SIGVI R2

User Manual

Index

1. Introduction

SIGVI stands for System Intelligent Management of Computer Vulnerabilities. It is a tool used to detect and manage vulnerabilities in software systems.

This project is developed and maintained by UPCnet, ICT service company of the group UPC (Polytechnical University of Catalonia). It has also been co-financed in 2008 by the Ministry of Industry, Tourism and Trade of Spain (MITYC, www.mityc.es) to obtain a pre-product.

The SIGVI is a Web application what consists of a set of programmed PHP scripts that implement the logic of the application and a relational database where data is stored. Some scripts run as batch processes (usually at night) to perform tasks that require no human interaction, such as loads from the sources of vulnerabilities, checks vulnerabilities in our systems, etc. The rest of the scripts are programmed inside the application site.

This application is targeted to the system administrator in his daily work of detection vulnerabilities on servers. But to simplify the tasks and operations there are several user profiles with different permissions.

Three user profiles:

•SIGVI Manager/Administrator: It is the general manager of the application, whose role will be to perform general administration tasks on the application.

•Groups Manager/Administrator: It is the figure that manages data from a group, usually the users who belong to it.

•Equipment Manager/Administrator: It is the user who ultimately will use the specific functions for managing vulnerabilities.

1.1. SIGVI Manager

Is the profile with greater access, allowing access to all sections of the application with full privileges, Which are:

•Group management

•User management of administrator users.

•Vulnerability sources manager

•Products sources manager

•News source manager

•Notification methods manager

•Global configuration and parameter manager

•Manage the implementation of bugs (if enabled)

In addition, he can:

•Manually launch the process of loading vulnerabilities

•Manually launch the process of checking for vulnerabilities

•View the logs of the application

•Interact with the database

1.2. Group Manager

The existence of this figure is due mainly to focus the management of a group of users with a level of

access between the general manager and the equipment manager. The most important function of the group manager is decide what user belongs to what group.

He also can:

•Validate or dismiss the pending warnings

•Manage the reporting and detection filters

•Manage the functions of calculating the impact factor (FAS)

1.3. Equipment manager

The equipment manager is the figure that represents on the application the operator or system administrator. Will be responsible for ensuring, among other things, the security status of their servers.

The main purpose of SIGVI is to assist the servers administrators to assure the security status of their servers.

The most important features that will be available for every day are:

•manage servers in his group (create, delete, change)

•manage the software installed on each server in his group

•manage alerts for vulnerabilities in his group.

In addition they may:

- •See notification filters
- •See the impact factor formula
- •See the overall vulnerability of the servers in his group
- •Access to general overviews
- •See application bugs and create new ones.

2. General elements in the application

Before starting to explain each section of the application we should briefly explain the common components you will see. You must know that all displays are created using the same template, which is divided into three parts: header, the page content, and footer.

In the next image we'll see an example:

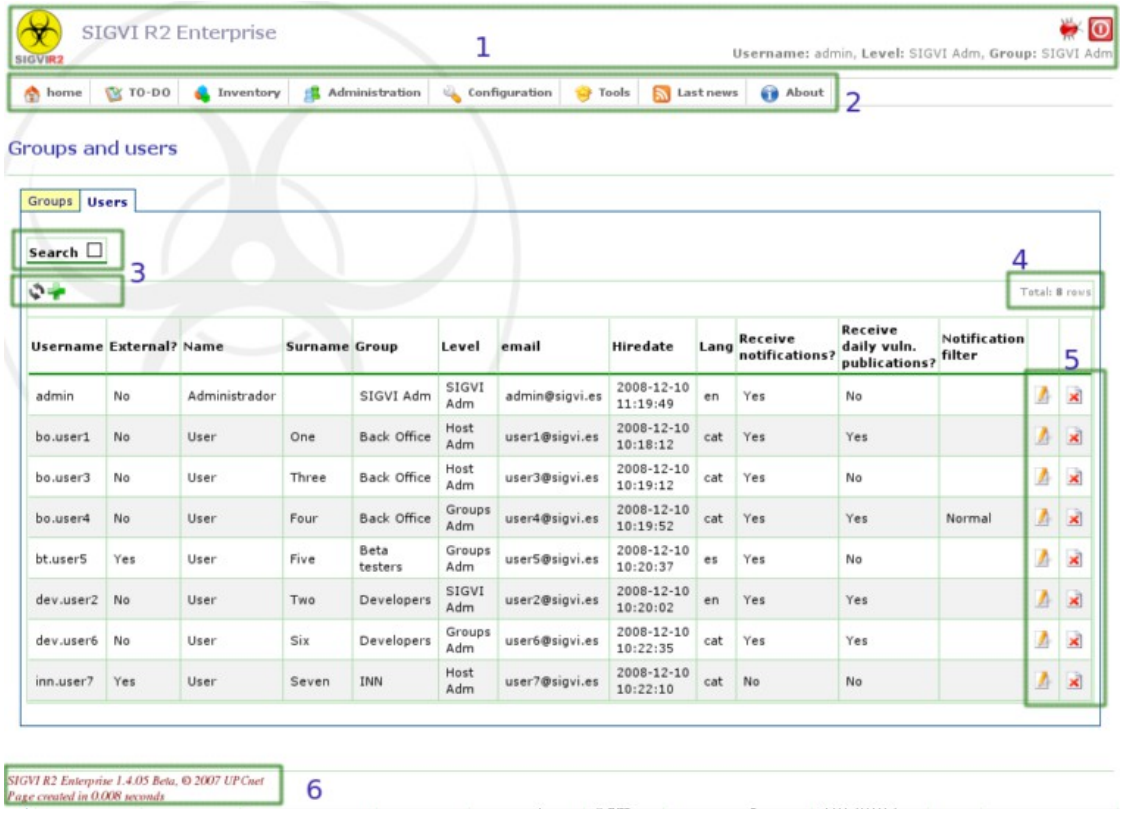


figure 1: Page format

- **1. Logo, title, user information and shortcuts**

  At the top left of the page we see the SIGVI image (which is a link to the initial page) along with the name of the installed version (in this case R2 Enterprise).

  In the upper right there are icons for rapid access to help (in the pages available), the creation of bugs (problems identified in the application) and logout. The bugs management should be enabled from the configuration file of the application (app.conf.php). And finally there are the user information: user name, group and access level.

- **2. Menu**

  The application menu is available from every page and grouped by themes, there are the accesses to the pages of management and implementation tools.

- **3. Search bar and maintenance tool**
  Some maintenance actions use searches to reduce the number of records that appear. Furthermore, if you have permission, you'll see these buttons to add a new record, refresh the search or export the results to a file in CSV format.

- **4. Number of rows displayed**

  Shows the number of records found. If the number of rows that have been found beyond a maximum you'll get a navigation bar with arrows to move through the pages.

- **5. Actions on the records**
  Depending on permissions, you can modify or delete records.
- **6. Page information**

  At the end you can see information about the creation time of the page and the release of this instance.

3. Pages

Let's take a quick look to the pages you'll find in the SIGVI R2. Remember that depending on your user profile, you will see just some of them and you only can perform certain tasks within them.

What is shown below is the view of an SIGVI manager.

***Note**: For this document, and in order to be able to represent the maximum information on the images, the corporate are disabled. They can be enabled in the general configuration file of the application.*

3.1. Login

When you access the SIGVI application, you must authenticate with a valid username and password at the login screen. The authentication can be done either using a local password (stored in the database), or remotely using services arranged for this purpose such as LDAP services.

figure 2: login page

Remember to notify every user what authentication method has to use to access the application.

3.2. Logout

To quit the application you must click the exit or logout link that appears in the header, this will close the session on the server and release all the information stored temporarily. However, the sessions have a limited life span, usually between 5 and 10 minutes, which is defined in the configuration of the Web server that hosts the instance of SIGVI. When that time passes the server automatically closes the session.
Once the session is closed, the next screen that appears when trying to access will be the login page.

3.3. *Main page*

After a proper authentication, you'll go to the main screen and see all the features available to your profile.

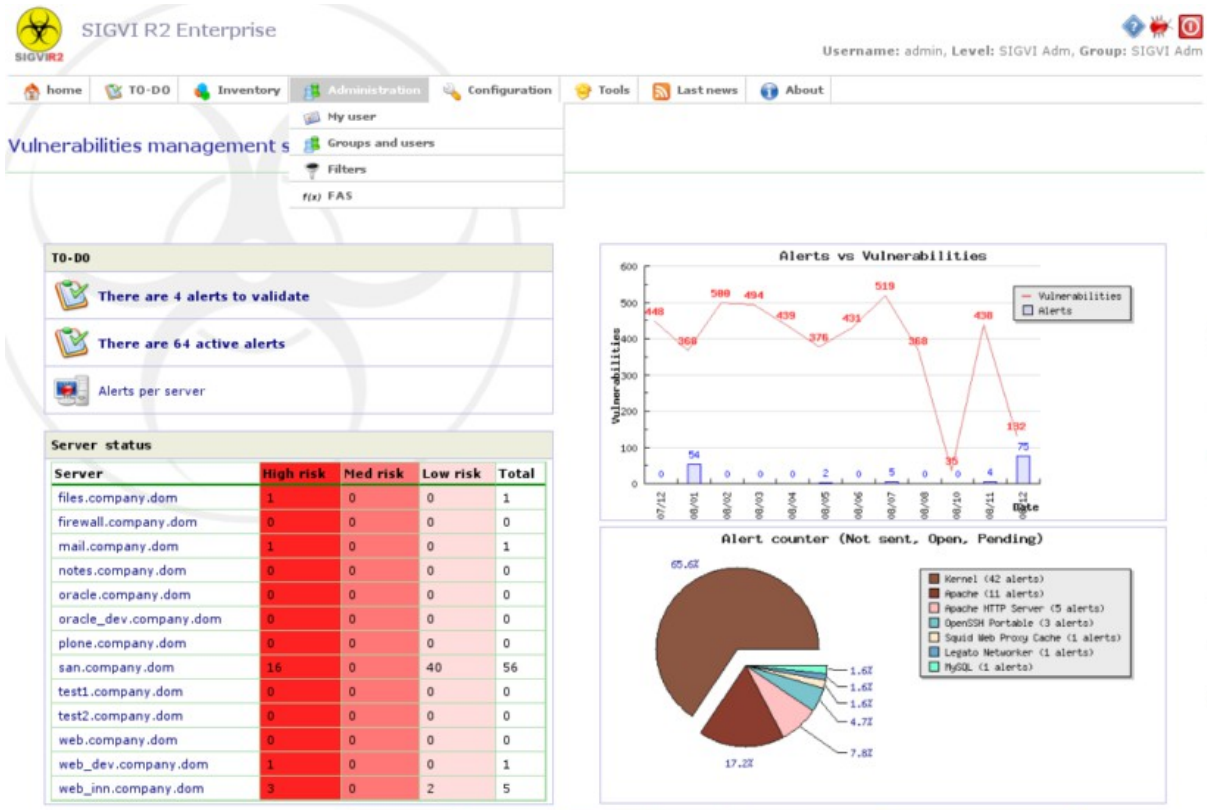


figure 3: main menu

Each of these parts are:

•Menu "TO-DO": You'll see the summary of the overall review and resolution vulnerabilities for the group.

•State of the servers: for each server in its group you'll see the number of vulnerabilities that are affected, ie: the number of open alerts.

•Graphic comparison with the ratio between the number of vulnerabilities and the alerts appeared on your servers in the past year.

•Graphic information about how to split the total alerts depending on the type of software that is affected.

3.4. *TO-DO*

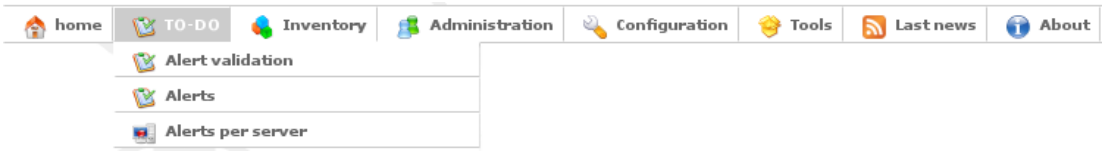


figure 4: TO-DO Menu

There are shortcuts to usual work pages, and indicates a summary of the volume of outstanding tasks. In the case of the equipment manager, there will be a link to the open alerts on servers in his group.

3.4.1. Pending alerts

In some cases, the SIGVI engine may have doubts about whether a vulnerability affects a product from a server. In these cases it is advisable to be reviewed by an administrator, so SIGVI generates an alert as "doubtful", and wait to the be reviewed by a group manager.

These alerts appear on the screen separately and they won't be visible to equipment managers.

The purpose of this feature is to reduce the number of false positives and to not generate more work than necessary.

Group managers will be responsible for reviewing regularly (preferably daily) this alerts in the group. The SIGVI has automatic mechanisms to remind this type of tasks to the managers.

Likewise, after a period defined in the application (default are 48 hours) this pending alerts are passed to "Unsent" state, then they will pass automatically to "Open" state and they will be notified.

3.4.2. Alerts

An alert is created when a product (a software installed on a server offering a service) from a server is affected by a vulnerability. This page will show the warnings of vulnerabilities found on the servers of our group.
Alerts can have 5 different states: Unsent, Open, Closed, Pending, or Discarded. You can manage and track any change.

The different states mean:
•Unsent: the result state from running the check process for vulnerabilities. Then, another process send notifications to the managers of all those alerts, and change their state automatically to "Open". If during the notification process there were any problem affecting the delivery, it will remain in state "Unsent" until the process of sending will be successful.
Setting manually an alert to “Unsent” forces to send a notification to the group managers with the alert.
•Open: the alert is ready to be analyzed.
•Closed: the vulnerability of the alert has been resolved.
•Pending: the alert is pending.
•Discarded: the vulnerability does not affect the product, or simply someone decide to discard it.

By default, in this page we only see our open or pending alerts.

Servers | **Alerts** | Alert validation

Change status for selected rows [ ] Change

Alerts search

Show [Only opened or pending alerts] Server [ ]

Affected product [ ] Vulnerabily [ ]

Note: *You can use SQL wildcards and the logic separators 'or' and 'and', p.e. '%apache% or %mysql%'*

Search | Reset

Total: **8** rows

Showing from row 26 to 33, of 33

	Server	Affected product	Vulnerabily	Creation date	Status	Criticity	Observations	Vulnerability updated	Time of resolution			
26	fileserver.local.net	Ubuntu, Ubuntu Linux, 7.04	CVE-2007-4601	2008/08/28 01:47:30	Open	7.50			0.00			
27	mail.local.net	Microsoft, windows, 2003 Server SP 1	CVE-2007-2228	2008/08/28 01:47:30	Open	8.13			0.00			
28	web.local.net	Apache Software Foundation, Tomcat, 6.0.9	CVE-2007-5342	2008/08/28 01:47:30	Open	9.38			0.00			
29	web.local.net	Apache Software Foundation, Tomcat, 6.0.9	CVE-2008-0002	2008/08/28 01:47:30	Open	4.26			0.00			
30	mail.local.net	IBM, Lotus Notes, 7.0.3	CVE-2008-0066	2008/08/28 01:47:30	Open	4.26			0.00			
31	fileserver.local.net	Drupal, Fileshare_Module, 5.x	CVE-2008-0277	2008/08/28 01:47:30	Open	4.22			0.00			
32	mail.local.net	IBM, Lotus Notes, 7.0.3	CVE-2008-1101	2008/08/28 01:47:30	Open	4.26			0.00			
33	ldap.local.net	redhat, enterprise_linux, ES 4	CVE-2008-1615	2008/08/28 01:47:30	Open	4.76			0.00			

Showing from row 26 to 33, of 33

figure 5: Alerts

3.4.3. Servers alert summary

From the previous page we can access to a summarized view of the number of alerts opened per server, and separated by alert severity:

Servers | Alerts | Alert validation

Server status

Server	High risk	Med risk	Low risk	Total
fileserver.local.net	0	1	1	2
firewall.local.net	2	0	1	3
ldap.local.net	1	0	1	2
mail.local.net	2	0	2	4
oracle.local.net	5	1	2	8
web.local.net	7	1	1	9

figure 6: Server alert summary

3.5. Inventory menu

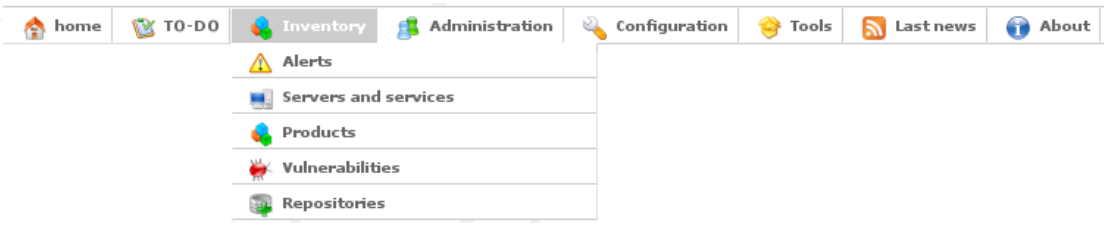


figura 7: Menú de inventario

In this menu we have the links related to administering alerts, servers, products, vulnerabilities and repositories.

3.5.1. Alerts

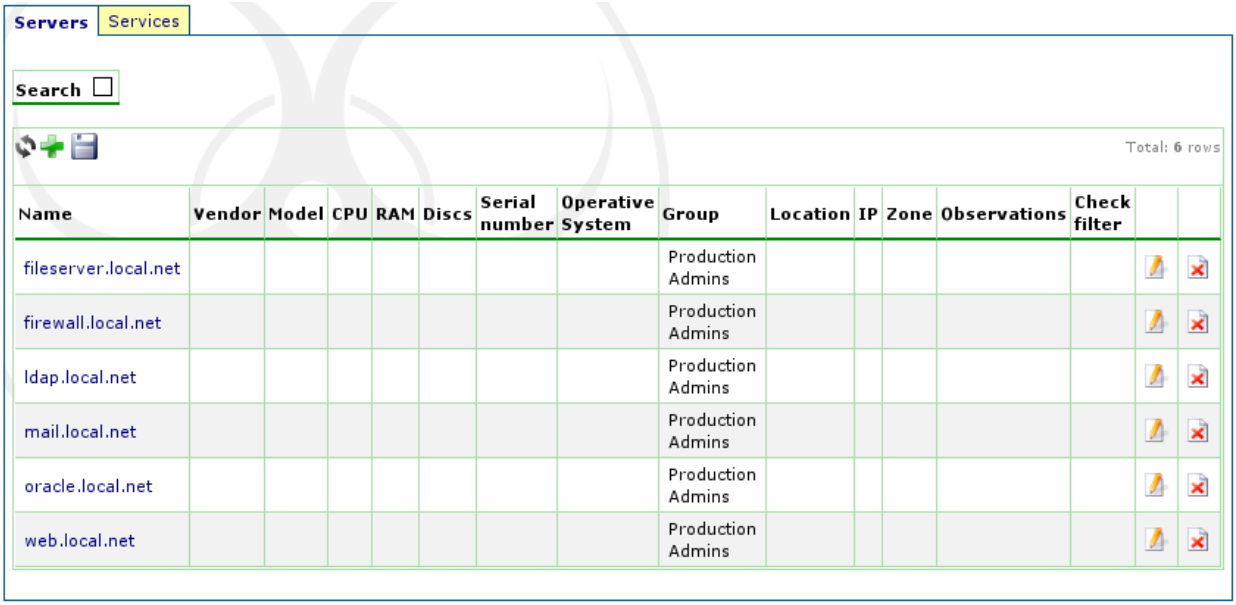
This link leads to alert management page described in section 3.4.2.

3.5.2. Servers and products

This is the entry point of information about servers and products, we have to reflect all as faithfully as possible. There is two tabs, one for servers and other for products.

Servers

In this first tab, there are all the servers from your group. As a equipment manager you can add and modify the server list. The data of the servers are quite arbitrary, we only use the server name and the filter (if one is indicated). The rest is descriptive information. A server may not be repeated within a group.



Name	Vendor	Model	CPU	RAM	Discs	Serial number	Operative System	Group	Location	IP	Zone	Observations	Check filter		
fileserver.local.net								Production Admins							
firewall.local.net								Production Admins							
ldap.local.net								Production Admins							
mail.local.net								Production Admins							
oracle.local.net								Production Admins							
web.local.net								Production Admins							

figure 8: Servers

Services: Products installed on servers

The second tab shows the products installed on servers. Add all the products per server can be a very hard work, and in some environments it will be impossible to maintain up to date all the data.

At the very beginning, it's recommendable to start only by detecting vulnerabilities at the operating system and on products offering services visible from the outside from our company, Internet, there are the most important alerts.

But, there is another project, developed in parallel with SIGVI, named NSDi. This project detects automatically the list of services and products (some of them) from all of our servers. Now, there is an alpha version that permits the integration with SIGVI but needs a lot of development as well.

Note: there is an application named nmap *(http://nmap.org/)* that can be used to detect the services from one server.

In this image we can see the software list on our servers:

Servers | Services

Search

Total: 13 rows

Server name	Product Identifier (review products list)	Is service filtered? (is not public)	Is a critical service?	Ports	Transmission Protocol (TCP,UDP,...)		
mail.local.net	Microsoft, windows, 2003 Server SP 1	Yes	No				
mail.local.net	IBM, Lotus Notes, 7.0.3	No	Yes				
web.local.net	Apache Software Foundation, Tomcat, 6.0.9	No	Yes				
web.local.net	Ubuntu, Ubuntu Linux, 7.04	Yes	No				
web.local.net	PostgreSQL, PostgreSQL, 8.2.5	Yes	Yes				
firewall.local.net	Netfilter Core Team, iptables, 1.2.3	No	Yes				
firewall.local.net	Ubuntu, Ubuntu Linux, 7.04	Yes	Yes				
oracle.local.net	Sun, Solaris, 5.6	Yes	Yes				
oracle.local.net	Oracle, Oracle10g Database Server Release 2, 10.2.0.3	No	Yes				
fileserver.local.net	Ubuntu, Ubuntu Linux, 7.04	Yes	No				
fileserver.local.net	Drupal, Fileshare, Module, 5.x	No	Yes				

figure 9: Services: products installed on servers

As we can see, there is only products that are offering a service. When we add a product, we must assign it to a server and inform about the accessibility from outside (if it's filtered or open) and if it is a critical service.

There is no rule to define how critical is a service, it depends on our judgment, we have to consider the chain of problems produced by this server attacked. For instance: the web server with our company web page, an LDAP service which authenticates users or services, etc.

The other fields are used only for description.

3.5.3. Products

This view is the products repository, a global list of all products. We can look for the products added to the system, and from this list we can find the products related to the servers.

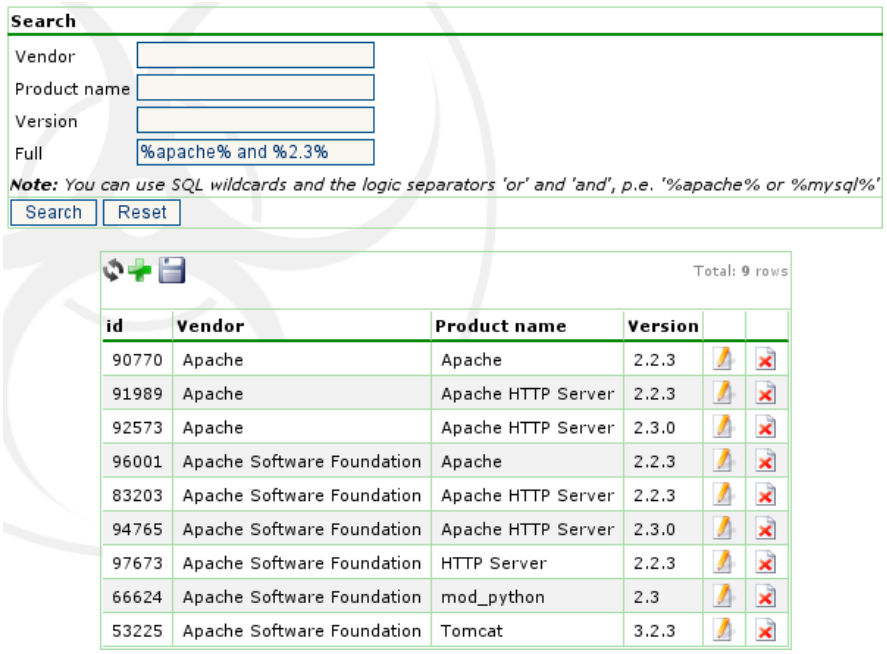


figure 10: Products repository

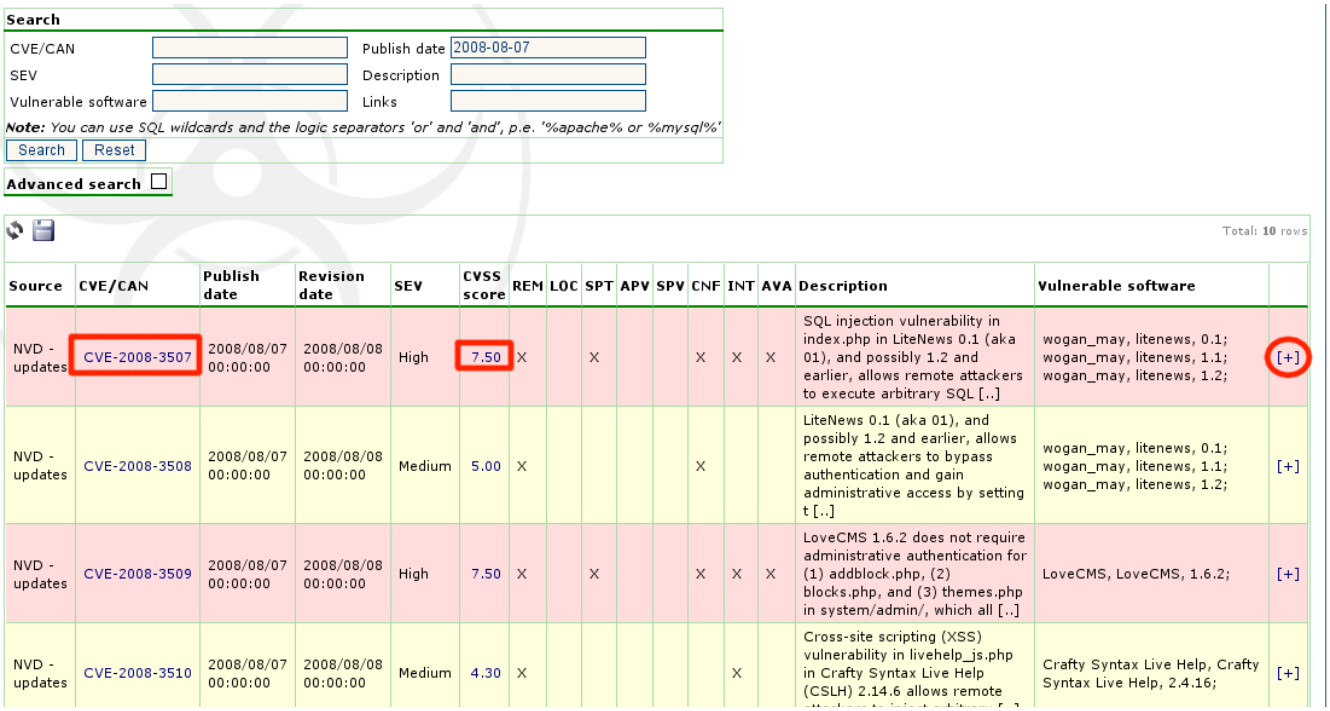
This list is created from the services or software marked as vulnerable and added from users. A service without vulnerability won't appear on this list automatically, we have to add manually.

It may occur that we have to associate a service that we don't have on our list, then we have to add it ourselves. This is a critic point in configuring the application, we can determine a vulnerable service by its name in comparison with the name provided by the Internet vulnerability provider, if that name is not exactly the same the application will miss the vulnerabilities.

Advice: each vendor uses a fixed schema for naming its products, we recommend to look for this schema when we have to add a product by ourselves.

3.5.4. Vulnerabilities

In this view we can see the vulnerability repository from today and all the vulnerabilities added by the batch process imported from different sources.



Search

CVE/CAN | Publish date 2008-08-07
SEV | Description
Vulnerable software | Links

Note: You can use SQL wildcards and the logic separators 'or' and 'and', p.e. '%apache% or %mysql%'

Search | Reset

Advanced search

Total: 10 rows

Source	CVE/CAN	Publish date	Revision date	SEV	CVSS score	REM	LOC	SPT	APV	SPV	CNF	INT	AVA	Description	Vulnerable software	
NVD - updates	CVE-2008-3507	2008/08/07 00:00:00	2008/08/08 00:00:00	High	7.50	X		X			X	X	X	SQL injection vulnerability in index.php in LiteNews 0.1 (aka 01), and possibly 1.2 and earlier, allows remote attackers to execute arbitrary SQL [..]	wogan_may, litenews, 0.1; wogan_may, litenews, 1.1; wogan_may, litenews, 1.2;	[+]
NVD - updates	CVE-2008-3508	2008/08/07 00:00:00	2008/08/08 00:00:00	Medium	5.00	X					X			LiteNews 0.1 (aka 01), and possibly 1.2 and earlier, allows remote attackers to bypass authentication and gain administrative access by setting t [..]	wogan_may, litenews, 0.1; wogan_may, litenews, 1.1; wogan_may, litenews, 1.2;	[+]
NVD - updates	CVE-2008-3509	2008/08/07 00:00:00	2008/08/08 00:00:00	High	7.50	X		X			X	X	X	LoveCMS 1.6.2 does not require administrative authentication for (1) addblock.php, (2) blocks.php, and (3) themes.php in system/admin/, which all [..]	LoveCMS, LoveCMS, 1.6.2;	[+]
NVD - updates	CVE-2008-3510	2008/08/07 00:00:00	2008/08/08 00:00:00	Medium	4.30	X						X		Cross-site scripting (XSS) vulnerability in livehelp_js.php in Crafty Syntax Live Help (CSLH) 2.14.6 allows remote	Crafty Syntax Live Help, Crafty Syntax Live Help, 2.4.16;	[+]

figure 11: Vulnerability repository

Every vulnerability has three links:

- CVE/CAN, links to the source page where this vulnerability was published (http://nvd.nist.gov/nvd.cfm). This was made for the CVE standard.
- CVSS, links to the NVD page (http://nvd.nist.gov/cvss.cfm) where we can see the information on the CVSS vector, following the CVSS standard.
- [+], links to more information that can provide SIGVI

3.6. Administration menu

figure 12: Administration menu

In this menu we have the links related to administering users, groups and filters.

3.6.1. My user

From this page you can modify your data:

Total: 1 rows

#1	
Username	admin
External?	No
Name	Administrador
Surname	
Group	SIGVI Adm
email	sebastian.gomez@upcnet.es
Level	SIGVI Adm
Hiredate	2008-08-10 00:24:25
Lang	en
Receive notifications?	Yes
Receive daily vuln. publications?	No
Notification filter	

figure 13: My user

- Username: The name you'll use to login on the application. This is a mandatory field.
- External: Assigned to “yes” implies that this user will authenticate with the authenticated system defined in this SIGVI instance. Assigned to “no” you must fill the password field.
- Name: The user name. This is a mandatory field.
- Surname.
- Group: A user have to belong to a group to set his permissions to see or manage data. In general a non-administrator user only can see and manage his group data. This is a mandatory field.
- Email: This is the email that the application will use to send the summaries or alerts from the batch processes.
- Level: The access level to the data. It's impossible to auto-increment this level, and this value will limit the access to the group data. Then, for example, an equipment administrator can't modify data from other users in his group. This is a mandatory field.
- Hire date: When the user was created. This is a read-only field.
- Receive notifications?: set to “no” if you don't want any summary or alert in your email.
- Receive daily vulnerability notification?: set to “no” if you don't want to receive the daily vulnerability notification as a result from the batch process of loading vulnerabilities.

3.6.2. Groups and users

There are the views for manage the application users and groups. Only the users with the “SIGVI manager” profile can see and manage the groups, and only the users with the “group manager” profile can see and manage users.

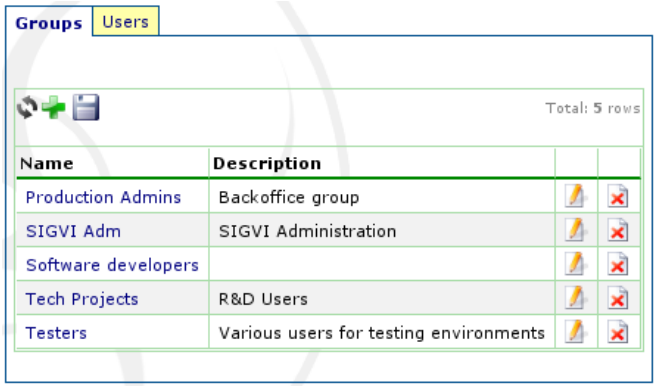


figure 14: Groups

The group name is an obligatory field and must be unique. The description is optional.

The groups will be used to group users and the resources related (servers, installed products on servers, alerts, etc.)

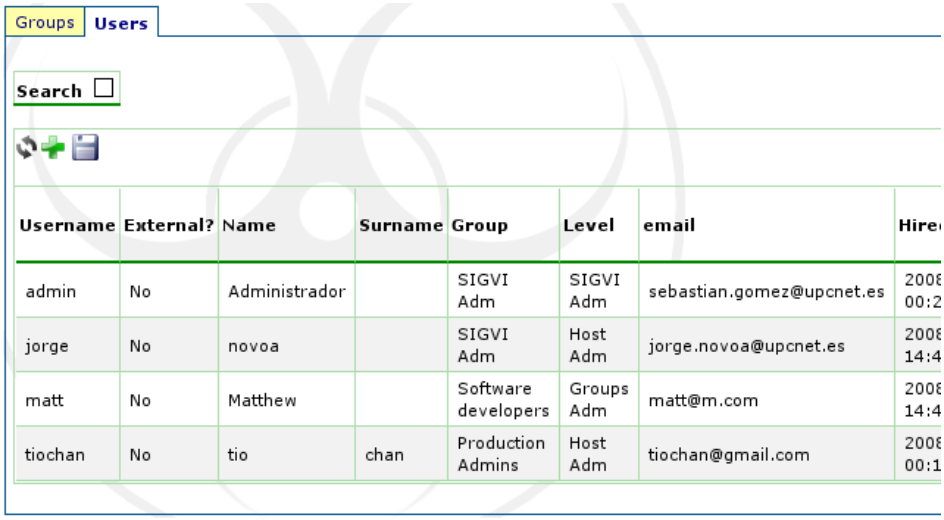


figure 15: Users

The data related to the users are the same presented and explained in the previous section “My user”.

3.6.3. Filters

We use filters for different things:

•to separate vulnerabilities when we use them.: when a product is affected, in the daily summary, etc.

•to send the daily summary to the users, every user can have his own filter.

•In server management, telling what filter we have to use in case one of our servers will be affected.

•Using filters adequately can reduce the number of alerts and improve personal efficiency. In many cases, having a lot of servers offering services, it's necessary to dismiss directly some type of vulnerabilities. For example, the vulnerabilities that require physical access to exploit, this is a basic filter defined by default.

Every user can set his own filters:

Total: 4 rows

Name	Grup	TYPE	SEV	REM	LOC	SPT	APV	SPV	CNF	INT	AVA	VAL	CON	OVF	AVE	ECE	ENV	CNF	RCN	OTH	Description		
Only REMOTELY EXP		Pass if all are equal		Yes																	Use to get only vulnerabilities that can be exploided remotely.		
High severity		Pass if all are equal	High																		Use to get only vulnerabilities rated as High		
Denial Of Service (DoS)		Pass if all are equal		Yes							Yes										To get only vulnerabilities that which consequences are DoS (Denial of Service)		
Normal		Pass if all are equal		Yes							No										DoS vulnerabilities that can be exploided remotely		

figure 16: Filters

Definition

The criteria used in filtering is based on the standardized fields from a vulnerability:

- Severity (high, medium, low)
- Is remotely exploitable? (yes/no)
- Consequences (lost of information, gain privileges, etc.)
- Type (error on authenticate, buffer overflow, etc.)

Furthermore, a filter can be created for one group or for every group.

An equipment manager only can see the filters created in his group or the global filters, but he can't modify any of them.

¿How it works?

When you create a filter you decide how it will work:

- Continue processing if all conditions are satisfied with that vulnerability.
- Continue processing if one condition is satisfied with that vulnerability.
- Apply filter if all conditions are satisfied with that vulnerability. The vulnerability won't be processed.
- Apply filter if one condition is satisfied with that vulnerability. The vulnerability won't be processed.

Uses

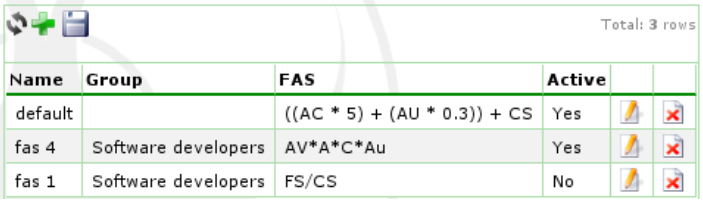
Filters have different goals:

- Select the vulnerabilities announced as an alert in a server. When a vulnerability affects a server product, if we have created a filter in the server definition, the application will use that for decide to create an alert. In this case, an easy form for dismiss vulnerabilities that need physical access to exploit is to apply this filter in the server definition.
- Select what vulnerabilities will be announced in the vulnerability summaries. Every user can apply a filter (in the user definition) for select the type of vulnerabilities he want to be noticed. For

example, an user can decide only to be notified for serious (high severity) vulnerabilities.

3.6.4. FAS

FAS stands for Final Absolute Severity.



Total: 3 rows

Name	Group	FAS	Active		
default		((AC * 5) + (AU * 0.3)) + CS	Yes		
fas 4	Software developers	AV*A*C*Au	Yes		
fas 1	Software developers	FS/CS	No		

Figure 17: Final Absolute Severity

This function will be used for determining the alert gravity. Remember that an alert is a server product affected by a vulnerability.

This value is used to inform about the gravity in that situation, it includes information from the vulnerability and from the service in that affected server.

In this three situations, what is more severe?

- A high severity vulnerability affecting an Apache service which has our corporative web. This is public service and can be exploited from outside.
- A high severity vulnerability affecting our MySQL service. This server is accessible only form our network and it's filtered from the outside, but the vulnerability can be exploited from outside.
- A high severity vulnerability affecting our LDAP authentication service installed on a public server. This service is used for most of our applications and the vulnerability needs physical access to be exploitable.

Every manager will answer differently. With FAS you can set your priorities.

¿What FAS I need?

We associate a FAS per group, that will affect all the servers in that group. A server without FAS assigned will use a global FAS.

Only the group manager or the SIGVI manager can modify or assign FAS to a group or for all groups respectively.

FAS decision workflow:

- If the server group has an **active** FAS, we'll use that for create the alert.
- If there is a global FAS (not assigned to any group), we'll use that.
- Else, we'll use the default FAS defined in the application, the value included in the vulnerability itself.

¿How to create a FAS?

Based on the data from the vulnerability itself and from the service we must create a mathematical function with an integer as a return value.

There are the variables we can use:

Acronym	Variable	Value

CS	Criticity Service	• 0: not critical • 1: critical
FS	Filtered Service	• 0: not filtered • 1: filtered
BS	Base Score	(0.6*Impact + 0.4*Exploitability - 1.5)*f(Impact)
Imp	Impact	10.41*(1 - (1-ConfImpact)*(1-IntegImpact)*(1-AvailImpact))
Exp	Exploitability	20*AccessComplexity*Authentication*AccessVector
Fimp	f(Impact)	• 0 if Impact=0 • 1.176 otherwise
AC	Access Complexity	• high: 0.35 • medium: 0.61 • low: 0.71
AU	Authentication	• Requires no authentication: 0.704 • Requires single instance of authentication: 0.56 • Requires multiple instances of authentication: 0.45
AV	Access Vector	• Requires local access: 0.395 • Local Network accessible: 0.646 • Network accessible: 1
C	Confidentiality Impact	• None: 0 • partial: 0.275 • complete: 0.660
I	Integrity Impact	• none: 0 • partial: 0.275 • complete: 0.660
A	Availability Impact	• None: 0 • partial: 0.275 • complete: 0.660

CS and FS are set by the service characteristics, obtained by the relation between server and product. The other variables are obtained by the characteristics of the vulnerability.

3.7. Configuration menu

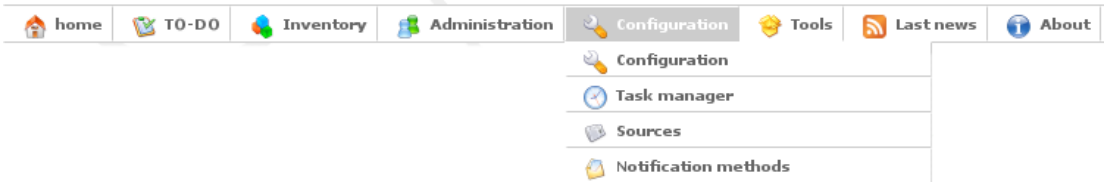


figure 18: Configuration menu

There are a set of tools only suitable for group managers and SIGVI managers.

3.7.1. General configuration

From this page you can configure the global parameters for the application.

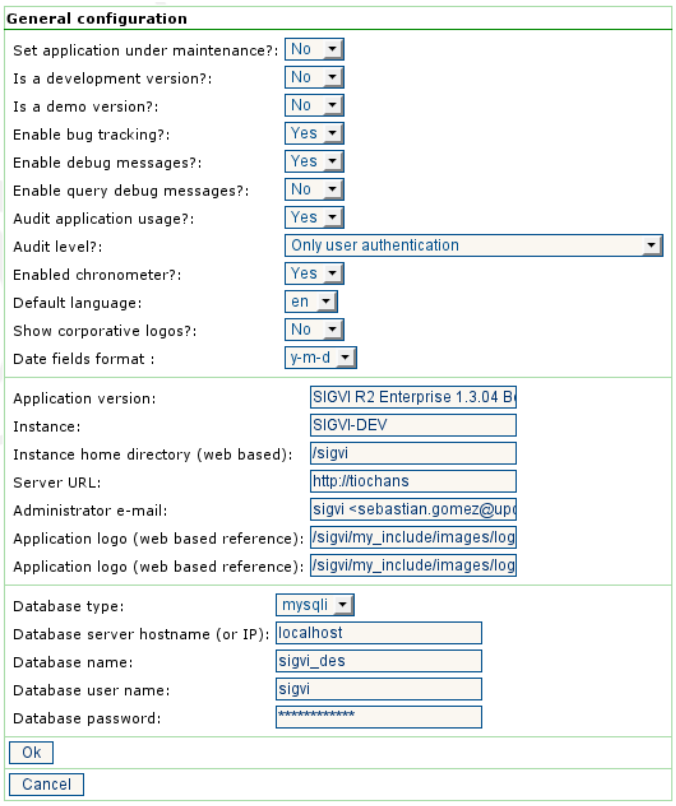
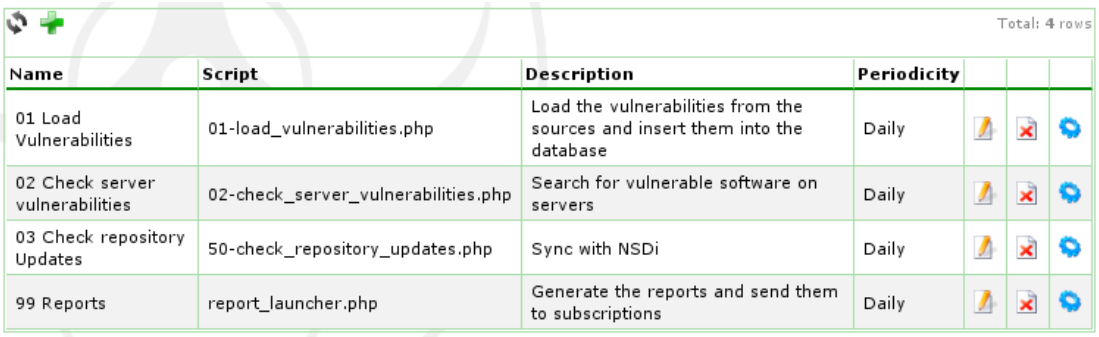


figure 19: General configuration

This page is under development and it's suitable to edit manually the configuration file. For more information go to the Administrator Manual.

3.7.2. Task manager

This page is accessible only by a SIGVI manager for modify the batch processes.



Total: 4 rows

Name	Script	Description	Periodicity			
01 Load Vulnerabilities	01-load_vulnerabilities.php	Load the vulnerabilities from the sources and insert them into the database	Daily			
02 Check server vulnerabilities	02-check_server_vulnerabilities.php	Search for vulnerable software on servers	Daily			
03 Check repository Updates	50-check_repository_updates.php	Sync with NSDi	Daily			
99 Reports	report_launcher.php	Generate the reports and send them to subscriptions	Daily			

figure 20: Task manager

All entries listed are PHP scripts located in the directory <sigvi_home>/cron. We can create as many entries as necessary. By default, we provide the minimum necessary set of scripts for running SIGVI properly.

It's possible to indicate how often you want to run: daily (every day), weekly (every Monday), monthly (the 1st of each month) or never, and you can start every task individually with the right icon of each row. This will cause to run the process immediately showing the results on the implementation screen.

More information about tasks can be found at the Installation Guide.

3.7.3. Sources

From this page we can manage the sources of vulnerabilities, RSS feeds and sources of product dictionaries (CPE support).

Vulnerability sources

Sources of vulnerabilities are one of the key pieces to get the system updated. To download a source of vulnerabilities there should be a plugin that is capable of downloading data, parsing and loading them in a database.

In the technical documentation is explained in detail how to create a parser for a particular source, but broadly it is to fill an array with instances of a class that defines the vulnerabilities characteristics.

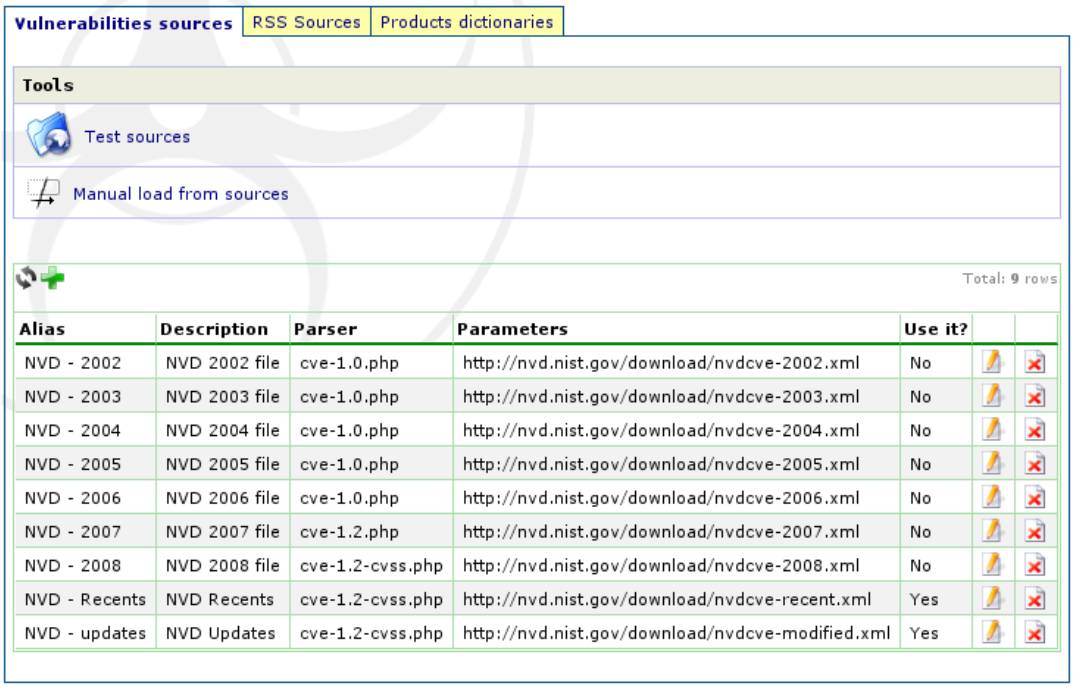
SIGVI uses the format specified by the CVE standard and provide the necessary plugins to download the vulnerabilities available in that format.

As can be seen in the figure below, there are different formats of CVE, which correspond to the evolution of it. Is not necessary to have activated all sources, just as in this case, those who have enabled only show recent changes.

Only it is advisable to activate all (and one by one) in the first load a new instance of SIGVI. The night download vulnerabilities process will process each enabled source (field "Use it" as true).

At the top of the window there are two links to tools:

- Test a vulnerability source. This is useful for checking whether the plugin works correctly. It's a simulation of a source without actually storing the data in the database, only displaying information useful for determining whether the "parser" works correctly or not.
- Manual loading. Run the nightly process to load all the vulnerabilities from sources.



Alias	Description	Parser	Parameters	Use it?		
NVD - 2002	NVD 2002 file	cve-1.0.php	http://nvd.nist.gov/download/nvdcve-2002.xml	No		
NVD - 2003	NVD 2003 file	cve-1.0.php	http://nvd.nist.gov/download/nvdcve-2003.xml	No		
NVD - 2004	NVD 2004 file	cve-1.0.php	http://nvd.nist.gov/download/nvdcve-2004.xml	No		
NVD - 2005	NVD 2005 file	cve-1.0.php	http://nvd.nist.gov/download/nvdcve-2005.xml	No		
NVD - 2006	NVD 2006 file	cve-1.0.php	http://nvd.nist.gov/download/nvdcve-2006.xml	No		
NVD - 2007	NVD 2007 file	cve-1.2.php	http://nvd.nist.gov/download/nvdcve-2007.xml	No		
NVD - 2008	NVD 2008 file	cve-1.2-cvss.php	http://nvd.nist.gov/download/nvdcve-2008.xml	No		
NVD - Recents	NVD Recents	cve-1.2-cvss.php	http://nvd.nist.gov/download/nvdcve-recent.xml	Yes		
NVD - updates	NVD Updates	cve-1.2-cvss.php	http://nvd.nist.gov/download/nvdcve-modified.xml	Yes		

Figure 21: Vulnerability sources manager

Managing the RSS sources

At this page we can add as many news feeds as we need, if these sources have the same pattern for the

default parser. Any other sources that do not use this pattern will require a special parser. How to create a parser for this purpose is discussed in the technical documentation.

The page from which you can view the sources contents will be accessed from the News menu.

Vulnerabilities sources | **RSS Sources** | Products dictionaries

Total: 4 rows

Alias	Description	Parser	Parameters	Use it?		
NVD RSS All		rss_reader.php	http://nvd.nist.gov/download/nvd-rss.xml	Yes		
NVD RSS Analyzed		rss_reader.php	http://nvd.nist.gov/download/nvd-rss-analyzed.xml	No		
Red Hat RSS Alerts		rss_reader.php	http://search.techrepublic.com.com/search /red+hat+inc.+and+vulnerability.html?t=0&s=0&o=1& mode=rss	No		
Sun Alert		rss_reader.php	http://blogs.sun.com/security/feed/entries/rss	No		

figure 22: Managing RSS sources

Managing product dictionaries (CPE)

This page is for the CPE SCAP product compatibility. This is only for informational purposes.

Vulnerabilities sources | RSS Sources | **Products dictionaries**

Tools

Test sources

Manual load from sources

Total: 2 rows

Alias	Description	Parser	Parameters	Use it?		
CPE 1.0	NVD CPE Dictionary, version 1.0	cpe-1.0.php	http://nvd.nist.gov/download/cpe-dictionary.xml	No		
CPE 2.1	NVD CPE Dictionary, version 2.1	cpe-2.1.php	http://nvd.nist.gov/download/cpe-dictionary-v2.1-20080421.xml	No		

Figure 23: Products dictionaries

3.7.4. Notification methods

By default, we provide the email method to send alerts to users using email.

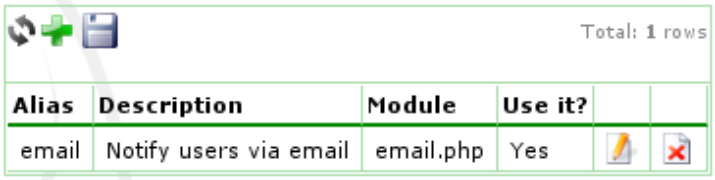


figure 24: Notification methods

In the technical documentation is explained how to create new notification methods.

3.8. Tools menu

From this menu we access to various application tools. Some are accessible only by SIGVI Managers or group users.

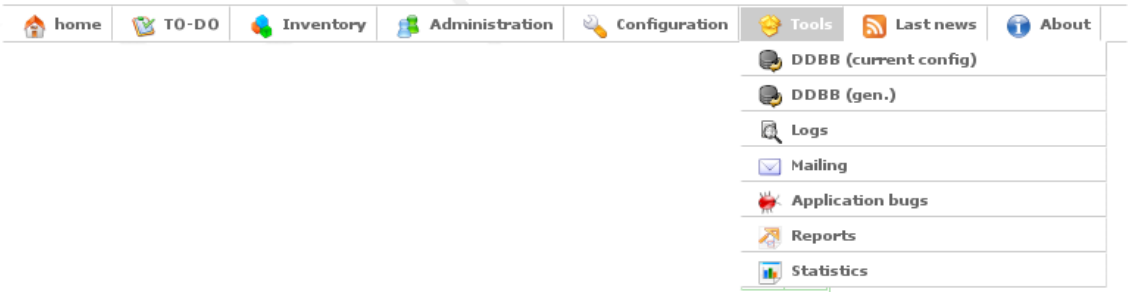


figure 25: Tools menu

3.8.1. Data base (DDBB)

This is a tool (only for SIGVI Managers) used to interact with any database application supported by the SIGVI library (Oracle, Postgres and MySQL).

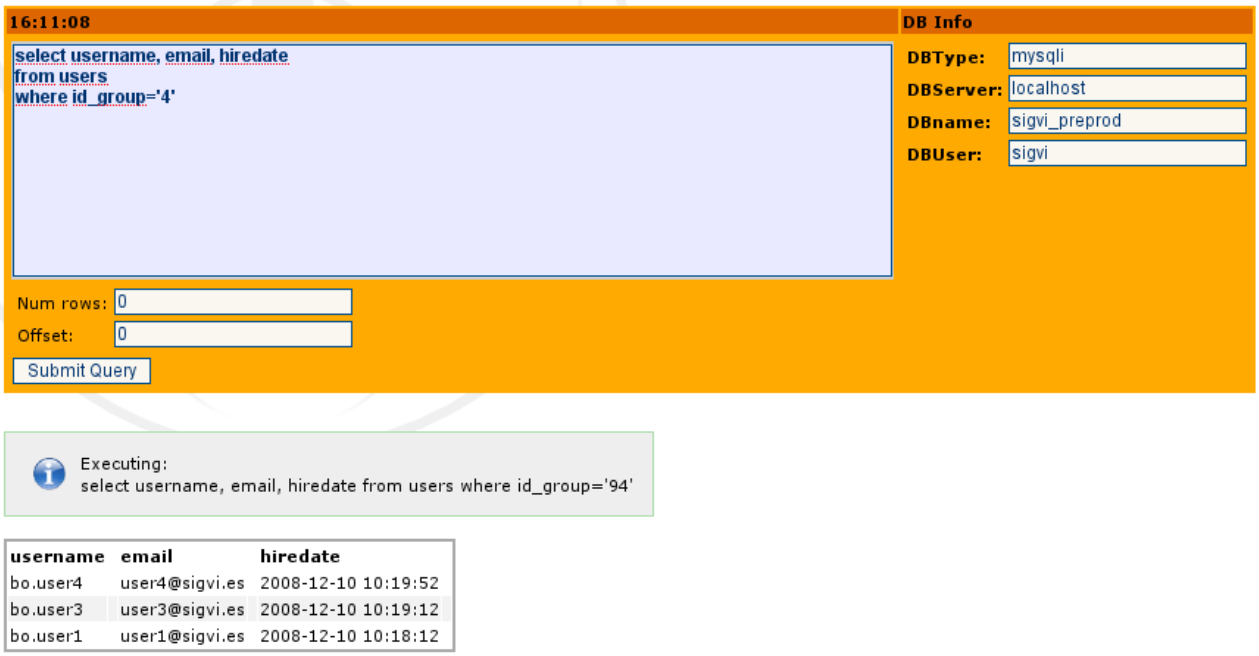


figure 26: Database interaction

3.8.2. Logs

This is an auditory system to show all changes made to the database (only by SIGVI manager): time,

origin and the user who caused it. You can store shortcuts to maintenance, correct entries in the application, login and logout to the application, authentication attempts, changes to records in the database (with old values and new values, etc.).

Through the general configuration file we decide whether audit is performed, and level. For more information see the technical documentation.

#	Date	User Id	Username	Level	Source	Module	Register
6908	2008/08/28 02:04:45	0	admin	SIGVI Adm	127.0.1.1	DBMS	update filters set name='Normal',id_group=null,f_type='0',severity='0',ar_la vulnerabilities that can be exploided remotely' where id_filt
6909	2008/08/28 02:04:45	0	admin	SIGVI Adm	127.0.1.1	FORM	Row modified on table filters, OLD Values(6,6,Normal,,0,0,1
6906	2008/08/28 02:03:29	0	admin	SIGVI Adm	127.0.1.1	DBMS	delete from filters where id_filter='5'
6907	2008/08/28 02:03:29	0	admin	SIGVI Adm	127.0.1.1	FORM	Row deleted on table filters, Values(5,5,prueba,,0,2,0,0,0,0
6905	2008/08/28 01:19:03	0	admin	SIGVI Adm	127.0.1.1	AUTH	User logged in
6904	2008/08/28 01:15:42	0	admin	SIGVI Adm	127.0.1.1	AUTH	User logged out

figure 27: Application Logs

3.8.3. Mailing

There is a simple mail interface to send emails to application users. We can send a mail to one or more groups, or send a mail to one or more profiles, or one or more users. If you select more than one block, the application will use only the first selected block. Finally fill the "Subject" and “Content” fields and click the button "Send".

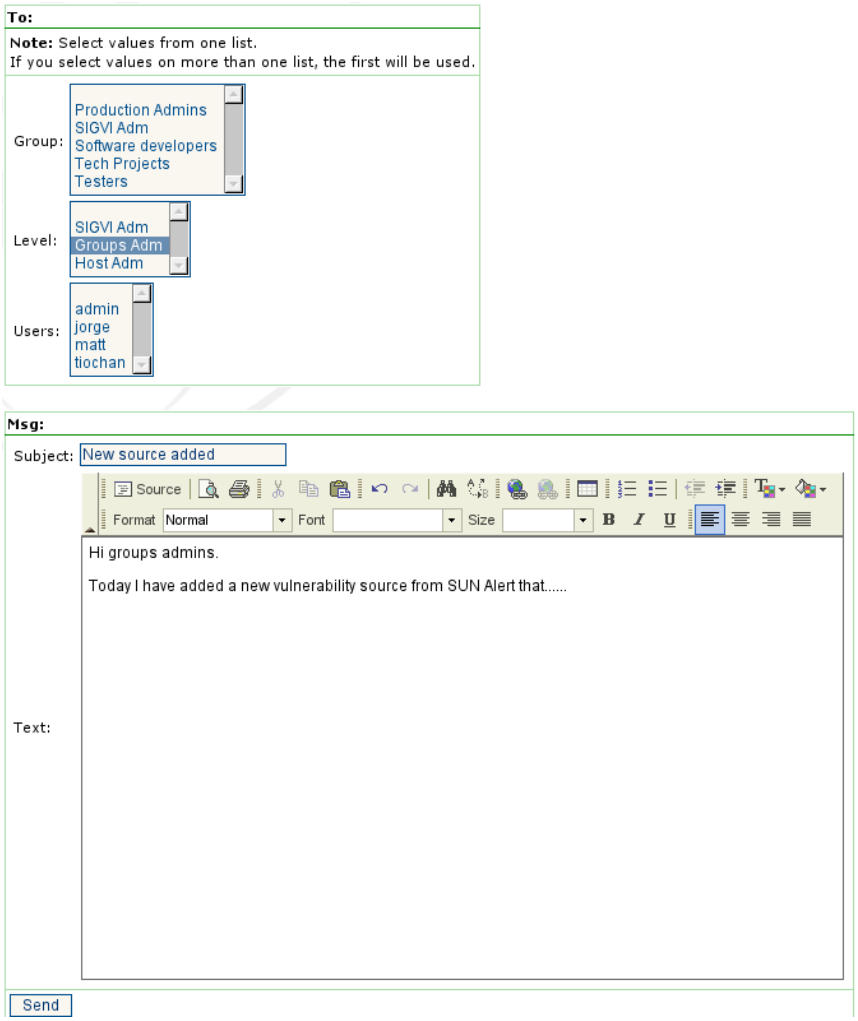


figure 28: Mailing

3.8.4. Application Bugs

This utility is designed to inform on the existence of a bug in the application for development versions. This option should be disabled in a real SIGVI instance.
However, despite being a simple interface it can be used for other purposes, a manager decision.

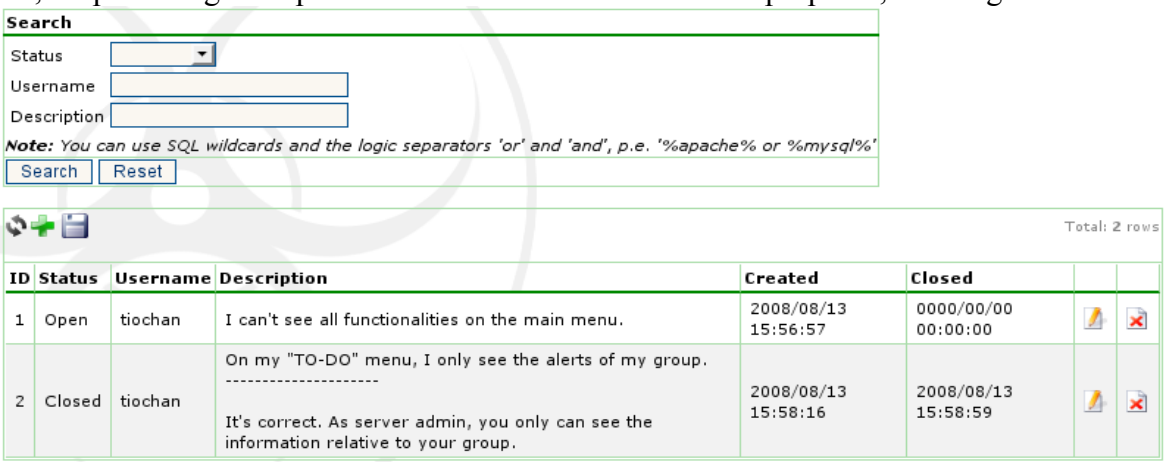


figure 29: Bugs

3.8.5. Reports

Our reports are designed as documents that may contain dynamic elements (tags) and to which anyone can subscribe if belongs to the group to which they were created.
In the task manager you can see the process that performs the daily execution reports. This process replace the tags or dynamic elements creating a document and sent it by email to the user.

A report can be created by a SIGVI manager or by a group manager, and any user or a user in that group can subscribe to it respectively.

A report has a defined periodicity. So we can create reports that run daily, weekly (every Monday), monthly (every day for 1 month) or never.

The reports are particularly useful for people who manage a group to receive data without having to periodically go the application.

Subscriptions to reports

This page is available to all users and everyone can see their own subscriptions. As usual, only the SIGVI manager can see all subscriptions.

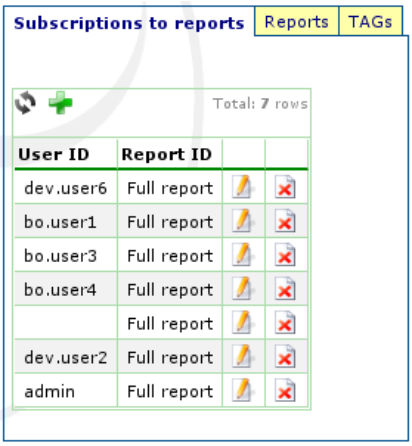


figure 30: Subscriptions to reports

Each execution of a subscribed report involves sending an email, unless we have disabled sending email to our profile (see 3.6.1).

Reports

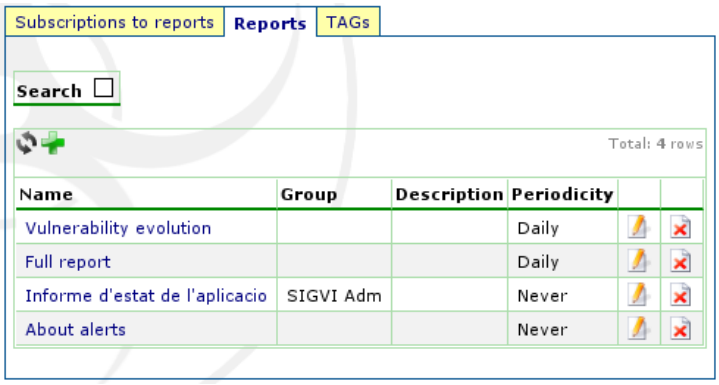


figure 31: Reports

The creation fields are:

- Name: The name of the report to which reference may be made,
- Group: If this is blank it may be used by any user of any group, whether a group is set only users of

that group have access to it.

- Content is the report itself. It is a rich text field that you can edit using the web editor. Within the report you may interspersed tags from the drop-down list that is just above or type in manually, that will be replaced by a value at the time of execution.
- Description: about the contents of the report
- Periodicity: daily, weekly, monthly or never.

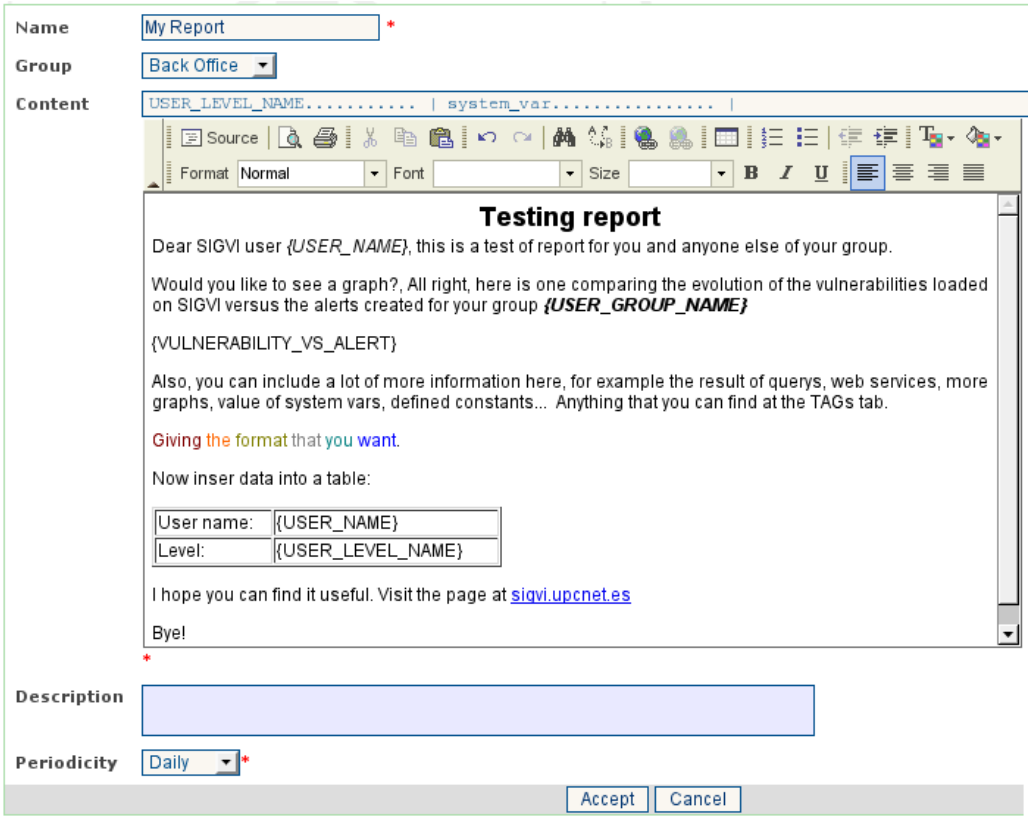


figure 32: Creating a report

Finally, we can preview the result. It should be remembered that many of the tags extract information from the user which that report is being created, and we'll obtain this data when it'll be launched from the batch process for each subscription. In the preview result, we use the user information that is making the report.

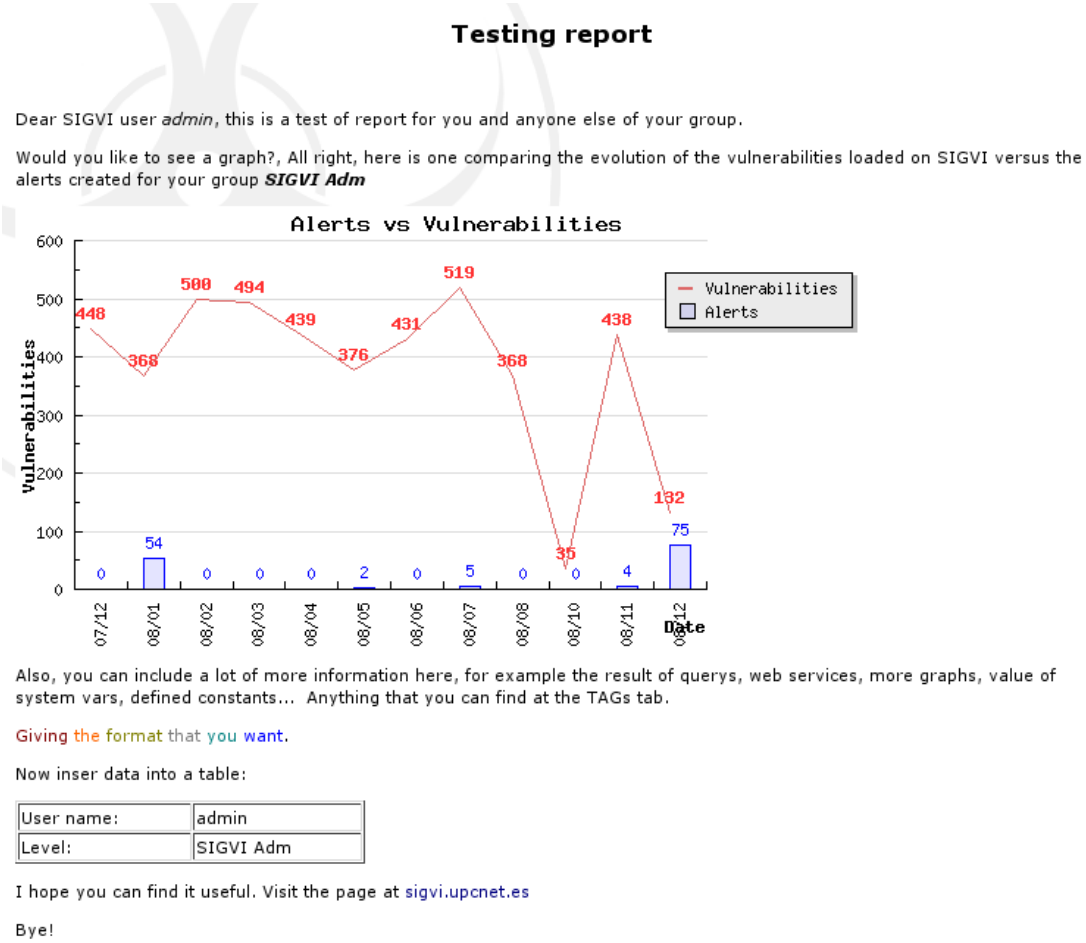


figure 33: Previsualizing a report

TAGs

These are the parts which we can build a dynamic report. The tags can be created only by a SIGVI manager given a query to the database.

This is a fragment of the original list:

Subscriptions to reports | Reports | TAGs

Search

Total: 25 rows

Showing from row 1 to 25, of 27

Name		Value	Description	Is public?		
ALERT_CLOSED_LAST_MONTH	Query	select count(*) from alerts a, servers s wh [..]	Total number of alerts closed last month for user group	Yes		
ALERT_DISCARDED_LAST_MONTH	Query	select count(*) from alerts a, servers s wh [..]	Total number of alerts discarded last month for user group	Yes		
ALERT_LAST_MONTH	Query	select count(*) from alerts a, servers s wh [..]	Number of alerts created last month	Yes		
ALERT_OPENED_LAST_MONTH	Query	select count(*) from alerts a, servers s wh [..]	Number of alerts still opened last month for the user group	Yes		
ALERT_PROGRESS	Graph	alert_progress	Bar graph that represents the alerts generated each month	Yes		
ALERT_STATUS	Graph	alert_status	Pie graph that represents each kind of alerts over the total	Yes		

figure 34: TAGs

A TAG may turn to other tags, which can end up in recursive tags. In this version of the reports it's only detected one level in recursion, we must take some care with this aspect since the process would end when they fill the memory associated with the process.

The tags can be of different types:

- Constant: the value is indicated directly in the "value" field.
- Graph: a reference to a PHP script that generates graphs
- Image: a reference to an image
- Operation: allows simple arithmetic operators (+, -, …)
- Query: a query to a database that returns a single value.
- Var: a variable from the application
- Web Service: make a call to a Web Service (in a specified format)

Finally it may be indicated if the TAG is global or not. If global it can be used by any user who can create a report. If not, it can be used only by SIGVI managers, both in a report and as referenced at runtime.

3.8.6. Statistics

Int his page we'll see predefined reports showing global data extracted from SIGVI.

- Vulnerability counter: shows the evolution of appeared vulnerabilities from the last year, every month.

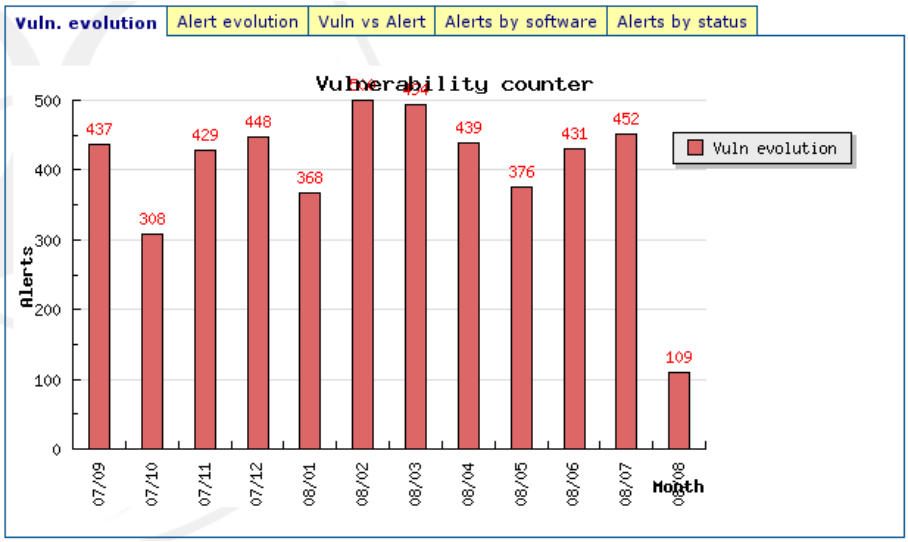


figure 35: vulnerability counter

- Alert evolution: shows the generated alerts every month during the last year

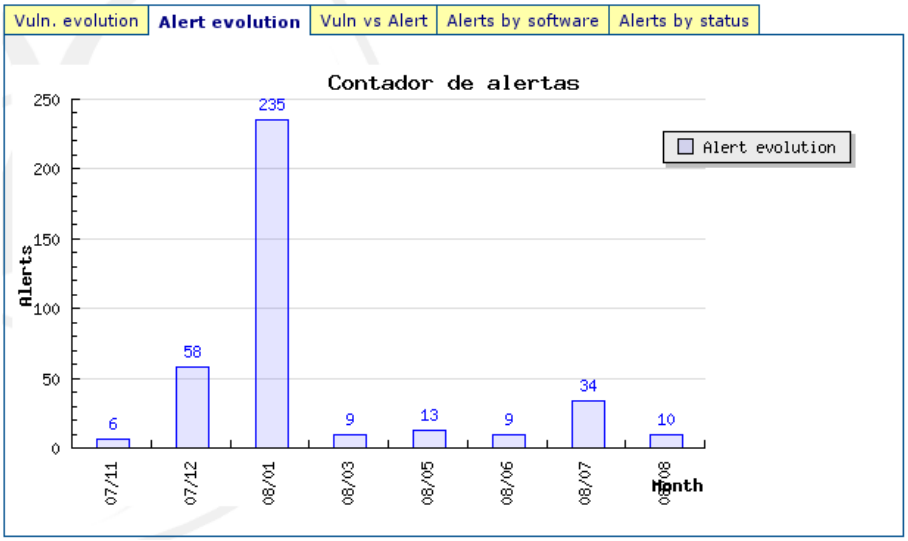


figure 36: Alert evolution

- Alerts vs vulnerabilities: shows the integration of the two previous graphs.

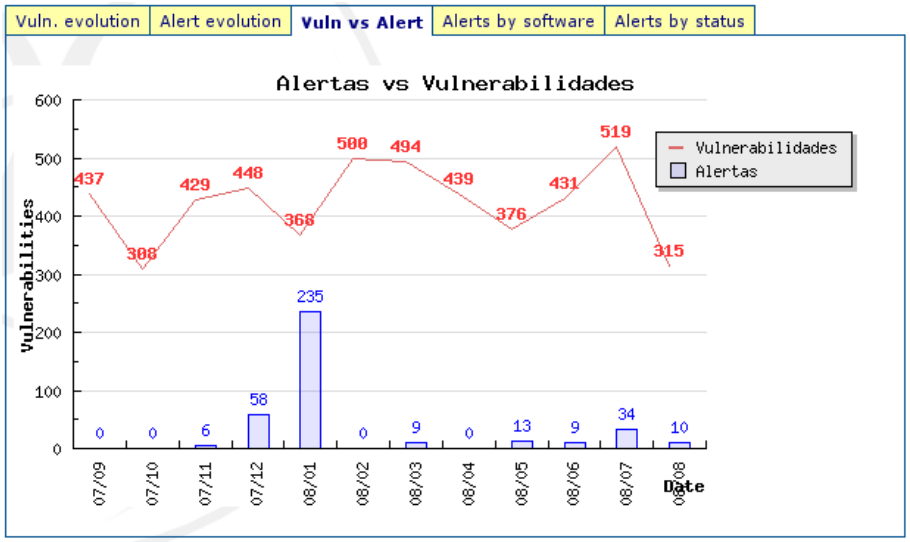


figure 37: alerts vs vulnerabilities

- Alerts by software: a pie graph showing what is our most affected product or service.

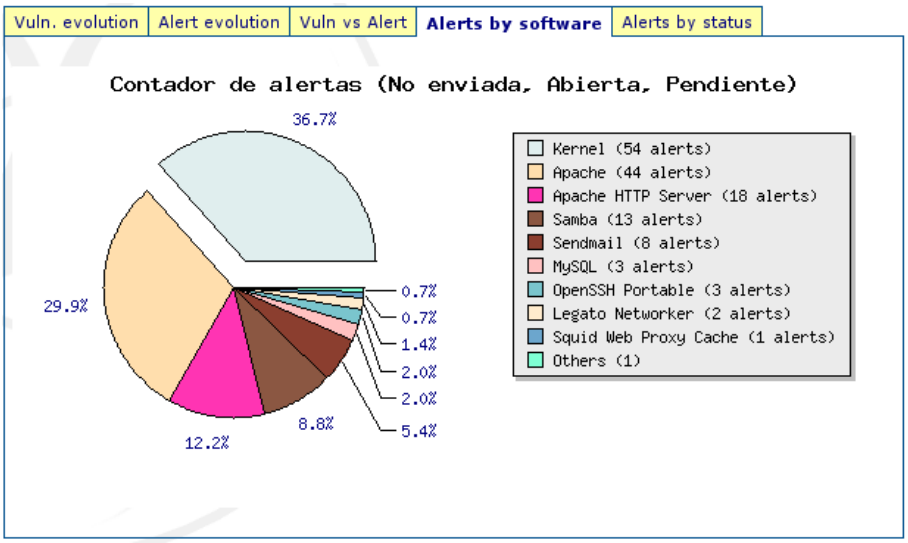


figure 38: alerts by software

- Alerts by status: a pie graph showing the alert status of all the alerts from our group.

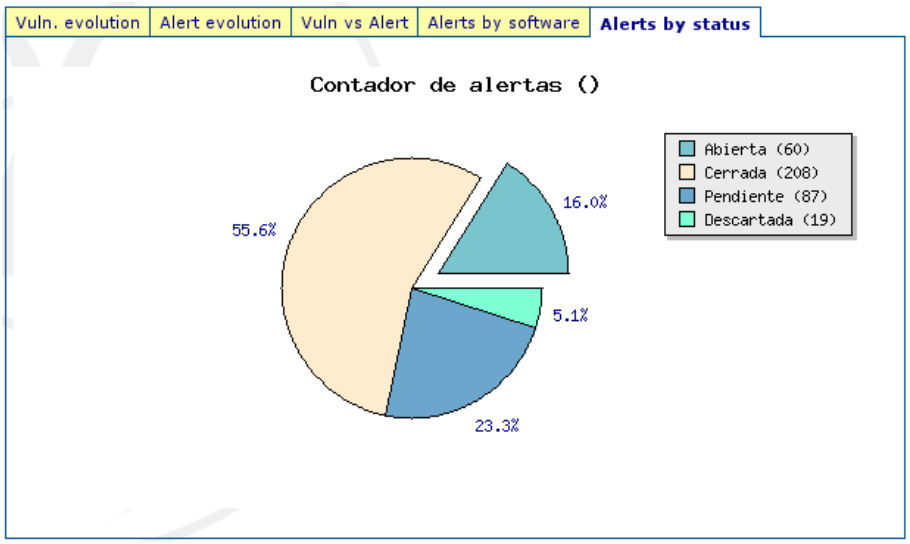


figure 39: Alerts by status

4. Using the SIGVI administrator

What are the SIGVI manager tasks?

- configure the environment of new SIGVI instances
- start with the vulnerabilities
- manage groups
- go over the global tasks: daily summaries, night tasks, etc.
- update periodically different parts of the application: vulnerability sources, etc.

For more information, go to the installation manual or the technical documentation.

4.1. At the beginning

The SIGVI manager has the responsibility of every new instance of SIGVI.

4.1.1. Environment configuration

Go to the technical documentation to understand the installation and configuration of the optional parts.

4.1.2. Vulnerability sources configuration

The usefulness of SIGVI is measurable to the quality of data we have introduced, both the vulnerabilities and the products installed on the servers. The responsibility for a up to date vulnerabilities database is for the SIGVI manager and the reliability of the data introduced is for the equipment managers.

By default SIGVI provides a set of sources and plugins based on the CVE standard definitions of vulnerabilities from the NVD. By default, only two sources concerning the updates and news are being active.

However, it is advisable to make a full load of all sources first. To perform this task, please refer to section 3.7.3

4.1.3. Creating the groups

End users are the equipment managers of SIGVI, who have to belong to a group. Group managers are the figures that are responsible for creating and managing users in every group.

SIGVI manager is the only one who can create and manage the definition of the groups. He is responsible for creating the groups in your environment and identifying those responsible for each of them, but is not his role managing the internal data of each group, such as servers, alerts, installed products, etc..

4.2. Daily use

Daily use of the SIGVI manager should focus primarily on correcting any problems or system configuration without having to go to review internal problems in the groups or their data.

The main task of the SIGVI manager is to review the state of the summaries of automatic processes.

4.2.1. Checking the state of the processes

The night processes sent a summary of the final statement to the SIGVI managers. They have the responsibility for ensuring the smooth functioning of processes, reviewing daily the results to correct any problems.

These problems could include, for example, that the vulnerability update has not been made because the network was not working. In this case is would be detected by the absence of state or by an incorrect summary of state, then you must manually load and launch the process.

5. Starting and using the group manager

What are the group manager tasks?

- Creating and managing the group users
- Creating and managing the group filters
- Creating and managing the FAS functions for the group.
- Reviewing the doubtful alerts for the group.

5.1. At the beginning

When the SIGVI manger had been created your group, you have to fill all the group information.

5.1.1. Managing users

You have to create the equipment manager users in your group, who have to start creating servers and associate them to products, this is indispensable information to make SIGVI useful

5.1.2. Managing filters

Using filters is optional, but using them can improve your effectiveness. Go to section 3.6.3.

5.1.3. Managing FAS functions

Using FAS functions is also optional, but using them you can improve the SIGVI effectiveness. Go to section 3.6.4.

5.1.4. Checking doubtful alerts

The group manager is responsible for check the doubtful alerts (go to section 3.4.1). This are the alerts that the SIGVI kernel isn't capable to decide if there are important or not, they are create as a “pending alerts” and it's the group manager who has to make that decision.

These alerts are invisible from the equipment managers, who are responsible for analyzing the impact at their servers. For this reason it's important to check the pending alerts as soon as possible.

6. Starting and using the equipment manager

As a equipment manager in SIGVI, what is the first step? Why I need this application and what can I do with it?

6.1. At the beginning

6.1.1. What SIGVI can do for me?

SIGVI is a tool that tries to help the server administrator in the detection and vulnerability management on his servers.

System administrators have to spend much time in the detection and vulnerability management. These routine tasks such as reading the notices sent from vulnerabilities subscriptions, compare it with the list of software in the servers, and finally, collect information and decide the actions to take.

The main functionality of SIGVI is to perform the whole process of analysis and detection, so the administrator only has to worry when receives a notification warning about a vulnerability in his servers.

SIGVI, from the list of servers and products that are installed, will consider every day if a vulnerability affects any of these products. If so, he will create an alert (see 3.4.2) and sent it to you via the mechanism that has been defined.

6.1.2. First step: introducing the data

Before SIGVI can notify administrators of vulnerabilities on their computers is necessary to register the servers, and then, for each of them to register the most important software you have installed (operating systems, software providing services to other servers or the Internet, etc.). Please, go to chapter 3.5.2.

Once updated on its servers and services (or products or software), you will receive your vulnerability alerts, if any.

6.2. Daily use

6.2.1. What is up with the email notifications?

When SIGVI detects a vulnerability in a product creates an alert in the alert repository and sent a notification to you (via email by default). This notification received is a summary of the warning, showing what server is concerned, which product is vulnerable and if the vulnerability affects you, including the URLs of where to go for seeking information concerning the decision or what action should be taken.

It also includes the FAS (Final Absolute Severity, see chapter 3.6.4), which is a number between 0 and 10 that indicates how serious the alert is, and help you to make a quick decision if it is critical or not.

After this notification you should work on the SIGVI alert, saving all the information related for future references and for help other equipment managers.

To do this go to your instance of SIGVI, enter your username and password and access the menu of active alerts, where are the open or pending alerts in your group. For each one, you can access the information on the vulnerability, which includes the details of the vulnerability and usually links to pages where the manufacturer or third parties recommended actions to take.

Think that this tool will not act for you, it is only trying to make available all information that you may need to make a decision.

6.2.2. Updating the software versions. Do I need to update SIGVI?

YES. Because if the data you have in SIGVI is not real, notifications and alerts won't be. The most updated information the most useful SIGVI will be.

6.3. Information about vulnerabilities

6.3.1. I'm tired on daily summaries. Can I deactivate them?

On your user settings page you can configure whether or not you want to be notified with a daily

summary of vulnerabilities in the "Get a daily summary of vulnerabilities."

6.3.2. The summaries have too much information.

Although the summaries are only informative, you can restrict the information in the summary, using the “filter notifications” field in your user settings page, go to section 3.6.3, about filters..

Index of figures