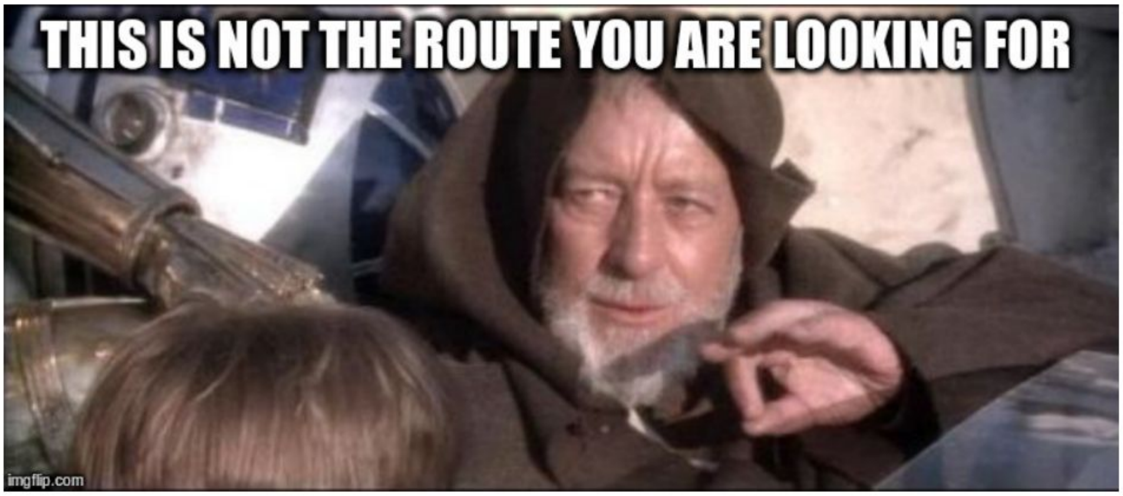
WEB: 50_slash_slash

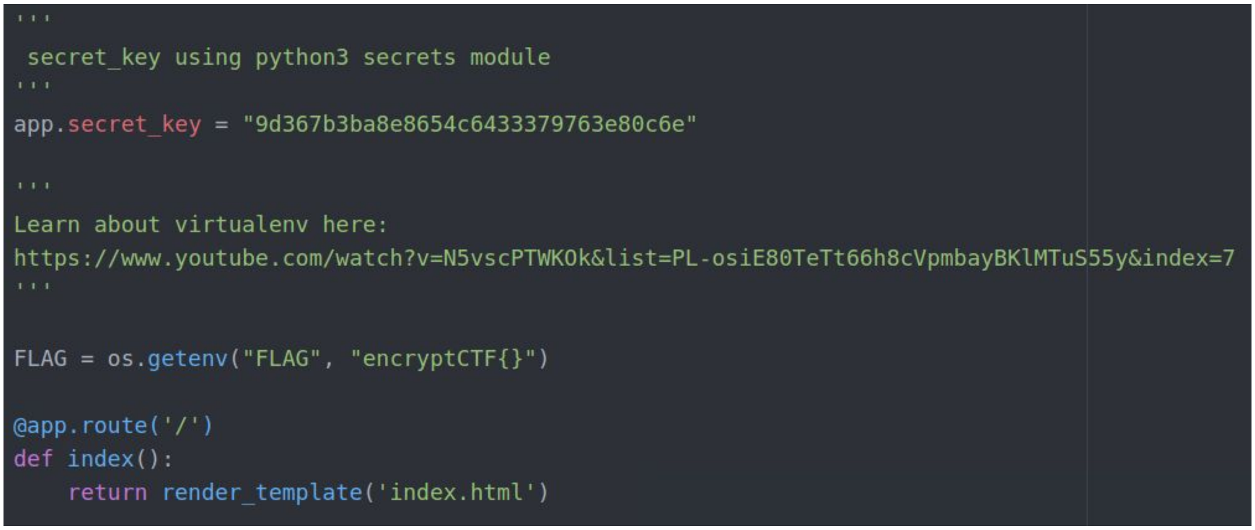
We are given a “7Z” file. The flag is contained inside, thus we need to look at it inside. If we de-compress the folder we obtain a folder called “app”. If we inspect its inside, we can see a file called “application.py”, a Flask application.

We can for example execute it; open a terminal and type:

python application.py



The flag is not here, so we can inspect the python code.



```
'''
 secret_key using python3 secrets module
'''
app.secret_key = "9d367b3ba8e8654c6433379763e80c6e"

'''
Learn about virtualenv here:
https://www.youtube.com/watch?v=N5vscPTWKOk&list=PL-osiE80TeTt66h8cVpmbayBKlMTuS55y&index=7
'''

FLAG = os.getenv("FLAG", "encryptCTF{}")

@app.route('/')
def index():
    return render_template('index.html')
```

It seems that the flag is contained inside a virtual environment called. Let’s go to inspect the activation file of the environment, which is contained at “./env/bin/activate”.

The last line of this file has the following:

export $(echo RkxBRwo= | base64 -d)="ZW5jcnlwdENURntjb21tZW50c18mX2luZGVudGF0aW9uc19tYWtlc19qb2hubnlfYV9nb29kX3Byb2dyYW1tZXJ9Cg==”

We can decrypt the base64 message as following:

Echo "ZW5jcnlwdENURntjb21tZW50c18mX2luZGVudGF0aW9uc19tYWtlc19qb2hubnlfYV9nb29kX3Byb2dyYW1tZXJ9Cg==" | base64 -d

Which gives us the flag:
encryptCTF{comments_&_indentations_makes_johnny_a_good_programmer}