# Fortify

This page was automatically generated and should not be edited.

The information on this page was provided by outside contributors and has not been verified by SEI CERT.

The table below can be re-ordered, by clicking column headers.

**Tool Version:** V. 5.0

| Checker | Guideline |
|---|---|
| HTTP_Response_Splitting | IDS00-J. Prevent SQL injection |
| Log_Forging | IDS03-J. Do not log unsanitized user input |
| Missing_Check_against_Null | EXP01-J. Do not use a null in a case where an object is required |
| Missing_XML_Validation | IDS16-J. Prevent XML Injection |
| Missing_XML_Validation | IDS17-J. Prevent XML External Entity Attacks |
| Not Implemented | VNA00-J. Ensure visibility when accessing shared primitive variables |
| Null_Dereference | EXP01-J. Do not use a null in a case where an object is required |
| Password_Management | MSC03-J. Never hard code sensitive information |
| Password_Management__Hardcoded_Password | MSC03-J. Never hard code sensitive information |
| Path_Manipulation | FIO16-J. Canonicalize path names before validating them |
| Process_Control | IDS01-J. Normalize strings before validating them |
| Redundant_Null_Check | EXP01-J. Do not use a null in a case where an object is required |
| SQL_Injection | IDS00-J. Prevent SQL injection |
| SQL_Injection__Persistence | IDS00-J. Prevent SQL injection |