



SUBPROGRAMA AVANZA I+D 2010

VulneraNET

TSI-020100-2010-966

Manual de instalación de VulneraNET

VulneraNET

Herramientas y Procesos Colaborativos de Detección, Predicción y Corrección de Vulnerabilidades de aplicaciones web para desarrolladores y auditores de seguridad

VULNERANET



Germinus XXI

Universidad Politécnica de Madrid

Universidad Carlos III de Madrid

Skyworks Media Group SL

Mántica Solutions



RESUMEN EJECUTIVO

Este documento es la guía de instalación de VulneraNET, en ella se recogen los requisitos de la herramienta y los pasos a seguir para su instalación.



Información del Documento

Proyecto FIT Número	TSI-020100-2010-966	Acrónimo	VulneraNET
Título completo	Herramientas y Procesos Colaborativos de Detección, Predicción y Corrección de Vulnerabilidades de aplicaciones web para desarrolladores y auditores de seguridad		
URL	http://vulneranet.grupogesfor.com/		
URL del documento			

Entregable	Número	Título	Manual de instalación de VulneraNET
Paquete de Trabajo	Número	PT2, PT3, PT4, PT5, PT6	Título PT2. Especificación de requisitos y definición de una arquitectura extensible de un panel de control para herramientas de seguridad PT3. Herramientas para la resolución colaborativa de vulnerabilidades basados en tecnologías web2.0 y semánticas PT4. Herramientas y procesos de detección y resolución de vulnerabilidades basadas en auditorías de caja negra PT5. Herramientas y procesos de detección y resolución de vulnerabilidades basadas en análisis de código PT6. Herramientas de predicción de fallos de seguridad
Tarea	Número	T2.4, T2.5, T3.1, T4.3, T5.4, T6.3	Título T2.4 Diseño de la arquitectura de plugins para poder incluir distintas herramientas de seguridad en VulneraNET T2.5 Creación de herramienta de generación de informes de auditoría T3.1 Aplicación de seguimiento de vulnerabilidades. T4.3 Integración de la herramienta Wapiti con VulneraNET T5.4 Integración de la herramienta en VulneraNET T6.3. Integración de la herramienta de predicción de vulnerabilidades en VulneraNET



ÍNDICE

A. Introducción.....	5
B. Requisitos generales.....	6
C. Instalación de VulneranET.....	7
C.1 Base de datos.....	7
C.1.1 Ejecución de base de datos de prueba.....	7
C.1.2 Instalación de la base de datos.....	7
C.2 Instalación en servidor de aplicaciones.....	8
C.3 Archivos de configuración.....	8
C.3.1 Configuración de carpeta de almacenamiento de ficheros.....	8
C.3.2 Configuración de la base de datos.....	9
D. Instalación de Wapiti.....	10
D.1 Requisitos de Wapiti.....	10
D.2 Instalación de Wapiti.....	10
D.3 Configuración de Wapiti.....	11
E. Instalación de LAPSE+.....	12
E.1 Requisitos de LAPSE+.....	12
E.2 Instalación de LAPSE+.....	12
E.3 Configuración de LAPSE+.....	12
F. Instalación de Herramienta de predicción.....	13
F.1 Requisitos de la Herramienta de Predicción.....	13
F.2 Instalación de la Herramienta de Predicción.....	13
F.3 Configuración de la Herramienta de Predicción.....	14
G. Índice de Ilustraciones.....	16
H. Referencias.....	17



A. Introducción

Este documento es la guía de instalación de la aplicación VulneraNET [VulURL] y en ella se explica de forma pormenorizada los pasos que hay que seguir para instalarla, así como los requisitos necesarios para su instalación.

VulneraNET integra herramientas de seguridad como Wapiti [WapURL] [Wap2URL] y LAPSE [L+URL] [L+2URL], y cuya instalación también está documentada en esta guía.



B. Requisitos generales

La aplicación VulneraNET [VulURL] necesita los siguientes requerimientos para ser instalado:

- El entorno Java Runtime Environment (JRE) 1.6.
- Un contenedor de servlets o servidor de aplicaciones J2EE (Apache Tomcat, JBoss, Weblogic, Glassfish, etc).
- Un sistema gestor de base de datos (HSQLDB, MySQL, Oracle, etc).

C. Instalación de VulneraNET

Si se desea usar la configuración por defecto, únicamente es necesario seguir los pasos C.1.1 Ejecución de base de datos de prueba y C.2 Instalación en servidor de aplicaciones

Para una instalación más avanzada se recomienda leer también los pasos C.1.2 Instalación de la base de datos, C.2 Instalación en servidor de aplicaciones y C.2 Instalación en servidor de aplicaciones.

La aplicación VulneraNET y su base de datos está empaquetado en un ZIP que se encuentra alojado en SourceForge:

<https://sourceforge.net/projects/vulneranet/files/VulneraNET/VulneraNET.zip/download>

C.1 Base de datos

AVISO: VulneraNET posee una configuración por defecto que utiliza HSQLDB ejecutado desde un fichero y no requiere de instalación de base de datos. Sin embargo, se recomienda instalar la base de datos en un sistema gestor de bases de datos para mayor eficiencia.

AVISO: La base de datos debe estar arrancada antes de iniciar el servidor aplicaciones o de desplegar VulneraNET en el servidor de aplicaciones.

C.1.1 Ejecución de base de datos de prueba

La base de datos se puede encontrar en la carpeta *database* dentro del ZIP de la aplicación que se encuentra alojado en SourceForge:

<https://sourceforge.net/projects/vulneranet/files/VulneraNET/VulneraNET.zip/download>

Para ejecutar la base de datos sin instalación se debe entrar en la carpeta *database* y:

- si usted trabaja con un entorno **GNU/Linux** debe ejecutar el archivo *script_db.sh*.
- si usted trabaja en un entorno **Windows** debe renombrar el archivo *script_db.sh* como *script_db.bat* y ejecutar *script_db.bat*.

C.1.2 Instalación de la base de datos

La base de datos se puede encontrar en la carpeta *database* dentro del ZIP de la aplicación que se encuentra alojado en SourceForge:

<https://sourceforge.net/projects/vulneranet/files/VulneraNET/VulneraNET.zip/download>

Para instalar la base de datos se deben seguir los siguientes pasos:



- Crear una nueva base de datos en el sistema gestor de bases de datos.
- Crear un usuario que tenga permisos sobre esa base de datos.
- Ejecutar el *script* que se encuentra en la ruta *database/vulneranetdb.script* para crear la estructura de tablas.
- Se debe colocar el driver java correspondiente al sistema gestor de base de datos en la ruta *WEB-INF/lib*. Visite [DriURL] [DriURL] para conocer la lista de bases de datos que tienen driver de conexión.

C.2 Instalación en servidor de aplicaciones

El WAR donde se distribuye VulneraNET debe ser desplegado en un servidor de aplicaciones.

VulneraNET.war viene empaquetado en un fichero ZIP, que se encuentra alojado en SourceForge:

<https://sourceforge.net/projects/vulneranet/files/VulneraNET/VulneraNET.zip/download>

C.3 Archivos de configuración

AVISO: Cada vez que se cambie un archivo de configuración es necesario reiniciar el servidor de aplicaciones o realizar un nuevo despliegue de VulnerNET en el servidor de aplicaciones con los archivos configurados.

C.3.1 Configuración de carpeta de almacenamiento de ficheros

Para configuración de las carpetas para almacenar ficheros (informes, logs, etc), es necesario editar el fichero *VulneraNET/WEB-INF/classes/conf/common/conf.xml*

```
<?xml version="1.0" encoding="UTF-8"?>
<beans xmlns="http://www.springframework.org/schema/beans"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:schemaLocation="http://www.springframework.org/schema/beans
                           http://www.springframework.org/schema/beans/spring-beans-
3.0.xsd">
  <bean id="properties" class="java.util.Properties">
    <constructor-arg>
      <props>
        <prop key="report.path">reports</prop>
        <prop key="log.path">logs</prop>
        <prop key="import.path">imports</prop>
      </props>
    </constructor-arg>
  </bean>
</beans>
```



Los textos en negrita son las carpetas donde se almacenarán los archivos correspondientes a:

- Informes (report.path)
- Logs (log.path)
- Informes importados (import.path)

AVISO: Se recomienda poner rutas absolutas. Si se especifica una ruta relativa, la carpeta se creará dentro de la jerarquía de carpetas del servidor de aplicaciones.

C.3.2 Configuración de la base de datos

Para configurar la conexión a base de datos se debe abrir el archivo *VulneraNET/WEB-INF/classes/hibernate.cfg.xml* y editar las siguientes líneas:

```
<property name="connection.driver_class">org.hsqldb.jdbcDriver
</property>
<property
name="connection.url">jdbc:hsqldb:hsqldb://localhost/vulneranetdb
</property>
<property name="connection.username">vulneranet</property>
<property name="connection.password">password</property>
```

Los parámetros son los siguientes:

- connection.driver_class: es el nombre del driver de conexión a base de datos
- connection.url: la URL donde se encuentra la base de datos
- connection.username: el usuario de base de datos
- connection.password: la contraseña para ese usuario.



D. Instalación de Wapiti

D.1 Requisitos de Wapiti

Wapiti [WapURL] [Wap2URL] es un auditor y escaner de aplicaciones web que se encuentra disponible en la distribución de VulneraNET, para realizar pruebas de caja negra sobre las aplicaciones.

Wapiti requiere de:

1. El entorno de ejecución de Python [PydURL] para ejecutarse ya que está implementado con ese lenguaje de programación [PytURL].
2. Una vez instalado, el ejecutable **python** (sistemas UNIX / GNU/Linux) o **python.exe** (sistemas MS-DOS / Windows) debe colocarse en la variable de entorno [VARURL] "PATH" para poder ser ejecutado desde cualquier directorio.

D.2 Instalación de Wapiti

Wapiti debe ser extraído del ZIP donde se distribuye y colocado en un directorio del sistema:

El zip se encuentra alojado en:

http://vulneranet.grupogesfor.com/c/document_library/get_file?p_l_id=57463&folderId=57476&name=DLFE-8335.zip

Para indicarle a la aplicación cual es la ruta hasta Wapiti, se debe indicar la ruta donde se encuentra instalado Wapiti, que debe ser *VulneraNET/WEB-INF/classes/conf/tools/wapiti.xml* dentro de la carpeta donde se despliegue el WAR.

O bien, si se desea instalar una nueva versión de Wapiti o cambiar Wapiti de directorio se debe indicar la ruta donde se encuentre instalado Wapiti.

```
<property name="parameters">
  <list>
    <bean class="es.gesfor.vulneranet.securitytool.Parameter">
      <property name="value"
value="/home/david/Presentaciones/OWASP/wapiti-svn/src/wapiti.py" />
      <property name="hidden" value="true" />
    </bean>
    .....
  </list>
</property>
```


E. Instalación de LAPSE+

LAPSE+ [L+URL] [L+2URL] es una herramienta destinada a detectar vulnerabilidades de seguridad en el código fuente de Aplicaciones Web Java. El manual de usuario y de instalación de LAPSE+ están disponibles en: http://evalues.es/downloads/lapse/LapsePlusTutorial_2.8.0.pdf

E.1 Requisitos de LAPSE+

1. La aplicación tiene como requisito la instalación de Apache ANT [AntURL].
2. Una vez instalado, el ejecutable **ant** (sistemas UNIX / GNU/Linux) o **ant.exe** (sistemas MS-DOS / Windows) debe colocarse en la variable de entorno [VARURL] "PATH" para poder ser ejecutado desde cualquier directorio.

E.2 Instalación de LAPSE+

LAPSE se puede descargar de:

http://evalues.es/downloads/lapse/LapsePlusConsola_2.8.0.zip

Una vez descargado es necesario descomprimir LAPSE+ en un directorio de nuestro disco duro.

E.3 Configuración de LAPSE+

Además, en el fichero de configuración de LAPSE (*VulneraNET/WEB-INF/classes/conf/tools/lapse.xml*) se ha de añadir la siguiente ruta apuntando a donde se encuentra instalada la aplicación (sustituir texto en negrita), es decir, donde se ha descomprimido previamente LAPSE+.

```
<bean id="lapse"
class="es.gesfor.vulneranet.securitytool.SecurityTool"
scope="prototype">
...
<property name="exec" value="ant -buildfile
/home/david/Programas/IDEs/lapsePlusConsola_2.8.0/build.xml run" />
...
</bean>
```

F. Instalación de Herramienta de predicción

La herramienta de predicción [PreURL] tiene por objetivo predecir posibles nuevos ataques en función de muestras de tráfico y patrones de ataques.

F.1 Requisitos de la Herramienta de Predicción

Para la instalación de la herramienta de predicción es necesario tener instalado Ruby [RubURL] en el sistema operativo. La herramienta ha sido testeada bajo las versiones de Ruby: 1.8, recomendada, y 1.9.

Una vez instalado, el ejecutable **ruby** (sistemas UNIX / GNU/Linux) o **ruby.exe** (sistemas MS-DOS / Windows) debe colocarse en la variable de entorno [VARURL] "PATH" para poder ser ejecutado desde cualquier directorio.

Además, hay que instalar las siguientes gemas:

- gem install decisiontree (testada bajo la versión 0.3.0)
- gem install rails

Posteriormente es necesario cambiar el archivo dentro del directorio principal de Ruby:

```
.\lib\ruby\gems\<version_ruby>\gems\decision-tree-0.3.0\lib\decisiontree\id3_tree.rb
```

por el archivo *id3_tree.rb* que se pasa dentro del archivo ZIP.

F.2 Instalación de la Herramienta de Predicción

La herramienta tiene dos versiones y puede descargarse de:

- Versión para Windows:
http://sourceforge.net/projects/vulneranet/files/prediccion/v0.8/herramienta_prediccion_v0.8_win.zip/download
- Versión para Linux:
http://sourceforge.net/projects/vulneranet/files/prediccion/v0.8/herramienta_prediccion_v0.8_linux.zip/download

La herramienta debe ser extraída del ZIP en el que se encuentra y colocada en un directorio del sistema. La descompresión generará los siguientes grupos de archivos:

- Directorio SOM_PARK.3R1: necesario para realizar tareas de clustering.
- id3_tree.rb: necesario para realizar tareas de clasificación por árbol de búsquedas.



- Resto de archivos .rb: contienen las funciones de la herramienta de predicción.
- vulnerabilityTypes.txt: contiene la lista de vulnerabilidades posibles a identificar. Están rellenos para el dataset de prueba.
- attributes.txt: contiene la lista de atributos que poseen los conjuntos de datos. Están rellenos para el dataset de prueba.
- kddcup.data_10_por_ciento: conjunto de datos (dataset) inicial para realizar pruebas.

La herramienta ha sido testeada bajo Windows y en Linux. En Linux, la herramienta SOM_PARK.3R1 no tiene los ejecutables creados sino estos tienen que ser creados por el usuario. Para ello es necesario acceder al directorio SOM_PARK.3R1 y ejecutar los comandos:

- cp makefile.unix makefile
- make -f makefile

F.3 Configuración de la Herramienta de Predicción

Además, para su correcto funcionamiento, en el fichero de configuración de la herramienta (*VulneranET/WEB-INF/classes/conf/tools/prediction/prediction-tool.xml*) se ha de indicar:

- El directorio donde se guardarán los ficheros de salida.
 - Ej: /home/ebarea/Vulneranet/prediccion
- El directorio donde se encuentra la aplicación
 - Ej: /home/ebarea/Vulneranet/HerramientaPrediccion/
- Directorio HOME del usuario.
 - Ej: /home/ebarea

```
<bean id="outputFilePath" class="java.lang.String">
  <constructor-arg>
    <value>/home/ebarea/Vulneranet/prediccion</value>
  </constructor-arg>
</bean>

<bean id="executionPath" class="java.lang.String">
  <constructor-arg>
    <value>/home/ebarea/Vulneranet/HerramientaPrediccion/</value>
  </constructor-arg>
</bean>

<bean id="home" class="java.lang.String">
  <constructor-arg>
```



```
<value>/home/ebarea</value>  
</constructor-arg>  
</bean>
```



G. Índice de Ilustraciones

H. Referencias

[AntURL]

Proyecto Apache Ant: <http://ant.apache.org/>

[DriURL]

Lista de drivers registrados por SUN:
<http://developers.sun.com/product/jdbc/drivers/>

[ISO-639-1]

Códigos del nombre de los idiomas según ISO-639-1:
http://www.loc.gov/standards/iso639-2/php/English_list.php

[ISO-3166]

Códigos del nombre de los países según ISO-3166:
http://www.iso.org/iso/english_country_names_and_code_elements

[JdbURL]

Empresas que tienen productos relacionados con el API JDBC:
<http://java.sun.com/products/jdbc/reference/industrysupport/index.html>

[L+URL]

Sitio web de LAPSE+,
<http://www.evalues.es/index.php/en/vulneranet/97-lapse.html>

[L+2URL]

Página web de LAPSE+ dentro del portal de VulneranET,
<http://vulneranet.grupogesfor.com/lapse>

[PreURL]

Página de descarga de Python,
<http://vulneranet.grupogesfor.com/herramienta-prediccion>

[PydURL]

Página de descarga de Python, <http://www.python.org/download/>

[PytURL]

Sitio web de Python, <http://www.python.org/>

[RubURL]

Sitio web de Ruby, <http://www.ruby-lang.org/>

[VARURL]

Wikipedia, entrada sobre variables de entorno,
http://es.wikipedia.org/wiki/Variable_de_entorno



[VuURL]

Sitio web de VulneraNET, <http://vulneranet.grupogesfor.com>

[WapURL]

Sitio web de Wapiti, <http://www.ict-romulus.eu/web/wapiti>

[Wap2URL]

Página web de Wapiti dentro del portal de VulneraNET,
<http://vulneranet.grupogesfor.com/owasp-wapiti>