SarCTF

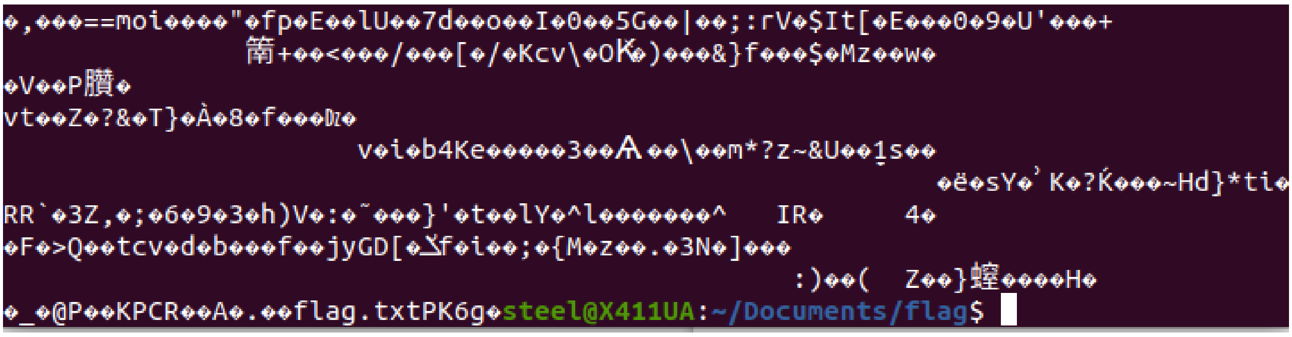
Misc : Deep dive

Description : Worth digging into these tricks.

Attachment : flag.txt

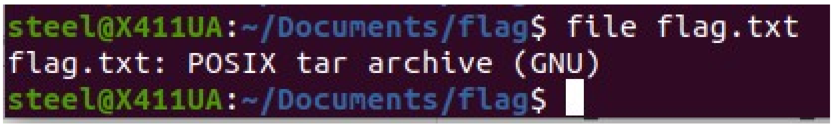
Solution :

A file called *flag.txt* is given for this challenge. We can try to see what it contains.



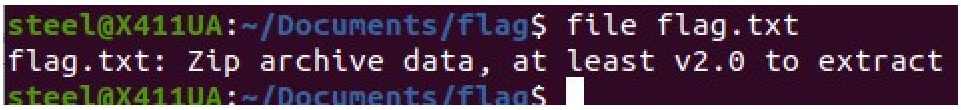
```
�,���==moi����"�fp�E��lU��7d���o��I�0��5G��|��;:rV�$It[�E���0�9�U'���+
                 脯+��<���/���[�/�Kcv\�OK̗�)���&}f���$�Mz��w�
�V��P臢�
vt��Z�?&�T}�À�8�f���Dz�
                         v�i�b4Ke�����3��Ѧ��\��m*?z~&U��1̱s��
                                                               �ë�sY�̓K�?Ḱ���~Hd}*ti�
RR`�3Z,�;�6�9�3�h)V�:�˜���}'�t��lY�^l�������^   IR�     4�
�F�>Q��tcv�d�b���f��jyGD[�ؕf�i��;�{M�z��.�3N�]���
                                                 :)��(  Z��}蝗����H�
�_�@P��KPCR��A�.��flag.txtPK6g�steel@X411UA:~/Documents/flag$ 
```

It doesn’t seem to be a text file. Let’s see what type it is.



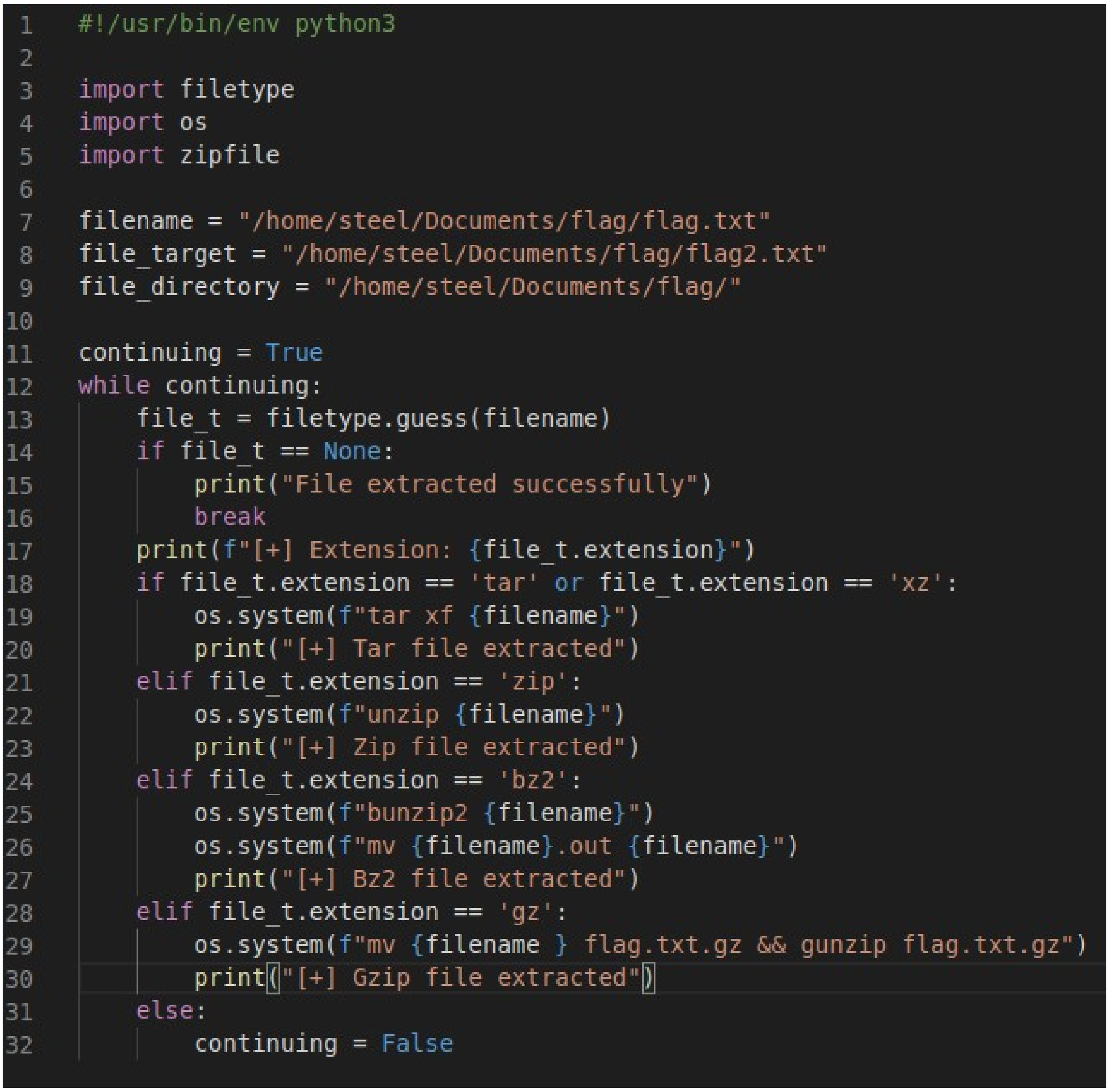
```
steel@X411UA:~/Documents/flag$ file flag.txt
flag.txt: POSIX tar archive (GNU)
steel@X411UA:~/Documents/flag$ 
```

A tar archive. Let’s extract it!
There is a file called a flag.txt in this archive.



```
steel@X411UA:~/Documents/flag$ file flag.txt
flag.txt: Zip archive data, at least v2.0 to extract
steel@X411UA:~/Documents/flag$ 
```

But this file is a zip archive. It seems that the flag has been archived many times.
Let’s program a script to get the flag quickly.



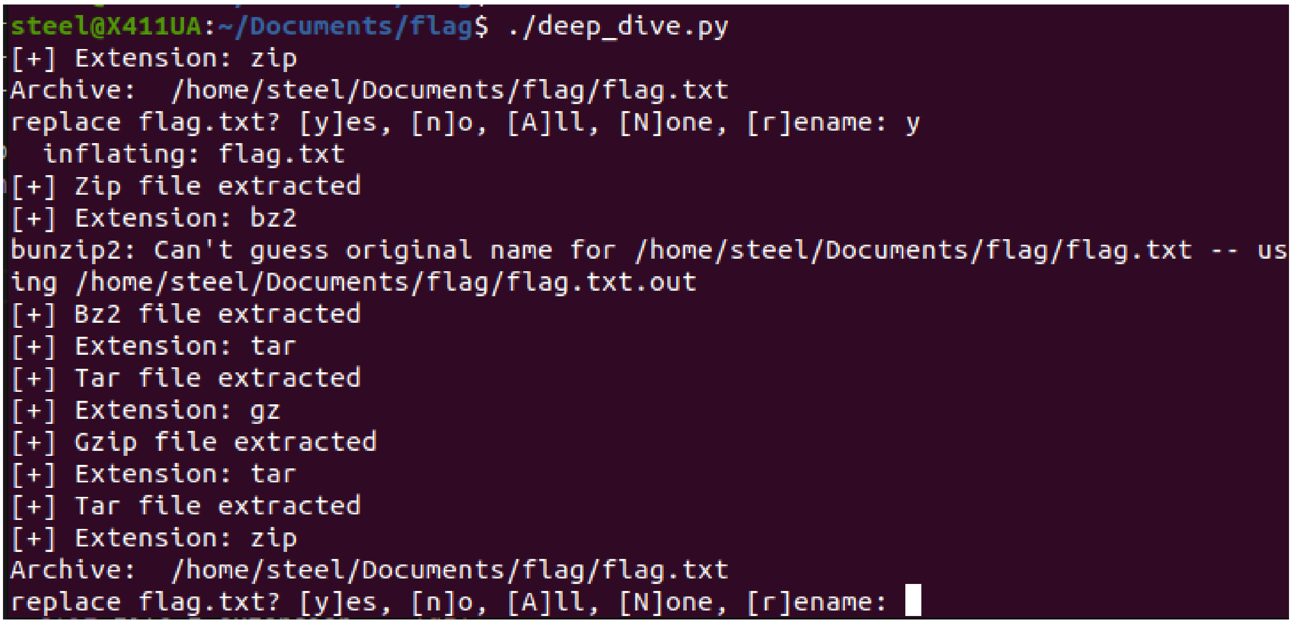
```python
#!/usr/bin/env python3

import filetype
import os
import zipfile

filename = "/home/steel/Documents/flag/flag.txt"
file_target = "/home/steel/Documents/flag/flag2.txt"
file_directory = "/home/steel/Documents/flag/"

continuing = True
while continuing:
    file_t = filetype.guess(filename)
    if file_t == None:
        print("File extracted successfully")
        break
    print(f"[+] Extension: {file_t.extension}")
    if file_t.extension == 'tar' or file_t.extension == 'xz':
        os.system(f"tar xf {filename}")
        print("[+] Tar file extracted")
    elif file_t.extension == 'zip':
        os.system(f"unzip {filename}")
        print("[+] Zip file extracted")
    elif file_t.extension == 'bz2':
        os.system(f"bunzip2 {filename}")
        os.system(f"mv {filename}.out {filename}")
        print("[+] Bz2 file extracted")
    elif file_t.extension == 'gz':
        os.system(f"mv {filename } flag.txt.gz && gunzip flag.txt.gz")
        print("[+] Gzip file extracted")
    else:
        continuing = False
```

For this program to run, you need to install the python module filetype with this command:

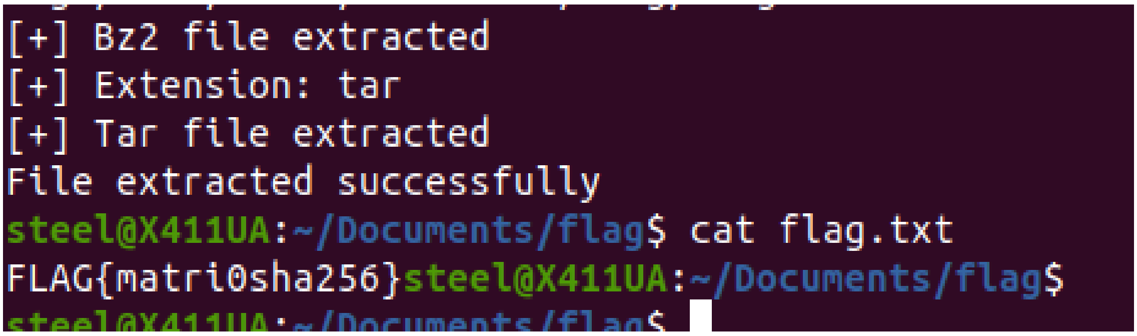
sudo pip3 install filetype

I had some problems with the modules tarfile and zipfiles because the extracted file has the same name as the archive, so I used system calls to perform the operations.

Gunzip extracted files with the name *flag.txt.out*, that’s why I rename it after.



```
steel@X411UA:~/Documents/flag$ ./deep_dive.py
[+] Extension: zip
Archive:  /home/steel/Documents/flag/flag.txt
replace flag.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
  inflating: flag.txt
[+] Zip file extracted
[+] Extension: bz2
bunzip2: Can't guess original name for /home/steel/Documents/flag/flag.txt -- us
ing /home/steel/Documents/flag/flag.txt.out
[+] Bz2 file extracted
[+] Extension: tar
[+] Tar file extracted
[+] Extension: gz
[+] Gzip file extracted
[+] Extension: tar
[+] Tar file extracted
[+] Extension: zip
Archive:  /home/steel/Documents/flag/flag.txt
replace flag.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename:
```



```
[+] Bz2 file extracted
[+] Extension: tar
[+] Tar file extracted
File extracted successfully
steel@X411UA:~/Documents/flag$ cat flag.txt
FLAG{matri0sha256}steel@X411UA:~/Documents/flag$
steel@X411UA:~/Documents/flag$
```

We finally get the flag after many extractions.

FLAG{matri0sha256}