

(HTTP 완벽 가이드) III. 식별, 인가, 보안

사용자를 식별하여 콘텐츠를 개인화 시키는 기법

11 클라이언트 식별과 쿠키



김수빈(kimziou77@naver.com)

2022.03.08.

- ✓ 11.1 개별접촉
- ✓ 11.2 HTTP헤더
- ✓ 11.3 클라이언트 IP주소
- ✓ 11.4 사용자 로그인
- ✓ 11.5 뚱뚱한 URL
- ✓ 11.6 쿠키

11.1 개별접촉

11.1 개별 접촉

✓ 개별인사

- 사용자에게 특화된 환영 메시지나 페이지 내용을 만든다.

✓ 사용자 맞춤 추천

- 고객이 좋아할 것이라고 예상되는 제품들을 추천

✓ 저장된 사용자 정보

- 온라인 쇼핑이 당신을 한번 식별하고 나면, 저장된 사용자 정보를 사용할 수 있다.
- 복잡한 주소와 신용카드 정보를 데이터베이스에 저장 등

✓ 세션추적

- HTTP 트랜잭션은 상태가 없다. (Stateless, 무상태성) ★ ★ ★ ★ ★
- 웹사이트는 각 사용자에게서 오는 HTTP 트랜잭션을 식별 방법이 필요

11.2 HTTP 헤더

11.2 HTTP 헤더

✓ From 헤더

- 각 사용자는 서로 다른 이메일 주소를 가짐 - 사용자 식별 가능
- 문제점 : 악성 서버의 스팸메일 발송문제
- 웹로봇이 문제 일으켰을때 대처

✓ User-Agent 헤더

- 브라우저 이름, 버전정보, 운영체제 정보 등
- 특정 브라우저 식별 o / 특정 사용자 식별은 큰 도움 x

user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36

✓ Referer 헤더

- 현재 페이지로 유입하게 한 웹 페이지의 URL
- 사용자 식별 x / 사용자의 웹 사용 행태 · 취향 파악 o

가장 일반적인 일곱가지 HTTP요청 헤더

헤더 이름	헤더 타입	설명
Form	요청	사용자의 이메일 주소
User-Agent	요청	→ 사용자를 확실히 식별하기엔 부족하다
Referer	요청	사용자가 현재 링크를 타고 온 근원 페이지
Authorization	요청	사용자 이름과 비밀번호
Client-ip	확장(요청)	클라이언트의 IP 주소
X-Forwarded-For	확장(요청)	클라이언트의 IP 주소
Cookie	확장(요청)	서버가 생성한 ID 라벨

표 11-1 사용자에게 대한 정보를 전달하는 HTTP 헤더

11.3 클라이언트 IP 주소

11.3 클라이언트 IP 주소 : 개요

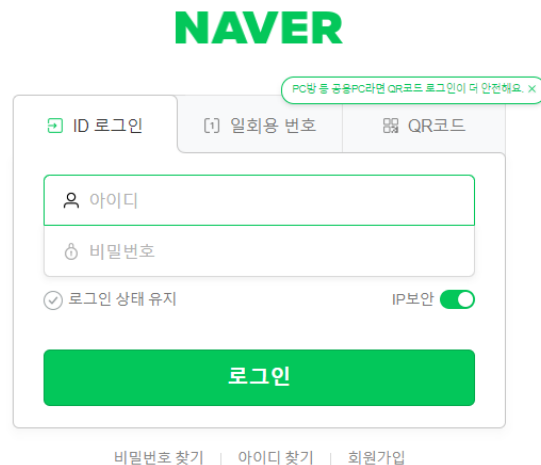
- ✓ 사용자는 IP주소를 가지고 있고, 이 주소가 잘 바뀌지 않는다.
- ✓ 웹 서버는 반대쪽 TCP 커넥션의 IP 주소를 알아낼 수 있다.

11.3 클라이언트 IP 주소 : 약점

- ✓ 클라이언트 IP 주소는 사용자가 아닌, 사용하는 컴퓨터를 가리킨다.
- ✓ 많은 인터넷 서비스 제공자(ISP)는 사용자가 로그인하면 동적으로 IP주소를 할당한다.
 - 로그인한 시간에 따라, 사용자는 매번 다른 주소를 받으므로, 웹 서버는 사용자를 IP주소로 식별할 수 없다.
- ✓ 흔히 네트워크 주소 변환 (Network Address Translation, NAT) 방화벽을 통해 인터넷 사용
 - 클라이언트의 실제 IP주소를 방화벽 뒤로 숨기고, 클라이언트의 실제 IP 주소를 내부에서 사용하는 하나의 방화벽 IP주소 (&포트번호) 로 변환한다.
- ✓ 웹 서버는 클라이언트의 IP주소 대신 프락시서버의 IP주소를 본다.

11.4 사용자 로그인

웹 서버는 사용자 이름과 비밀번호로 인증(로그인)할 것을 요구해서 사용자에게 명시적으로 식별 요청을 할 수 있다.

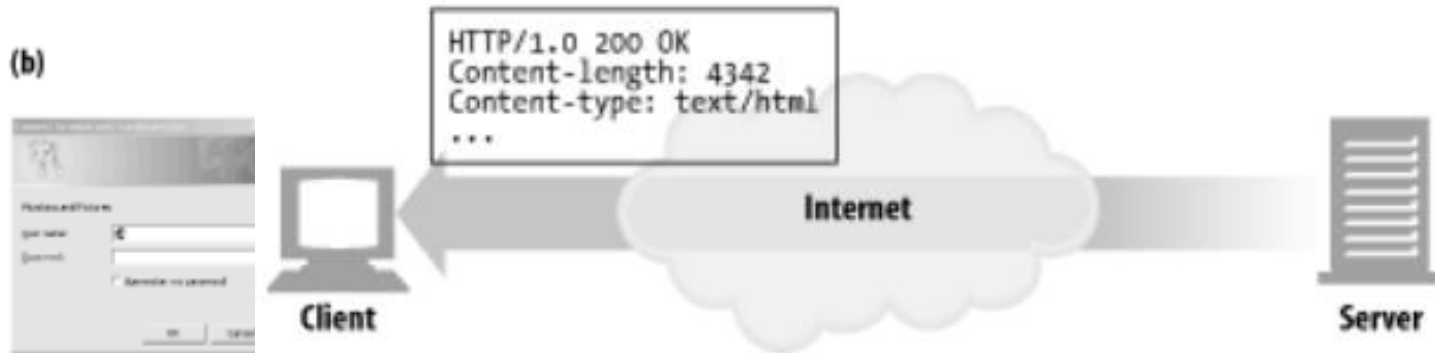


The image shows the Naver login interface. At the top is the 'NAVER' logo in green. Below it is a warning banner: 'PC방 등 공용PC라면 QR코드 로그인이 더 안전해요. X'. The login form has three tabs: 'ID 로그인' (selected), '[1] 일회용 번호', and 'QR코드'. The 'ID 로그인' tab contains two input fields: '아이디' (ID) and '비밀번호' (Password). Below these fields are two checkboxes: '로그인 상태 유지' (checked) and 'IP보안' (unchecked). A large green '로그인' (Login) button is at the bottom. At the very bottom, there are links: '비밀번호 찾기' (Find Password), '아이디 찾기' (Find ID), and '회원가입' (Sign Up).

11.4 사용자 로그인 : 개요

- ✓ HTTP는 웹 사이트에 사용자 이름을 전달하는 자체적인 체계를 가지고 있다.
 - WWW-Authenticate 헤더
 - Authorization 헤더
- ✓ 브라우저는 사이트로 보내는 요청에 이 로그인 정보를 함께 보낸다.

11.4 사용자 로그인 : 과정



11.4 사용자 로그인 : 단점

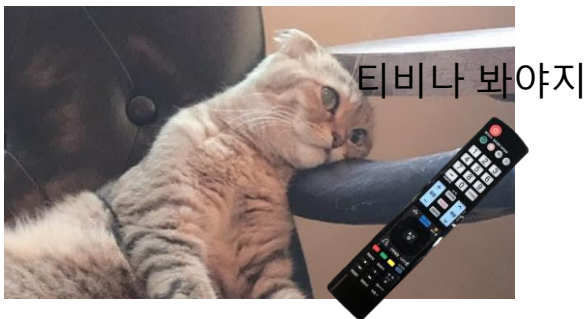
- * 8~12자 이내 영문,숫자,특수문자 중 2가지 이상을 조합해야 합니다.
- * 사용 불가 특수 문자: ' " + / \ ; : - _ ^ & () < > 제외

✓ 로그인은 귀찮다

- 이용하는 각 사이트에 로그인을 해야한다
- 서로 다른 로그인 정보(아이디, 비밀번호)를 기억해야 한다.
 - 아이디 선점 문제
 - 서로 다른 비밀번호 조합규칙

※ 비밀번호 설정 안내

비밀번호는 10~20자의 영문 대소문자, 숫자, 일부 특수기호만 사용할 수 있습니다. (사용 가능한 특수기호: !@#\$%^&*()-_+=|~`~?~<~>)
 설정할 수 없는 비밀번호 조합: 공백, 3자 이상 연속된 영문 혹은 숫자, 아이디에 포함된 문자/숫자와 연속 3자 이상 동일한 경우 유추하기 쉬운!
 한 비밀번호를 사용하면 포인트 도용의 위험이 있습니다.



11.5 뚱뚱한 URL

11.5 뚱뚱한 URL

- ✓ 사용자의 상태정보를 포함하고 있는 URL
- ✓ URL은 URL경로의 처음이나 끝에 상태정보를 추가해 확장한다
 - 사용자가 그 사이트를 돌아다니면, 웹 서버는 URL에 있는 상태 정보를 유지하는 하이퍼링크를 동적으로 생성한다.
- ✓ HTTP 트랜잭션을 하나의 '세션' 혹은 '방문'으로 묶는 용도
 - 사용자가 웹 사이트에 처음 방문하면 유일한 ID가 생성되고, 그 값은 서버가 인식할 수 있는 방식으로 URL에 추가되며, 서버는 클라이언트를 이 뚱뚱한 URL로 리다이렉트 시킨다.
- ✓ 밖으로 향하는 모든 하이퍼링크를 뚱뚱한 URL로 바꾼다.
 - ID와 관련된 추가적인 정보(쇼핑카트, 프로필 등)를 찾는다

11.5 뚱뚱한 URL

✓ 못생긴 URL

✓ 공유하지 못하는 URL

- 뚱뚱한 URL은 특정 사용자와 세션에 대한 상태정보를 포함한다.

- 만약 그 주소를 누군가에게 메일로 보내면, 당신의 누적된 개인 정보를 본의 아니게 공유하게 되는 것이다.

✓ 캐시를 사용할 수 없음

- URL로 만드는 것은, URL이 달라지기 때문에 기존 캐시에 접근할 수 없다는 것을 의미한다.

✓ 서버 부하 가중

- 서버는 뚱뚱한 URL에 해당하는 HTML 페이지를 다시 그려야 한다.

✓ 이탈

- 사용자가 링크를 타고 다른 사이트로 이동하거나 특정 URL을 요청해서 의도치않게 뚱뚱한 URL 세션에서 '이탈'하기 쉽다.

- 사용자가 이탈하게 되면, 지금까지의 진척상황들(아마도 상품으로 채워진 쇼핑 장바구니)이 초기화 되고 다시 처음부터 시작해야 될 것이다.

11.6 쿠키

11.6.1 쿠키의 타입

11.6.2 쿠키는 어떻게 동작하는가

11.6.3 쿠키 상자: 클라이언트 측 상태

11.6.4 사이트마다 각기 다른 쿠키들

11.6.5 쿠키 구성요소

11.6.6 Version 0 (넷스케이프) 쿠키

11.6.7 Version 1 (RFC 2965) 쿠키

11.6.8 쿠키와 세션추적

11.6.9 쿠키와 캐싱

11.6.10 쿠키, 보안 그리고 개인정보



3부 식별 · 인가 · 보안

**Cookie
Storage**



**Session
Token**

11.6.0 식별 · 인가 · 보안

✓ 인증 (Authentication)

- 내가 누구인가? (식별)
- 로그인하기

✓ 인가 (Authorization)

- 인증된 '내'가 '할 수 있는 일'은 무엇인가?
- 인증된 정보로 사용할 수 있는 권한

11.6.1 쿠키 (1/3)

- ✓ 넷스케이프 최초 개발
- ✓ Set-Cookie : {name}={value} ; path={경로}; expires={날짜}
- ✓ Cookie: {name}={value}; {name2}={value2}; {name3}={value3}
- ```
cookie: _ga=GA1.2.1989652959.1642644461; _gid=GA1.2.97710506.1646670150; lux_uid=164670839256621723
```
- ✓ 브라우저에 저장되는 작은 크기의 문자열로 최대 4KB까지 저장
- ✓ 같은 도메인에서 만든 쿠키만 전송



## 11.6.1 쿠키 (2/3)

### ✓ 쿠키의 종류

- 세션 쿠키
  - 만료기간 X (탭닫으면삭제)
- 지속 쿠키
  - 만료기간 O (기간동안 재부팅, 탭닫기 해도 유지됨)
- 퍼스트파티 쿠키
  - 같은 도메인&서브 도메인 쿠키
- 서드파티 쿠키
  - 다른 도메인 쿠키

### 일반 설정

☐ 모든 쿠키 허용

☒ 시크릿 모드에서 타사 쿠키 차단



사이트에서 사용자의 로그인 상태를 유지하거나 장바구니 개선하기 위해 쿠키를 사용할 수 있습니다.



시크릿 모드에 있는 동안에는 사이트에서 사용자의 다양한 설정 등의 작업을 하는 데 쿠키를 사용할 수 없습니다. 일 수 있습니다.

☐ 타사 쿠키 차단

☐ 모든 쿠키 차단(권장되지 않음)

모든 창이 닫히면 쿠키 및 사이트 데이터 삭제

탐색 트래픽과 함께 '추적 안함' 요청 전송

## 11.6.1 쿠키 (3/3)

일반 설정

☐ 모든 쿠키 허용

▼

☒ 시크릿 모드에서 타사 쿠키 차단

▲



사이트에서 사용자의 로그인 상태를 유지하거나 장바구니에 담긴 상품을 기억하는 등 탐색 환경을 개선하기 위해 쿠키를 사용할 수 있습니다.



시크릿 모드에 있는 동안에는 사이트에서 사용자의 다양한 사이트 탐색 활동 정보를 이용해 광고 및 추천 등 작업하는 데 쿠키를 사용할 수 없습니다. 일부 사이트에서는 기능이 작동하지 않을 수 있습니다.

☐ 타사 쿠키 차단

▼

☐ 모든 쿠키 차단(권장되지 않음)

▼

모든 창이 닫히면 쿠키 및 사이트 데이터 삭제

☐

탐색 트래픽과 함께 '추적 안함' 요청 전송

☐

## 11.6.2 스토리지 (1)

---

- ✓ HTML5에서 제공한 웹스토리지 기능
- ✓ 브라우저에 저장되는 문자열로 최대 5MB까지 저장
- ✓ 만료기간 설정 불가능
- ✓ 웹브라우저 버전에 따라 지원 안할수도 있음

## 11.6.2 스토리지 (2)

---

### ✓ 스토리지 종류

- 세션 스토리지
  - 직접 삭제하기 전까지 계속 유효 (도메인, 브라우저 범위)
- 로컬스토리지
  - 탭 종료시 삭제 (탭, 도메인, 브라우저 범위)



## 11.6 쿠키와 스토리지

---

### ✓ 세션 쿠키

- 탭 종료시 삭제

### ✓ 지속 쿠키

- 만료기간동안 유지

→ **4KB, 만료기간 설정 가능**

### ✓ 세션 스토리지

- 탭 종료시 삭제

### ✓ 로컬 스토리지

- 직접 삭제

→ **5MB, 만료기간 설정 불가능**

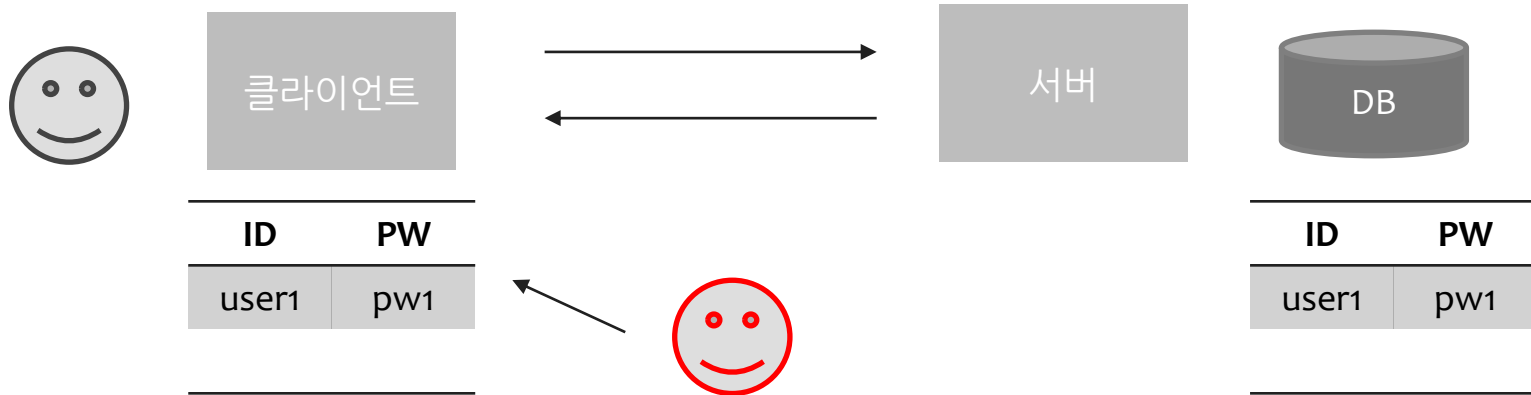
### 11.6.3 인증과 인가 (1/2)

---

- ✓ 사용자를 식별함으로써 콘텐츠의 개인화, 편리성 증가
- ✓ 사용자를 식별하기 위한 로그인 기술
- ✓ 로그인된 정보를 유지하는 기술

## 11.6.3 인증과 인가 (2/2)

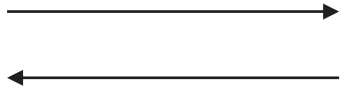
✓ 클라이언트에 저장?



## 11.6.3 세션



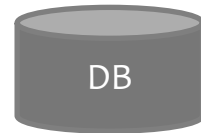
클라이언트



서버

서버

서버



DB

ID

PW

user1

pw1

key

value

세션

세션ID

세션DB

SESSION ID

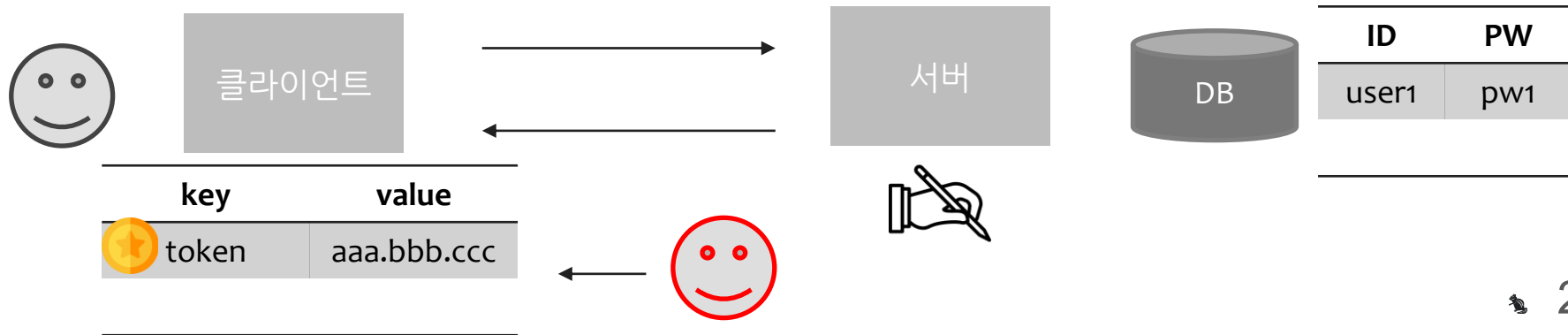
user

세션ID

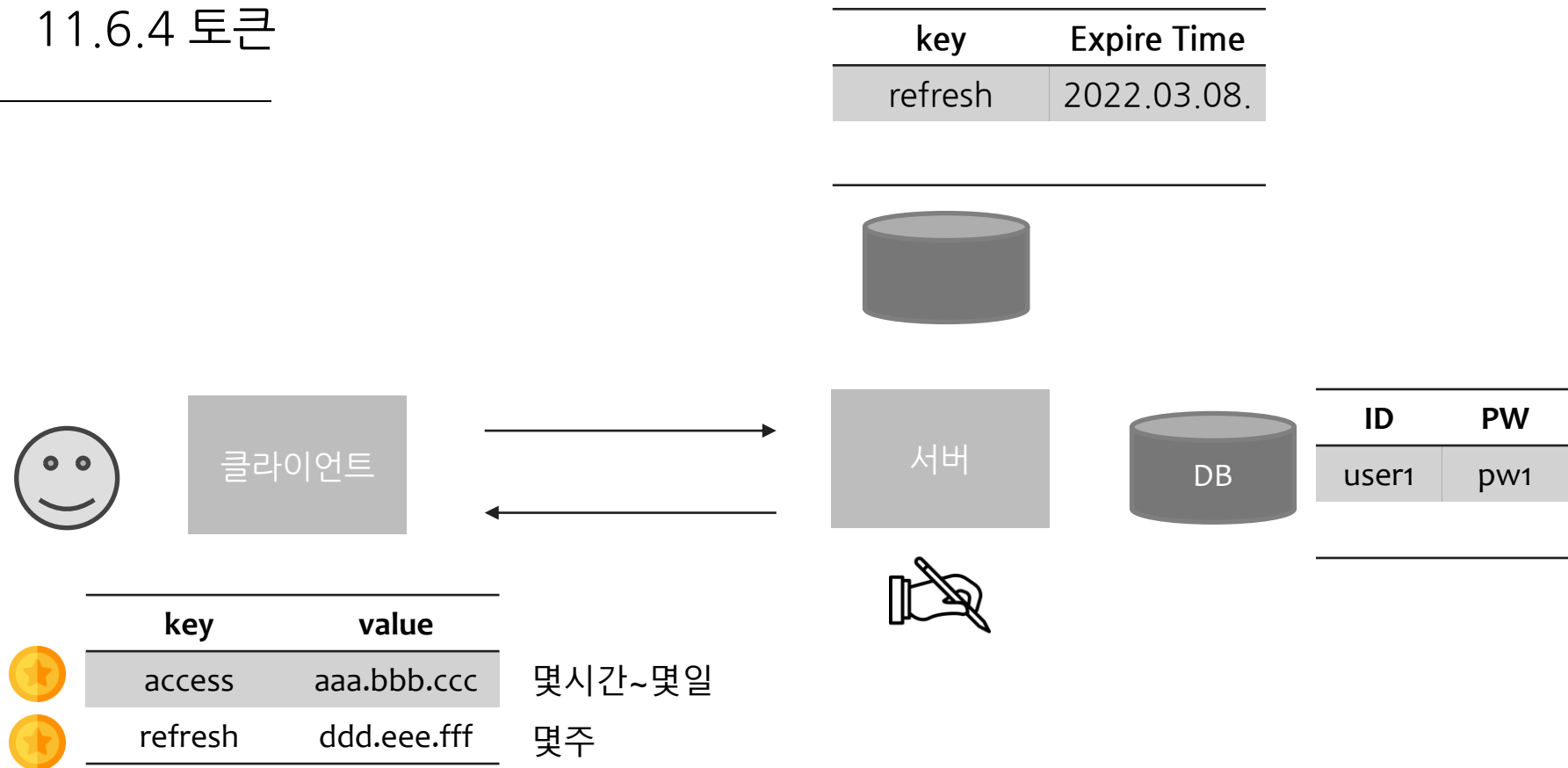
user1

## 11.6.4 토큰

- ✓ 구성 : [헤더. 페이로드. 서명]
- ✓ JWT (Json Web Token)



## 11.6.4 토큰



## 11.6 세션과 토큰

---

### ✓ 세션

- 로그인 된 모든 유저의 정보를 추적
- DB관리 뻥셈
- 계정공유 숫자 제한, 악의적인 사용자 퇴출

### ✓ 토큰

- 생성된 토큰을 추적하지 않고 토큰의 유효성만 검사
- 위처럼 그다지 뻥센 인증이 필요하지 않은경우 간단히 사용

# 3부 식별 · 인가 · 보안

→ 인증 · 인가

**Cookie  
Storage**

→ 브라우저 저장소



**Session  
Token**

→ 서버가 우리를 기억하는 방식

+OAuth





# 출처

---

- ✓ [토니의 인증과 인가](#)
- ✓ [디토의 웹스토리지 & 쿠키](#)
- ✓ [쿠키, 세션, 캐시가 무엇인가요?](#)
- ✓ [세션vs토큰vs쿠키? 노마드코더](#)
- ✓ HTTP완벽가이드
- ✓ [MDN Web docs](#)

QnA