

SIGVI R2

Manual del Usuario

Índice

1. Introducción.....	4
1.1. Administrador del SIGVI.....	4
1.2. Administrador de grupos.....	5
1.3. El administrador de equipos.....	5
2. Elementos generales de las pantallas.....	6
3. Páginas.....	8
3.1. Login.....	8
3.2. Logout.....	8
3.3. Página principal.....	9
3.4. TO-DO.....	12
3.4.1.Alertas pendientes de validar.....	13
3.4.2.Alertas.....	13
3.4.3.Resumen de alertas en los servidores.....	16
3.5. Menú de inventario.....	16
3.5.1.Alertas.....	16
3.5.2.Servidores y productos.....	16
Servidores.....	17
Servicios: Productos instalados en los servidores.....	17
3.5.3.Productos.....	18
3.5.4.Vulnerabilidades.....	19
3.6. Administración.....	20
3.6.1.Mi usuario.....	20
3.6.2.Grupos y usuarios.....	21
3.6.3.Filtros.....	22
Definición.....	23
¿Cómo se filtra?.....	24
Usos.....	24
3.6.4.FAS.....	24
¿Cuál es mi FAS?.....	25
¿Cómo se construye una FAS?.....	25
3.7. Configuración.....	26
3.7.1.Configuración (general).....	27
Configuración.....	27
Parámetros globales.....	27
3.7.2.Administración de tareas.....	27
3.7.3.Fuentes.....	28
Fuentes de vulnerabilidades.....	28
Gestión de las fuentes RSS.....	30
Gestión de los diccionarios de productos (CPE).....	30
3.7.4.Métodos de notificación.....	31
3.8. Herramientas.....	31
3.8.1.Base de datos (DDBB).....	31
3.8.2.Logs.....	32
3.8.3.Mailing.....	33

3.8.4.	Bugs de la aplicación.....	34
3.8.5.	Informes.....	34
	Suscripciones a informes.....	34
	Informes.....	35
	TAGs.....	37
3.8.6.	Estadísticas.....	38
4.	Inicio y uso del SIGVI R2 del Administrador del SIGVI.....	42
4.1.	Inicio.....	42
4.1.1.	Configuración del entorno.....	42
4.1.2.	Configuración de las fuentes de vulnerabilidades.....	42
4.1.3.	Crear los grupos.....	42
4.2.	Uso diario.....	43
4.2.1.	Revisar los resúmenes de estado de los procesos.....	43
5.	Inicio y uso del SIGVI R2 del Administrador de grupos.....	44
5.1.	Inicio y uso.....	44
5.1.1.	Gestión de usuarios.....	44
5.1.2.	Gestión de los filtros.....	44
5.1.3.	Gestión de las funciones FAS.....	44
5.1.4.	Revisión de las alertas dudosas.....	44
6.	Inicio y uso del SIGVI R2 del Administrador de equipos.....	45
6.1.	Inicio.....	45
6.1.1.	¿Qué es el SIGVI y para qué sirve?.....	45
6.1.2.	Primer paso: introducción de los datos.....	45
6.2.	Uso diario.....	45
6.2.1.	Me ha llegado una notificación por email, ¿ahora qué hago?.....	45
6.2.2.	He actualizado la versión de un programa en el servidor, ¿tengo que cambiarlo en SIGVI?.....	46
6.3.	Información de las vulnerabilidades.....	46
6.3.1.	Me he cansado de tanto resumen diario, ¿Cómo puedo desactivarlos?.....	46
6.3.2.	Los resúmenes tienen demasiada información.....	46

1. Introducción

SIGVI son las siglas de Sistema Inteligente de Gestión de Vulnerabilidades Informáticas. Es una herramienta que sirve para detectar y gestionar las vulnerabilidades de sistemas informáticos.

Este proyecto se desarrolla y mantiene desde UPCnet, empresa de servicios TIC del grupo UPC (Universidad Politécnica de Cataluña). También ha sido co-financiado durante el 2008 por el Ministerio de Industria, Turismo Y Comercio de España (MITYC, www.mityc.es) para la obtención de un producto precompetitivo.

El SIGVI es una aplicación Web compuesta por un conjunto de scripts programados en PHP que implementan la lógica de la aplicación y una base de datos relacional donde se guardan los datos. Algunos scripts se ejecutan como procesos batch (generalmente por la noche) para realizar las tareas que no requieren la interacción humana, como por ejemplo las cargas de vulnerabilidades desde las fuentes, el chequeo de las vulnerabilidades en nuestros sistemas, etc. El resto son los scripts que programan la propia aplicación Web.

Esta aplicación está orientada al usuario final, al administrador de sistemas en su labor diaria de detección y gestión de vulnerabilidades en los servidores. Pero para facilitarle la tarea se han definido varios perfiles de usuario, dejando labores de administración de la propia aplicación a otras figuras.

De este modo, hay tres perfiles de usuario:

- Administrador del SIGVI: Es el administrador general de la aplicación, cuya función será la de realizar tareas de administración general en la aplicación.
- Administrador de Grupos: Es la figura que administra los datos generales de un grupo, que a groso modo sería la gestión de los usuarios de éste.
- Administrador de Equipos: Es el usuario que finalmente hará uso de las funcionalidades propias de la gestión de vulnerabilidades.

1.1. *Administrador del SIGVI*

Es el perfil con mayor nivel de acceso, permitiéndole acceder a todos los apartados de la aplicación con todos los privilegios. No obstante la labor principal del administrador del SIGVI será la gestión de aquellos apartados a los que sólo él tiene acceso:

- gestionar los grupos (altas y bajas)
- gestión de usuarios de nivel “Administrador del SIGVI”
- gestión de las fuentes de vulnerabilidades
- gestión de las fuentes de productos (CPE)
- gestión de las fuentes RSS de noticias
- gestión de los métodos de notificación
- gestión de los parámetros globales de la aplicación
- gestión de la configuración global de la aplicación
- gestionar los bugs de aplicación (si estuviera habilitado)

Además, podrá:

- lanzar manualmente los procesos de cargas de vulnerabilidades
- lanzar manualmente los procesos de comprobación de vulnerabilidades
- visualizar los logs de la aplicación
- interactuar con la base de datos

1.2. Administrador de grupos

El hecho de que exista esta figura se debe básicamente a centrar la gestión de los usuarios de un grupo en una figura con un nivel de acceso intermedio entre el administrador del SIGVI y el administrador de equipos. La función más importante del administrador de grupos será la alta, baja y modificación de los usuarios de su grupo.

Además podrá:

- validar o descartar las alertas pendientes de validación
- gestionar los filtros de notificación y detección del grupo
- gestionar las funciones de cálculo del factor de impacto (FAS) del grupo

1.3. El administrador de equipos

El administrador de equipos es la figura de la aplicación que representa el operador o administrador de sistemas. Será el encargado de velar, entre otras cosas, del estado de seguridad de sus servidores.

La finalidad del SIGVI es ayudar en las tareas de supervisión del estado de seguridad de los servidores al administrador de equipos.

Las funcionalidades más importantes que tendrá disponibles para su día a día son:

- gestionar los servidores de su grupo (altas, bajas, modificaciones),
- gestionar el software que tiene instalado cada uno de los servidores de su grupo,
- gestionar las alertas de vulnerabilidades de su grupo.

Además de éstas podrá:

- ver los filtros de notificación,
- ver las fórmulas de cálculo del factor de impacto,
- ver el estado general de vulnerabilidades de los servidores de su grupo,
- acceder a los resúmenes generales,
- acceder a los bugs de la aplicación y crear nuevos.

2. Elementos generales de las pantallas

Antes de comenzar a explicar con detalle cada uno de los apartados de la aplicación es conveniente explicar brevemente los componentes de las pantallas comunes a la aplicación.

Prácticamente todas las pantallas están creadas usando la misma plantilla, que se divide en tres partes: cabecera, contenido de la propia página, y pie de página.

En la siguiente imagen las vemos desglosadas donde además aparece un ejemplo de un mantenimiento típico:

The screenshot shows the 'Groups and users' page in the SIGVI R2 Enterprise application. The page is annotated with numbers 1 through 6:

- 1:** The top header area containing the logo, version 'SIGVI R2 Enterprise', and user information: 'Username: admin, Level: SIGVI Adm, Group: SIGVI Adm'.
- 2:** The navigation menu with items: home, TO-DO, Inventory, Administration, Configuration, Tools, Last news, and About.
- 3:** The search input field and a refresh button.
- 4:** The table header and the 'Total: 8 rows' indicator.
- 5:** The table body containing user records.
- 6:** The footer area with version 'SIGVI R2 Enterprise 1.4.05 Beta, © 2007 UPCnet' and page creation time 'Page created in 0.008 seconds'.

Username	External?	Name	Surname	Group	Level	email	Hiredate	Lang	Receive notifications?	Receive daily vuln. publications?	Notification filter	
admin	No	Administrador		SIGVI Adm	SIGVI Adm	admin@sigvi.es	2008-12-10 11:19:49	en	Yes	No		
bo.user1	No	User	One	Back Office	Host Adm	user1@sigvi.es	2008-12-10 10:18:12	cat	Yes	Yes		
bo.user3	No	User	Three	Back Office	Host Adm	user3@sigvi.es	2008-12-10 10:19:12	cat	Yes	No		
bo.user4	No	User	Four	Back Office	Groups Adm	user4@sigvi.es	2008-12-10 10:19:52	cat	Yes	Yes	Normal	
bt.user5	Yes	User	Five	Beta testers	Groups Adm	user5@sigvi.es	2008-12-10 10:20:37	es	Yes	No		
dev.user2	No	User	Two	Developers	SIGVI Adm	user2@sigvi.es	2008-12-10 10:20:02	en	Yes	Yes		
dev.user6	No	User	Six	Developers	Groups Adm	user6@sigvi.es	2008-12-10 10:22:35	cat	Yes	Yes		
inn.user7	Yes	User	Seven	INN	Host Adm	user7@sigvi.es	2008-12-10 10:22:10	cat	No	No		

figura 1: Formato de las páginas

- **1. Logo, título, información de usuario y accesos rápidos**

En la parte superior izquierda de la página aparece el logo del SIGVI (que es un enlace con la página principal) junto con el nombre de la versión instalada (en este caso R2 Enterprise).

En la parte superior derecha se muestran iconos de acceso rápido a ayuda (en las páginas que esté disponible), a la declaración de bugs (problemas detectados en la aplicación) y desconexión. La gestión de bugs deberá ser habilitada desde el fichero de configuración de la aplicación (app.conf.php).

Bajo esta botonera aparece información del usuario: nombre de usuario, grupo y nivel de acceso.

- **2. Menú**

Es el menú de la aplicación accesible desde cualquier página. Agrupados por temas, se encuentran los accesos a las páginas de gestión y de herramientas de la aplicación.

- **3. Barra de búsqueda y de herramientas de un mantenimiento**

Algunos mantenimientos permiten realizar búsquedas para reducir el número de registros que aparecen o encontrar un resultado.

Además, y si tenemos los permisos suficientes, aparecerán estos botones, que permitirán refrescar el contenido del mantenimiento, agregar un nuevo registro o bien, si el mantenimiento lo permite, exportar los resultados a un fichero en un formato que podremos usar desde una hoja de cálculo (CSV).

- **4. Número de filas mostradas**

Se muestra el número de registros encontrados. Si el número de filas que se han encontrado superan un máximo de página se producirá una paginación, donde aparecerá una barra de navegación con flechar para moverse a través de las páginas.

- **5. Acciones sobre los registros**

Dependiendo de los permisos, podremos modificar los registros o eliminarlos.

- **6. Información de página**

Finalmente aparece información sobre el tiempo de creación de la página y la versión de la instancia.

3. Páginas

Veamos rápidamente las páginas que existen en el SIGVI R2. Dependiendo de su perfil de usuario, usted verá disponibles sólo algunas de ellas, y dependiendo de éstas usted sólo podrá realizar ciertas tareas dentro de ellas.

Lo que se mostrará a continuación es la vista de un administrador del SIGVI.

Nota: Para este documento, y con la finalidad de poder representar el máximo de información posible en las ilustraciones, aparecerán desactivadas las imágenes corporativas que pueden ser activadas o desactivadas a través del fichero general de configuración de la aplicación.

3.1. Login

Cuando accedamos a la instancia de la aplicación SIGVI, lo primero que tendremos que hacer será autenticarnos desde la pantalla de login. En la pantalla de login deberemos indicar un usuario y una contraseña válidos. Mientras la autenticación no sea correcta no podremos avanzar.

La comprobación del usuario y la contraseña se realizará en función de cómo se haya dado de alta el usuario, ya que la autenticación tanto se puede hacer usando una contraseña local (almacenada en la base de datos), o remotamente usando servicios dispuestos a tal fin, como por ejemplo servicios LDAP.



figura 2: página de login

Quien cree el usuario deberá notificar al usuario cuál es el método de autenticación que deberá usar para acceder a la aplicación.

3.2. Logout

Para salir de la aplicación podemos presionar el enlace de salida o logout que aparece en la cabecera, de esta manera se cerrará la sesión en el servidor y se liberará toda la información temporal almacenada. No obstante, las sesiones tienen un tiempo de vida limitado, normalmente de entre 5 y 10 minutos, que viene definido en la configuración del servidor Web donde se aloja la instancia del SIGVI. Cuando pasa ese intervalo de tiempo sin conexión desde el cliente, se cierra automáticamente esa sesión.

Una vez cerrada la sesión, la próxima pantalla que aparezca al intentar acceder a la instancia del SIGVI será la de login.

3.3. Página principal

Tras una autenticación correcta, pasaremos a la pantalla principal, donde tendremos disponibles todas las funcionalidades de nuestro perfil. A continuación se muestra la pantalla que vería un administrador del SIGVI:

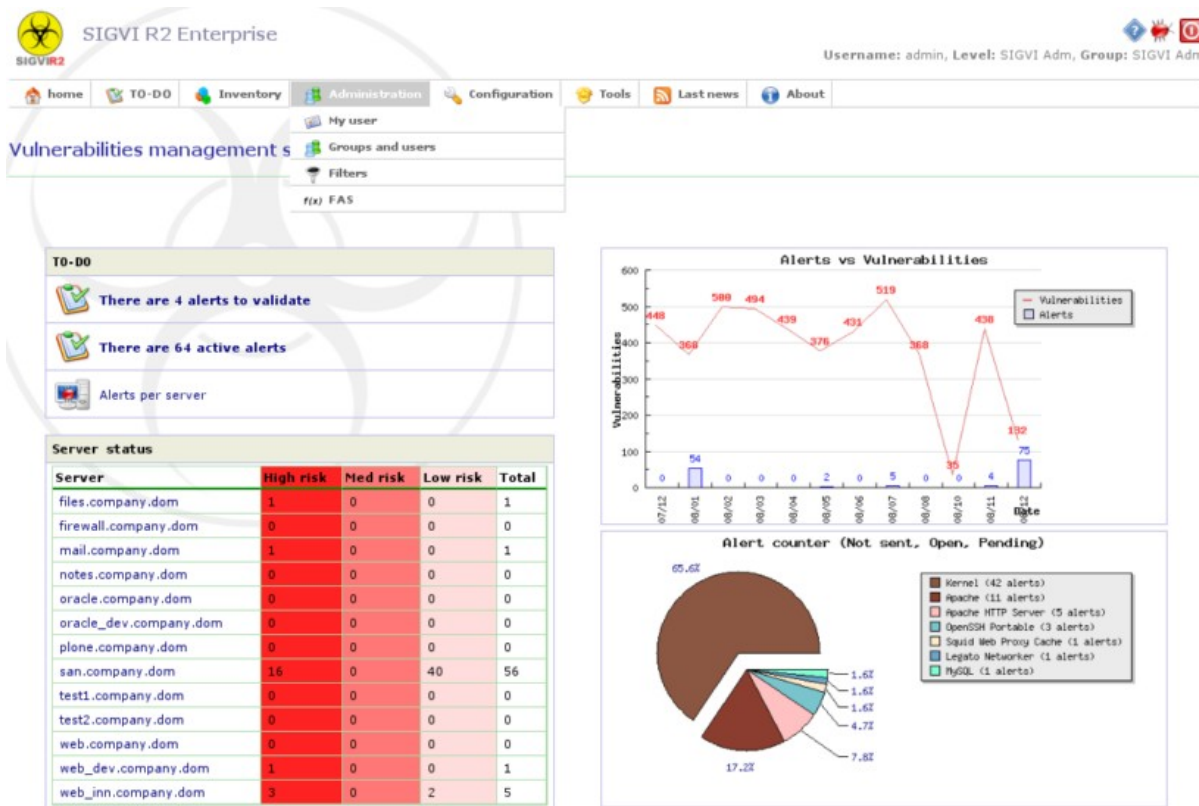


figura 3: página principal

Cada una de estas partes son:

- Cabecera de la página: logo, accesos rápidos, información de usuario, menú, título de página.
- Menú “TO-DO”: donde aparece el resumen del estado general de revisión y resolución de vulnerabilidades para su grupo.
- Estado de los servidores: para cada uno de los servidores de su grupo aparece desglosado el número de vulnerabilidades por los que se ve afectado, es decir, el número de alertas abiertas.
- Gráfica comparativa entre la evolución del número de vulnerabilidades descargadas vs las alertas aparecidas en sus servidores en el último año.
- Gráfica informativa acerca de cómo se reparte el total de alertas en función del tipo de software que se ve afectado.

3.4. TO-DO

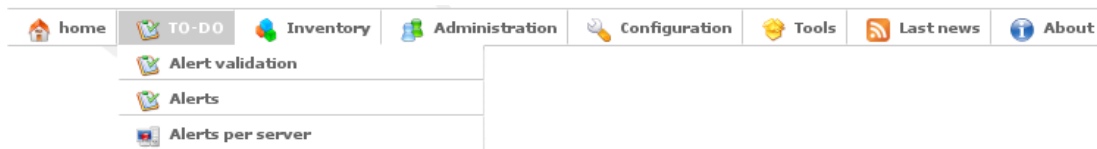


figura 4: Menú TO-DO

Este es el grupo de enlaces a las páginas habituales de trabajo, donde se indicará un resumen del volumen de tareas pendientes.

En el caso del administrador de usuario, aquí aparecerá únicamente el enlace con las alertas abiertas en los servidores de su grupo.

3.4.1. Alertas pendientes de validar

En ciertas ocasiones el motor de búsqueda del SIGVI puede tener dudas acerca de si una vulnerabilidad afecta a un producto de un servidor. En estos casos no es aconsejable descartarlas, así que se genera una alerta como “dudosa”. Este tipo de alertas no se notifican hasta que algún administrador de SIGVI o de grupo decida qué hacer con ellas.

Estas alertas aparecerán en esta pantalla separada, que no será visible por los administradores de equipos.

La finalidad de ésta funcionalidad es disminuir el número de falsos positivos de la aplicación para no generar más trabajo del realmente necesario. No obstante SIGVI R2 no decidirá por el usuario si las alertas dudosas deben ser descartadas, porque eso podría provocar la pérdida de alertas reales.

Los administradores de grupo tendrán la responsabilidad de revisar periódicamente (preferiblemente diariamente) este tipo de alertas del grupo. El SIGVI dispone de mecanismos automáticos para recordar a los responsables de esta tarea de la revisión de estas alertas.

Así mismo, pasado un período definido en la aplicación (por defecto 48 horas) las alertas en estado dudoso se pasarán a estado “no enviado”, de manera que entrarán en el siguiente proceso de notificación tras el cual pasarán automáticamente a estado “abierta”.

3.4.2. Alertas

Una alerta se crea cuando un producto de un servidor está afectado por una vulnerabilidad. En esta página se nos mostrarán las alertas de vulnerabilidades que se han detectado en los servidores de nuestro grupo.

Las alertas pueden tener 5 estados posibles: No enviada, Abierta, Cerrada, Pendiente o Descartada. En este mantenimiento podremos realizar el seguimiento de las vulnerabilidades de nuestros servidores para pasarlos de un estado inicial (abierto) hasta que se cierren o se descarten:

Servers Alerts Alert validation

Change status for selected rows Change

Alerts search

Show Server

Affected product Vulnerability

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

Server	Affected product	Vulnerability	Creation date	Status	Criticality	Observations	Vulnerability updated	Time of resolution			
26	fileservr.local.net	Ubuntu, Ubuntu Linux, 7.04	CVE-2007-4601	2008/08/28 01:47:30	Open	7.50		0.00			<input type="checkbox"/>
27	mail.local.net	Microsoft, windows, 2003 Server SP 1	CVE-2007-2228	2008/08/28 01:47:30	Open	8.13		0.00			<input type="checkbox"/>
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			<input type="checkbox"/>
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			<input type="checkbox"/>
30	mail.local.net	IBM, Lotus Notes, 7.0.3	CVE-2008-0066	2008/08/28 01:47:30	Open	4.26		0.00			<input type="checkbox"/>
31	fileservr.local.net	Drupal, Fileshare_Module, 5.x	CVE-2008-0277	2008/08/28 01:47:30	Open	4.22		0.00			<input type="checkbox"/>
32	mail.local.net	IBM, Lotus Notes, 7.0.3	CVE-2008-1101	2008/08/28 01:47:30	Open	4.26		0.00			<input type="checkbox"/>
33	ldap.local.net	redhat, enterprise_linux, ES 4	CVE-2008-1615	2008/08/28 01:47:30	Open	4.76		0.00			<input type="checkbox"/>

Total: 8 rows
Showing from row 26 to 33, of 33

Showing from row 26 to 33, of 33

figura 5: Alertas

Por defecto, al entrar en esta página sólo nos mostrará las alertas abiertas o pendientes.

El significado de los estados es:

- *No enviado*: Cada vez que se ejecuta el proceso de chequeo de vulnerabilidades, se crean las alertas en estado no enviado, lo que provoca que otro proceso posterior envíe notificaciones a todos los administradores de todas aquellas alertas en estado “No enviado”. Acto seguido se cambia, automáticamente a “Abierta”. Si durante el proceso de notificación se produjera algún problema por el cual no pudiera realizarse el envío la alerta continuará en estado “no enviado” para ser procesada de nuevo la próxima vez que se ejecute este proceso.

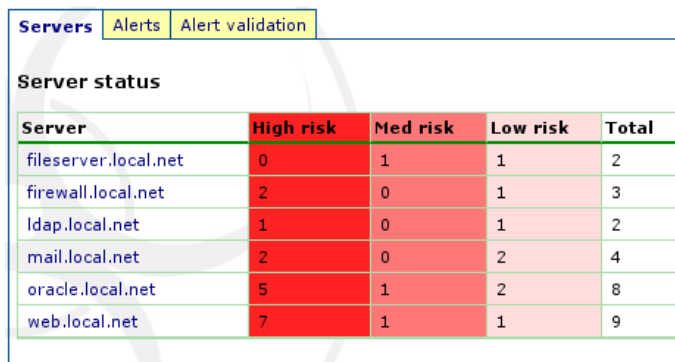
Poniendo una alerta en estado “No enviada” implicará que se envíe una notificación sobre ésta a los administradores del grupo al que corresponde la alerta.

- *Abierto*: La alerta está lista para ser analizada.
- *Cerrada*: La vulnerabilidad de la alerta ha sido solucionada.
- *Pendiente*: La alerta está pendiente.
- *Descartada*: La vulnerabilidad no afectaba al producto indicado, o simplemente se decide descartar

la alerta y no actuar sobre ella.

3.4.3. Resumen de alertas en los servidores

Desde la página anterior podemos acceder a una vista resumida de número de alertas abiertas por servidor, y separadas por gravedad de la alerta:



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

figura 6: Resumen de estado de alertas

3.5. Menú de inventario

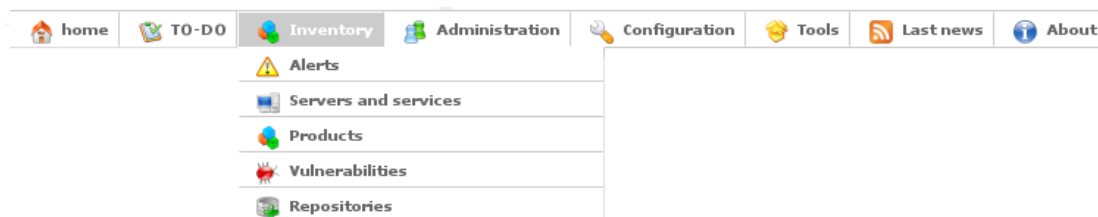


figura 7: Menú de inventario

En este grupo aparecen los enlaces relacionados con la administración de los datos referentes a las alertas, los servidores, los productos, las vulnerabilidades y los repositorios.

3.5.1. Alertas

Este enlace nos lleva a la página de gestión de alertas descrito en el punto 3.4.2.

3.5.2. Servidores y productos

Este es el punto de entrada de la información de nuestro entorno. Para poder conocer el estado de nuestros servidores deberemos reflejarlos de la manera más fiel posible.

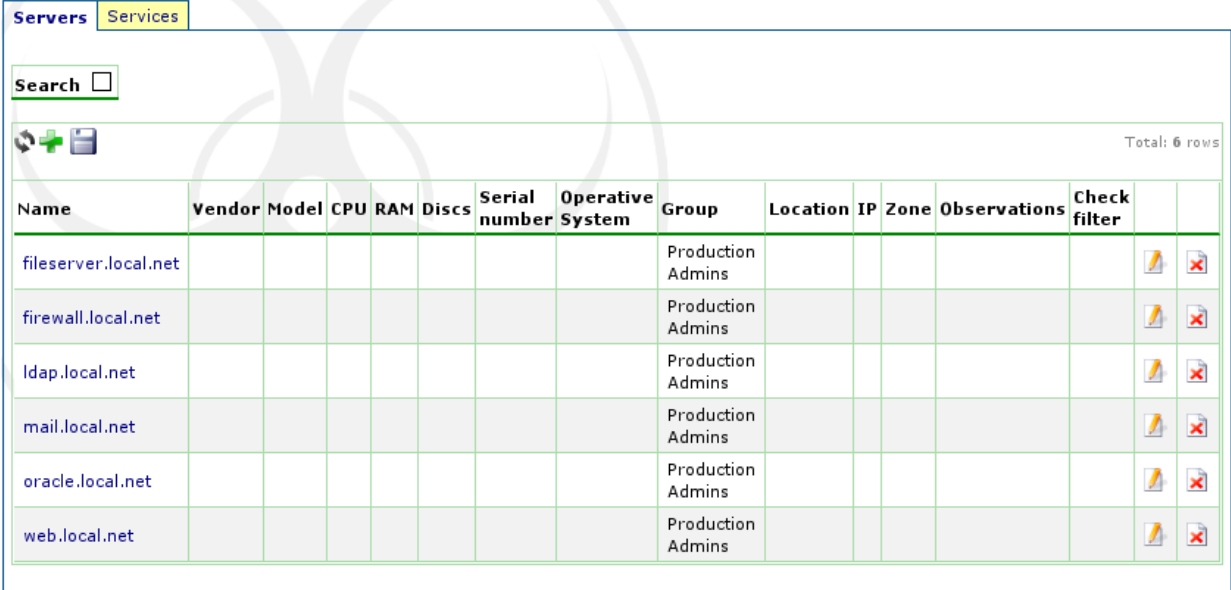
En este mantenimiento encontraremos dos pestañas, una donde se definirán los servidores y otro donde se indicará los productos que tiene instalados.

Servidores

La primera pestaña, servidores, le mostrará los servidores de su grupo. Como administrador de equipos podrá agregar y modificar la lista de servidores.

Los datos de los servidores son bastante arbitrarios. Únicamente se usará el nombre del servidor y el filtro (si se indicara alguno). El resto es información descriptiva.

Un servidor no podrá estar repetido dentro de un grupo.



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							

figura 8: Servidores

Servicios: Productos instalados en los servidores

La segunda pestaña mostrará los productos instalados en los servidores. Dar de alta todos los productos que tiene instalado un servidor puede ser una tarea bastante costosa, y si esto lo multiplicamos por N servidores, el resultado puede llegar a ser inviable en algunos entornos.

Para comenzar, y en una primera fase de determinar el estado de vulnerabilidades, podemos centrarnos únicamente el sistema operativo y en los productos instalados que ofrecen algún servicio al exterior del servidor, por ejemplo, un servidor Web, no daremos de alta todas las librerías que tiene instaladas, podemos comenzar con el producto que tiene instalado y que da el servicio Web (Apache, IIS, Tomcat, ...). Al fin y al cabo, serán los servicios abiertos los que puedan explotarse remotamente (los casos de alerta más peligrosos).

Existe un proyecto paralelo al SIGVI R2 llamado **NSDi**, el cual servirá para detectar automáticamente el listado de software de los servidores. Es un proyecto que actualmente (en la versión actual del SIGVI) es una versión Alpha, que ya permite la integración con el SIGVI, pero que aún requiere trabajo de ingeniería, programación y testeado).

Nota: El comando `nmap` (<http://nmap.org/>) nos podrá ayudar a determinar qué servicios está ofreciendo un servidor.

En el siguiente ejemplo vemos un fragmento del listado de software instalado en los servidores:

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, Filechare Module 5 v	No	Yes				

figura 9: Servicios: productos instalados en los servidores

Como puede verse, únicamente se ha dado de alta los productos que están dando el servicio.

Cuando damos de alta un producto en un servidor, deberemos indicar obligatoriamente el servidor, el producto y además, para este caso concreto si el servicio está filtrado (si es accesible desde Internet), y si está proporcionando un servicio crítico (a nuestro juicio).

Puede ser un servicio crítico, el servidor Web corporativo (cara de nuestra empresa), un servicio LDAP de autenticación en el que se basen diferentes aplicaciones, un servicio ORACLE de SAP, etc.

No hay una regla genérica que lo defina. Simplemente será a nuestro juicio si nos parece crítico que ese servicio caiga o no (si llegara a ser atacado por una vulnerabilidad).

Puede ocurrir que al asociar el producto éste aún no exista en el listado de productos. Si se diera este caso vea el siguiente punto Productos (repositorio).

El resto de los campos son puramente descriptivos.

3.5.3. Productos

Se refiere al repositorio de productos, el listado global de productos que se ha ido generando. En esta pantalla podremos consultar los productos que se han ido introduciendo en el sistema. De esta lista es de donde se obtendrán los productos relacionados con los servidores.

Search

Vendor

Product name

Version

Full

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

Total: 9 rows

id	Vendor	Product name	Version		
90770	Apache	Apache	2.2.3		
91989	Apache	Apache HTTP Server	2.2.3		
92573	Apache	Apache HTTP Server	2.3.0		
96001	Apache Software Foundation	Apache	2.2.3		
83203	Apache Software Foundation	Apache HTTP Server	2.2.3		
94765	Apache Software Foundation	Apache HTTP Server	2.3.0		
97673	Apache Software Foundation	HTTP Server	2.2.3		
66624	Apache Software Foundation	mod_python	2.3		
53225	Apache Software Foundation	Tomcat	3.2.3		

figura 10: Repositorio de productos

El listado se construye a partir del software vulnerable y las entradas de los propios usuarios. Es decir, que un software que por el momento no se haya encontrado vulnerabilidad alguna, no aparecerá en esta lista a menos que algún usuario lo haya introducido manualmente.

Puede ocurrir que tengamos que asociar un software que aún no existe en la lista. Debemos, en tal caso, darlo de alta nosotros mismos. Este es el punto más crítico de la configuración de la aplicación, dado que el hecho de determinar si un software es vulnerable o no se basa en la comparación del nombre de ese software con el del presentado en el listado de software de la vulnerabilidad. Si el nombre presentara algún tipo de desviación del estándar, es probable que acabe por pasar inadvertidas las vulnerabilidades, y esto es precisamente lo que se trata de evitar.

Consejo: Cada vendedor suele seguir un esquema de nomenclatura, es aconsejable, si hay que dar de alta un nuevo producto, primero ver cómo se les ha llamado a otros similares y usar ese mismo esquema para el nuevo.

3.5.4. Vulnerabilidades

En esta pantalla accedemos al repositorio de vulnerabilidades que se han ido almacenando a través de las cargas de las fuentes de vulnerabilidades en los procesos batch.

Por defecto, al acceder a esta página nos mostrará las vulnerabilidades del último día:

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 attackers to inject arbitrary HTML and JavaScript [...]	Crafty Syntax Live Help, Crafty Syntax Live Help, 2.4.16;	[+]

figura 11: Respositorio de vulnerabilidades

Para cada vulnerabilidad, podemos ver que se presentan tres enlaces:

- CVE/CAN, enlaza con la página de la fuente donde se publica la vulnerabilidad (<http://nvd.nist.gov/nvd.cfm>) para cumplir con el estándar CVE.
- CVSS, enlaza con la página del NVD (<http://nvd.nist.gov/cvss.cfm>) donde se muestra el desglose del vector CVSS (si lo tuviera) para cumplir con el estándar CVSS.
- [+], enlaza con el detalle de la vulnerabilidad en SIGVI.

3.6. Administración



figura 12: Menú de administración

En este grupo aparecen los enlaces con las páginas de configuración básica.

3.6.1. Mi usuario

A través de esta página podrá modificar sus datos:

#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	

figura 13: Mi usuario

Los datos del usuario son:

- Username: El nombre de usuario que usará para realizar el login en la aplicación. Este campo es obligatorio.
- Externo: Si el valor es “Si”, la autenticación se realizará usando el sistema de autenticación que se haya definido en la instancia del SIGVI, si el valor es “No” se usará la contraseña indicada en el campo de contraseña.
- Nombre: El nombre del usuario. Este campo es obligatorio.
- Apellidos: Los apellidos del usuario.
- Grupo: El grupo al que pertenece el usuario. Esta asociación limitará el subconjunto de datos a mostrar y/o gestionar. En general, el usuario que no sea un administrador del SIGVI sólo podrá ver y gestionar los datos de su grupo. Este campo es obligatorio.
- Email: La dirección de correo del usuario. Es la que se usará para enviar las notificaciones y resúmenes resultantes de los procesos batch.
- Nivel: El nivel de acceso a los datos. No se puede auto-incrementarse el nivel de acceso, y esta asociación limitará el grado de acceso a los datos del grupo. Así, por ejemplo, un administrador de equipo no podrá modificar los datos de otros usuarios de su grupo. Este campo es obligatorio.
- Fecha de alta: Es la fecha de creación del usuario. Es un campo de lectura y no se puede modificar.
- Recibir notificaciones?: Si el valor de este campo es “No”, no se le enviará ningún tipo de notificación de nuevas alertas ni resúmenes.
- Recibir resumen diario de vulnerabilidades?: Si el valor de este campo es “No”, el usuario no recibirá el resumen diario de vulnerabilidades, resultante del proceso batch de carga de vulnerabilidades.

3.6.2. Grupos y usuarios

Son los mantenimientos mediante los cuales se gestionará los grupos y los usuarios de la aplicación.

Sólo usuarios con perfil “administrador del SIGVI” podrá visualizar y gestionar el mantenimiento de grupos, y sólo éstos o usuarios con perfil “administrador de grupo” podrá visualizar y gestionar el mantenimiento de usuarios.

Name	Description		
Production Admins	Backoffice group		
SIGVI Adm	SIGVI Administration		
Software developers			
Tech Projects	R&D Users		
Testers	Various users for testing environments		

figura 14: Grupos

El nombre de los grupos es obligatorio y debe ser único. La descripción es optativa.

Los grupos se usarán para agrupar los usuarios y los recursos de éstos (servidores, productos instalados en los servidores, alertas, etc.).

Username	External?	Name	Surname	Group	Level	email	Hire date
admin	No	Administrador		SIGVI Adm	SIGVI Adm	sebastian.gomez@upcnet.es	2008-00:20
jorge	No	novoa		SIGVI Adm	Host Adm	jorge.novoa@upcnet.es	2008-14:4
matt	No	Matthew		Software developers	Groups Adm	matt@m.com	2008-14:4
tiochan	No	tio	chan	Production Admins	Host Adm	tiochan@gmail.com	2008-00:1

figura 15: Usuarios

Los datos relacionados con los usuarios son los mismos que los que se presentan y se explican en el punto anterior “[Mi usuario](#)”.

3.6.3. Filtros

Los filtros se usan para discriminar las vulnerabilidades a la hora de usarlas, bien sea cuando afecta a un producto de un servidor, o bien a la hora de incluirla en el resumen diario de vulnerabilidades.

Los filtros se podrán usar en el mantenimiento de usuarios para cada uno de ellos, indicando el filtro de vulnerabilidades a utilizar en el resumen diario de carga de vulnerabilidades.

También se podrán usar en el mantenimiento de servidores, indicando el filtro de vulnerabilidades a utilizar en caso de que una vulnerabilidad afecte a uno de sus productos.

El uso de filtros que se adecuen a sus necesidades podrá reducir la cantidad de avisos y ahorrar el tiempo de revisión de alertas que por norma se descartan.

En muchas ocasiones, debido al gran número de servidores y servicios, es necesario descartar directamente cierto tipo de vulnerabilidades. Muchas vulnerabilidades requieren acceso físico a un servidor para poder ser explotadas. Es habitual descartarlas.

Por defecto el SIGVI se despliega con algunos filtros básicos, por ejemplo para filtrar todas aquellas vulnerabilidades que no puedan ser explotables remotamente.

El usuario podrá determinar en ambos casos el tipo de vulnerabilidades que deberán ser filtradas:

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 exploited 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 exploited remotely		

figura 16: Filtros

Definición

Los criterios de comparación se basarán en las características propias de la vulnerabilidad:

- Severidad (alta, media, baja)
- Si puede ser explotado remotamente (si/no)
- Consecuencias (pérdida de protección, aumento de privilegios, ...)
- Tipo (error de validación, error de condición, buffer overflow, ...)

Además, un filtro se puede crear para un grupo en concreto, o bien para cualquier grupo (si no se indica ninguno).

Un administrador de equipos únicamente podrá visualizar los filtros creados para su grupo o los genéricos, no podrá agregar ni modificar ninguno.

¿Cómo se filtra?

Los filtros se ejecutarán en función del modo en que se hayan declarado:

- Pasa si cumple todos, es decir, que si la vulnerabilidad cumple con todas las características indicadas, continuará procesando.
- Pasa si cumple alguno, es decir, que si la vulnerabilidad cumple con alguna de las características indicadas, continuará procesando.
- Filtra si cumple todos, es decir, que si la vulnerabilidad cumple con todas las características indicadas, no procesará la vulnerabilidad.
- Filtra si cumple alguno, es decir, que si la vulnerabilidad cumple con alguna de las características indicadas, no procesará la vulnerabilidad.

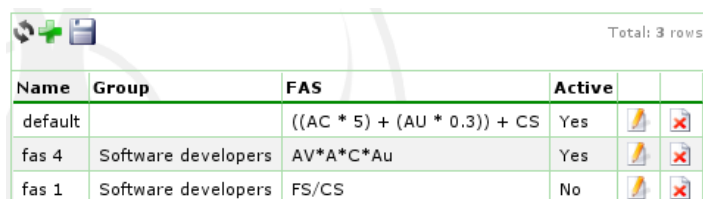
Usos

Los filtros tienen varias finalidades:

- Determinar qué vulnerabilidades se anuncian en los servidores. Cuando una vulnerabilidad afecta a un producto de un servidor, si se ha indicado un filtro en la definición del servidor, se usará éste para determinar si se crea una alerta o no. De esta manera, por ejemplo, si únicamente queremos que se tengan en cuenta vulnerabilidades que se puedan ser explotadas remotamente, y descartar aquellas que requieran acceso físico, podremos indicar ese filtro en la definición del servidor.
- Determinar qué vulnerabilidades se anuncian en los resúmenes de vulnerabilidades. Cada usuario podrá indicar qué filtro usar para determinar el tipo de vulnerabilidades de las que quiere ser informado. Así, cuando se prepara el resumen de vulnerabilidades diaria para enviar a los usuarios que así lo hayan dispuesto (si tienen activado el envío en la definición del usuario), se aplicará el filtro a cada una de las vulnerabilidades. Podrá restringir, por ejemplo, que se le notifique únicamente de vulnerabilidades graves indicando ese filtro en la definición de su usuario.

3.6.4. FAS

FAS son las siglas de Final Absolute Severity.



The screenshot shows a table with 5 columns: Name, Group, FAS, Active, and two empty columns. The table contains three rows: 'default', 'fas 4', and 'fas 1'. The 'Active' column has 'Yes' for the first two rows and 'No' for the last. The 'FAS' column contains mathematical formulas: '((AC * 5) + (AU * 0.3)) + CS', 'AV*A*C*Au', and 'FS/CS'. The table also has icons for adding, deleting, and refreshing 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		

figura 17: Final Absolute Severity

Esta es la función que se usará para calcular la gravedad de la alerta. Recordemos que una alerta es una vulnerabilidad que afecta a un producto instalado en un servidor.

Esta puntuación que se calcula sirve para determinar la gravedad de la situación. Para ello se deben tener en cuenta tanto las características de la vulnerabilidad como las características del propio servicio que ofrece ese producto en ese servidor.

Veamos las siguientes situaciones y determine cuál es la más grave:

- Una vulnerabilidad de riesgo alto afecta al servicio Apache de nuestra Web corporativa que está instalado en un servidor público (accesible desde Internet). Esta vulnerabilidad, además, puede explotarse remotamente.
- Una vulnerabilidad de riesgo alto afecta al servicio MySQL de un servidor interno filtrado y accesible únicamente desde nuestra red. La vulnerabilidad puede explotarse remotamente.
- Una vulnerabilidad de riesgo alto afecta al servicio de autenticación LDAP instalado en un servidor de acceso público sobre el cual se basan la mayoría de nuestras aplicaciones de nuestra Intranet. La vulnerabilidad requiere acceso físico al servidor.

Quizá para algunos administradores la primera situación sea la más grave, y quizá otros no. Mediante las FAS se podrá determinar sus prioridades.

¿Cuál es mi FAS?

La FAS es un elemento que se asocia a nivel de grupo completo, es decir, si hay una FAS definida para un grupo se usará esa función de cálculo para cualquier alerta de un servidor de ese grupo, si no la hay se usará la genérica (sin grupo asignado).

Como se puede ver en la figura anterior, en este ejemplo sólo hay una función definida, y no tiene grupo, eso quiere decir que será ésta la función que se usará para todos los grupos.

Como administrador de equipos no podrá crear ni modificar funciones FAS, dado que es un elemento que se usa a nivel de un grupo completo, será el administrador de su grupo quien cree las funciones para su grupo, o bien el administrador de la aplicación quien cree las funciones para todos los grupos.

El orden de decisión de qué FAS usar es:

- Si el grupo al que pertenece el servidor, al cual se le está creando la alerta, tiene una FAS **activa**, se usará esta.
- Si no, si existe una FAS sin grupo, y **activa**, se usará esta.
- Si no, se usará una FAS que está definida en la instancia de la aplicación y que simplemente es la puntuación de la propia vulnerabilidad.

¿Cómo se construye una FAS?

Como hemos comentado, las FAS se usan para determinar la gravedad de una alerta, es decir, cuan grave es la situación de una vulnerabilidad que afecta a nuestro sistema.

Para construir una FAS disponemos de las características de la vulnerabilidad y las del servicio. Debemos construir una función “matemática” que retorne un número.

Estas son las variables que podemos usar:

Acronym	Variable	Value
CS	Criticality Service	<ul style="list-style-type: none"> • 0: not critical • 1: critical
FS	Filtered Service	<ul style="list-style-type: none"> • 0: not filtered • 1: filtered

BS	Base Score	$(0.6 * \text{Impact} + 0.4 * \text{Exploitability} - 1.5) * f(\text{Impact})$
Imp	Impact	$10.41 * (1 - (1 - \text{ConfImpact}) * (1 - \text{IntegImpact}) * (1 - \text{AvailImpact}))$
Exp	Exploitability	$20 * \text{AccessComplexity} * \text{Authentication} * \text{AccessVector}$
Fimp	f(Impact)	<ul style="list-style-type: none"> • 0 if Impact=0 • 1.176 otherwise
AC	Access Complexity	<ul style="list-style-type: none"> • high: 0.35 • medium: 0.61 • low: 0.71
AU	Authentication	<ul style="list-style-type: none"> • Requires no authentication: 0.704 • Requires single instance of authentication: 0.56 • Requires multiple instances of authentication: 0.45
AV	Access Vector	<ul style="list-style-type: none"> • Requires local access: 0.395 • Local Network accessible: 0.646 • Network accessible: 1
C	Confidentiality Impact	<ul style="list-style-type: none"> • None: 0 • partial: 0.275 • complete: 0.660
I	Integrity Impact	<ul style="list-style-type: none"> • none: 0 • partial: 0.275 • complete: 0.660
A	Availability Impact	<ul style="list-style-type: none"> • None: 0 • partial: 0.275 • complete: 0.660

Las dos primeras variables: CS y FS se obtendrán de las características del servicio en la asociación entre servidor y el producto. El resto de variables se obtienen de las características de la vulnerabilidad que afecta ese producto.

3.7. Configuración



figura 18: Menú de configuración

Son un conjunto de herramientas algunas de las cuales están disponibles sólo para administradores del SIGVI y algunas para administradores de grupo.

3.7.1. Configuración (general)

Desde esta página accedemos a la configuración del fichero general de la aplicación y a los parámetros guardados en la base de datos.

Configuración

Mantenimiento aún en desarrollo mediante el cual se podrá editar el fichero general de configuración de la instancia.

General configuration	
Set application under maintenance?:	<input type="button" value="No"/>
Is a development version?:	<input type="button" value="No"/>
Is a demo version?:	<input type="button" value="No"/>
Enable bug tracking?:	<input type="button" value="Yes"/>
Enable debug messages?:	<input type="button" value="Yes"/>
Enable query debug messages?:	<input type="button" value="No"/>
Audit application usage?:	<input type="button" value="Yes"/>
Audit level?:	<input type="button" value="Only user authentication"/>
Enabled chronometer?:	<input type="button" value="Yes"/>
Default language:	<input type="button" value="en"/>
Show corporative logos?:	<input type="button" value="No"/>
Date fields format :	<input type="button" value="y-m-d"/>
Application version:	<input type="text" value="SIGVI R2 Enterprise 1.3.04 B"/>
Instance:	<input type="text" value="SIGVI-DEV"/>
Instance home directory (web based):	<input type="text" value="/sigvi"/>
Server URL:	<input type="text" value="http://tiochans"/>
Administrator e-mail:	<input type="text" value="sigvi <sebastian.gomez@up"/>
Application logo (web based reference):	<input type="text" value="/sigvi/my_include/images/log"/>
Application logo (web based reference):	<input type="text" value="/sigvi/my_include/images/log"/>
Database type:	<input type="button" value="mysql"/>
Database server hostname (or IP):	<input type="text" value="localhost"/>
Database name:	<input type="text" value="sigvi_des"/>
Database user name:	<input type="text" value="sigvi"/>
Database password:	<input type="text" value="*****"/>
<input type="button" value="Ok"/>	
<input type="button" value="Cancel"/>	

figura 19: Configuración general de la instancia

Es más aconsejable editar directamente el fichero general de configuración tal como se indica en el manual del administrador.

Parámetros globales

En este mantenimiento se definen algunos parámetros de la aplicación, como por ejemplo la dirección de email por defecto del administrador.

3.7.2. Administración de tareas

En esta pantalla, accesible únicamente por un usuario con perfil de administrador del SIGVI, podrá gestionar los procesos batch que se ejecutan y con qué periodicidad.

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			

figura 20: Administrador de tareas

Todas las entradas que aparecen deben ser scripts PHP localizados en el directorio <sigvi_home>/cron. Podremos crear tantas entradas como sean necesarias. Las que aparecen por defecto son las mínimas indispensables para el correcto funcionamiento del SIGVI.

Podremos indicar la frecuencia con la que queremos que se ejecuten, así podremos indicar si queremos que se ejecute diariamente (todos los días), semanalmente (cada lunes), mensualmente (el día 1 de cada mes) o nunca.

A su vez podremos lanzar desde este mismo mantenimiento cada tarea por separado con el icono de la derecha de cada fila. Esto provocará que se ejecute inmediatamente ese proceso mostrando los resultados de la ejecución por pantalla.

Cómo configurar e integrar las tareas en su sistema se explica en la guía de instalación.

3.7.3. Fuentes

Desde este mantenimiento podremos gestionar las fuentes de vulnerabilidades, las fuentes RSS y las fuentes de diccionarios de producto (compatibilidad CPE).

Fuentes de vulnerabilidades

Las fuentes de vulnerabilidades son una de las piezas fundamentales para tener el sistema actualizado.

El proceso nocturno de descarga de vulnerabilidades procesará cada una de las fuentes activadas (campo “Use it?” sea cierto).





















Vulnerabilities sources					RSS Sources	Products dictionaries
Tools						
 Test sources						
 Manual load from sources						
						Total: 9 rows
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		

figura 21: Administrador de fuentes de vulnerabilidades

Para poder descargar las vulnerabilidades de una fuente debe existir un plugin que sea capaz de descargar los datos, parsearlos y cargarlos en la base de datos.

En la documentación técnica se explica con detalle cómo crear un parser para una fuente concreta, pero a grandes rasgos se trata de que rellenen un array con instancias de una clase que define las características comunes en las vulnerabilidades.

En el SIGVI R2 se usa el formato definido por el estándar CVE, y se proporcionan los plugins necesarios para descargar las vulnerabilidades que se dispongan en ese formato.

Como se puede ver en la figura siguiente, existen distintos formatos del CVE, que corresponden a la evolución del mismo. No será necesario tener activadas todas las fuentes, bastará, como en este caso, tener activadas aquellas que sólo muestran los cambios recientes.

Únicamente es aconsejable activarlas todas (y mejor una por una) en la primera carga de una nueva instancia del SIGVI). En este caso, los parámetros corresponden al fichero remoto que usará para parsear.

En la parte superior de la ventana aparecen dos enlaces a herramientas:

- Probar una fuente de vulnerabilidades: es útil para comprobar si un plugin funciona correctamente. Lo que hace es una simulación de carga de una fuente de vulnerabilidades que le indicamos sin llegar a almacenar los datos en la base de datos, mostrando información por pantalla útil para determinar si el “parser” funciona correctamente o no.
- Carga manual de las vulnerabilidades desde las fuentes: básicamente ejecutará inmediatamente el proceso que se ejecuta nocturnamente para todas las fuentes activas.

Gestión de las fuentes RSS

En este mantenimiento podremos agregar tantas fuentes RSS de noticias como necesitemos, siempre y cuando dichas fuentes mantengan el patrón predefinido para el parser. Cualquier otra fuente que no use dicho patrón requerirá un parser especial. Sobre cómo crear un parser a tal efecto se habla en la documentación técnica.

La pantalla desde la que se podrá consultar el contenido de las fuentes se accederá desde menú → Noticias.










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		

figura 22: Gestión de fuentes RSS

Gestión de los diccionarios de productos (CPE)

Este mantenimiento sirve para la compatibilidad de productos CPE del SCAP. En la versión actual (Release Candidate 1) la aplicación está preparada para soportar este tipo de diccionarios. No obstante no será hasta la próxima versión en la que quedará integrado los diccionarios CPE con el repositorio de productos.

Es una pantalla transitoria que por el momento únicamente aporta valor informativo.








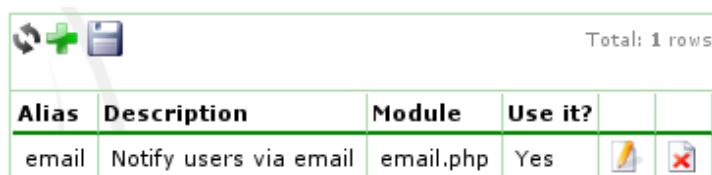
Vulnerabilities sources RSS Sources Products dictionaries						
Tools						
 Test sources						
 Manual load from sources						
						Total: 2 rows
Alias	Description	Parser	Parameters	Use it?		
CPE 1.0	NVD CPE Dictionary, version 1.0	cpe-1.0.php	http://nvd.nist.gov/download/cpe-dictionary.xml	No		
CPE 2.1	NVD CPE Dictionary, version 2.1	cpe-2.1.php	http://nvd.nist.gov/download/cpe-dictionary-v2.1-20080421.xml	No		

figura 23: Gestión de diccionarios CPE

3.7.4. Métodos de notificación

Indica los posibles métodos de notificar las alertas de las vulnerabilidades. Por defecto se provee un método “email”, por el cual la vía de notificación de las alertas a los usuarios de un grupo es el email.





Alias	Description	Module	Use it?		
email	Notify users via email	email.php	Yes		

figura 24: Métodos de notificación

En la documentación técnica se indica cómo crear sus propios métodos de notificación.

3.8. Herramientas

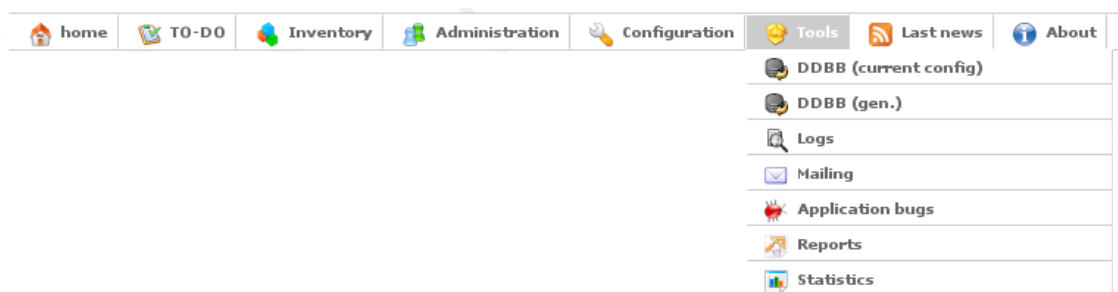


figura 25: menú de herramientas

Desde este menú accede a diversas herramientas de la aplicación. Algunas estarán accesibles únicamente para usuarios con nivel de administradores del SIGVI, otros para administradores de grupo y otros para todos los usuarios registrados.

3.8.1. Base de datos (DDBB)

Existe una herramienta que sirve para interactuar con la base de datos de la aplicación (current config) y otra para interactuar con cualquier tipo de base de datos soportada por la librería del SIGVI (Oracle, Postgres y MySQL).

Éstas están disponibles únicamente para usuarios con nivel de Administrador de SIGVI. Podrá realizar consultas SQL contra la base de datos.

16:11:08

```
select username, email, hiredate
from users
where id_group='4'
```

DB Info

DBType:


DBServer:

DBname:

DBUser:

Num rows:

Offset:

 Executing:
select username, email, hiredate from users where id_group='94'


username	email	hiredate
bo.user4	user4@sigvi.es	2008-12-10 10:19:52
bo.user3	user3@sigvi.es	2008-12-10 10:19:12
bo.user1	user1@sigvi.es	2008-12-10 10:18:12

figura 26: Interacción con la Base de Datos

3.8.2. Logs

Este mantenimiento es accesible únicamente por un perfil de “Administrador del SIGVI”, y muestra una auditoría de todos los cambios realizados en la base de datos, la hora, el origen y el usuario que lo ha generado. Puede almacenar accesos a mantenimientos, entradas correctas en la aplicación, salidas de la aplicación, intentos incorrectos de autenticación, cambios en registros de la base de datos (indicando los valores antiguos y los nuevos valores), etc.

A través del fichero general de configuración se decide si se realiza auditoría o no, y el nivel. Para más información sobre la configuración consulte la documentación técnica.



#	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 exploited 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

figura 27: Logs de la aplicación

3.8.3. Mailing

La pantalla de mailing es una sencilla interfaz para enviar emails a los usuarios de la aplicación.

La siguiente figura representa esa pantalla, donde vemos que primero está el “To”, donde deberemos seleccionar en uno de los tres bloques.

Es decir:

- podemos enviar un mail a uno o varios grupos
- **o bien** enviar un mail a uno o varios perfiles
- **o bien** a uno o varios usuarios

Si seleccionamos en más de un bloque, la aplicación usará sólo los del primer bloque donde haya algo seleccionado.

Indicaremos un “Subject” y un contenido y le damos al botón “Send”.

To:

Note: Select values from one list.
If you select values on more than one list, the first will be used.

Group:

- Production Admins
- SIGVI Adm
- Software developers
- Tech Projects
- Testers

Level:

- SIGVI Adm
- Groups Adm
- Host Adm

Users:

- admin
- jorge
- matt
- tiochan

Msg:

Subject:

Format: Normal Font: Size: **B** *I* U

Text:

Hi groups admins.

Today I have added a new vulnerability source from SUN Alert that.....

figura 28: Mailing

3.8.4. Bugs de la aplicación

Esta utilidad está más pensada para informar sobre la existencia de un fallo en la aplicación para versiones en desarrollo. Esta opción deberá estar desactivada en instancias del SIGVI en producción.

No obstante, pese a ser una interfaz sencilla sin posibilidad de asignación a personas, puede ser utilizada para otros fines, a decisión del administrador.

Search						
Status	<input type="text"/>					
Username	<input type="text"/>					
Description	<input type="text"/>					
Note: You can use SQL wildcards and the logic separators 'or' and 'and', p.e. '%apache% or %mysql%'						
<input type="button" value="Search"/>		<input type="button" value="Reset"/>				

ID	Status	Username	Description	Created	Closed		
1	Open	tiochan	I can't see all functionalities on the main menu.	2008/08/13 15:56:57	0000/00/00 00:00:00		
2	Closed	tiochan	On my "TO-DO" menu, I only see the alerts of my group. ----- It's correct. As server admin, you only can see the information relative to your group.	2008/08/13 15:58:16	2008/08/13 15:58:59		

figura 29: Bugs

3.8.5. Informes

Los informes son documentos que pueden contener elementos dinámicos (TAGs) y a los cuales podrá suscribirse cualquier usuario que esté dentro del grupo para el cual se han creado.

Dentro de la programación de tareas hay un proceso **diario** que realiza la ejecución de los informes, que se consiste en construir, para cada suscripción de un usuario a un informe, un documento sustituyendo los TAGs o elementos dinámicos por su valor usando ese usuario como referencia. El documento se enviará por email al usuario (si éste tiene activada el envío de notificaciones en su perfil).

Un informe o report lo podrá crear un administrador del SIGVI de manera genérica y al cual podrá suscribirse cualquier otro usuario de la aplicación, o bien un administrador de un grupo, a cuyos reports podrán suscribirse sólo los usuarios de ese grupo.

Un informe tiene definida una periodicidad. Así podremos crear reports que se ejecuten diariamente, semanalmente (cada lunes), mensualmente (cada día 1 de mes), o nunca.

Los informes son especialmente útiles para las personas que gestionan un grupo para recibir los datos periódicamente sin tener que ir a buscarlos a la aplicación.

Veamos cada uno de los apartados:

Suscripciones a informes

A este mantenimiento tiene acceso todos los usuarios, no obstante sólo un usuario de nivel Administrador de SIGVI podrá ver todas las suscripciones, de otro modo un usuario sólo podrá ver las suyas.

Subscriptions to reports		Reports	TAGs
		Total: 7 rows	
User ID	Report ID		
dev.user6	Full report		
bo.user1	Full report		
bo.user3	Full report		
bo.user4	Full report		
	Full report		
dev.user2	Full report		
admin	Full report		

figura 30: Suscripciones a informes

Cada ejecución de un report al que estemos suscritos implica el envío de un email, a menos que tengamos inhabilitado el envío de email en nuestro perfil (ver [3.6.1](#)).

Informes

Los informes los podrán crear administradores de SIGVI y administradores de grupos. Dependiendo del nivel podrán crearlos con un espectro mayor de uso, es decir, que los informes que cree un administrador de grupo sólo podrán usarse dentro de su grupo.

Subscriptions to reports		Reports	TAGs
Search <input type="checkbox"/>		Total: 4 rows	
Name	Group	Description	Periodicity
Vulnerability evolution			Daily
Full report			Daily
Informe d'estat de l'aplicacio	SIGVI Adm		Never
About alerts			Never

figura 31: Informes

En la pantalla de creación aparecen los campos:

- Nombre: es el nombre del informe al cual se podrá hacer referencia,
- Grupo: Si está en blanco podrá ser usado por cualquier usuario de cualquier grupo, si está fijado a un grupo sólo los usuarios de ese grupo tendrán acceso a él. Si somos un Administrador del SIGVI como en el siguiente ejemplo, podremos fijar el grupo que podrá usar el informe o bien dejarlo en blanco de manera que cualquier grupo podrá usarlo, de otra manera aparecerá fijado por el grupo del usuario.
- Contenido: es el informe en sí. Es un campo de texto enriquecido en el que podremos editar usando las opciones del editor Web. Dentro del informe podremos ir intercalando los TAGs que podemos ir extrayendo del desplegable que está justo encima o bien teclearlos a mano. Estos TAGs son los que

serán sustituidos por un valor en el momento de ejecución.

- Descripción: orientativo del contenido del informe
- Periodicidad: diario, semanal, mensual o nunca.

The screenshot shows a dialog box for creating a report. It has several fields and a large text area:

- Name:** My Report *
- Group:** Back Office
- Content:** A rich text editor containing the following text:
Testing report
Dear SIGVI user {USER_NAME}, this is a test of report for you and anyone else of your group.
Would you like to see a graph?. All right, here is one comparing the evolution of the vulnerabilities loaded on SIGVI versus the alerts created for your group {USER_GROUP_NAME}
{VULNERABILITY_VS_ALERT}
Also, you can include a lot of more information here, for example the result of queries, web services, more graphs, value of system vars, defined constants... Anything that you can find at the TAGs tab.
Giving the format that you want.
Now inser data into a table:

User name:	{USER_NAME}
Level:	{USER_LEVEL_NAME}

I hope you can find it useful. Visit the page at sigvi.upcnet.es
Bye!
- Description:** A large empty text area.
- Periodicity:** Daily *
- Buttons:** Accept, Cancel

figura 32: Creación de un informe

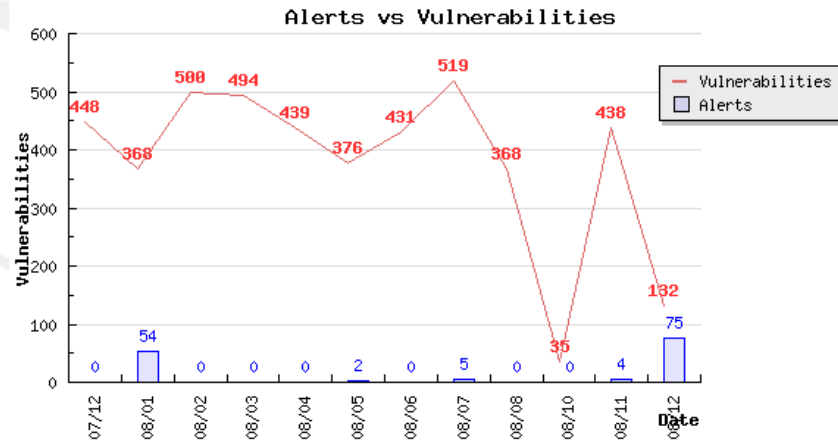
Al finalizar podemos presionar sobre el enlace del nombre del nuevo report y podremos previsualizar el resultado. Hay que tener en cuenta que muchos de los TAGs extraen información en función del usuario para el cual se está creando. Esta información en tiempo de ejecución cuando se lanza desde el proceso batch se obtiene por cada suscripción.

En la previsualización la información de usuario que se usa es la del que está conectado:

Testing report

Dear SIGVI user *admin*, this is a test of report for you and anyone else of your group.

Would you like to see a graph?, All right, here is one comparing the evolution of the vulnerabilities loaded on SIGVI versus the alerts created for your group **SIGVI Adm**



Also, you can include a lot of more information here, for example the result of queries, web services, more graphs, value of system vars, defined constants... Anything that you can find at the TAGs tab.

Giving the format that you want.

Now inser data into a table:

User name:	admin
Level:	SIGVI Adm

I hope you can find it useful. Visit the page at sigvi.upcnet.es

Bye!

figura 33: Previsualización de un informe

TAGs

Son las piezas con las que podemos construir la parte dinámica de un informe. Los tags solamente pueden ser creados por un Administrador del SIGVI, dado que permiten realizar consultas contra la base de datos.

En la primera versión RC1 se distribuirán una batería inicial con los más inmediatos, pero es una lista que puede crecer rápidamente.

Este es un fragmento del listado inicial:

Subscriptions to reports		Reports	TAGs			
Search <input type="text"/>			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		

figura 34: TAGs

Un TAG podrá incluir a su vez otros TAGs, lo que puede acabar en recursividad. En la primera versión de reports no se detecta la recursividad a mayor nivel de 1 (que esté incluido en sí mismo). Por tanto hay que tener cierto cuidado con este aspecto ya que el proceso acabaría cuando se llenara la memoria asociada al proceso.

Los TAGs pueden ser de distintos tipos:

- Constant: el valor está indicado directamente en el campo “valor”
- Graph: referencia un script PHP que genera graficas
- Image: referencia una imagen
- Operation: permite operadores aritméticos simples (+, -, ...)
- Query: una consulta a base de datos que retorna un único valor.
- Var: retornará el valor de una variable de la aplicación (si existiera)
- Web Service: realiza una llamada a un Web Service (en un formato concreto)

Finalmente podrá indicarse si el TAG es público o no. Si es público podrá ser usado por cualquier usuario que pueda crear un informe. Si no es público sólo podrá ser usado por administradores del SIGVI, tanto a la hora de referenciarlos en un informe como en tiempo de ejecución.

3.8.6. Estadísticas

En esta página encontramos diversos resúmenes predefinidos mostrando información relativa a los datos recogidos por SIGVI.

En la versión actual (R2 Release Candidate 1) son:

- Contador de vulnerabilidades: Muestra la evolución del último año del número de vulnerabilidades aparecidas cada mes.

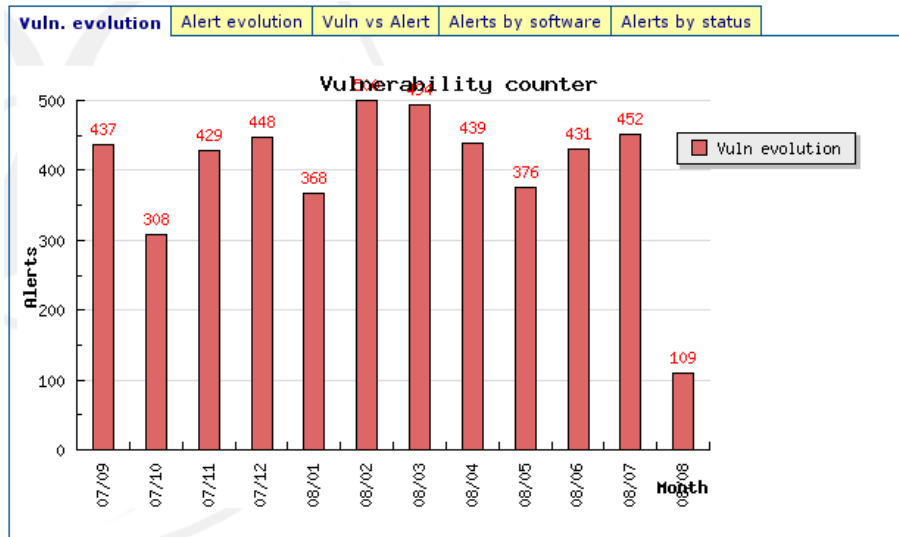


figura 35: gráfica de evolución de vulnerabilidades

- Evolución de las alertas: Muestra la evolución del número de alertas generadas cada mes durante el último año.

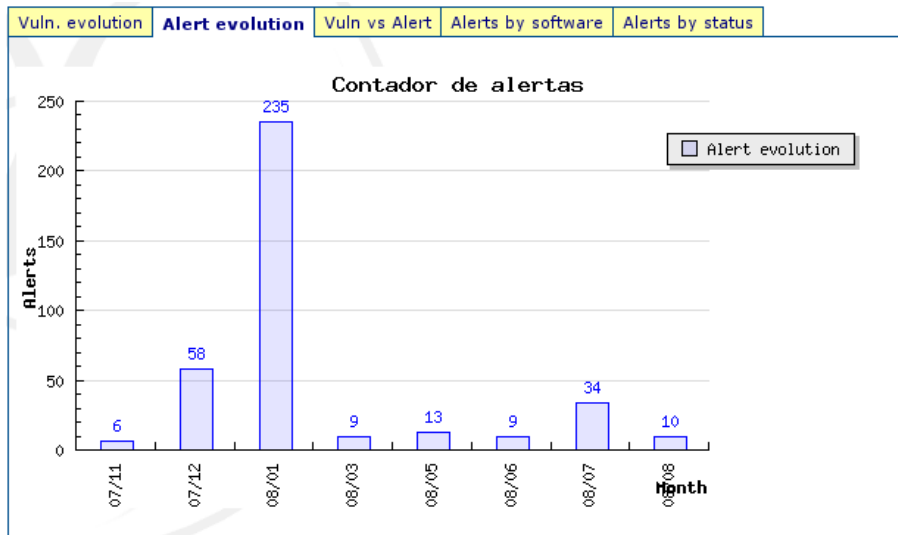


figura 36: gráfica de evolución de alertas

- Comparación de la evolución de las vulnerabilidades con la evolución de las alertas: Muestra en una misma gráfica las dos anteriores con los valores del último año. Para cada mes aparecen representadas el número de vulnerabilidades y de alertas generadas.

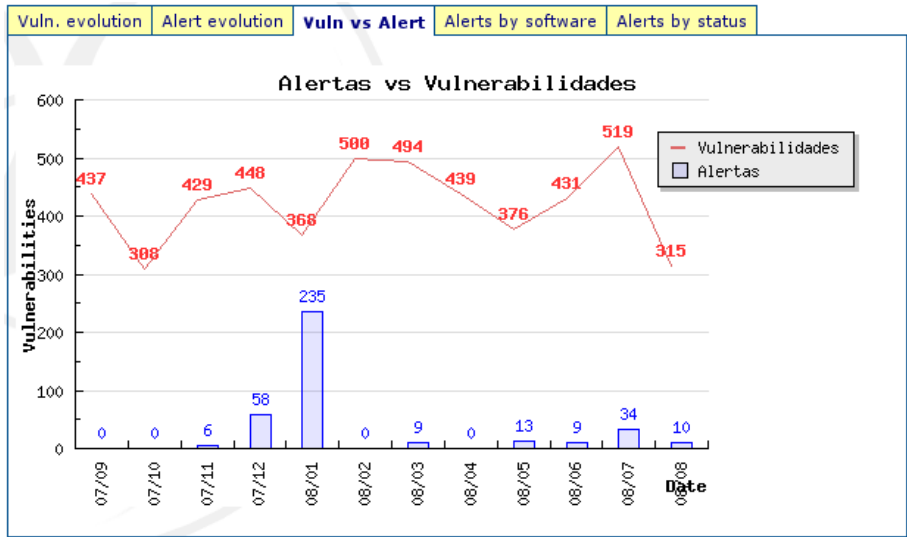


figura 37: gráfica comparativa de evolución vulnerabilidades vs alertas

- Desglose de las alertas por el software afectado: Un gráfico de pastel donde podremos ver en qué se reparte el total de alertas en cuanto a tipo de software afectado.

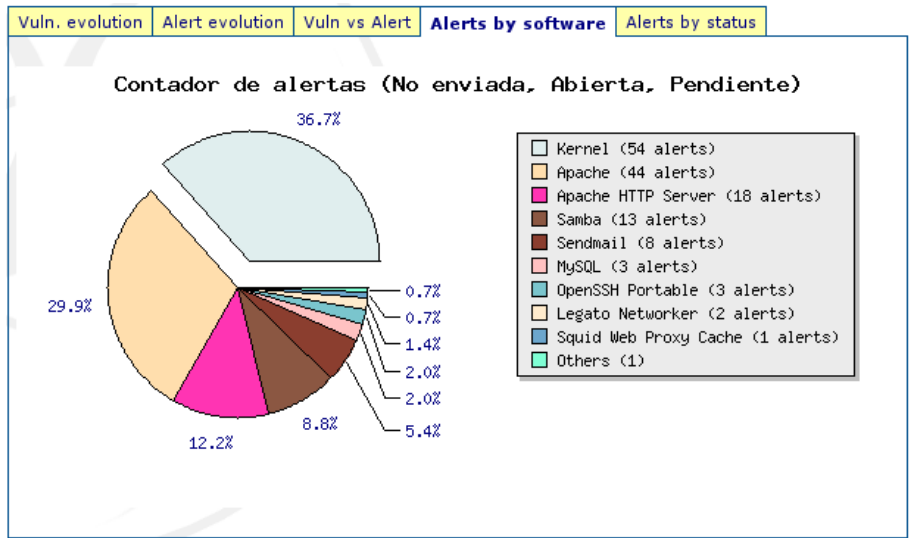


figura 38: gráfica de agrupamiento de alertas por producto

- Alertas por estado: nos permitirá ver rápidamente el estado de las alertas de nuestro grupo.

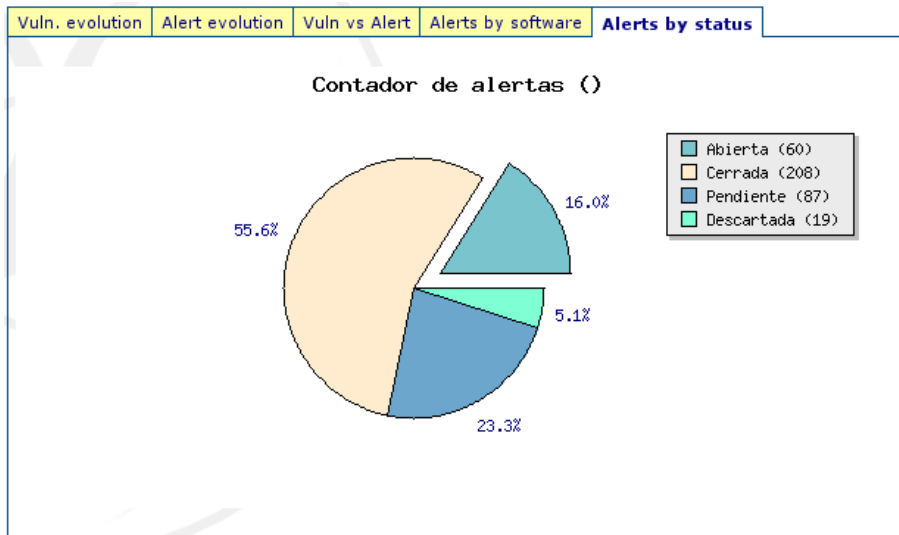


figura 39: gráfica de agrupamiento de alertas por estado

4. Inicio y uso del SIGVI R2 del Administrador del SIGVI

¿Cuáles son las funciones del administrador del SIGVI?

Las funciones del administrador del SIGVI son básicamente:

- configurar el entorno de la nueva instancia del SIGVI
- inicialización de las vulnerabilidades
- alta y gestión de los grupos
- mantener el correcto funcionamiento del entorno, estando al tanto de los resúmenes diarios del estado final de los procesos nocturnos
- actualización periódica de ciertas partes de la aplicación, como por ejemplo las fuentes de vulnerabilidades

Al comenzar a usar la instancia del SIGVI será el administrador del SIGVI quien deberá configurar el nuevo despliegue.

Además de las tareas de configuración general de la instancia que se explica en la documentación técnica, hay que realizar varias tareas para dejar el entorno a punto para su correcto funcionamiento.

4.1. Inicio

Al comenzar con una nueva instancia del SIGVI, será el administrador del SIGVI el responsable de la configuración inicial, tanto a nivel de sistema, de configuración interna, como de despliegue.

4.1.1. Configuración del entorno

Consulte el manual técnico para ver cómo se instala y se configura inicialmente el SIGVI para que se pueda acceder correctamente, así como la activación o desactivación de las partes optativas.

4.1.2. Configuración de las fuentes de vulnerabilidades

La utilidad del SIGVI radica en tener datos reales, fiables y actualizados tanto de las vulnerabilidades como de los productos instalados en los servidores. De la segunda parte se encargarán los administradores de equipos, pero la primera es responsabilidad directa del administrador del SIGVI.

Por defecto el SIGVI proporciona una serie de fuentes y plugins basados en el estándar CVE para descargar las definiciones de las vulnerabilidades desde el NVD. Por defecto sólo dos fuentes referentes a actualizaciones y novedades son las que están activas.

No obstante, es recomendable realizar una carga de todas ellas al principio. Para realizar esta tarea puede consultar el capítulo [3.7.3](#), donde se explica cómo.

4.1.3. Crear los grupos

Los usuarios finales del SIGVI son los administradores de equipo, que pertenecen a un grupo. Los administradores de grupo son las figuras que deben encargarse de la creación y gestión de los usuarios de su grupo.

El administrador del SIGVI es el único que puede crear y gestionar la definición de los grupos. De este modo inicialmente deberá crear los grupos necesarios en su entorno y definir los responsables de cada uno de ellos (pueden ser varios). No es su función la gestión de los datos internos de cada grupo, como los servidores, alertas, productos instalados, etc.

4.2. *Uso diario*

El uso diario del administrador del SIGVI se debería centrar básicamente en corregir posibles problemas de sistema o de configuración, sin tener que entrar a revisar problemas internos en los grupos o sus datos.

La tarea principal y rutinaria del administrador del SIGVI es la revisión de los resúmenes de estado de los procesos.

4.2.1. *Revisar los resúmenes de estado de los procesos*

Los procesos nocturnos envían un resumen del estado final de éstos a los administradores del SIGVI. Es, por tanto, esta figura la responsable de velar por el perfecto funcionamiento de los procesos, revisando diariamente los resultados de estado para corregir posibles problemas.

Entre estos problemas podríamos encontrarnos, por ejemplo, que no se haya realizado la carga de vulnerabilidades porque, por ejemplo, en ese momento no funcionaba la red. En este caso sea bien por la ausencia del resumen de estado o bien por un resumen de estado incorrecto, deberá realizar la carga manual y lanzar el proceso de chequeo manualmente.

5. Inicio y uso del SIGVI R2 del Administrador de grupos

La figura del administrador de equipos tiene como funciones básicas:

- Alta y gestión de los usuarios del grupo
- Alta y gestión de los filtros para el grupo
- Alta y gestión de las funciones FAS para el grupo
- Revisión de las alertas dudosas de su grupo

5.1. Inicio y uso

Una vez el administrador del SIGVI haya creado su grupo y su usuario, usted deberá iniciar la información de su grupo.

5.1.1. Gestión de usuarios

Lo primero será comenzar creando usuarios del nivel administrador de equipos en su grupo, quienes podrán realizar el resto de tareas de alta y gestión de servidores y asociarlos a productos, información necesaria para que el SIGVI represente una utilidad para su grupo.

5.1.2. Gestión de los filtros

Aunque no es necesario, puesto que el uso de los filtros es optativo, usted podrá crear los filtros que considere necesarios para los usuarios de su grupo (consulte el punto [3.6.3](#)).

5.1.3. Gestión de las funciones FAS

Del mismo modo ocurre con las funciones FAS (consulte el punto [3.6.4](#)).

5.1.4. Revisión de las alertas dudosas

En cuanto a las tareas diarias, el administrador del grupo será el responsable de validar o descartar las alertas dudosas (consulte el punto [3.4.1](#)). Las alertas que el motor de comparación del SIGVI no está seguro de si descartarlas o no, se crean como “pendientes de validar” de manera que es responsabilidad del administrador del grupo tomar esa decisión.

Este tipo de alertas no son visibles por los administradores de equipos, que son quienes finalmente analizarán las alertas para determinar qué hay que hacer. Es importante validar o descartar las alertas lo antes posible para poder actuar lo antes posible.

6. Inicio y uso del SIGVI R2 del Administrador de equipos

Como administrador de equipos en SIGVI R2, ¿cuál es el primer paso? ¿Para qué me sirve esta aplicación y qué puedo hacer con ella?

6.1. Inicio

6.1.1. ¿Qué es el SIGVI y para qué sirve?

El SIGVI es una herramienta que trata de ayudar precisamente al administrador de los servidores en la detección y gestión de vulnerabilidades informáticas en los servidores.

Los administradores de sistemas tienen que dedicar mucho tiempo en la detección y gestión de vulnerabilidades. Estas tareas rutinarias como son leer las notificaciones de vulnerabilidades que envían desde las subscripciones, comparar con el listado de software de los servidores que administra, y finalmente, si afecta, recavar información de acciones a tomar y actuar.

La funcionalidad final del SIGVI es delegar en él todo ese proceso, a excepción de la actuación, la detección y gestión de las vulnerabilidades de nuestros equipos, para que el administrador únicamente deba preocuparse cuando el SIGVI le envíe una notificación avisando sobre una vulnerabilidad en uno de sus equipos.

El SIGVI, partiendo de la lista de sus servidores y de los productos que ha declarado que tienen instalados, examinará cada día por si aparece alguna vulnerabilidad que afecte a alguno de esos productos. En caso afirmativo creará una alerta (ver [3.4.2](#)) y le enviará por el mecanismo que se haya definido en la instancia del SIGVI (por defecto vía email).

6.1.2. Primer paso: introducción de los datos

Para que el SIGVI pueda notificar a los administradores de las vulnerabilidades en sus equipos es necesario, primero, dar de alta los servidores, y luego, para cada uno de ellos dar de alta el software más importante que tenga instalado (Sistema Operativo, Software que da servicio a otros servidores o Internet, ...). Para ello vea el capítulo [3.5.2](#) sobre el inventario, concretamente servidores y productos.

Una vez haya dado de alta sus servidores y los servicios (o software o productos) más importantes ya comenzará a recibir, a partir de la siguiente ejecución de los procesos nocturnos, las alertas de vulnerabilidades (cuando las haya).

6.2. Uso diario

6.2.1. Me ha llegado una notificación por email, ¿ahora qué hago?

Cuando SIGVI detecta que una vulnerabilidad en alguno de los productos crea una alerta en el repositorio de alertas y le enviará una notificación (por defecto vía email). Esta notificación que recibe es un resumen de la alerta, mostrando cuál es el servidor, afectado, el producto vulnerable y la vulnerabilidad que lo afecta, incluyendo las URLs del declarante donde poder acudir a buscar información relativa a la resolución o qué medidas se deben tomar.

Además incluye el FAS (Final Absolute Severity, ver capítulo [3.6.4](#) sobre las funciones FAS), que es un número entre 0 y 10 que indica cómo de grave es el asunto, de este modo ayudarle a tomar una decisión rápida y saber si es crítico o no.

A partir de esta notificación debería trabajar con la alerta del SIGVI, donde podrá determinar el estado de la alerta, agregar los comentarios oportunos para el trabajo en equipo, etc.

Para ello acceda a su instancia del SIGVI, introduzca su usuario y su contraseña y acceda al menú de alertas activas, donde encontrará las alertas abiertas o pendientes de su grupo.

Para cada una de ellas, podrá acceder a la información de la vulnerabilidad, donde, además de los detalles de la propia vulnerabilidad, encontrará por lo general enlaces a páginas donde el fabricante o terceros recomiendan acciones a tomar.

Piense que esta herramienta no actuará por usted, lo que intenta es poner a su disposición toda la información que pueda necesitar para tomar una decisión.

6.2.2. He actualizado la versión de un programa en el servidor, ¿tengo que cambiarlo en SIGVI?

Si. Piense que si no lo hace, las alertas y notificaciones que se generan en el SIGVI es usando la información que usted haya introducido. Si los datos que tenga en el SIGVI no son los reales, las notificaciones y alertas no tienen por qué serlo.

Es muy importante que la información del SIGVI refleje la realidad.

6.3. Información de las vulnerabilidades

6.3.1. Me he cansado de tanto resumen diario, ¿Cómo puedo desactivarlos?

En la página de configuración de su usuario usted podrá configurar si desea ser notificado o no con el resumen diario de vulnerabilidades en el campo “Recibe el resumen diario de vulnerabilidades”.

6.3.2. Los resúmenes tienen demasiada información

Pese a que los resúmenes son únicamente a modo informativo, dado que el control de la detección de las vulnerabilidades lo tendrá el SIGVI, usted puede restringir la información del resumen, usando el filtro de notificaciones que podrá indicar en la página de configuración de su usuario, concretamente el campo “Filtro de notificaciones”.

Vea el punto [3.6.3](#), sobre filtros.

Índice de figuras

figura 1: Formato de las páginas.....	6
figura 2: página de login.....	8
figura 3: página principal.....	12
figura 4: Menú TO-DO.....	12
figura 5: Alertas.....	15
figura 6: Resumen de estado de alertas.....	16
figura 7: Menú de inventario.....	16
figura 8: Servidores.....	17
figura 9: Servicios: productos instalados en los servidores.....	18
figura 10: Repositorio de productos.....	19
figura 11: Respositorio de vulnerabilidades.....	20
figura 12: Menú de administración.....	20
figura 13: Mi usuario.....	21
figura 14: Grupos.....	22
figura 15: Usuarios.....	22
figura 16: Filtros.....	23
figura 17: Final Absolute Severity.....	24
figura 18: Menú de configuración.....	26
figura 19: Configuración general de la instancia.....	27
figura 20: Administrador de tareas.....	28
figura 21: Administrador de fuentes de vulnerabilidades.....	29
figura 22: Gestión de fuentes RSS.....	30
figura 23: Gestión de diccionarios CPE.....	30
figura 24: Métodos de notificación.....	31
figura 25: menú de herramientas.....	31
figura 26: Interacción con la Base de Datos.....	32
figura 27: Logs de la aplicación.....	32
figura 28: Mailing.....	33
figura 29: Bugs.....	34
figura 30: Subscripciones a informes.....	35
figura 31: Informes.....	35
figura 32: Creación de un informe.....	36
figura 33: Previsualización de un informe.....	37
figura 34: TAGs.....	38
figura 35: gráfica de evolución de vulnerabilidades.....	39
figura 36: gráfica de evolución de alertas.....	39
figura 37: gráfica comparativa de evolución vulnerabilidades vs alertas.....	40
figura 38: gráfica de agrupamiento de alertas por producto.....	40
figura 39: gráfica de agrupamiento de alertas por estado.....	41