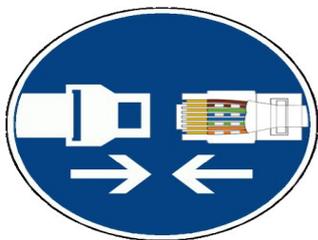


[www.seguridadpyme.es](http://www.seguridadpyme.es)

*ASISTENCIA TÉCNICA A LA SEGURIDAD INFORMÁTICA EN PYMES*

# *MANUAL FLUNYMOUS*





www.seguridadpyme.es

## Flunym0us

*Bueno esta herramienta llamada flunym0us, nos servirá para realizar escaneos en websites que tengan el CMS wordpress y Moodle.*

### 1. Funcionalidades de Flunym0us 2.0 :

- *Fingerprint de versión de WordPress: Extrae de los archivos "Readme.html" la versión actual instalada de WordPress.*
- *Descubrimiento de vulnerabilidades por Path Disclosure en WordPress que dejan expuesta la ruta de instalación.*
- *Descubrimiento de versión de plugins instalados en WordPress.*
- *Aviso de versiones obsoletas de instalaciones de WordPress.*
- *Aviso de versiones obsoletas de instalaciones de plugins en WordPress.*
- *Descubrimiento de usuarios registrados.*
- *Aumento en la velocidad de análisis gracias al procesamiento en paralelo con múltiples procesos parametrizables.*
- *Ocultación de User-Agent por uno aleatorio a través de un diccionario incluido de User-Agents reales.*

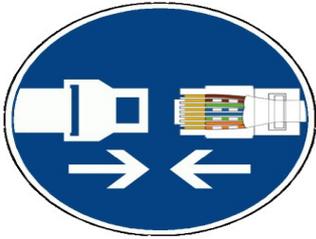
### 2. Uso e Instalacion:

*Descargamos la herramienta: <http://code.google.com/p/flunym0us/downloads/list>*

*Lo dejamos en nuestro escritorio y seguimos los pasos.*

#### *Primero descomprimir:*

- *cd Desktop*
- *tar -xvf flunym0us2.0.tar.gz*
- *guardamos los archivos en una carpeta, en este caso : flunym0us*
- *vamos a la carpeta : cd Desktop/flunym0us*
- *python flunym0us.py y tendremos listo para realizar el escaneo.*



[www.seguridadpyme.es](http://www.seguridadpyme.es)

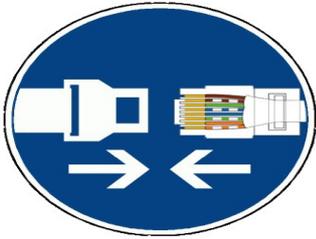
### Comandos :

- *-h, -help: Show this help message and exit*
- *-wp, -wordpress: Scan WordPress site*
- *-mo, -moodle: Scan Moodle site*
- *-H HOST, -host HOST: Website to be scanned*
- *-w WORDLIST, -wordlist WORDLIST: Path to the wordlist to use*
- *-t TIMEOUT, -timeout TIMEOUT: Connection timeout*
- *-r RETRIES, -retries RETRIES: Connection retries*
- *-p PROCESS, -process PROCESS: Number of process to use*
- *-T THREADS, -threads THREADS: Number of threads (per process) to use*
- *Y el comando del ataque: `python flunym0us.py -H http://www.target.com -wp -w wp-plugins.lst -t 60 -r 1 -T`*

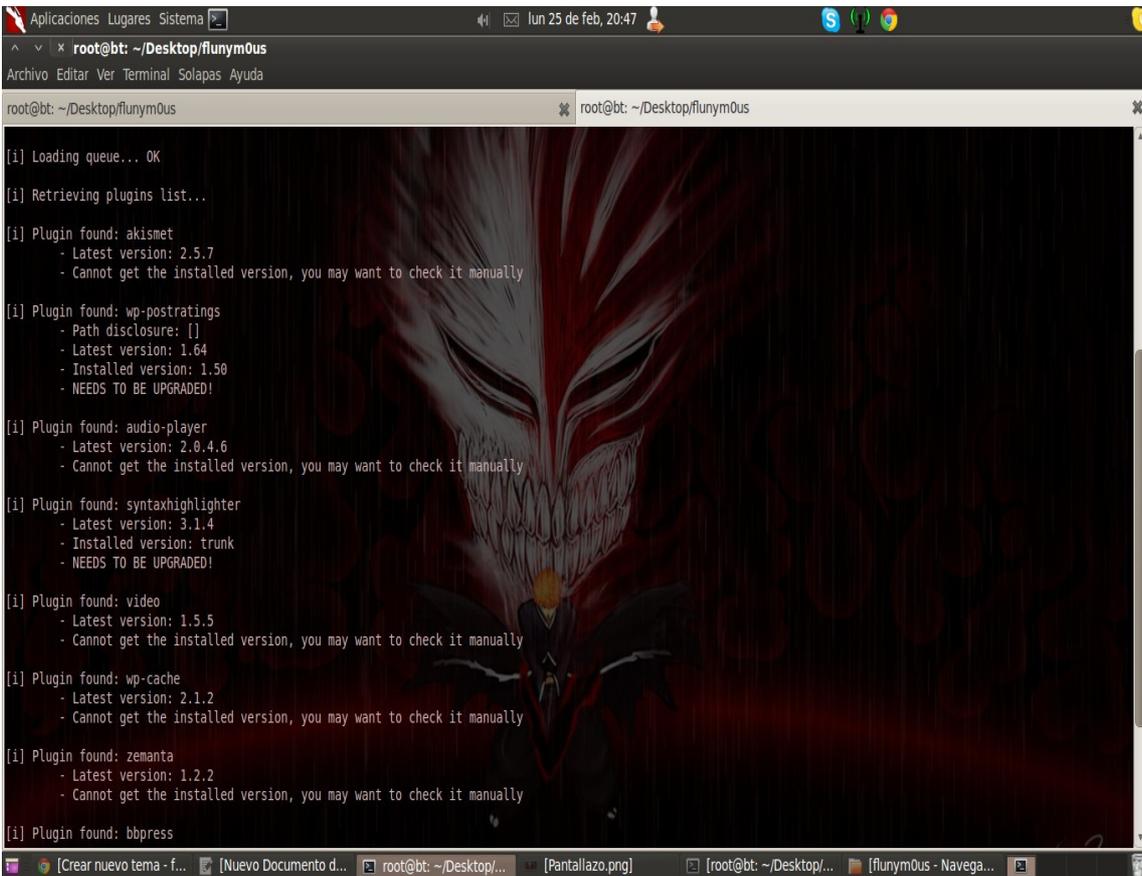
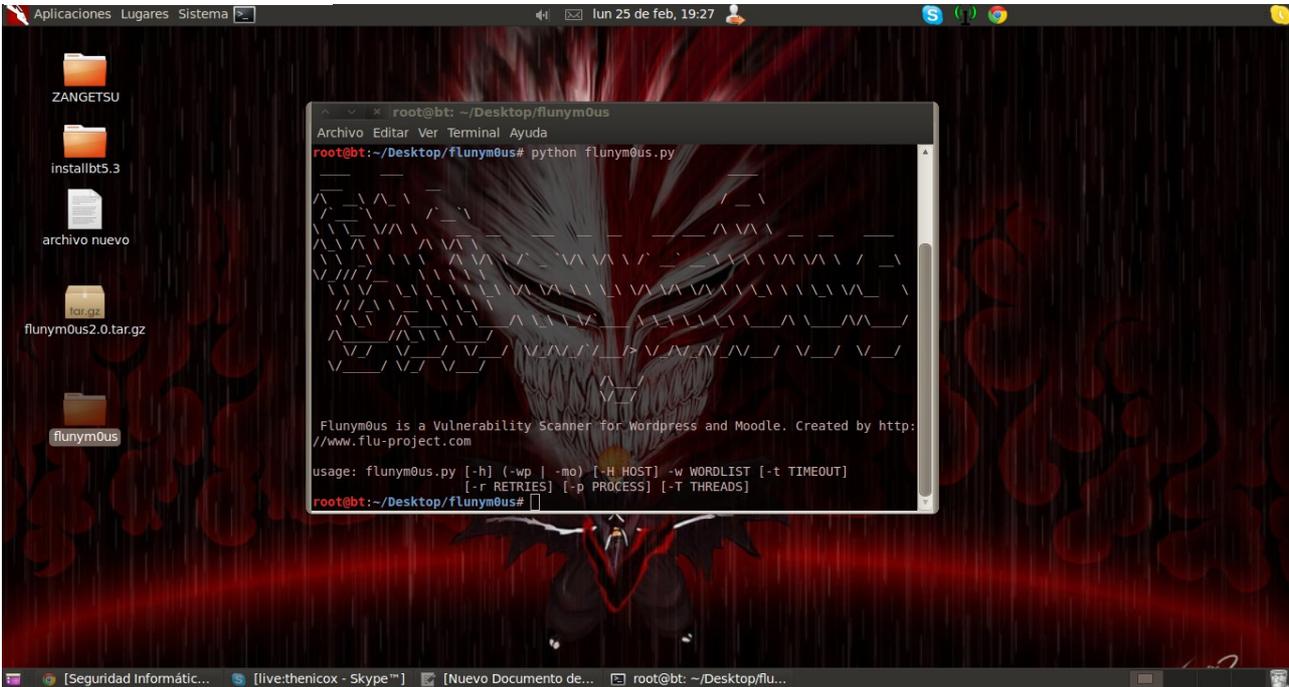
The screenshot shows a Linux desktop with a dark red and black background. A terminal window is open in the center, displaying the following commands and output:

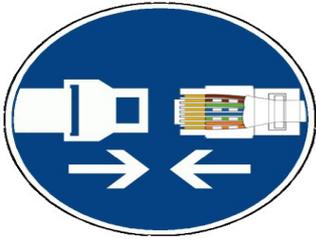
```
root@bt:~# cd Desktop
root@bt:~/Desktop# ls
archivo nuevo  flunym0us2.0.tar.gz  installbt5.3  ZANGETSU
root@bt:~/Desktop# tar -xvf flunym0us2.0.tar.gz
wp-plugins.lst
useragents.lst
useragents.py
moodle-plugins.lst
flunym0us.py
root@bt:~/Desktop#
```

The desktop contains several icons, including folders like 'ZANGETSU' and 'installbt5.3', and files like 'useragents.pyc', 'wp-plugins.lst', 'flunym0us2.0.tar.gz', 'flunym0us.py', 'moodle-plugins.lst', and 'useragents.py'. The terminal window title is 'root@bt: ~/Desktop'.



[www.seguridadpyme.es](http://www.seguridadpyme.es)





[www.seguridaddpyme.es](http://www.seguridaddpyme.es)

```
root@bt: ~/Desktop/flunym0us
[i] Plugin found: wp-postratings
  - Path disclosure: []
  - Latest version: 1.64
  - Installed version: 1.50
  - NEEDS TO BE UPGRADED!

[i] Plugin found: audio-player
  - Latest version: 2.0.4.6
  - Cannot get the installed version, you may want to check it manually

[i] Plugin found: syntaxhighlighter
  - Latest version: 3.1.4
  - Installed version: trunk
  - NEEDS TO BE UPGRADED!

[i] Plugin found: video
  - Latest version: 1.5.5
  - Cannot get the installed version, you may want to check it manually

[i] Plugin found: wp-cache
  - Latest version: 2.1.2
  - Cannot get the installed version, you may want to check it manually

[i] Plugin found: zemanta
  - Latest version: 1.2.2
  - Cannot get the installed version, you may want to check it manually

[i] Plugin found: bbpress
  - Latest version: 2.2.4
  - Installed version: 2.2.4

[i] Plugin found: wp-latex
  - Latest version: 1.7
  - Installed version: 1.7
```

<http://blackkzangetsu.blogspot.com.es/2013/02/flunym0us-20-herramienta-scan.html>