

SIGVI R2

Manual de l'Usuari

Índex

1. Introducció.....	4
1.1. Administrador del SIGVI.....	4
1.2. Administrador de grup.....	5
1.3. Administrador de equips.....	5
2. Elements generals de les pantalles.....	6
3. Pàgines.....	8
3.1. Login.....	8
3.2. Logout.....	8
3.3. Menú principal.....	9
3.4. TO-DO.....	12
3.4.1. Alertes pendents de validar.....	12
3.4.2. Alertes.....	12
3.4.3. Resum d'alertes en els servidors.....	16
3.5. Menú d'inventari.....	17
3.5.1. Alertes.....	17
3.5.2. Servidors i productes.....	17
Servidors.....	17
Serveis: Productes instal·lats en els servidors.....	19
3.5.3. Productes.....	20
3.5.4. Vulnerabilitats.....	21
3.6. Administració.....	22
3.6.1. El meu usuari.....	22
3.6.2. Grups i usuaris.....	23
3.6.3. Filtres.....	25
Definició.....	26
¿Cóm es filtra?.....	26
Usos.....	27
3.6.4. FAS.....	27
Quin és el meu FAS?.....	29
Com es construeix una FAS?.....	30
3.7. Configuració.....	31
3.7.1. Configuració (genèric).....	31
Configuració.....	31
Paràmetres globals.....	34
3.7.2. Administració de tasques.....	34
3.7.3. Fonts.....	35
Fonts de vulnerabilitats.....	35
Gestió de les fonts RSS.....	37
Gestió dels diccionaris de productes (CPE).....	37
3.7.4. Mètodes de notificació.....	38
3.8. Eines.....	38
3.8.1. Base de datos (DDBB).....	39

3.8.2.Logs.....	39
3.8.3.Mailing.....	40
3.8.4.Bugs de l'aplicació.....	41
3.8.5.Informes.....	42
3.8.6.Estadístiques.....	42
4. Inici i ús del SIGVI R2 de l'Administrador del SIGVI.....	45
4.1. Inici.....	45
4.1.1.Configuració de l'entorn.....	45
4.1.2.Configuració de les fonts de vulnerabilitats.....	45
4.1.3.Crear els grups.....	45
4.2. Ús diari.....	46
4.2.1.Revisar els resums d'estat dels processos.....	46
5. Inici i ús del SIGVI R2 de l'Administrador de grups.....	47
5.1. Inici i ús.....	47
5.1.1.Gestió de usuaris.....	47
5.1.2.Gestió dels filtres.....	47
5.1.3.Gestió de les funcions FAS.....	47
5.1.4.Revisió de les alertes dubtoses.....	47
6. Inici i ús del SIGVI R2 de l'Administrador de equips.....	48
6.1. Inici.....	48
6.1.1.Què és el SIGVI i per a què serveix?.....	48
6.1.2.Primer pas: introducció de les dades.....	48
6.2. Ús diari.....	48
6.2.1.M'ha arribat una notificació per e-mail, ara què faig?.....	48
6.2.2.He actualitzat la versió d'un programa en el servidor, he de canviar-lo en SIGVI?.....	49
6.3. Informació de les vulnerabilitats.....	49
6.3.1.M'he cansat de tant resum diari, com puc desactivar-los?.....	49
6.3.2.Els resums tenen massa informació.....	49

1. Introducció

SIGVI són les sigles de Sistema Intel·ligent de Gestió de Vulnerabilitats Informàtiques. És una eina que serveix per a detectar i gestionar les vulnerabilitats dels sistemes informàtics.

Aquest projecte es desenvolupa i manté des de UPCnet, empresa de serveis TIC del grup UPC (Universitat Politècnica de Catalunya). També ha estat co-finançat durant el 2008 pel Ministeri d'Indústria, Turisme i Comerç d'Espanya (MITYC, www.mityc.es) per a l'obtenció d'un producte precompetitiu.

El SIGVI és una aplicació Web composta per un conjunt de scripts programats en PHP que implementen la lògica de l'aplicació i una base de dades relacional on es guarden les dades. Alguns scripts s'executen com a processos batch (generalment per la nit) per realitzar les tasques que no requereixen la interacció humana, com per exemple les càrregues de vulnerabilitats des de les fonts, la revisió de les vulnerabilitats en els nostres sistemes, etc. La resta són els scripts que programa la pròpia aplicació Web.

Aquesta aplicació està orientada a l'usuari final, a l'administrador de sistemes en la seva feina diària de detecció i gestió de vulnerabilitats en els servidors. Però per a facilitar-li la tasca s'han definit diversos perfils d'usuari, deixant labors d'administració de la pròpia aplicació a altres figures.

D'aquesta manera, hi ha tres perfils d'usuari:

- Administrador del SIGVI: És l'administrador general de l'aplicació, la seva funció serà la de realitzar tasques d'administració general en l'aplicació.
- Administrador de Grups: És la figura que administra les dades generals d'un grup, responsable de la gestió dels usuaris d'aquest i d'altres tasques administratives.
- Administrador d'Equips: És l'usuari que finalment farà ús de les funcionalitats pròpies de la gestió de vulnerabilitats.

1.1. *Administrador del SIGVI*

És el perfil amb major nivell d'accés, permetent-li accedir a tots els apartats de l'aplicació amb tots els privilegis. No obstant això, la labor principal de l'administrador del SIGVI serà la gestió d'aquells apartats als quals només ell té accés:

- gestionar els grups (altes i baixes)
- gestió d'usuaris de nivell “Administrador del SIGVI” i “Administrador de Grup”
- gestió de les fonts de vulnerabilitats
- gestió de les fonts de productes (CPE)
- gestió de les fonts RSS de notícies
- gestió dels mètodes de notificació
- gestió dels paràmetres globals de l'aplicació
- gestió de la configuració global de l'aplicació
- gestionar els bugs d'aplicació (si estigués habilitat)

A més a més podrà:

- executar manualment els processos de càrregues de vulnerabilitats
- executar manualment els processos de comprovació de vulnerabilitats
- visualitzar els logs de l'aplicació
- interaccionar amb la base de dades

1.2. Administrador de grup

El fet que existeixi aquesta figura es déu bàsicament a centrar la gestió dels usuaris d'un grup en una figura amb un nivell d'accés intermedi entre l'administrador del SIGVI i l'administrador d'equips. La funció més important de l'administrador de grups serà l'alta, baixa i modificació dels usuaris del seu grup.

A més a més podrà:

- validar o descartar les alertes pendents de validació
- gestionar els filtres de notificació i detecció del grup
- gestionar les funcions de càlcul del factor d'impacte (FAS) del grup

1.3. Administrador de equips

L'administrador d'equips és la figura de l'aplicació que representa l'operador o administrador de sistemes. Serà l'encarregat de vetllar, entre altres coses, de l'estat de seguretat dels seus servidors.

La finalitat del SIGVI és ajudar en las tasques de supervisió de l'estat de seguretat dels servidors al administrador d'equips.

Les funcionalitats més importants que tindrà disponibles per al seu dia a dia són:

- gestionar els servidors del seu grup (altes, baixes, modificacions),
- gestionar el software que té instal·lat cadascun dels servidors del seu grup,
- gestionar les alertes de vulnerabilitats del seu grup.

A més d'aquestes podrà:

- veure els filtres de notificació,
- veure les fórmules de càlcul del factor d'impacte,
- veure l'estat general de vulnerabilitats dels servidors del seu grup,
- accedir als resums generals,
- accedir als bugs de l'aplicació i crear nous.

2. Elements generals de les pantalles

Abans de començar a explicar amb detall cadascun dels apartats de l'aplicació és convenient explicar breument els components de les pantalles comunes a l'aplicació.

Pràcticament totes les pantalles estan creades usant la mateixa plantilla, que es divideix en tres parts: capçalera, contingut de la pròpia pàgina, i peu de pàgina.

En la següent imatge les veiem desglossades en un exemple d'una pàgina:

The screenshot shows the 'Groups and users' page in the SIGVI R2 Enterprise application. The interface is divided into three main sections: a header, a main content area, and a footer. The header (1) contains the application logo, version, and user information. The main content area (2) includes a navigation menu, a search bar (3), and a table of users. The table (4) has columns for user details and actions. The footer (6) contains version and copyright information.

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: Format de les pàgines

- **1. Logotip, títol, informació d'usuari i accessos ràpids**

En la part superior esquerra de la pàgina apareix el logotip del SIGVI (que és un enllaç amb la pàgina principal) junt amb el nom de la versió instal·lada (en aquest cas R2 Enterprise).

En la part superior dreta es mostren les icones d'accés ràpid a l'ajut (en les pàgines que sigui disponible), a la declaració de bugs (problemes detectats en la aplicació) i desconnexió. La gestió de bugs haurà de ser habilitada al fitxer de configuració de la aplicació (app.conf.php).

Sota aquesta botonera apareix informació de l'usuari connectat: nom d'usuari, grup i nivell d'accés.

- **2. Menú**

És el menú de l'aplicació accessible des de qualsevol pàgina. Agrupats per temes, trobarem els accessos a las pàgines de gestió i d'eines de l'aplicació.

- **3. Barra de cerca i d'eines d'un manteniment**

Alguns manteniments permeten realitzar cerques per reduir els registres que apareixen.

D'altra banda, i si tenim els permisos suficients, apareixeran aquests botons, que permetran refrescar el contingut del manteniment, afegir un nou registre o bé, si el manteniment ho permet, exportar els resultats a un fitxer en un format que podrem usar des d'una full de càlcul (CSV).

- **4. Nombre de files mostrades**

Es mostra el nombre de registres trobats. Si el nombre de files que s'han trobat superen un màxim de pàgina es produirà una paginació, on apareixerà una barra de navegació amb fletxes per a moure's a través de les pàgines.

- **5. Accions sobre els registres**

Depenent dels permisos, podrem modificar els registres o eliminar-los.

- **6. Informació de pàgina**

Finalment apareix informació sobre el temps de creació de la pàgina i la versió de la instància.

3. Pàgines

Vegem ràpidament les pàgines que existeixen en el SIGVI R2. Depenent del seu perfil d'usuari, vostè veurà disponibles només algunes d'elles, i depenent d'aquestes vostè només podrà realitzar certes tasques dintre d'elles.

El que es mostrarà a continuació és la vista d'un administrador del SIGVI.

Nota: Per a aquest document, i amb la finalitat de poder representar el màxim d'informació possible en les il·lustracions, apareixeran desactivades les imatges corporatives que poden ser activades o desactivades a través del fitxer general de configuració de l'aplicació.

3.1. Login

Quan accedim a la instància de l'aplicació SIGVI, el primer que hauríem de fer serà autenticar-nos des de la pantalla de login. En la pantalla de login hauríem d'indicar un usuari i una contrasenya vàlids. Mentre l'autenticació no sigui correcte no podrem avançar.

La comprovació de l'usuari i la contrasenya es realitzarà en funció de com s'hagi donat d'alta l'usuari, ja que l'autenticació tant es pot fer usant una contrasenya local (emmagatzemada en la base de dades), o remotament usant serveis disponibles a tal fi, com per exemple serveis LDAP.



figura 2: pàgina de login

Qui creu l'usuari haurà de notificar a l'usuari quin és el mètode d'autenticació que haurà d'usar per a accedir a l'aplicació.

3.2. Logout

Per a sortir de l'aplicació podem pressionar l'enllaç de sortida o logout que apareix en la capçalera, d'aquesta manera es tancarà la sessió en el servidor s'alliberarà tota la informació temporal emmagatzemada. No obstant això, les sessions tenen un temps de vida limitat, normalment d'entre 5 i 10 minuts, que ve definit en la configuració del servidor Web on s'allotja la instància del SIGVI. Quan passa aquest interval de temps sense connexió des de el client, es tanca automàticament aquesta sessió.

Una vegada tancada la sessió, la pròxima pantalla que aparegui al intentar accedir a la instància del SIGVI serà la de login.

3.3. Menú principal

Després d'una autenticació correcta, passarem a la pantalla principal, on tindrem disponibles totes les funcionalitats del nostre perfil. A continuació es mostra la pantalla que veuria un administrador del SIGVI:

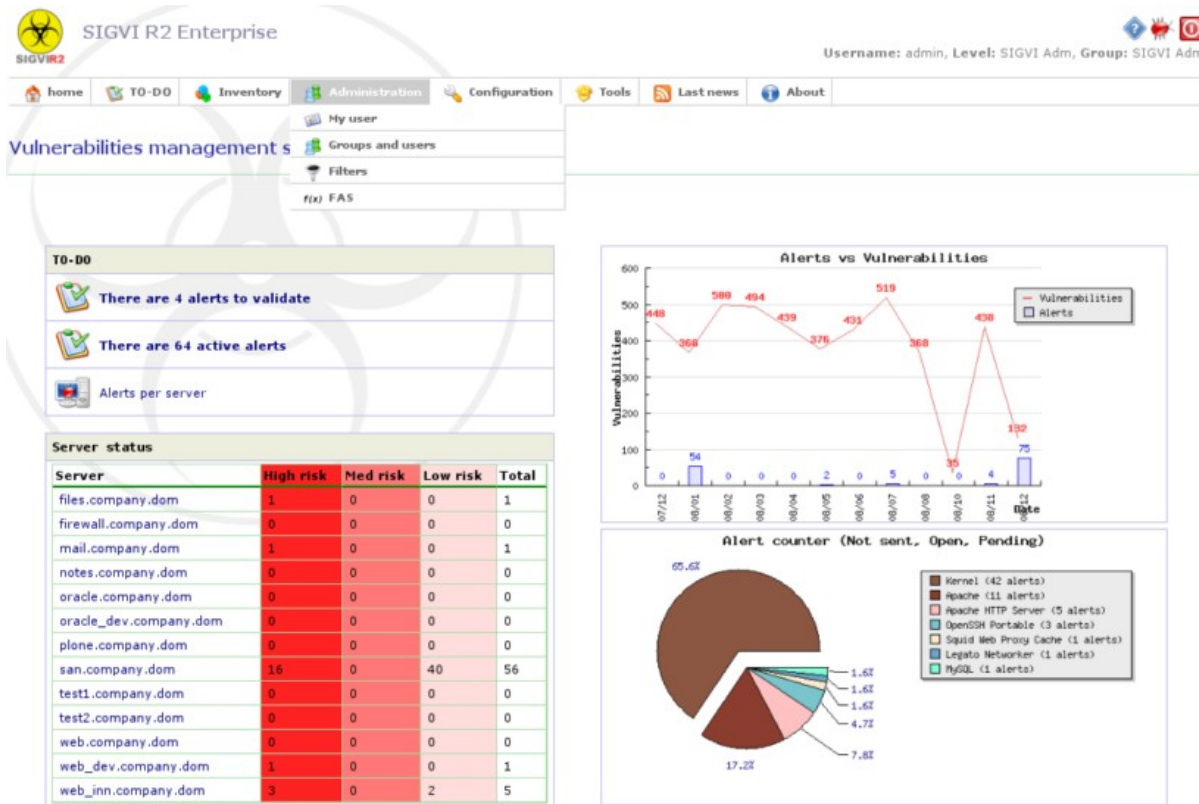


figura 3: pàgina principal

Cadascuna d'aquestes parts són:

- Capçalera de la pàgina: logotip, accessos ràpids, informació d'usuari, menú, títol de pàgina.
- Menú "TO-DO": on apareix el resum de l'estat general de revisió i resolució de vulnerabilitats per al seu grup.
- Estat dels servidors: per a cadascun dels servidors del seu grup, apareix desglossat el nombre de vulnerabilitats pel que es veu afectat, és a dir, el nombre d'alertes obertes.
- Gràfica comparativa entre l'evolució del nombre de vulnerabilitats descarregades vs les alertes aparegudes als seus servidors l'últim any.
- Gràfica informativa sobre com es reparteix el total d'alertes en funció del tipus de software.

3.4. TO-DO



figura 4: Menú TO-DO

Aquest és el grup d'enllaços a les pàgines habituals de treball, on s'indicarà un resum del volum de tasques pendents.

En el cas de l'administrador d'usuari, aquí apareixerà únicament l'enllaç amb les alertes obertes en els servidors del seu grup.

3.4.1. Alertes pendents de validar

En certes ocasions el motor de recerca del SIGVI pot tenir dubtes sobre si una vulnerabilitat afecta a un producte d'un servidor. En aquests casos no és aconsellable descartar-les, així que es genera una alerta como “dubtosa”. Aquest tipus d>alertes no es notifiquen fins que algun administrador de SIGVI o de grup decideixi què fer amb elles.

Aquestes alertes apareixeran en aquesta pantalla separada, que no serà visible pels administradors d'equips.

La finalitat d'aquesta funcionalitat es disminuir el nombre de falsos positius de l'aplicació per a no generar més treball del realment necessari. No obstant això SIGVI R2 no decidirà per l'usuari si les alertes dubtoses han de ser descartades, perquè això podria provocar la pèrdua d>alertes reals.

Els administradors de grup tindran la responsabilitat de revisar periòdicament (preferiblement diàriament) aquest tipus d>alertes del grup. El SIGVI disposa de mecanismes automàtics per a recordar als responsables d'aquesta tasca de la revisió d'aquestes alertes.

Així mateix, passat un període definit en l'aplicació (per defecte 48 hores) las alertes en estat dubtós es passaran a estat “no enviat”, de manera que entraran en el següent procés de notificació després del qual passaran automàticament a estat “oberta”.

3.4.2. Alertes

Una alerta es crea quan un producte d'un servidor està afectat per una vulnerabilitat. En aquesta pàgina se'ns mostraran les alertes de vulnerabilitats que s'han detectat en els servidors del nostre grup.

Les alertes poden tenir 5 estats possibles: No enviada, Oberta, Tancada, Pendent o Descartada. En aquest manteniment podrem realitzar el seguiment de les vulnerabilitats dels nostres servidors per a passar-los d'un estat inicial (obert) fins que es tanquin o es descartin:

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%'

Total: 8 rows

Showing from row 26 to 33, of 33

	Server	Affected product	Vulnerability	Creation date	Status	Criticality	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			<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	fileserver.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"/>

Showing from row 26 to 33, of 33

figura 5: Alertes

Per defecte, quan ingresseu en aquesta pàgina només ens mostrarà les alertes obertes o pendents.

El significat dels estats és:

- *No enviada*: Cada vegada que s'executa el procés de revisió de vulnerabilitats, es creen les alertes en estat no enviat, el que provoca que altre procés posterior enviï notificacions a tots els administradors de totes aquelles alertes en estat "No enviada". Tot seguit es canvia, automàticament a "Obert". Si durant el procés de notificació es produís algun problema pel qual no pogués realitzar-se l'enviament l'alerta continuarà en estat "no enviada" per a ser processada de nou la pròxima vegada que s'executi aquest procés.

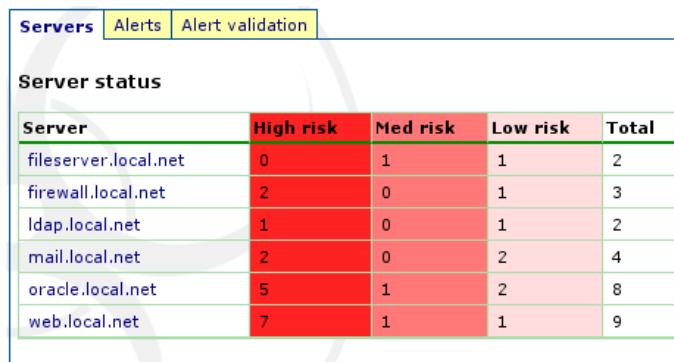
Posant una alerta en estat "No enviada" implicarà que s'envii una notificació sobre aquesta als administradors del grup al que correspon l'alerta.

- *Obert*: La alerta està llesta per a ser analitzada.
- *Tancada*: La vulnerabilitat de l'alerta ha estat solucionada.
- *Pendent*: La alerta està pendent.
- *Descartada*: La vulnerabilitat no afectava al producte indicat, o simplement es decideix descartar

l'alerta i no actuar sobre ella.

3.4.3. Resum d'alertes en els servidors

Des de la pàgina anterior podem accedir a una vista resumida de nombre d'alertes obertes per servidor, i separades per gravetat de l'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: Resum de estat d'alertes

3.5. Menú d'inventari

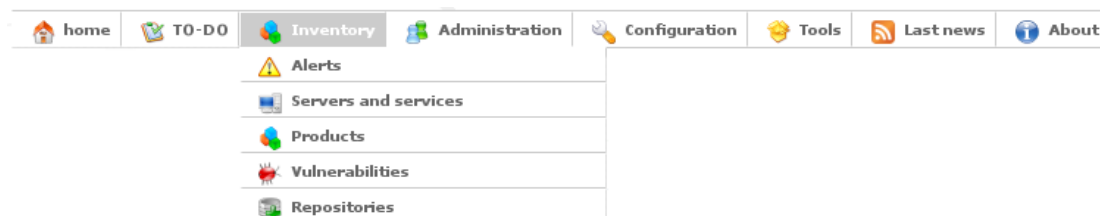


figura 7: Menú d'inventari

En aquest grup apareixen els enllaços relacionats amb la administració de les dades referents a les alertes, servidors i els seus serveis, els productes, les vulnerabilitats i els repositoris.

3.5.1. Alertes

Aquest enllaç ens porta a la pàgina de gestió de les alertes descrit en el punt 3.4.2.

3.5.2. Servidors i productes

Aquest és el punt d'entrada de la informació del nostre entorn. Per a poder conèixer l'estat dels nostres servidors hauríem de reflectir-los de la manera més fidel possible.

En aquest manteniment trobarem dues pestanyes, una on es definiran els servidors i un altre on s'indicarà els productes que té instal·lats.

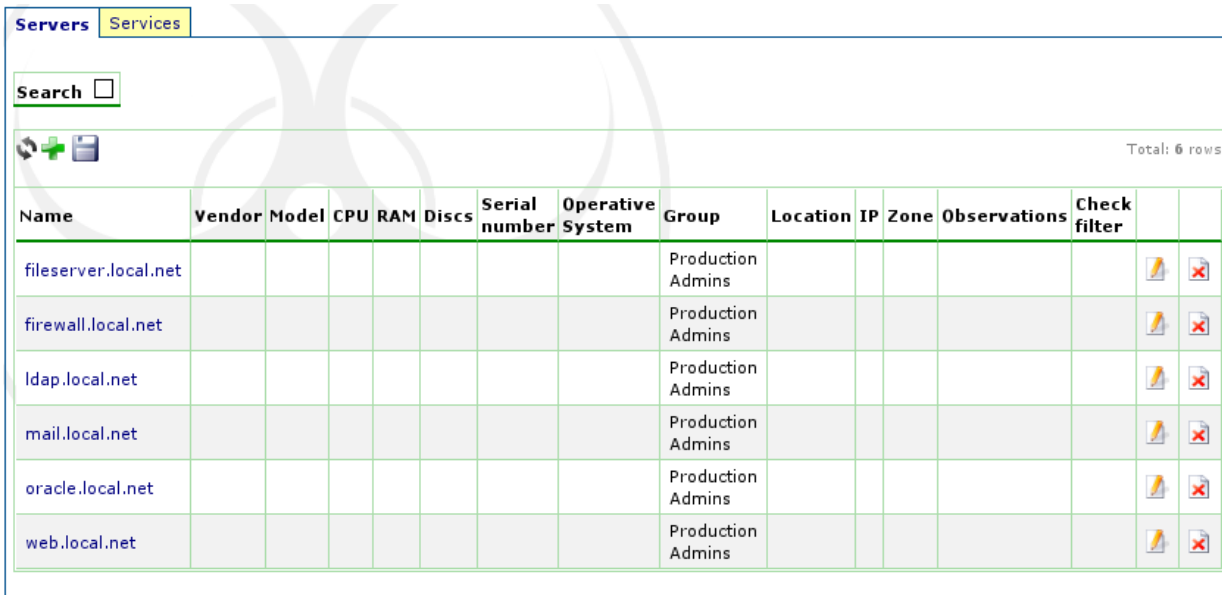
Servidors

La primera pestanya, servidors, li mostrarà els servidors del seu grup. Com administrador d'equips

podrà agregar i modificar la llista de servidors.

Les dades dels servidors són bastant arbitraris. Únicament s'usarà el nom del servidor i el filtre (si s'indiqués algun). La resta és informació descriptiva.

Un servidor no podrà estar repetit dins d'un grup.



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: Servidors

Serveis: Productes instal·lats en els servidors

La segona pestanya mostrarà els productes instal·lats en els servidors. Donar d'alta tots els productes que té instal·lat un servidor pot ser una tasca molt costosa, i si això ho multipliquem per N servidors, el resultat pot arribar a ser inviable en alguns entorns.

Per a començar, i en una primera fase de determinar l'estat de vulnerabilitats, podem centrar-nos únicament en el sistema operatiu i en els productes instal·lats que ofereixen algun servei a l'exterior del servidor, per exemple, un servidor Web, no donarem d'alta totes les llibreries que té instal·lades, podem començar amb el producte que té instal·lat i que dona el servei Web (Apache, IIS, Tomcat, ...). Al cap i a la fi, seran els serveis oberts els que puguin explotar-se remotament (els casos d'alerta més perillosos).

Existeix un projecte paral·lel al SIGVI R2 cridat **NSDi**, el qual servirà per a detectar automàticament el llistat de software dels servidors. És un projecte que actualment (en la versió actual del SIGVI) és una versió Alpha, que ja permet la integració amb el SIGVI, però que encara requereix treball d'enginyeria, programació i proves).

Nota: El comando nmap (<http://nmap.org/>) ens podrà ajudar a determinar quins serveis està oferint un servidor.

En el següent exemple veiem un fragment del llistat de software instal·lat en els servidors:

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 x	No	Yes				

figura 9: Serveis: productes instal·lats en els servidors

Com pot veure's, únicament s'ha donat d'alta els productes que estan donant el servei.

Quan donem d'alta un producte en un servidor, hauríem d'indicar obligatòriament el servidor, el producte i a més, per a aquest cas concret si el servei està filtrat (si és accessible des d'Internet), i si està proporcionant un servei crític (al nostre judici).

Pot ser un servei crític, el servidor Web corporatiu (imatge de la nostre empresa), un servei LDAP d'autenticació en el que es basin diferents aplicacions, un servei ORACLE de SAP, etc.

No hi ha una regla genèrica que ho defineixi. Simplement serà al nostre judici si ens sembla crític que aquest servei caigui o no (si arribés a ser atacat per una vulnerabilitat).

Pot passar que a l'associar el producte aquest encara no existeixi en el llistat de productes. Si es donés aquest cas vegi el següent punt: Productes (repositoris).

La resta dels camps son purament descriptius.

3.5.3. Productes

Es refereix al repositori de productes, el llistat global de productes que s'ha anat generant. En aquesta pantalla podrem consultar els productes que s'han anat introduint en el sistema. D'aquesta llista es de on s'obtidran els productes relacionats amb els servidors.

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: Repositoris de productes

El llistat es construeix a partir del software vulnerable i les entrades dels propis usuaris. És a dir, que un software que de moment no s'hagi trobat cap vulnerabilitat, no apareixerà en aquesta llista tret que algun usuari ho hagi introduït manualment.

Pot ocórrer que hàgim d'associar un software que encara no existeix en la llista. Hauríem de, en tal caso, donar-lo d'alta nosaltres mateixos. Aquest és el punt més crític de la configuració de l'aplicació, atès que el fet de determinar si un software és vulnerable o no es basa en la comparança del nom d'aquest software amb el del presentat en el llistat de software de la vulnerabilitat. Si el nom presentés algun tipus de desviació de l'estàndard, es probable que acabi per passar inadvertides les vulnerabilitats, i això és precisament el que es tracta d'evitar.

Consell: Cada venedor sol seguir un esquema de nomenclatura, és aconsellable, si cal donar d'alta un nou producte, primer veure com se'ls ha cridat a altres similars i usar aquest mateix esquema per al nou.

3.5.4. Vulnerabilitats

En aquesta pantalla accedim al repositoris de vulnerabilitats que s'han anat emmagatzemant a través de les càrregues de les fonts de vulnerabilitats en els processos batch.

Per defecte, al accedir a aquesta pàgina ens mostrarà les vulnerabilitats de l'últim dia:

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: Repositoris de vulnerabilitats

Per a cada vulnerabilitat, podem veure que es presenten tres enllaços:

- CVE/CAN, enllaça amb la pàgina de la font on es publica la vulnerabilitat (<http://nvd.nist.gov/nvd.cfm>) per a complir amb l'estàndard CVE.
- CVSS, enllaça amb la pàgina del NVD (<http://nvd.nist.gov/cvss.cfm>) on es mostre el desglossament del vector CVSS (si ho tingués) per a complir amb l'estàndard CVSS.
- [+], enllaça amb detall de la vulnerabilitat en SIGVI.

3.6. Administració



figura 12: Menú d'administració

En aquest grup apareixen els enllaços amb les pàgines de configuració bàsica.

3.6.1. El meu usuari

A través d'aquesta pàgina podrà modificar les seves dades:

#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: El meu usuari

Les dades de l'usuari son:

- Username: El nom d'usuari que farà servir per a realitzar el Login en l'aplicació. Aquest camp és obligatori.
- Extern: Si el valor és “Si”, la autenticació es realitzarà usant el sistema d'autenticació que s'hagi definit en la instància del SIGVI, si el valor és “No” s'usarà la contrasenya indicada en el camp de contrasenya.
- Nom: El nom de l'usuari. Aquest camp és obligatori.
- Cognoms: Els cognoms de l'usuari.
- Grup: El grup al que pertany l'usuari. Aquesta associació limitarà el subconjunt de dades a mostrar i/o gestionar. En general, l'usuari que no sigui administrador del SIGVI només podrà veure i gestionar les dades del seu grup. Aquest camp és obligatori.
- E-mail: La adreça de correu electrònic de l'usuari. És la qual s'usarà per a enviar les notificacions i resums resultants dels processos batch.
- Nivell: El nivell d'accés a les dades. No es pot auto-incrementar-se el nivell d'accés, i aquesta associació limitarà el grau d'accés a les dades del grup. Així, per exemple, un administrador d'equip no podrà modificar les dades d'altres usuaris del seu grup. Aquest camp és obligatori.
- Data d'alta: Es la data de creació de l'usuari. És un camp de lectura i no es pot modificar.
- Rebre notificacions?: Si el valor d'aquest camp és “No”, no se li enviarà cap tipus de notificació de noves alertes ni resums.
- Rebre resum diari de vulnerabilitats?: Si el valor d'aquest camp és “No”, l'usuari no rebrà el resum diari de vulnerabilitats, resultant del procés batch de càrrega de vulnerabilitats.

3.6.2. Grups i usuaris

Són els manteniments mitjançant els quals es gestionarà els grups i els usuaris de l'aplicació.

Només usuaris amb perfil “administrador del SIGVI” podran visualitzar i gestionar el manteniment de

grups, i només aquests o usuaris amb perfil “administrador de grup” podran visualitzar i gestionar el manteniment d'usuaris.

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: Grups

El nom dels grups és obligatori i té que ser únic. La descripció és optativa.

Els grups s'usaran per a agrupar els usuaris i els recursos d'aquests (servidors, productes instal·lats en els servidors, alertes, etc.).

Username	External?	Name	Surname	Group	Level	email	Hire
admin	No	Administrador		SIGVI Adm	SIGVI Adm	sebastian.gomez@upcnet.es	2008-00:2
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: Usuaris

Les dades relacionats amb es usuaris son els mateixos que els que es presenten i s'expliquen en el punt anterior “[El meu usuari](#)”.

3.6.3. Filtres

Els filtres s'usen per a discriminar las vulnerabilitats a l'hora d'usar-les, bé sigui quan afecta a un producte d'un servidor, o bé a l'hora d'incloure-la en el resum diari de vulnerabilitats.

Els filtres es podran usar en el manteniment d'usuaris per a cadascun d'ells, indicant el filtre de

vulnerabilitats a utilitzar en el resum diari de càrrega de vulnerabilitats.

També es podran usar en el manteniment de servidors, indicant el filtre de vulnerabilitats a utilitzar en cas de que una vulnerabilitat afecte a un dels seus productes.

L'ús de filtres que s'adeqüin a les seves necessitats podrà reduir la quantitat d'avisos i estalviar el temps de revisió d>alertes que per norma es descarten.

En moltes ocasions, degut al gran nombre de servidors i serveis, es necessari descartar directament cert tipus de vulnerabilitats. Moltes vulnerabilitats requereixen accés físic a un servidor per a poder ser explotades. És habitual descartar-les.

Per defecte el SIGVI es desplega amb alguns filtres bàsics, per exemple per a filtrar totes aquelles vulnerabilitats que no puguin ser explotables remotament.

L'usuari podrà determinar en ambdós casos el tipus de vulnerabilitats que haurien de ser filtrades:

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: Filtres

Definició

Els criteris de comparació se basaran en las característiques pròpies de la vulnerabilitat:

- Severitat (alta, mitjana, baixa)
- Si pot ser explotat remotament (si/no)
- Conseqüències (pèrdua de protecció, augment de privilegis, ...)
- Tipus (error de validació, error de condició, buffer overflow, ...)

A més, un filtre es pot crear per a un grup en concret, o bé per a qualsevol grup (si no s'indica cap).

Un administrador d'equips únicament podrà visualitzar els filtres creats per al seu grup o els genèrics, no podrà agregar ni modificar cap.

¿Cóm es filtra?

Els filtres s'executaran en funció de la manera en que s'hagin declarat:

- Passa si compleix tots, és a dir, que si la vulnerabilitat compleix amb totes les característiques indicades, continuarà processant.
- Passa si compleix algun, és a dir, que si la vulnerabilitat compleix amb alguna de les característiques indicades, continuarà processant.
- Filtra si compleix tots, és a dir, que si la vulnerabilitat compleix amb totes les característiques indicades, no processarà la vulnerabilitat.
- Filtra si compleix algun, és a dir, que si la vulnerabilitat compleix amb alguna de les característiques indicades, no processarà la vulnerabilitat.

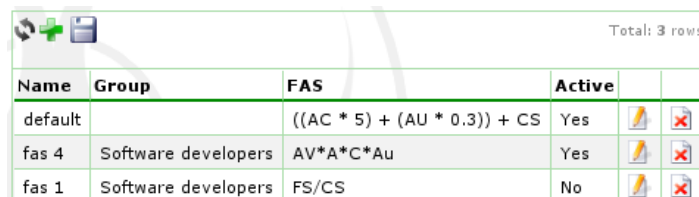
Usos

Els filtres tenen diverses finalitats:

- Determinar quines vulnerabilitats s'anuncien en els servidors. Quan una vulnerabilitat afecta a un producte d'un servidor, si s'ha indicat un filtre en la definició del servidor, s'usarà aquest per a determinar si es crea una alerta o no. D'aquesta manera, per exemple, si únicament volem que en tingui en compte vulnerabilitats que puguin ser explotades remotament, i descartar aquelles que requereixen accés físic, podrem indicar aquest filtre en la definició del servidor.
- Determinar quines vulnerabilitats s'anuncien en els resums de vulnerabilitats. Cada usuari podrà indicar que filtre usar per a determinar el tipus de vulnerabilitats de les quals vol ser informat. Així, quan es prepara el resum de vulnerabilitats diària per a enviar als usuaris que així ho hagin disposat (si tenen activat l'enviament en la definició de l'usuari), s'aplicarà el filtre a cadascuna de les vulnerabilitats. Podrà restringir, per exemple, que se li notifiqui únicament de vulnerabilitats greus indicant aquest filtre en la definició del seu usuari.

3.6.4. FAS

FAS són les sigles de Final Absolute Severity.



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

Aquesta és la funció que s'usarà per a calcular la gravetat de l'alerta. Recordem que una alerta és una vulnerabilitat que afecta a un producte instal·lat en un servidor.

Aquesta puntuació que es calcula serveix per a determinar la gravetat de la situació. Per a això s'han de tenir en compte tant les característiques de la vulnerabilitat com les característiques del propi servei que ofereix aquest producte en aquest servidor.

Vegem les següents situacions i determini quin és la més greu:

- Una vulnerabilitat de risc alt afecta al servei Apache de la nostra Web corporativa que està instal·lat en un servidor públic (accessible des d'Internet). Aquesta vulnerabilitat, a més, pot explotar-se remotament.
- Una vulnerabilitat de risc alt afecta al servei MySQL d'un servidor intern filtrat i accessible únicament des de la nostra xarxa. La vulnerabilitat pot explotar-se remotament.
- Una vulnerabilitat de risc alt afecta al servei d'autenticació LDAP instal·lat en un servidor d'accés públic sobre el qual es basen la majoria de les nostres aplicacions de la nostra Intranet. La vulnerabilitat requereix accés físic al servidor.

Potser per alguns administradors la primera situació sigui la més greu, i potser per altres no. Mitjançant les FAS es podrà determinar les seves prioritats.

Quin és el meu FAS?

La FAS és un element que s'associa a nivell de grup complet, és a dir, si hi ha una FAS definida per a un grup s'usarà aquesta funció de càlcul per a qualsevol alerta d'un servidor d'aquest grup, si no hi ha s'usarà la genèrica (sense grup assignat).

Com es pot veure en la figura anterior, en aquest exemple només hi ha una funció definida, i no té grup, això vol dir que serà aquesta la funció que s'usarà per a tots els grups.

Com administrador d'equips no podrà crear ni modificar funcions FAS, atès que és un element que s'usa a nivell d'un grup complet, serà l'administrador del seu grup qui creu les funcions per al seu grup, o bé l'administrador de l'aplicació qui creu les funcions per a tots els grups.

L'ordre de decisió de què FAS usar és:

- Si el grup al que pertany el servidor, al qual se li està creant l'alerta, té una FAS **activa**, s'usarà aquesta.
- Si no, si existeix una FAS sense grup, i **activa**, s'usarà aquesta.
- Si no, s'usarà una FAS que està definida en la instància de l'aplicació i que simplement és la puntuació de la pròpia vulnerabilitat.

Com es construeix una FAS?

Com hem comentat, les FAS s'usen per a determinar la gravetat d'una alerta, és a dir, quan greu és la situació d'una vulnerabilitat que afecta al nostre sistema.

Per a construir una FAS disposem de les característiques de la vulnerabilitat i las del servei.

Hauríem de construir una funció “matemàtica” que retorni un nombre.

Aquestes són les variables que podem fer servir:

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

Les dues primeres variables: CS i FS s'obtinran de les característiques del servei en l'associació entre servidor i el producte. La resta de variables s'obtenen de las característiques de la vulnerabilitat que afecta aquest producte.

3.7. Configuració



figura 18: Menú de configuració

Són un conjunt d'eines algunes de les quals estan disponibles només per a administradors del SIGVI i altres per a administradors de grup.

3.7.1. Configuració (genèric)

Des de aquesta pàgina accedim a la configuració del fitxer general de l'aplicació i als paràmetres emmagatzemats a la base de dades.

Configuració

Manteniment encara en desenvolupament mitjançant el qual es podrà editar el fitxer general de configuració de la instància.

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

figura 19: Configuració general de la instància

És més aconsellable editar directament el fitxer general de configuració tal com s'indica en el manual de l'administrador.

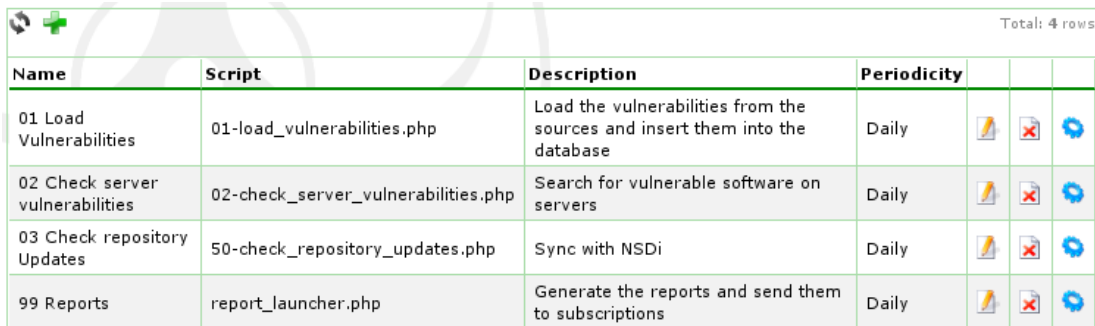
Paràmetres globals

En aquest manteniment es defineixen alguns paràmetres de l'aplicació, com per exemple la adreça de e-mail per defecte de l'administrador.

3.7.2. Administració de tasques

En aquesta pantalla, accessible únicament per un usuari amb perfil d'administrador del SIGVI, podrà

gestionar els processos batch que s'executaran i amb quina periodicitat.















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

Totes les entrades que apareixen són scripts PHP localitzats en el directori <sigvi_home>/cron. Podrem crear tantes tasques com siguin necessàries, no obstant les que apareixen per defecte són justament les indispensables per al correcte funcionament del SIGVI.

Podrem indicar la freqüència amb la que volem que s'executin, així podrem indicar si s'executarà diàriament (cada dia), semanalment (cada dilluns), mensualment (cada dia 1) o mai.

També podrem executar manualment una tasca mitjançant el botó a la dreta de cada fila. El procés s'executarà immediatament i el resultat es mostrarà per pantalla.

Com configurar i integrar les tasques al sistema s'explica a la guia d'instal·lació.

3.7.3. Fonts

Des de aquesta pàgina accedim als manteniments per gestionar les fonts de vulnerabilitats, les fonts RSS i les fonts de diccionaris de productes (compatibilitat CPE).

Fonts de vulnerabilitats

Les fonts de vulnerabilitats són una de les peces fonamentals per a tenir el sistema actualitzat.

El procés nocturn de descàrrega de vulnerabilitats processarà cadascuna de les fonts activades (camp "Use it?" sigui cert).





















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 fonts de vulnerabilitats

Per a poder descarregar les vulnerabilitats d'una font ha d'existir un plugin que sigui capaç de descarregar les dades, “parsearlos” i carregar-los en la base de dades.

En la documentació tècnica s'explica amb més detall com crear un parser per a una font concreta, però a grans trets es tracta de que emplenin un vector amb instàncies d'una classe que defineix les característiques comunes en les vulnerabilitats.

En el SIGVI R2 s'usa el format definit per l'estàndard CVE, i es proporcionen els plugins necessaris per a descarregar les vulnerabilitats que es disposin en aquest format.

Com es pot veure en la figura següent, existeixen diferents formats del CVE, que corresponen a la evolució del mateix. No serà necessari tenir activades totes les fonts, bastarà, com en aquest cas, tenir activades aquelles que només mostren els canvis recents.

Únicament és aconsellable activar-les totes (i millor una per una) en la primera càrrega d'una nova instància del SIGVI). En aquest cas, els paràmetres corresponen al fitxer remot que usarà per a “parsear”.

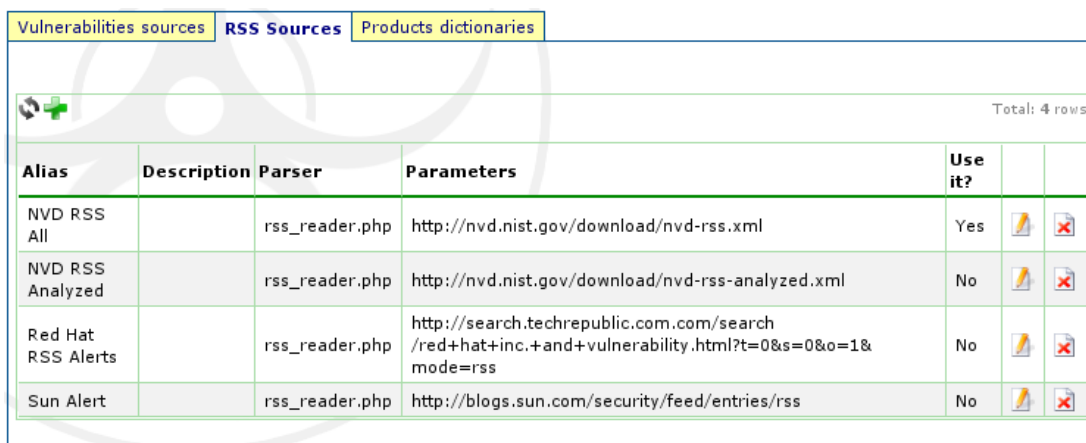
En la part superior de la finestra apareixen dos enllaços a eines:

- Provar una font de vulnerabilitats: és útil per a comprovar si un plugin funciona correctament. El que fa és una simulació de càrrega d'una font de vulnerabilitats que li indiquem sense arribar a emmagatzemar les dades en la base de dades, mostrant informació per pantalla útil per a determinar si el “parser” funciona correctament o no.
- Càrrega manual de les vulnerabilitats des de les fonts: bàsicament executarà immediatament el procés que s'executa per les nits per a totes les fonts actives.

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.



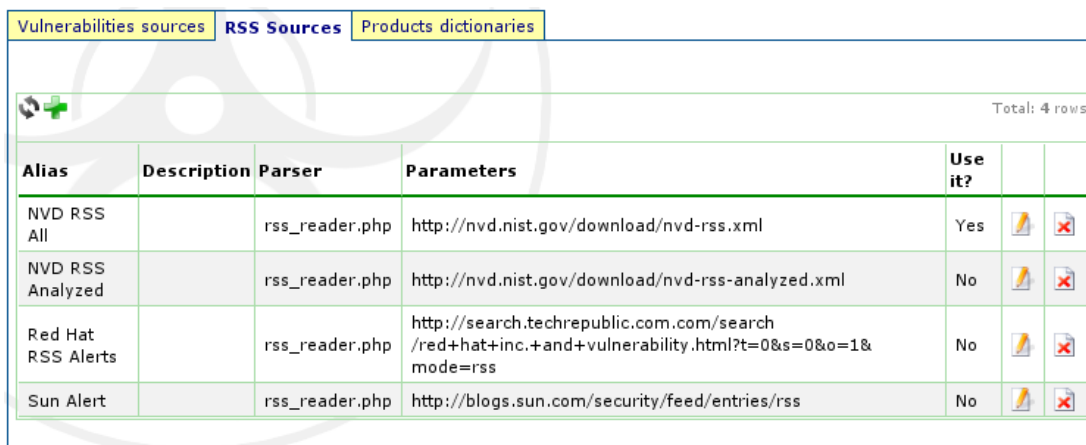
Alias	Description	Parser	Parameters	Use it?		
NVD RSS All		rss_reader.php	http://nvd.nist.gov/download/nvd-rss.xml	Yes		
NVD RSS Analyzed		rss_reader.php	http://nvd.nist.gov/download/nvd-rss-analyzed.xml	No		
Red Hat RSS Alerts		rss_reader.php	http://search.techrepublic.com.com/search/red+hat+inc.+and+vulnerability.html?t=0&s=0&o=1&mode=rss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

figura 22: Gestión de fuentes RSS

Gestió de les fonts RSS

Des de aquest podrem gestionar les fonts RSS de notícies. Per afegir una nova cal tenir en compte que si no compleix el plugin de lectura de RSS que es proporciona amb l'aplicació caldrà crear-ne un (d'aquest punt es parla al document tècnic).

La pantalla en la qual es visualitzaran les notícies s'accedeix des de menú → Noticias.



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		

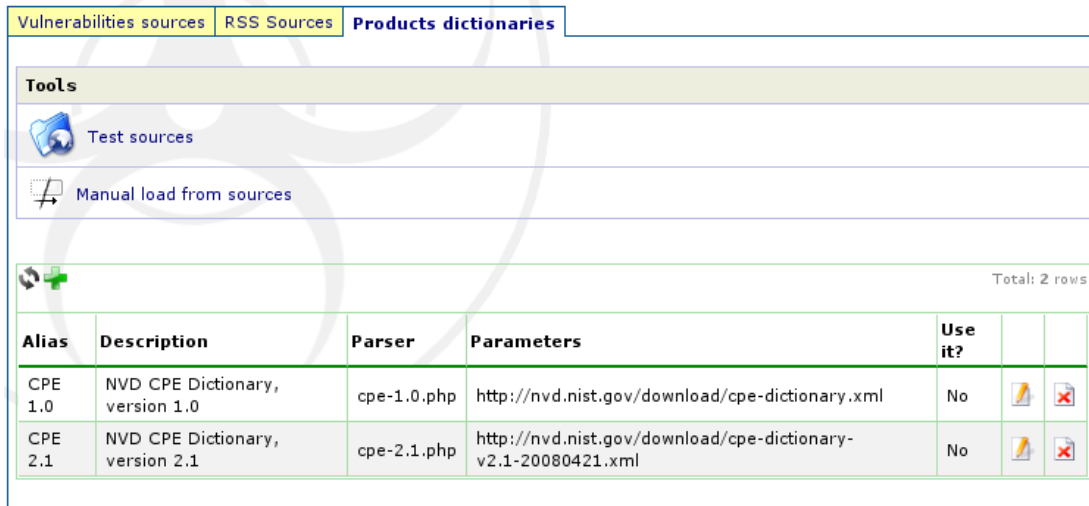
figura 23: Gestión de fuentes RSS

Gestió dels diccionaris de productes (CPE)

Aquest manteniment és una peça per la compatibilitat amb els diccionaris de productes CPE del SCAP. A la versió actual (Release Candidate 1) l'aplicació està preparada per a suportar aquest tipus de diccionaris. No obstant no serà fins la propera versió on quedaran integrats els diccionaris CPE amb el

repositori de productes.

És una pantalla transitòria que, pel moment, únicament aporta valor informatiu.

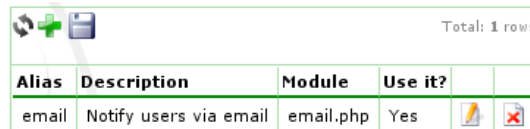


Alias	Description	Parser	Parameters	Use it?		
CPE 1.0	NVD CPE Dictionary, version 1.0	cpe-1.0.php	http://nvd.nist.gov/download/cpe-dictionary.xml	No		
CPE 2.1	NVD CPE Dictionary, version 2.1	cpe-2.1.php	http://nvd.nist.gov/download/cpe-dictionary-v2.1-20080421.xml	No		

figura 24: Gestió de diccionaris CPE

3.7.4. Mètodes de notificació

Indica els possibles mètodes de notificar les alertes de les vulnerabilitats. Per defecte es proveïx un mètode “e-mail”, pel qual la via de notificació de les alertes als usuaris d'un grup és el e-mail.

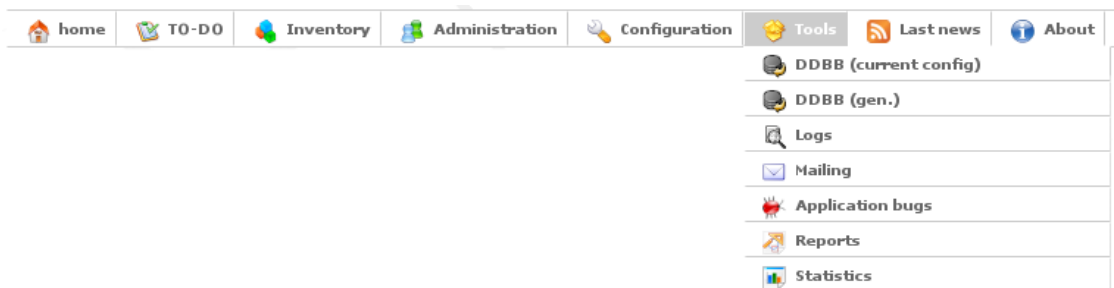


Alias	Description	Module	Use it?		
email	Notify users via email	email.php	Yes		

figura 25: Mètodes de notificació

En la documentació tècnica s'indica com crear els seus propis mètodes de notificació.

3.8. Eines



home	TO-DO	Inventory	Administration	Configuration	Tools	Last news	About
					DDBB (current config)		
					DDBB (gen.)		
					Logs		
					Mailing		
					Application bugs		
					Reports		
					Statistics		

figura 26: menú d'eines

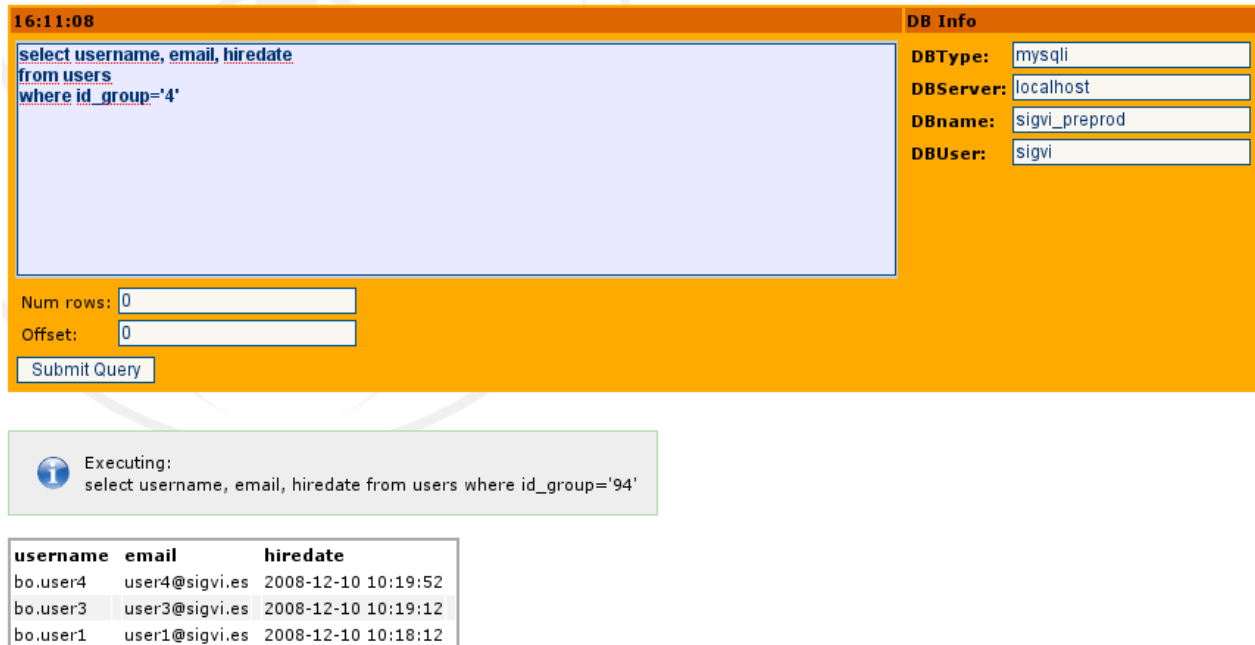
Des d'aquest menú s'accedeix a diverses eines de l'aplicació. Algunes estaran accessibles únicament per a usuaris amb nivell d'administradores del SIGVI, d'altres per a administradors de grup i altres per a

tots els usuaris registrats.

3.8.1. Base de datos (DDBB)

Existe una herramienta que sirve para interaccionar con la base de datos de la aplicación (current config) y otra para interaccionar 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.



The screenshot shows a web-based database query interface. At the top left, the time is 16:11:08. The main area contains a text input field with the following SQL query: `select username, email, hiredate from users where id_group='4'`. To the right, under "DB Info", there are four input fields: DBType (mysql), DBServer (localhost), DBname (sigvi_preprod), and DBUser (sigvi). Below the query field, there are two input fields for "Num rows" and "Offset", both set to 0, and a "Submit Query" button. Below the main interface, a status bar indicates "Executing: select username, email, hiredate from users where id_group='94'". At the bottom, a table displays the query results:

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 27: Interacció amb la Base de Dades

3.8.2. Logs

Aquest manteniment és accessible únicament per un perfil de "Administrador del SIGVI", i mostra una auditoria de tots els canvis realitzats en la base de dades, l'hora, l'origen i l'usuari que ho ha generat. Pot emmagatzemar accessos a manteniments, entrades correctes en la aplicació, sortides de l'aplicació, intents incorrectes d'autenticació, canvis en registres de la base de dades (indicant els valors antics i els nous valors), etc.

A través del fitxer general de configuració es decideix si es realitza auditoria o no, i el nivell. Per a més informació sobre la configuració consulti la documentació tècnica.

#	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 28: Logs de l'aplicació

3.8.3. Mailing

La pantalla de “mailing” és una senzilla interfície per a enviar e-mails als usuaris de l'aplicació.

La següent figura representa aquesta pantalla, on veiem que primer sigui el “To”, on hauríem de seleccionar en un dels tres blocs.

És a dir:

- podem enviar un e-mail a un o diversos grups
- **o bé** enviar un e-mail a un o diversos perfils
- **o bé** a un o diversos usuaris

Si seleccionem en més d'un bloc, l'aplicació usarà només els del primer bloc on s'hagi seleccionat.

Indicarem un “Subject” i un contingut i li donem al botó “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: New source added

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

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

Text:

Send

figura 29: Mailing

3.8.4. Bugs de l'aplicació

Aquesta utilitat està més pensada per a informar sobre l'existència d'errors en l'aplicació per a versions en desenvolupament. Aquest opció haurà d'estar desactivada en instàncies del SIGVI en producció.

No obstant això, malgrat ser una interfície senzilla sense possibilitat d'assignació a persones, pot ser utilitzada per a altres fins, a decisió de l'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"/>				








   Total: 2 rows						
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 30: Bugs

3.8.5. Informes

3.8.6. Estadístiques

En aquesta pàgina trobem diversos resums ja definits mostrant informació relativa a les dades recollides per SIGVI.

Alguns d'aquests resums són:

- Comptador de vulnerabilitats: Mostra l'evolució de l'últim any del nombre de vulnerabilitats aparegudes cada mes.

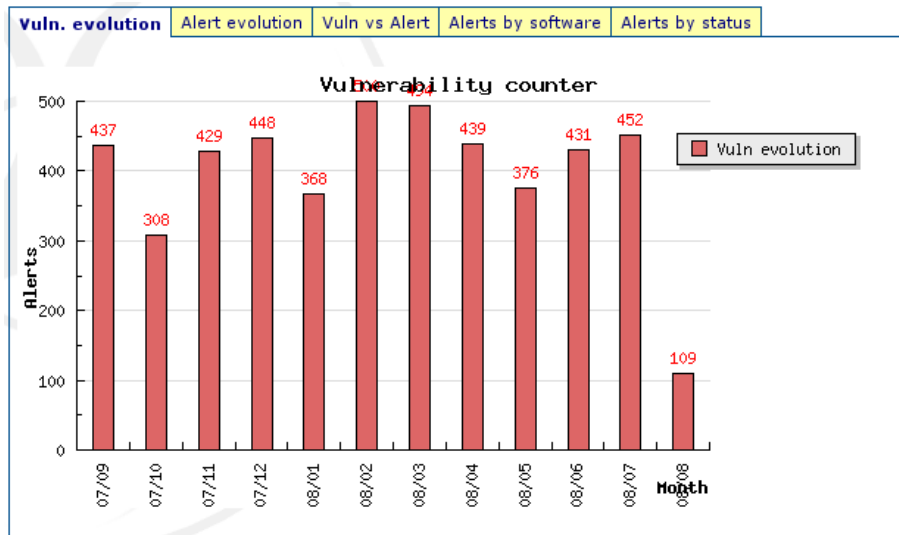


figura 31: gràfica d'evolució de vulnerabilitats

- Evolució de les alertes: Mostra l'evolució del nombre d'alertes generades cada mes durant l'últim any.

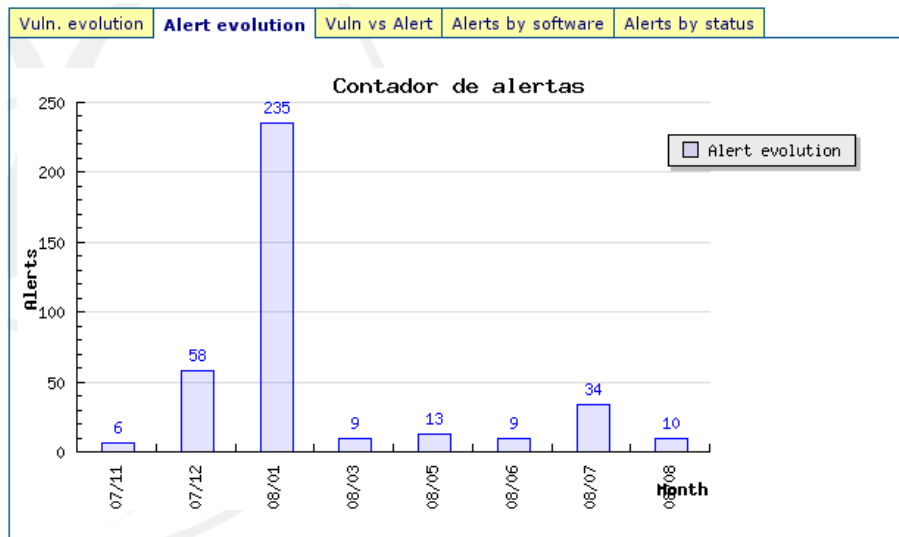


figura 32: gràfica d'evolució d'alertes

- Comparació de l'evolució de les vulnerabilitats amb l'evolució de les alertes: Mostra en una mateixa gràfica las dos anteriors amb els valors de l'últim any. Per a cada mes apareixen representades el nombre de vulnerabilitats i d'alertes generades.

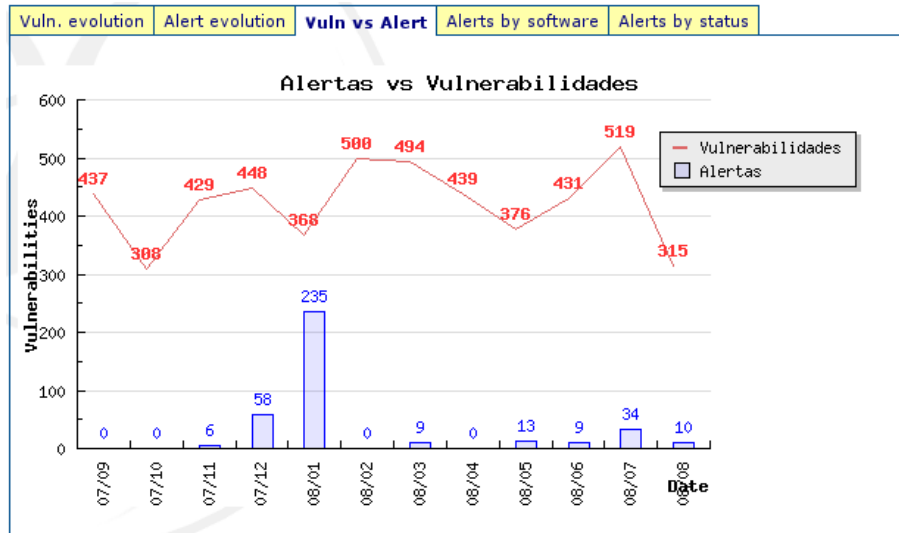


figura 33: gràfica comparativa d'evolució vulnerabilitats vs alertes

- Desglossament de les alertes per el software afectat: Un gràfic de pastis on podem veure en què es reparteix el total de alertes quant a tipus de software afectat.

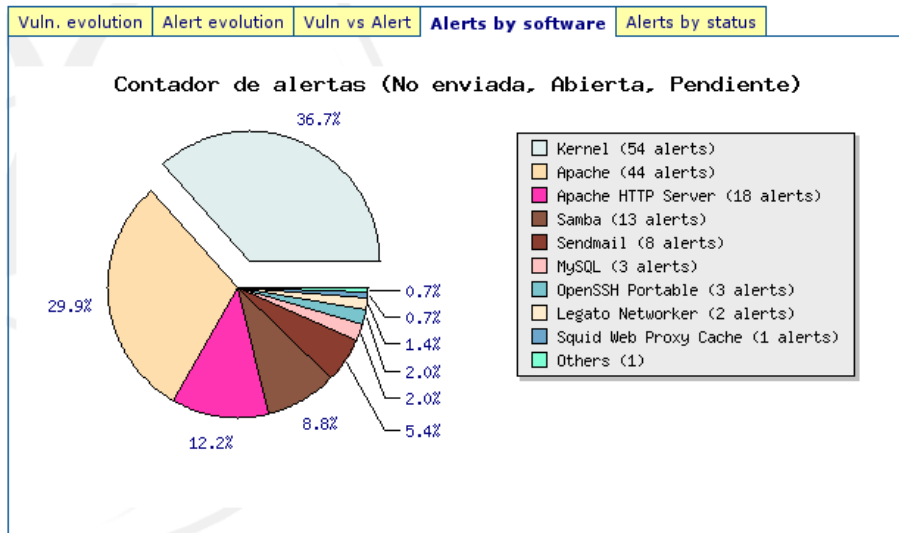


figura 34: gràfica de agrupament d>alertes per producte

- Alertes per estat: ens permetrà veure ràpidament l'estat de les alertes del nostre grup.

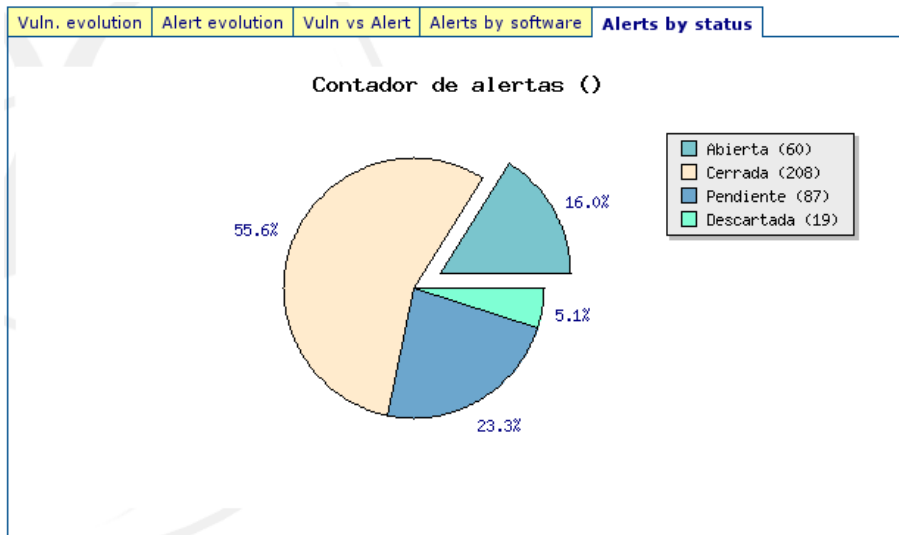


figura 35: gràfica de agrupament d>alertes per estat

4. Inici i ús del SIGVI R2 de l'Administrador del SIGVI

Quines són les funcions de l'administrador del SIGVI?

Les funcions de l'administrador del SIGVI són:

- configurar l'entorn de la nova instància del SIGVI
- inicialització de les vulnerabilitats
- alta i gestió dels grups
- mantenir el correcte funcionament de l'entorn, supervisant els resums diaris de l'estat final dels processos nocturns
- actualització periòdica de certes parts de l'aplicació, com per exemple les fonts de vulnerabilitats

Al començar a utilitzar la instància del SIGVI serà l'administrador del SIGVI qui haurà de configurar el nou desplegament.

A més a més de les tasques de configuració general de la instància que s'explica en la documentació tècnica, cal realitzar diverses tasques per a deixar l'entorn a punt per al seu correcte funcionament.

4.1. Inici

Al començar amb una nova instància del SIGVI, serà l'administrador del SIGVI el responsable de la configuració inicial, tant a nivell de sistema, de configuració interna, com de desplegament.

4.1.1. Configuració de l'entorn

Consulti el manual d'instal·lació per a veure com s'instal·la i es configura inicialment el SIGVI perquè es pugui accedir correctament, així com l'activació o desactivació de les parts optatives.

4.1.2. Configuració de les fonts de vulnerabilitats

La utilitat del SIGVI radica en tenir dades reals, fiables i actualitzades, tant de les vulnerabilitats com dels productes instal·lats en els servidors. De la segona part s'encarregaran els administradors d'equips, però la primera és responsabilitat directa de l'administrador del SIGVI.

Per defecte el SIGVI proporciona una sèrie de fonts i plugins basats en l'estàndard CVE per a descarregar les definicions de les vulnerabilitats des del NVD. Per defecte només dues fonts referents a actualitzacions i novetats són les actives.

Es recomana realitzar una càrrega inicial de totes les fonts de vulnerabilitats. Per a realitzar aquesta tasca pot consultar el capítol [3.7.3](#), on s'explica com fer-ho.

4.1.3. Crear els grups

Els usuaris finals del SIGVI són els administradors d'equip, que pertanyen a un grup. Els administradors de grup són les figures que han d'encarregar-se de la creació i gestió dels usuaris del seu grup.

L'administrador del SIGVI és l'únic que pot crear i gestionar la definició dels grups. Així doncs, haurà

de crear, al iniciar l'entorn, els grups necessaris i definir els responsables de cadascun d'ells (poden ser varis). No és la seva funció la gestió de les dades internes de cada grup, com els servidors, alertes, productes instal·lats, etc.

4.2. Ús diari

L'ús diari de l'administrador del SIGVI s'hauria de centrar en corregir possibles problemes de sistema o de configuració, sense haver d'entrar a revisar problemes interns en els grups o les seves dades.

La tasca principal i rutinària de l'administrador del SIGVI és la revisió dels resums d'estat dels processos.

4.2.1. Revisar els resums d'estat dels processos

Els processos nocturns envien un resum de l'estat final d'aquests als administradors del SIGVI. És, per tant, aquest figura la responsable de vetllar per el perfecte funcionament dels processos, revisant diàriament l'estat per a corregir possibles problemes.

Entre aquest problemes podríem trobar-nos, per exemple, que no s'hagi realitzat la càrrega de vulnerabilitats perquè, per exemple, en aquest moment no funcionava la xarxa. En aquest cas sigui bé per l'absència del resum d'estat o bé per un resum d'estat incorrecte, haurà d'executar manualment els processos de càrrega de vulnerabilitats i de revisió de les vulnerabilitats als servidors.

5. Inici i ús del SIGVI R2 de l'Administrador de grups

La figura de l'administrador d'equips té com funcions bàsiques:

- Alta i gestió dels usuaris del grup
- Alta i gestió dels filtres per al grup
- Alta i gestió de les funcions FAS per al grup
- Revisió de les alertes dubtoses del seu grup

5.1. Inici i ús

Una vegada l'administrador del SIGVI hagi creat el seu grup i el seu usuari, vostè haurà d'iniciar la informació del seu grup.

5.1.1. Gestió de usuaris

Haurà de començar creant usuaris del nivell administrador d'equips en el seu grup, que podran realitzar la resta de tasques d'alta i gestió de servidors i associar-los a productes, informació necessària perquè el SIGVI representi una utilitat per al seu grup.

5.1.2. Gestió dels filtres

Encara que no és necessari, ja que l'ús dels filtres és optatiu, vostè podrà crear els filtres que consideri necessaris per als usuaris del seu grup (consulti el punt [3.6.3](#)).

5.1.3. Gestió de les funcions FAS

De la mateixa manera passa amb les funcions FAS (consulti el punt [3.6.4](#)).

5.1.4. Revisió de les alertes dubtoses

Quant a les tasques diàries, l'administrador del grup serà el responsable de validar o descartar les alertes dubtoses (consulti el punt [3.4.1](#)). Les alertes que el motor de comparació del SIGVI no està segur de si descartar-les o no, es creen com a “pendents de validar” de manera que és responsabilitat de l'administrador del grup prendre aquesta decisió.

Aquest tipus d'alertes no són visibles pels administradors d'equips, que són qui finalment analitzaran les alertes per a determinar què cal fer. És important validar o descartar les alertes com més aviat millor per a poder actuar amb rapidesa.

6. Inici i ús del SIGVI R2 de l'Administrador de equips

Com a administrador d'equips en SIGVI R2, quin és el primer pas? ¿Para quin em serveix aquesta aplicació i què puc fer amb ella?

6.1. Inici

6.1.1. Què és el SIGVI i per a què serveix?

El SIGVI és una eina que tracta d'ajudar precisament a l'administrador dels servidors en la detecció i gestió de les vulnerabilitats informàtiques dels servidors.

Els administradors de sistemes han de dedicar molt de temps en tot el que és la detecció i gestió de vulnerabilitats. Aquestes tasques rutinàries com són llegir les notificacions de vulnerabilitats del centres subscrits, determinar si afecta a algun dels nostres sistemes comparant amb el llistat de software dels servidors que administra, i finalment, si afecta, recollir informació d'accions a prendre i actuar.

La funcionalitat final del SIGVI és delegar en ell tot aquest procés, llevat de l'actuació, perquè l'administrador únicament hagi de preocupar-se quan el SIGVI li enviï una notificació avisant sobre una vulnerabilitat en un dels seus equips.

El SIGVI, partint de la llista dels seus servidors i dels productes que ha declarat que tenen instal·lats, examinarà cada dia per si apareix alguna vulnerabilitat que afecti a algun d'aquest productes. En cas afirmatiu crearà una alerta (veure [3.4.2](#)) i li enviarà pel mecanisme que s'hagi definit en la instància del SIGVI (per defecte via e-mail).

6.1.2. Primer pas: introducció de les dades

Perquè el SIGVI pugui notificar als administradors de les vulnerabilitats en els seus equips és necessari, primer, donar d'alta els servidors, i després, per a cadascun d'ells donar d'alta el software més important que tingui instal·lat (Sistema Operatiu, Software que dona servei a altres servidors o Internet, ...). Per a això vegi el capítol [3.5.2](#) sobre l'inventari, concretament servidors i productes.

Una vegada hagi donat d'alta els seus servidors i els serveis (o software o productes) més importants ja començarà a rebre, a partir de la següent execució dels processos nocturns, les alertes de vulnerabilitats (quan les tingui).

6.2. Ús diari

6.2.1. M'ha arribat una notificació per e-mail, ara què faig?

Quan SIGVI detecta que una vulnerabilitat en algun dels productes crea una alerta en el repositori d>alertes i li enviarà una notificació (per defecte via e-mail). Aquesta notificació que rep és un resum de l'alerta, mostrant quin es el servidor, afectat, el producte vulnerable i la vulnerabilitat que ho afecta, incloent les URLs del declarant on poder acudir a trobar informació relativa a la resolució o quines mesures s'han de prendre.

A més a més inclou el FAS (Final Absolute Severity, veure capítol [3.6.4](#) sobre les funcions FAS), que és

un nombre entre 0 i 10 que indica com de greu és l'assumpte, d'aquesta manera ajudar-li a prendre una decisió ràpida i saber si és crític o no.

A partir d'aquesta notificació hauria de treballar amb l'alerta del SIGVI, on podrà determinar l'estat de l'alerta, agregar els comentaris oportuns per al treball en equip, etc.

Per a això accedeixi a la seva instància del SIGVI, introdueixi el seu usuari i la seva contrasenya i accedeixi al menú d'alertes actives, on trobarà les alertes obertes o pendents del seu grup.

Per a cadascuna d'elles, podrà accedir a la informació de la vulnerabilitat, on, a més dels detalls de la pròpia vulnerabilitat, trobarà en general enllaços a pàgines on el fabricant o tercers recomanen accions a prendre.

Pensi que aquesta eina no actuarà per vostè, el que intenta es posar a la seva disposició tota la informació que pugui necessitar per a prendre una decisió.

6.2.2. He actualitzat la versió d'un programa en el servidor, he de canviar-lo en SIGVI?

Si. Pensi que les alertes i notificacions que es generen en el SIGVI és usant la informació que vostè hagi introduït. Si les dades que tingui en el SIGVI no són reals, les notificacions i alertes no tenen per què ser-ho.

És molt important que la informació del SIGVI reflecteixi la realitat.

6.3. Informació de les vulnerabilitats

6.3.1. M'he cansat de tant resum diari, com puc desactivar-los?

En la pàgina de configuració del seu usuari vostè podrà configurar si desitja ser notificat o no amb el resum diari de vulnerabilitats en el camp “Rep el resum diari de vulnerabilitats”.

6.3.2. Els resums tenen massa informació

Malgrat que els resums són únicament a manera informativa, atès que el control de la detecció de les vulnerabilitats ho tindrà el SIGVI, vostè pot restringir la informació del resum, usant el filtre de notificacions que podrà indicar en la pàgina de configuració del seu usuari, concretament en el camp “Filtre de notificacions”.

Vegi el punt [3.6.3](#), sobre filtres.

Índex de figures

figura 1: Format de les pàgines.....	6
figura 2: pàgina de login.....	8
figura 3: pàgina principal.....	11
figura 4: Menú TO-DO.....	12
figura 5: Alertes.....	15
figura 6: Resum de estat d>alertes.....	17
figura 7: Menú d'inventari.....	17
figura 8: Servidors.....	19
figura 9: Serveis: productes instal·lats en els servidors.....	20
figura 10: Repositoris de productes.....	21
figura 11: Repositoris de vulnerabilitats.....	22
figura 12: Menú d'administració.....	22
figura 13: El meu usuari.....	23
figura 14: Grups.....	25
figura 15: Usuaris.....	25
figura 16: Filtres.....	26
figura 17: Final Absolute Severity.....	29
figura 18: Menú de configuració.....	31
figura 19: Configuració general de la instància.....	34
figura 20: Administrador de tareas.....	35
figura 21: Administrador de fonts de vulnerabilitats.....	36
figura 22: Gestión de fuentes RSS.....	37
figura 23: Gestión de fuentes RSS.....	37
figura 24: Gestión de diccionarios CPE.....	38
figura 25: Mètodes de notificació.....	38
figura 26: menú d'eines.....	38
figura 27: Interacció amb la Base de Dades.....	39
figura 28: Logs de l'aplicació.....	40
figura 29: Mailing.....	41
figura 30: Bugs.....	42
figura 31: gràfica d'evolució de vulnerabilitats.....	42
figura 32: gràfica d'evolució d>alertes.....	43
figura 33: gràfica comparativa d'evolució vulnerabilitats vs alertes.....	43
figura 34: gràfica de agrupament d>alertes per producte.....	44
figura 35: gràfica de agrupament d>alertes per estat.....	44