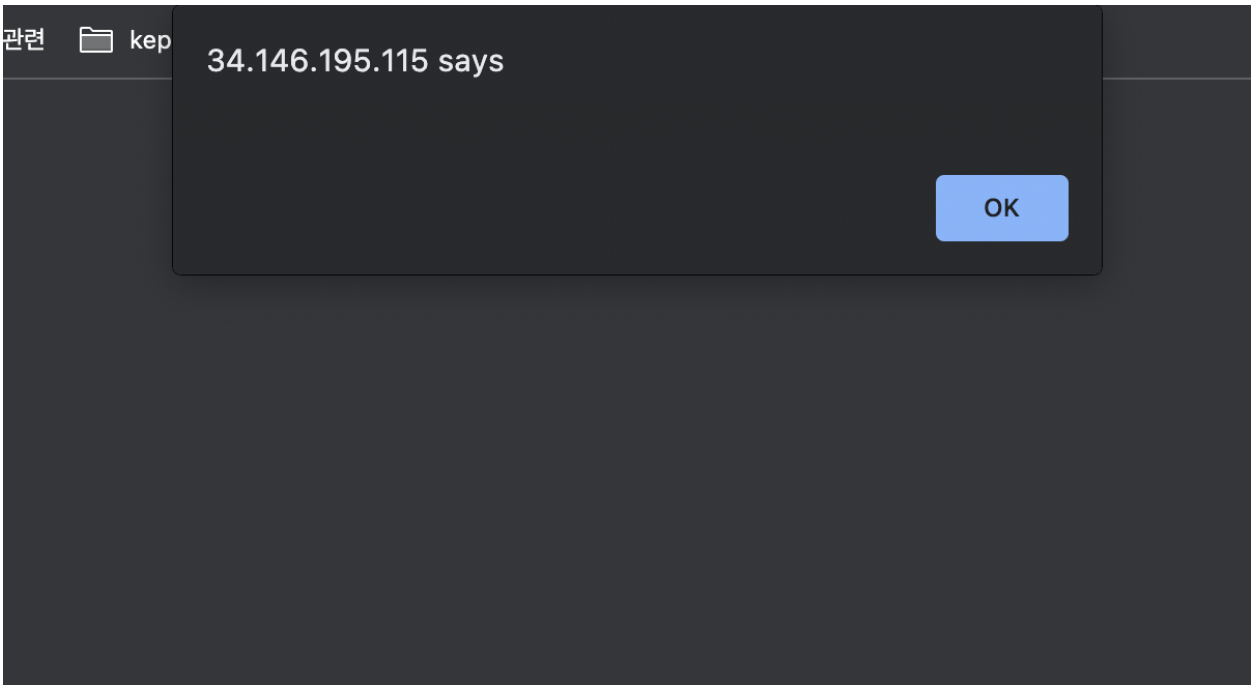
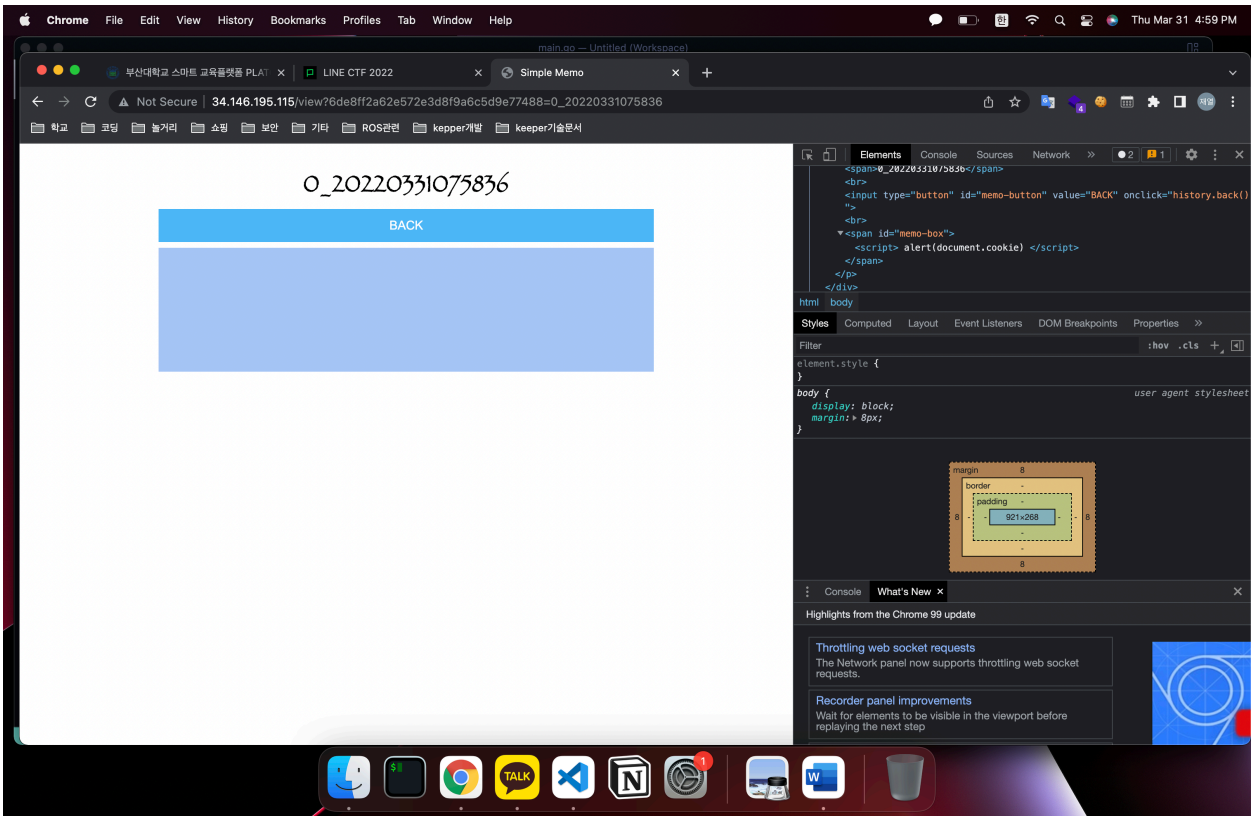
[Line CTF] Memo Drive

초기 접속 화면이다 소스코드에 jinja2 가 import 되어 있길래 ssti 인가 싶어서 {{ 7*7 }}을 삽입했는데 아무런 반응이 없었다.
그래서 xss 인가 싶어서 <script> alert(document.cookie) </script>를 입력해봤다.



이렇게 알림이 뜨고 스크립트 태그도 정상적으로 삽입이 된 것을 확인할 수 있었다.



입력값에 별다른 필터링이 없기 때문에 html 태그는 전부 삽입이 가능했고 이를 활용해서 파일 저장 위치 기준으로 ../flag 를 읽으면 되겠다고 생각했지만 이를 읽을 방법을 찾지 못해서 결국 풀지는 못 했다.