

YBG_CTF2

디렉토리 트레버설 문제

문제 풀이

YBG Storage

Upload Your Own Memo

Filename

example.txt

Content

Write your memo here...

Upload

/upload 화면이다. 크게 특별한 점은 없어 보이고, 메모를 업로드하여 전체적인 로직을 확인해 보자.

/upload

문제 풀이

Upload Your Own Memo

Filename

hi

Content

.

Upload

/upload

Uploaded Memos

hi

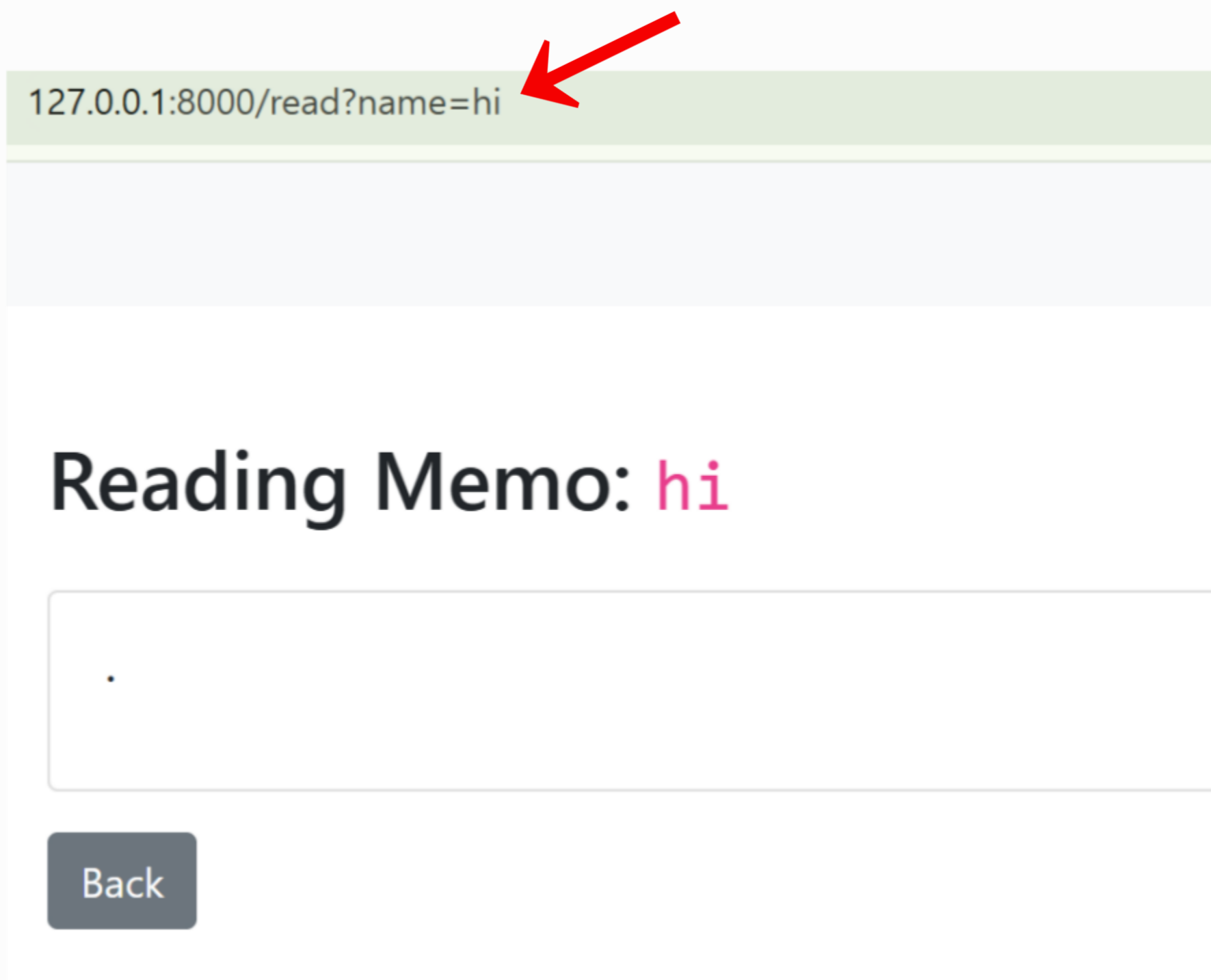
Read

/

'hi'라는 메모를 업로드하면, /에 업로드된
메모 목록이 뜨게 된다.

Read를 눌러 읽어 보자.

문제 풀이



메모를 업로드했을 때,
url에서 파일 이름이 파라미터로 전달되고 있다는
사실을 알 수 있다.

이런 구조라면 상대 경로 조작(../)을 시도해 볼 수
있을 것으로 보인다.

/read?name=

문제 풀이

Upload Result

Invalid filename.

[Back to Home](#)

'../flag.txt'를 제목으로 하여
메모를 생성하려고 했지만,
Invalid filename이라며 막혀 있다.

그렇다면 url을 이용해 보자.

/upload

문제 풀이



`/read?name=../../flag.txt`를 입력해 보자.

문제 풀이

127.0.0.1:8000/read?name=.././flag.txt

Reading Memo: `.././flag.txt`

YBG{download_path_escape}

Back

플래그를 구할 수 있었다.

/read?name=.././flag.txt