Fast campus Copyright FASTCAMPUS Corp.All Rights Reserved

프론트 엔드 개발자가 알아야 하는 컴퓨터 공학 지식
웹(Web)

웹(Web) | 프론드 엔드 개발자가 알아야 하는 CS 지식

강사 나동빈

fast campus Copyright FASTCAMPUS Corp.All Rights Reserved

프론트 엔드 개발자가 알아야 하는 컴퓨터 공학 지식

웹(Web)

fast campus Copyright FASTCAMPUS Corp.All Rights Reserved

JSON 형식(Format)

컴퓨터
공학 지식
웹(Web)

- JSON(JavaScript Object Notation)은 데이터를 주고받기 위해 사용하는 경량의 데이터 형식(format) 중 하나다.
- JSON 형식에서는 키(key)와 값(value)의 쌍으로 이루어진 데이터 객체를 사용한다.

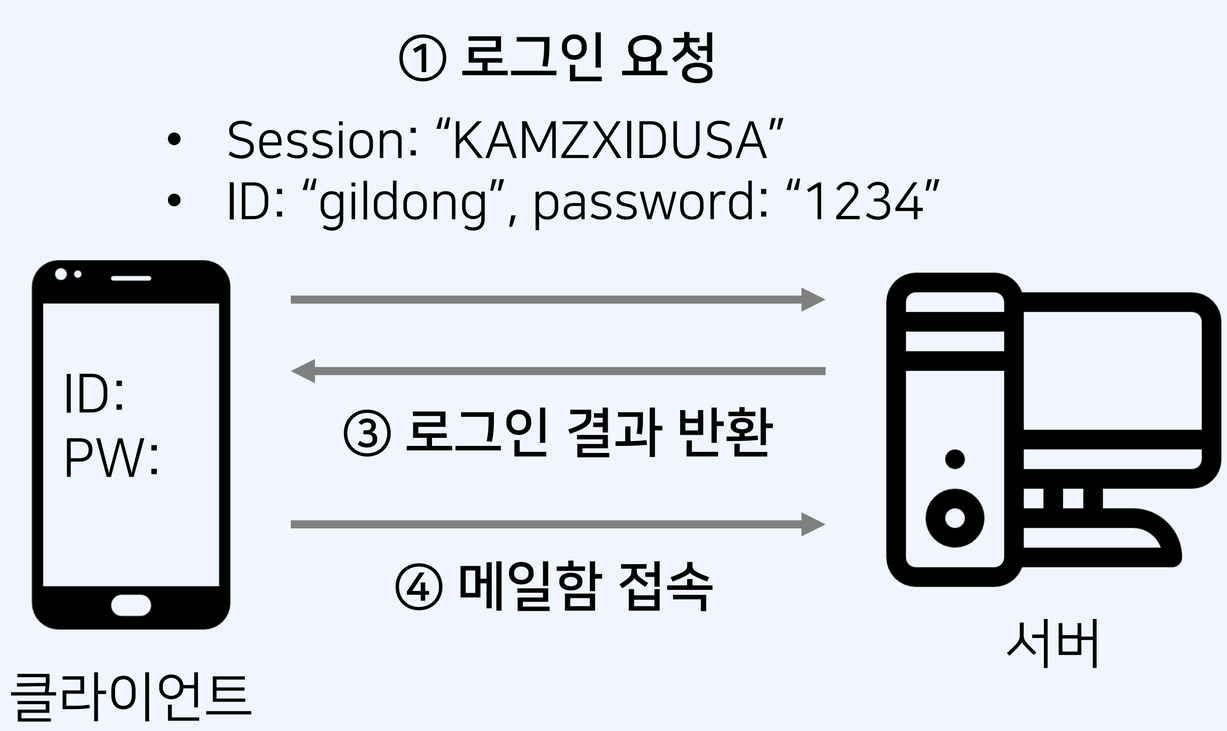
id	“gildong”
password	“1234”
age	30
job	[“programmer”, “dancer”]

```
{
    "id" : "gildong"
    "password" : "1234",
    "age": 30,
    "job": [
        "programmer",
        "dancer"
    ]
}
```

fast campus Copyright FASTCAMPUS Corp.All Rights Reserved

세션(Session) 개요

- 서버에서 가지고 있는 객체로, 특정 사용자의 로그인 정보를 유지하기 위해 사용할 수 있다.



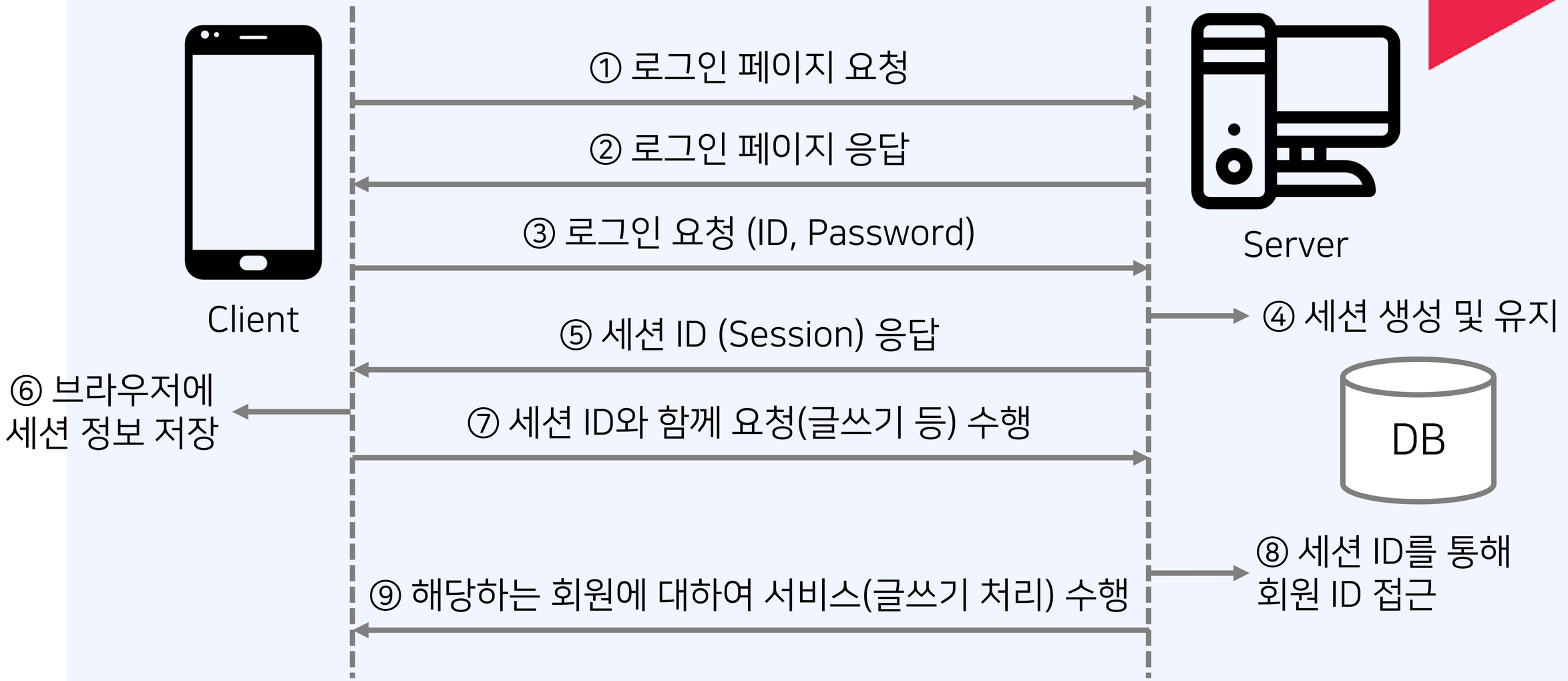
② 세션 정보 기록

Session ID	정보
“JKLAMFJDIS”	ID: “minjeong”, …
“KAMZXIDUSA”	ID: “gildong”, …
…	…

fast campus Copyright FASTCAMPUS Corp.All Rights Reserved

세션(Session) 인증 방식 예시

컴퓨터
공학 지식
웹(Web)



fast campus Copyright FASTCAMPUS Corp.All Rights Reserved

세션(Session) 방식의 특징

[장점]

- 클라이언트에게는 **세션 ID(회원 식별 목적)**을 제공하고, 회원에 대한 중요한 정보를 서버가 가지고 있다.
- 민감한 데이터를 클라이언트에 직접적으로 보내지 않는다.
- 클라이언트 브라우저가 가지고 있는 세션(Session) ID 자체에는 개인정보를 포함하고 있지 않다.

[단점]

- 악의적인 공격자가 세션 ID를 탈취하여 사용자인 척 위장할 수 있다.

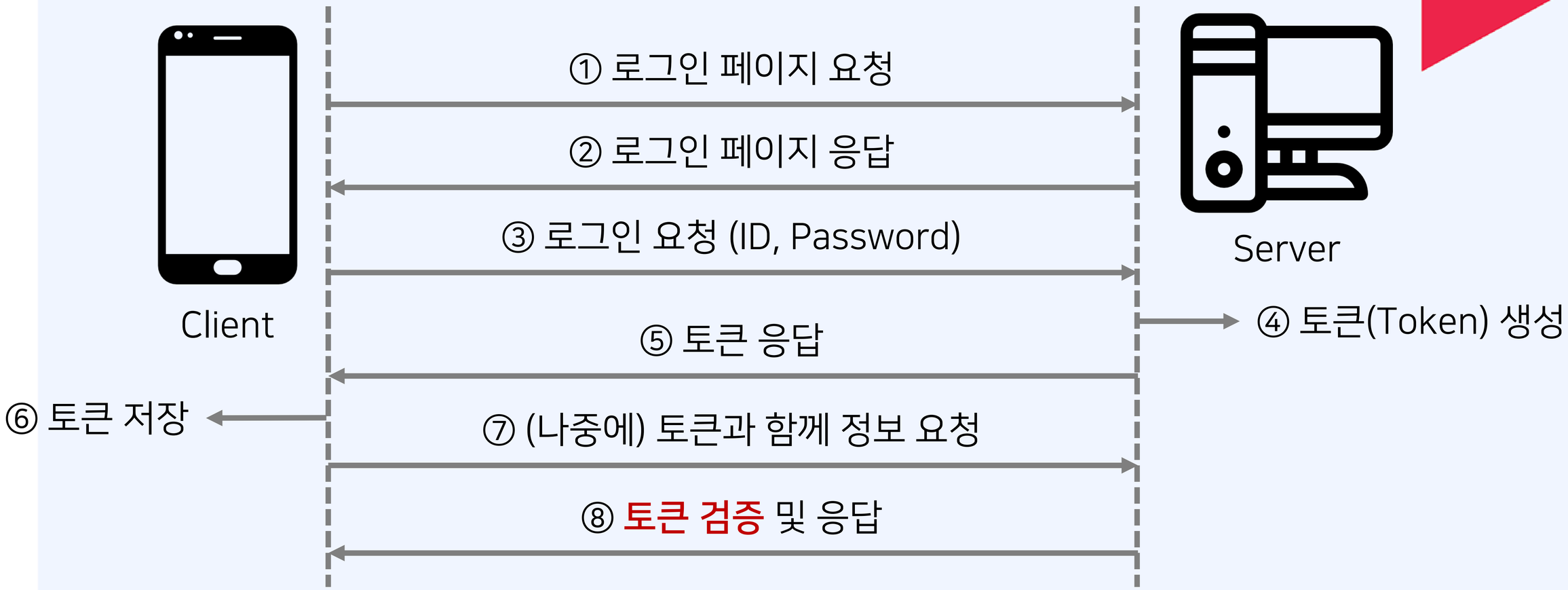
→ 세션 ID를 탈취당하는 경우, 사용자의 많은 권한 및 개인 정보를 탈취당할 수 있다.

- 웹 서버에 세션 정보를 기록하고 있어야 하므로, 접속자가 많을 때 서버에 메모리 부하가 존재할 수 있다.

fast campus Copyright FASTCAMPUS Corp.All Rights Reserved

Token 인증 방식

컴퓨터 공학 지식
웹(Web)



- 토큰에 요청한 사람의 정보가 포함되어, 서버는 DB를 조회하지 않고 토큰을 검증할 수 있다.
- 서버 내부에서는 비밀키(key) 하나만 가지고 있으면, 토큰 검증을 수행할 수 있다.

fast campus Copyright FASTCAMPUS Corp.All Rights Reserved

JWT (JSON Web Token)이란?

컴퓨터
공학 지식
웹(Web)

- JWT는 인증에 필요한 정보를 암호화한 **JSON 형식의 토큰**이다.
- JWT 토큰을 HTTP 헤더에 실어 서버가 클라이언트를 식별할 수 있도록 한다.

fast campus Copyright FASTCAMPUS Corp.All Rights Reserved

JWT (JSON Web Token)이란?

컴퓨터
공학 지식
웹(Web)

- JWT는 세 가지 구성요소(Header, Payload, Signature)를 가진다.
- 사용자가 인증을 수행하면, 서버는 다음의 정보를 가진 JWT 토큰을 발급한다.
- **Header**: 사용할 해시 알고리즘 등의 메타 정보를 포함
- **Payload**: 키(key)와 값(value) 형식으로 이루어진 정보(claim)의 구성

→ 이 값을 서버로 전달한다.

- **Signature**: (헤더 + 페이로드 + 키(key)) 정보를 **해싱하여** Client에게 함께 전달한다.

xxxxx[Header].yyyyy[Payload].zzzzz[Signature]

fast campus Copyright FASTCAMPUS Corp.All Rights Reserved

JWT 예시

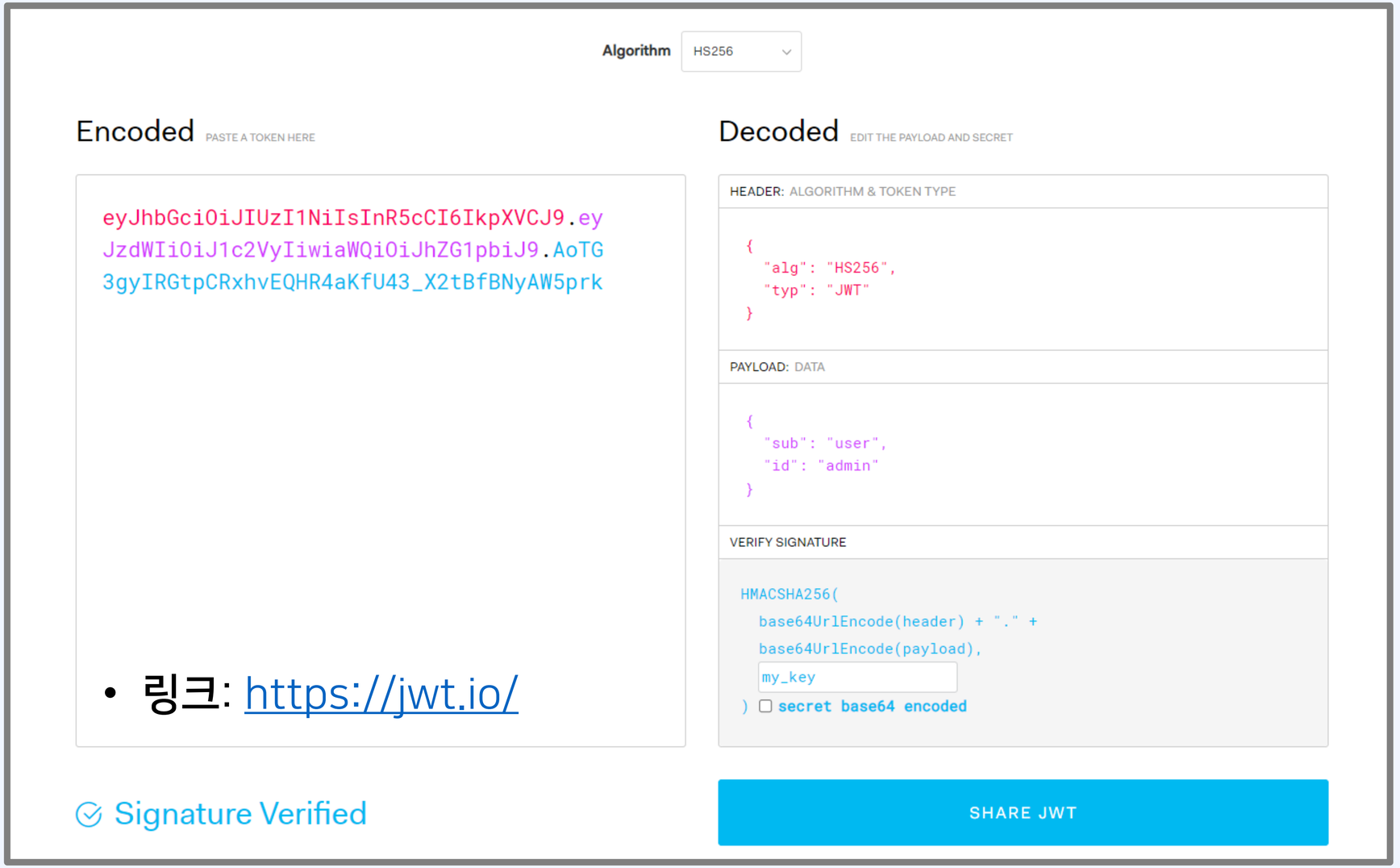
컴퓨터
공학 지식
웹(Web)

- **Header**: {"alg": "HS256", "typ": "JWT"}
- **Payload**: {"sub": "user", "id": "admin"}
- **Signature**: 위 두 내용에 대하여 적절한 서버 키(key) 값을 더해 해싱한 값

fast campus Copyright FASTCAMPUS Corp.All Rights Reserved

JWT 예시

컴퓨터
공학 지식
웹(Web)



- 링크: https://jwt.io/

fast campus Copyright FASTCAMPUS Corp.All Rights Reserved

JWT를 이용한 인증

컴퓨터
공학 지식
웹(Web)

- 나중에 사용자(client)는 자신이 받았던 **JWT 토큰**을 다시 서버에 전달한다.
- 서버는 (헤더 + 페이로드 + 서버 내에 있는 키(Key))를 **해싱한 값**이 사용자로부터 전달받은 것과 일치하는지 체크한다.
- 이 과정에서 서버가 가지고 있는 **비밀키(secret key)**를 사용한다.

fast campus Copyright FASTCAMPUS Corp.All Rights Reserved

JWT 인증 원리

컴퓨터
공학 지식
웹(Web)

- 사용자는 서버가 처음에 부여했던 **권한**만큼의 작업을 요청할 수 있다.
- 데이터를 변경하면 **해시 값이 변경**되므로, 악의적인 공격자가 Payload를 수정하는 것이 불가능하다.
- 예를 들어 사용자의 등급이 1, 2, 3, 4, 5일 때 5등급의 사람이 1등급으로 Payload를 변경해 보냈다고 해보자. 이 경우, **서버의 키**를 모르므로, 서명 값이 일치하지 않아 서버가 **위조 여부**를 알 수 있다.

fast campus Copyright FASTCAMPUS Corp.All Rights Reserved

JWT 방식의 특징

[장점]

- 세션 기반 인증 방식에 비해 서버(Server)가 DB에 세션 정보를 가지고 있을 필요가 없다.
- 각 해시 값이 어떤 Header와 Payload를 가지는지 일일이 서버 DB에서 저장할 이유가 없다.

→ 서버에서 상태 정보를 저장하지 않아도 되므로, 무상태성(stateless)이 유지된다.

- 토큰 기반이므로, 서로 다른 웹 서버에 대해서도 동작할 수 있다. (웹 브라우저의 쿠키와 다른 점)

[단점]

- 세션에 비하여 토큰 자체의 데이터 길이가 길다.
- 페이로드(payload)는 암호화되지 않으므로, 중요한 정보를 담기 적절하지 않을 수 있다.
- 토큰을 탈취당하는 경우 보안상의 문제가 발생할 수 있다. (때문에 토큰에 사용 기한을 부여한다.)

fast campus Copyright FASTCAMPUS Corp.All Rights Reserved

JWT 토큰의 유의사항

컴퓨터
공학 지식
웹(Web)

[JWT 토큰의 유의사항]

- Payload 자체는 중간자 공격에 의해 노출될 수 있으므로, 페이로드에는 가능한 민감 정보를 넣지 않는다.
- 기본적으로 JWT의 목적은 오직 정보 보호보다는 다음의 목적에 가깝다.

1. 위조 방지
2. 서버의 메모리 가용 이점(DB 조회 필요 없음)

fast campus Copyright FASTCAMPUS Corp.All Rights Reserved

실제 인증 방식 사례