies to multiple instances of an issue, multiple instances may be selected and the comment applied to all the selected instances at the same time.

HPE Fortify Version	4.40 and later
Programming Language	<input checked="" type="checkbox"/> C/C++ <input checked="" type="checkbox"/> .NET <input checked="" type="checkbox"/> Java <input checked="" type="checkbox"/> Objective-C <input checked="" type="checkbox"/> Other
Fortify Audit Workbench	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Fortify IDE Plugin	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Other Fortify Component	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

Request code review tools, validations, and support [HERE](#).

## References

- [VA Top 10 Fortify Scan Issues For 2017 \(Q1\)](#)
- [VA Top 10 Fortify Scan Issues For 2016 \(Q1\)](#)