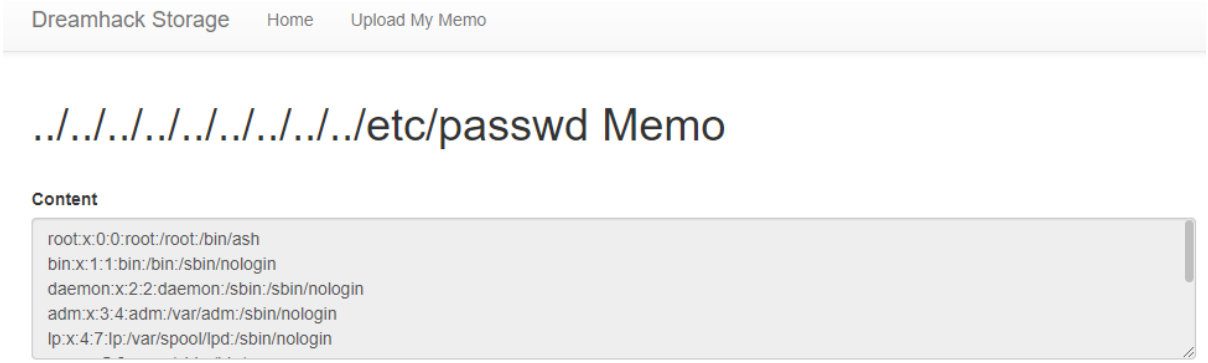
DreamHack file_download-1 문제

2021-09-05

```python
@APP.route('/read')
def read_memo():
    error = False
    data = b''

    filename = request.args.get('name', '')

    try:
        with open(f'{UPLOAD_DIR}/{filename}', 'rb') as f:
            data = f.read()
    except (IsADirectoryError, FileNotFoundError):
        error = True


    return render_template('read.html',
                           filename=filename,
                           content=data.decode('utf-8'),
                           error=error)
```

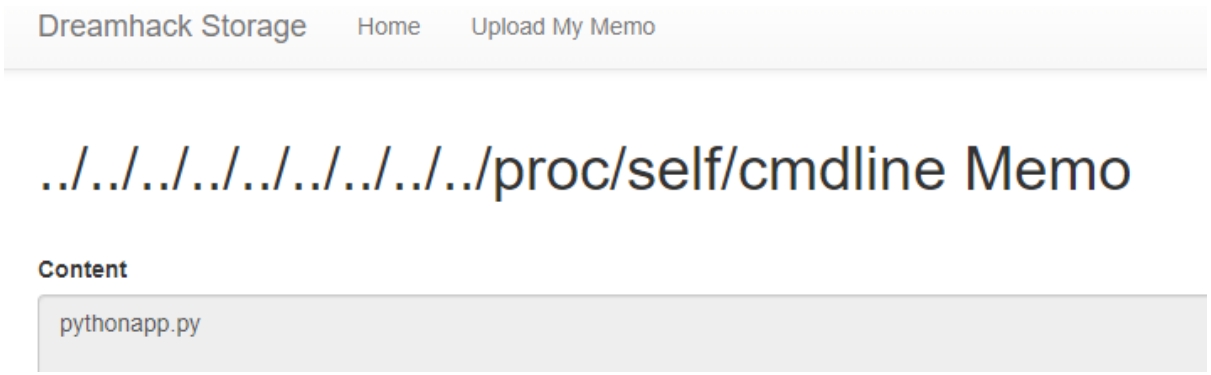
file의 내용을 볼 수 있는 코드가 웹페이지에 포함되어 있는 것을 볼 수 있다. 또한 UPLOAD_DIR과 filename이 다른 처리없이 /로 연결되어 있어 ../를 이용해 상위 DIR에 접근 가능할 것으로 예상된다. 이를 확인하기위해

http://host1.dreamhack.games:9055/read?name=../../../../../../../../etc/passwd로 접속해 /etc/passwd를 확인해보면

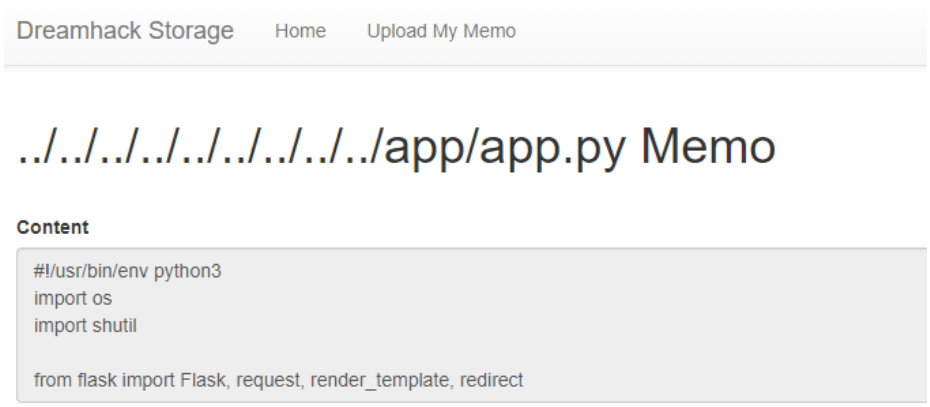


이와 같이 잘 확인이 된다. (../의 개수는 부족하지만 않으면 상관없다.)

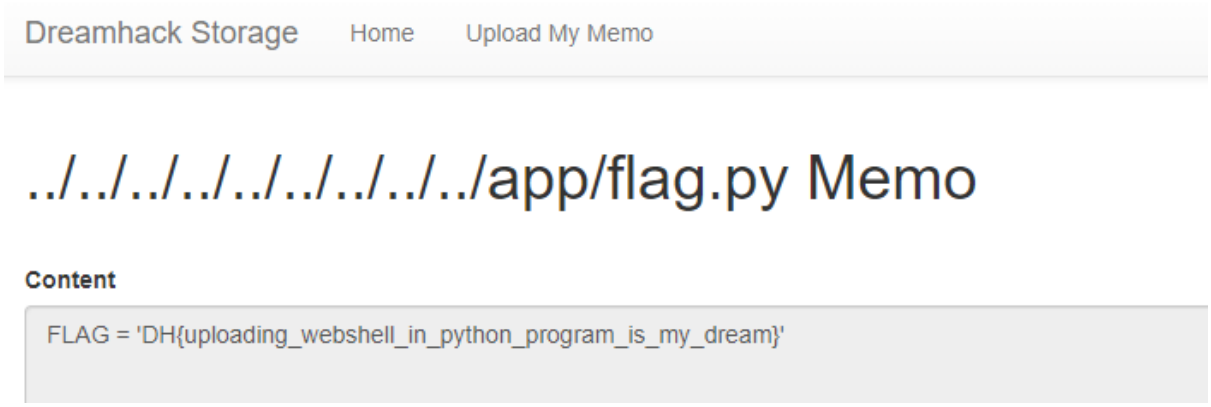
이를 이용해 무슨 프로그램으로 동작되는지 확인하면



pythonapp으로 동작되는 것을 볼 수 있고 파이썬 코드를 보면



이와 같이 볼 수 있다. 이 코드에서 import 하는 flag를 보기위해 flag.py를 확인하면



이와 같이 Flag를 얻을 수 있다.