JWT

Created	@January 18, 2024 9:41 AM
Tags	

- JWT 특징
  - 헤더+페이로드+시그니처 구조
    - 헤더 : 알고리즘 타입
    - 페이로드 : 데이터(노출되는 정보 담으면x)
    - 시그니처 : 검증
  - base64 형태로 암호화되어 있음, 공백x : 중간에 암호화
- 페이로드 = Claim
  - 등록된 클레임 : iss, iat, exp, sub, aud, nbf, jti, …
    - 구현해야 하는 부분
  - 공개 클레임 : uri 형태로 충돌 방지
  - 비공개 클레임 : 클라이언트와 서버 간 합의 하에 사용되는 이름들
- 사용 이유
  - self-contained : 스스로 인증에 필요한 데이터 가짐
  - stateless : 세션과 다르게 백엔드 서버 바뀌어도 인증 가능
  - 모바일 환경에서 다시 로그인할 필요 없음
- Stateless 장점
  - scale out 해도 대응 가능
    - scale up : 서버의 사양 업그레이드 O 서버 증축X
    - scale out : 요청을 여러 서버에 분산 처리
      - 안전성
      - 비용 적음

        - 무중단 서비스 제공 가능
    - 비번 다시 입력할 필요x
    - validation check만으로 검증 가능
        - 한데 white list 방식으로 추가 검증하는 경우도 있음
- Access toekn, Refresh token 사용
    - 액세스 토큰은 짧게, 리프레시 토큰은 긴 생명주기 가짐
    - 서버 요청할 때는 액세스 토큰 사용, 만료되면 리프레시 토큰 이용하여 새로운 액세스 토큰 가져옴
    - 액세스 토큰 탈취 당하기 전에 SSL을 이용한 암호화 통신 사용
    - 보안이 중요하면 redis 이용하기도
- 보안 공격
    - XSS : 링크 클릭
    - CSRF :
- jwt 저장 방식
    - 로컬 스토리지
        - JS 내에 글로번 변수로 읽고 쓰기, XSS방식에 취약
    - 쿠키 저장
        - 리프레쉬토큰을 secure httpOnly쿠키로, 액세스 토큰은 JSON payload로 받아와서 웹 어플리케이션 내 로컬 변수로 이용
        - withCredential
- Access/Refresh Token 검사
    - 재발급