File-Download-1

접속 정보

Host: host3.dreamhack.games

Port: 8492/tcp

---

nc host3.dreamhack.games 8492

http://host3.dreamhack.games:8492/

문제 파일

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/85d0499c-2030-475a-993c-a85fc3c03875/a09e654b-fd89-4e8c-aa00-5ea6823eca78.zip

문제 풀이

```
#!/usr/bin/env python3
import os
import shutil

from flask import Flask, request, render_template, redirect

from flag import FLAG

APP = Flask(__name__)

UPLOAD_DIR = 'uploads'


@APP.route('/')
def index():
    files = os.listdir(UPLOAD_DIR)
    return render_template('index.html', files=files)
```

```
@APP.route('/upload', methods=['GET', 'POST'])
def upload_memo():
    if request.method == 'POST':
        filename = request.form.get('filename')
        content = request.form.get('content').encode('utf-8')

        if filename.find('..') != -1:
            return render_template('upload_result.html', data='bad characters,,')

        with open(f'{UPLOAD_DIR}/{filename}', 'wb') as f:
            f.write(content)

        return redirect('/')

    return render_template('upload.html')


@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)


if __name__ == '__main__':
    if os.path.exists(UPLOAD_DIR):
        shutil.rmtree(UPLOAD_DIR)

    os.mkdir(UPLOAD_DIR)

    APP.run(host='0.0.0.0', port=8000)
```

```
@APP.route('/upload', methods=['GET', 'POST'])
def upload_memo():
    if request.method == 'POST':
        filename = request.form.get('filename')
        content = request.form.get('content').encode('utf-8')
```

```
        if filename.find('..') != -1:
            return render_template('upload_result.html', data='bad characters,,')

        with open(f'{UPLOAD_DIR}/{filename}', 'wb') as f:
            f.write(content)

        return redirect('/')

    return render_template('upload.html')
```

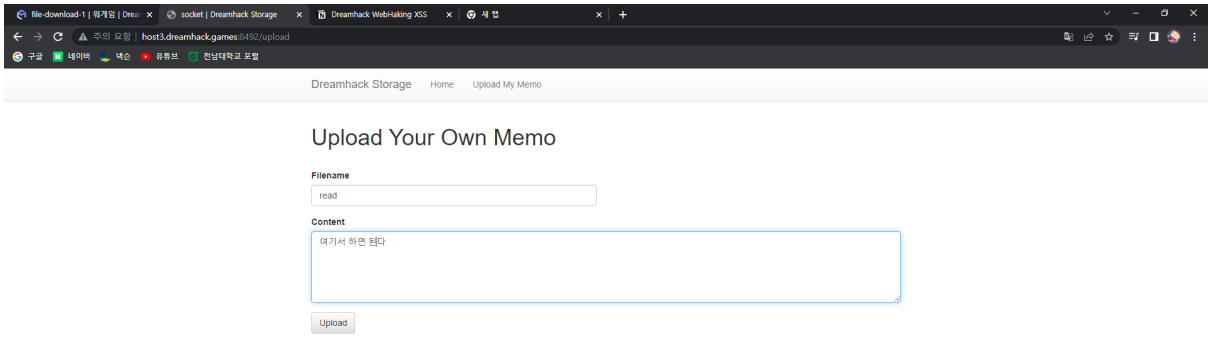
위는 upload 페이지 부분의 코드이다. 중간에 filenamed을 받는 코드를 보자

```
 if filename.find('..') != -1:
            return render_template('upload_result.html', data='bad characters,,')
```

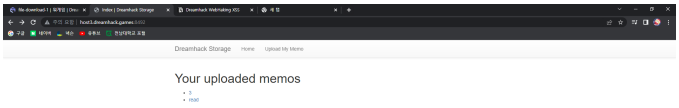
이 명령어 때문에 filename에 ../plag.py 입력하면 ..필터링이 되기 때문에 오류가 난다.

```
@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)
```

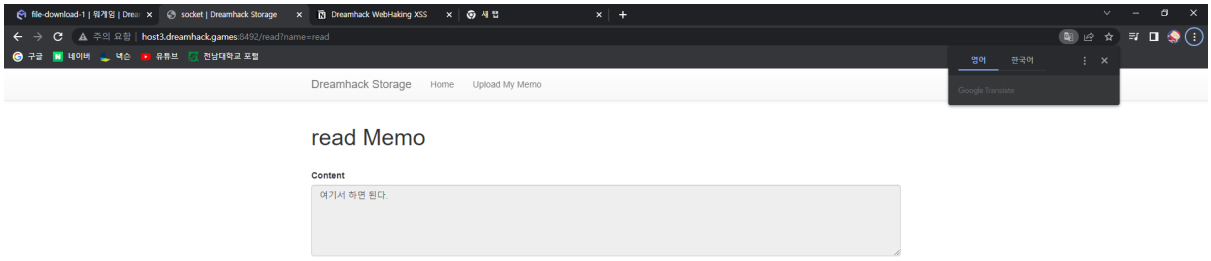
하지만 올려본 파일을 읽을 수 있는 페이지인 /read 페이지에는 이런 우회가 없는 것을 확인할 수 있다.



이를 이용해서 임의의 파일을 하나 업로드 해준다.



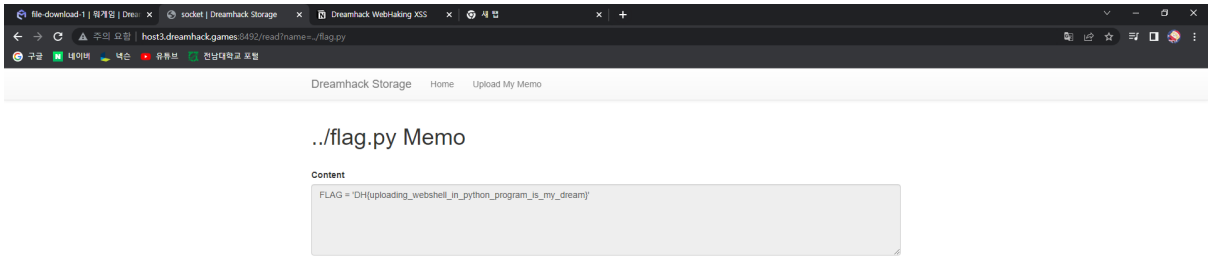
방금 써준 임의의 파일은 read에 들어가준다.



성공적으로 /read 페이지로 들어왔다.

/read 페이지에는 따로 우회가 없으므로 URL을 이용해서 flag.py를 실행해주면 된다.

read?name=read 를 read?name=../flag.py로 바꿔주고 f5를 통해서 새로고침을 하게되면



위와 같이 flag값이 나오게 된다.