

SIGVI R2

Guia d'Instal·lació

Índex

1. Introducció.....	3
2. Requeriments.....	4
2.1. Plataforma.....	4
2.2. Servidor Web.....	4
2.3. Servidor de bases de dades relacionals.....	4
2.4. Intèrpret de PHP5.....	4
3. Instal·lació.....	5
3.1. Dades de sistema.....	5
3.2. Instal·lació de l'aplicació.....	6
3.3. Creació de la base de dades.....	6
3.4. Adaptant l'aplicació al seu entorn.....	6
3.5. Comprovar accessos LDAP.....	7
3.6. Configuració dels processos batch.....	7
3.7. Accedint per primera vegada.....	8
4. Més ajuda.....	8

1. Introducció

SIGVI són les sigles de Sistema Intel·ligent de Gestió de Vulnerabilitats Informàtiques. És una eina per a poder gestionar les vulnerabilitats dels nostres sistemes.

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.

Aquest document tracta de detallar com instal·lar una nova instància del SIGVI.

2. Requeriments

El SIGVI R2 és una aplicació Web implementada en PHP5 i que necessita una base de dades relacional per a emmagatzemar les dades.

2.1. Plataforma

L'aplicació ha estat desenvolupada i testada sobre plataformes Linux. El procés d'instal·lació serà el mateix en qualsevol plataforma UNIX (salvant els directoris Web, que dependrà més del propi servidor Web). Atès que és un llenguatge interpretat també funcionarà en plataformes Windows, encara que hi ha diferències en la configuració dels processos batch.

Es recomana instal·lar l'aplicació en una plataforma Linux.

2.2. Servidor Web

Serà necessari un servidor Web que permeti interpretar scripts de PHP5. Aquesta aplicació ha estat desenvolupada i testada en un entorn Web basat en **Apache Web Server, versió 2** amb el mòdul de **PHP5** (opcionalment amb el mòdul SSL).

Si el seu servidor Web és altre diferent, ha de tenir en compte que l'aplicació es basa en un sistema de directoris. Existeixen directoris comuns, on s'allotgen les classes, imatges, icones, etc. I altres directoris que contenen la lògica pròpia de l'aplicació.

Les referències internes requereixen tant accessos relatius i accessos absoluts.

Exemple d'instal·lació en sistemes basats en “apt”:

```
> apt-get install apache2-mpm-prefork libapache2-mod-php5
```

2.3. Servidor de bases de dades relacionals

SIGVI R2 proporciona una capa d'abstracció de bases de dades, permetent-li funcionar sobre qualsevol tipus que implementi aquesta capa. Aquesta versió es proveix amb accés a RDBMs MySQL, Postgres i Oracle.

Però això és únicament a nivell funcional, atès que el fitxer de càrrega inicial de la base de dades correspon a MySQL. En futures versions està previst solucionar aquesta part proveint inicialment el codi necessari per a la resta de servidors suportats.

Es recomana tenir instal·lada com servidor de bases de dades MySQL Server versió 5.0 o superior. En altre cas serà necessari modificar el fitxer SQL de càrrega inicial per a adaptar-lo al seu sistema.

Exemple d'instal·lació en sistemes basats en “apt”:

```
> apt-get install mysql-server-5.0
```

2.4. Intèrpret de PHP5

Com ja s'ha indicat, l'aplicació està implementada en PHP5. Quan es parla sobre els requeriments del servidor web, ja s'ha explicat que haurà de ser capaç d'interpretar scripts PHP5.

Però a més és necessari disposar de diversos mòduls de PHP5:

- Llibreries d'accés al seu servidor de bases de dades (mysql, oracle, postgres)

Són necessàries les llibreries d'accés a la base de dades. Si per exemple usa MySQL com a servidor de base de dades necessitarà el mòdul de PHP amb les llibreries necessàries (mòduls php5-mysql, php5-pgsql, ...).

- Llibreries de generació d'imatges GD

L'aplicació necessita generar gràfiques per als resums i gràfiques d'estat. Necessita tenir instal·lada el mòdul de PHP per a generar imatges (mòdul php5-gd).

- Intèrpret de línia de comandos

Part de l'aplicació són scripts que formen processos batch, és a dir, s'executen en diferit i no s'interpreten a través del servidor Web, si no directament des del sistema. Per a això és necessari disposar del mòdul de PHP de línia de comandos (php5-cli).

3. Instal·lació

El SIGVI R2 es distribuïx en un paquet comprimit amb els comandos tar i gzip. Aquest conté:

- Un fitxer ChangeLog, on s'expliquen les últimes novetats aportades en la versió del paquet
- Un fitxer INSTALL on s'explica breument com instal·lar l'aplicació
- Un fitxer SQL per a crear la base de dades de l'aplicació i realitzar la càrrega inicial.
- L'arbre de directoris i scripts que formen la pròpia aplicació.

Primer haurà d'extreure el contingut del paquet:

```
> tar xzvf sigvi-xxxx.tgz
```

3.1. Dades de sistema

Per a explicar la instal·lació prendrem com exemple un entorn concret amb la següent configuració:

Descripció del software:

- Sistema Operatiu: Ubuntu Desktop 7.04
- Servidor Web: Apache Web Server 2.2.8-1 amb mòdul PHP5
- Intèrpret de línia de comandos PHP5
- Servidor de bases de dades MySQL 5.0.51a

Descripció de l'entorn:

- Directori arrel del servidor Web: /var/www
- Usuari sobre el qual s'executen els processos de Apache: www-data
- Usuari de sistema amb el que realitzarem la instal·lació: root
- Usuari de base de dades MySQL amb permisos per a crear bases de dades: root

Haurà d'adaptar les referències als del seu sistema.

3.2. Instal·lació de l'aplicació

Dintre del paquet existeix un directori anomenat “sigvi” que conté l'aplicació. Hauríem de moure aquest directori dintre de l'arbre de directoris del nostre servidor Web (en algunes versions es diu httdocs):

```
# mv sigvi /var/www/sigvi
```

Després hauríem de modificar els permisos d'aquest directori perquè l'usuari amb el qual s'executa Apache pugui accedir als scripts a través dels directoris. En les últimes versions de Apache aquest usuari es diu “www-data”, però pot consultar-lo mirant el propietari dels processos, per exemple “apache” que pot visualitzar amb el comando “ps -efa”

```
# chown -R www-data:www-data /var/www/sigvi
```

```
# chmod -R 750 /var/www/sigvi
```

A partir d'aquest moment el servidor Web ja tindrà accés a l'aplicació, però no funcionarà perquè falta per completar la resta de la instal·lació.

3.3. Creació de la base de dades

Com ja s'ha comentat, SIGVI R2 proveix una capa d'abstracció de base de dades que li permetria treballar amb qualsevol tipus de RDBMS. No obstant això el fitxer SQL mitjançant el qual es genera la base de dades i s'inicialitza pertany a MySQL.

Per a crear la base de dades necessitarem usar un usuari de MySQL amb privilegis de creació, que en aquest cas és root.

Per a realitzar la càrrega inicial, en la qual ja es crea la base de dades usarem el fitxer .sql que trobarem dintre del paquet, en el mateix directori on està el fitxer INSTALL. Aquest fitxer .sql es completa amb la versió del SIGVI que estiguem instal·lant. Per exemple, si estem instal·lant la versió 1.3.0 del SIGVI R2 executarem:

```
# mysql -u root -p < sigvi-1.3.0.sql
```

Al finalitzar, si no s'han produït errors, tindrem creada la base de dades del SIGVI, juntament amb un usuari “sigvi” i totes les taules inicialitzades.

3.4. Adaptant l'aplicació al seu entorn

Una vegada complerts els passos anteriors faltaria configurar l'aplicació per a poder accedir a ella via Web. Per això hauríem d'editar el fitxer app.conf.php que es troba dintre del directori “conf” del SIGVI.

Concretament haurà de revisar els paràmetres HOME, ADM_EMAIL, SERVER_URL, i la configuració de la base de dades (al final del fitxer).

3.4.1. HOME i SERVER_URL

Tingui especial cura amb la constant HOME, donat que és la constant que indica internament la referència a la pròpia aplicació a través del navegador. Dependrà de la URL que fem servir per a accedir a l'aplicació, és a dir, el camí que hi ha al darrere de la URL del propi servidor.

Com definir correctament aquesta constant?

Aquests són exemples de diferents situacions d'instal·lació de l'aplicació i com definir-la en cada cas.

- Per a accedir al SIGVI usem una URL com aquesta: <http://server.localdomain.domain/sigvi>
Llavors el valor de HOME serà: `define("HOME", "/sigvi")` parant esment a la barra final.
El valor del SERVER_URL serà: `define("SERVER_URL", "server.localdomain.domain")`
- Usem una URL com aquesta: http://server.localdomain.domain/my_applications/sigvi_r2
Llavors el valor de HOME serà: `define("HOME", "/my_applications/sigvi_r2")`
El valor del SERVER_URL serà: `define("SERVER_URL", "server.localdomain.domain")`
- Tenim instal·lat el SIGVI en un Virtual Host, i per a accedir a ell usem aquesta URL: <http://server.localdomain.domain:81/>
Llavors el valor de HOME serà: `define("HOME", "")`, important veure que no hi ha `"/`.
El valor del SERVER_URL serà: `define("SERVER_URL", "server.localdomain.domain:81")`

3.5. Comprovar accessos LDAP

El SIGVI permet validar les contrasenyes dels usuaris contra serveis externs. Per a això bastarà tenir el plugin necessari. En aquesta versió es proveïx un plugin per a autenticació via LDAP.

Si en el seu entorn es realitzen les validacions via LDAP podrà configurar el SIGVI perquè validi els usuaris que creu en ell contra el seu servei. Per a configurar-lo vaga al final del fitxer `app.conf.php` dintre del directori `conf` i adapti'l al seu entorn.

Els usuaris que tinguin el camp "extern" a cert, es validaran usant aquest mètode.

3.6. Configuració dels processos batch

Els processos batch, o processos diferits són els encarregats d'actualitzar les dades de la base de dades com per exemple descarregar les vulnerabilitats i actualitzar la taula de vulnerabilitats, comprovar quins productes, dels quals té instal·lats en els seus servidors, estan afectats per alguna vulnerabilitat, avisar als administradors, etc.

Encara que l'aplicació proveïx de mecanismes a través de la interfície Web per a executar manualment els processos més importants, és aconsellable la configuració d'execució en diferit per a automatitzar les tasques i minimitzar el seguiment i la fallada humana.

En els sistemes UNIX la configuració es realitza via `crontab`, que pot realitzar-se de dues maneres: usant el fitxer de sistema `/etc/crontab` o bé el `crontab` de l'usuari (comando `crontab -l` per a visualitzar, o `crontab -e` per a editar-lo).

Primer tindrem que editar el fitxer `cron.sh` que es troba dintre del directori `cron` del SIGVI. Revisi les tres primeres variables:

- PHP: Que indica el path a l'executable de l'interpret de php de línia de comandos (generalment `/usr/bin/php5`)
- DIR: el directori on ha instal·lat el SIGVI (en aquest exemple és `/var/www/sigvi`)
- OUTPUT: el fitxer de sistema on es redirigirà la sortida estàndard i d'error dels processos.

Després faci servir el mètode que prefereixi, ja sigui editant el fitxer `/etc/crontab` o usant el `crontab` d'un usuari (`crontab -e`). Tingui en compte que aquest usuari haurà de tenir accés al directori Web on està

allotjat el SIGVI (per exemple www-data, o root).

- Opció 1: /etc/crontab. Com root, editarem el fitxer /etc/crontab i agregarem una línia com aquesta:

```
0 5 * * * www-data /var/www/sigvi/cron/cron.sh > /dev/null 2>&1
```

En aquest cas hem indicat que l'usuari sota el qual s'executarà el procés és www-data, que té accés al directori Web del SIGVI. També haurà d'adaptar el directori indicat (/var/www/sigvi) al de la seva instal·lació.

- Opció 2: crontab -e. Ja sigui com root, o com un usuari amb accés al directori Web (per exemple www-data) executem el comando “crontab -e” i afegim la següent línia:

```
0 5 * * * /var/www/sigvi/cron/cron.sh > /dev/null 2>&1
```

Adaptant el directori al de la seva instal·lació.

Finalment s'aconsella executar manualment el shell script cron.sh i comprovar la sortida, per a detectar i corregir possibles errors de configuració.

Si la seva plataforma és Windows, haurà de crear una tasca programada per a executar els scripts .php tal com fa el shell script cron.sh:

- plugins/sources/load_vulnerabilities.php
- plugins/sources/check_server_vulnerabilities.php
- plugins/discoverer/cron/check_repository_updates.php

3.7. Accedint per primera vegada

Obri un navegador Web i accedeixi al servidor (per exemple <http://server.localdomain.domain/sigvi>) i accedirà a la pàgina de login.

Per defecte existeix un únic usuari: “admin”, la contrasenya és “admin”.

Canviï la contrasenya com més aviat millor.

Una vegada validat accedirà al menú principal. En aquesta trobarà en la part superior del menú una icona d'informació a través del qual podrà accedir a una pàgina on se li indicarà quins són els passos a seguir després d'instal·lar una nova instància del SIGVI.

Per a més informació sobre les tasques inicials, llegeixi per favor el manual de l'usuari, en l'apartat de cada perfil trobarà un apartat de tasques inicials on s'explica amb més detall quines tasques ha d'executar per a deixar llista la seva nova instància.

4. Més ajuda

Si necessita més ajuda pot demanar informació a sebastian.gomez@upcnet.es

Gràcies pel seu interès, esperem que li resulti útil.