06 /
JSON Web Token

JWT란?
JWT 구조
JWT 장단점

06 / JSON Web Token - JWT란?

JSON 객체로 안전하게 데이터를 전송하기 위한 표준(RFC 7519)입니다.

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJodHRwczovL2Jlb215LmdpdGh1Yi5pby9pZCI6ImJFb015IiwiZW1haWwiOiJhQGEuYSIsImlhdCI6MTYwNTEzODc4
OCwiZXhwIjoxNjA1MjI1MTg4fQ.
bND3EEVyqyU2TeLy8zD0rImYc-R9X5_HjajK7PqMIj0

- JSON 객체를 Base64로 인코딩 한 토큰입니다.
- Base64로 인코딩 된 토큰이기 때문에 Base64로 디코딩해 토큰에 담긴 값을 확인 할 수 있습니다.
- JWT 공식 홈페이지에서 JWT 토큰을 디코딩해 보실 수 있습니다.

06 / JSON Web Token - JWT 구조

JWT는 . 으로 구분된 헤더(Header), 내용(Payload), 서명(Signature) 3부분으로 나눠집니다.

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJodHRwczovL2Jlb215LmdpdGh1Yi5pby9pZCI6ImJFb015IiwiZW1haWwiOiJhQGEuYSIsImlhdCI6MTYwNTEzODc4
OCwiZXhwIjoxNjA1MjI1MTg4fQ.
bND3EEVyqyU2TeLy8zD0rImYc-R9X5_HjajK7PqMIj0

헤더(Header) - eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9

Base64 디코딩

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

alg: HMAC, SHA256, RSA 등 사용한 서명 알고리즘

typ: 토큰 타입

내용(Payload) -

eyJodHRwczovL2Jlb215LmdpdGh1Yi5pby9pZCI6ImJFb015IiwiZW1haWwiOiJhQGEuYSIsImlhdCI6MTYwNTEzODc4OCwiZXhwIjoxNjA1MjI1MTg4fQ

Base64 디코딩

{

"https://beomy.github.io/id": "bEoMy",	공개 클레임
"email": "a@a.a",	비공개 클레임
"iat": 1605138788,	지정된 클레임
"exp": 1605225188	지정된 클레임

}

클레임의 종류

1. 지정된 클레임(registered claim)
2. 공개 클레임(public claim)
3. 비공개 클레임(private claim)

내용(Payload) -

eyJodHRwczovL2Jlb215LmdpdGh1Yi5pby9pZCI6ImJFb015IiwiZW1haWwiOiJhQGEuYSIsImlhdCI6MTYwNTEzODc4OCwiZXhwIjoxNjA1MjI1MTg4fQ

Base64 디코딩

```
{
  "https://beomy.github.io/id": "bEoMy",    공개 클레임
  "email": "a@a.a",                         비공개 클레임
  "iat": 1605138788,                        등록된 클레임
  "exp": 1605225188                         등록된 클레임
}
```

등록된 클레임(registered claim)

토큰에 대한 정보를 담기 위해 이미 정해진 클레임입니다.

- iss: 토큰 발급자
- sub: 토큰 제목
- aud: 토큰 대상자
- exp: 토큰 만료시간
- nbf: Not Before, 이 시간 이전에는 토큰을 처리 하지 않아야 합니다.
- iat: 토큰 발급시간
- jti: JWT 고유식별자

내용(Payload) -

eyJodHRwczovL2Jlb215LmdpdGh1Yi5pby9pZCI6ImJFb015IiwiZW1haWwiOiJhQGEuYSIsImlhdCI6MTYwNTEzODc4OCwiZXhwIjoxNjA1MjI1MTg4fQ

Base64 디코딩

```
{
  "https://beomy.github.io/id": "bEoMy",    공개 클레임
  "email": "a@a.a",                         비공개 클레임
  "iat": 1605138788,                        등록된 클레임
  "exp": 1605225188                         등록된 클레임
}
```

공개 클레임(public claim)

JWT 사용자들 간에 공개된 정보입니다.

IANA JSON Web Token Registry에 정의 되어 있지만,

이 곳에 정의 되어 있지 않다면, 클레임 이름 중복 방지를

위해 URI 형태로 작성해 줘야 합니다.

내용(Payload) -

eyJodHRwczovL2Jlb215LmdpdGh1Yi5pby9pZCI6ImJFb015IiwiZW1haWwiOiJhQGEuYSIsImlhdCI6MTYwNTEzODc4OCwiZXhwIjoxNjA1MjI1MTg4fQ

Base64 디코딩

```
{
"https://beomy.github.io/id": "bEoMy",    공개 클레임
"email": "a@a.a",                         비공개 클레임
"iat": 1605138788,                        등록된 클레임
"exp": 1605225188                         등록된 클레임
}
```

비공개 클레임(private claim):

등록된 클레임과 공개 클레임을 제외한 클레임입니다.

당사자 간(클라이언트 <-> 서버)의 약속된 사용자 지정 클레임입니다.

서명(Signature) - bND3EEVyqyU2TeLy8zD0rImYc-R9X5_HjajK7PqMIj0

슈도코드(pseudocode)

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  secret
)
```

인코딩 된 Header와 인코딩 된 Payload, 시크릿 키를 Header의 alg에 저장된 알고리즘을 사용해서 암호화 해서 만듭니다.

서명은 토큰이 위조되었는지 확인하는데 사용됩니다.

장점

- Stateless (무상태)이기 때문에 서버 확장성이 높습니다.
- 쿠키를 사용하지 않아, 쿠키 사용으로 발생하는 보안 취약점이 없습니다.
- 토큰만 유효하다면 요청이 정상적으로 처리되기 때문에 어떤 디바이스를 사용하던 상관없습니다.

단점

- 토큰에 담는 정보가 많아 질 수록 토큰의 길이가 길어집니다.
- 토큰이 거의 모든 요청에 포함되기 때문에 트레픽이 증가 할 수 있습니다.
- 정해진 토큰의 기간 동안 서버에서 제어가 불가능합니다.

JWT 사용시 주의 사항

- Payload는 암호화 되지 않고 Base64로 인코딩 한 데이터이기 때문에 Payload에 민감한 정보를 저장하는 것은 피해야 합니다.

THANK YOU