



SSA

Security System Analyzer

An OVAL™ Based Scanner

USER MANUAL

For SSA 1.5 and 1.5.1

[English]



SSA Manual Version 1.2, Last Updated 7th Feb. 2007

© 2006 - 2007 Security-Database

Security Database

<http://www.security-database.com>

General info : info@security-database.com

SSA Team : ssa@security-database.com

SSA (Free Edition) is copyright of Security Database (<http://www.security-database.com>)

SSA Security System Scanner uses technology from the following entities or companies.

- ✓ OVAL™ interpreter version **5.2 build 11** (<http://OVAL.mitre.org>)
- ✓ 7za file archiver from <http://www.7-zip.org> (original files are included in the SSA package). This software is Igor Pavlov copyright
- ✓ MD5 hash library MD5Lib.dll appears courtesy to Teddy from AHK Project (<http://www.autohotkey.net/file/users/Members/MD5Lib.dll>)

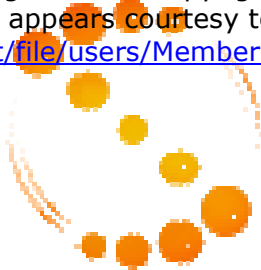
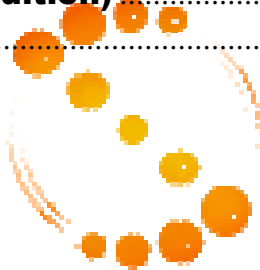


Table of Contents

INTRODUCTION	4
INSTALLING	5
System Requirements	5
Installation	5
GETTING STARTED	6
Settings	6
Front End	7
Configuring	8
Scanning	10
Analyzing reports	11
Updating The Oval Definitions files	13
[New] Plug-ins	14
Roadmap and Evolution	16
SSA HACKS FOR FUN NOT FOR PROFIT	17
SSA hacks (this hacks will be added with the release Pre 2.0)	17
Config.ini hacks (this hacks be added with the free edition release Pre 2.0)	17
License Agreement (Free Edition)	18
SSA, new logo	18



INTRODUCTION

SSA, Security System Analyzer is based upon the OVAL™ (Open Vulnerability and Assessment Language) concept.

Here is the OVAL™ definition as it comes on the [mitre.org](https://www.mitre.org) website.

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.

**Source : oval.mitre.org
Check FAQs for more information**

Security-database.com recommends you to understand the OVAL™ concept and procedures before going through installing and using Security-Database's SSA.

The SSA project has been initiated for some major reasons :

- The OVAL™ framework is a good and simple solution to map local vulnerabilities, discrepancies (with CVE references) and softwares inventory during the security assessments and audits. Thus will lead administrators and security officers to set priorities during the patch management process.
- The OVAL™ interpreter is a powerful command-line piece of software but sometimes hard to maintain (copying results.html, viewing logs, updating XML definitions, cleaning process if it hangs..). The idea behind SSA is to create a front end that makes that process easy to understand. SSA acts as an advanced GUI with some features that will help you out to scan, detect and analyze vulnerabilities identified.
- As we adopted the OVAL framework since its first releases, we decided to offer this free edition to the community.

INSTALLING

System Requirements

- Windows 2000, Windows XP, Windows 2003, (Vista under test)
- Internet Explorer 5.1 or higher / Firefox / Safari (needed to read HTML report)

Installation

SSA software could be downloaded as setup package or zipped file.

Setup.exe pack installation process

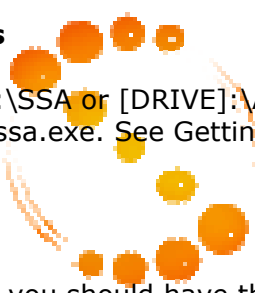
- Double click on SSA-setup.exe to start the install process (case of setup pack)
- Follow the instructions (set the directory you want SSA.exe to be installed into)
- After SSA installation, start ssa.exe. Some configurations are needed to be done (See. Getting Started for more explanation)

Zipped pack installation process

- Unzip ssa.vX.zip to [DRIVE]:\SSA or [DRIVE]:\Any_Directory
- After file decompress, start ssa.exe. See Getting Started for more explanation.

Verification

After installing or unzipping, you should have these files into the [DRIVE]:\[SSA_FOLDER_WHERE_YOU_INSTALLED_IT]



05/12/2006	15:47	<REP>	.
05/12/2006	15:47	<REP>	..
14/12/2006	16:45		511 config.ini
06/12/2006	16:35	<REP>	logo
06/12/2006	16:35	<REP>	oval.xml.files
06/12/2006	16:36	<REP>	results
07/09/2005	22:15		126 976 MD5Lib.dll
06/12/2006	16:42		202 235 ssa.exe
06/12/2006	16:45	<REP>	utilities
07/12/2006	14:35		206 501 Updater.exe
06/12/2006	16:43	<REP>	version5.2

Note: SSA Vx.zip (x means the release or version number)

GETTING STARTED

Settings

SSA package comes with no XML definitions files. These files are vital for OVAL™ interpreter.

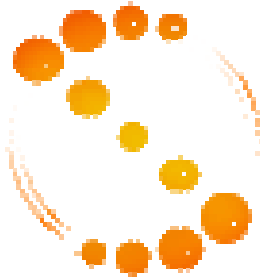
Hence, SSA software will ask you to update the definition database at the first start.

Normally, SSA will grab the necessary files from oval.mitre.org server (see SSA Hacks, if you want to change manually these parameters).

WARNING :

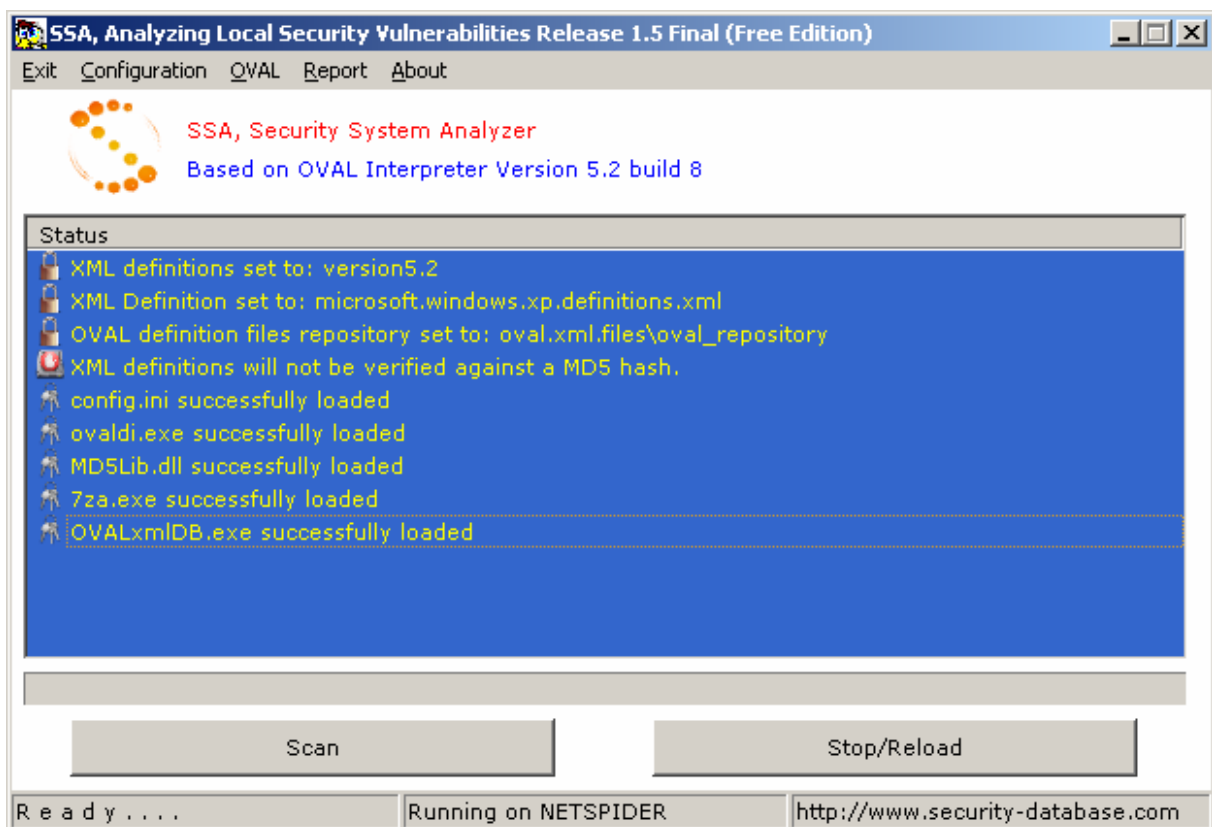
SSA comes with an original config.ini file. If modified manually without any knowledge of how SSA operates, this could lead to a malfunction (please refer to SSA hacks for tips and tricks to bypass some restrictions)

The configuration menu item updates this file automatically. Any modification will be reported, stored and re-used for the next scan session.



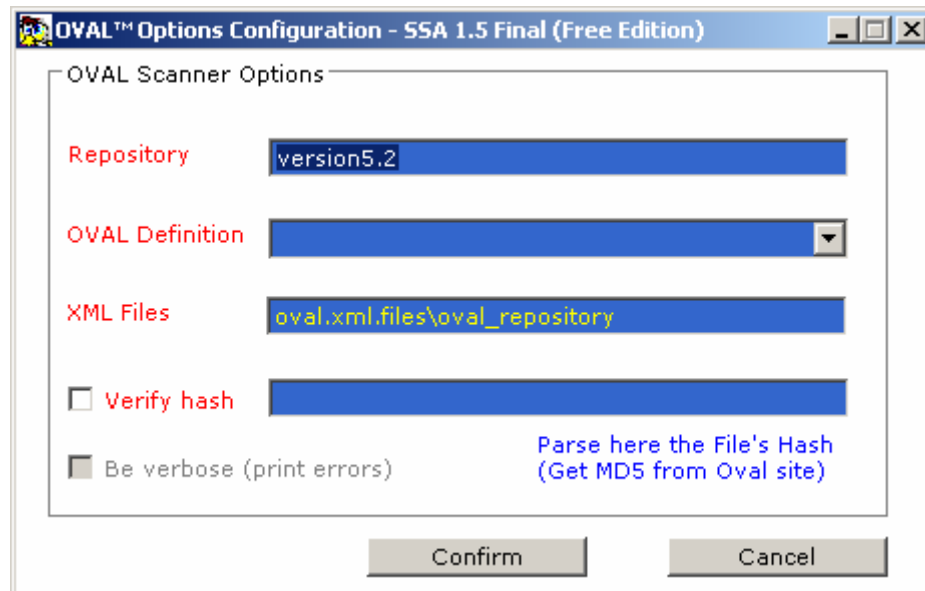
Front End

- Menu is linking to these items:
 - *Exit*
 - *Configuration*
 - *OVAL*
 - *Report (View HTML report, Delete HTML report)*
 - *About (About, Update)*
- The realtime console displays errors and logs.
- The bar indicates the progress status during the loading and scanning phases.



Configuring

Start SSA.exe and select configuration item.



Options are :

Repository [Required] : The folder where is stored the ovaldi.exe interpreter and all files that come along with it. If missed, SSA will not start.

OVAL Definition [Required] : This is the XML definition file used by the OVAL™ interpreter. If missed, SSA will ask you to update it (See Updating the OVAL definitions files for more information)

XML Files [Optional]: SSA has an embedded XML reader. This connects to each identified file and read the information (CVE, platform....). This option will be required for the next coming release 2.0.
SSA will rely on XML file to generate an history report (useful for system vulnerabilities evolutions).

Verify Hash [Optional]: Verify the file against its MD5 hash. SSA uses two methods for this purpose:

- Calculating MD5 using the OVAL™ interpreter feature.
- Calculating MD5 using the MD5lib.dll.

The local MD5 hash will be compared with the one available (copied and parsed manually) at oval.mitre.org.

OVAl - Download OVAl Repository Content - Microsoft Internet Explorer provided by [redacted]

Adresse: <http://oval.mitre.org/repository/download/index.html>

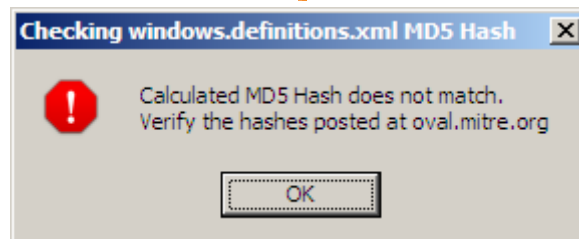
Liens: Bourse cours Boursorama ClickOptions Gmail iActu - News du 17-10-2005 Security Database W 5G Warrants SquirrelMail - Login Webmaster Hub

Platform Data File Downloads

File Name	MD5 Hash (checksum)	Date	Size
hp_ux.10.definitions.xml	3000c981b7ed11878fdcaa0a500af53d	2006-12-15	25 KB
hp_ux.11.definitions.xml	1fb29a51b3ec1cd6e8014996e13c766b	2006-12-15	334 KB
microsoft.windows.2000.definitions.xml	7f82d4b55488beb186837c4511bfbe77	2006-12-15	2.707 MB
microsoft.windows.95.definitions.xml	27929984d1ed63b3e2e251131b5672c0	2006-12-15	89 KB
microsoft.windows.98.definitions.xml	b7f54ff5e9dbff5a49954309cfee0598	2006-12-15	259 KB
microsoft.windows.me.definitions.xml	c463393e1d5062e45bc61ebd313a2a31	2006-12-15	381 KB
microsoft.windows.nt.definitions.xml	a397e5552b8c1ffb556f22f6fdc49bee	2006-12-15	1.082 MB
microsoft.windows.server.2003.definitions.xml	563a9c203fe81236840ef1d0f11e3ddd	2006-12-15	1.813 MB
microsoft.windows.xp.definitions.xml	328b2be2d22dcc42ff0004ec6e7d726c	2006-12-15	2.424 MB
red.hat.enterprise.linux.3.definitions.xml	2ea1f07c0b6498e62834c5a955f454f6	2006-12-15	892 KB
red.hat.enterprise.linux.4.definitions.xml	8d7642fb4b963c5d958931df9740796a	2006-12-15	30 KB
red.hat.linux.9.definitions.xml	582e9f86f13c62964385782fdef209c	2006-12-15	918 KB
sun.solaris.10.definitions.xml	b5bd309fa1d6ef701a9a7d699919af76	2006-12-15	191 KB
sun.solaris.7.definitions.xml	64a111c02597b6e2d3413b34345a9dde	2006-12-15	399 KB

SSA will keep in the config.ini the XML definition with its related MD5 hash (not calculated but pasted from oval website).

Bad hash returns this error message.



Scanning

To perform a scan, just click on the "Scan" button.

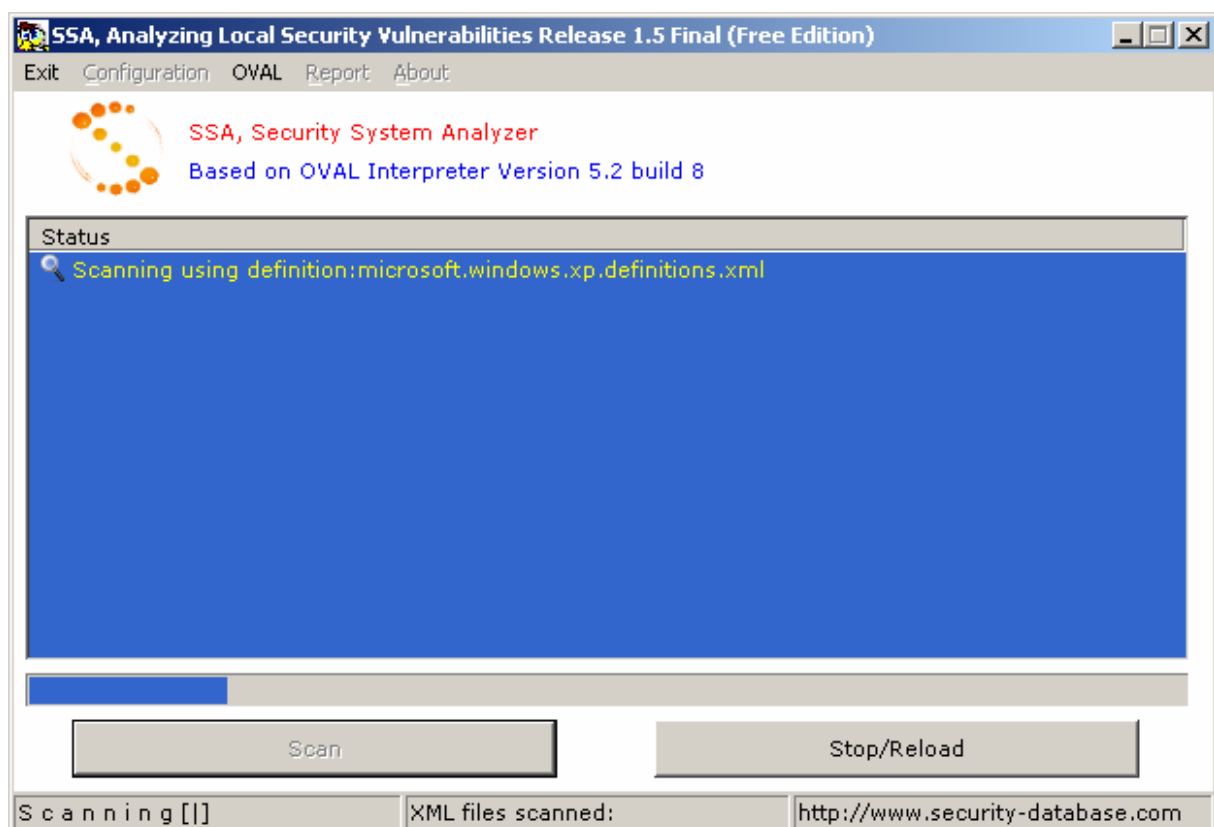
The scanning session will be performed using the parameters loaded and stored.

You can interrupt at all moment the scanning process by exiting the program (Menu: Exit). When pressed, SSA will clean temporary files and kill ovaldi.exe process.

A bar indicates you the scanning progress.

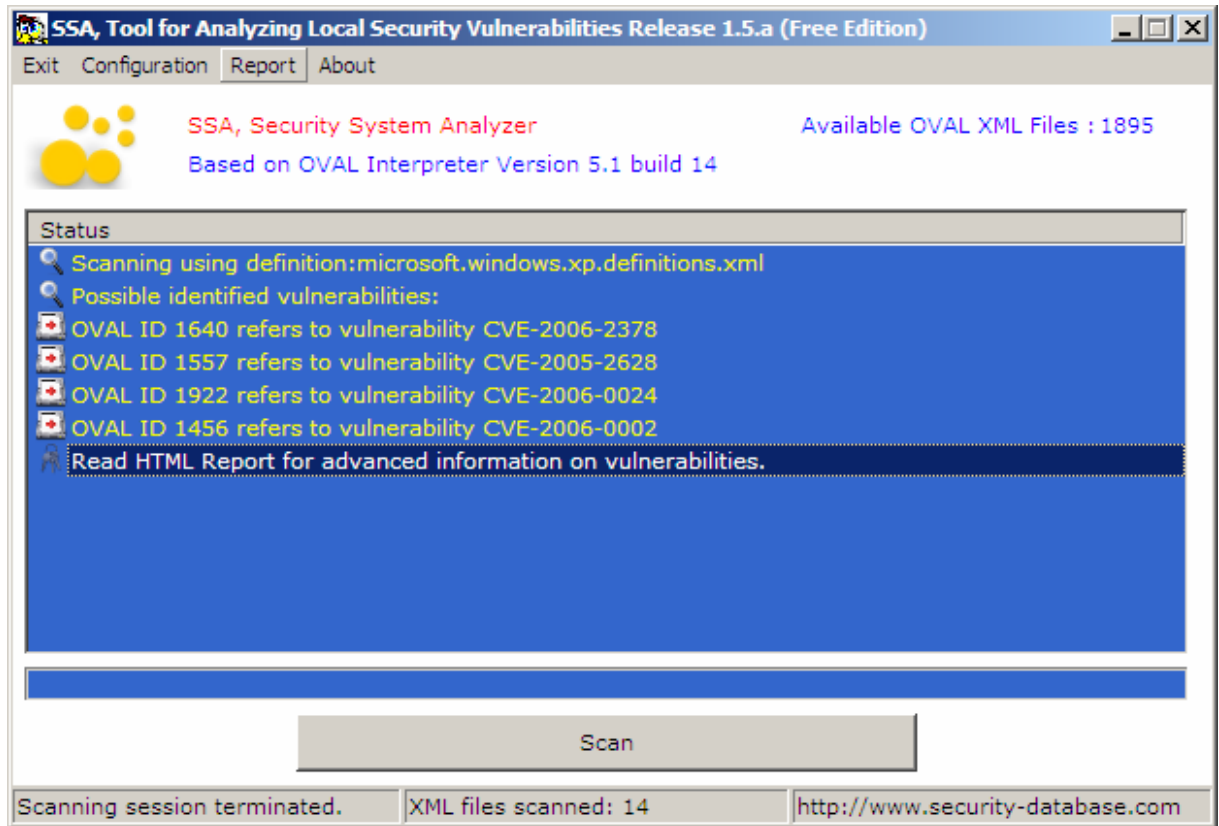
When the scan is done, a report is generated and stored in results folder. For this release, SSA relies on the original report provided by ovaldi. It's clean, well generated and useful.

For our next coming release, we will provide more in-depth information (users, patches missed, processes, running applications, binding protocols....)

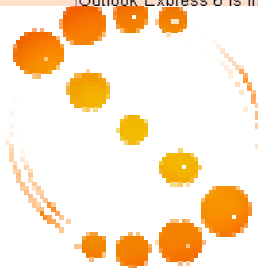


Analyzing reports

The report is generated by the OVAL™ interpreter.
Click on report and select "View HTML Report".



OVAL Results Generator Information					OVAL Definition Generator Information						
Schema Version	Product Name	Product Version	Date	Time	Schema Version	Product Name	Product Version	Date			
5.2	OVAL Definition Interpreter	5.2 Build: 8	2007-02-14	10:42:30	5.2	The MITRE Corporation		2007-0			
System Information											
Host Name		NetSpider									
Operating System		Microsoft Windows XP Home Edition Service Pack 2									
Operating System Version		5.1.2600									
Architecture		INTEL32									
Interfaces		Interface Name	[REDACTED]								
		IP Address	[REDACTED]								
		MAC Address	[REDACTED]								
OVAL System Characteristics Generator Information											
Schema Version	Product Name	Product Version	Date	Time							
5.2	OVAL Definition Interpreter	5.2 Build: 8	2007-02-14	10:42:30							
Oval Definition Results											
<input checked="" type="checkbox"/>	True	<input type="checkbox"/>	False	<input type="checkbox"/>	Error	<input type="checkbox"/>	Unknown	<input type="checkbox"/>	Not Applicable	<input type="checkbox"/>	Not Evaluated
OVAL ID	Result	Class	CVE ID	Title							
oval.org.mitre.oval:def:105	true	inventory		Microsoft Windows XP is installed							
oval.org.mitre.oval:def:521	true	inventory		Microsoft Windows XP, SP2 is installed							
oval.org.mitre.oval:def:1002	true	inventory		Microsoft XML Core Services 4 is installed							
oval.org.mitre.oval:def:425	true	inventory		Outlook Express 6 is installed							

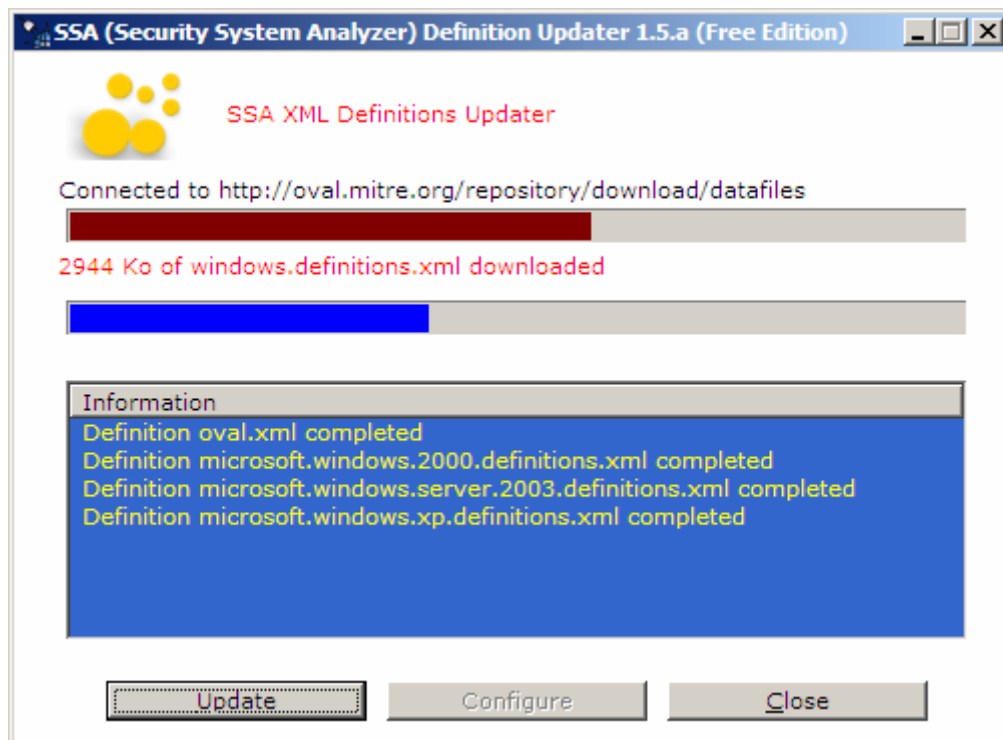


Updating The Oval Definitions files

XML definitions are frequently updated by OVAL community, we added an updater plug-in to automatically download them.

The update could be launched from the SSA program or by executing the Updater.exe plug-in.

Here is a screenshot of the updater plug-in.



The configure button will be activated for the next 1.6 release







These XML files are downloaded and installed.

```
oval.xml.files.zip
oval.xml
microsoft.windows.2000.definitions.xml
microsoft.windows.server.2003.definitions.xml
microsoft.windows.xp.definitions.xml
windows.definitions.xml
```

When the Update process is finished, SSA will automatically restarted.




[New] Plug-ins

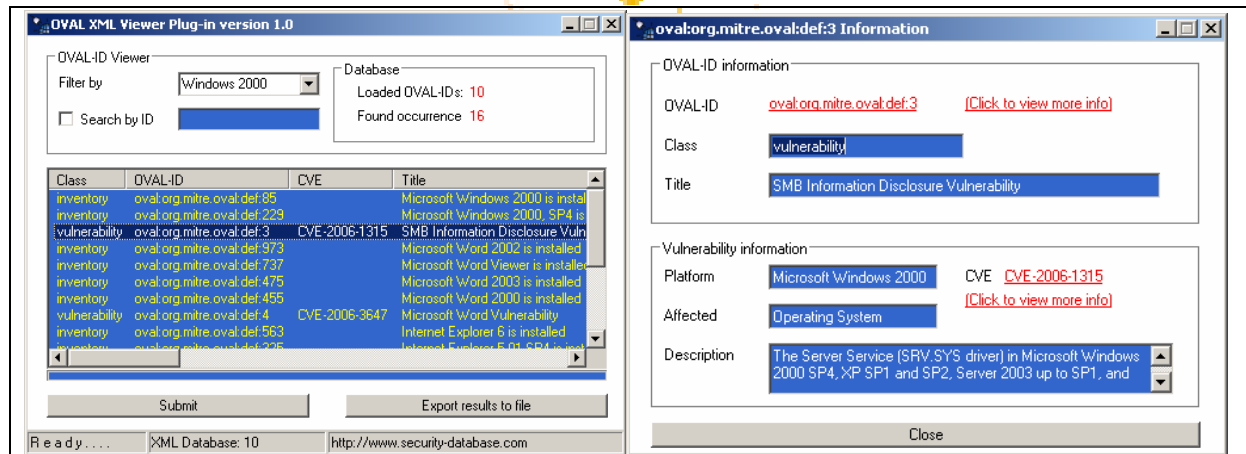
With the new version of SSA, we have introduced plug-ins and add-ons. Here is a list of available and planned plug-ins :

-  OVAL XML Files Database Viewer [Available]
-  CVSS Calculator [Planned]
-  CVE Database Search [Planned]
-  Updater [Planned]
-  Advanced Report Generator [Planned]
-  Security-Database Search Interface [Planned]

Plug-in : OVAL XML Files Database Viewer

The Oval XML Files Database viewer grabs information from the downloaded XML.files. It could be helpful for

-  Viewing only vulnerabilities and inventories of a specific OS
-  Searching the database by OVAL Id.
-  Get more information on entries by double clicking on it. You will then get
 - OVAL ID with the link to Oval.mitre.org
 - CVE information with the link to our "cross-linked" SD Alerts Watch". This offers in-depth information about vulnerabilities
 - CVSS Base scoring
 - Link to appropriate missed patch (windows) (see snapshots)
 - References



When clicking on CVE, you will be pointed to Security-Database.com SD Alerts Watch service.

Here is a snapshot of the CVE-2006-1315 information. You will notice that we cross-linked to the appropriate Microsoft MS bulletin.

INFORMATIONS		SCORING		SECURITY DATABASE	
Name	: CVE-2006-1315	Cvss Base Score	: 2.3	SDCon	:  (Low)
Last Modification	: 2006-07-12	Attack Range	: Remote		
First Publication	: 2006-07-11	Attack Complexity	: Low		
Severity	: 	Authentication	: Not Require		
INTERNAL RELATED ALERTS					
Source	Name	Severity	Title		
Microsoft	MS06-035	 (High)	Vulnerability in Server Service Could Allow Remot...		

If we follow the Microsoft MS bulletin MS06-035 link:

MICROSOFT ALERT					
<div>INFORMATIONS</div> <div><div>Name:MS06-035</div><div>Date:0000-00-00</div><div>Detail:Vulnerability in Server Service Could Allow Remote Code Execution (917159)</div></div>				<div>SECURITY DATABASE</div> <div><div>SDCon:</div><div><div></div>(High)</div></div>	
INTERNAL CVE SOURCES					
Name	Severity	Cvss Base Score	Attack Range	Attack Complexity	Authentication
CVE-2006-1315	<div></div> (Low)	2.3	Remote	Low	Not Require
CVE-2006-1314	<div></div> (High)	7	Remote	Low	Not Require

Roadmap and Evolution

Release 1.5.1 (intermediate build)

- Based on OVAL 5.2 build 11 (bugs fixed)
 - o Corrected bug in EntityComparator::ParseVersionStr(). Added error checking to the function to ensure that the input version strings are in a valid format.
 - o Removed VC7 project from source distributions.
- Fixed bugs into scan() function
 - o Handle exception: Error while parsed corrupted XML File (thanks to Drew Buttner from OVAL project)
 - o Handle exception: Error while using unsupported schema
- Fixed a latency in function "stop/reload"
- Fixed the PATH bug.

Release 1.6

- Adding more plug-ins
 - o Update existant OVAL XML Database Viewer
 - o CVSS calculator
 - o CVE Database Search
 - o SD Alerts Watch Interface
 - o Updater plug-in
 - Updating SSA Software
 - Updating Plug-ins
 - Updating XML Definitions
- Adding a new Report Manager
 - o New report will be generated with (CVE info, CVSS, MS Patches.....)
 - o We will keep the OVAL based report.
 - o Managing old reports
- The ability to download updates via proxy servers (in progress)
- The ability to run under linux environment (in-progress:many bugs)
- Complete the license agreement

Release beta 2.0

- The ability to scan remote computers (client feature)
- Map users policy, processes, patches installed, patches missed

Release 3.0

- This is a secret ;)

SSA HACKS FOR FUN NOT FOR PROFIT

SSA hacks (this hacks will be added with the release Pre 2.0)

Force SSA.exe to start even if XML definition is missing.
Clear the entry XMLDefFile in the config.ini file

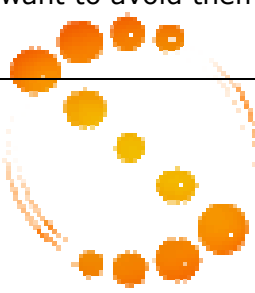
```
[Options]
OvalDefinitionsRepository=version5.1
XMLDefFile=
```

Config.ini hacks (this hacks be added with the free edition release Pre 2.0)

Edit config.ini

You can change the download XML server.

You can bootstrap XML files (if you want to avoid them to be downloaded) using # before each line. Example



```
[Updater]
.
.
.
Def1=oval.xml
Def1_Size=8000
.
.

#Def4=microsoft.windows.xp.definitions.xml
Def4_Size=2400

Def5=windows.definitions.xml
Def5_Size=5000
```

Results : microsoft.windows.xp.definitions.xml will not be download during the update Process.

License Agreement (Free Edition)

Copy it, use it, distribute it as long as these files belong to their owners

- ✓ OVAL™ interpreter version 5.2 build 11 (<http://OVAL.mitre.org>)
- ✓ 7za file archiver from <http://www.7-zip.org> (original files are included in the SSA package). This software is Igor Pavlov copyright
- ✓ MD5 hash library MD5Lib.dll appears courtesy to Teddy from AHK Project (<http://www.autohotkey.net/file/users/Members/MD5Lib.dll>)
- ✓ SSA.exe and Updater.exe are Security-Database.com copyrighted
- ✓ Readme.txt file should be kept

SSA, new logo

