Security bugtracker

User Manual

Eric Therond

Contents

Chapter 1

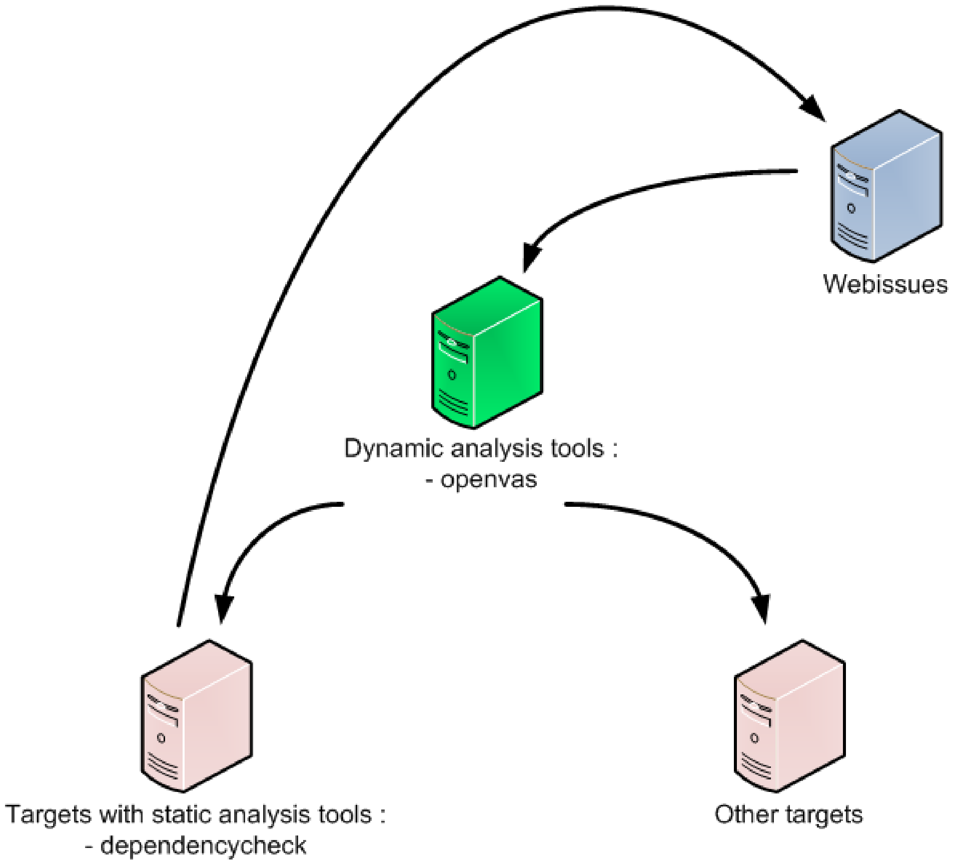
Installation

1.1 Overview

Security-bugtracker is currently a tool based on three dependencies :

- webissues : a bug tracker
  http://webissues.mimec.org/
- openvas : a dynamic security vulnerabilities assessment tool
  http://www.openvas.org/
- dependency-check : a static security vulnerabilities assessment tool
  https://github.com/jeremylong/DependencyCheck

Each of this tool can be installed on different or same server.
The aim of this project is to produce automated security tests and track detected default in a bugtracker.



1.2 Openvas

See the documentation on the official web site : http://www.openvas.org/install-source.html
On the same server install a web server and php, then copy the following module of this project to the directory of your web server :/security-bugtracker/security_tools/openvas
Then edit /security-bugracker/security_tools/openvas/openvas.conf.php :

```php
<?php

$CONF_WS_OPENVAS_LOGIN = "test";
$CONF_WS_OPENVAS_PASSWORD = "test";
$CONF_WEBISSUES_OPENVAS_LOGIN = "openvas";
$CONF_WEBISSUES_OPENVAS_PASSWORD = "openvas";
$CONF_WEBISSUES_WS_ENDPOINT = "http://localhost:8080/webissues-server-1.1.4/client/webservices.php";
$CONF_OPENVAS_ALERT_URL = "http://localhost:8080/webissues-server-1.1.4/client/security_tools/openvas/openvas.php";
$CONF_OPENVAS_ADMIN_LOGIN = "admin";
$CONF_OPENVAS_ADMIN_PASSWORD = "0825839c-0d3f-4417-a118-954a78e2553c";
$CONF_OPENVAS_CONFIG_ID = "a0e8fed8-45c1-4890-bd08-671257f63308";
$CONF_OPENVAS_PATH_OMP = "/usr/local/bin/omp";
$CONF_OPENVAS_PORT_OMP = "9393";

?>
```

- CONF_WS_OPENVAS_LOGIN
- CONF_WS_OPENVAS_PASSWORD

are the credentials for the web services of this module.

- CONF_WEBISSUES_OPENVAS_LOGIN
- CONF_WEBISSUES_OPENVAS_PASSWORD
- CONF_WEBISSUES_WS_ENDPOINT

will be completed later.

- CONF_OPENVAS_ALERT_URL

is the address of this module on this web server.

- CONF_OPENVAS_ADMIN_LOGIN
- CONF_OPENVAS_ADMIN_PASSWORD

are the openvas admin credentials.

- CONF_OPENVAS_CONFIG_ID

is the default config id for run a scan with openvas, check your config with this openvas command

```
linux-3ig5:/home/eric/security-bugracker/documentation # omp -u admin -w 0825839c-0d3f-4417-a118-954a78e2553c -p 9393 --get-configs
8715c877-47a0-438d-98a3-27c7a6ab2196  Discovery
085569ce-73ed-11df-83c3-002264764cea  empty
daba56c8-73ec-11df-a475-002264764cea  Full and fast
698f691e-7489-11df-9d8c-002264764cea  Full and fast ultimate
708f25c4-7489-11df-8094-002264764cea  Full and very deep
a0e8fed8-45c1-4890-bd08-671257f63308  Full and very deep Clone 1
74db13d6-7489-11df-91b9-002264764cea  Full and very deep ultimate
2d3f051c-55ba-11e3-bf43-406186ea4fc5  Host Discovery
bbca7412-a950-11e3-9109-406186ea4fc5  System Discovery
```

- CONF_OPENVAS_PATH_OMP

is the path of your omp binary on this server.

- CONF_OPENVAS_PORT_OMP

is the tcp port which on openvas / omp is running

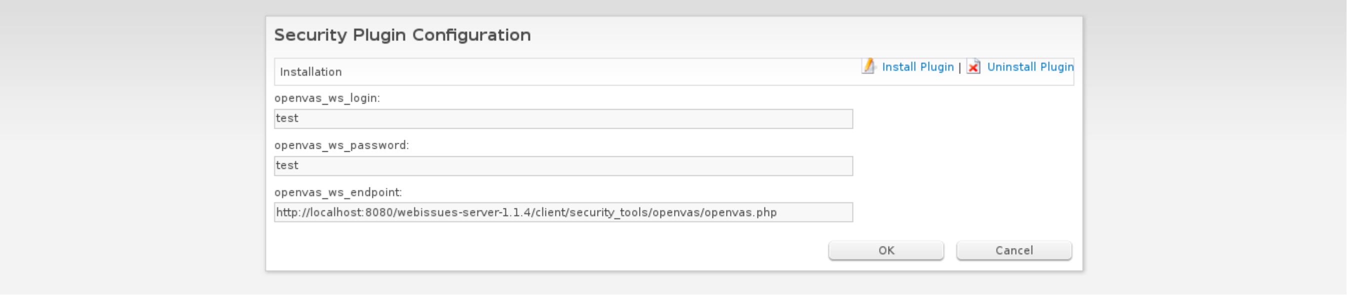
1.3 Dependency-check

See the documentation on the official web site : https://github.com/jeremylong/DependencyCheck

1.4 Webissues

See the documentation on the official web site : http://wiki.mimec.org/wiki/WebIssues/Installation. Once the bugtracker is installed, copy the following module of this project to your webissues root directory : /security-bugracker/webissues-server-1.1.4

Next go at this address (replace the name, port, path with rights informations) :
http://localhost:8080/webissues-server-1.1.4/client/securityplugin.php


Security Plugin Configuration

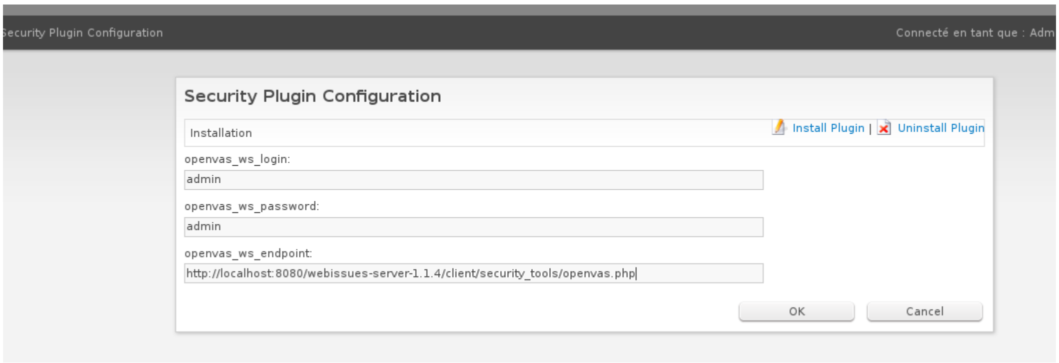
openvas_ws_login: test

openvas_ws_password: test

openvas_ws_endpoint: http://localhost:8080/webissues-server-1.1.4/client/security_tools/openvas/openvas.php

Select *install plugin* and enter choosen values when the openvas module was installed above :

- CONF_WS_OPENVAS_LOGIN
- CONF_WS_OPENVAS_PASSWORD
- CONF_OPENVAS_ALERT_URL


Security Plugin Configuration

openvas_ws_login: admin

openvas_ws_password: admin

openvas_ws_endpoint: http://localhost:8080/webissues-server-1.1.4/client/security_tools/openvas.php

ecurity Plugin Configuration
Connecté en tant que : Adm
Installation
Install Plugin | Uninstall Plugin
OK
Cancel

Now create *openvas* and *Dependency-check* users on webissues.

Chapter 2

Use

Don't forget to use *basic authentification* with a login which have the good rights on webissues when using the webservices.

2.1 add a project

Add a project with the following web service method or via the traditional him of web issues :

```xml
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:v1="http://securitybugtracker/V1">
   <soapenv:Header/>
   <soapenv:Body>
      <v1:addproject>
         <name>TEST</name>
         <description>TEST</description>
      </v1:addproject>
   </soapenv:Body>
</soapenv:Envelope>
```

Remember the ids returned with the response :

```xml
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ns1="http://securitybugtracker/V1">
   <SOAP-ENV:Body>
      <ns1:addproject_Response>
         <id_details>
            <id_project>29</id_project>
            <id_folder_bugs>81</id_folder_bugs>
            <id_folder_servers>82</id_folder_servers>
            <id_folder_codes>83</id_folder_codes>
            <id_folder_scans>84</id_folder_scans>
         </id_details>
      </ns1:addproject_Response>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

2.2 add a member

Add a *robot* member for this project (the *openvas* account created during the installation) :

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:v1="http://securitybugtracker/V1">
   <soapenv:Header/>
   <soapenv:Body>
      <v1:addmember>
         <id_user>4</id_user>
         <id_project>29</id_project>
         <access>admin</access>
      </v1:addmember>
   </soapenv:Body>
</soapenv:Envelope>
```

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ns1="http://securitybugtracker/V1">
   <SOAP-ENV:Body>
      <ns1:addmember_Response>
         <result_details>
            <result>true</result>
         </result_details>
      </ns1:addmember_Response>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

2.3 add a server

Add a target server for this project, you can add multiple ips separated by the , character and the values of *use parameter* must be one of thoses :

- Development : for a development environment server
- Test : for a test environment server
- Production : for a production environment server

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:v1="http://securitybugtracker/V1">
   <soapenv:Header/>
   <soapenv:Body>
      <v1:addserver>
         <id_folder_servers>82</id_folder_servers>
         <hostname>eric-pc</hostname>
         <description>eric-pc</description>
         <use>Production</use>
         <ipsaddress>127.0.0.1</ipsaddress>
      </v1:addserver>
   </soapenv:Body>
</soapenv:Envelope>
```

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ns1="http://securitybugtracker/V1">
   <SOAP-ENV:Body>
      <ns1:addserver_Response>
         <result_addserver_details>
            <id_server>1676</id_server>
         </result_addserver_details>
      </ns1:addserver_Response>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

2.4 add a code

Add a target code path for this project, the *code parameter* is the path of the directory which contain librairies to be scanned by the dependency-check security tool.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:v1="http://securitybugtracker/V1">
   <soapenv:Header/>
   <soapenv:Body>
      <v1:addcode>
         <id_folder_codes>83</id_folder_codes>
         <name>java test</name>
         <description>java tes</description>
         <code>/home/eric/test/libs-java</code>
      </v1:addcode>
   </soapenv:Body>
</soapenv:Envelope>
```

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ns1="http://securitybugtracker/V1">
   <SOAP-ENV:Body>
      <ns1:addcode_Response>
         <result_addcode_details>
            <id_code>1680</id_code>
         </result_addcode_details>
      </ns1:addcode_Response>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

2.5 scan the targets

2.5.1 Dynamic scan with openvas

Run a scan with openvas security tool, select openvas value for the *tool parameter*, select a specific openvas config scan if you don't want to use the default config parametered during the installation and select a filter which can be :

- info : only add issues with a severity equal or upper to info
- minor : only add issues with a severity equal or upper to minor
- medium : only add issues with a severity equal or upper to medium
- high : only add issues with a severity equal to high

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:v1="http://securitybugtracker/V1">
   <soapenv:Header/>
   <soapenv:Body>
      <v1:addscan>
         <id_folder_scans>88</id_folder_scans>
         <name>test scan soap ui</name>
         <description>test scan soap ui</description>
         <tool>openvas</tool>
         <filter>medium</filter>
         <!--Optional:-->
         <id_config_openvas>?</id_config_openvas>
      </v1:addscan>
   </soapenv:Body>
</soapenv:Envelope>
```

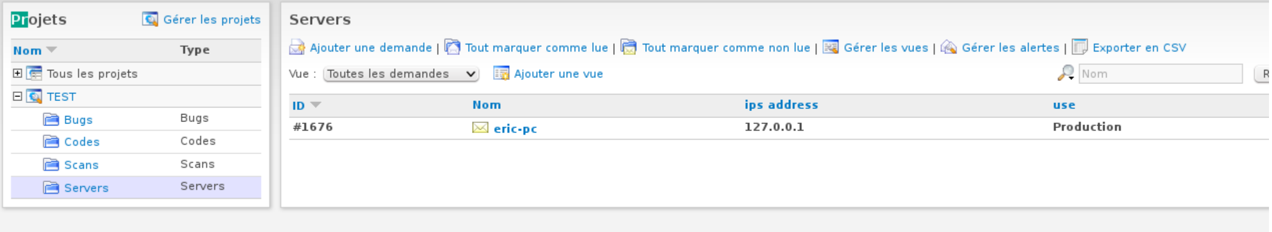
```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ns1="
    http://securitybugtracker/V1">
   <SOAP-ENV:Body>
      <ns1:addscan_Response>
         <result_addscan_details>
            <id_scan>2422</id_scan>
         </result_addscan_details>
      </ns1:addscan_Response>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

2.5.2 Static scan with dependency-check

The static scan must me run localy, see jobs chapter.

2.6 Results

You can view the results of your precedings actions with th him of webissues :



Projets | Gérer les projets

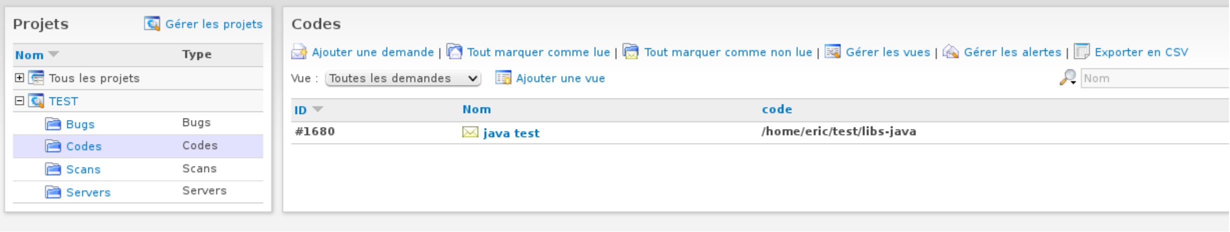
Nom	Type
⊞ Tous les projets	
⊟ TEST	
Bugs	Bugs
Codes	Codes
Scans	Scans
Servers	Servers

Servers

Ajouter une demande | Tout marquer comme lue | Tout marquer comme non lue | Gérer les vues | Gérer les alertes | Exporter en CSV

Vue : Toutes les demandes | Ajouter une vue | Nom

ID	Nom	ips address	use
#1676	eric-pc	127.0.0.1	Production



Projets | Gérer les projets

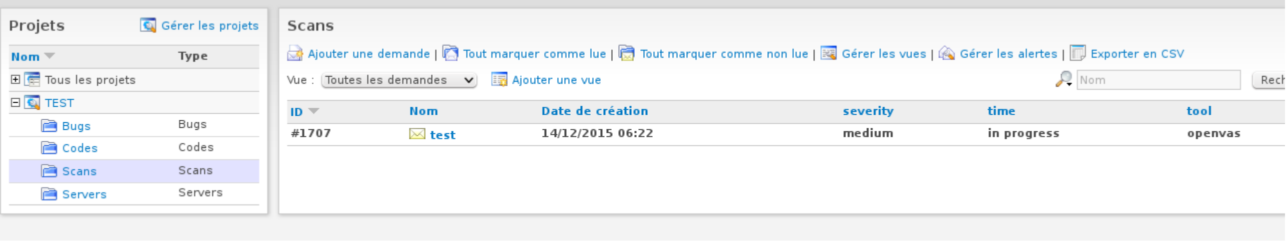
Nom	Type
⊞ Tous les projets	
⊟ TEST	
Bugs	Bugs
Codes	Codes
Scans	Scans
Servers	Servers

Codes

Ajouter une demande | Tout marquer comme lue | Tout marquer comme non lue | Gérer les vues | Gérer les alertes | Exporter en CSV

Vue : Toutes les demandes | Ajouter une vue | Nom

ID	Nom	code
#1680	java test	/home/eric/test/libs-java



Projets | Gérer les projets

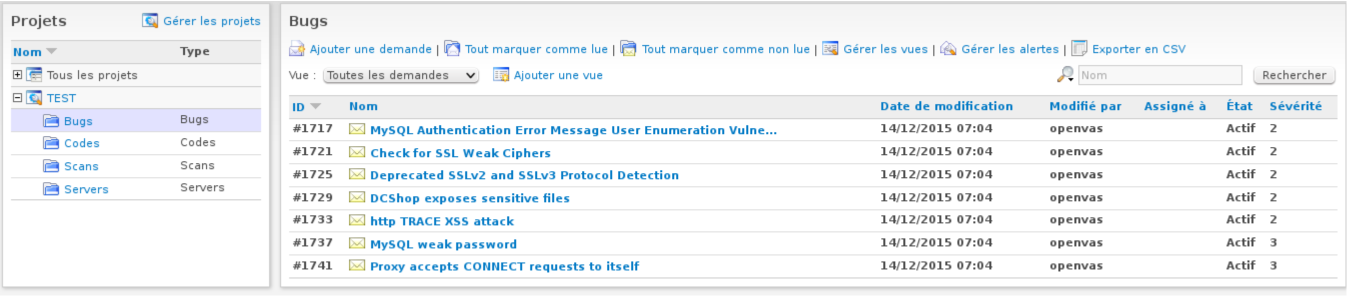
Nom	Type
⊞ Tous les projets	
⊟ TEST	
Bugs	Bugs
Codes	Codes
Scans	Scans
Servers	Servers

Scans

Ajouter une demande | Tout marquer comme lue | Tout marquer comme non lue | Gérer les vues | Gérer les alertes | Exporter en CSV

Vue : Toutes les demandes | Ajouter une vue | Nom | Rech

ID	Nom	Date de création	severity	time	tool
#1707	test	14/12/2015 06:22	medium	in progress	openvas



Projets | Gérer les projets

Nom	Type
⊞ Tous les projets	
⊟ TEST	
Bugs	Bugs
Codes	Codes
Scans	Scans
Servers	Servers

Bugs

Ajouter une demande | Tout marquer comme lue | Tout marquer comme non lue | Gérer les vues | Gérer les alertes | Exporter en CSV

Vue : Toutes les demandes | Ajouter une vue | Nom | Rechercher

ID	Nom	Date de modification	Modifié par	Assigné à	État	Sévérité
#1717	MySQL Authentication Error Message User Enumeration Vulne...	14/12/2015 07:04	openvas		Actif	2
#1721	Check for SSL Weak Ciphers	14/12/2015 07:04	openvas		Actif	2
#1725	Deprecated SSLv2 and SSLv3 Protocol Detection	14/12/2015 07:04	openvas		Actif	2
#1729	DCShop exposes sensitive files	14/12/2015 07:04	openvas		Actif	2
#1733	http TRACE XSS attack	14/12/2015 07:04	openvas		Actif	2
#1737	MySQL weak password	14/12/2015 07:04	openvas		Actif	3
#1741	Proxy accepts CONNECT requests to itself	14/12/2015 07:04	openvas		Actif	3

Chapter 3

Jobs

You can easily script a job which can interact with your configuration management tool for example for requesting automatically the web services and running security scans.
You can see examples in the jobs directory :
/security-bugracker/security_tools/jobs/run_dependencycheck.php
/security-bugracker/security_tools/jobs/run_openvas.php