Validating an OVAL™ Document

Version 5.1

Introduction

The structure of an XML document written in OVAL is guided by an XML schema. This schema determines things like what entities are available to specific tests and the order of objects and states within the language. The goal of validation is enforce a common and expected structure amongst the OVAL documents being passed between different users. This allows tools to be written against this expectation.

In a way, validation makes sure that an OVAL document is in fact an OVAL document.

Note that an OVAL document could be an OVAL Definition file, an OVAL System Characteristics file, or an OVAL Results file.

OVAL Overview

Open Vulnerability and Assessment Language (OVAL™) is an international, information security, community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services. OVAL includes a language used to encode system details, and an assortment of content repositories held throughout the community. The language standardizes the three main steps of the assessment process: representing configuration information of systems for testing; analyzing the system for the presence of the specified machine state (vulnerability, configuration, patch state, etc.); and reporting the results of this assessment. The repositories are collections of publicly available and open content that utilize the language.

The OVAL community has developed three schemas written in Extensible Markup Language (XML) to serve as the framework and vocabulary of the OVAL Language. These schemas correspond to the three steps of the assessment process: an OVAL System Characteristics schema for representing system information, an OVAL Definition schema for expressing a specific machine state, and an OVAL Results schema for reporting the results of an assessment.

Content written in the OVAL Language is located in one of the many repositories found within the community. One such repository, known as the OVAL Repository, is hosted by The MITRE Corporation. It is the central meeting place for the OVAL Community to discuss, analyze, store, and disseminate OVAL Definitions. Each definition in the OVAL Repository determines whether a specified software vulnerability, configuration issue, program, or patch is present on a system.

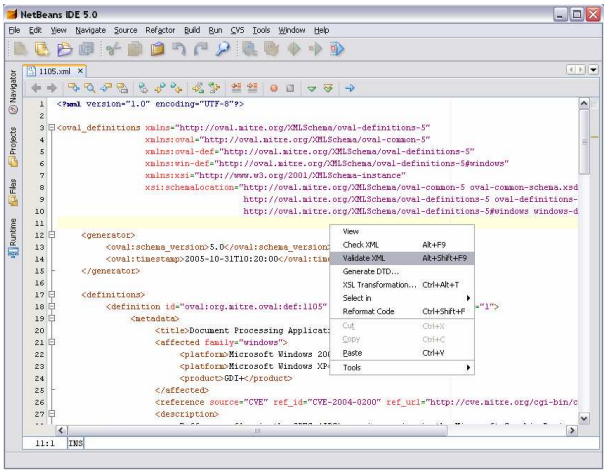
The information security community contributes to the development of OVAL by participating in the creation of the OVAL Language on the OVAL Developers Forum and by writing definitions for the OVAL Repository through the OVAL Community Forum. An OVAL Board consisting of representatives from a broad spectrum of industry, academia, and government organizations from around the world oversees and approves the OVAL Language and monitors the posting of the definitions hosted on the OVAL Web site. This means that the OVAL, which is funded by US-CERT at the U.S. Department of Homeland Security for the benefit of the community, reflects the insights and combined expertise of the broadest possible collection of security and system administration professionals worldwide.

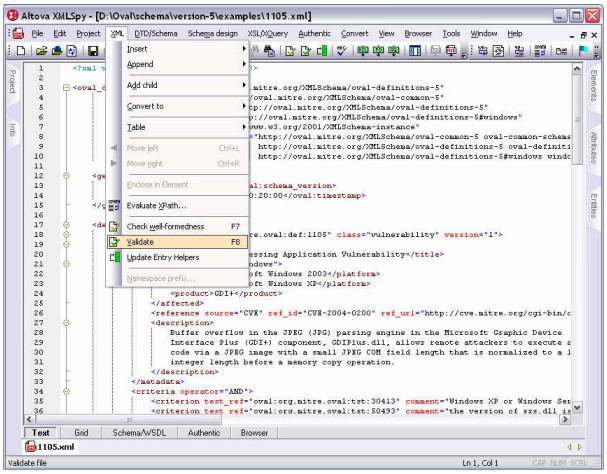
W3C Schema Validation

W3C Schema, also known as XSD, is an XML format used to describe the things like elements and types that are found within a specific XML instance document. A XML document is an OVAL document when it validates against the OVAL W3C Schema.

Performing this validation step is provided in most XML tools. You will usually need to place the OVAL documents in the same directory as the OVAL Schema files. This requirement can be worked around but will not be discussed here.

Once all the files are in the same directory, use your XML tool to open up the OVAL document you wish to validate. Then find the menu item that says Validate XML. You should be presented with a success or failure result and any problems should be pointed reported. Of course, each tool is different so consult your specific tool's documentation for more details.



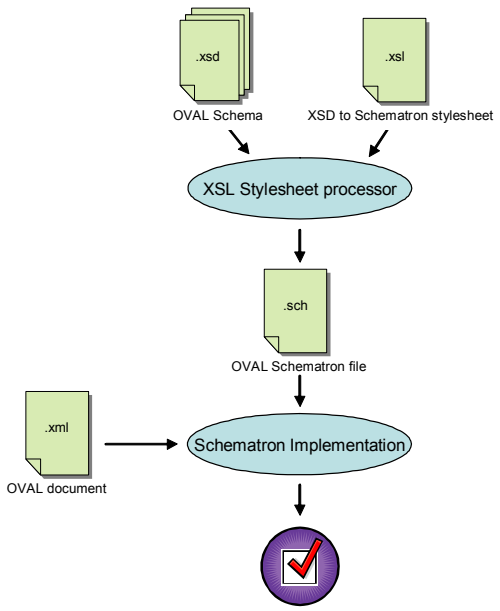


For those working on developing OVAL-Compatible tools, W3C Schema validation can be performed behind the scenes and hidden from the user. Libraries are in many of the most popular languages and can be added to your code to perform the necessary validation. Validation of incoming documents is generally a good idea as it makes certain that it is an OVAL document that is being worked on. Some popular code libraries are pointed out in the reference section at the end of this document.

Schematron Validation

Unfortunately, there are many things that cannot be validated with W3C Schema. Maybe the most pertinent example is trying to validate that a particular element exists based on the value of an attribute. To validate these types of conditions, ISO Schematron rules have been included with the OVAL Schema.

The process of Schematron Validation is a bit more complex than W3C Schema Validation. The Schematron rules found imbedded within the OVAL Schema must be collected into their own file. This can be done one of two ways. The first (and by far the simplest) is to go to the OVAL Web site and download the Schematron file. The other way is to use an XSL Stylesheet to pull the Schematron rules out from the OVAL Schema.



Once a copy of the OVAL Schematron file has been found/generated, a Schematron implementation can be used to perform the validation. There are many different types of Schematron implementations available. Some convert the Schematron file into a XSL stylesheet and use standard XSL tools to perform the validation. Others read in the Schematron file directly and perform Schematron validation in a similar way to W3C Schema validation.

As with W3C Schema validation, Schematron can be imbedded inside the code of an OVAL-Compatible tool. Schematron libraries have been for most major programming languages. Some popular code libraries are pointed out in the reference section at the end of this document.

References

Answers to almost every question pertaining to XML, W3C Schema Validation, and Schematron can be found at:

O'Reilly XML.com	-- http://www.xml.com
W3C XML Schema	-- http://www.w3.org/XML/Schema
ISO Schematron	-- http://www.schematron.com

W3C Schema Validation tools:

NetBeans	-- http://www.netbeans.org
<oXygen/>	-- http://www.oxygenxml.com
Altova XMLSpy	-- http://www.altova.com
W3C XSV	-- http://www.w3.org/2001/03/webdata/xsv

Code library:

Xerces	-- http://xml.apache.org

Schematron Validation tools:

topologi	-- http://www.topologi.com
<oXygen/>	-- http://www.oxygenxml.com