

SecQua v.0.6

Constantinos Patsakis

August 5, 2012



1 About

SecQua is an open source project written in Python, that tries to quantify the security of a given Information System, using a novel security metric.

The data that are being used are from the [National Vulnerability Database](#), for latest exports you may visit this [link](#).

For any comments please email [me](#).

2 Dependencies

The project depends on the following open and free projects/libraries:

- Python
- MySQL Server
- SciPy
- NumPy
- matplotlib and
- MySQL-Python
- xwPyption

3 Install

3.1 Ubuntu/Debian

For Ubuntu users you should have installed MySQL, if not run:

```
sudo apt-get install mysql-server
```

To install Python and the needed libraries open a terminal and type:

```
sudo apt-get install python python-mysqldb python-matplotlib  
python-scipy python-wxgtk2.8
```

Download the latest version and extract it in a folder. Open file config.ini and edit the file according to your MySQL installation, add your name for author of the report, fix paper size, the type of splines etc.

To import the database, extract the file named nvd.zip, open a terminal and go to the extracted file. Then open a terminal, browse to the folder where you extracted the compressed file and type:

```
mysql -u root -p <nvd.sql
```

3.2 Windows

Download and install the following:

- Python 2.7.3 Windows Installer from [here](#)
- MySQL Server from [here](#)
- SciPy 2.7 super pack from [here](#)
- NumPy 2.7 super pack from [here](#)
- matplotlib from [here](#)
- MySQL-Python from [here](#) (for easier installation, get it from [here](#)).
- wx-Python 2.8 from [here](#)

Open file config.ini and edit the file according to your MySQL installation, add your name for author of the report, fix paper size, the type of splines etc. Finally, open a command line and execute:

```
mysql -u root -p <nvd.sql
```

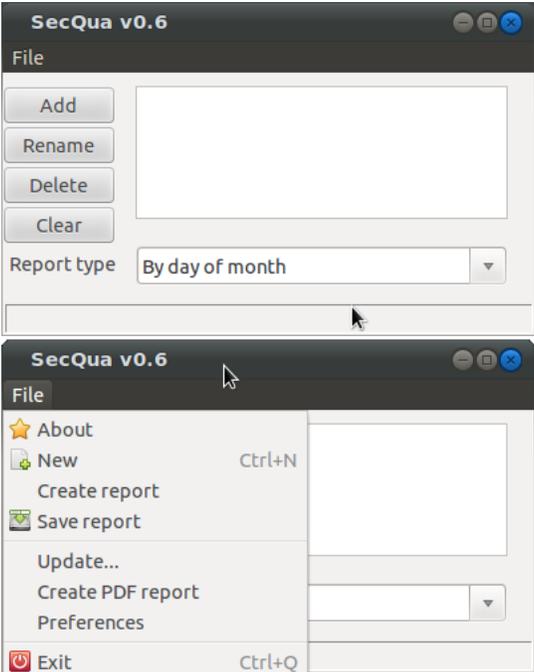


Figure 1: Main window and menu.

4 Run

From the folder you extracted the files run:

```
python secqua-gui.py
```

A window will pop up, figure 1, where you choose the report type by day of week, day of month etc. To add, edit, delete components press the according buttons. The supported format supports SQL regular expression syntax. For example typing **windows** will try to find any vulnerabilities regarding windows, that means all software that in their name have the word windows. To better quantify the security level, as the previous query will not only return results for Microsoft Windows, but for other software as well, refine the query e.g. **windows_server_2008** or **windows_xp**. Even better, type **kernel:2.6.[23][0-9]** in order to search for linux kernels from 2.6.20 and above or even **microsoft*.windows_server_2003** to ensure that only Microsoft products have been selected. Leave blank and press <enter> to finish with IS software.

When finished with the data entry, go to **File>Create report**, a figure displaying the security status over the selected period will be shown and the calculated security level as well, figure 2. To save the report, go to **File>Save**, just remember it is a \LaTeX file. If you have installed \LaTeX , you may create the PDF file by selecting **File>Create PDF report**.

A typical report can be download from [here](#).

The exported graphs are like the ones in figure 2.

To update the database you go to **File>Update...** and either type the local address of the XML file you have downloaded from National Vulnerability Database or just the URL with the link to this XML file.

5 Licence

SecQua is licensed under the GPL ver.2. The full text of the license is available [here](#).

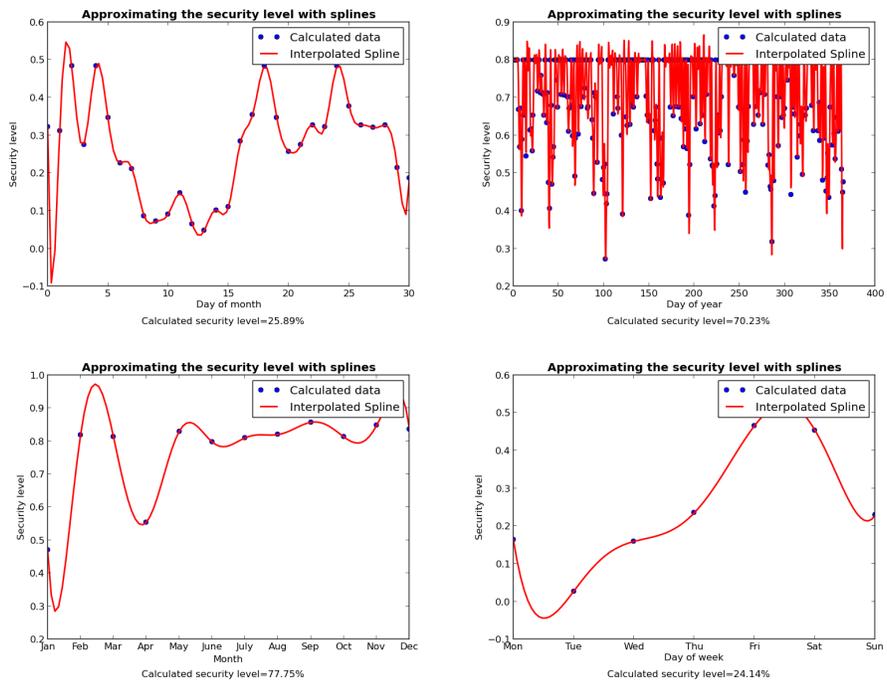


Figure 2: Example graphs.