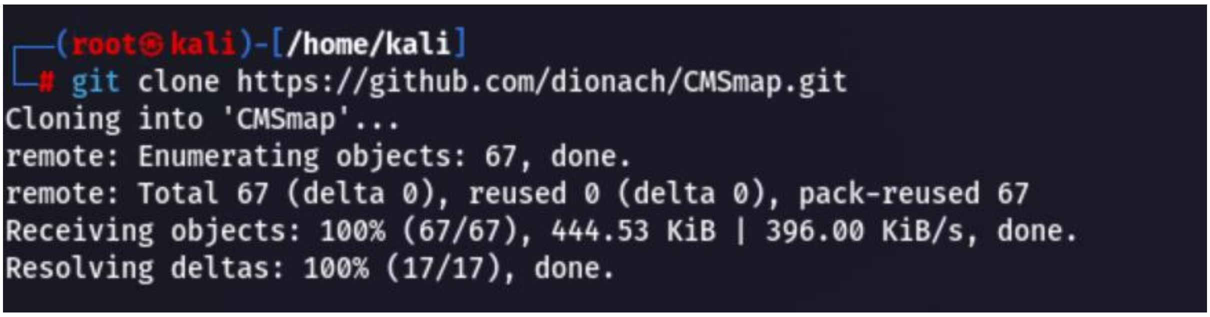
CMSmap

CMSmap is a Python open source CMS scanner that automates the method of detecting security flaws of the foremost popular CMSs. The main purpose of this tool is to integrate common vulnerabilities for different types of CMSs into a single tool. at the instant, there’s support for WordPress, Joomla, Drupal, and Moodle. CMSmap tool is freely available on GitHub. CMSmap tool supports multiple target domain scanning and saves the results in text file format. CMSmap tool has the ability to set custom user-agent and header. CMSmap tool Support for SSL encryption. CMSmap tool supports Verbose mode for debugging purposes.

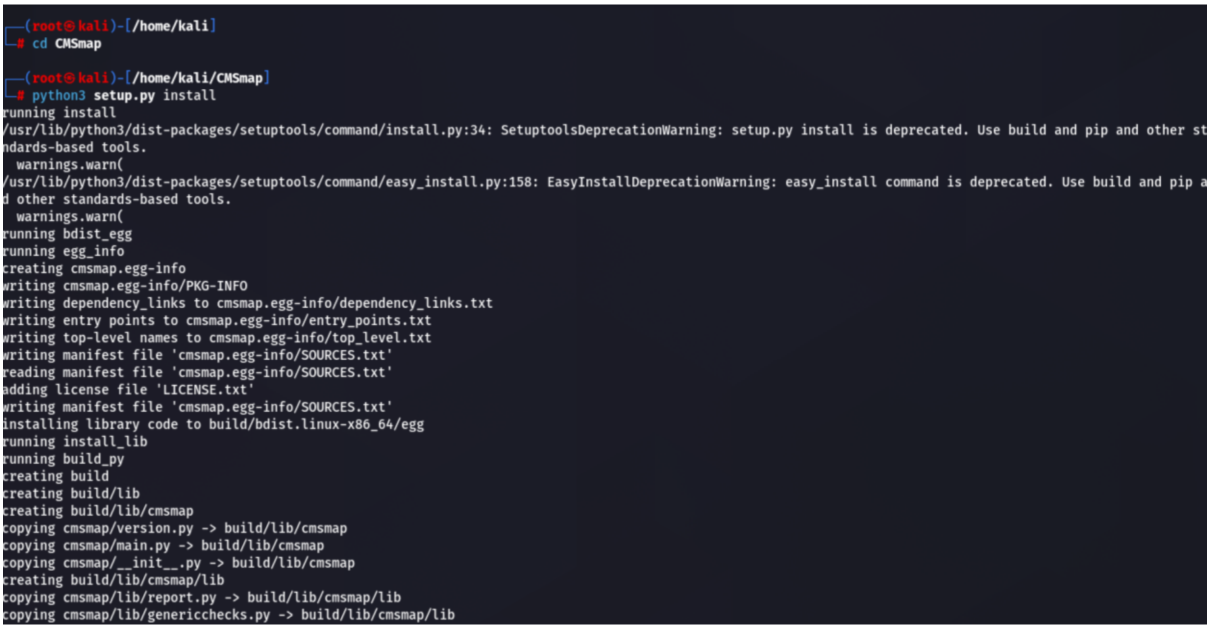
Examples: -

1. We can install CMSmap from its github repository using git clone command.



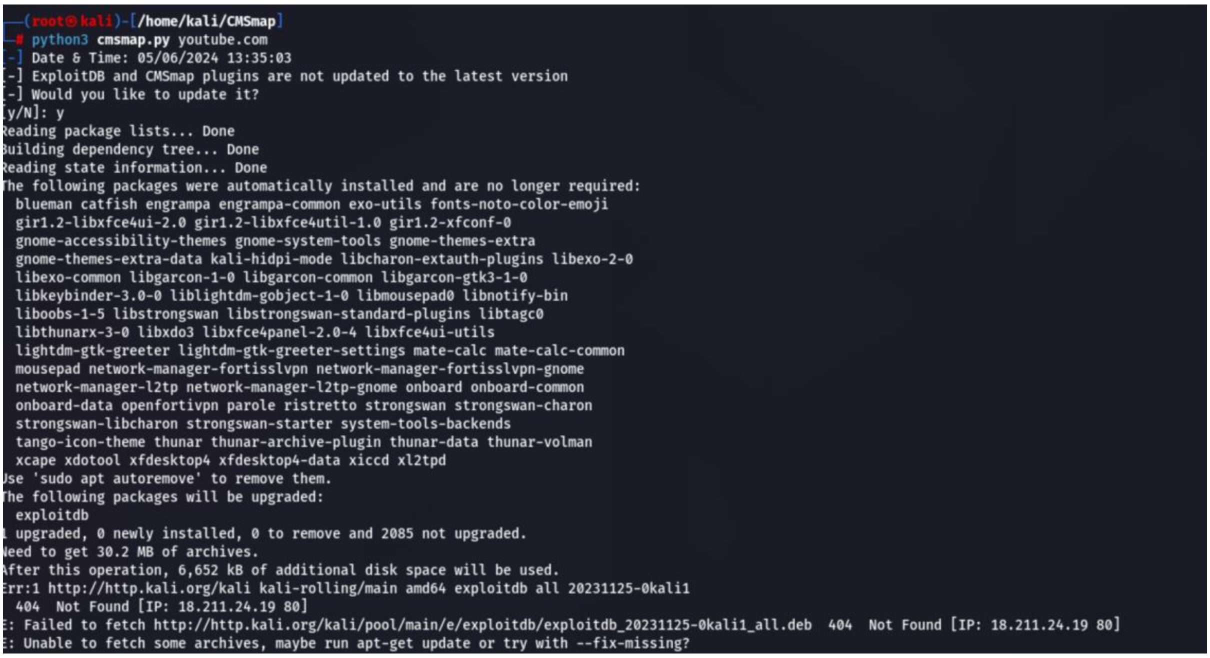
```
┌──(root㉿kali)-[/home/kali]
└─# git clone https://github.com/dionach/CMSmap.git
Cloning into 'CMSmap'...
remote: Enumerating objects: 67, done.
remote: Total 67 (delta 0), reused 0 (delta 0), pack-reused 67
Receiving objects: 100% (67/67), 444.53 KiB | 396.00 KiB/s, done.
Resolving deltas: 100% (17/17), done.
```

2. Now move to the CMSmap directory and install the python file using python3.



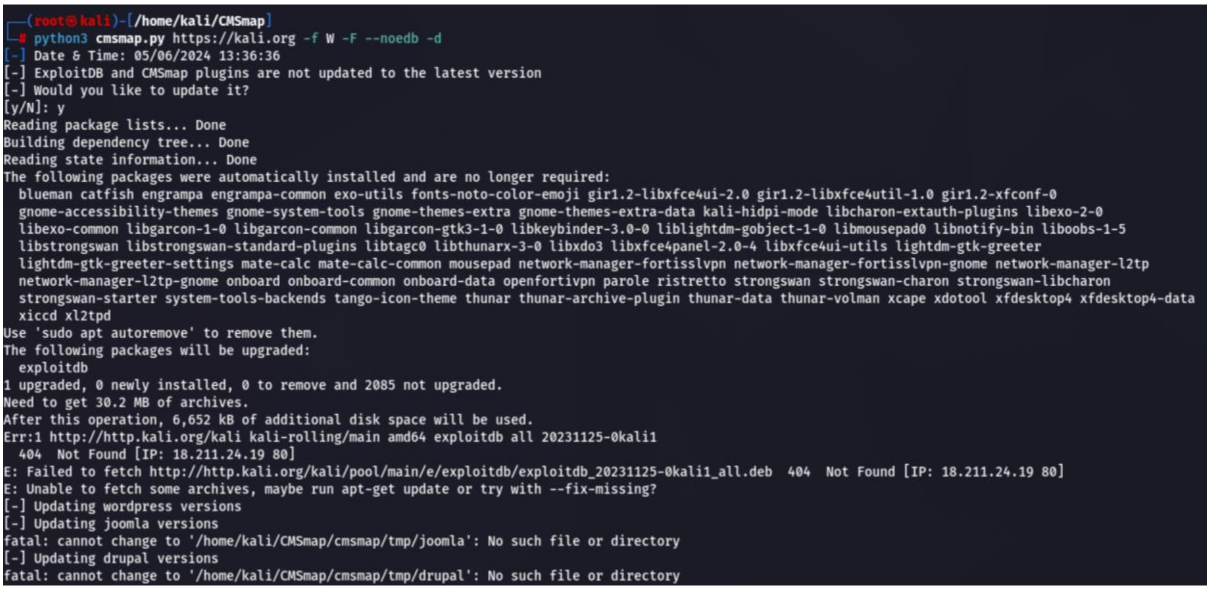
```
┌──(root㉿kali)-[/home/kali]
└─# cd CMSmap

┌──(root㉿kali)-[/home/kali/CMSmap]
└─# python3 setup.py install
running install
/usr/lib/python3/dist-packages/setuptools/command/install.py:34: SetuptoolsDeprecationWarning: setup.py install is deprecated. Use build and pip and other st
ndards-based tools.
  warnings.warn(
/usr/lib/python3/dist-packages/setuptools/command/easy_install.py:158: EasyInstallDeprecationWarning: easy_install command is deprecated. Use build and pip a
d other standards-based tools.
  warnings.warn(
running bdist_egg
running egg_info
creating cmsmap.egg-info
writing cmsmap.egg-info/PKG-INFO
writing dependency_links to cmsmap.egg-info/dependency_links.txt
writing entry points to cmsmap.egg-info/entry_points.txt
writing top-level names to cmsmap.egg-info/top_level.txt
writing manifest file 'cmsmap.egg-info/SOURCES.txt'
reading manifest file 'cmsmap.egg-info/SOURCES.txt'
adding license file 'LICENSE.txt'
writing manifest file 'cmsmap.egg-info/SOURCES.txt'
installing library code to build/bdist.linux-x86_64/egg
running install_lib
running build_py
creating build
creating build/lib
creating build/lib/cmsmap
copying cmsmap/version.py -> build/lib/cmsmap
copying cmsmap/main.py -> build/lib/cmsmap
copying cmsmap/__init__.py -> build/lib/cmsmap
creating build/lib/cmsmap/lib
copying cmsmap/lib/report.py -> build/lib/cmsmap/lib
copying cmsmap/lib/genericchecks.py -> build/lib/cmsmap/lib
```

3. Now use cmnscam.py along with the target website to have a scan.



```
┌──(root㉿kali)-[/home/kali/CMSmap]
└─# python3 cmsmap.py youtube.com
[-] Date & Time: 05/06/2024 13:35:03
[-] ExploitDB and CMSmap plugins are not updated to the latest version
[-] Would you like to update it?
[y/N]: y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  blueman catfish engrampa engrampa-common exo-utils fonts-noto-color-emoji
  gir1.2-libxfce4ui-2.0 gir1.2-libxfce4util-1.0 gir1.2-xfconf-0
  gnome-accessibility-themes gnome-system-tools gnome-themes-extra
  gnome-themes-extra-data kali-hidpi-mode libcharon-extauth-plugins libexo-2-0
  libexo-common libgarcon-1-0 libgarcon-common libgarcon-gtk3-1-0
  libkeybinder-3.0-0 liblightdm-gobject-1-0 libmousepad0 libnotify-bin
  liboobs-1-5 libstrongswan libstrongswan-standard-plugins libtagc0
  libthunarx-3-0 libxdo3 libxfce4panel-2.0-4 libxfce4ui-utils
  lightdm-gtk-greeter lightdm-gtk-greeter-settings mate-calc mate-calc-common
  mousepad network-manager-fortisslvpn network-manager-fortisslvpn-gnome
  network-manager-l2tp network-manager-l2tp-gnome onboard onboard-common
  onboard-data openfortivpn parole ristretto strongswan strongswan-charon
  strongswan-libcharon strongswan-starter system-tools-backends
  tango-icon-theme thunar thunar-archive-plugin thunar-data thunar-volman
  xcape xdotool xfdesktop4 xfdesktop4-data xiccd xl2tpd
Use 'sudo apt autoremove' to remove them.
The following packages will be upgraded:
  exploitdb
1 upgraded, 0 newly installed, 0 to remove and 2085 not upgraded.
Need to get 30.2 MB of archives.
After this operation, 6,652 kB of additional disk space will be used.
Err:1 http://http.kali.org/kali kali-rolling/main amd64 exploitdb all 20231125-0kali1
  404  Not Found [IP: 18.211.24.19 80]
E: Failed to fetch http://http.kali.org/kali/pool/main/e/exploitdb/exploitdb_20231125-0kali1_all.deb  404  Not Found [IP: 18.211.24.19 80]
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?
```

4. Now, we are performing a Force scan of WordPress CMS on our target website.



```
┌──(root㉿kali)-[/home/kali/CMSmap]
└─# python3 cmsmap.py https://kali.org -f W -F --noedb -d
[-] Date & Time: 05/06/2024 13:36:36
[-] ExploitDB and CMSmap plugins are not updated to the latest version
[-] Would you like to update it?
[y/N]: y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  blueman catfish engrampa engrampa-common exo-utils fonts-noto-color-emoji gir1.2-libxfce4ui-2.0 gir1.2-libxfce4util-1.0 gir1.2-xfconf-0
  gnome-accessibility-themes gnome-system-tools gnome-themes-extra gnome-themes-extra-data kali-hidpi-mode libcharon-extauth-plugins libexo-2-0
  libexo-common libgarcon-1-0 libgarcon-common libgarcon-gtk3-1-0 libkeybinder-3.0-0 liblightdm-gobject-1-0 libmousepad0 libnotify-bin liboobs-1-5
  libstrongswan libstrongswan-standard-plugins libtagc0 libthunarx-3-0 libxdo3 libxfce4panel-2.0-4 libxfce4ui-utils lightdm-gtk-greeter
  lightdm-gtk-greeter-settings mate-calc mate-calc-common mousepad network-manager-fortisslvpn network-manager-fortisslvpn-gnome network-manager-l2tp
  network-manager-l2tp-gnome onboard onboard-common onboard-data openfortivpn parole ristretto strongswan strongswan-charon strongswan-libcharon
  strongswan-starter system-tools-backends tango-icon-theme thunar thunar-archive-plugin thunar-data thunar-volman xcape xdotool xfdesktop4 xfdesktop4-data
  xiccd xl2tpd
Use 'sudo apt autoremove' to remove them.
The following packages will be upgraded:
  exploitdb
1 upgraded, 0 newly installed, 0 to remove and 2085 not upgraded.
Need to get 30.2 MB of archives.
After this operation, 6,652 kB of additional disk space will be used.
Err:1 http://http.kali.org/kali kali-rolling/main amd64 exploitdb all 20231125-0kali1
  404  Not Found [IP: 18.211.24.19 80]
E: Failed to fetch http://http.kali.org/kali/pool/main/e/exploitdb/exploitdb_20231125-0kali1_all.deb  404  Not Found [IP: 18.211.24.19 80]
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?
[-] Updating wordpress versions
[-] Updating joomla versions
fatal: cannot change to '/home/kali/CMSmap/cmsmap/tmp/joomla': No such file or directory
[-] Updating drupal versions
fatal: cannot change to '/home/kali/CMSmap/cmsmap/tmp/drupal': No such file or directory
```