Security Dashboard - Application Investigation

Application Investigation view

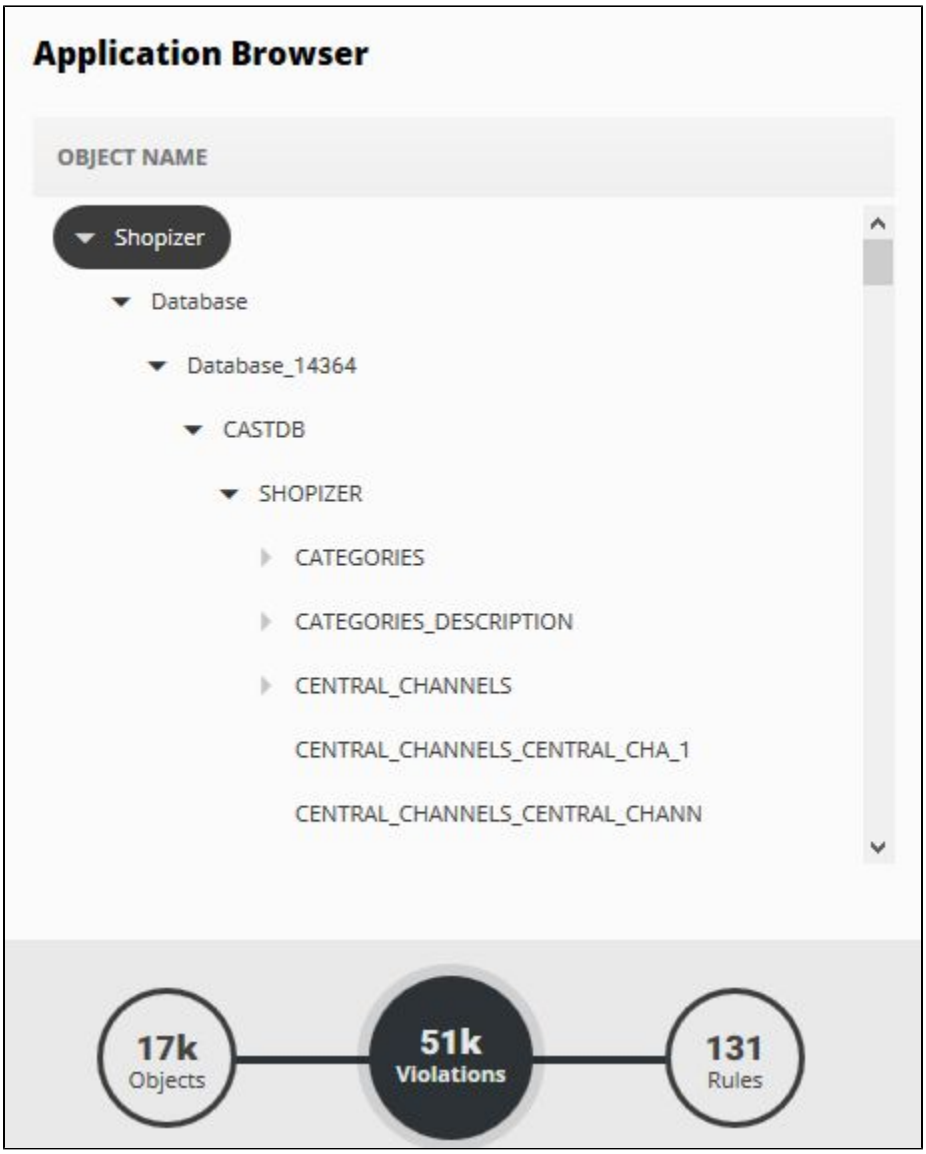
Note that the Application Investigation view is **not available** when viewing data from a previous snapshot.

Accessible from the sidebar menu  or by clicking the **Application Components tile**, this view enables investigation of the objects in the Application. Data is presented in a series of **tables** on the left and right hand side of the page enabling you to drill down from an **Application** right down to an **individual object** within that Application, and view the Rules that those objects have violated.

The default **Health Measure** used for this view is **Security:**

Application Browser

The **Application Browser** provides a hierarchical tree view of the **Application**, its **modules** and the individual **projects** and **objects** that make up the Application:

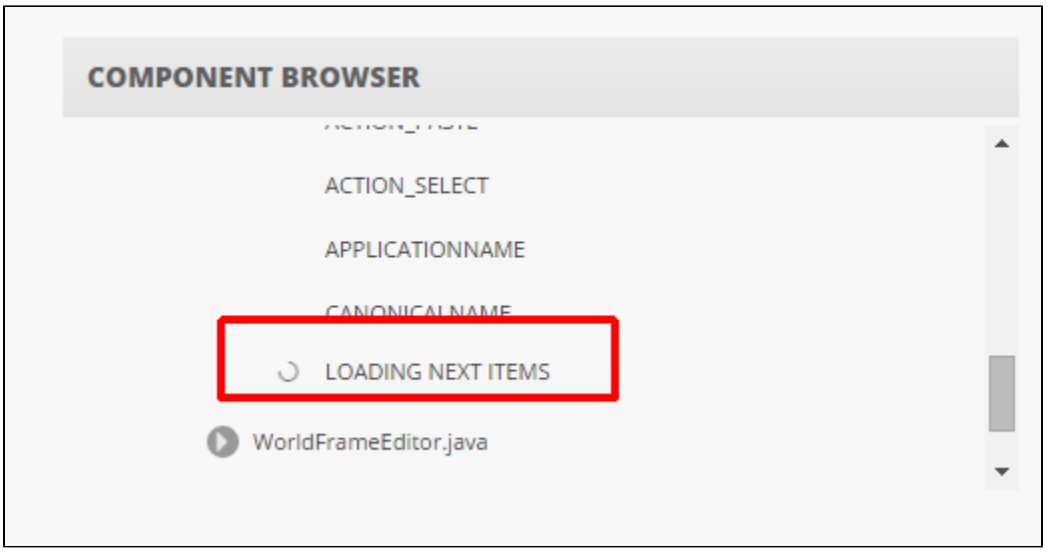


Selecting an item in the tree will do two things:

- Update the **right hand side** (see below) of the screen with a list of Rules that the item is violating - so for example, selecting the **root Application** in the tree will display ALL the Rules that have been violated in the Application. Selecting an **individual object** will only display the Rules that the selected object has violated.
- Update the **circular "at a glance" views** underneath the hierarchical object tree, to display:
  - **Objects**: the number of objects that have violated a Rule for the selected item - if you select the root Application, the total number of objects that have violated at least one Rule will be displayed.
  - **Critical Violation/Violations**: the number of Critical Violations or Violations of Rules that the selected item has - this value will always be equal to or higher than the value for the "Rules" circle (the display depends on whether only Critical Violations or ALL Violations are being displayed (see Data Filtering on Critical Violations)
  - **Rules**: the number of Rules that the selected item is violating

Handling large applications contain a large number of objects

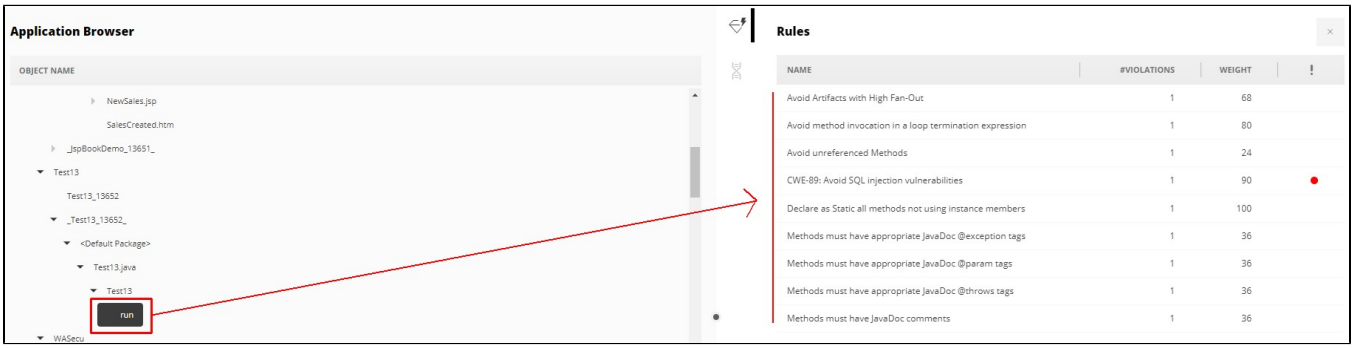
When applications are large and flat (flat project structure), the number of items can be large, leading to slow loading and page rendering. A pagination mechanism has been designed in order to improving the usability: only a subset of items are loaded (~100 by default) and, upon scroll in the browser, more content will load in a lazy fashion with the message "Loading Next Items":



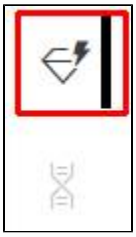
Rules with violations list

Selecting **an item** (Application, Module, Project, Object) in the left hand section will update the **right hand** section. This section lists **Rules that the selected item is violating** and the object's **Technical Properties** (see below). Rules are listed by the number of times they have been violated by the selected item (and all its constituent items in the case of an Application, Module or Project) and whether the Rule is critical (flagged with a red dot):

Click to enlarge



Note that an icon indicates the list you are working in:



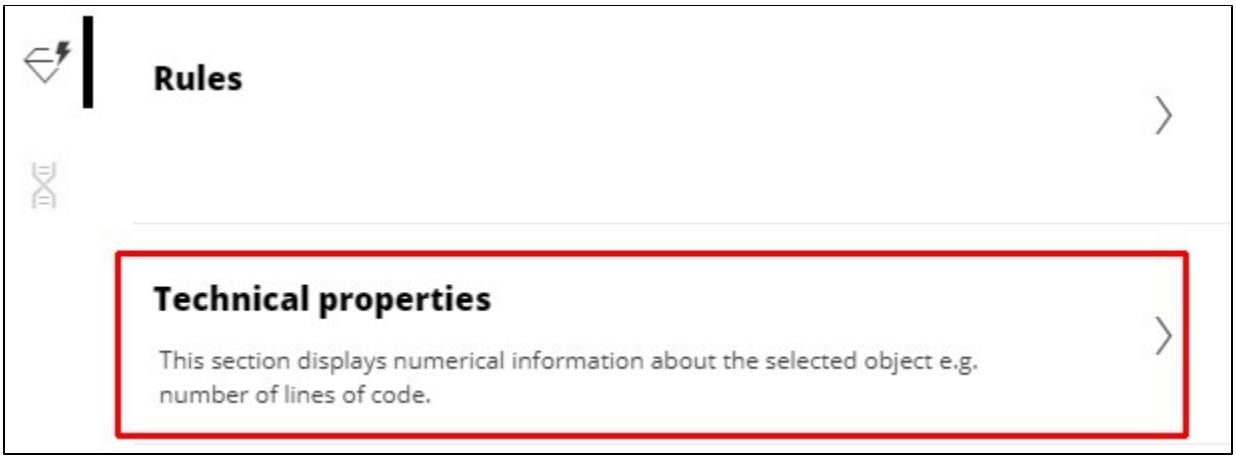
Column	Explanation
Name	Name of the Rule that the selected item is violating.
#Violations / #Critical Violations	The number of Critical Violations or Violations that the selected Rule has (the display depends on whether only Critical Violations or ALL Violations are being displayed (see Data Filtering on Critical Violations)).

Weight	Displays the compounded weight of the Rule in the parent Technical Criterion. The higher the value, the more weight the Rule carries. Clicking the **Weight** column header will sort the Rules as follows: • by weight descending and highlights grey gauge when clicking for the first time • by weight ascending and highlights grey gauge when clicking for the second time • by critical Rules descending and highlights red dot when clicking for the third time • by critical Rules ascending and highlights red dot when clicking for the fourth time Compounded weight is calculated as follows: `weight of the parent technical criterion X weight of the Rule`
Critical Rule	A red dot in this column indicates that the Rule has been set as **critical** in the Assessment Model.

Technical Properties

Selecting **an item** (Application, Module, Project, Object) in the left hand section will update the **right hand** section. This section lists Rules that the selected item is violating (see above) and the object's Technical Context. This section displays the properties of the selected objects. It has two views:

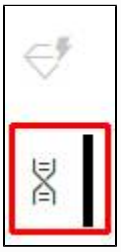
- **Global view**: provides a description of the technical properties ("This section displays numeral information about the selected object e.g. number of lines of code").



- **Detail view**: lists the object's properties:
  - Number of code lines
  - Number of comment lines
  - Number of commented code lines
  - Coupling
  - Cyclomatic Complexity
  - Distinct Operands
  - Distinct Operators
  - Essential Complexity
  - Fan In
  - Fan Out
  - Halstead Program Length
  - Halstead Program Vocabulary
  - Halstead Volume
  - Integration Complexity
  - Ratio of Comment Lines to Code Lines

Note that:

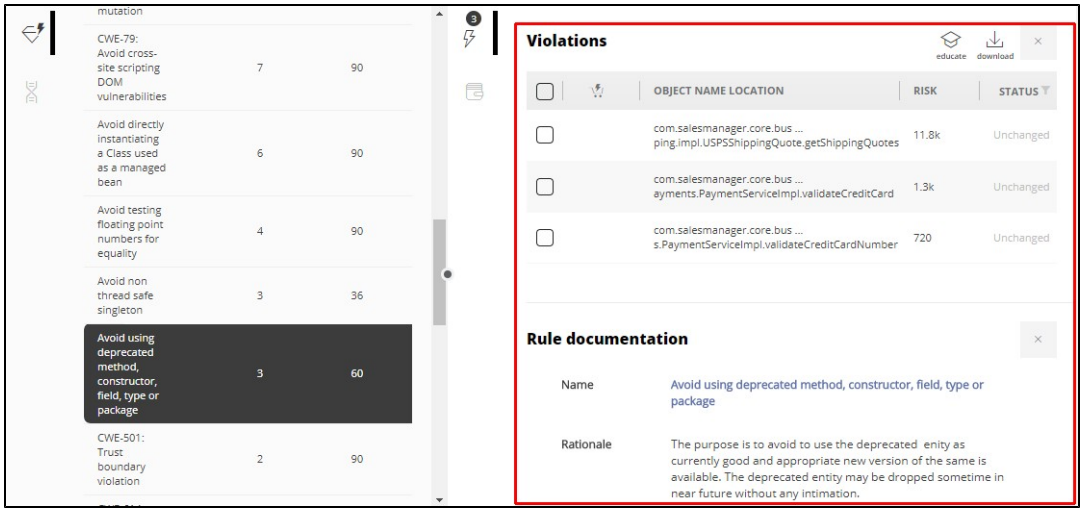
- Detail View provides a description "No Technical Properties available for this object" when there is no Technical Properties available for the selected object.
- An icon indicates the list you are working in:



Violations and Rule Documentation

Clicking a Rule in the right hand section will move the right hand panel over to the left hand side, and display a new panel containing:

- a **list of objects** that are violating the selected Rule, listed in alphabetical order
- a section containing **documentation** about the selected Rule



- Please see Violation table from the Risk Investigation view for an an explanation of the column headings **Plan**, **Object Name Location**, **Risk** and **Status**.
- Note that when there are many violations to display, a "**Show More**" button will be available. By default, only 10 violations are displayed to improve performance. You can choose to display more using the various options (+10, +100 etc.). By default an upper maximum of 5000 violations is set when the "All" option is clicked. You can change the upper maximum if required (see the **violationsCount** option in Dashboard wide configuration options in json in the CAST AIP documentation).

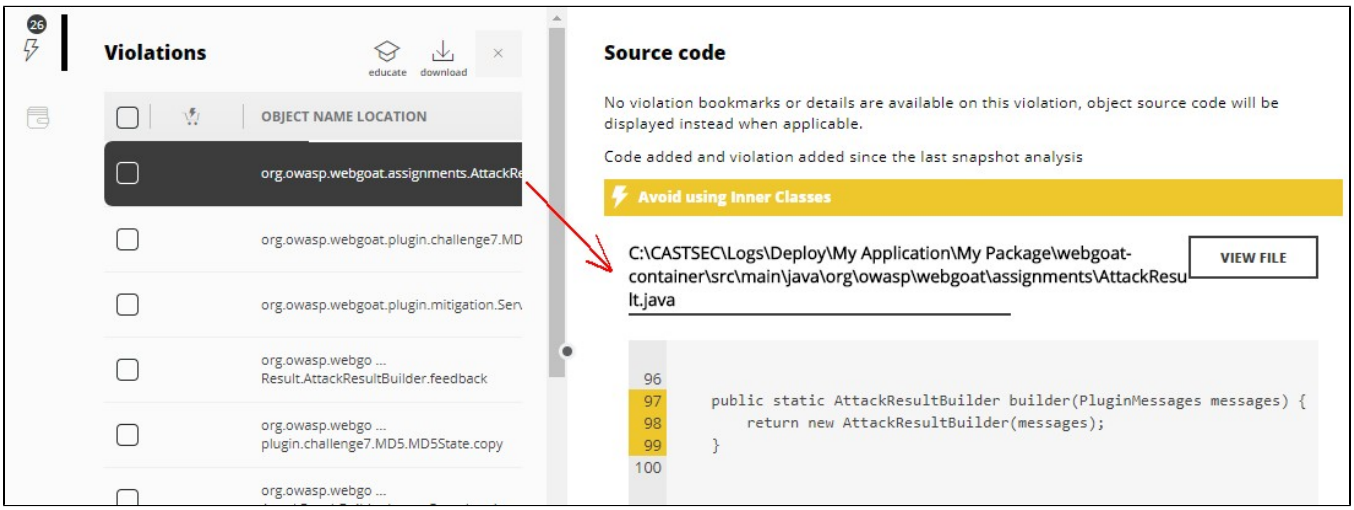
Header icons

The following icons will be available:

Educate	Click this icon to add the associated Rule to the Security Dashboard - Education list.
Download	Click this icon to export the list of violations to Excel.

Source code

Selecting an object in the Violations and Rule Documentation section will move the right hand panel over to the left hand side, and display a new panel containing the source code of the selected object:



Note that analyzed source code from the following technologies is not visible in the Security Dashboard:

- PowerBuilder
- BusinessObjects

Please also note that in the current release of CAST AIP, the display of source code is limited in functionality:

- The source code is in fact a display of the entire file that contains the selected object, therefore display performance can be affected if the file is very large
- Bookmarks in the source code showing the location of the violation are not displayed, instead the entire object within the parent source code file is highlighted
- The source code does not currently show all violations for Rules that reference User Input Security elements, such as:
  - OWASP security rules
  - The Rule "Avoid direct or indirect remote calls inside a loop"
  - Any Rule referencing copy/paste rules