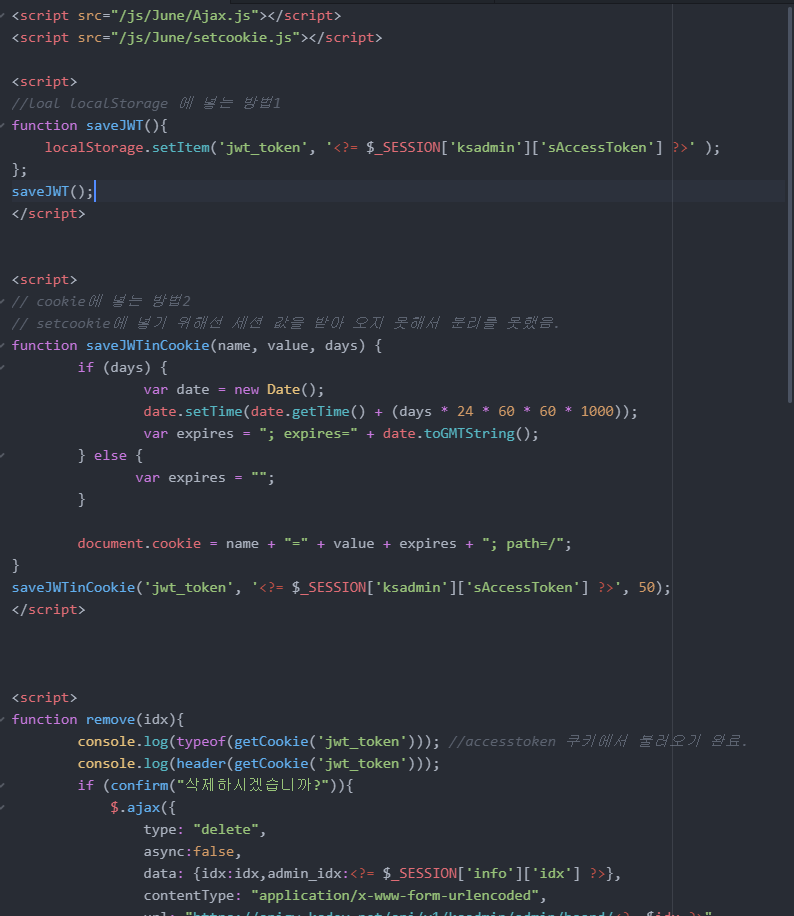
2021.08.04 수요일 \_ 업무내용(정준호)

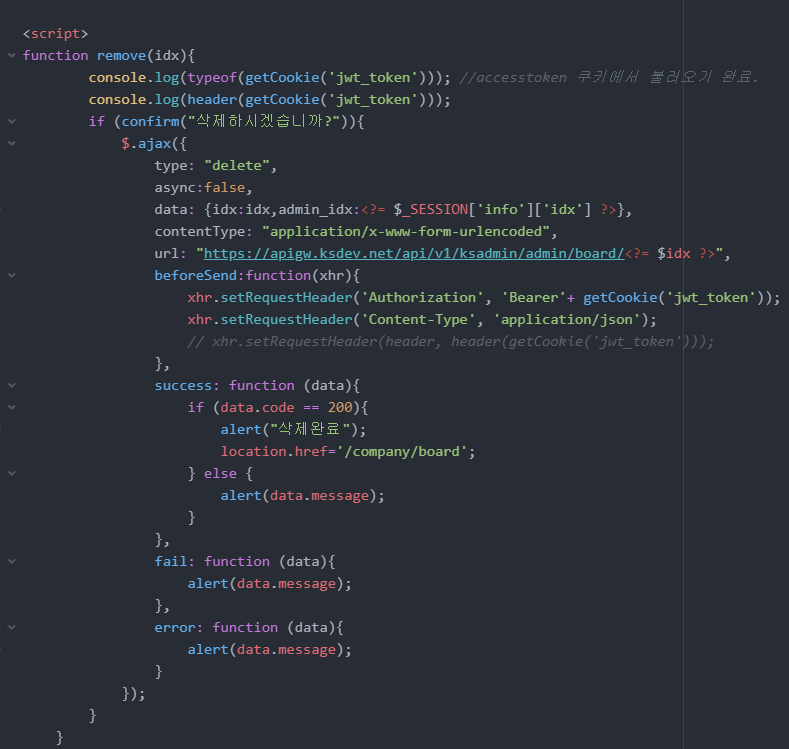
JWT token을 보호하는 방법 각각 개발 진행

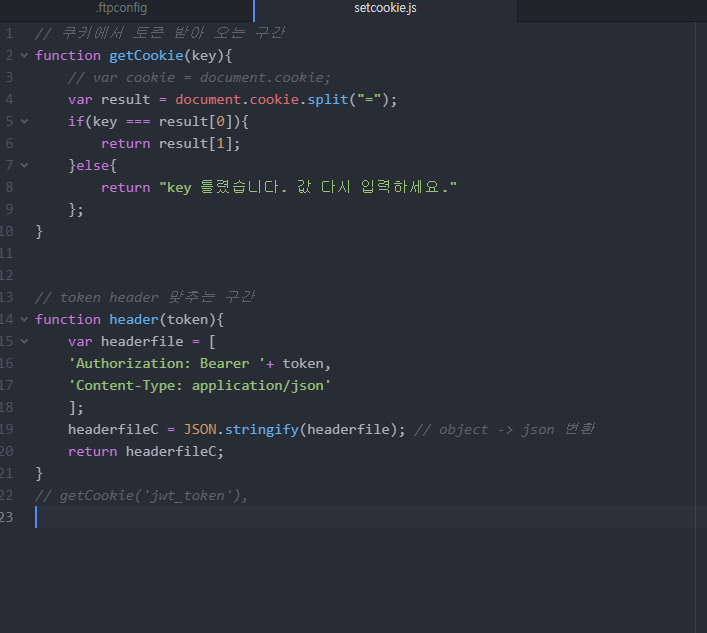
1. Local storage
2. Memory
3. **Cookie**



쿠키를 잘 들고 오고 있는 것을 볼 수 있음.

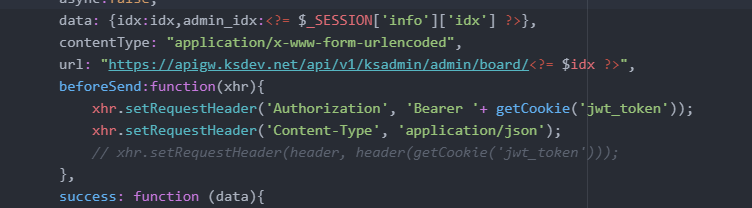






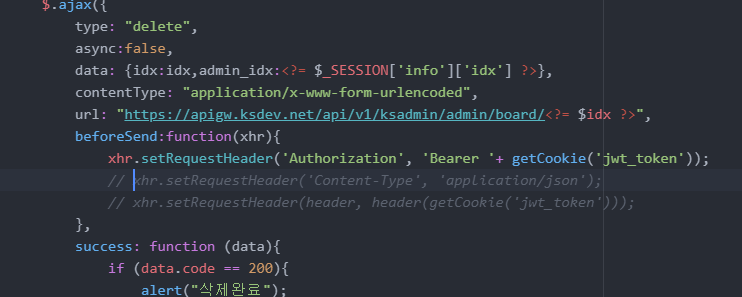
토큰의 정보를 cookie에 숨겨서 전달하기 위해서, public 하위 js에 getcookie와 header 부분을 설계한 후, ajax 안에 beforehand key, value에 함수호출로 access를 처리하였음.

헤더는 key : value 형태로 되어 있기 때문에,



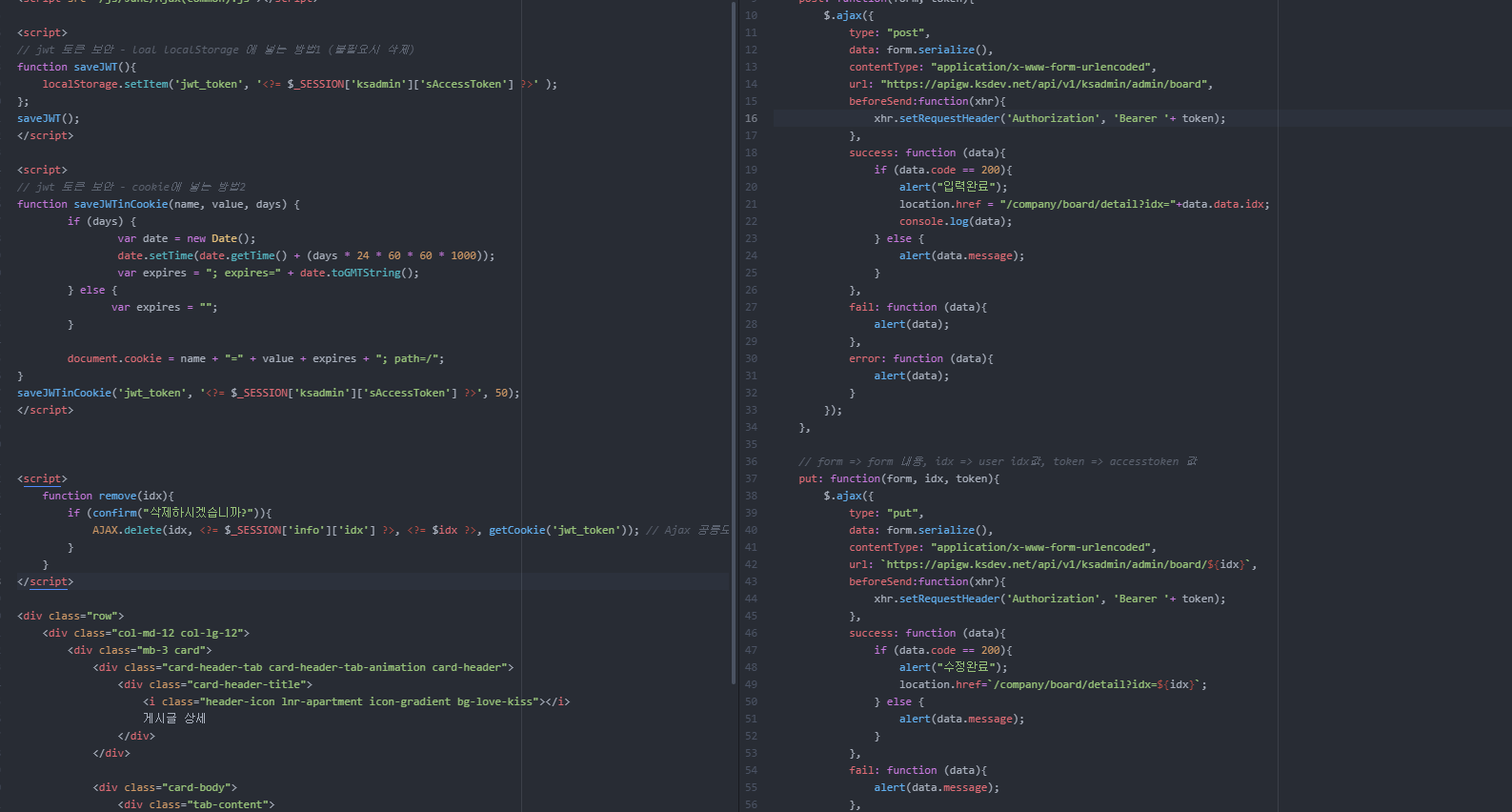
이와 같이 헤더를 보내서 미리 api access를 하는 beforeSend 부분에 key, value를 넣었음.

하지만 이후에 접근권한 제어 에러가 발생했다. 그 이유는 form을 data로 변경하는 과정에서 데이터 포멧이 x-www-form-urlencoded라는 것을 알 수 있는데, 이를 header에서 다시 contentType을 application/json으로 변환해줘서 에러가 발생하는 것.



이렇게 하면 문제 없이 api 호출이 실행됨.

각 페이지 별 인증을 설계한 후, ajax 공통 모듈 설계 진행.



공통 모듈 분리완료. -> refresh token 재발급 logic 설계 및, url, param, call back 함수 설계

이전에 httponly 를 cookie에 삽입하려고 하였으나, 이것은 서버 헤더에 넣어야 한다.

