Built-in Static Analysis Rules

This topic describes the preconfigured "built-in" static analysis standard rules that are included with SOAtest.

Sections include:

- Understanding Rule Categories
- Viewing Rule Descriptions
- Severity Levels
- Custom Rules

Understanding Rule Categories

SOAtest checks over 500+rules that check whether expectations for security, reliability, and compliance are met. Rules are organized into thematic categories such as:

- Accessibility - WCAG 1.0 / Section 508
- Accessibility - WCAG 2.0 / ACC - WCAG2
- Browser Compatibility
- Coding Conventions
- Check HTML Well-Formedness
- Check Links
- Check Spelling
- Forms
- Interoperability
- Invalid Code
- Localization
- Maintainability
- Navigation
- Performance
- Presentation
- Security
- Utility
- Unused Code
- Validate XML

Viewing Rule Descriptions

To view descriptions of all the static analysis rules that are included with SOAtest, choose **Parasoft> Help**, open the **SOAtest Static Analysis Rules** book, then browse the available rule description files.

To view a list of all static analysis rules that a given Test Configuration is configured to check, as well as descriptions of these rules:

1. Open the Test Configurations dialog by choosing **Parasoft> Test Configurations** or by choosing **Test Configurations** in the drop-down menu on the **Test Using** toolbar button.
2. Select the Test Configuration that you want a rule list for.
3. Open the **Static** tab.
4. Click **Printable Docs**.

If you want to print the list of rules and all related rule descriptions, enable your browser’s **Print all linked documents** printer option before you print the main the list of rules.

Notes

- Rules are listed in the following format: Rule description (RULE ID- RULE SEVERITY LEVEL)
  - RULE ID is the string used to identify this rule in the Test Configurations panel and to identify violations of this rule in reports and results.
  - SEVERITY LEVEL is a number from 1 to 5 that indicates the chance that a violation of the rule will cause a serious error. Possible severity levels (listed from most severe to least severe) are Level 1, Level 2, Level 3, Level 4, and Level 5.
- Special wizard hat icons are used to indicate rule properties as follows:
  - A new rule (a rule added since the previous SOAtest release) has an icon that contains the text "NEW."
  - A parameterizable rule (a rule that you can customize by modifying the available rule parameters) has an icon with a radio button.

Severity Levels

Each rule is assigned a severity level. The severity level indicates the chance that a violation of the rule will cause a serious construction defect (a coding construct that causes application problems such as slow performance, memory leaks, security vulnerabilities, and so on). Possible severity levels (listed from most severe to least severe) are:

- Highest - Level 1
- High - Level 2
- Medium - Level 3
- Low - Level 4
- Lowest - Level 5

Custom Rules

SOAtest can also check any number of custom rules that you design with the RuleWizard module. With RuleWizard, rules are created graphically (by creating a flow-chart-like representation of the rule) or automatically (by providing code that demonstrates a sample rule violation). By creating and checking custom rules, teams can verify unique project and organizational requirements, as well as prevent their most common errors from recurring.

RuleWizard can be used to modify built-in coding standards and to add additional ones. For more information about creating custom coding rules, see Creating Custom Static Analysis Rules.